YAGYAM BATRA
A004

DATE: / /
PAGE:

① Users and groups:

① **Users**: 1) Individuals who can log in to a cloud service with unique credentials

Access control: Users are assigned specific permissions to determine what resources and actions they can access.

Authentication and Authorization: Verifying user identity and granting appropriate permissions.

② **Groups**: 1) A collection of users with similar access rights and permissions

Simplified management: Groups allow administration to manage access rights efficiently by assigning permissions to multiple users at once.

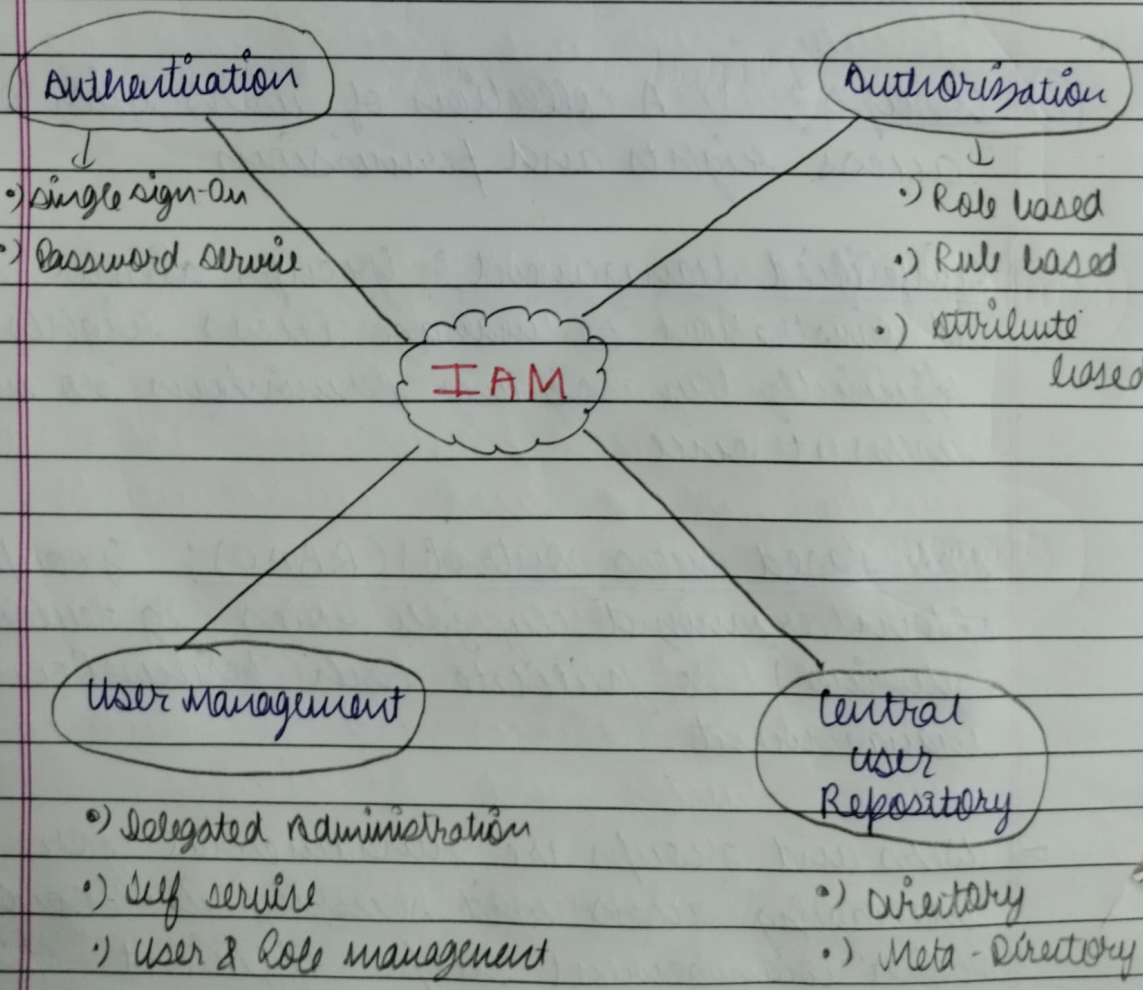
Role Based Access control (RBAC): Groups are often organized by job roles (eg developers, admins) to facilitate easy permission management.

⇒ Users and groups are fundamental for managing access and security in cloud env. Proper management helps efficient operations, enhanced security, and compliance with regulatory requirements.

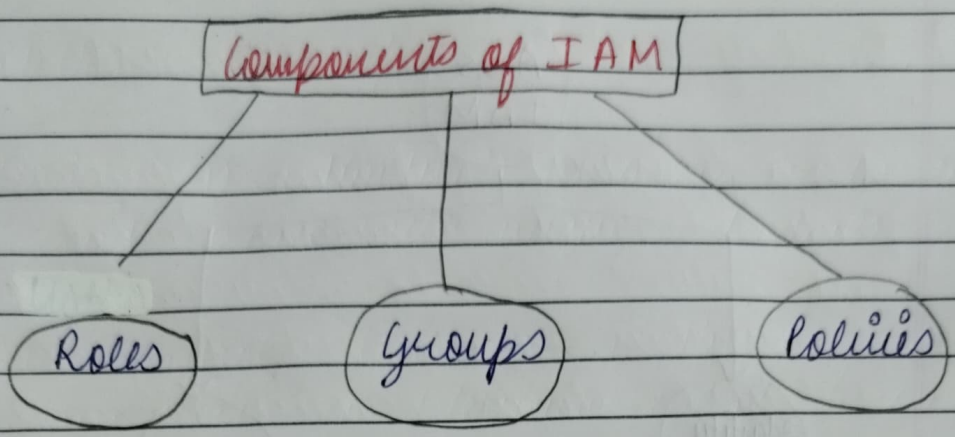
DATE: / /
PAGE:

② Identity and Access Management (IAM):

It is a framework of policies, technologies, and practices designed to manage digital identities and control access to resources within an organization. In the context of CC, It plays a crucial role in securing access to cloud services and ensuring that only authorized users and services have the necessary permissions to perform actions on cloud resources.



DATE: / /
PAGE:



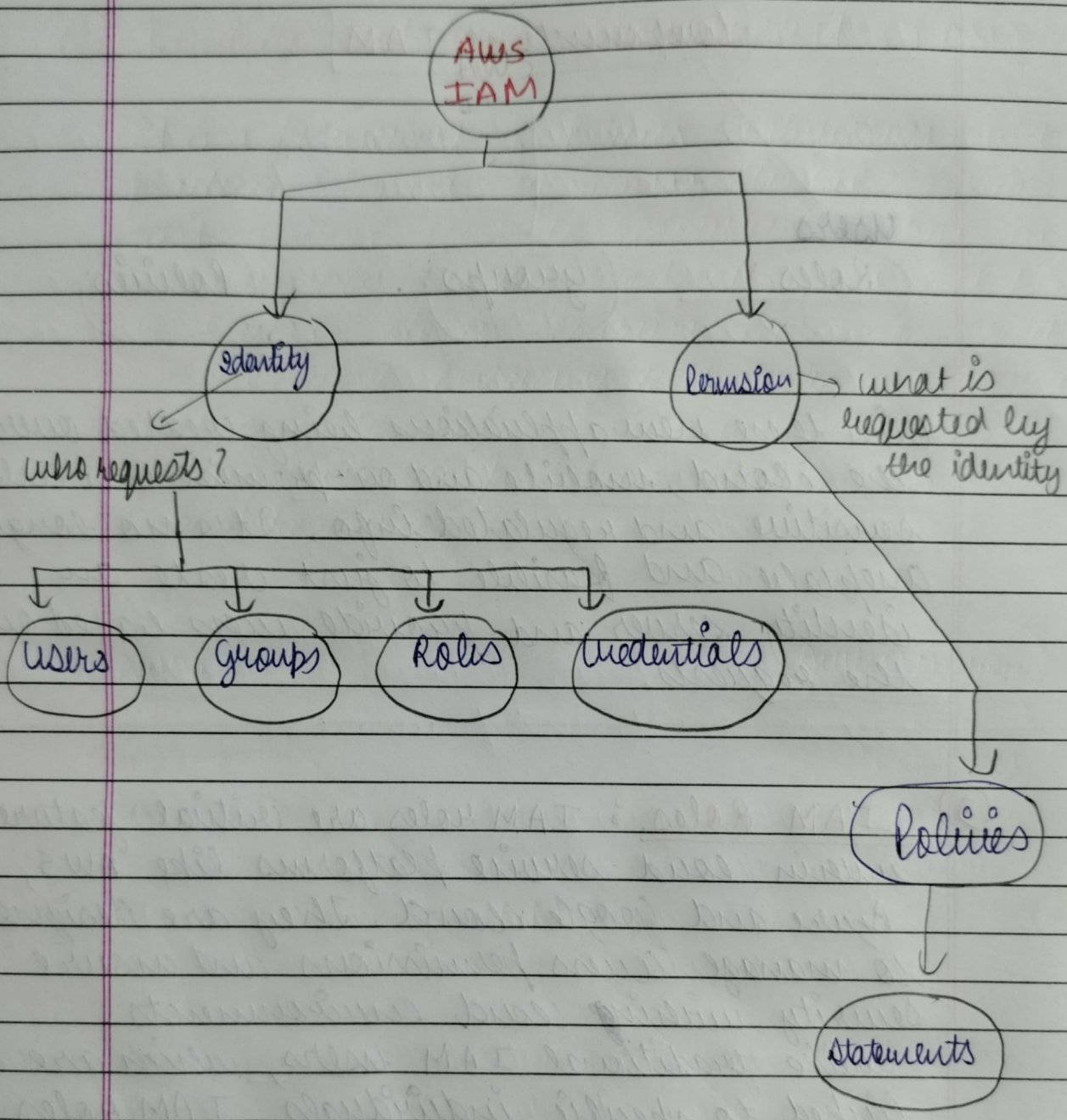
With these new applications being created over the cloud, mobile and on-premise can hold sensitive and regulated info. It is no longer acceptable and feasible to just create an identity server and provide axes based on the requests.

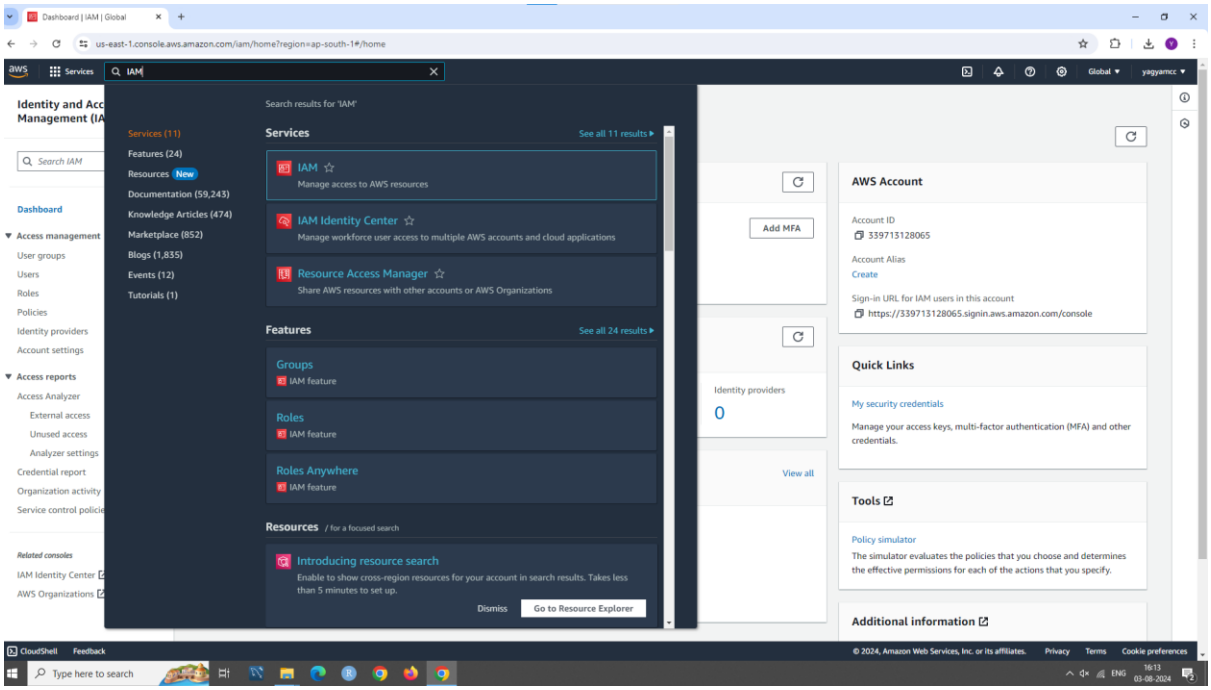
(3) **IAM Roles**: IAM roles are critical feature within cloud service platforms like AWS, Azure and Google cloud. They are designed to manage axess permissions and ensure security within cloud environments. Unlike traditional IAM users, which are linked to specific individuals, IAM roles provide temprory credentials that can be used by various entities, including users, services, and applications.

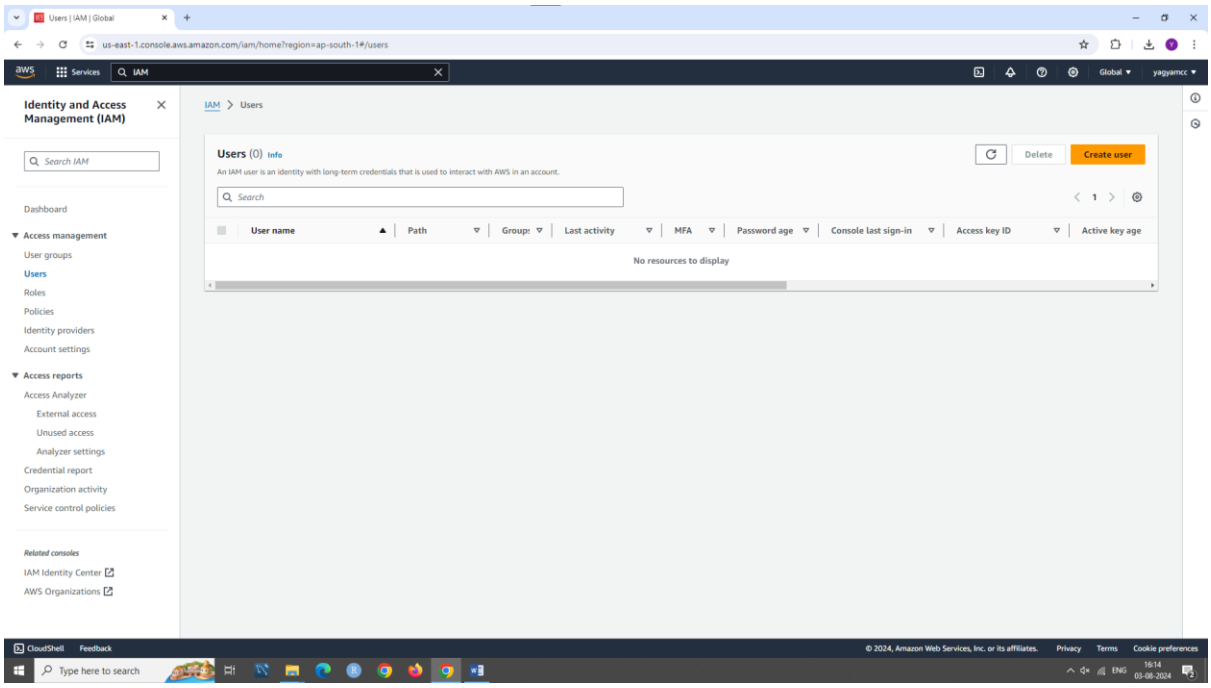
Use cases: 1) Services Axess: Allowing AWS services like EC2 etc.

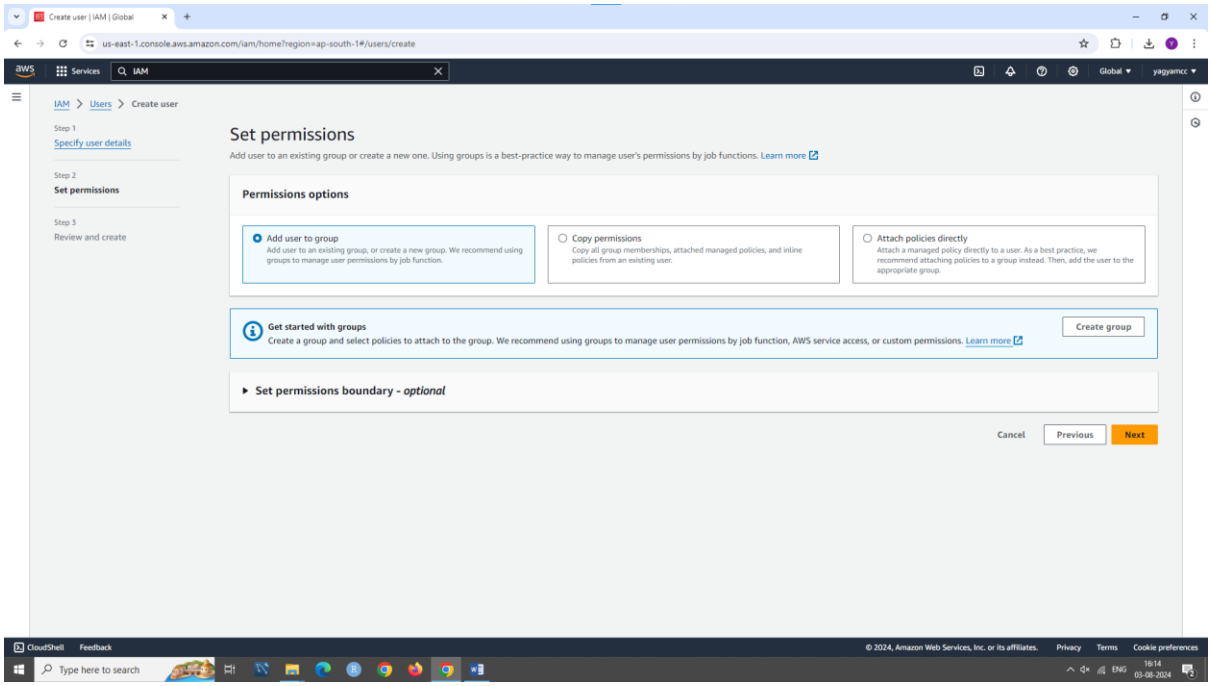
2) Temporary Usage Axess: Granting short term axess.

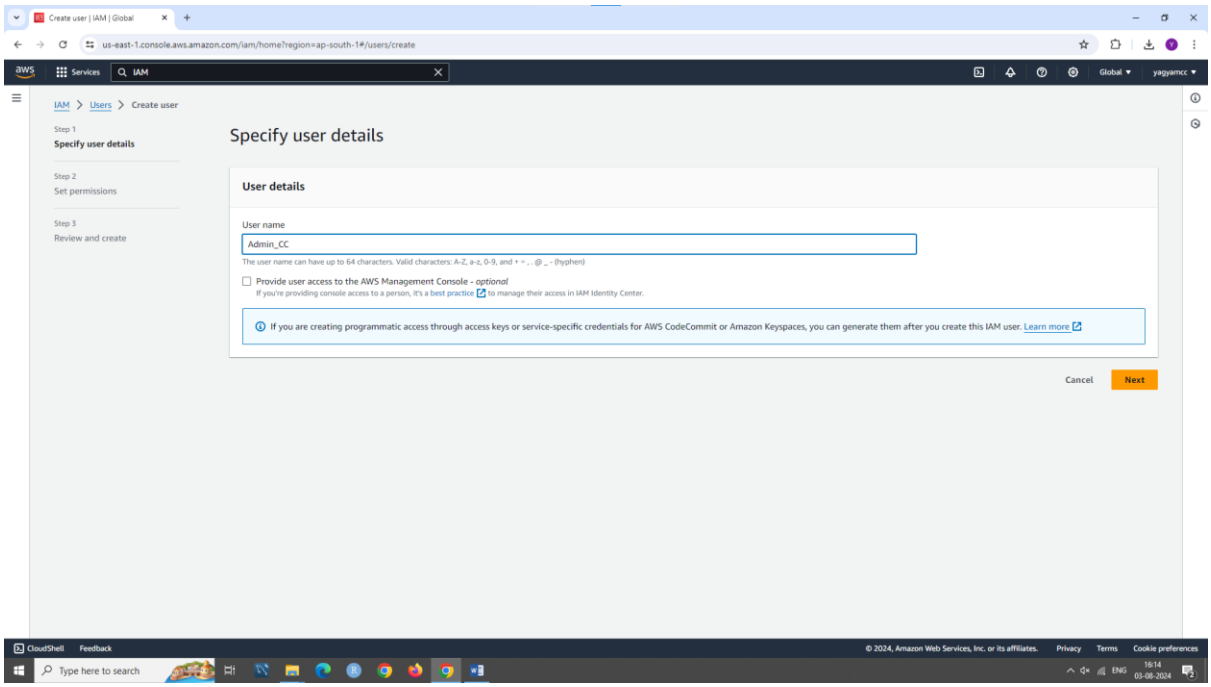
DATE: / /
PAGE:

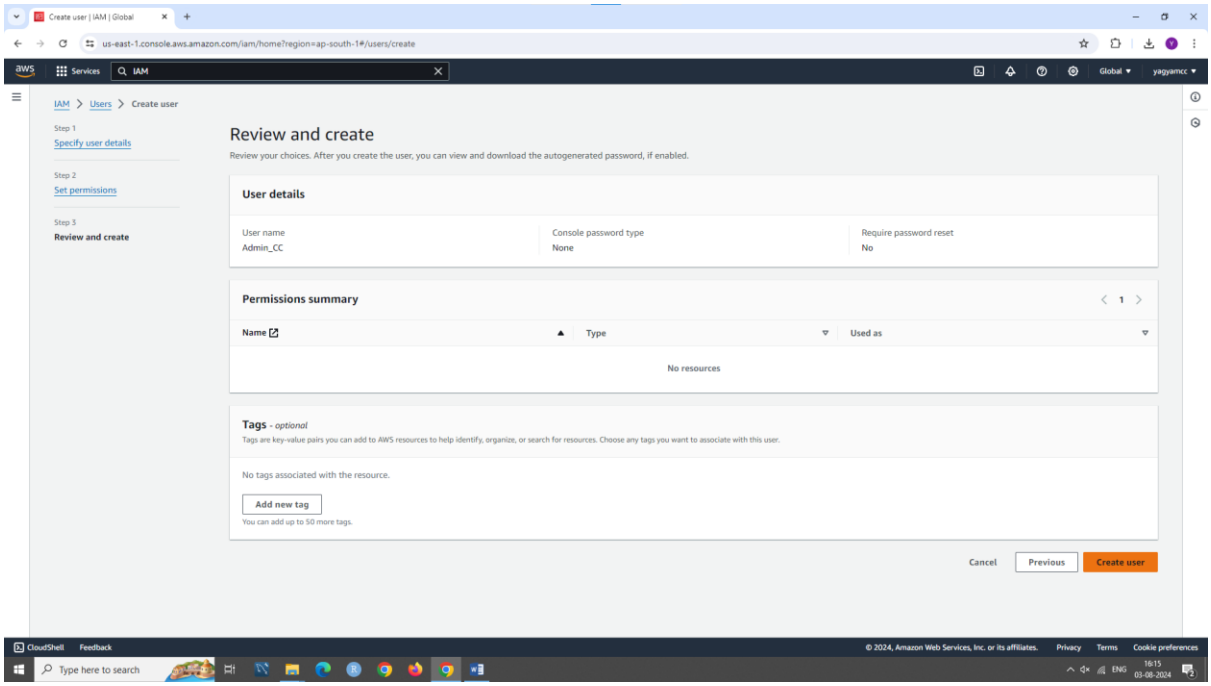

AWS IAM
Identity
Permission
what is requested by the identity
who requests ?
Users
Groups
Roles
Credentials
Policies
Statements

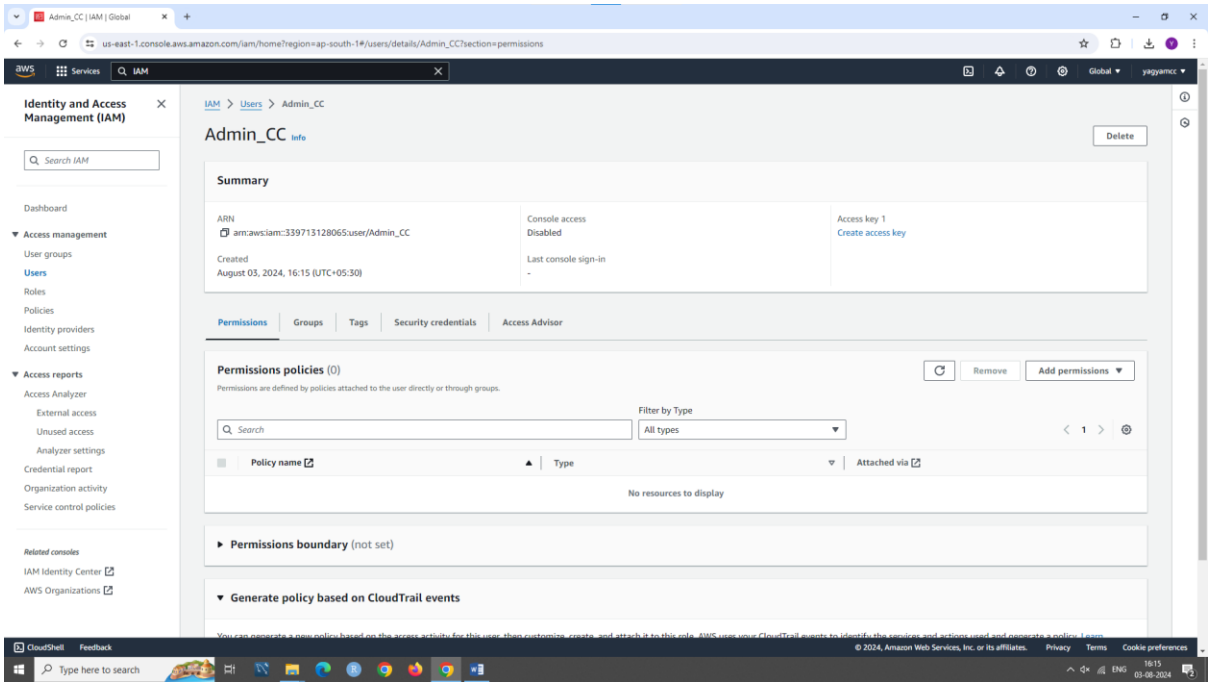

Dashboard | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/home
Services
IAM
Global
yagyamcc
Search results for 'IAM'
Services (11)
Features (24)
Resources New
Documentation (59,243)
Knowledge Articles (474)
Marketplace (852)
Blogs (1,835)
Events (12)
Tutorials (1)
Services
See all 11 results
IAM
Manage access to AWS resources
IAM Identity Center
Manage workforce user access to multiple AWS accounts and cloud applications
Resource Access Manager
Share AWS resources with other accounts or AWS Organizations
Features
See all 24 results
Groups
IAM feature
Roles
IAM feature
Roles Anywhere
IAM feature
Resources / for a focused search
Introducing resource search
Enable to show cross-region resources for your account in search results. Takes less than 5 minutes to set up.
Dismiss
Go to Resource Explorer
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
AWS Organizations
Add MFA
Identity providers
0
View all
AWS Account
Account ID
339713128065
Account Alias
Create
Sign-in URL for IAM users in this account
https://339713128065.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
Additional information
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:13
03-08-2024

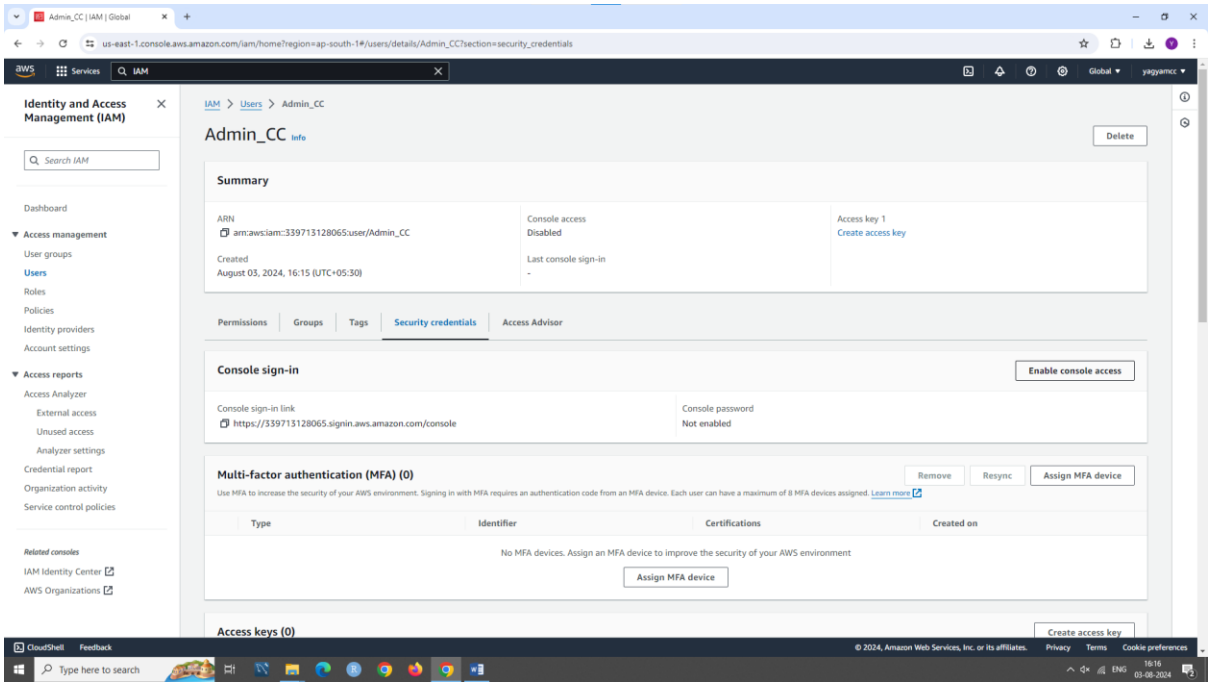

Users | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
IAM > Users
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Group
Last activity
MFA
Password age
Console last sign-in
Access key ID
Active key age
No resources to display
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:14
03-08-2024

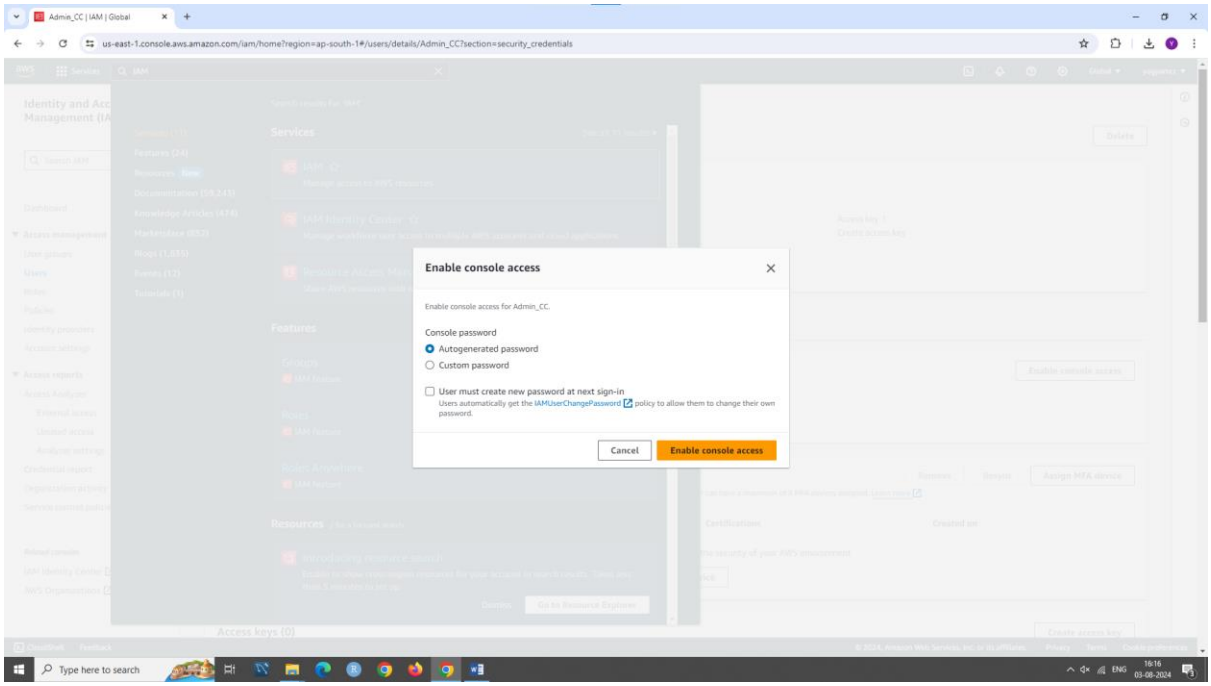

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Services
IAM
Global
yagyamcc
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set permissions
Add user to an existing group or create a new one. Using 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:14
03-08-2024

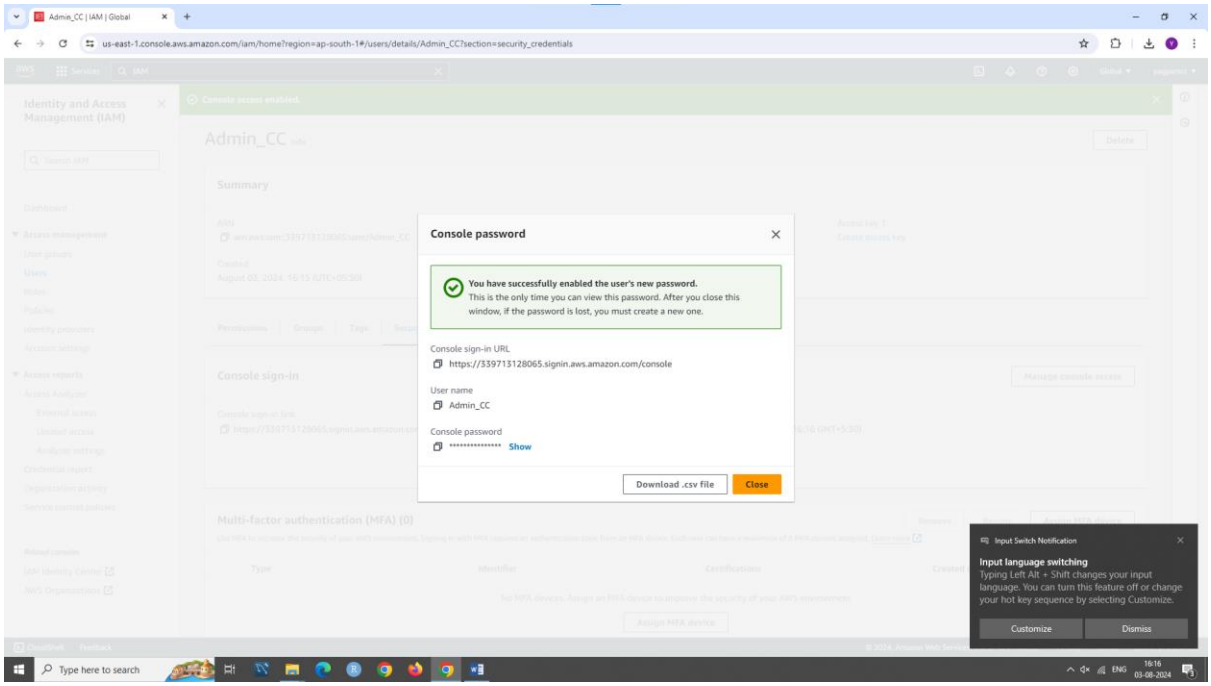

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Services
IAM
Global
yagyamcc
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
Admin_CC
The user name can 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:14
03-08-2024

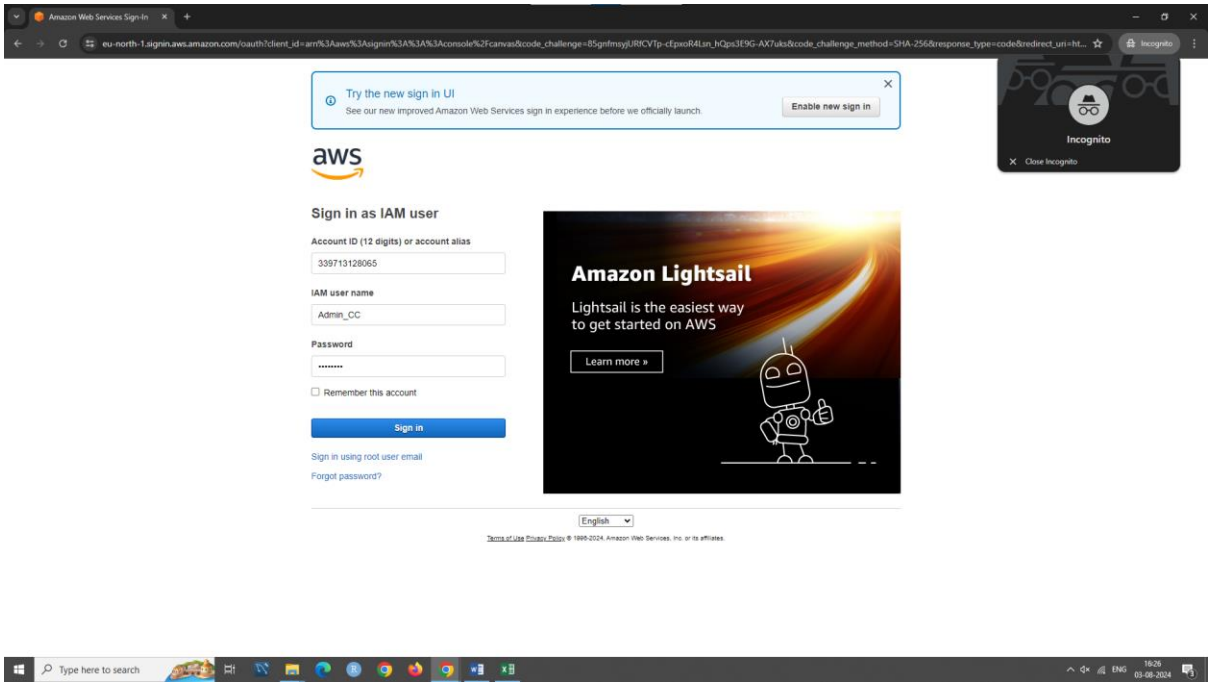

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Services
IAM
Global
yagyamcc
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Admin_CC
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:15
03-08-2024

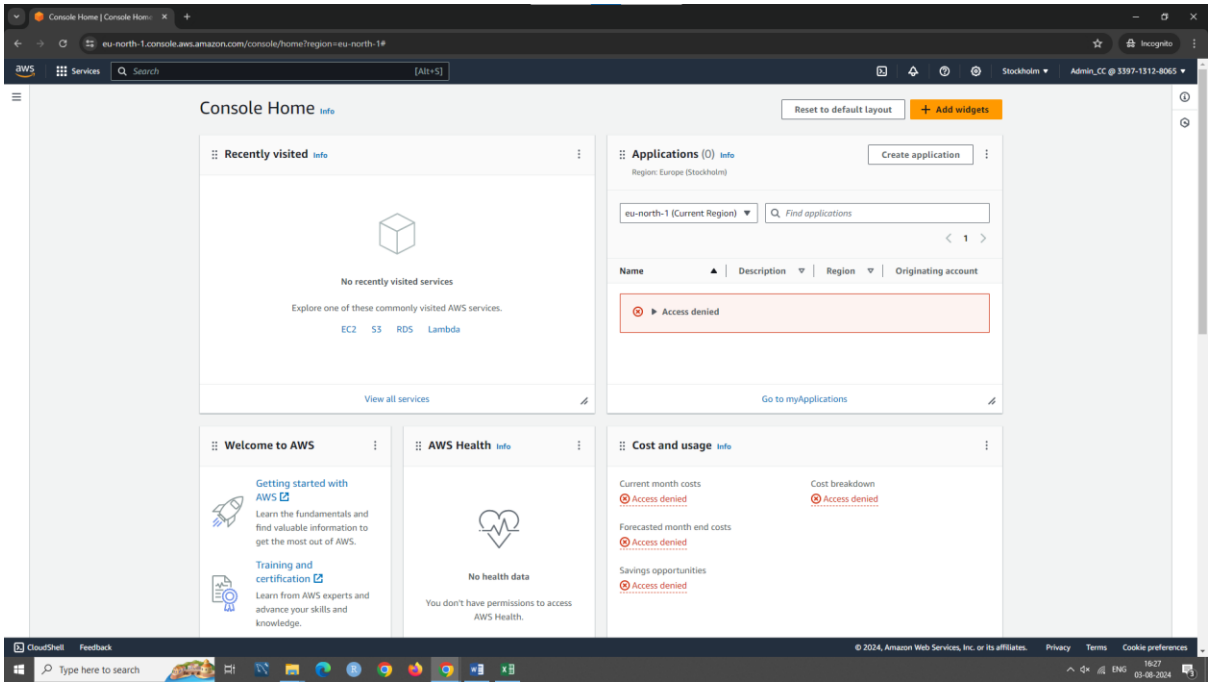

Admin_CC | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC?section=permissions
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
IAM > Users > Admin_CC
Admin_CC Info
Delete
Summary
ARN
arn:aws:iam::339713128065:user/Admin_CC
Console access
Disabled
Access key 1
Create access key
Created
August 03, 2024, 16:15 (UTC+05:30)
Last console sign-in
-
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
Filter by Type
Search
All types
Policy name
Type
Attached via
No resources to display
Permissions boundary (not set)
Generate policy based on CloudTrail events
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:15
03-08-2024

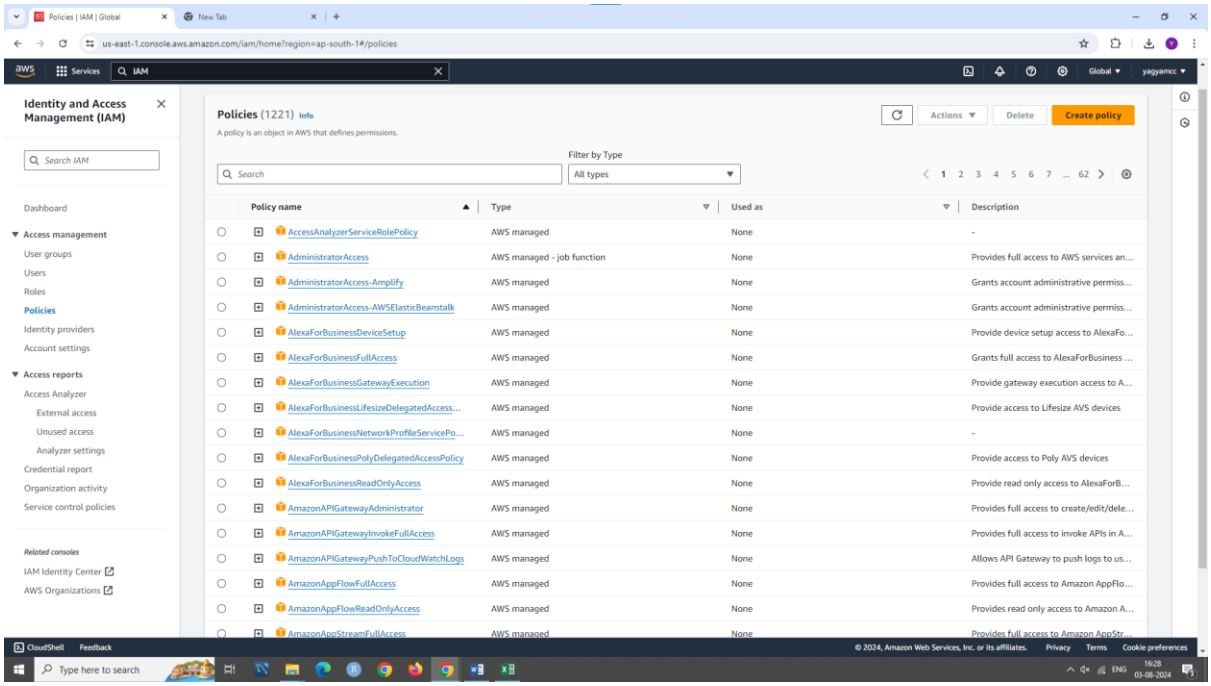

Admin_CC | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC?section=security_credentials
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
IAM > Users > Admin_CC
Admin_CC Info
Delete
Summary
ARN
arn:aws:iam::339713128065:user/Admin_CC
Console access
Disabled
Access key 1
Create access key
Created
August 03, 2024, 16:15 (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://339713128065.signin.aws.amazon.com/console
Console password
Not enabled
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
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
Type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (0)
Create access key
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:16
03-08-2024

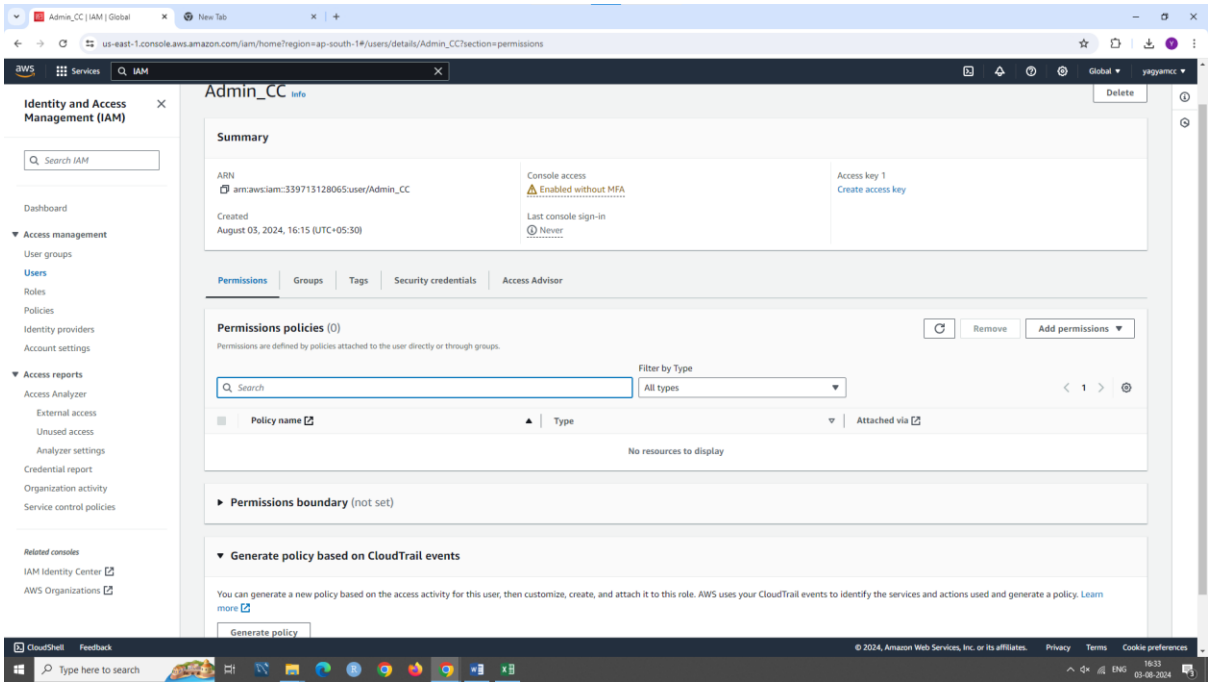

Admin_CC | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC?section=security_credentials
Enable console access
Enable console access for Admin_CC.
Console password
Autogenerated password
Custom password
User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
Cancel
Enable console access
Type here to search
ENG
16:16
03-08-2024

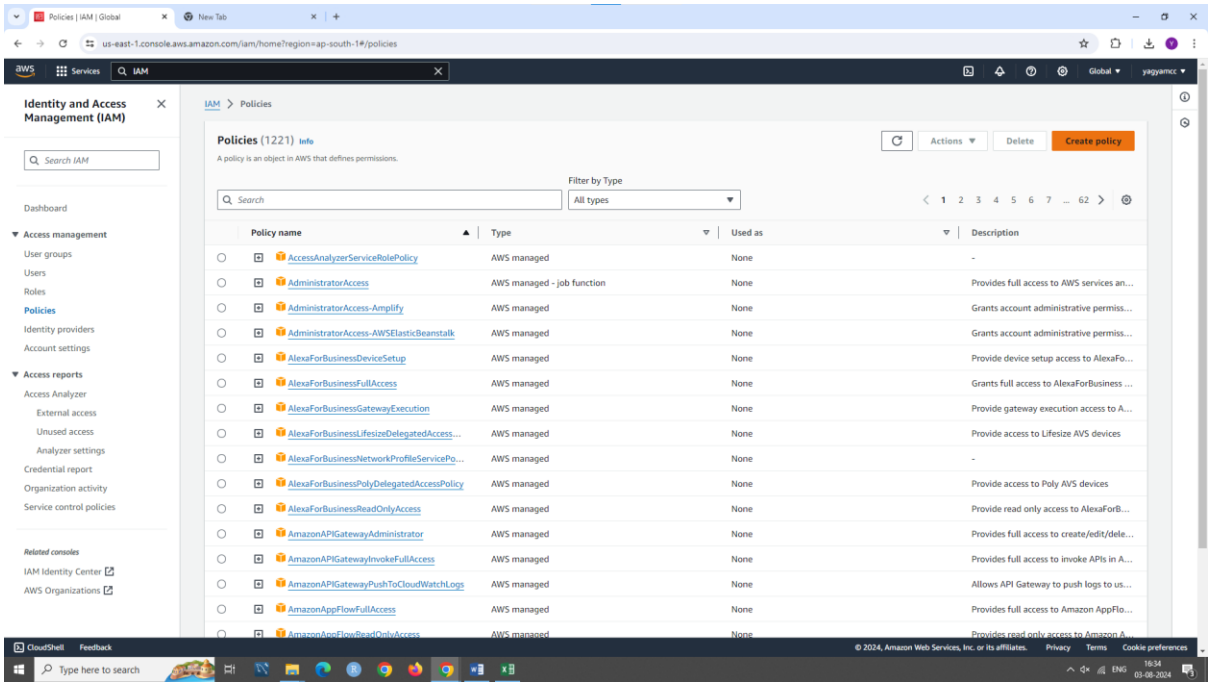

Admin_CC | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC?section=security_credentials
Identity and Access Management (IAM)
Admin_CC
Summary
Console password
You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.
Console sign-in URL
https://339713128065.signin.aws.amazon.com/console
User name
Admin_CC
Console password
Show
Download .csv file
Close
Console sign-in
Multi-factor authentication (MFA) (0)
Input Switch Notification
Input language switching
Typing Left Alt + Shift changes your input language. You can turn this feature off or change your hot key sequence by selecting Customize.
Customize
Dismiss
Type here to search
ENG
16:16
03-08-2024

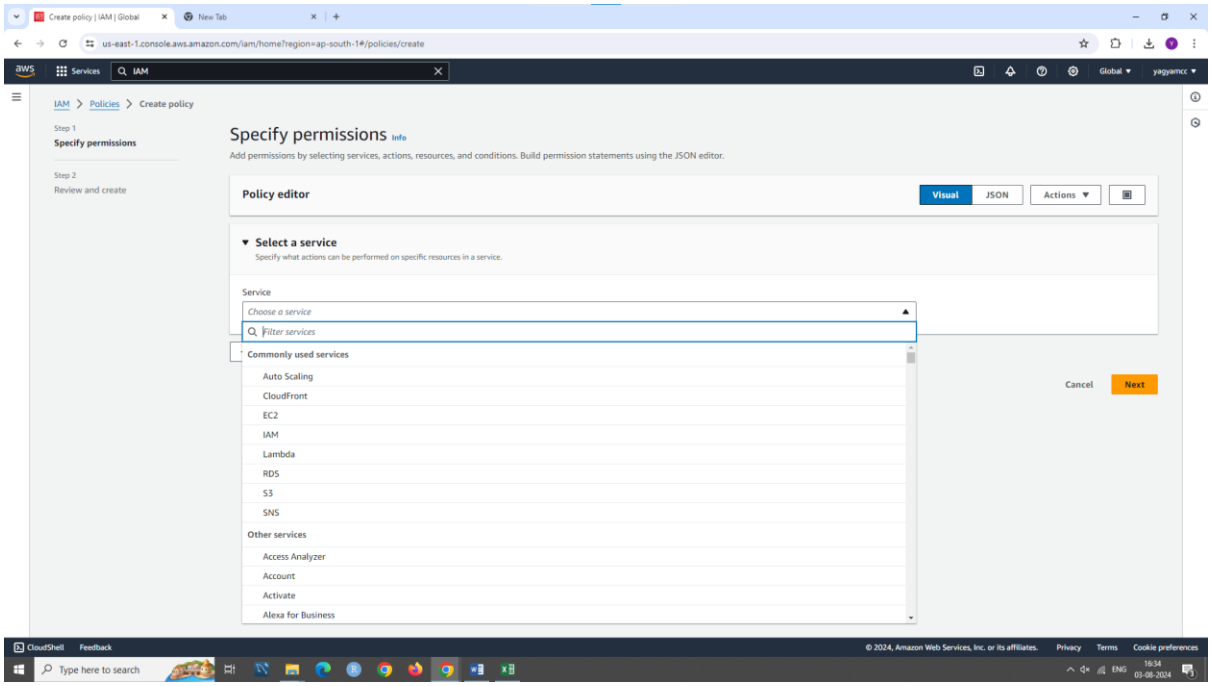

Amazon Web Services Sign-In
eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=85gnfmsyjURfCVTp-cEpxoR4Lsn_hQps3E9G-AX7uks&code_challenge_method=SHA-256&response_type=code&redirect_uri=ht...
Incognito
Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.
Enable new sign in
Incognito
Close Incognito
aws
Sign in as IAM user
Account ID (12 digits) or account alias
339713128065
IAM user name
Admin_CC
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »
English
Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.
Type here to search
ENG
16:26
03-08-2024

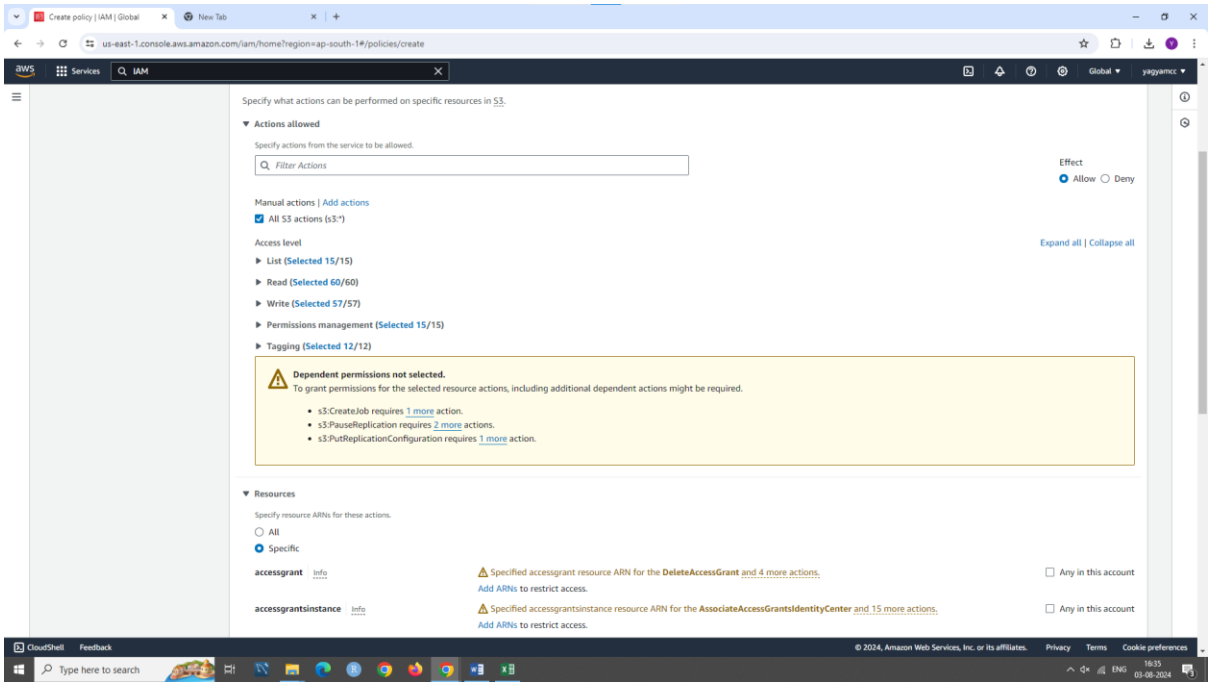

Console Home | Console Home
eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#
Services
Search
[Alt+S]
Stockholm
Admin_CC @ 3397-1312-8065
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
EC2 S3 RDS Lambda
View all services
Applications (0) Info
Region: Europe (Stockholm)
Create application
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
Learn from AWS experts and advance your skills and knowledge.
AWS Health Info
No health data
You don't have permissions to access AWS Health.
Cost and usage Info
Current month costs
Access denied
Cost breakdown
Access denied
Forecasted month end costs
Access denied
Savings opportunities
Access denied
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:27
03-08-2024

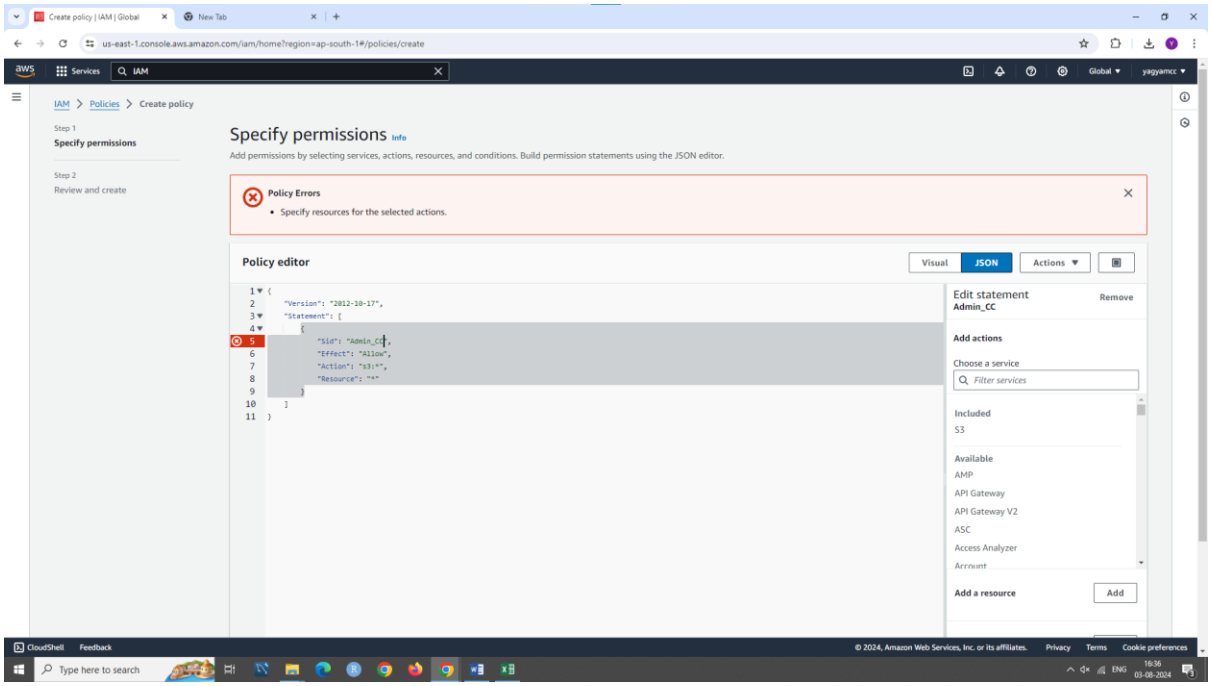

Policies | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
Policies (1221) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Search
Filter by Type
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...
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...
AmazonAPIGatewayInvokeFullAccess AWS managed None Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWatchLogs AWS managed None Allows API Gateway to push logs to us...
AmazonAppFlowFullAccess AWS managed None Provides full access to Amazon AppFlo...
AmazonAppFlowReadOnlyAccess AWS managed None Provides read only access to Amazon A...
AmazonAppStreamFullAccess AWS managed None Provides full access to Amazon AppStr...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:28
03-08-2024

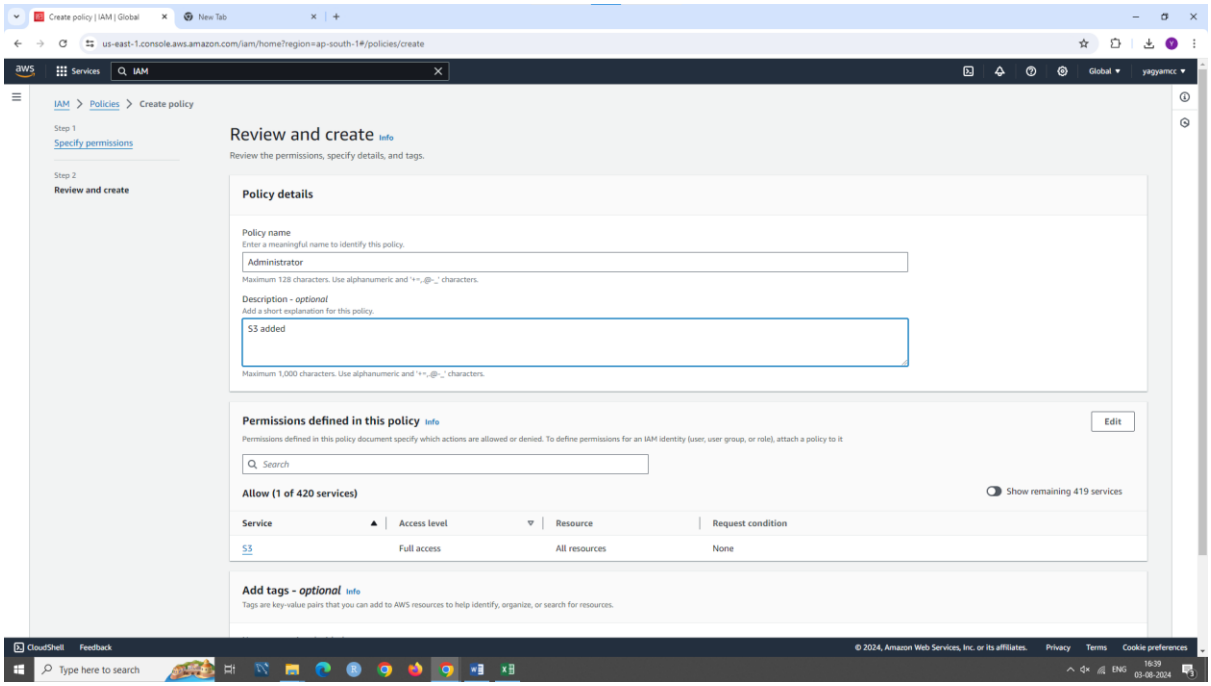

Admin_CC | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC?section=permissions
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
Admin_CC Info
Delete
Summary
ARN
arn:aws:iam::339713128065:user/Admin_CC
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:15 (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
Filter by Type
Search
All types
Policy name
Type
Attached via
No resources to display
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:33
03-08-2024

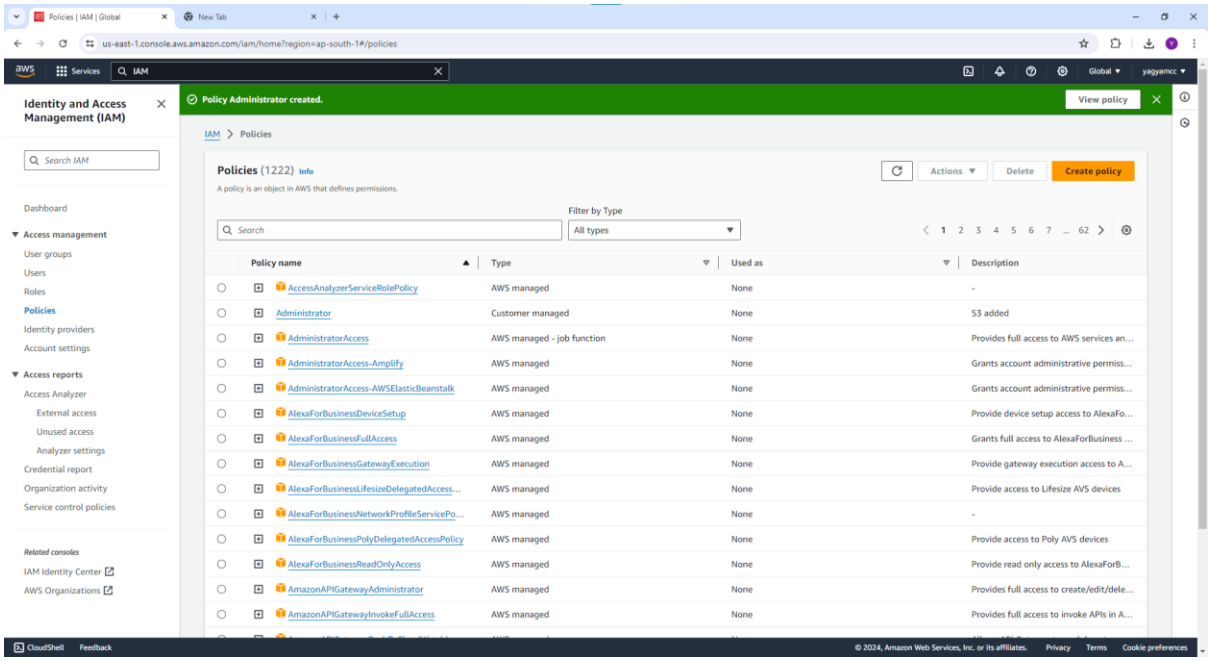

Policies | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
IAM > Policies
Policies (1221) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 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...
AmazonAPIGatewayInvokeFullAccess AWS managed None Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWatchLogs AWS managed None Allows API Gateway to push logs to us...
AmazonAppFlowFullAccess AWS managed None Provides full access to Amazon AppFlo...
AmazonAppFlowReadOnlyAccess AWS managed None Provides read only access to Amazon A...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:34
03-08-2024

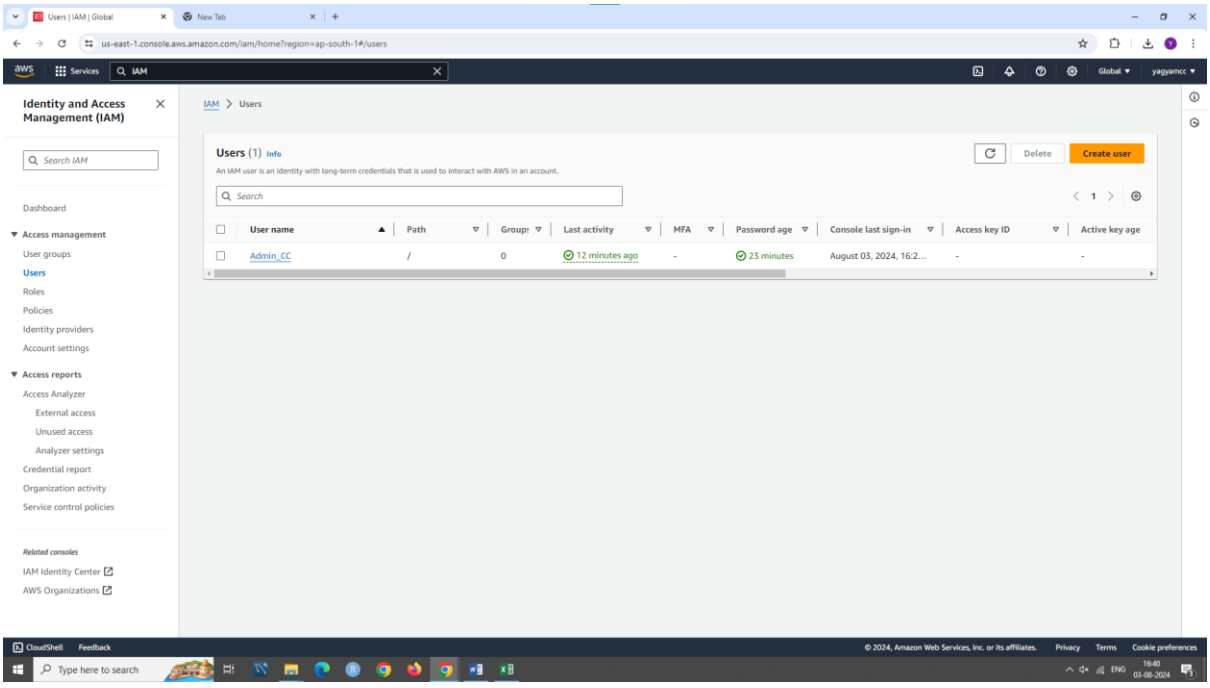

Create policy | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
aws
Services
IAM
Global
yagyamcc
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
Select a service
Specify what actions can be performed on specific resources in a service.
Service
Choose a service
Filter services
Commonly used services
Auto Scaling
CloudFront
EC2
IAM
Lambda
RDS
S3
SNS
Other services
Access Analyzer
Account
Activate
Alexa for Business
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:34
03-08-2024

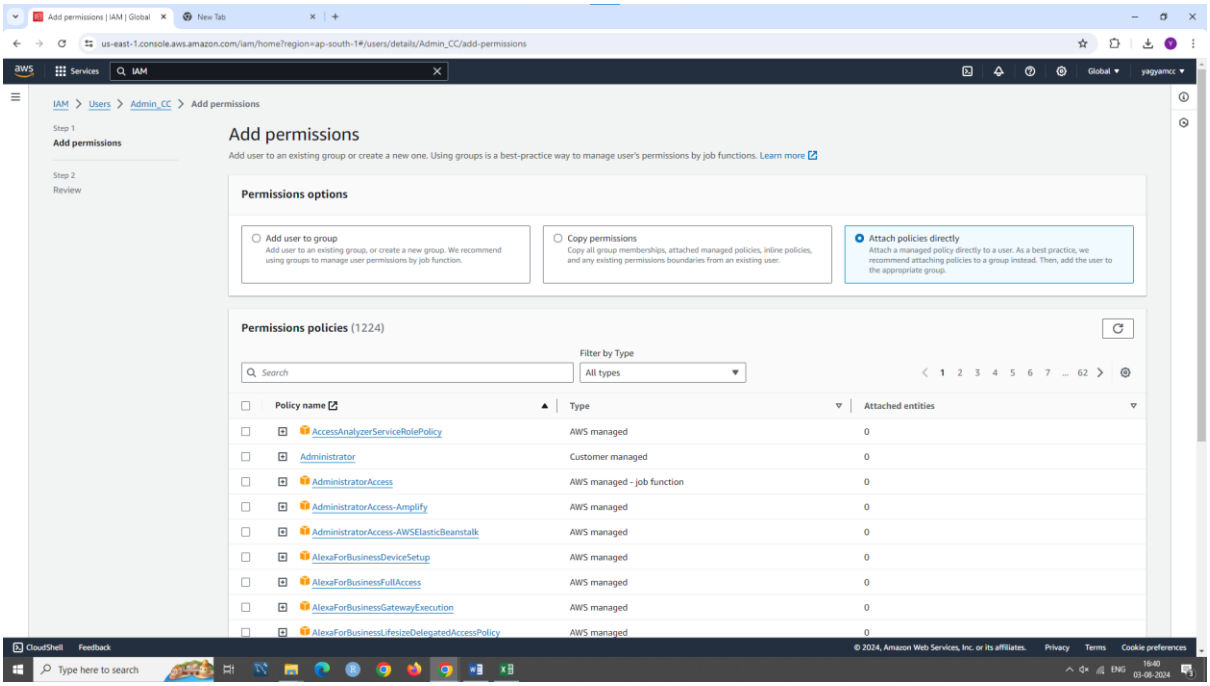

Create policy | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
aws
Services
IAM
Global
yagyamcc
Specify what actions can be performed on specific resources in S3.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
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
accessgrant
Info
Specified accessgrant resource ARN for the DeleteAccessGrant and 4 more actions.
Add ARNs to restrict access.
Any in this account
accessgrantsinstance
Info
Specified accessgrantsinstance resource ARN for the AssociateAccessGrantsIdentityCenter and 15 more actions.
Add ARNs to restrict access.
Any in this account
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:35
03-08-2024

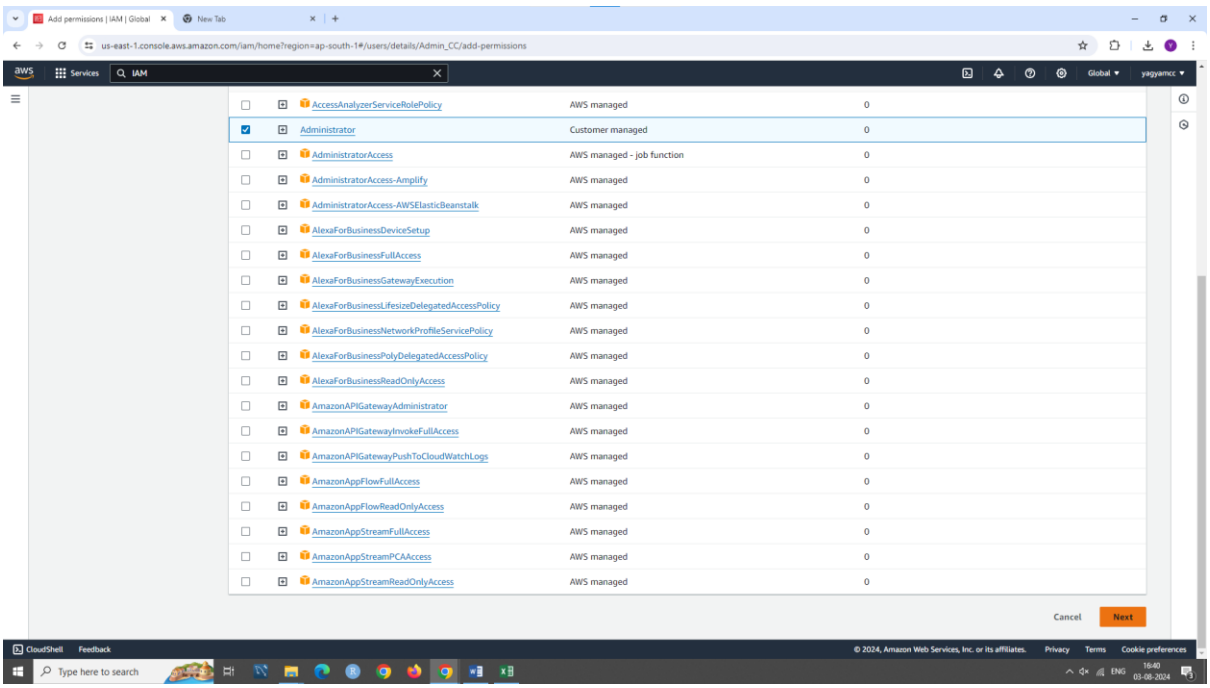

Create policy | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
aws
Services
IAM
Global
yagyamcc
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy Errors
Specify resources for the selected actions.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Admin_CC",
"Effect": "Allow",
"Action": "s3:*",
"Resource": "*"
}
]
}
Edit statement
Admin_CC
Remove
Add actions
Choose a service
Filter services
Included
S3
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
Add a resource
Add
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:36
03-08-2024

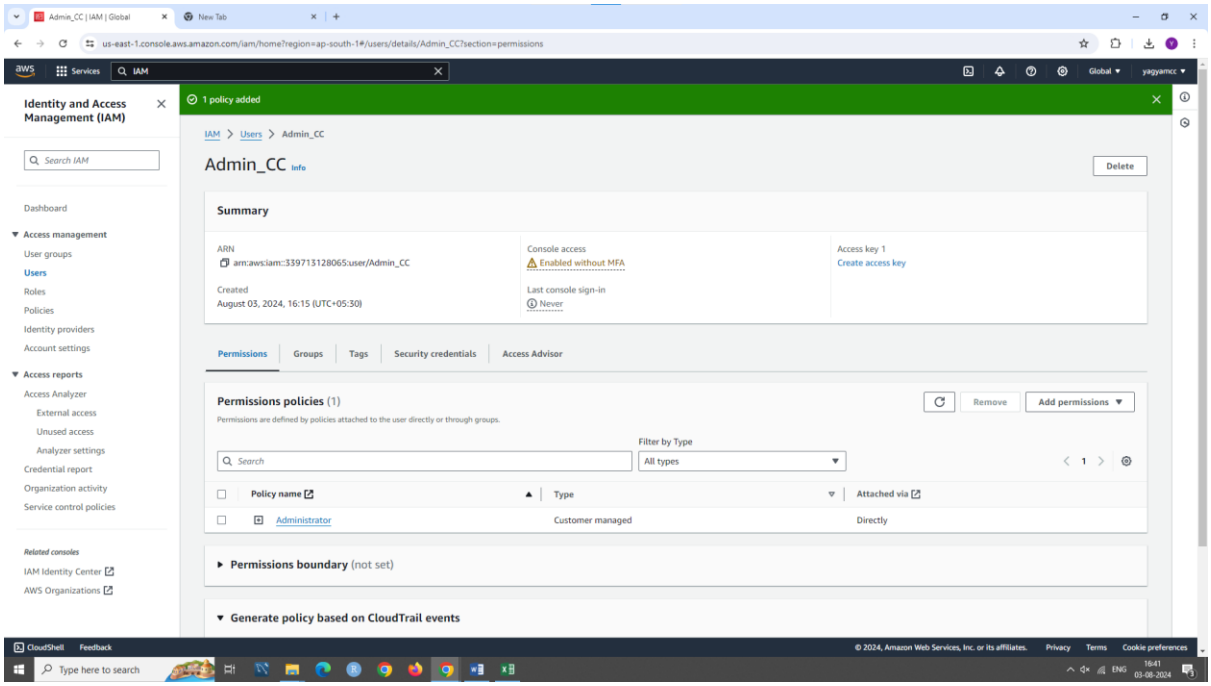

Create policy | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
aws
Services
IAM
Global
yagyamcc
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Administrator
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
S3 added
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
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:39
03-08-2024

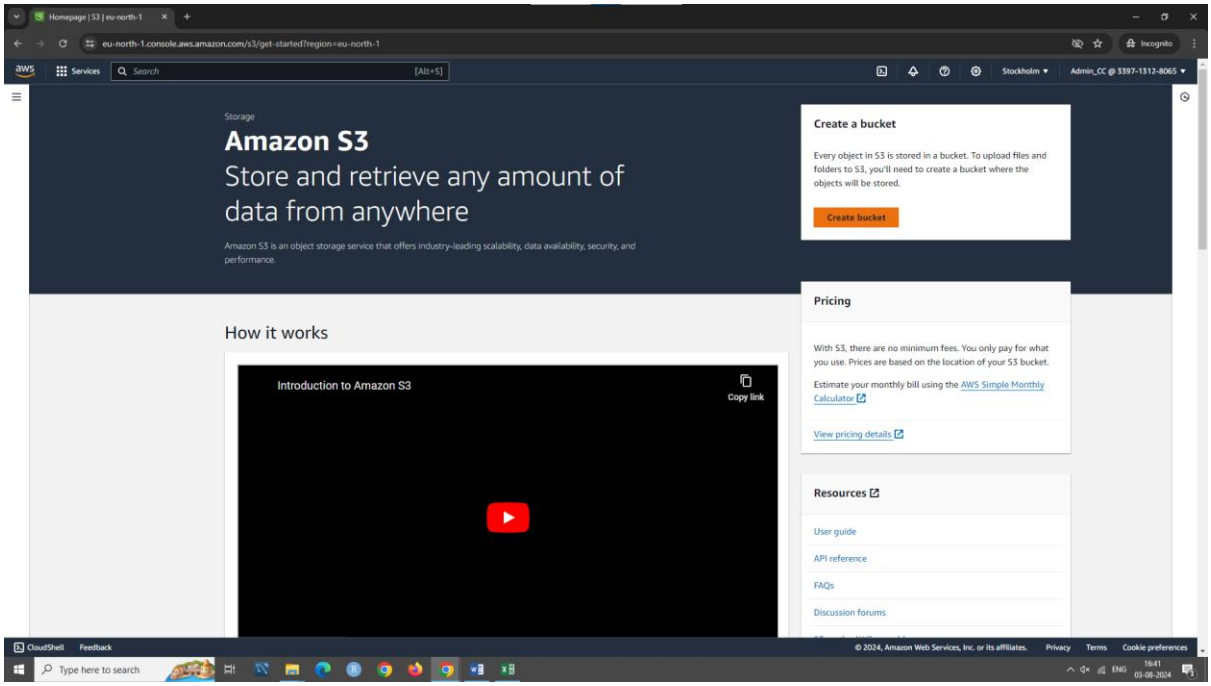

Policies | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies
aws
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
Policy Administrator 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
-
Administrator
Customer managed
None
S3 added
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...
AmazonAPIGatewayInvokeFullAccess
AWS managed
None
Provides full access to invoke APIs in A...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

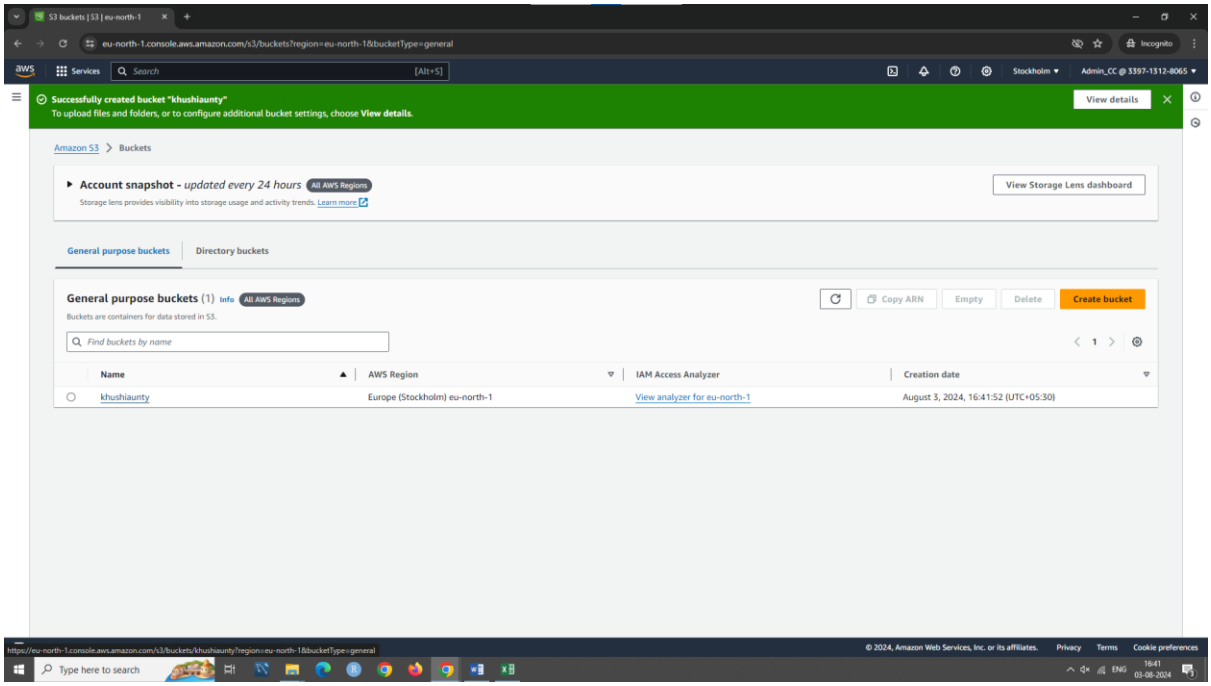

Users | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users
aws
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
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
1
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
Access key ID
Active key age
Admin_CC
/
0
12 minutes ago
-
23 minutes
August 03, 2024, 16:2...
-
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:40
03-08-2024

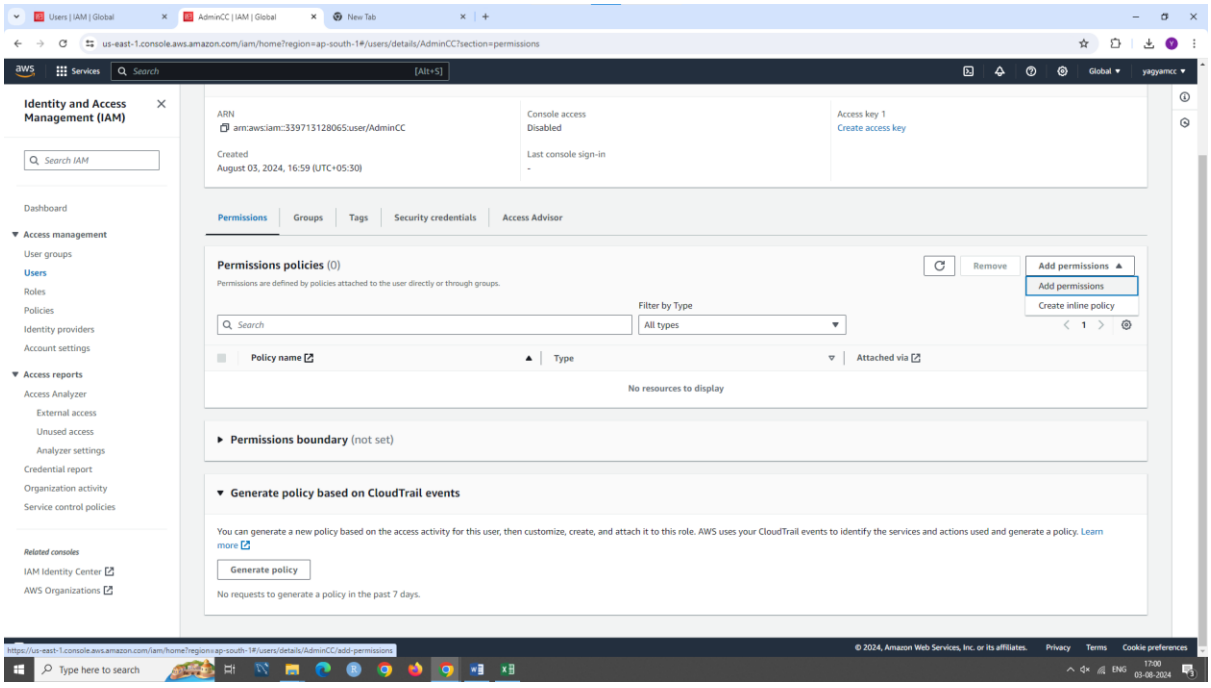

Add permissions | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC/add-permissions
Services
IAM
Global
yagyamcc
IAM > Users > Admin_CC > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create 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
1 2 3 4 5 6 7 ... 62
Policy name
Type
Attached entities
AccessAnalyzerServiceRolePolicy AWS managed 0
Administrator Customer managed 0
AdministratorAccess AWS managed - job function 0
AdministratorAccess-Amplify AWS managed 0
AdministratorAccess-AWSElasticBeanstalk AWS managed 0
AlexaForBusinessDeviceSetup AWS managed 0
AlexaForBusinessFullAccess AWS managed 0
AlexaForBusinessGatewayExecution AWS managed 0
AlexaForBusinessLifesizeDelegatedAccessPolicy AWS managed 0
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:40
03-08-2024

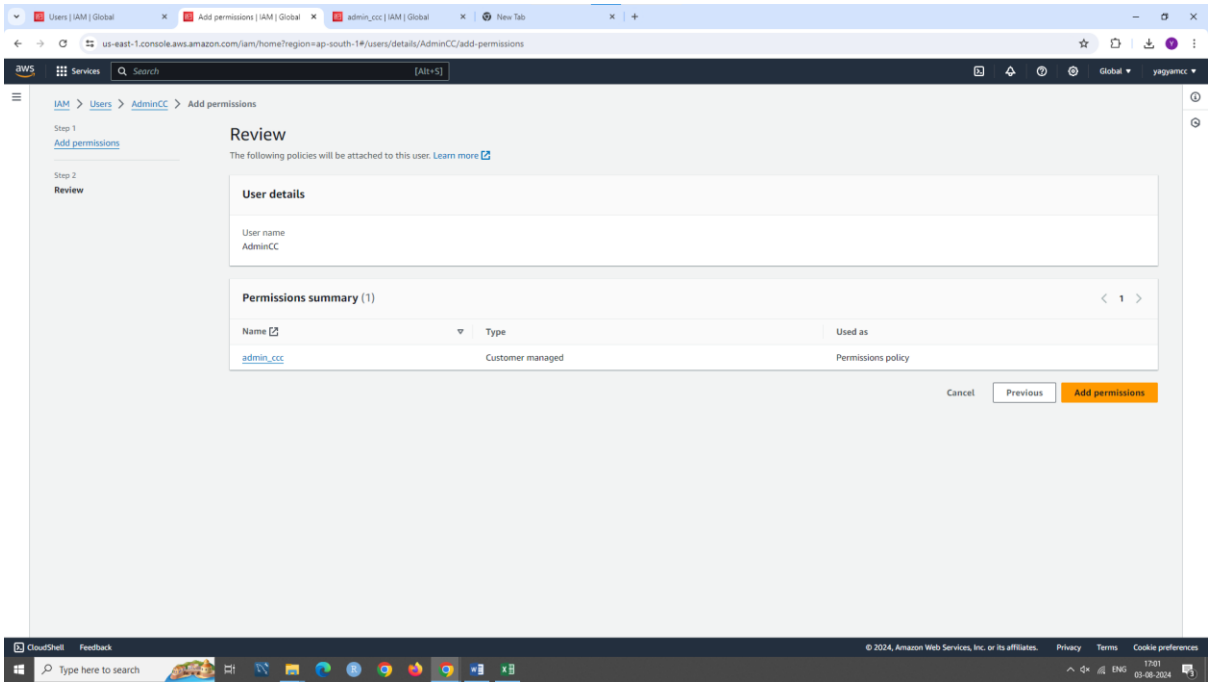

Add permissions | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC/add-permissions
Services
IAM
Global
yagyamcc
AccessAnalyzerServiceRolePolicy AWS managed 0
Administrator Customer managed 0
AdministratorAccess AWS managed - job function 0
AdministratorAccess-Amplify AWS managed 0
AdministratorAccess-AWSElasticBeanstalk AWS managed 0
AlexaForBusinessDeviceSetup AWS managed 0
AlexaForBusinessFullAccess AWS managed 0
AlexaForBusinessGatewayExecution AWS managed 0
AlexaForBusinessLifesizeDelegatedAccessPolicy AWS managed 0
AlexaForBusinessNetworkProfileServicePolicy AWS managed 0
AlexaForBusinessPolyDelegatedAccessPolicy AWS managed 0
AlexaForBusinessReadOnlyAccess AWS managed 0
AmazonAPIGatewayAdministrator AWS managed 0
AmazonAPIGatewayInvokeFullAccess AWS managed 0
AmazonAPIGatewayPushToCloudWatchLogs AWS managed 0
AmazonAppFlowFullAccess AWS managed 0
AmazonAppFlowReadOnlyAccess AWS managed 0
AmazonAppStreamFullAccess AWS managed 0
AmazonAppStreamPCAAccess AWS managed 0
AmazonAppStreamReadOnlyAccess AWS managed 0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:40
03-08-2024

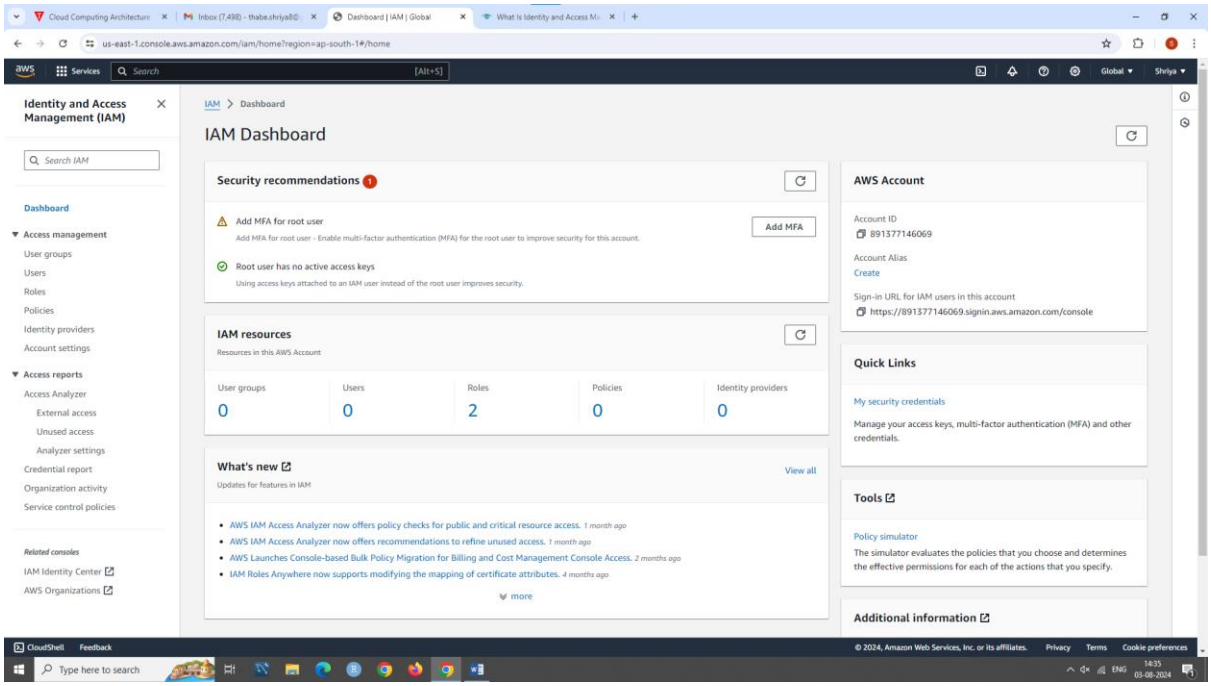

Admin_CC | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Admin_CC?section=permissions
Services
IAM
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
1 policy added
IAM > Users > Admin_CC
Admin_CC Info
Delete
Summary
ARN
arn:aws:iam::339713128065:user/Admin_CC
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:15 (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
Administrator
Customer managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:41
03-08-2024

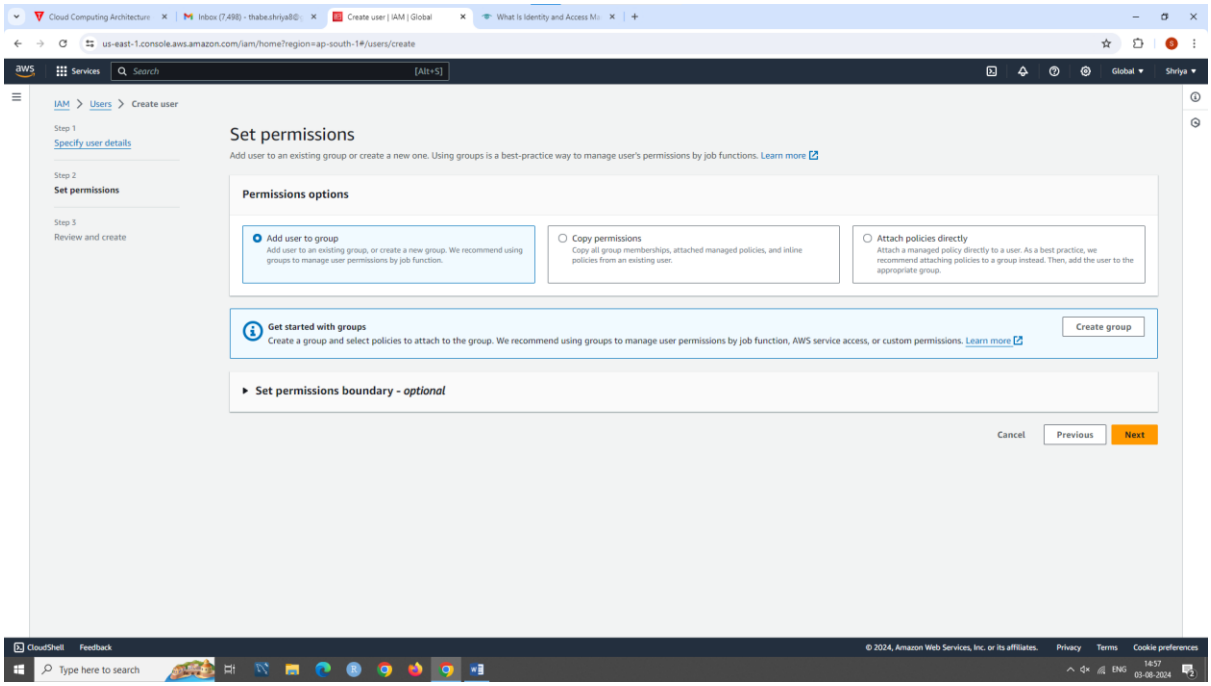

Homepage | S3 | eu-north-1
eu-north-1.console.aws.amazon.com/s3/get-started?region=eu-north-1
Incognito
Services
Search
[Alt+S]
Stockholm
Admin_CC @ 3397-1312-8065
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
Create a bucket
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
Create bucket
Pricing
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.
Estimate your monthly bill using the AWS Simple Monthly Calculator
View pricing details
Resources
User guide
API reference
FAQs
Discussion forums
How it works
Introduction to Amazon S3
Copy link
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:41
03-08-2024

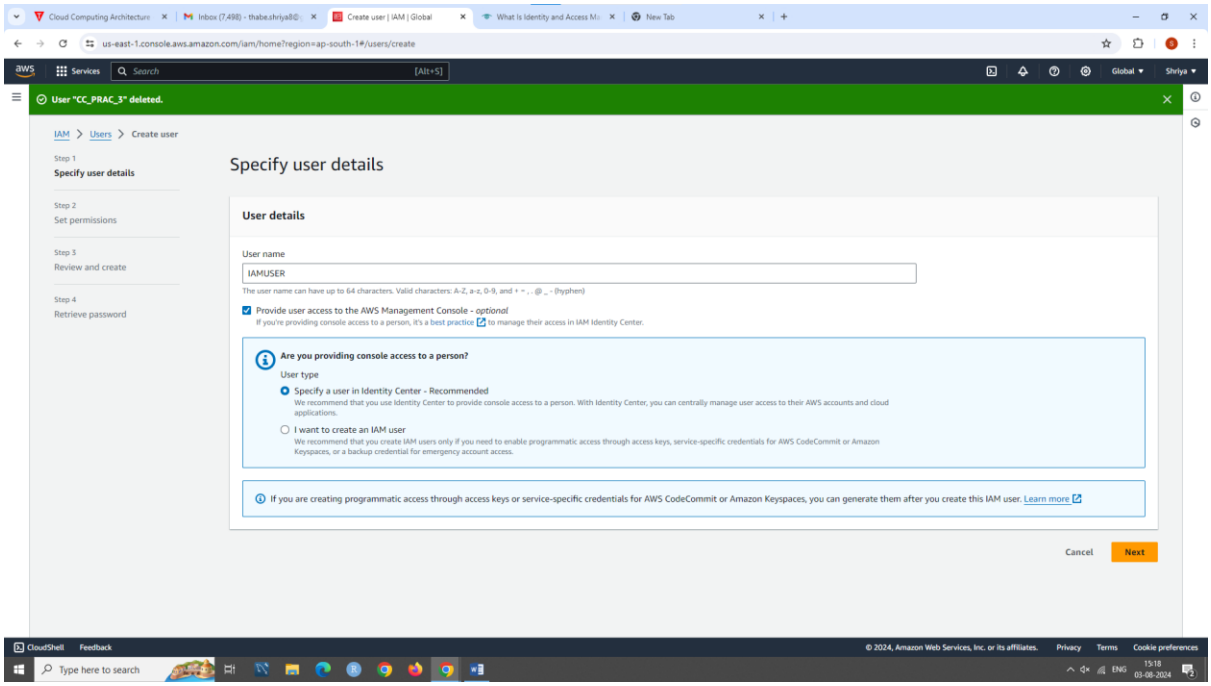

S3 buckets | S3 | eu-north-1
eu-north-1.console.aws.amazon.com/s3/buckets?region=eu-north-1&bucketType=general
Services
Search
[Alt+S]
Stockholm
Admin_CC @ 3397-1312-8065
Successfully created bucket "khushiaunty"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
khushiaunty
Europe (Stockholm) eu-north-1
View analyzer for eu-north-1
August 3, 2024, 16:41:52 (UTC+05:30)
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
16:41
03-08-2024

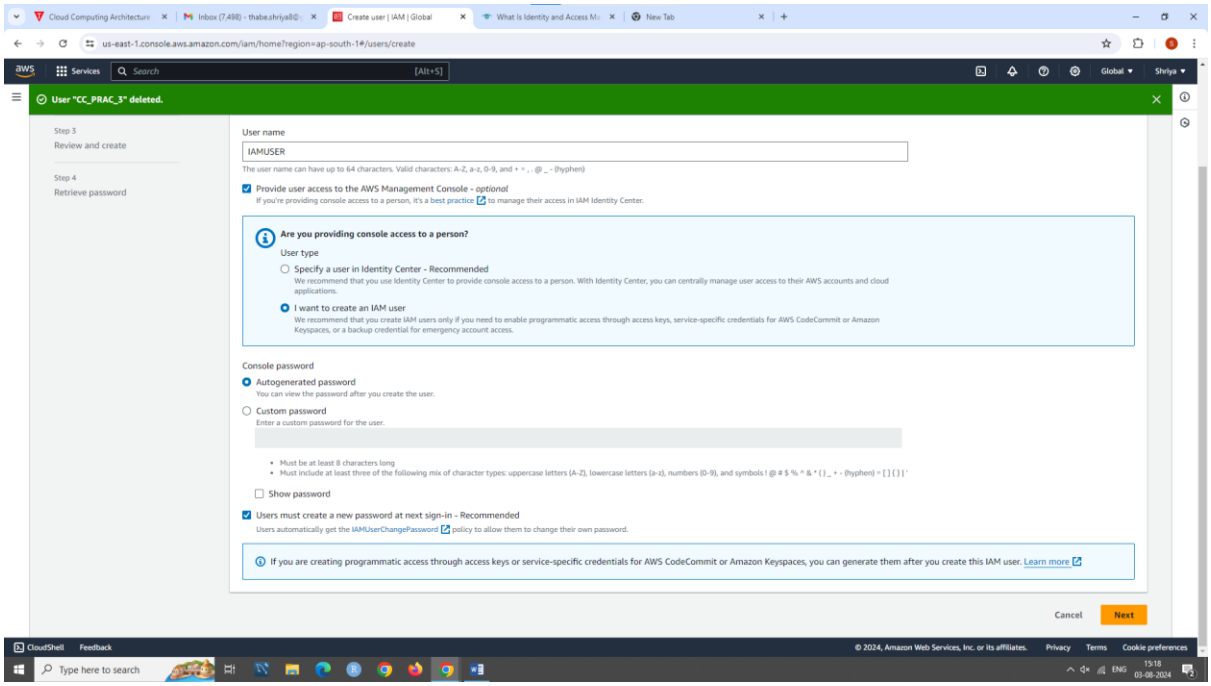

Users | IAM | Global
AdminCC | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/AdminCC?section=permissions
Services
Search
[Alt+S]
Global
yagyamcc
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
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
AWS Organizations
ARN
arn:aws:iam::339713128065:user/AdminCC
Console access
Disabled
Access key 1
Create access key
Created
August 03, 2024, 16:59 (UTC+05:30)
Last console sign-in
-
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
Policy name
Type
Attached via
No resources to display
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy
No requests to generate a policy in the past 7 days.
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
17:00
03-08-2024

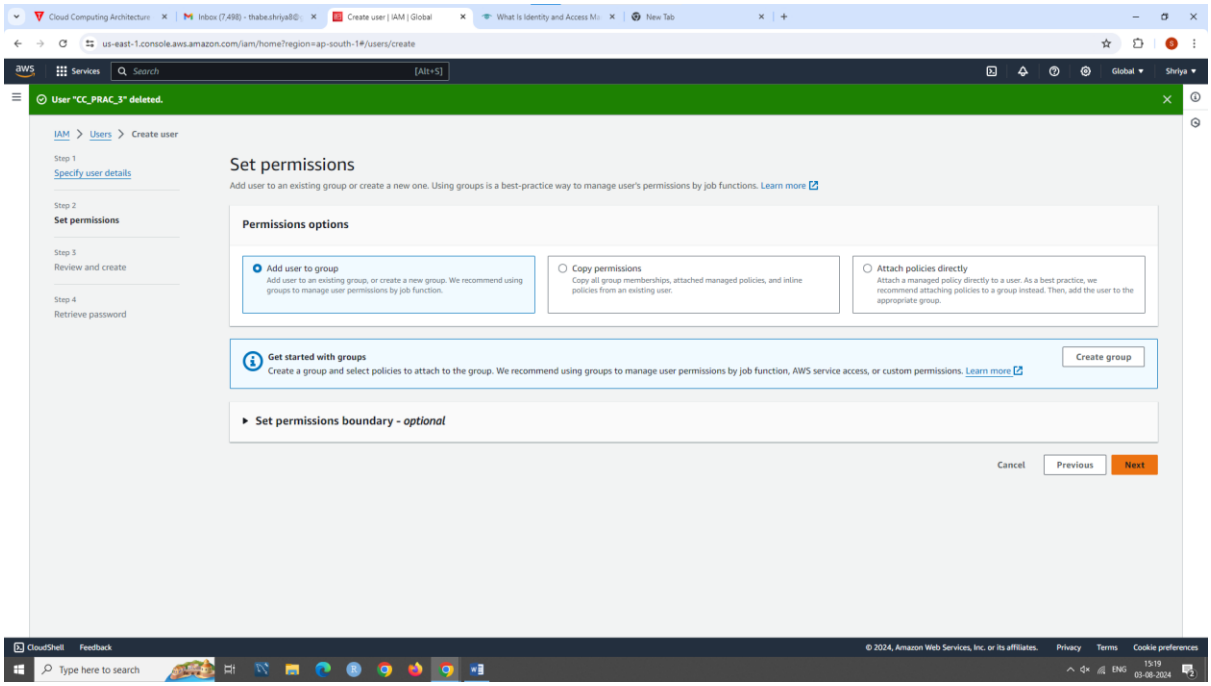

Users | IAM | Global
Add permissions | IAM | Global
admin_ccc | IAM | Global
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/AdminCC/add-permissions
Services
Search
[Alt+S]
Global
yagyamcc
IAM > Users > AdminCC > Add permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
AdminCC
Permissions summary (1)
Name
Type
Used as
admin_ccc
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
17:01
03-08-2024

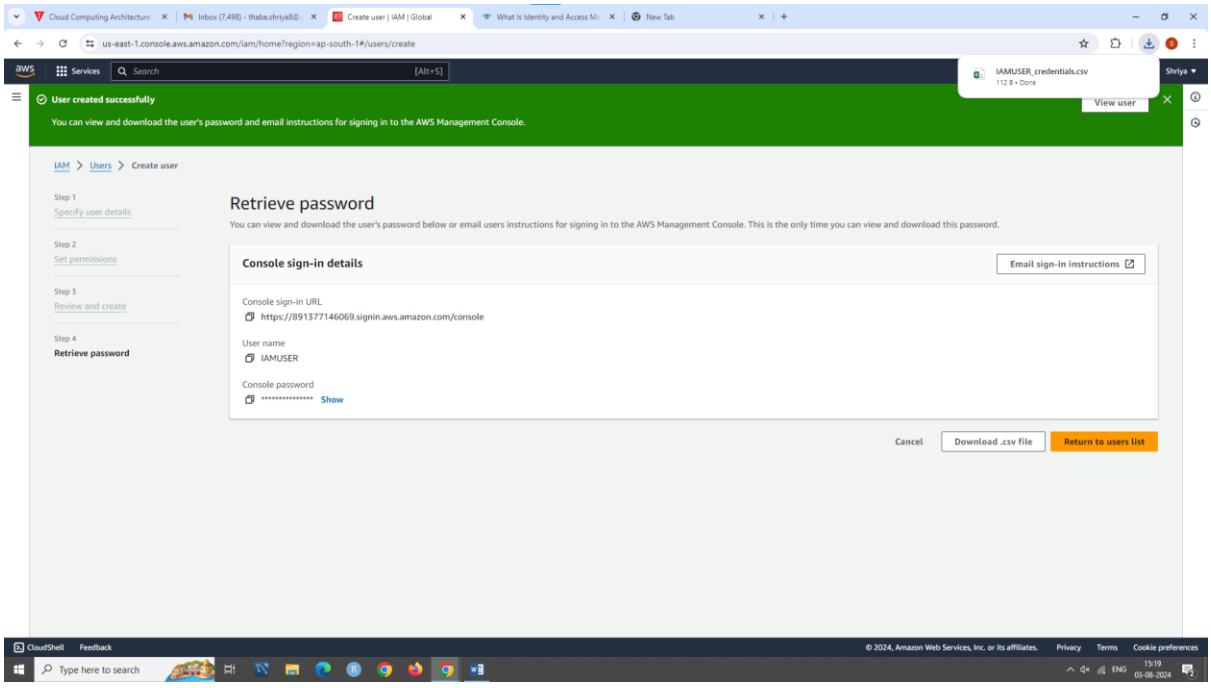

Cloud Computing Architecture
Inbox (7,498) - thabe.shriya8@
Dashboard | IAM | Global
What Is Identity and Access M
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/home
Services
Search
[Alt+S]
Global
Shriya
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
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
AWS Organizations
IAM > Dashboard
IAM Dashboard
Security recommendations 1
Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
Add MFA
Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.
IAM resources
Resources in this AWS Account
User groups
0
Users
0
Roles
2
Policies
0
Identity providers
0
What's new
Updates for features in IAM
View all
AWS IAM Access Analyzer now offers policy checks for public and critical resource access. 1 month ago
AWS IAM Access Analyzer now offers recommendations to refine unused access. 1 month ago
AWS Launches Console-based Bulk Policy Migration for Billing and Cost Management Console Access. 2 months ago
IAM Roles Anywhere now supports modifying the mapping of certificate attributes. 4 months ago
more
AWS Account
Account ID
891577146069
Account Alias
Create
Sign-in URL for IAM users in this account
https://891577146069.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
Additional information
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
14:35
03-08-2024

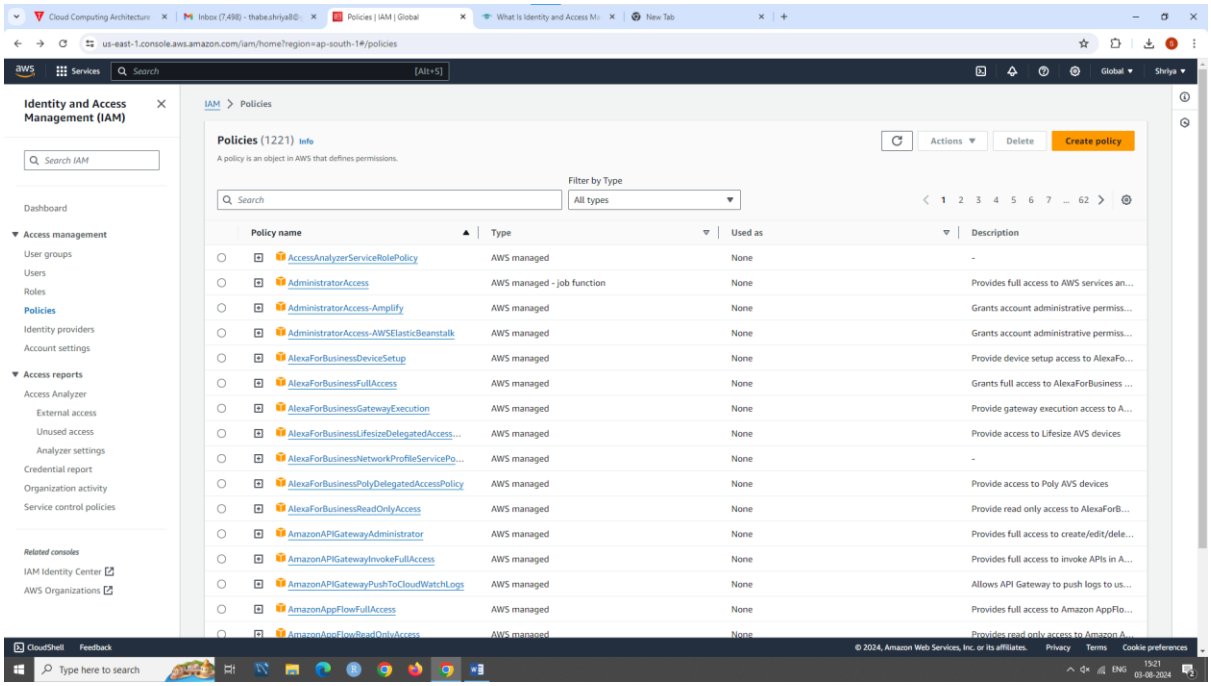

Cloud Computing Architecture
Inbox (7,498) - thabe.shriya8@
Create user | IAM | Global
What Is Identity and Access M
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
aws
Services
Search
[Alt+S]
Global
Shriya
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
14:57
03-08-2024

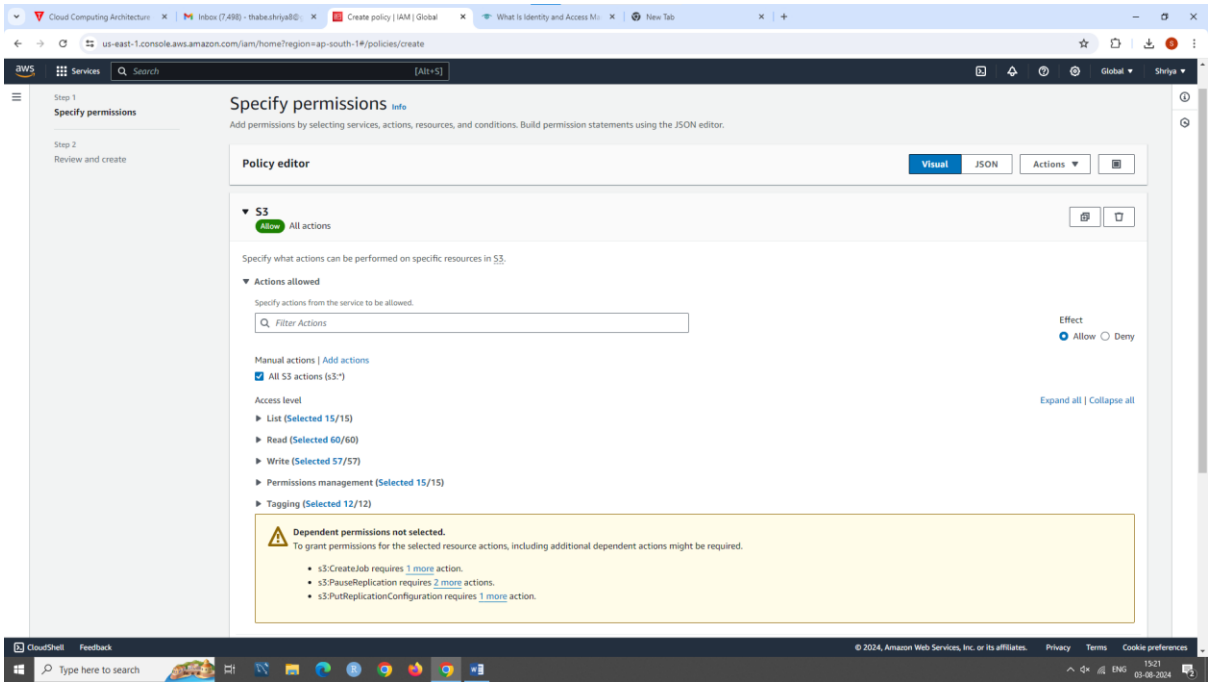

User "CC_PRAC_5" deleted.
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
IAMUSER
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
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

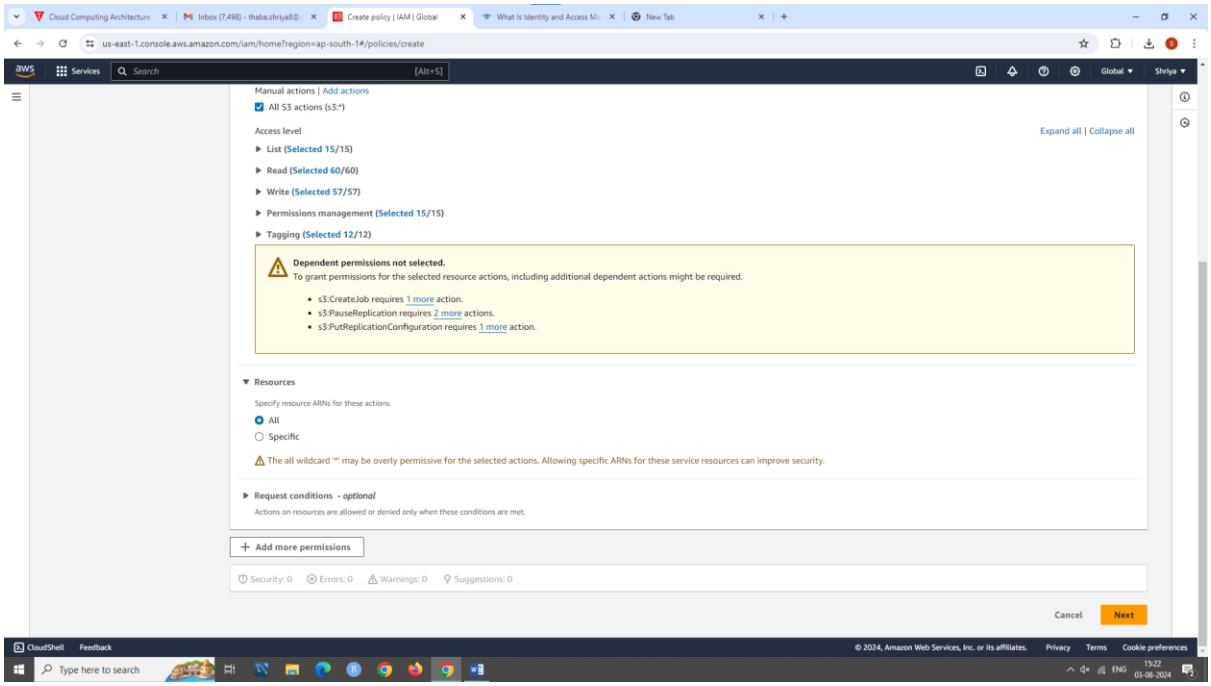

User "CC_PRAC_5" deleted.
Step 3
Review and create
Step 4
Retrieve password
User name
IAMUSER
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next

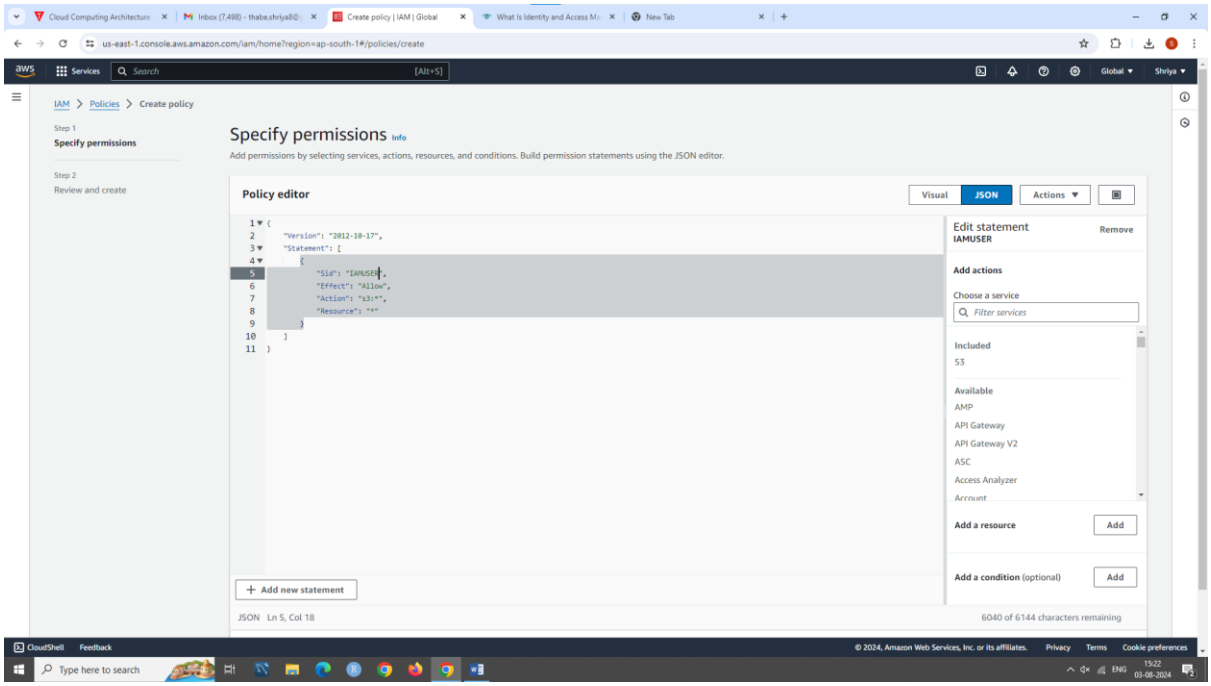

User "CC_PRAC_3" deleted.
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
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

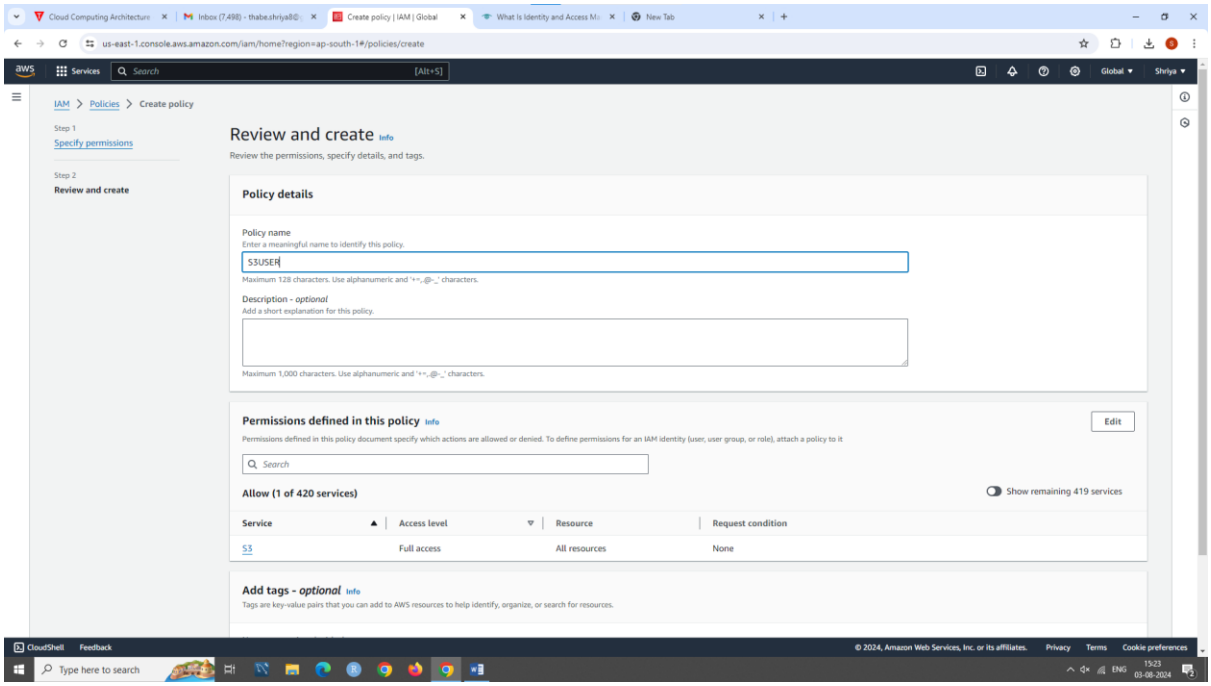

IAMUSER_credentials.csv
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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://891377146069.signin.aws.amazon.com/console
User name
IAMUSER
Console password
Show
Cancel
Download .csv file
Return to users list

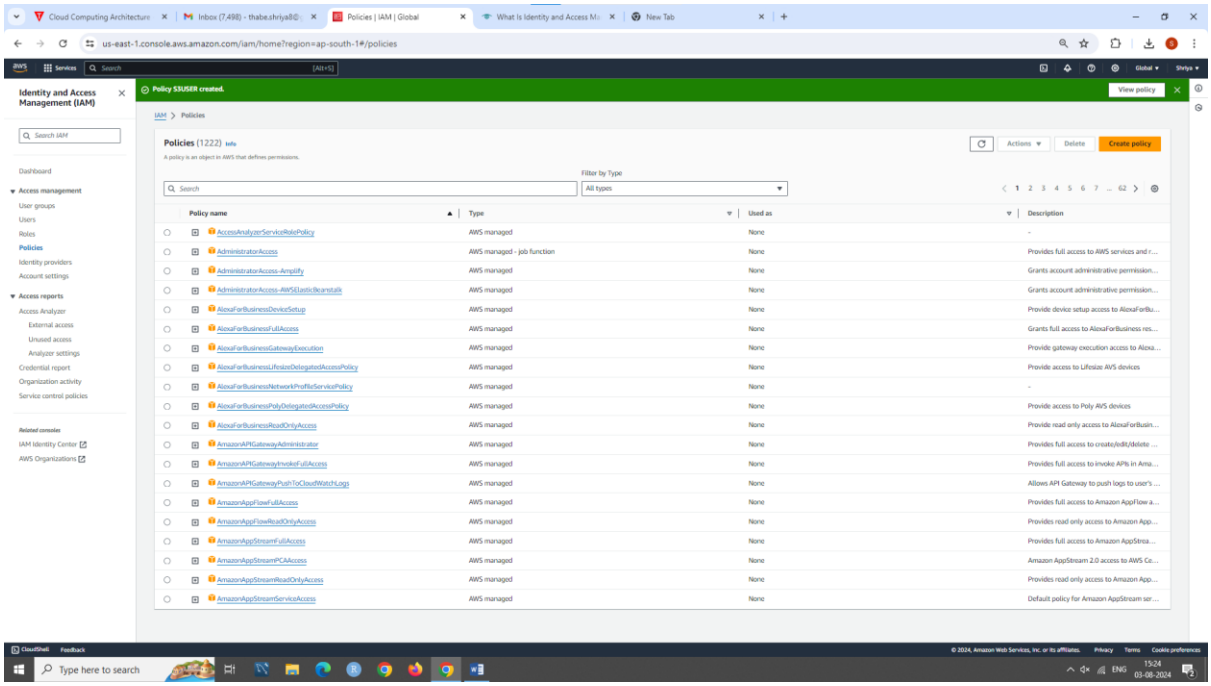

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
IAM > Policies
Policies (1221) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Search
Filter by Type
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...
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...
AmazonAPIGatewayInvokeFullAccess | AWS managed | None | Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWatchLogs | AWS managed | None | Allows API Gateway to push logs to us...
AmazonAppFlowFullAccess | AWS managed | None | Provides full access to Amazon AppFlo...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

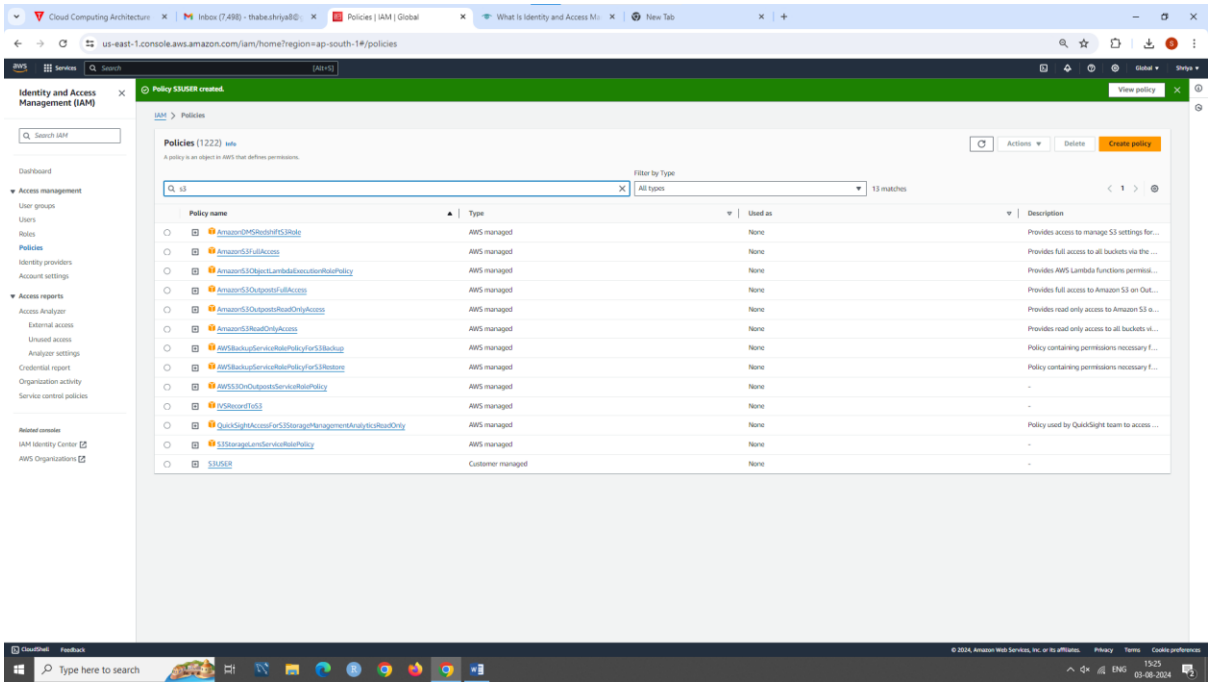

Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
S3
Allow
All actions
Specify what actions can be performed on specific 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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

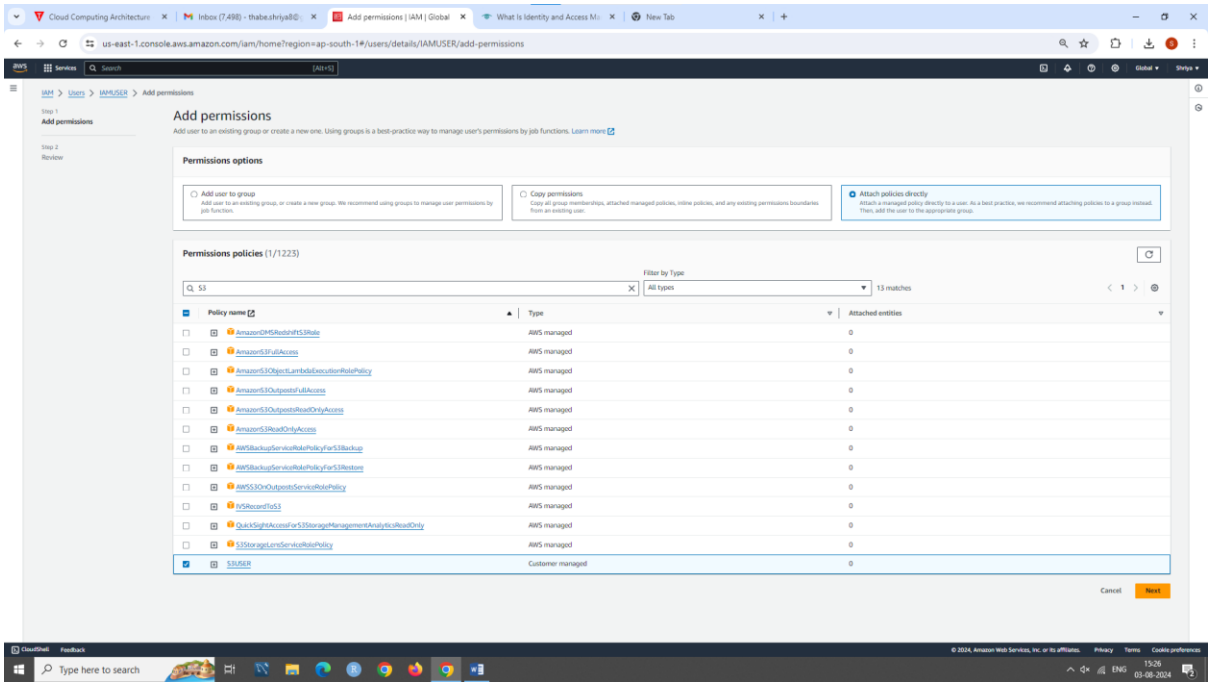

Manual actions | Add actions
All S3 actions (s3:*)
Access level
Expand all | Collapse all
List (Selected 15/15)
Read (Selected 60/60)
Write (Selected 57/57)
Permissions management (Selected 15/15)
Tagging (Selected 12/12)
Dependent permissions not selected.
To grant permissions for the selected resource 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
Actions on resources are allowed or denied only when these conditions are met.
Add more permissions
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next

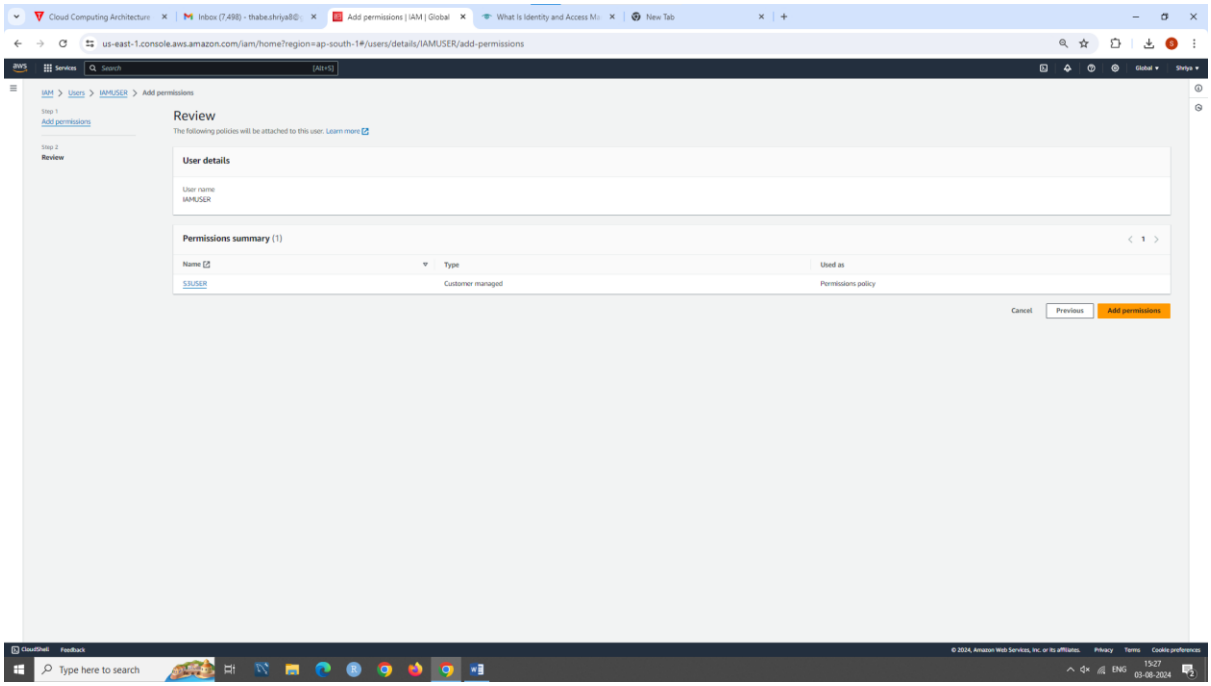

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions
Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "IAMUSER",
"Effect": "Allow",
"Action": "s3:*",
"Resource": "*"
}
]
}
Edit statement
IAMUSER
Remove
Add actions
Choose a service
Filter services
Included
S3
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
Add a resource
Add
Add a condition (optional)
Add
Add new statement
JSON Ln 5, Col 18
6040 of 6144 characters remaining

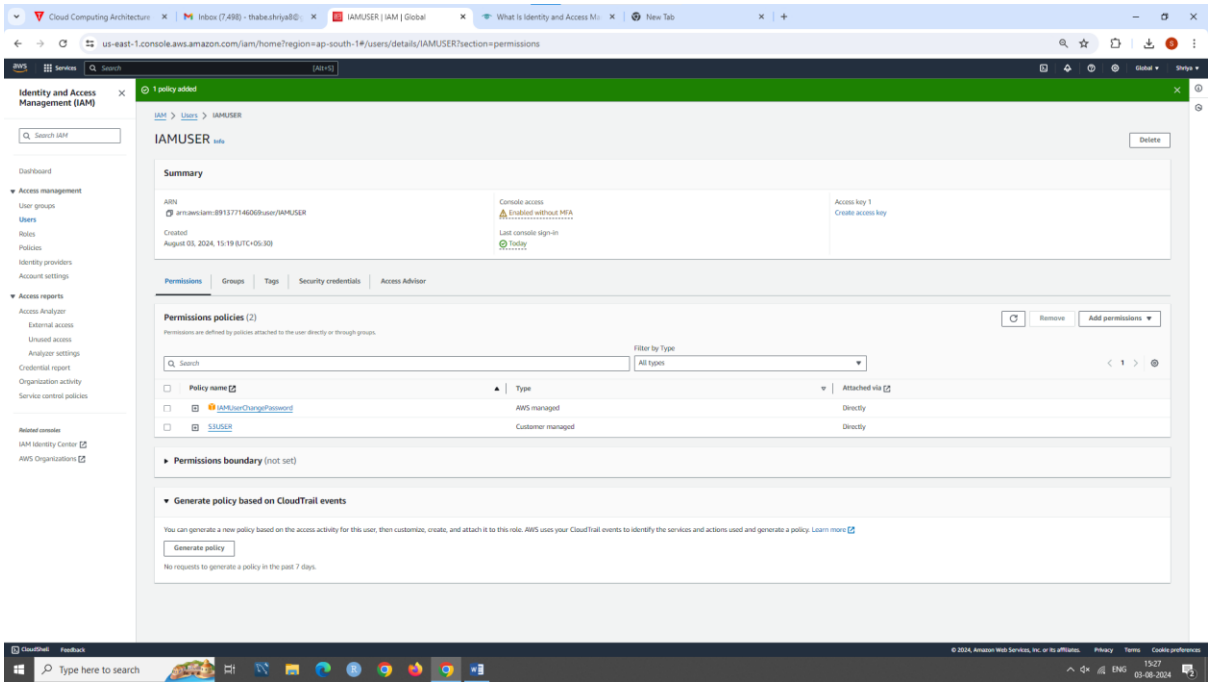

Cloud Computing Architecture
Inbox (7,498) - thabe.shriya8@
Create policy | IAM | Global
What Is Identity and Access M
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create
Services
Search
[Alt+S]
Global
Shriya
IAM > Policies > Create policy
Step 1
Specify permissions
Step 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.
S3USER
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
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
15:23
03-08-2024

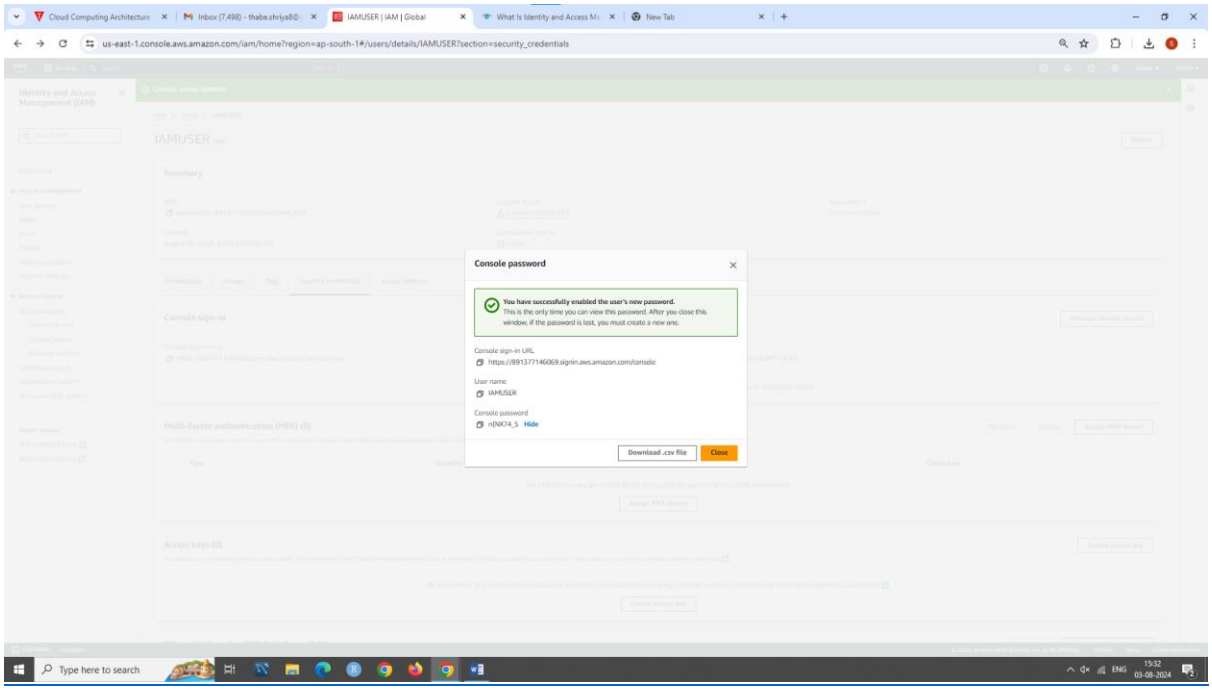

Cloud Computing Architecture
Inbox (7,498) - thabe.shriya8@
Policies | IAM | Global
What Is Identity and Access M
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies
Identity and Access Management (IAM)
Policy S3USER created.
View policy
IAM > Policies
Policies (1222) Info
A 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 and r...
AdministratorAccess-Amplify
AWS managed
None
Grants account administrative permission...
AdministratorAccess-AWSElasticBeanstalk
AWS managed
None
Grants account administrative permission...
AlexaForBusinessDeviceSetup
AWS managed
None
Provide device setup access to AlexaForBu...
AlexaForBusinessFullAccess
AWS managed
None
Grants full access to AlexaForBusiness res...
AlexaForBusinessGatewayExecution
AWS managed
None
Provide gateway execution access to Alexa...
AlexaForBusinessLifesizeDelegatedAccessPolicy
AWS managed
None
Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfileServicePolicy
AWS managed
None
AlexaForBusinessPolyDelegatedAccessPolicy
AWS managed
None
Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess
AWS managed
None
Provide read only access to AlexaForBusin...
AmazonAPIGatewayAdministrator
AWS managed
None
Provides full access to create/edit/delete ...
AmazonAPIGatewayInvokeFullAccess
AWS managed
None
Provides full access to invoke APIs in Ama...
AmazonAPIGatewayPushToCloudWatchLogs
AWS managed
None
Allows API Gateway to push logs to user's ...
AmazonAppFlowFullAccess
AWS managed
None
Provides full access to Amazon AppFlow a...
AmazonAppFlowReadOnlyAccess
AWS managed
None
Provides read only access to Amazon App...
AmazonAppStreamFullAccess
AWS managed
None
Provides full access to Amazon AppStrea...
AmazonAppStreamPCAAccess
AWS managed
None
Amazon AppStream 2.0 access to AWS Ce...
AmazonAppStreamReadOnlyAccess
AWS managed
None
Provides read only access to Amazon App...
AmazonAppStreamServiceAccess
AWS managed
None
Default policy for Amazon AppStream ser...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
15:24
03-08-2024


Policy S3USER created.
View policy
Identity and Access Management (IAM)
Policies (1222)
Create policy
Delete
Actions
s3
13 matches
Policy name
Type
Used as
Description
AmazonDMSRedshiftS3Role
AmazonS3FullAccess
AmazonS3ObjectLambdaExecutionRolePolicy
AmazonS3OutpostsFullAccess
AmazonS3OutpostsReadOnlyAccess
AmazonS3ReadOnlyAccess
AWSBackupServiceRolePolicyForS3Backup
AWSBackupServiceRolePolicyForS3Restore
AWSS3OnOutpostsServiceRolePolicy
IVSRecordToS3
QuickSightAccessForS3StorageManagementAnalyticsReadOnly
S3StorageLensServiceRolePolicy
S3USER
Customer managed


Add permissions
Permissions options
Add user to group
Copy permissions
Attach policies directly
Permissions policies (1/1223)
s3
13 matches
Policy name
Type
Attached entities
S3USER
Customer managed
Cancel
Next


Review
The following policies will be attached to this user. Learn more
User details
User name
IAMUSER
Permissions summary (1)
Name
Type
Used as
S3USER
Customer managed
Permissions policy
Cancel
Previous
Add permissions


1 policy added
IAMUSER Info
Delete
Summary
ARN
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 15:19 (UTC+05:30)
Last console sign-in
Today
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (2)
Remove
Add permissions
Filter by Type
All types
Policy name
Type
Attached via
IAMUserChangePassword
AWS managed
Directly
S3USER
Customer managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
Generate policy
No requests to generate a policy in the past 7 days.


Cloud Computing Architecture
Inbox (7,498) - thabe.shriya@
IAMUSER | IAM | Global
What Is Identity and Access M
New Tab
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/IAMUSER?section=security_credentials
Identity and Access Management (IAM)
IAMUSER
Summary
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://891377146069.signin.aws.amazon.com/console
User name
IAMUSER
Console password
n{NK74_5 Hide
Download .csv file
Close
Console sign-in
Multi-factor authentication (MFA) (0)
Access keys (0)
Type here to search
ENG
15:32
03-08-2024