→ Name: Khushi Jain ROLLNO: A023 SAPID: 86062300023

* Write up :-

1. Users and groups :

USERS :

⇒ In cloud computing, users are individuals entities that require access to cloud resource and services. Users can be human individuals or non-human entities (such as applications or services). Each user has a unique identity and is authenticated through credentials like usernames, passwords, SSH keys, or certificates. Users are assigned permissions that define what actions they can perform within the cloud environment.

Key aspects of Users :

- Identity Management : Ensures each user has a unique identity.
- Authentication : Verifies user identity through methods like passwords or multi-factor authentication.
- Authorization : Determines what actions a user can perform based on permissions.
- Types : End users, service accounts, administrators and external users.

GROUPS:

→ Groups in cloud computing are collections of users who share similar roles or access needs. Groups simplify permission management by allowing administrators to assign permissions and policies collectively rather than individually. This approach is approach is especially useful in large organizations, where managing individual user permissions can be complex.

Key Aspects of groups :

- Role-Based Access Control (RBAC): Assigns permissions based on roles to enhance security and reduce administrative tasks.
- Policy Enforcement: Ensures consistent application of security policies across all groups members.
- Scalability: Facilitates management of permissions for large number of users.
- Types: Security groups, resource groups, and user groups.

2) Identity and Access Management (IAM)?

→ Identity and Access Management (IAM) is a combination of policies of technologies that allows organizations to identify users and provide the right form of access as and when required. There has been a hurst in

the market with new applications, and the requirements for an organization to use these applications has increased drastically. The services and resources you want to access can be specified in IAM. IAM doesn't provide any replica or backup. IAM can be used for many purpose such as, if one wants to control access of individual & group access for your AWS resources. With IAM policies, managing permissions to your workforce and systems to ensure least-privilege permissions becomes easier. The AWS IAM is a global service.

→ Components of identity and access management (IAM)

1. Role
2. Groups
3. Policies

→ IAM identities classified as

1. IAM users
2. IAM Groups
3. IAM roles

3. IAM Roles :

→ A role is a set of permissions that grant access to actions and resources in AWS. These permissions are attached to the role, not to an IAM user or a group.

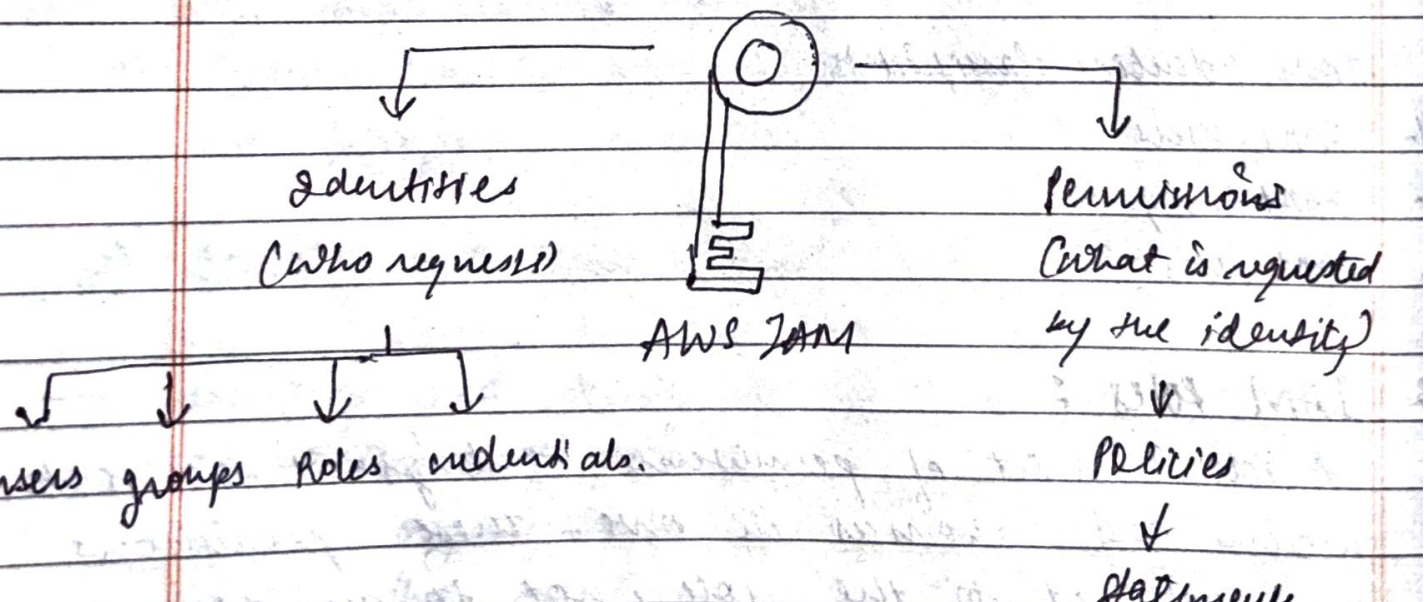
→ An IAM User can use a role in the same AWS account or a different account.

→ An IAM User is similar to an IAM user; role is also an AWS identity with permission policies that determine what the identity can & cannot do in AWS.

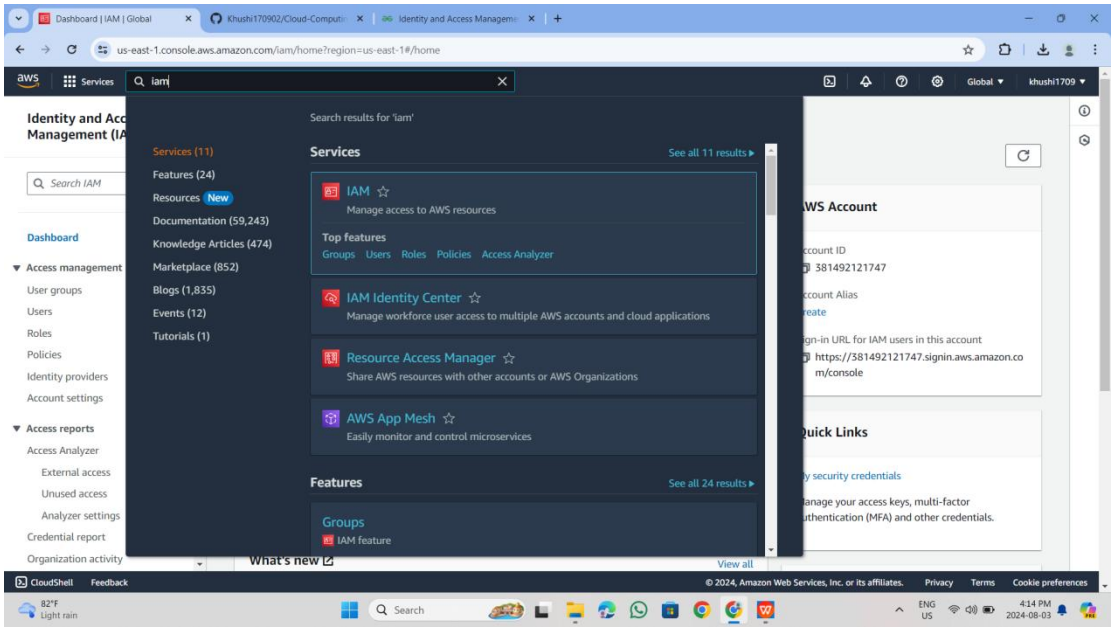
→ A role is a not uniquely associated with a single person; it can be used by anyone who needs it.

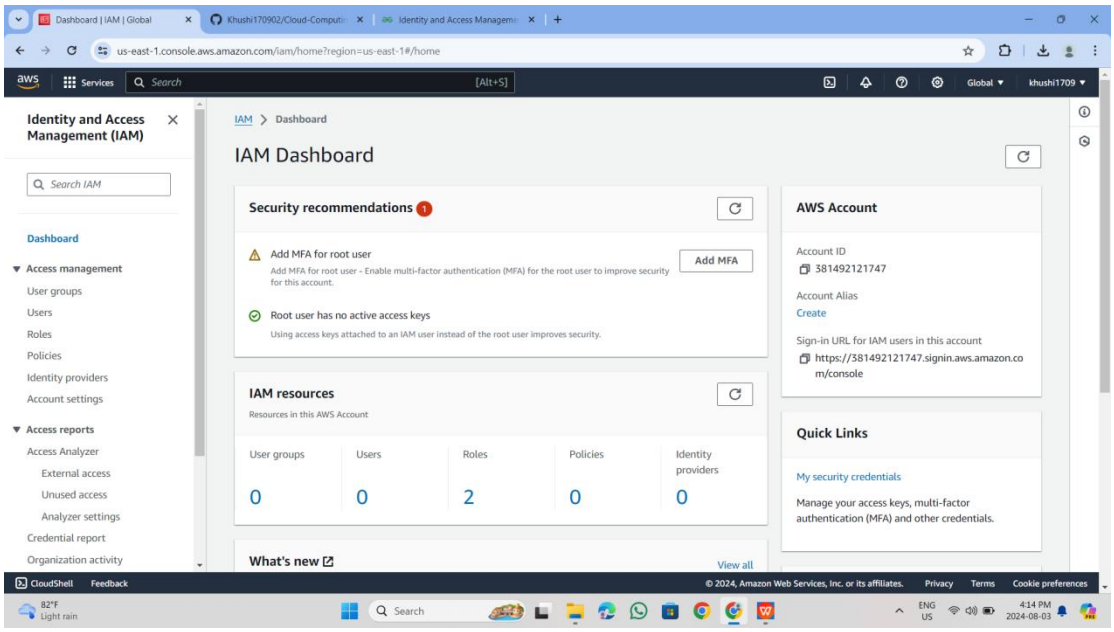
→ A role ~~it~~ does not have long term security credential, i.e password or security key. Instead, if the user uses a role, temporarily security credentials are created & provided to the user.

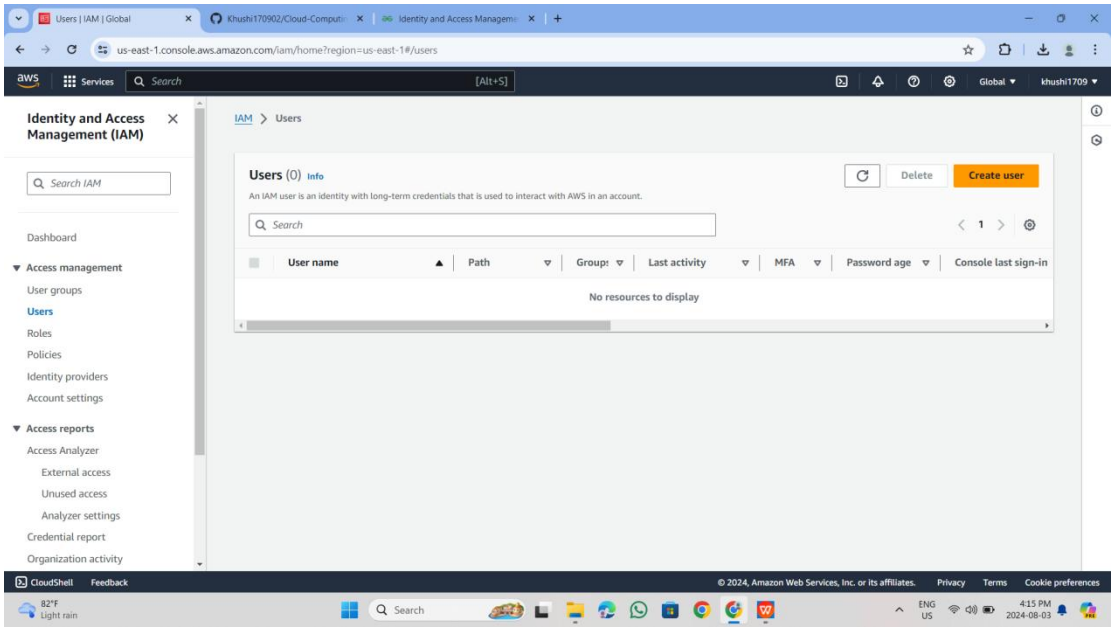
→ You can use the roles to delegate access to users, applications or services that generally donot have access to your AWS account/ resources.

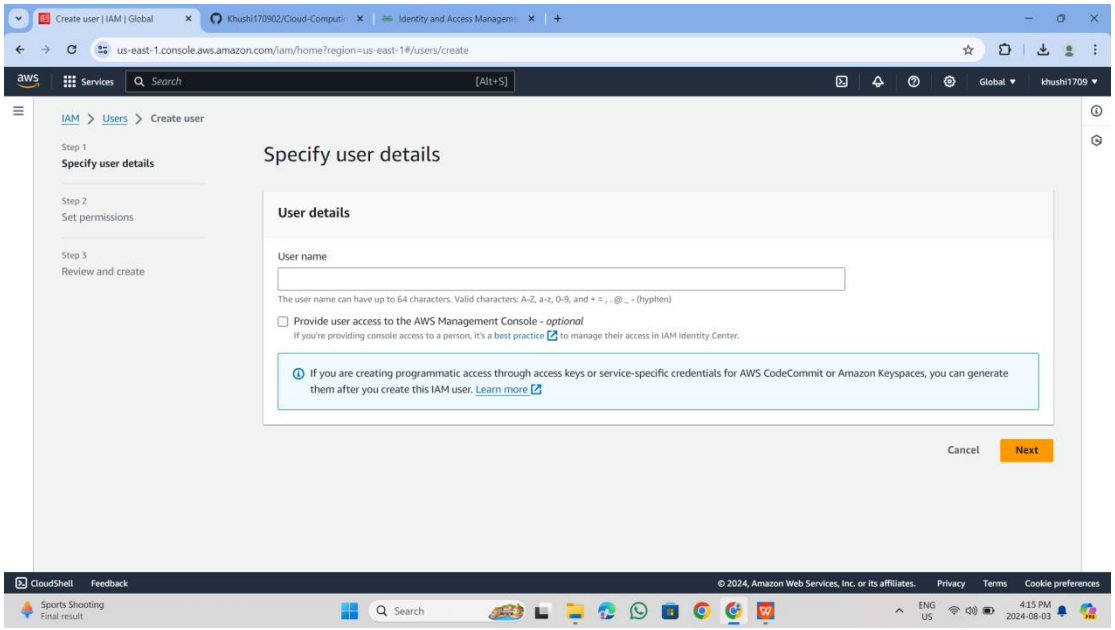


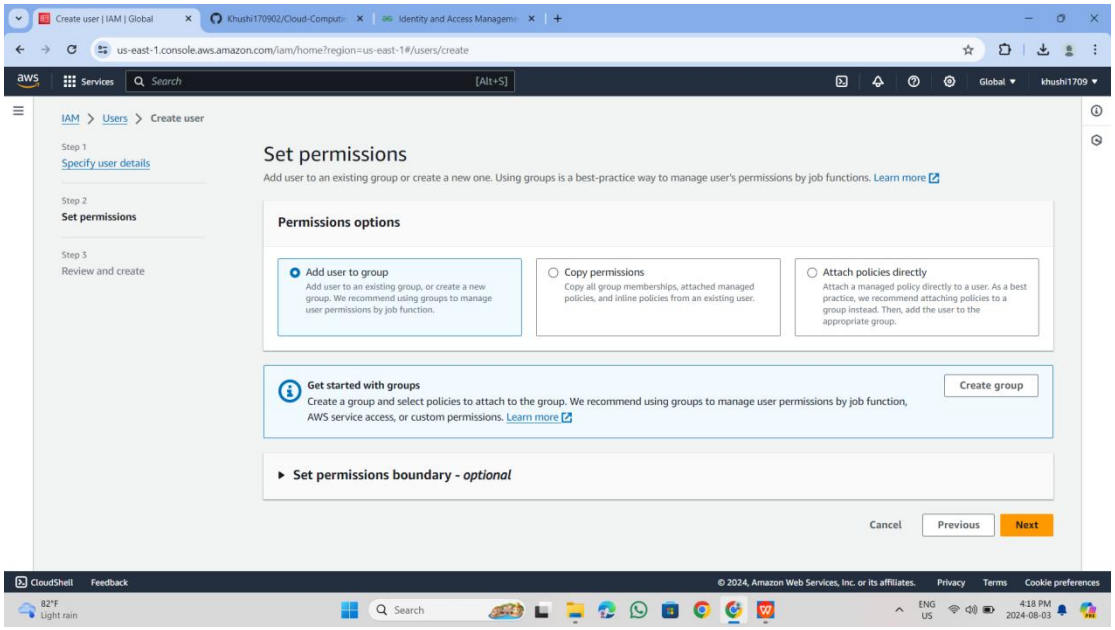
IAM USER

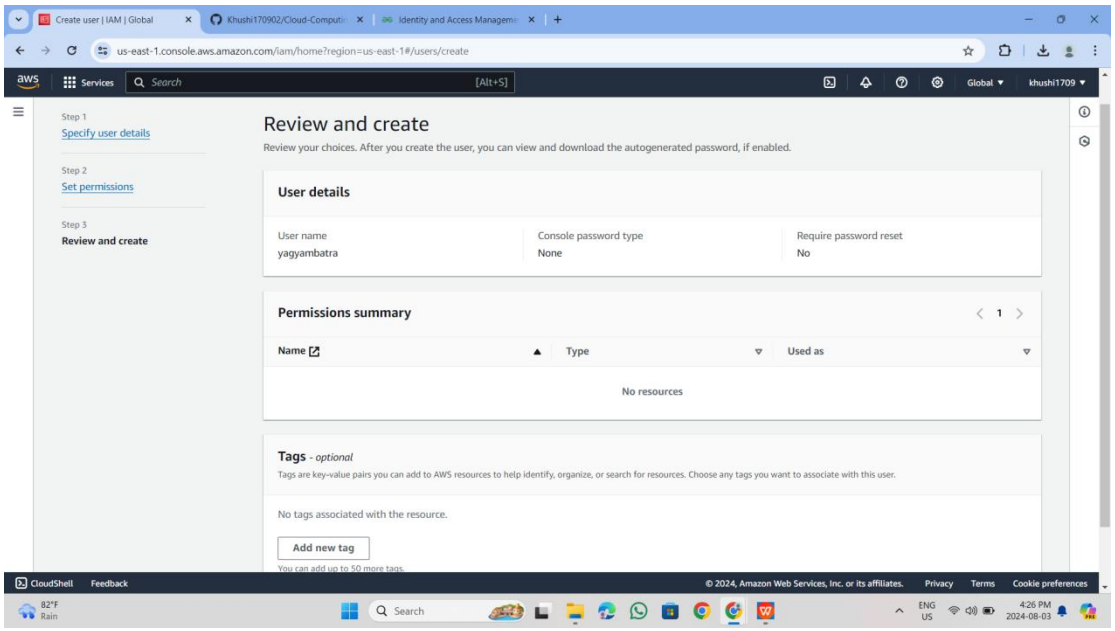

Dashboard | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home
aws
Services
iam
Global
khushi1709
Search results for 'iam'
Services (11)
Features (24)
Resources New
Documentation (59,243)
Knowledge Articles (474)
Marketplace (852)
Blogs (1,835)
Events (12)
Tutorials (1)
Services
See all 11 results
IAM
Manage access to AWS resources
Top features
Groups Users Roles Policies Access Analyzer
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
AWS App Mesh
Easily monitor and control microservices
Features
See all 24 results
Groups
IAM feature
Identity and Acc
Management (IA
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
What's new
View all
AWS Account
Account ID
381492121747
Account Alias
Create
Sign-in URL for IAM users in this account
https://381492121747.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
82°F
Light rain
Search
ENG
US
4:14 PM
2024-08-03

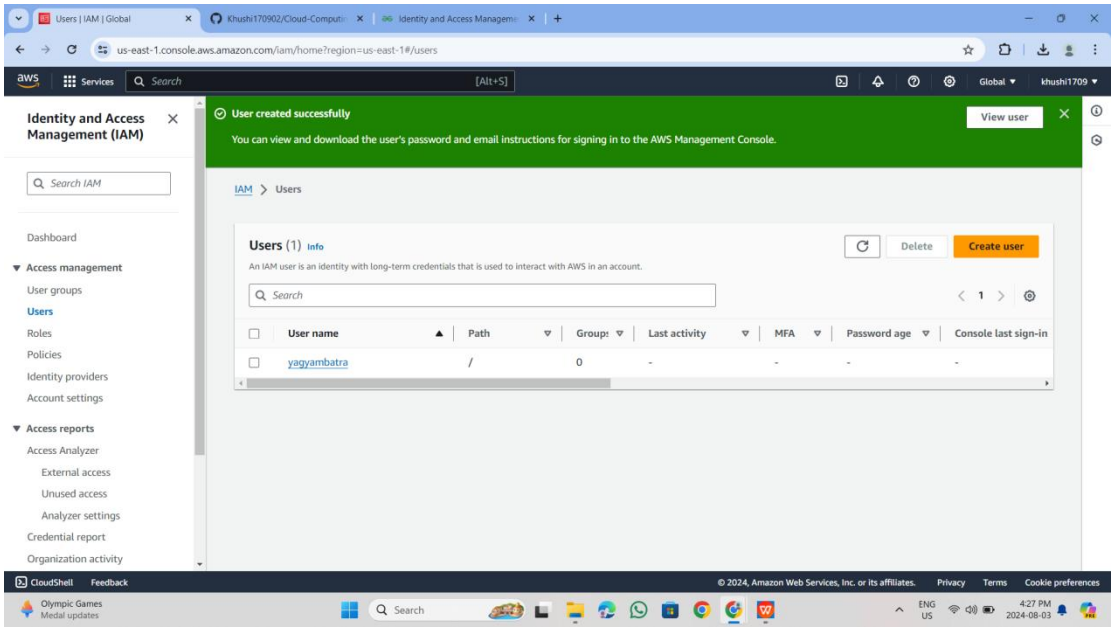

Dashboard | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home
aws
Services
Search
[Alt+S]
Global
khushi1709
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
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
View all
AWS Account
Account ID
381492121747
Account Alias
Create
Sign-in URL for IAM users in this account
https://381492121747.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
82°F
Light rain
Search
ENG
US
4:14 PM
2024-08-03

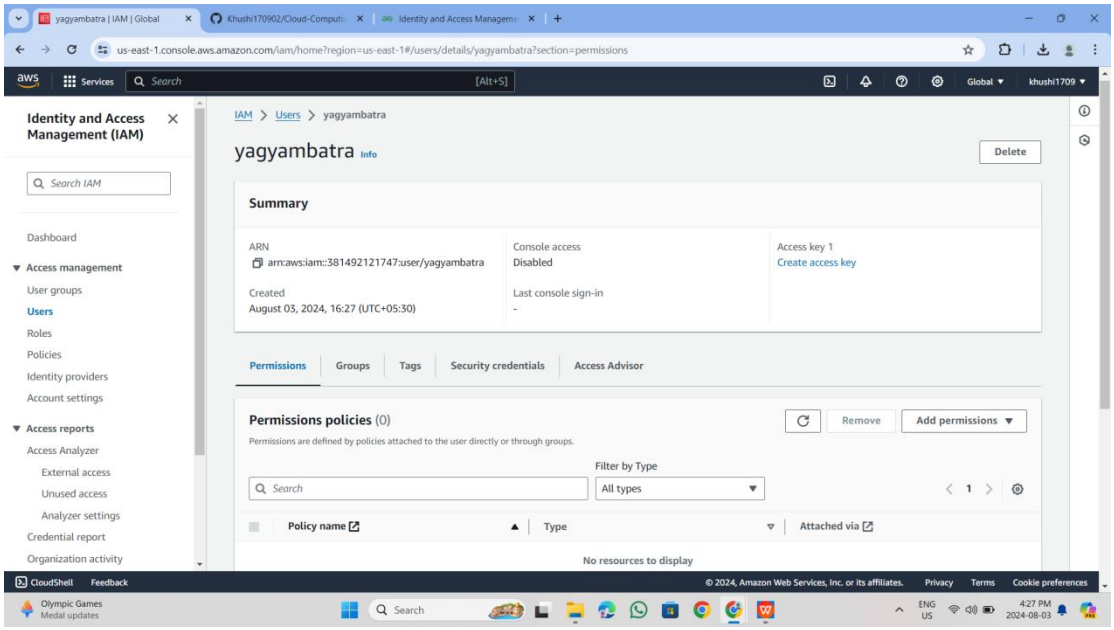

Users | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
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
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
No resources to display
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

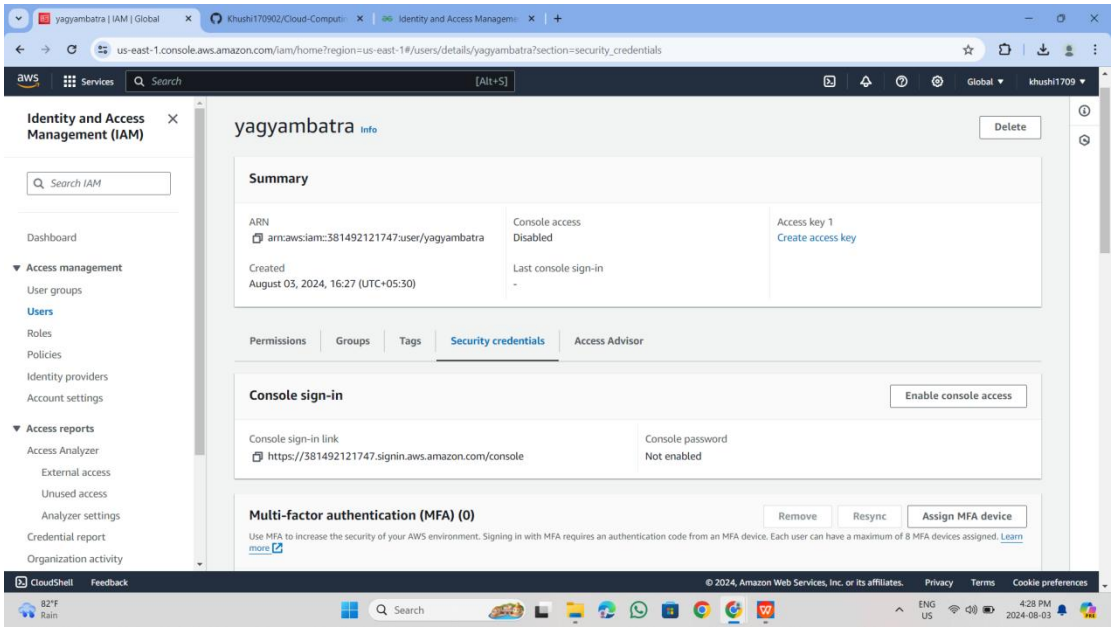

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
The user name can have up to 64 characters. Valid characters: 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

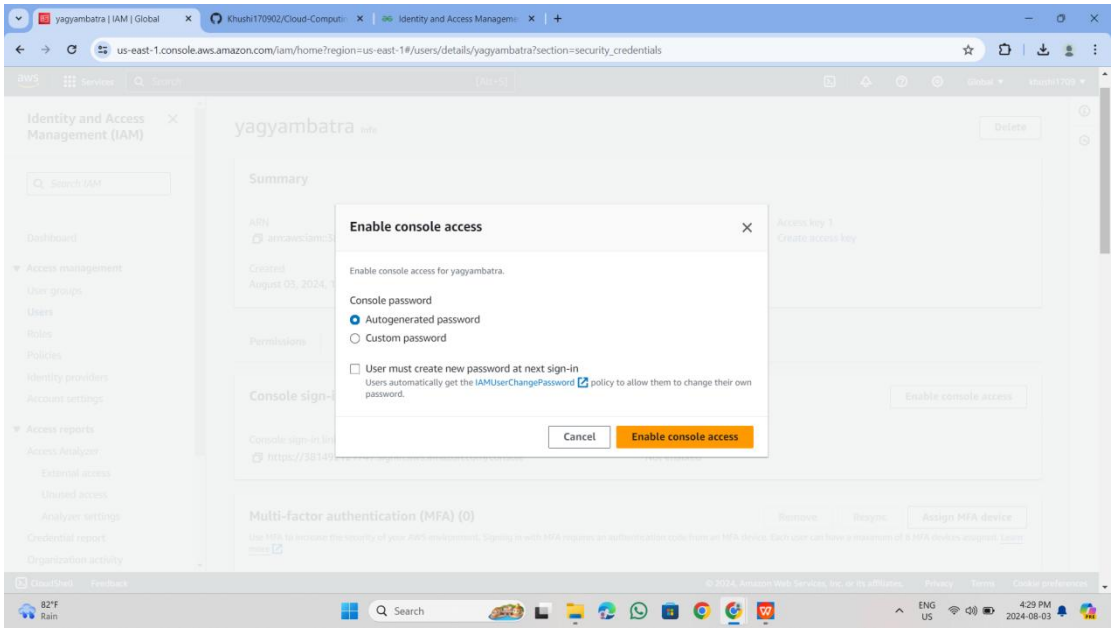

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
Services
Search
[Alt+S]
Global
khushi1709
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set permissions
Add user to an existing group or create a 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
82°F
Light rain
Search
ENG
US
4:18 PM
2024-08-03

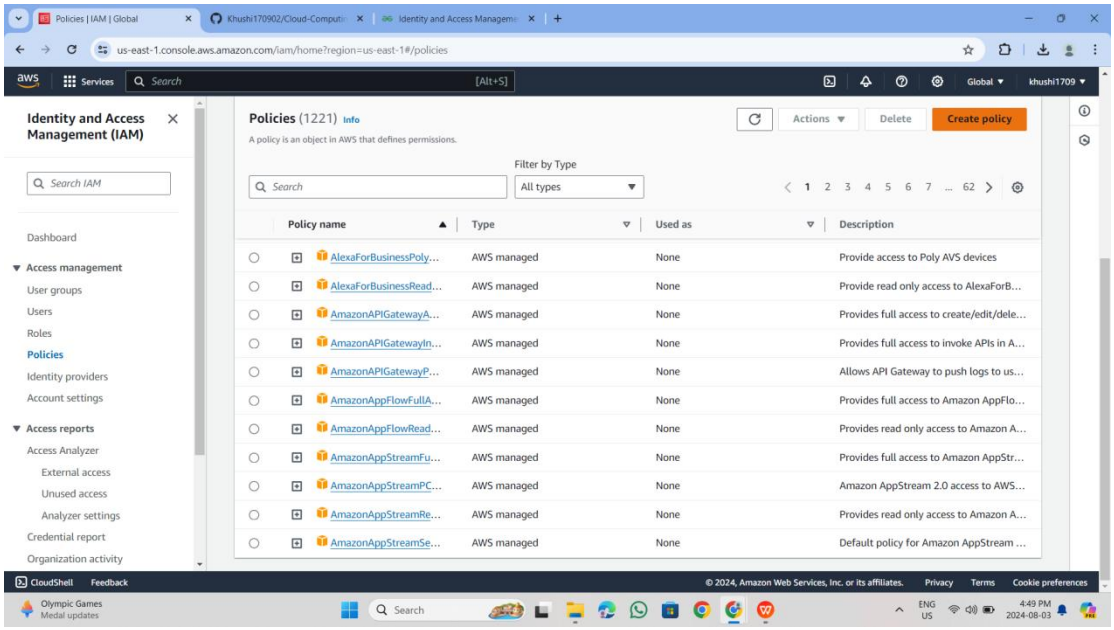

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
Services
Search
[Alt+S]
Global
khushi1709
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
yagyambatra
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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
82°F
Rain
Search
ENG
US
4:26 PM
2024-08-03

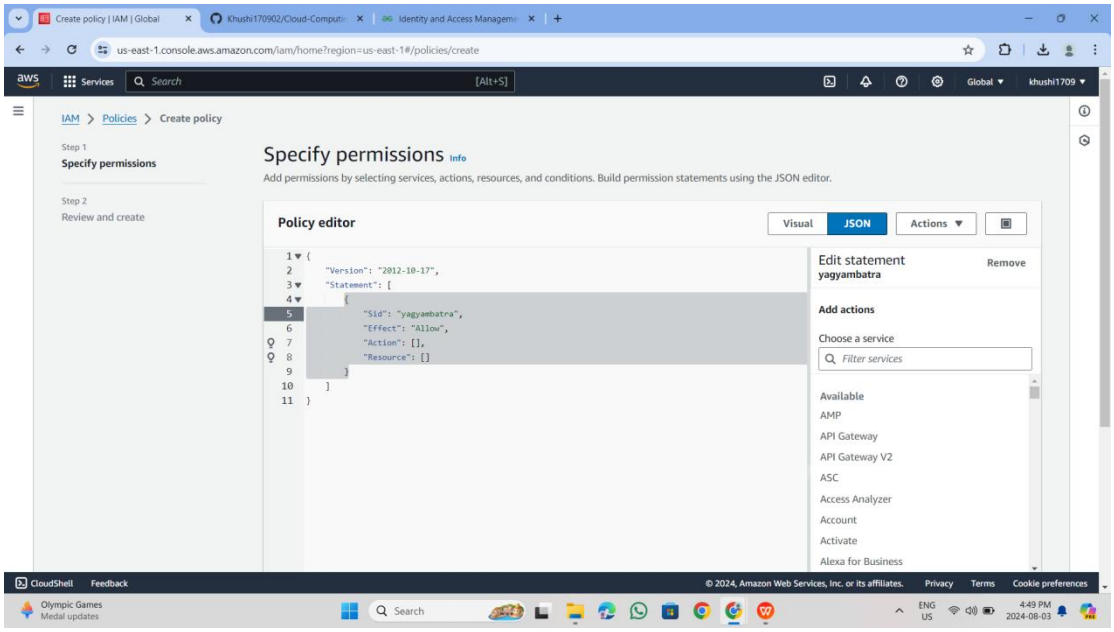

Users | IAM | Global
Khushi170902/Cloud-Computi
Identity and Access Managem
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users
Services
Search
[Alt+S]
Global
khushi1709
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
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
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
Groups
Last activity
MFA
Password age
Console last sign-in
yagyambatra
/
0
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Olympic Games
Medal updates
Search
ENG
US
4:27 PM
2024-08-03

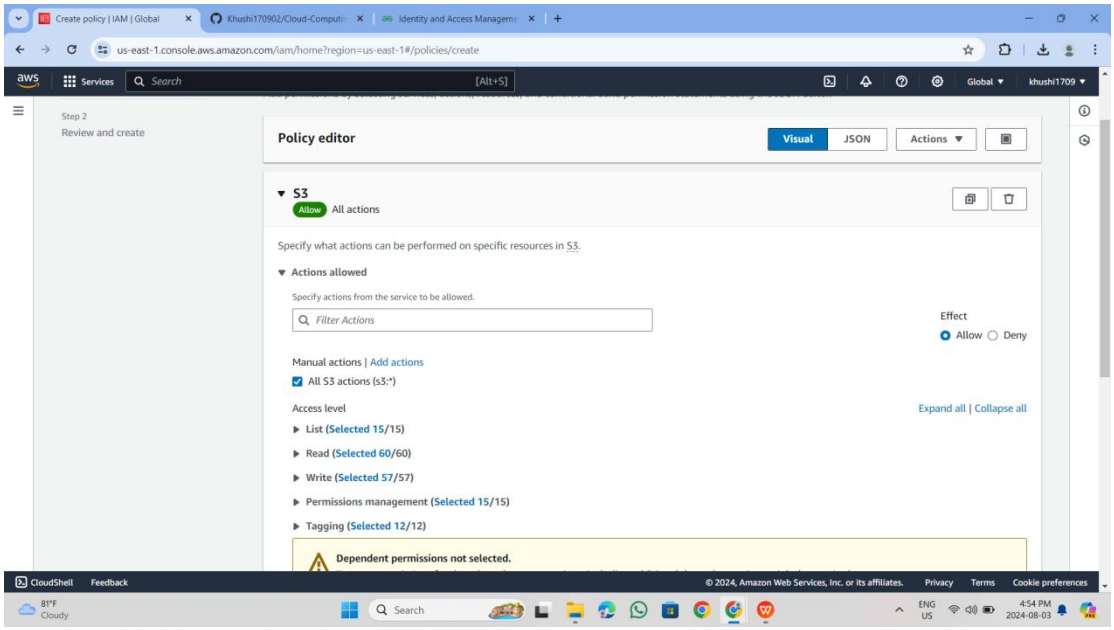

yagyambatra | IAM | Global
Khushi170902/Cloud-Computi
Identity and Access Managem
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra?section=permissions
Services
Search
[Alt+S]
Global
khushi1709
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
IAM > Users > yagyambatra
yagyambatra Info
Delete
Summary
ARN
arn:aws:iam::381492121747:user/yagyambatra
Console access
Disabled
Access key 1
Create access key
Created
August 03, 2024, 16:27 (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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Olympic Games
Medal updates
Search
ENG
US
4:27 PM
2024-08-03

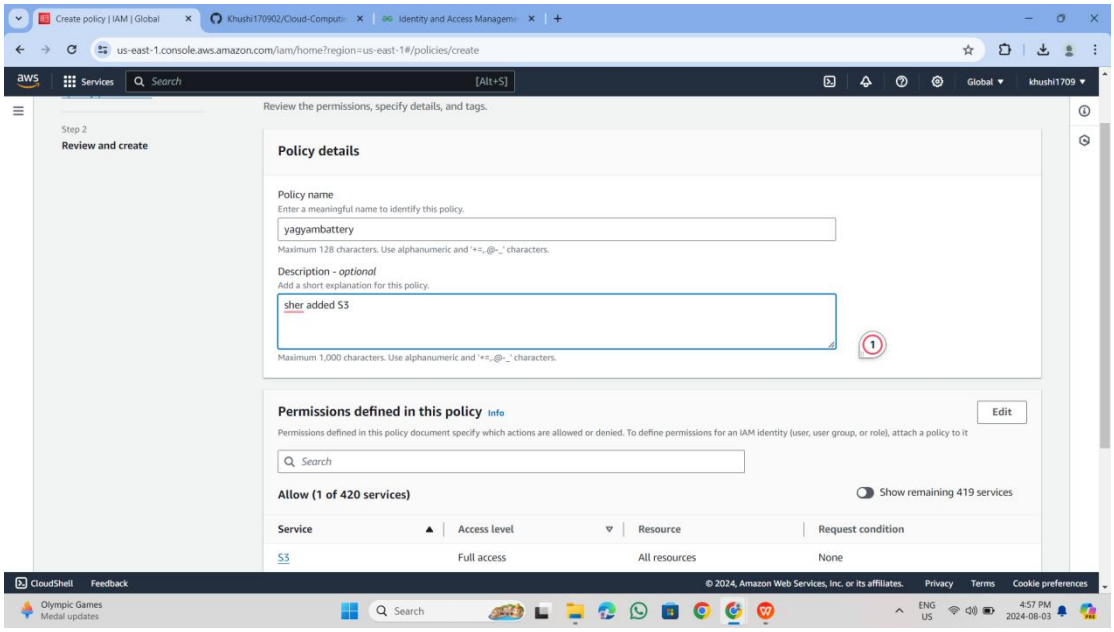

yagyambatra | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra?section=security_credentials
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
yagyambatra Info
Delete
Summary
ARN
arn:aws:iam::381492121747:user/yagyambatra
Console access
Disabled
Access key 1
Create access key
Created
August 03, 2024, 16:27 (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://381492121747.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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

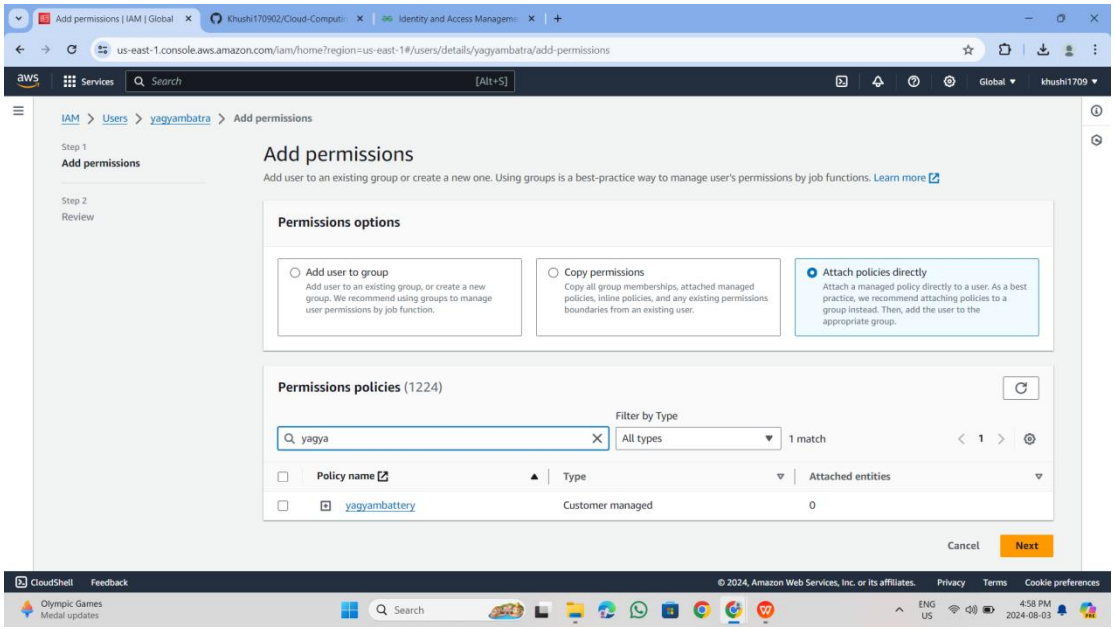

Enable console access
Enable console access for yagyambatra.
Console password
Autogenerated password
Custom password
User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
Cancel
Enable console access

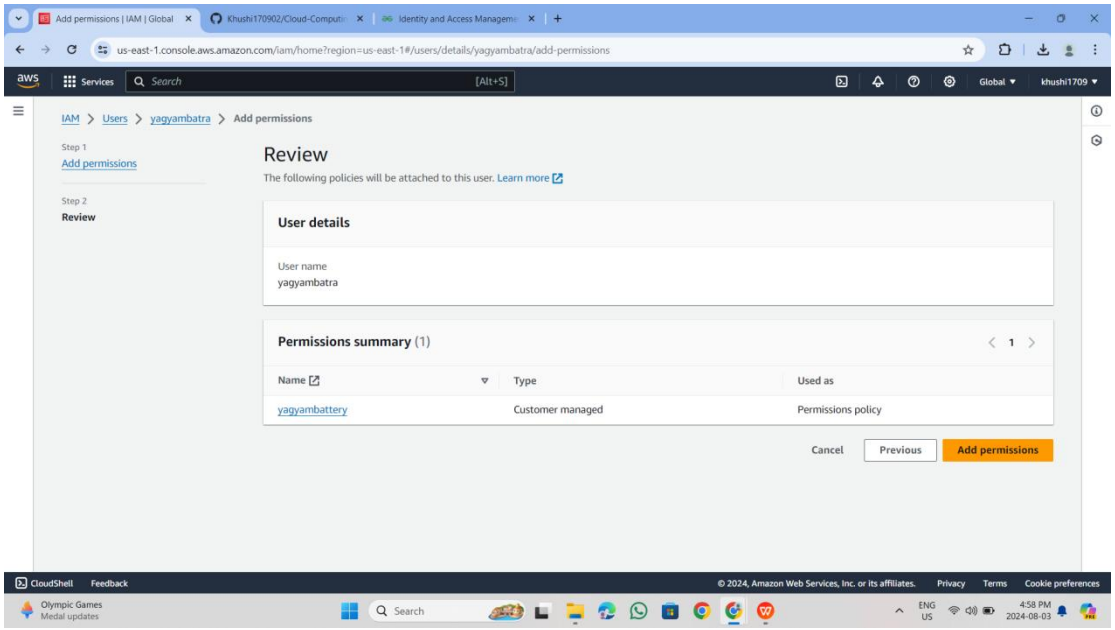

Policies | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Policies (1221) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
All types
Policy name
Type
Used as
Description
AlexaForBusinessPoly... AWS managed None Provide access to Poly AVS devices
AlexaForBusinessRead... AWS managed None Provide read only access to AlexaForB...
AmazonAPIGatewayA... AWS managed None Provides full access to create/edit/dele...
AmazonAPIGatewayIn... AWS managed None Provides full access to invoke APIs in A...
AmazonAPIGatewayP... AWS managed None Allows API Gateway to push logs to us...
AmazonAppFlowFullA... AWS managed None Provides full access to Amazon AppFlo...
AmazonAppFlowRead... AWS managed None Provides read only access to Amazon A...
AmazonAppStreamFu... AWS managed None Provides full access to Amazon AppStr...
AmazonAppStreamPC... AWS managed None Amazon AppStream 2.0 access to AWS...
AmazonAppStreamRe... AWS managed None Provides read only access to Amazon A...
AmazonAppStreamSe... AWS managed None Default policy for Amazon AppStream ...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

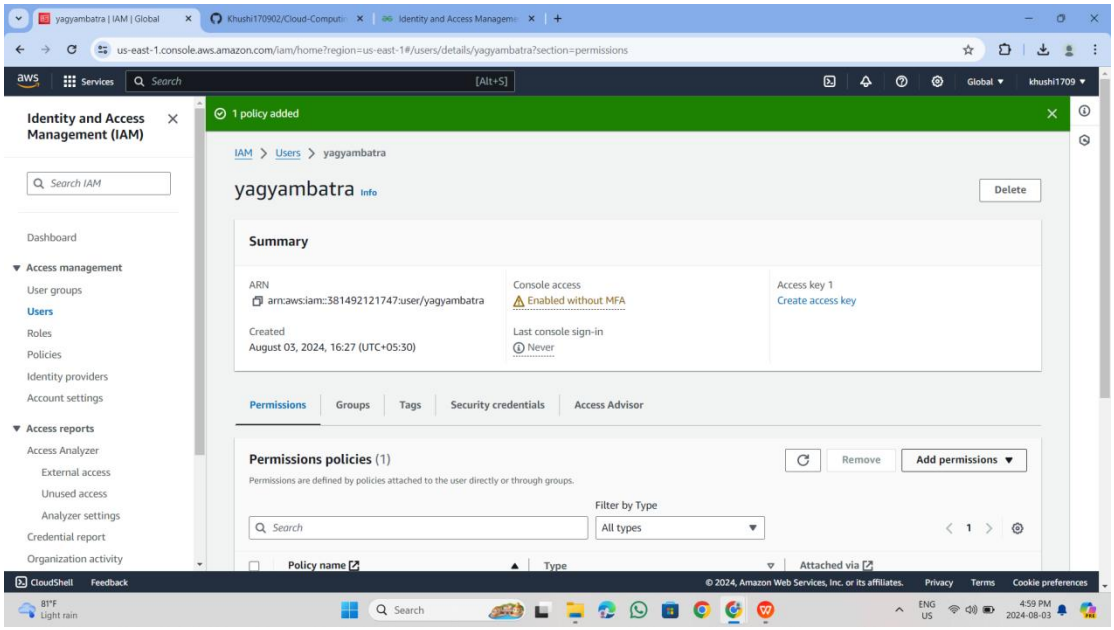

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "yagyambatra",
"Effect": "Allow",
"Action": [],
"Resource": []
}
]
}
Edit statement
yagyambatra
Remove
Add actions
Choose a service
Filter services
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
Activate
Alexa for Business
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

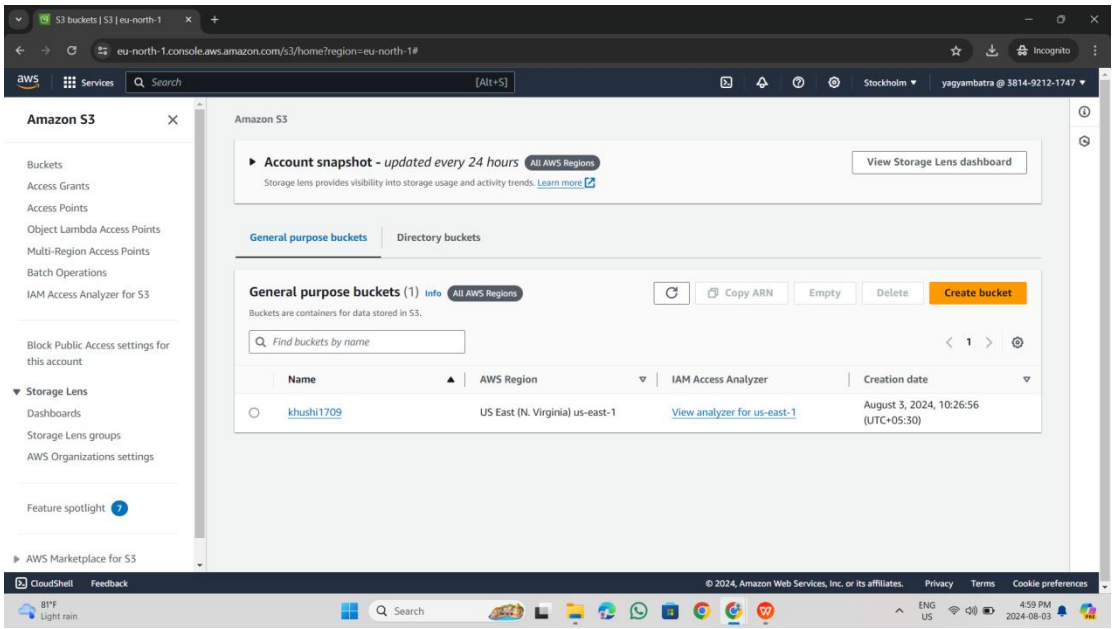

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Services
Search
[Alt+S]
Global
khushi1709
Step 2
Review and create
Policy editor
Visual
JSON
Actions
S3
Allow
All actions
Specify what actions can be performed on specific resources in S3.
Actions 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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
81°F
Cloudy
Search
ENG
US
4:54 PM
2024-08-03

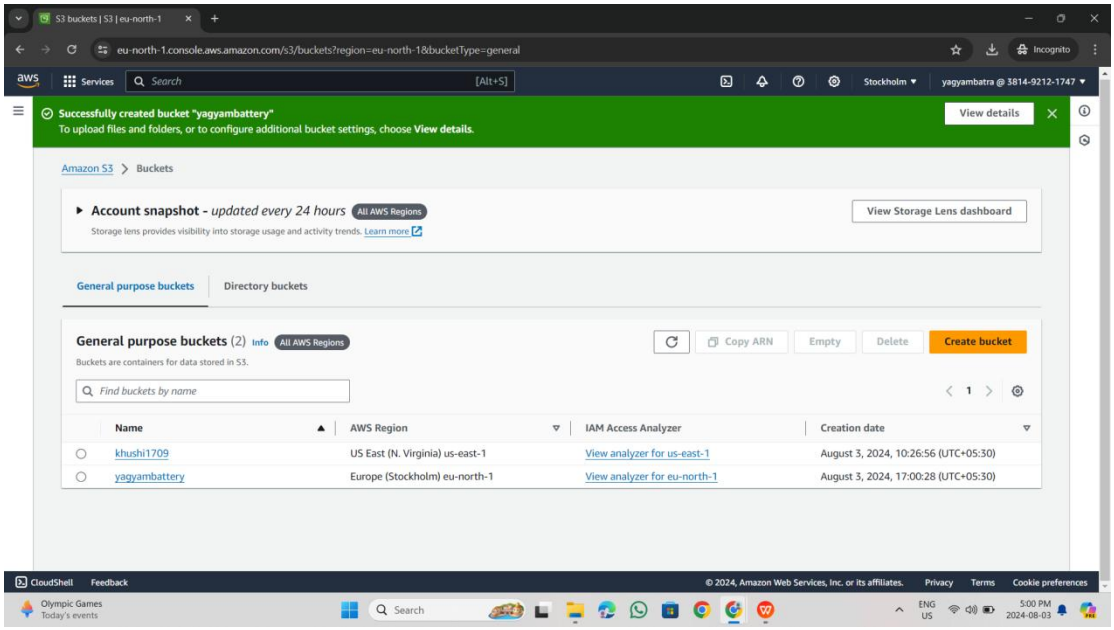

Create policy | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Services
Search
[Alt+S]
Global
khushi1709
Review the permissions, specify details, and tags.
Step 2
Review and create
Policy details
Policy name
Enter a meaningful name to identify this policy.
yagyambattery
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
sher added S3
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Olympic Games
Medal updates
Search
ENG
US
4:57 PM
2024-08-03

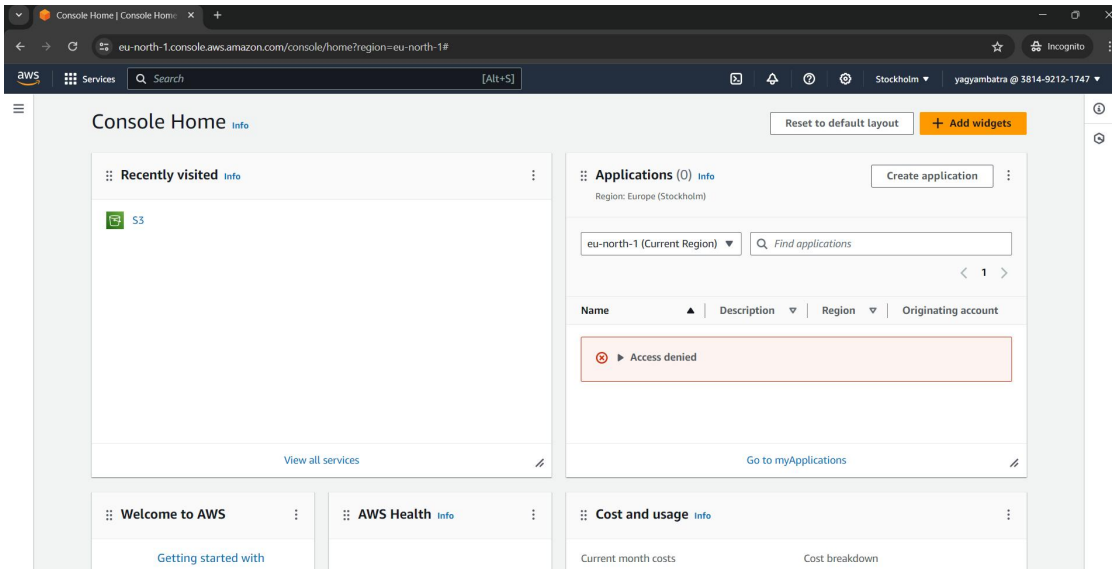

Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra/add-permissions
Services
Search
[Alt+S]
Global
khushi1709
IAM > Users > yagyambatra > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group 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
yagya
All types
1 match
Policy name
Type
Attached entities
yagyambattery
Customer managed
0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Olympic Games
Medal updates
Search
ENG
US
4:58 PM
2024-08-03


Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra/add-permissions
Services
Search
[Alt+S]
Global
khushi1709
IAM > Users > yagyambatra > 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
yagyambatra
Permissions summary (1)
Name
Type
Used as
yagyambattery
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Olympic Games
Medal updates
Search
ENG
US
4:58 PM
2024-08-03

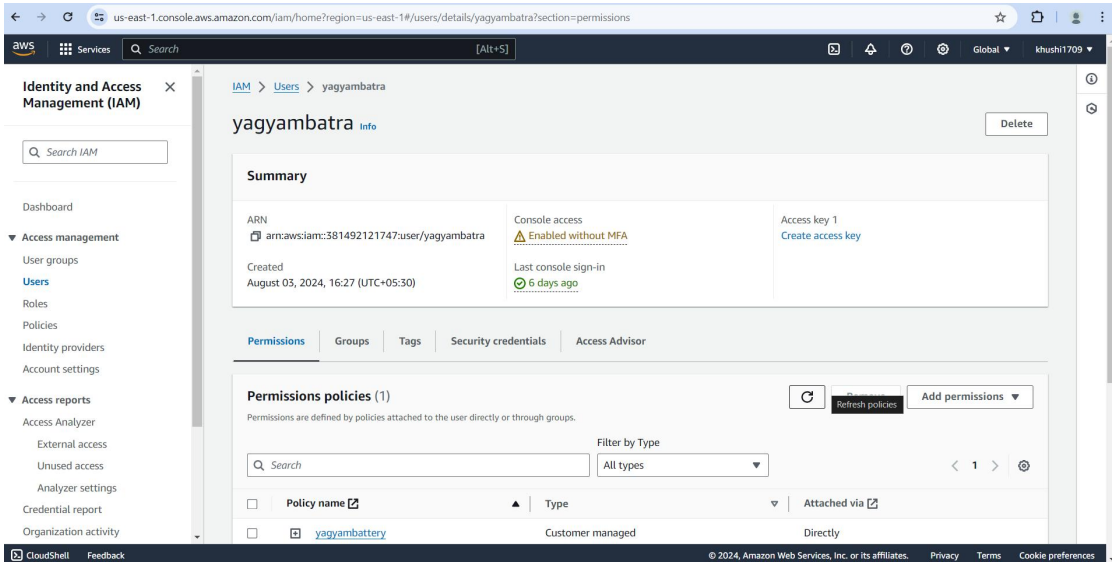

yagyambatra | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra?section=permissions
Identity and Access Management (IAM)
1 policy added
IAM > Users > yagyambatra
yagyambatra Info
Delete
Summary
ARN
arn:aws:iam::381492121747:user/yagyambatra
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:27 (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
All types
Policy name
Type
Attached via
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

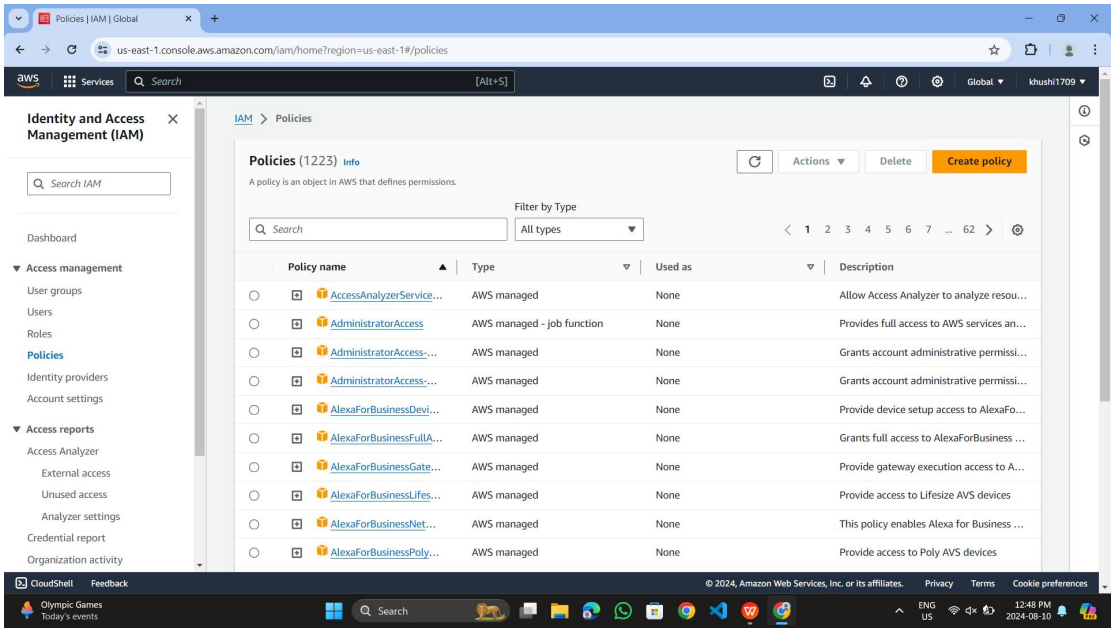

S3 buckets | S3 | eu-north-1
eu-north-1.console.aws.amazon.com/s3/home?region=eu-north-1#
Amazon S3
Amazon S3
Account snapshot - updated every 24 hours
All AWS Regions
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
khushi1709
US East (N. Virginia) us-east-1
View analyzer for us-east-1
August 3, 2024, 10:26:56 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

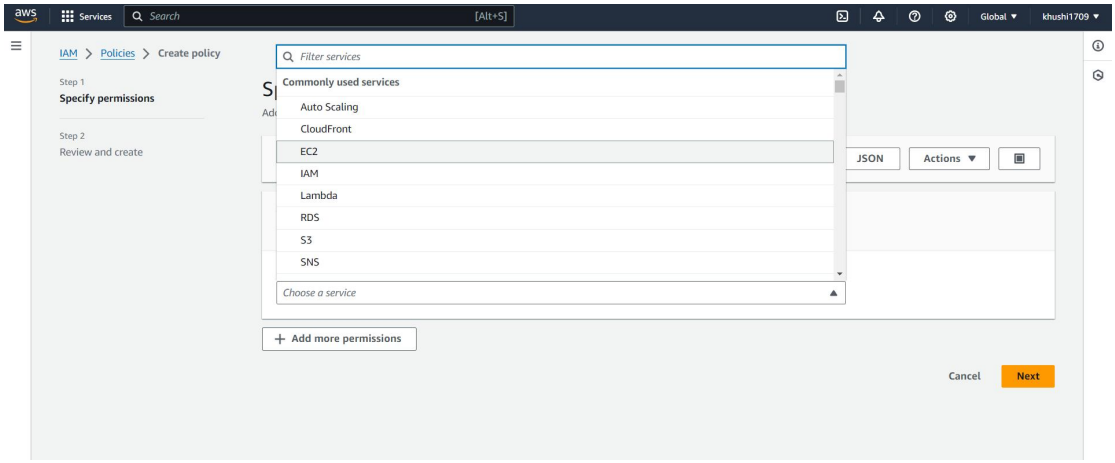

S3 buckets | S3 | eu-north-1
eu-north-1.console.aws.amazon.com/s3/buckets?region=eu-north-1&bucketType=general
Incognito
Services
Search
[Alt+S]
Stockholm
yagyambatra @ 3814-9212-1747
Successfully created bucket "yagyambattery"
To upload files and folders, or to configure additional bucket settings, 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 (2) 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
khushi1709
US East (N. Virginia) us-east-1
View analyzer for us-east-1
August 3, 2024, 10:26:56 (UTC+05:30)
yagyambattery
Europe (Stockholm) eu-north-1
View analyzer for eu-north-1
August 3, 2024, 17:00:28 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Olympic Games
Today's events
Search
ENG
US
5:00 PM
2024-08-03

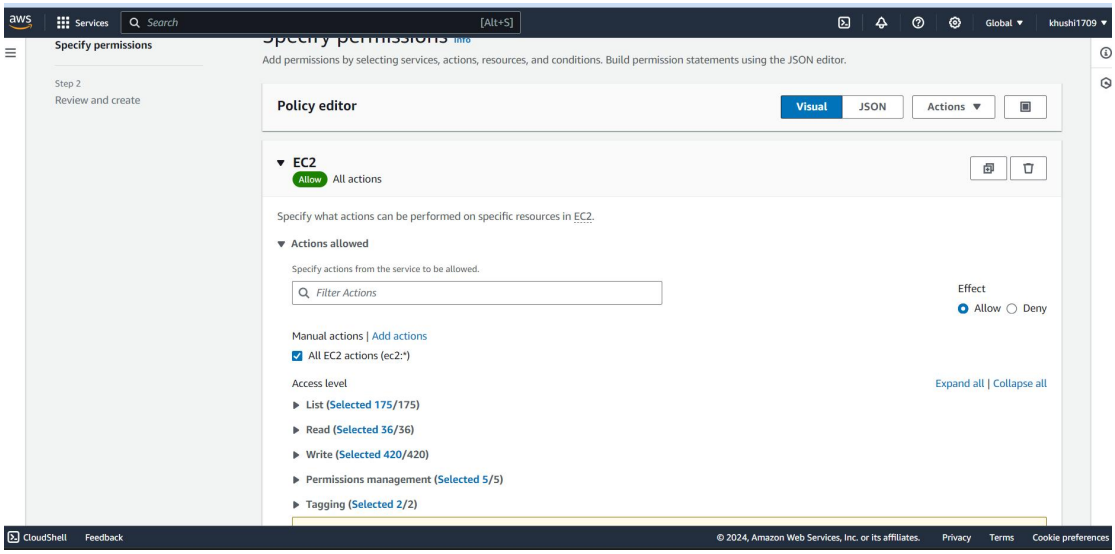

Console Home | Console Home
eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#
Incognito
Services
Search
[Alt+S]
Stockholm
yagyambatra @ 3814-9212-1747
Console Home Info
Reset to default layout
Add widgets
Recently visited Info
S3
View all services
Applications (0) Info
Region: Europe (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 Health Info
Cost and usage Info
Current month costs
Cost breakdown

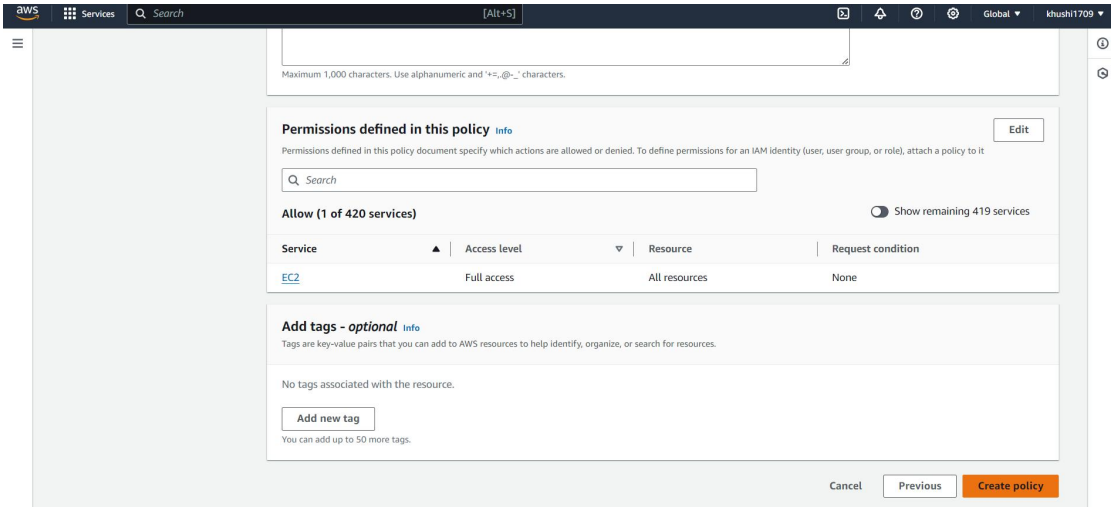
For EC2

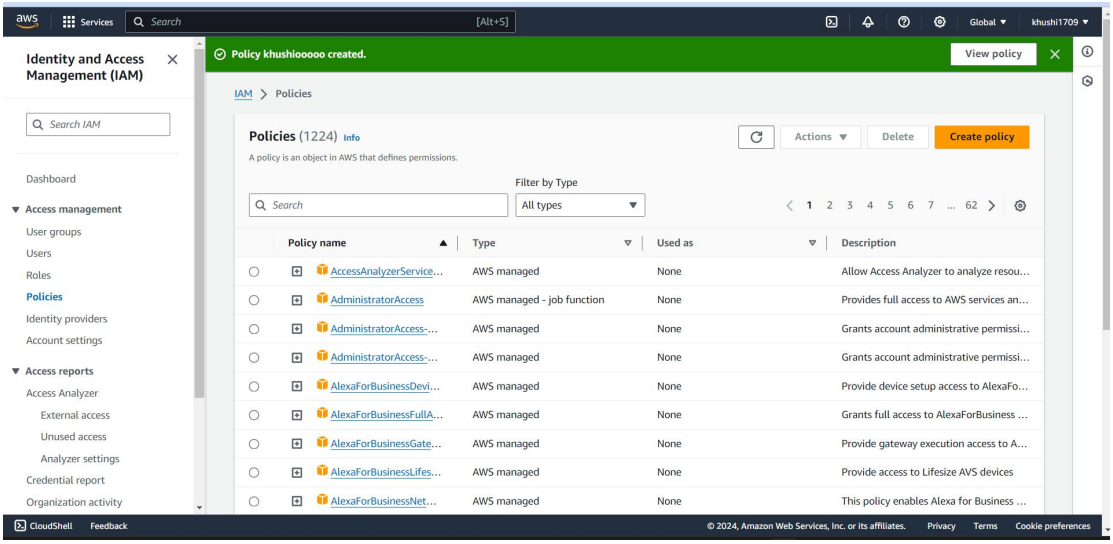

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra?section=permissions
Identity and Access Management (IAM)
IAM > Users > yagyambatra
yagyambatra Info
Delete
Summary
ARN
arn:aws:iam::381492121747:user/yagyambatra
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:27 (UTC+05:30)
Last console sign-in
6 days ago
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Refresh policies
Add permissions
Filter by Type
All types
Policy name
Type
Attached via
yagyambattery
Customer managed
Directly

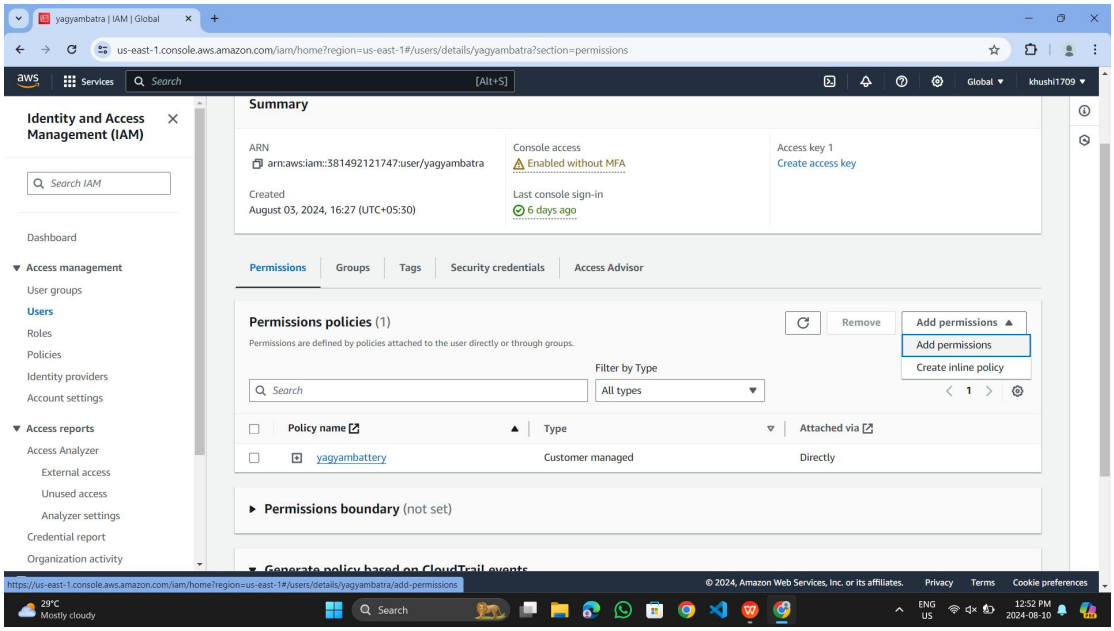

Policies | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies
Identity and Access Management (IAM)
IAM > Policies
Policies (1223) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
All types
Policy name
Type
Used as
Description
AccessAnalyzerService...
AWS managed
None
Allow Access Analyzer to analyze resou...
AdministratorAccess
AWS managed - job function
None
Provides full access to AWS services an...
AdministratorAccess-...
AWS managed
None
Grants account administrative permissi...
AlexaForBusinessDevi...
AlexaForBusinessFullA...
AlexaForBusinessGate...
AlexaForBusinessLifes...
AlexaForBusinessNet...
AlexaForBusinessPoly...
Provide device setup access to AlexaFo...
Grants full access to AlexaForBusiness ...
Provide gateway execution access to A...
Provide access to Lifesize AVS devices
This policy enables Alexa for Business ...
Provide access to Poly AVS devices

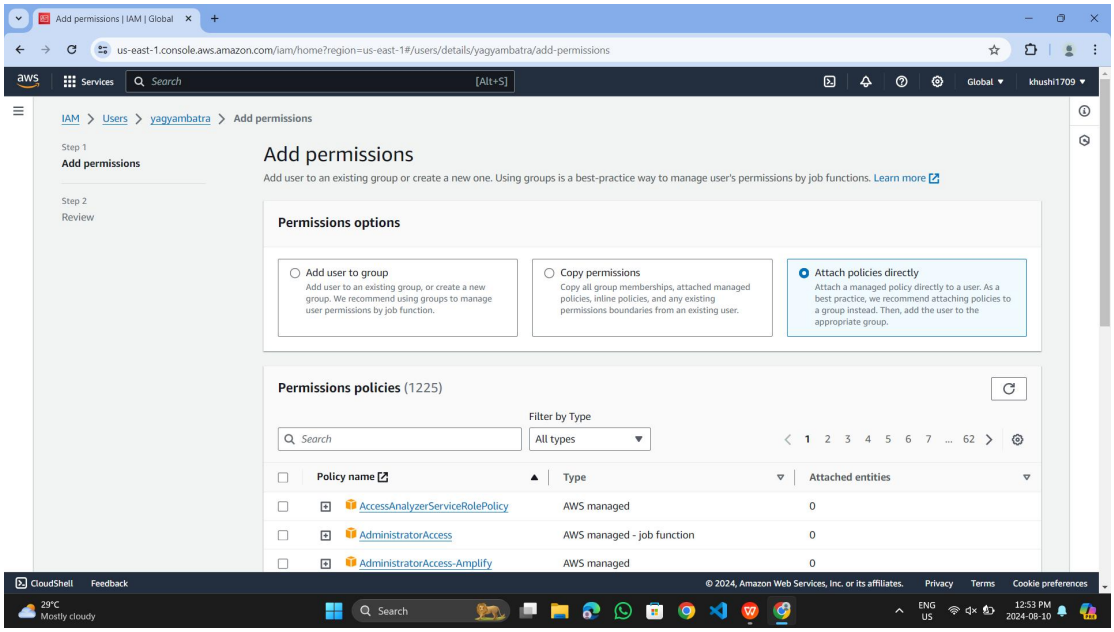

aws
Services
Search
[Alt+S]
Global
khushi1709
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Filter services
Commonly used services
Auto Scaling
CloudFront
EC2
IAM
Lambda
RDS
S3
SNS
Choose a service
JSON
Actions
Add more permissions
Cancel
Next

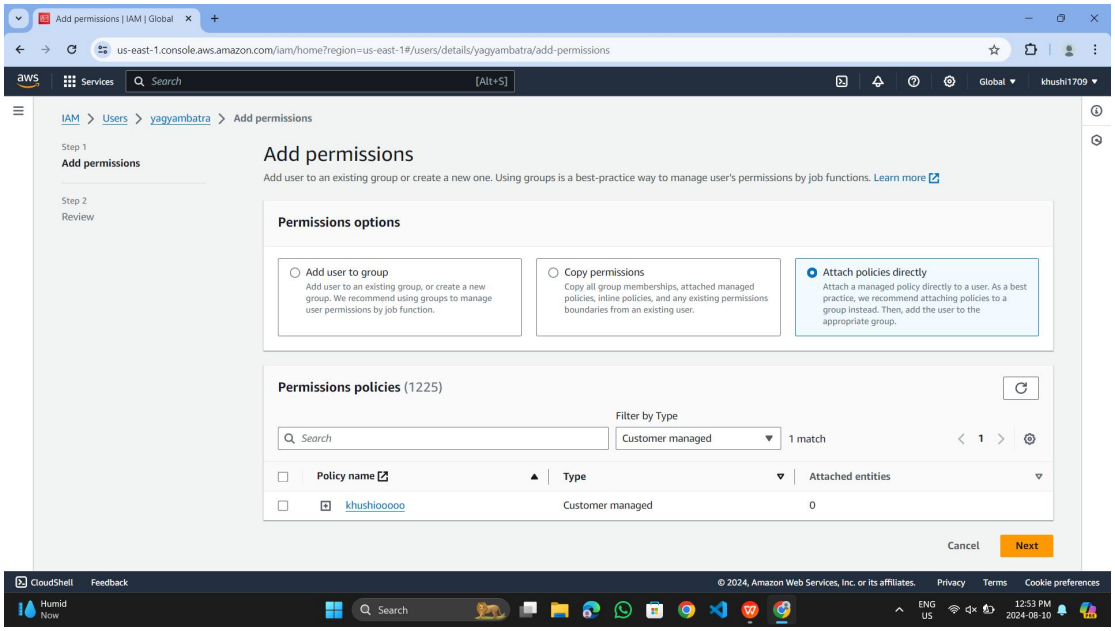

aws
Services
Search
[Alt+S]
Global
khushi1709
Specify permissions
Step 2
Review and create
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
EC2
Allow
All actions
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All EC2 actions (ec2:*)
Access level
Expand all | Collapse all
List (Selected 175/175)
Read (Selected 36/36)
Write (Selected 420/420)
Permissions management (Selected 5/5)
Tagging (Selected 2/2)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

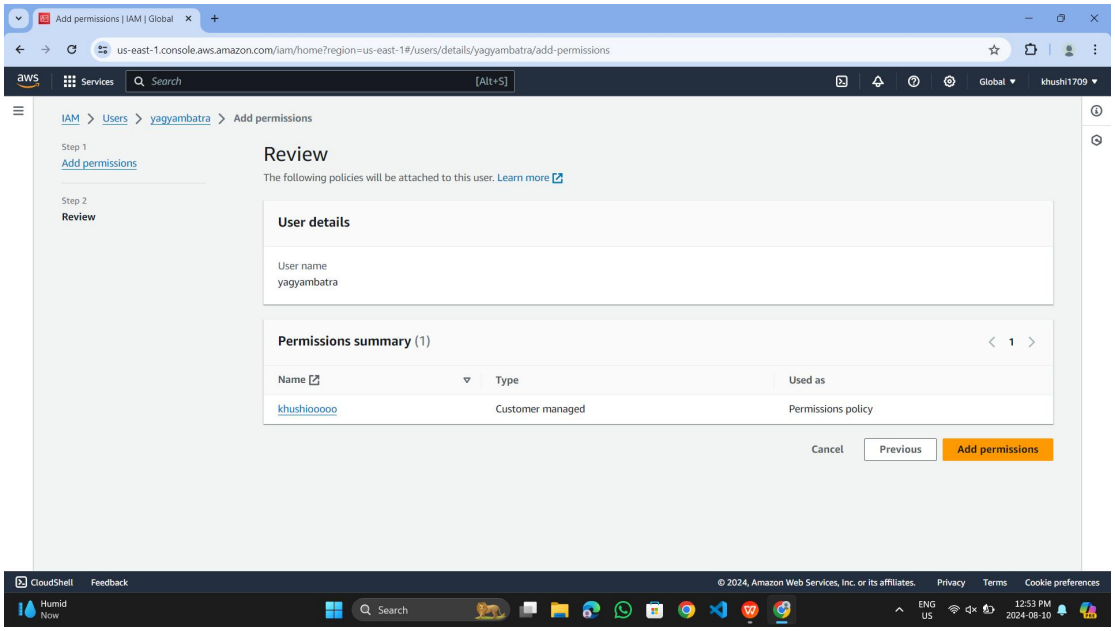

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 420 services)
Show remaining 419 services
Service
Access level
Resource
Request condition
EC2
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.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create policy

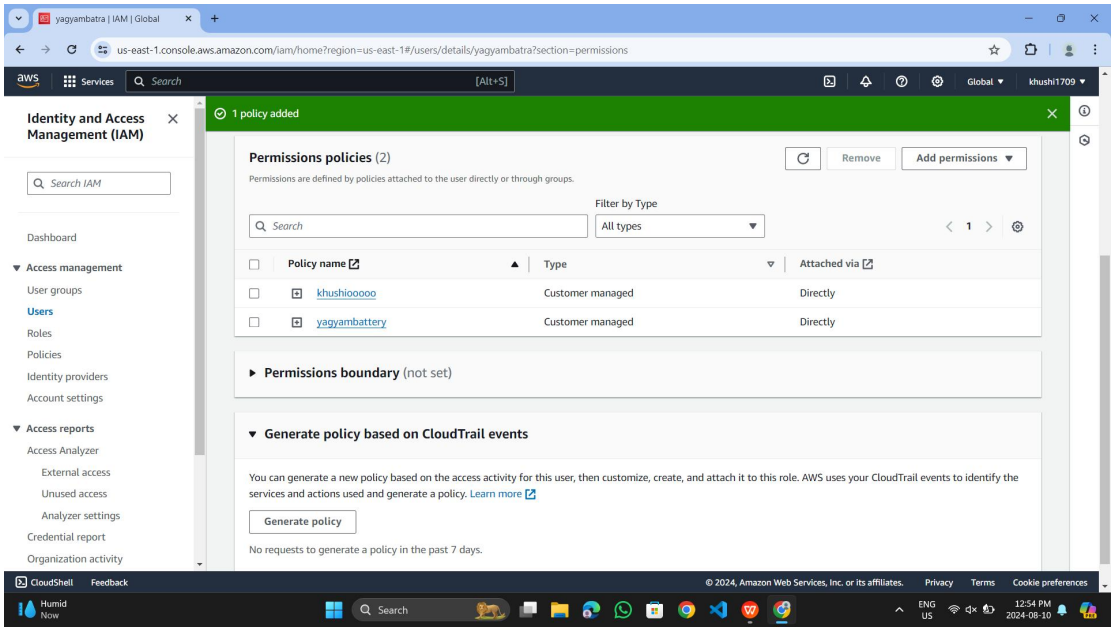

Policy khushioooo created.
View policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
IAM > Policies
Policies (1224) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
All types
Policy name
Type
Used as
Description
AccessAnalyzerService...
AWS managed
None
Allow Access Analyzer to analyze resou...
AdministratorAccess
AWS managed - job function
None
Provides full access to AWS services an...
AdministratorAccess-...
AWS managed
None
Grants account administrative permissi...
AdministratorAccess-...
AWS managed
None
Grants account administrative permissi...
AlexaForBusinessDevi...
AWS managed
None
Provide device setup access to AlexaFo...
AlexaForBusinessFullA...
AWS managed
None
Grants full access to AlexaForBusiness ...
AlexaForBusinessGate...
AWS managed
None
Provide gateway execution access to A...
AlexaForBusinessLifes...
AWS managed
None
Provide access to Lifesize AVS devices
AlexaForBusinessNet...
AWS managed
None
This policy enables Alexa for Business ...
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

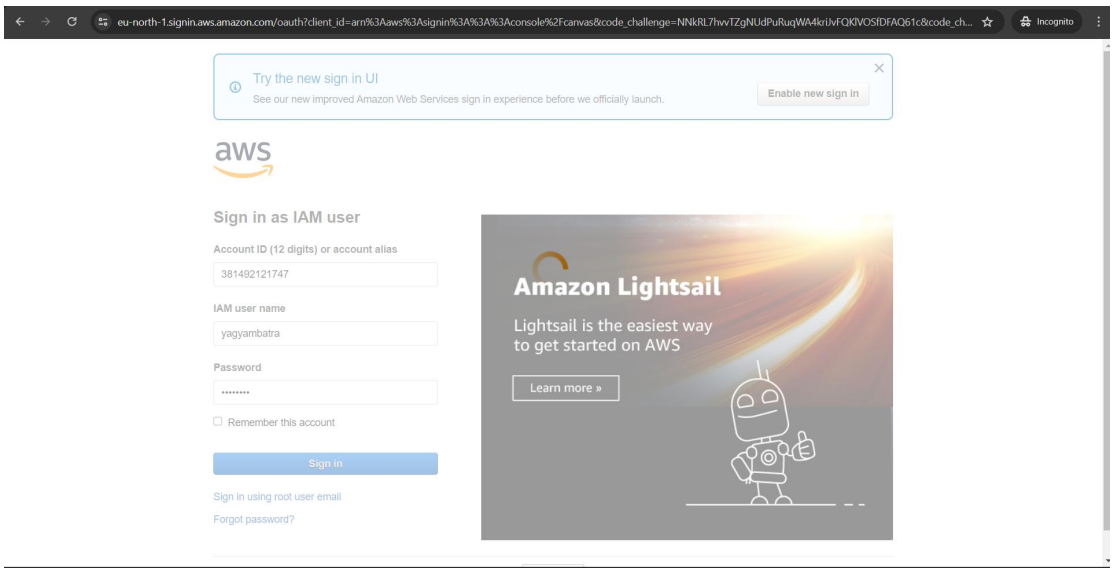

yagyambatra | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra?section=permissions
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Summary
ARN
arn:aws:iam::381492121747:user/yagyambatra
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:27 (UTC+05:30)
Last console sign-in
6 days ago
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Add permissions
Create inline policy
Filter by Type
Search
All types
Policy name
Type
Attached via
yagyambattery
Customer managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Mostly cloudy
Search
ENG
US
12:52 PM
2024-08-10

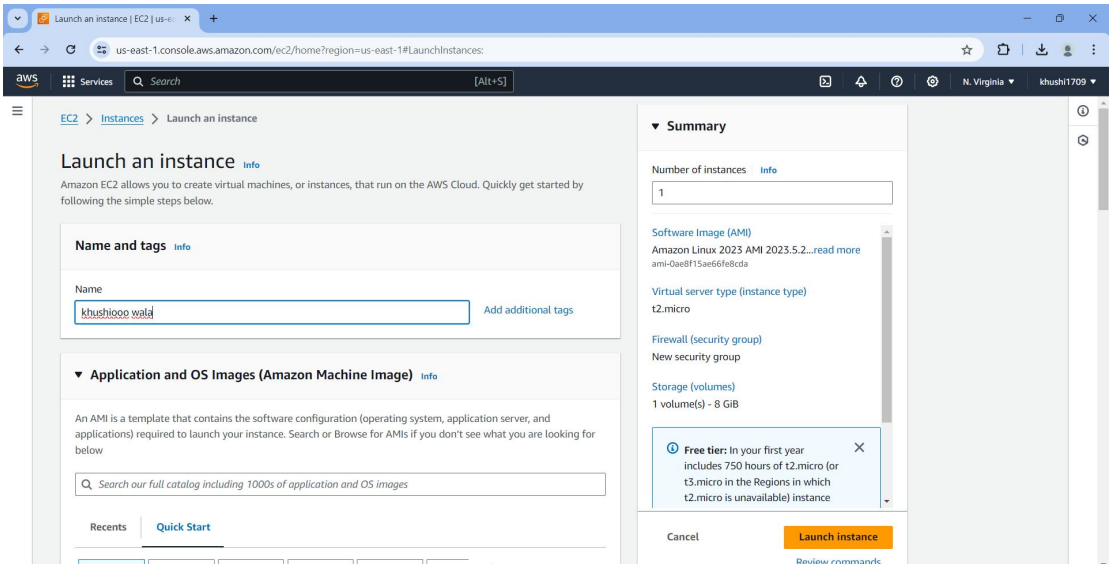

Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra/add-permissions
IAM > Users > yagyambatra > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice 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 (1225)
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 62
Policy name
Type
Attached entities
AccessAnalyzerServiceRolePolicy
AWS managed
0
AdministratorAccess
AWS managed - job function
0
AdministratorAccess-Amplify
AWS managed
0
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Mostly cloudy
Search
ENG
US
12:53 PM
2024-08-10

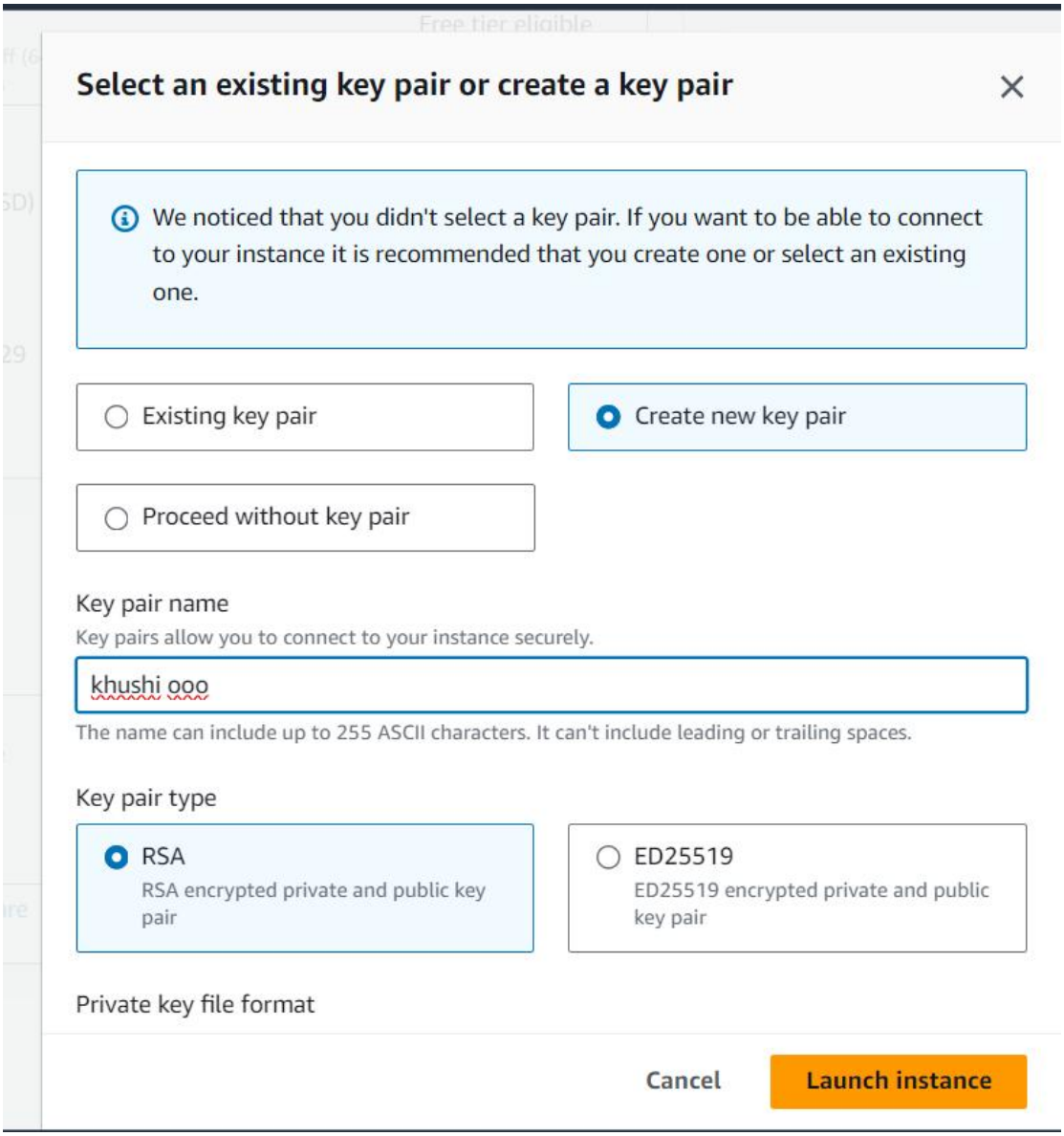

Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra/add-permissions
Services
Search
[Alt+S]
Global
khushi1709
IAM > Users > yagyambatra > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group 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 (1225)
Filter by Type
Search
Customer managed
1 match
Policy name
Type
Attached entities
khushiooooo
Customer managed
0
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Humid
Now
Search
ENG
US
12:53 PM
2024-08-10

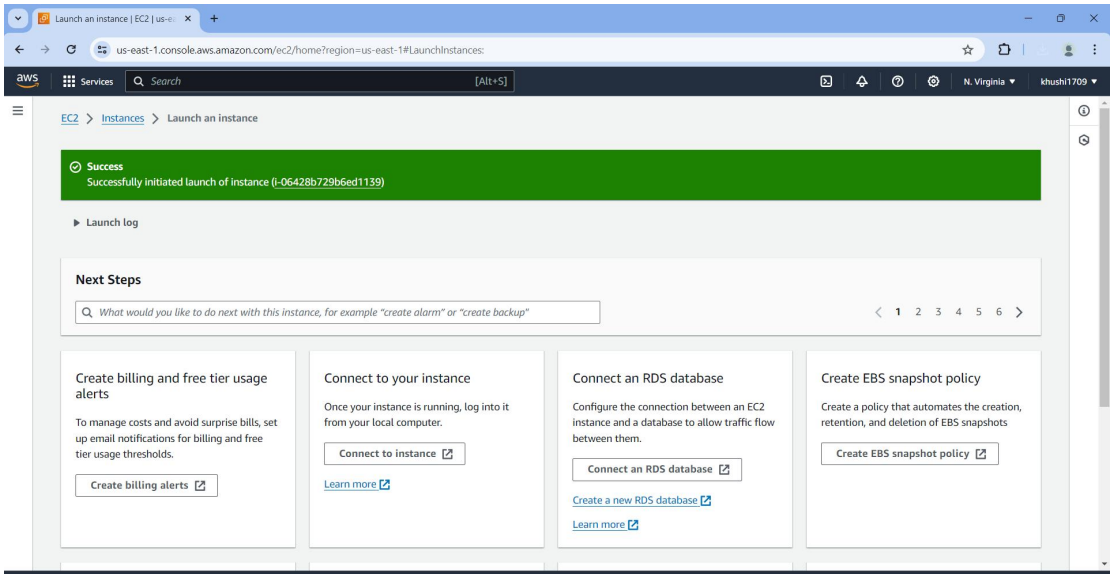

Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra/add-permissions
Services
Search
[Alt+S]
Global
khushi1709
IAM > Users > yagyambatra > Add permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
yagyambatra
Permissions summary (1)
Name
Type
Used as
khushiooooo
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Humid
Now
Search
ENG
US
12:53 PM
2024-08-10

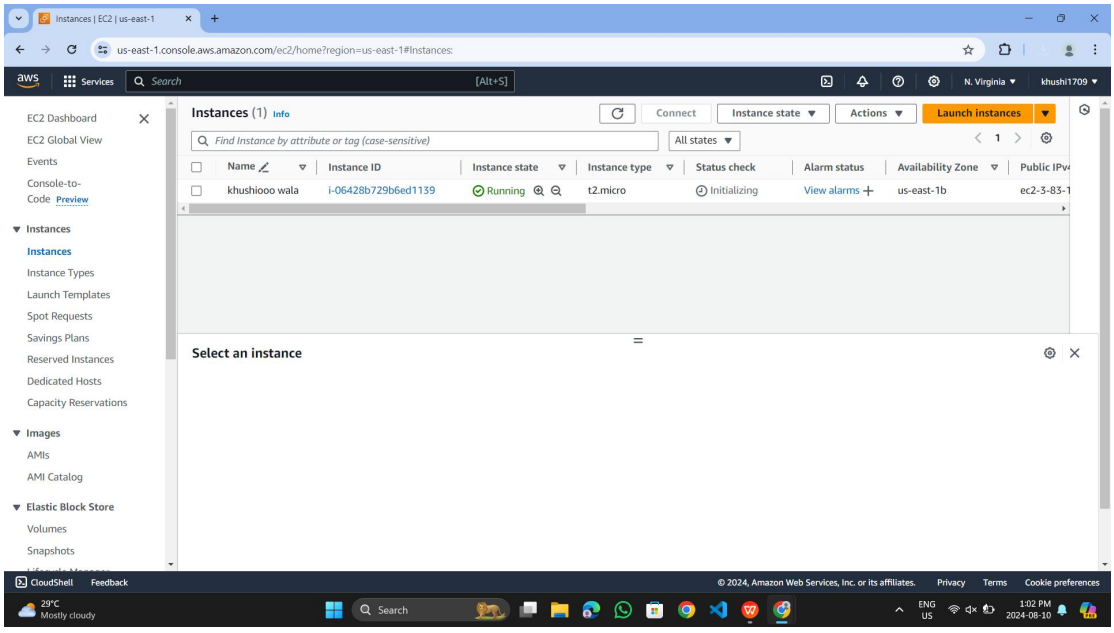

yagyambatra | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/yagyambatra?section=permissions
Identity and Access Management (IAM)
1 policy added
Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
All types
Policy name
Type
Attached via
khushioooooo
Customer managed
Directly
yagyambattery
Customer managed
Directly
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.
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=NNkRL7hvvTZgNUdPuRuqWA4kriJvFQKfVOSfDFAQ61c&code_ch...
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
Sign in as IAM user
Account ID (12 digits) or account alias
381492121747
IAM user name
yagyambatra
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 »


Launch an instance | EC2 | us-e
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Services
Search
[Alt+S]
N. Virginia
khushi1709
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
khushiooo wala
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-0ae8f15ae66fe8cda
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance
Cancel
Launch instance
Review commands


Select an existing key pair or create a key pair
We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one or select an existing one.
Existing key pair
Create new key pair
Proceed without key pair
Key pair name
Key pairs allow you to connect to your instance securely.
khushi ooo
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
Cancel
Launch instance


Launch an instance | EC2 | us-e
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search
[Alt+S]
N. Virginia
khushi1709
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-06428b729b6ed1139)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy


Instances | EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Services
Search
[Alt+S]
N. Virginia
khushi1709
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4
khushiooo wala
i-06428b729b6ed1139
Running
t2.micro
Initializing
View alarms
us-east-1b
ec2-3-83-1
Select an instance
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Mostly cloudy
Search
ENG
US
1:02 PM
2024-08-10