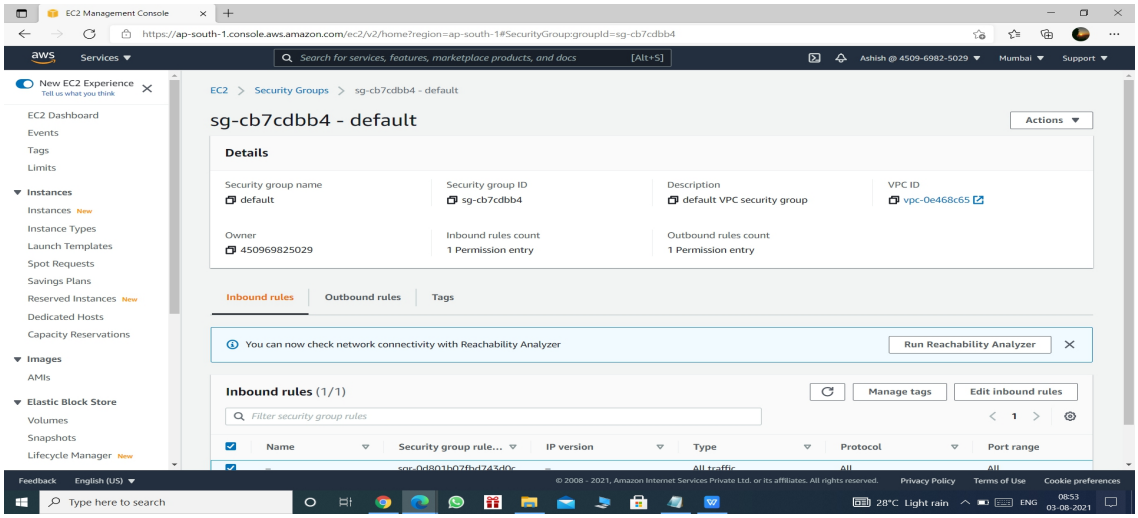
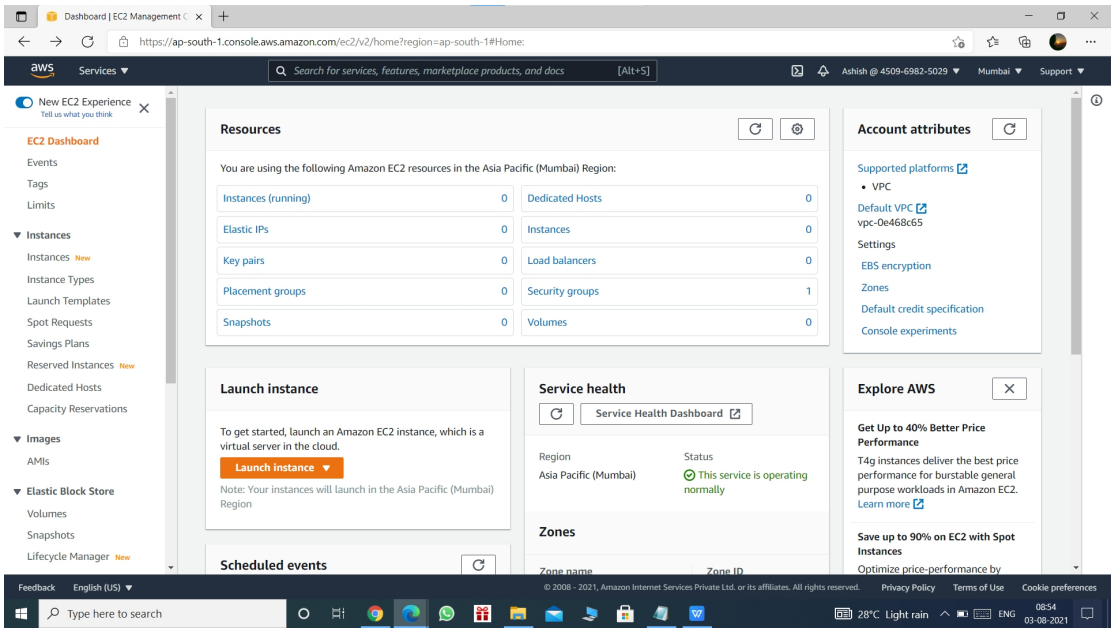
AWS Cloud Computing ZERO TO HERO Ess. JUL

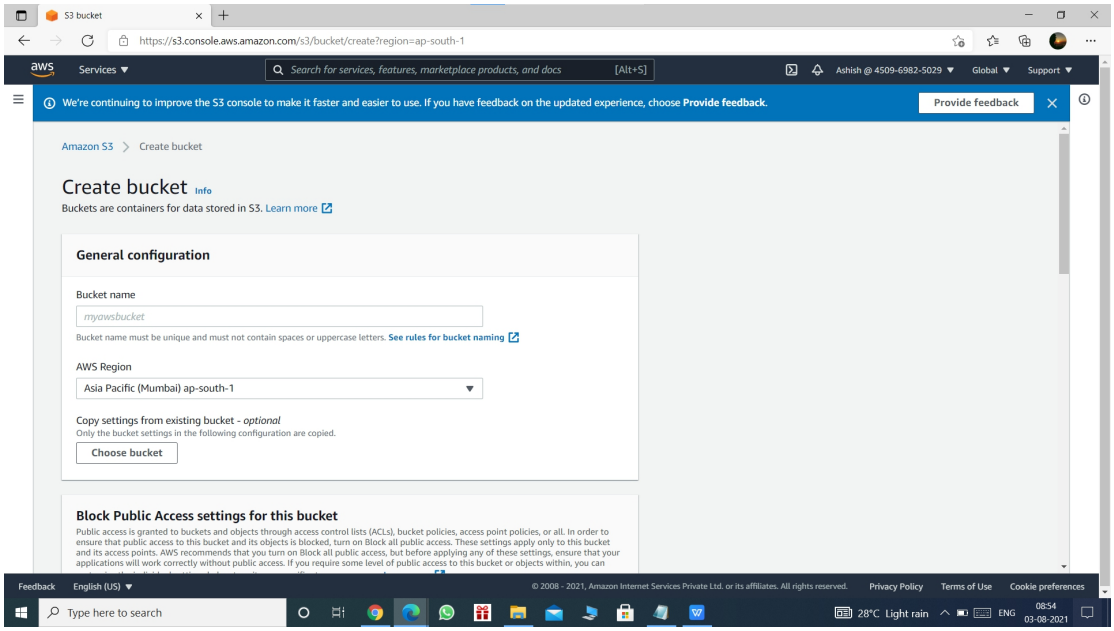
Assignment 1

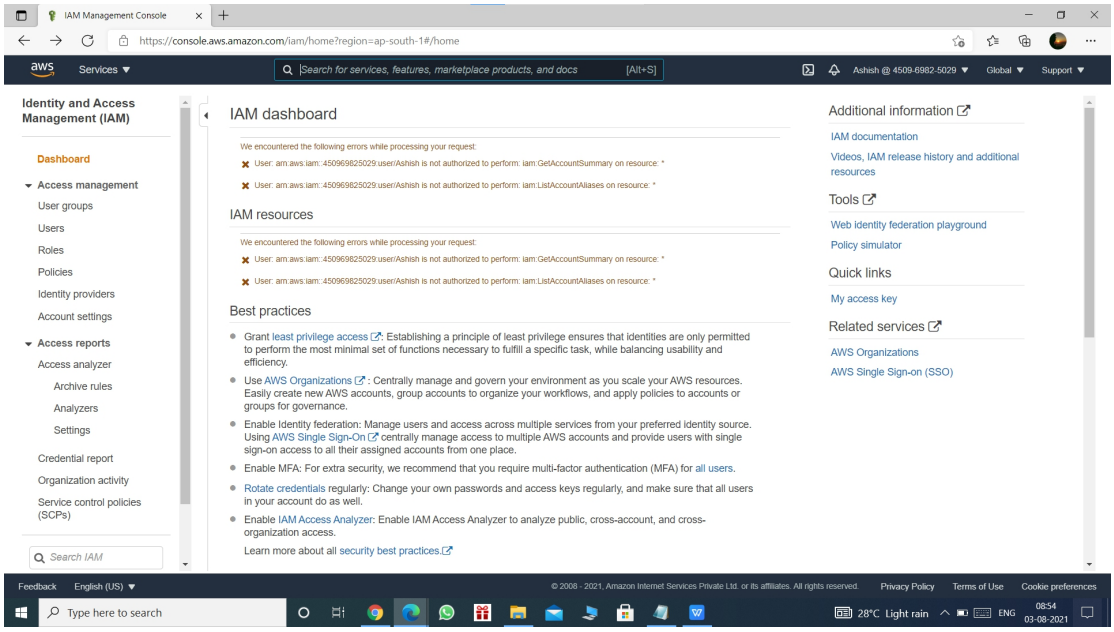
Working with IAM
Create 3 Users
Create one group
Set user permissions
Set a unique group permission
Add users tp group
Login as the IAM user
Show the the user permission and the group permissions are applied
Check which policy gives access to IAM.

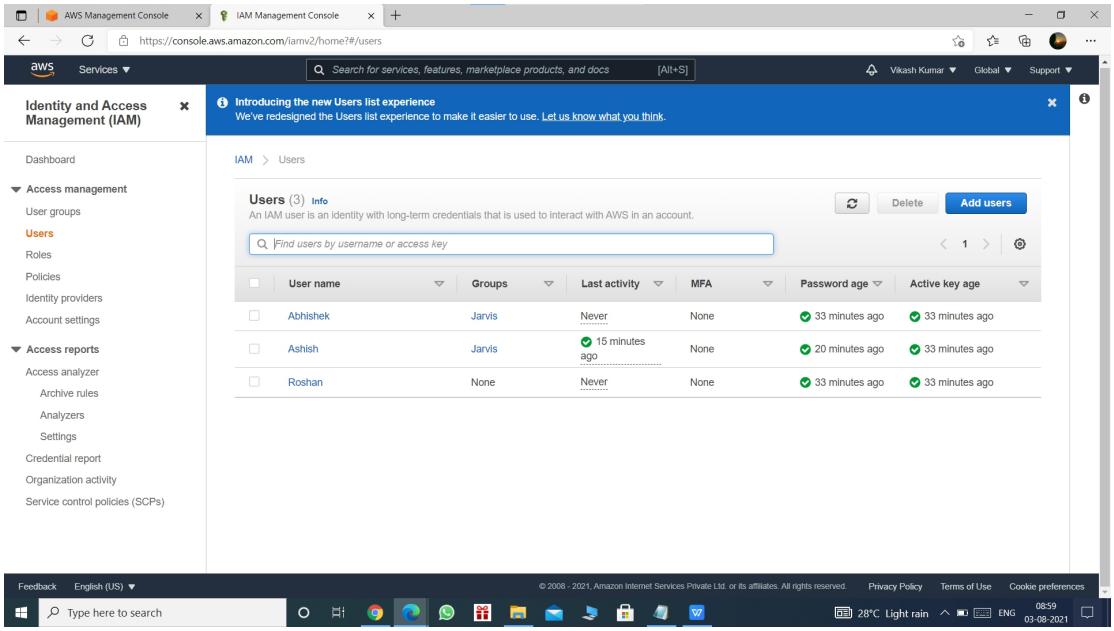
Sol.

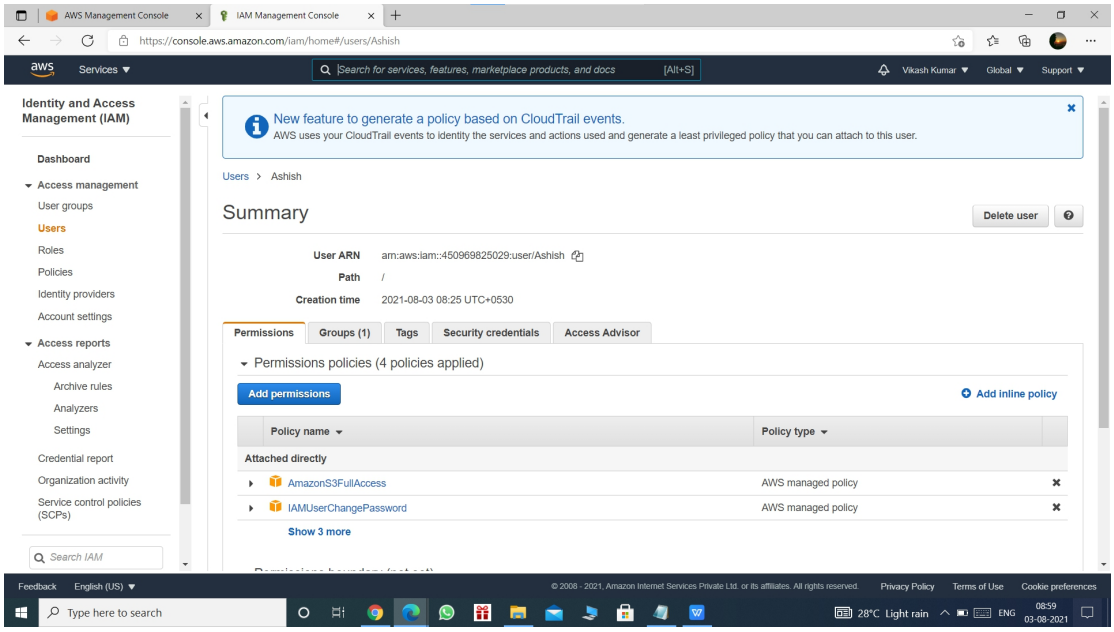


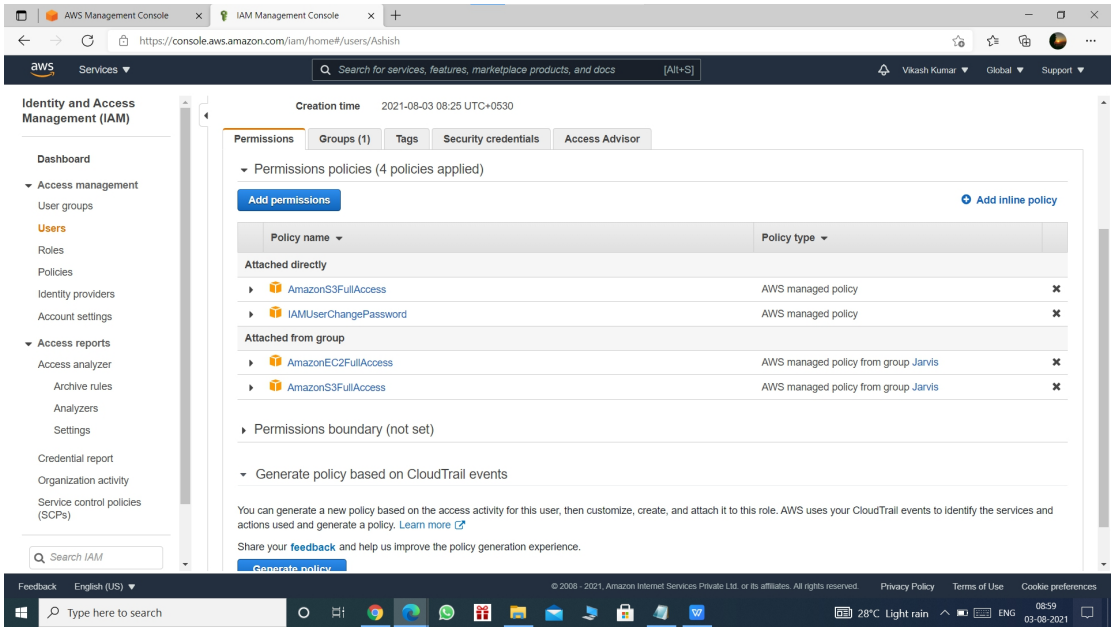


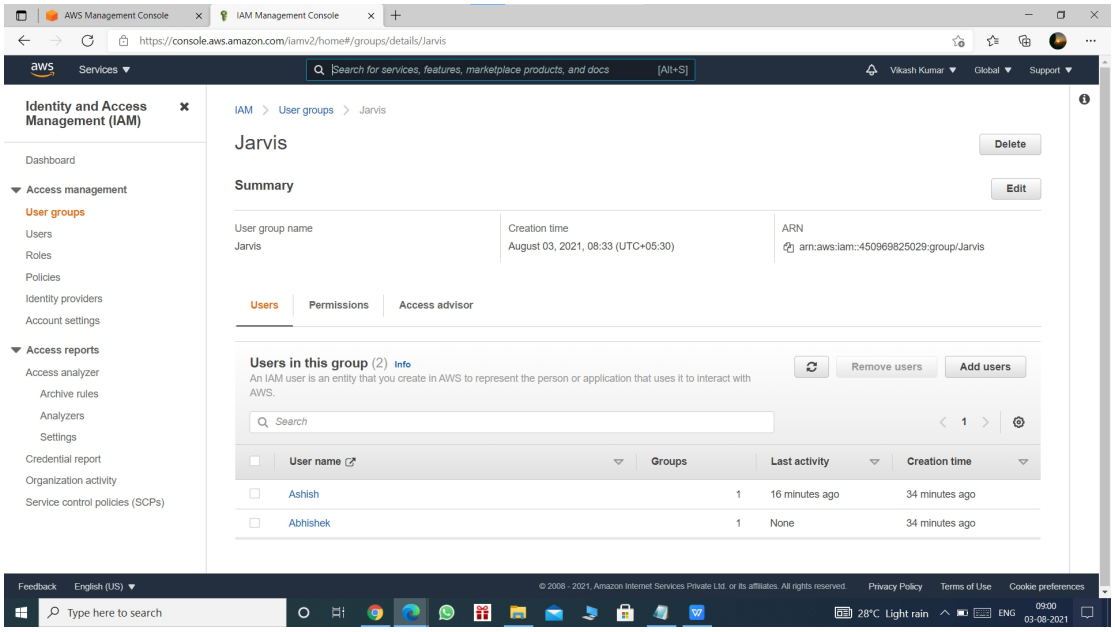

S3 bucket
https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Ashish @ 4509-6982-5029
Global
Support
We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.
Provide feedback
Amazon S3 > Create bucket
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
myawsbucket
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming
AWS Region
Asia Pacific (Mumbai) ap-south-1
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
08:54
03-08-2021

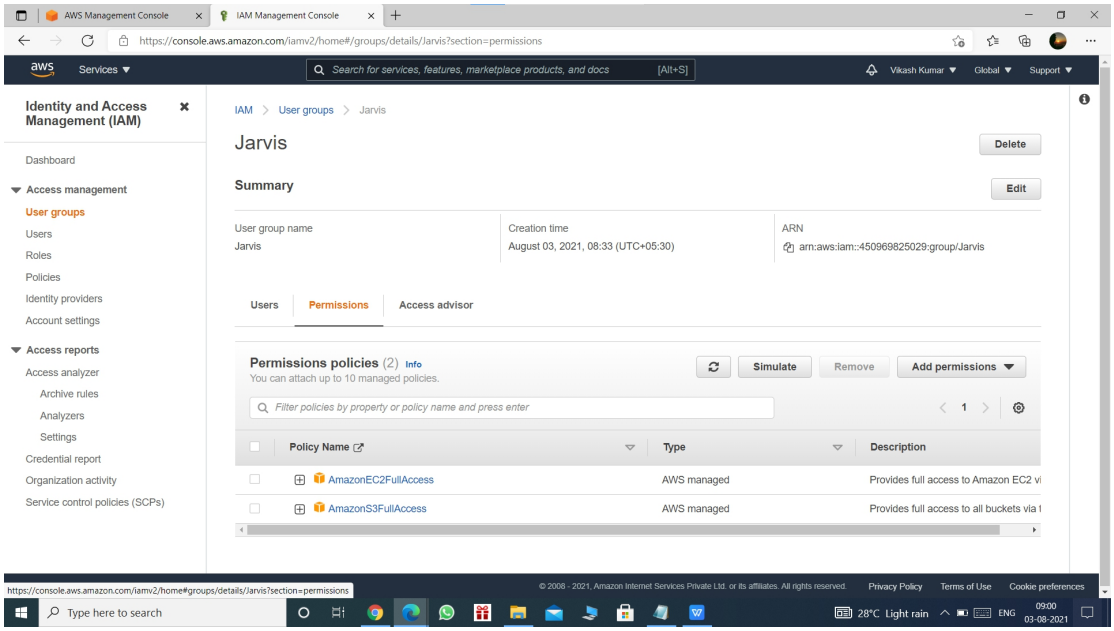

IAM Management Console
https://console.aws.amazon.com/iam/home?region=ap-south-1#/home
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Ashish @ 4509-6982-5029
Global
Support
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Search IAM
IAM dashboard
We encountered the following errors while processing your request:
User: arn:aws:iam::450969825029:user/Ashish is not authorized to perform: iam:GetAccountSummary on resource: *
User: arn:aws:iam::450969825029:user/Ashish is not authorized to perform: iam:ListAccountAliases on resource: *
IAM resources
We encountered the following errors while processing your request:
User: arn:aws:iam::450969825029:user/Ashish is not authorized to perform: iam:GetAccountSummary on resource: *
User: arn:aws:iam::450969825029:user/Ashish is not authorized to perform: iam:ListAccountAliases on resource: *
Best practices
Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
Use AWS Organizations: Centrally manage and govern your environment as you scale your AWS resources. Easily create new AWS accounts, group accounts to organize your workflows, and apply policies to accounts or groups for governance.
Enable Identity federation: Manage users and access across multiple services from your preferred identity source. Using AWS Single Sign-On centrally manage access to multiple AWS accounts and provide users with single sign-on access to all their assigned accounts from one place.
Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
Rotate credentials regularly: Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
Enable IAM Access Analyzer: Enable IAM Access Analyzer to analyze public, cross-account, and cross-organization access.
Learn more about all security best practices.
Additional information
IAM documentation
Videos, IAM release history and additional resources
Tools
Web identity federation playground
Policy simulator
Quick links
My access key
Related services
AWS Organizations
AWS Single Sign-on (SSO)
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
08:54
03-08-2021

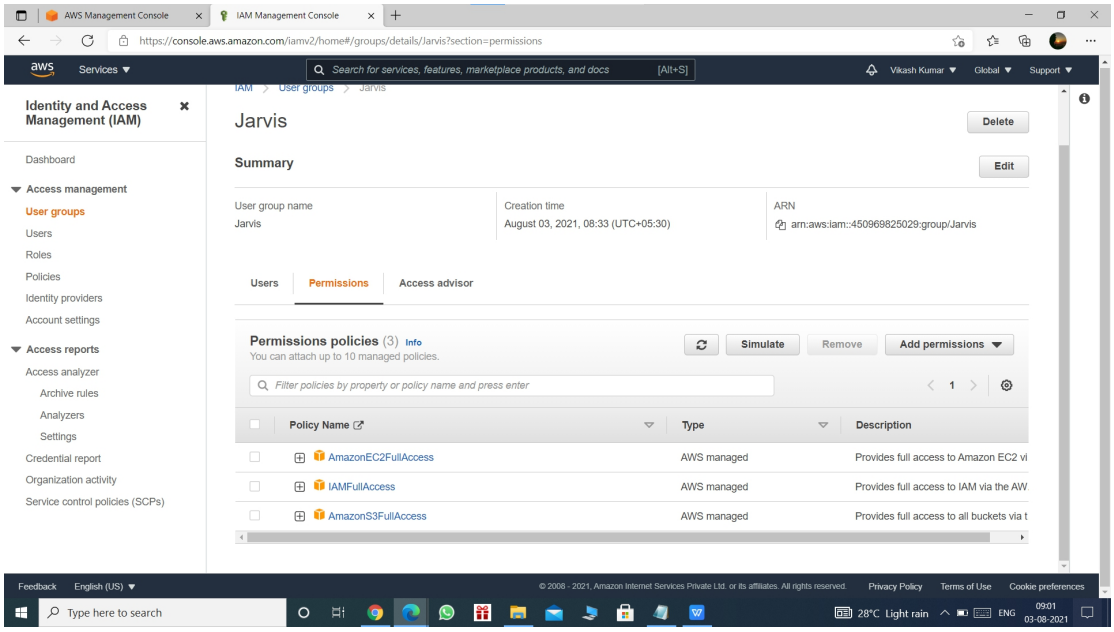

AWS Management Console
IAM Management Console
https://console.aws.amazon.com/iamv2/home?#/users
Services
Search for services, features, marketplace products, and docs [Alt+S]
Vikash Kumar
Global
Support
Identity and Access Management (IAM)
Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > Users
Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Add users
Find users by username or access key
User name
Groups
Last activity
MFA
Password age
Active key age
Abhishek
Jarvis
Never
None
33 minutes ago
33 minutes ago
Ashish
Jarvis
15 minutes ago
None
20 minutes ago
33 minutes ago
Roshan
None
Never
None
33 minutes ago
33 minutes ago
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
08:59
03-08-2021

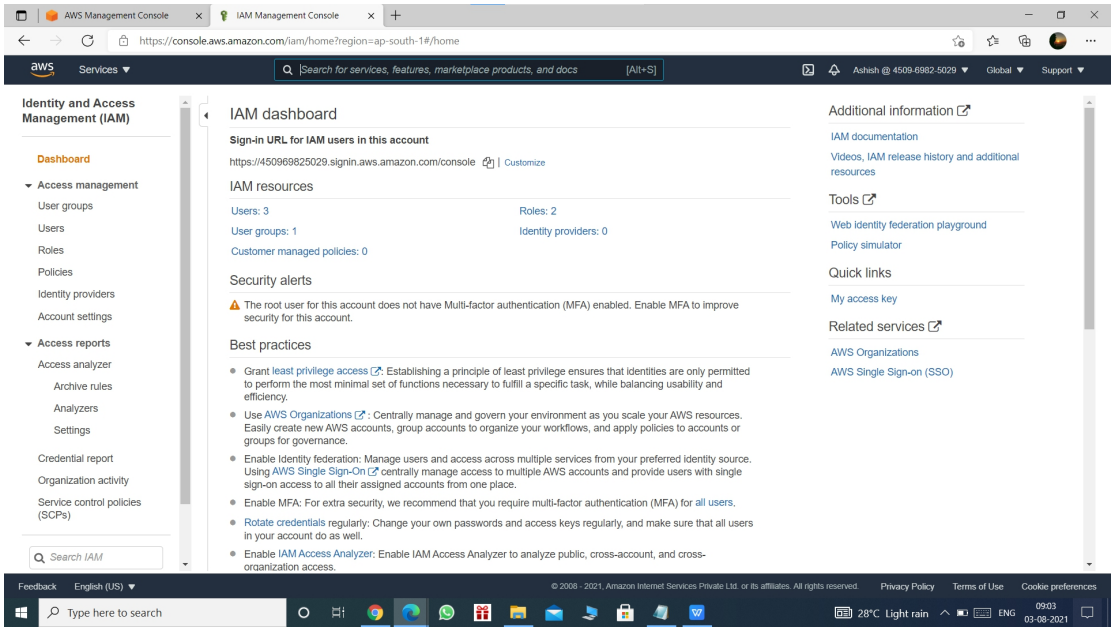

AWS Management Console
IAM Management Console
https://console.aws.amazon.com/iam/home#/users/Ashish
Services
Search for services, features, marketplace products, and docs [Alt+S]
Vikash Kumar
Global
Support
Identity and Access Management (IAM)
New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identity the services and actions used and generate a least privileged policy that you can attach to this user.
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Search IAM
Users > Ashish
Summary
Delete user
User ARN arn:aws:iam::450969825029:user/Ashish
Path /
Creation time 2021-08-03 08:25 UTC+0530
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (4 policies applied)
Add permissions
Add inline policy
Policy name
Policy type
Attached directly
AmazonS3FullAccess
AWS managed policy
IAMUserChangePassword
AWS managed policy
Show 3 more
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
08:59
03-08-2021


AWS Management Console
IAM Management Console
https://console.aws.amazon.com/iam/home#/users/Ashish
Services
Search for services, features, marketplace products, and docs [Alt+S]
Vikash Kumar
Global
Support
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Search IAM
Creation time 2021-08-03 08:25 UTC+0530
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (4 policies applied)
Add permissions
Add inline policy
Policy name
Policy type
Attached directly
AmazonS3FullAccess
AWS managed policy
IAMUserChangePassword
AWS managed policy
Attached from group
AmazonEC2FullAccess
AWS managed policy from group Jarvis
AmazonS3FullAccess
AWS managed policy from group Jarvis
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
Share your feedback and help us improve the policy generation experience.
Generate policy
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
08:59
03-08-2021


AWS Management Console
IAM Management Console
https://console.aws.amazon.com/iamv2/home#/groups/details/Jarvis
Services
Search for services, features, marketplace products, and docs [Alt+S]
Vikash Kumar
Global
Support
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > Jarvis
Jarvis
Delete
Summary
Edit
User group name
Jarvis
Creation time
August 03, 2021, 08:33 (UTC+05:30)
ARN
arn:aws:iam::450969825029:group/Jarvis
Users
Permissions
Access advisor
Users in this group (2) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Remove users
Add users
Search
User name
Groups
Last activity
Creation time
Ashish
1
16 minutes ago
34 minutes ago
Abhishek
1
None
34 minutes ago
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
09:00
03-08-2021


AWS Management Console
IAM Management Console
https://console.aws.amazon.com/iamv2/home#/groups/details/Jarvis?section=permissions
Services
Search for services, features, marketplace products, and docs [Alt+S]
Vikash Kumar
Global
Support
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > Jarvis
Jarvis
Delete
Summary
Edit
User group name
Jarvis
Creation time
August 03, 2021, 08:33 (UTC+05:30)
ARN
arn:aws:iam::450969825029:group/Jarvis
Users
Permissions
Access advisor
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter policies by property or policy name and press enter
Policy Name
Type
Description
AmazonEC2FullAccess
AWS managed
Provides full access to Amazon EC2 vi
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via t
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
https://console.aws.amazon.com/iamv2/home#groups/details/Jarvis?section=permissions
Type here to search
28°C Light rain
ENG
09:00
03-08-2021


AWS Management Console
IAM Management Console
https://console.aws.amazon.com/iamv2/home#/groups/details/Jarvis?section=permissions
Services
Search for services, features, marketplace products, and docs [Alt+S]
Vikash Kumar
Global
Support
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > Jarvis
Jarvis
Delete
Summary
Edit
User group name
Jarvis
Creation time
August 03, 2021, 08:33 (UTC+05:30)
ARN
arn:aws:iam::450969825029:group/Jarvis
Users
Permissions
Access advisor
Permissions policies (3) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter policies by property or policy name and press enter
Policy Name
Type
Description
AmazonEC2FullAccess
AWS managed
Provides full access to Amazon EC2 vi
IAMFullAccess
AWS managed
Provides full access to IAM via the AW
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via t
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
09:01
03-08-2021


AWS Management Console
IAM Management Console
https://console.aws.amazon.com/iam/home?region=ap-south-1#/home
aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
Ashish @ 4509-6982-5029
Global
Support
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Search IAM
IAM dashboard
Sign-in URL for IAM users in this account
https://450969825029.signin.aws.amazon.com/console | Customize
IAM resources
Users: 3
Roles: 2
User groups: 1
Identity providers: 0
Customer managed policies: 0
Security alerts
The root user for this account does not have Multi-factor authentication (MFA) enabled. Enable MFA to improve security for this account.
Best practices
Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
Use AWS Organizations: Centrally manage and govern your environment as you scale your AWS resources. Easily create new AWS accounts, group accounts to organize your workflows, and apply policies to accounts or groups for governance.
Enable Identity federation: Manage users and access across multiple services from your preferred identity source. Using AWS Single Sign-On centrally manage access to multiple AWS accounts and provide users with single sign-on access to all their assigned accounts from one place.
Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
Rotate credentials regularly: Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
Enable IAM Access Analyzer: Enable IAM Access Analyzer to analyze public, cross-account, and cross-organization access.
Additional information
IAM documentation
Videos, IAM release history and additional resources
Tools
Web identity federation playground
Policy simulator
Quick links
My access key
Related services
AWS Organizations
AWS Single Sign-on (SSO)
Feedback
English (US)
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Cookie preferences
Type here to search
28°C Light rain
ENG
09:03
03-08-2021