Ishita Hardasmalani

C14-2103058

EXPERIMENT NO . 7

Aim: To study and implement Storage as a Service using Own Cloud

Theory:

Access management refers to the processes and practices used to control and monitor who has access to resources, systems, and data within an organization. It involves defining, enforcing, and managing access policies and permissions to ensure that users have the appropriate level of access to perform their roles and responsibilities while minimizing security risks.

The concept of access management is essential for several reasons:

1. **Data Security**: Access management helps prevent unauthorized access to sensitive data and resources, reducing the risk of data breaches, data loss, and other security incidents. By enforcing least privilege principles, organizations can ensure that users only have access to the information and resources necessary to perform their job functions.

2. **Compliance Requirements**: Many industries and organizations are subject to regulatory compliance requirements that mandate strict access controls and data protection measures. Access management helps organizations comply with regulations such as GDPR, HIPAA, PCI DSS, and others by ensuring that access to sensitive data is restricted to authorized individuals and that access activities are logged and monitored.

3. **Risk Mitigation**: Effective access management helps mitigate security risks associated with insider threats, external attacks, and human error. By implementing robust authentication mechanisms, access controls, and monitoring systems, organizations can detect and respond to suspicious or unauthorized access attempts promptly, minimizing the impact of security incidents.

4. **Resource Optimization**: Access management enables organizations to optimize resource utilization by ensuring that users have access to the resources they need, when they need them. By granting appropriate permissions based on roles, responsibilities, and business requirements, organizations can prevent unnecessary access requests and streamline access provisioning processes.

5. **Business Continuity**: Access management plays a crucial role in ensuring business continuity by preventing unauthorized access to critical systems and data. By implementing robust authentication, authorization, and identity management controls, organizations can protect their infrastructure and data assets from unauthorized access attempts, ensuring uninterrupted operations and service availability.

Overall, access management is essential for protecting sensitive data, complying with regulatory requirements, mitigating security risks, optimizing resource utilization, and ensuring business continuity. By implementing effective access controls, organizations can protect their assets, maintain trust with stakeholders, and achieve their business objectives securely and efficiently.

IAM stands for Identity and Access Management, which is a service provided by cloud computing platforms like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and others. IAM enables organizations to manage user identities, access permissions, and security policies centrally across their cloud environments. It helps ensure that only authorized individuals and systems have access to resources and data while maintaining security, compliance, and operational efficiency. Below are the components of IAM:

1. **Users**:

- Users represent individuals or entities that interact with the cloud environment. Each user is assigned a unique identity (username) and associated credentials (password, access keys, or multi-factor authentication tokens) for authentication and access management.

2. **Groups**:

- Groups are collections of users with similar roles, responsibilities, or access requirements. Instead of assigning permissions to individual users, organizations can assign permissions to groups, making it easier to manage access at scale. Users can be added to or removed from groups dynamically, simplifying access management.

3. **Roles**:

- Roles define a set of permissions that govern what actions users or services can perform within the cloud environment. Roles are typically assigned to users, groups, or services (such as EC2 instances or Lambda functions) and are used to grant temporary permissions for specific tasks or operations. Roles can be assigned to users or services within the same AWS account or across different AWS accounts using cross-account access.

4. **Policies**:

- Policies are JSON documents that define the permissions and access controls for IAM entities (users, groups, and roles). Policies specify what actions are allowed or denied on which resources. IAM policies can be attached to users, groups, roles, or resources, allowing organizations to enforce fine-grained access controls based on their security requirements.

5. **Access Keys**:

- Access keys consist of an access key ID and a secret access key and are used to authenticate programmatic access to AWS resources via APIs, SDKs, or CLI commands. Access keys are associated with IAM users and provide secure access to AWS services without the need for interactive authentication. Access keys should be securely managed and rotated regularly to minimize the risk of unauthorized access.

6. **Multi-factor Authentication (MFA)**:

- Multi-factor authentication adds an extra layer of security to IAM users' authentication process by requiring them to provide an additional authentication factor (such as a one-time password generated by a

hardware token, software token, or SMS message) along with their username and password. MFA helps prevent unauthorized access, even if a user's credentials are compromised.

7. **Identity Providers (IdPs)**:

- Identity providers are external systems or services that authenticate and authorize users before granting access to cloud resources. IAM supports integration with external identity providers such as Active Directory, LDAP, SAML, or OpenID Connect, enabling organizations to centralize user authentication and access control policies across their cloud and on-premises environments.

By leveraging these components, organizations can effectively manage user identities, enforce access controls, and maintain security and compliance posture within their cloud environments. IAM provides granular control over who can access what resources and actions, enabling organizations to protect their data, applications, and infrastructure from unauthorized access and security threats.

Root Users vs. Other IAM Users:

Aspect	Root Users	IAM Users
Default Access	Has unrestricted access to all AWS services and resources in the account.	Has no default access and must be explicitly granted permissions to access AWS services and resources.
Management	Root users have full control over the AWS account and its resources.	IAM users are managed entities within the AWS account and can be created, modified, and deleted by the root user or other IAM users with appropriate permissions.
Security	Root user credentials should be securely stored and protected to prevent unauthorized access.	IAM users have separate credentials (username and password) or access keys and can be assigned multi-factor authentication (MFA) for additional security.
Best Practices	Best practice is to create IAM users for day-to-day tasks and avoid using root user credentials except for initial account setup and critical administrative tasks.	Best practice is to follow the principle of least privilege and grant IAM users only the permissions necessary to perform their specific roles and responsibilities.

Aspect	Root Users	IAM Users
Audit Trail	Actions performed by root users are logged in AWS CloudTrail for auditing and monitoring purposes.	Actions performed by IAM users are also logged in CloudTrail, providing a comprehensive audit trail of user activity within the account.

Roles vs. Policies:

Aspect	Roles	Policies
Purpose	Used to delegate temporary permissions to entities (users, services, or resources) for specific tasks or operations.	Define permissions and access controls that govern what actions are allowed or denied on AWS resources.
Assignment	Roles are assigned to entities (users, groups, or services) and can be assumed dynamically as needed.	Policies are attached to IAM identities (users, groups, or roles) or resources and apply to all entities associated with them.
Granularity	Roles define a set of permissions that can be assumed by entities, and the permissions are activated when the entity assumes the role.	Policies specify permissions and access controls at a granular level, defining what actions are allowed or denied for specific resources.
Temporary Access	Roles can provide temporary access to resources by defining session duration and allowing entities to assume the role for a limited time period.	Policies are static and provide persistent permissions that are enforced whenever the associated IAM identity or resource is accessed.
Trust Relationships	Roles establish trust relationships with trusted entities (such as AWS accounts or services) and define who can assume the role and under what conditions.	Policies are standalone documents that define permissions and access controls independently of trust relationships.

In AWS IAM (Identity and Access Management), policies are JSON documents that define permissions and access controls for IAM users, groups, roles, or resources. AWS provides two main types of policies: inline policies and managed policies (often referred to as custom policies). Here's an explanation of each:

1. **Inline Policies**:

- Inline policies are policies that are directly attached to an IAM user, group, or role.

- These policies are embedded within the IAM entity's configuration and are part of the entity's definition.

- Inline policies are created and managed directly within the context of the IAM entity to which they are attached.

- Inline policies are convenient for defining permissions that are specific to a particular IAM entity and are not reused elsewhere.

- They are suitable for scenarios where you need fine-grained control over the permissions of individual IAM entities without creating separate policies.

2. **Managed Policies (Custom Policies)**:

- Managed policies are standalone policies that can be created and managed independently of IAM entities.

- These policies are created separately from IAM entities and can be attached to multiple users, groups, or roles across the AWS account.

- Managed policies can be reused across multiple IAM entities, allowing for centralized management and easier policy updates.

- AWS provides a set of managed policies that cover common use cases, such as granting access to specific AWS services or enforcing security best practices.

- Custom managed policies can also be created to define custom permissions tailored to the organization's specific requirements.

- Managed policies can be versioned, allowing for the management of policy changes over time and rollback to previous versions if needed.

- Changes to managed policies take effect immediately for all IAM entities to which the policy is attached.

In summary, inline policies are directly embedded within IAM entities and are managed within the context of those entities, while managed policies are standalone documents that can be attached to multiple IAM entities and managed independently. Both types of policies provide flexible mechanisms for defining permissions and access controls in AWS IAM, allowing organizations to enforce security policies and manage access to AWS resources effectively.

Multi-Factor Authentication (MFA) is an additional layer of security for user authentication that requires users to provide two or more forms of authentication factors to verify their identity. In the context of AWS (Amazon Web Services), MFA adds an extra layer of protection to AWS accounts, making it more difficult for unauthorized users to gain access to sensitive resources and data. Here's how MFA works in AWS:

1. **Authentication Factors**:

   - MFA requires users to provide two or more authentication factors from different categories:

     - **Something you know**: Typically, a password or PIN.

     - **Something you have**: A physical device or token, such as a hardware MFA device or a virtual MFA device (e.g., a smartphone app).

     - **Something you are**: Biometric characteristics, such as fingerprint or retina scans (although AWS primarily uses the first two factors).

2. **Enabling MFA**:

   - In AWS, MFA can be enabled for individual IAM users or the AWS root account.

   - Users must first associate an MFA device with their IAM user account. This involves setting up the MFA device using the AWS Management Console or CLI and scanning a QR code or manually entering a secret key provided by AWS.

   - Once the MFA device is configured, users must authenticate with both their password and a one-time code generated by the MFA device during the login process.

3. **MFA Devices**:

   - AWS supports various types of MFA devices, including hardware tokens (such as YubiKey or Gemalto devices) and virtual MFA devices (such as Google Authenticator, Authy, or AWS Virtual MFA app).

- Hardware MFA devices are physical tokens that users carry with them, while virtual MFA devices are smartphone apps that generate one-time codes.

4. **Authentication Process**:

- When MFA is enabled for an IAM user, the user is required to provide their username, password, and a one-time code generated by their MFA device during the login process.

- After entering the correct credentials, the user is prompted to enter the one-time code from their MFA device.

- If the correct MFA code is provided, the user is granted access to the AWS Management Console, CLI, or API, depending on their permissions.

5. **Benefits of MFA**:

- MFA significantly enhances the security of AWS accounts by adding an extra layer of protection beyond passwords.

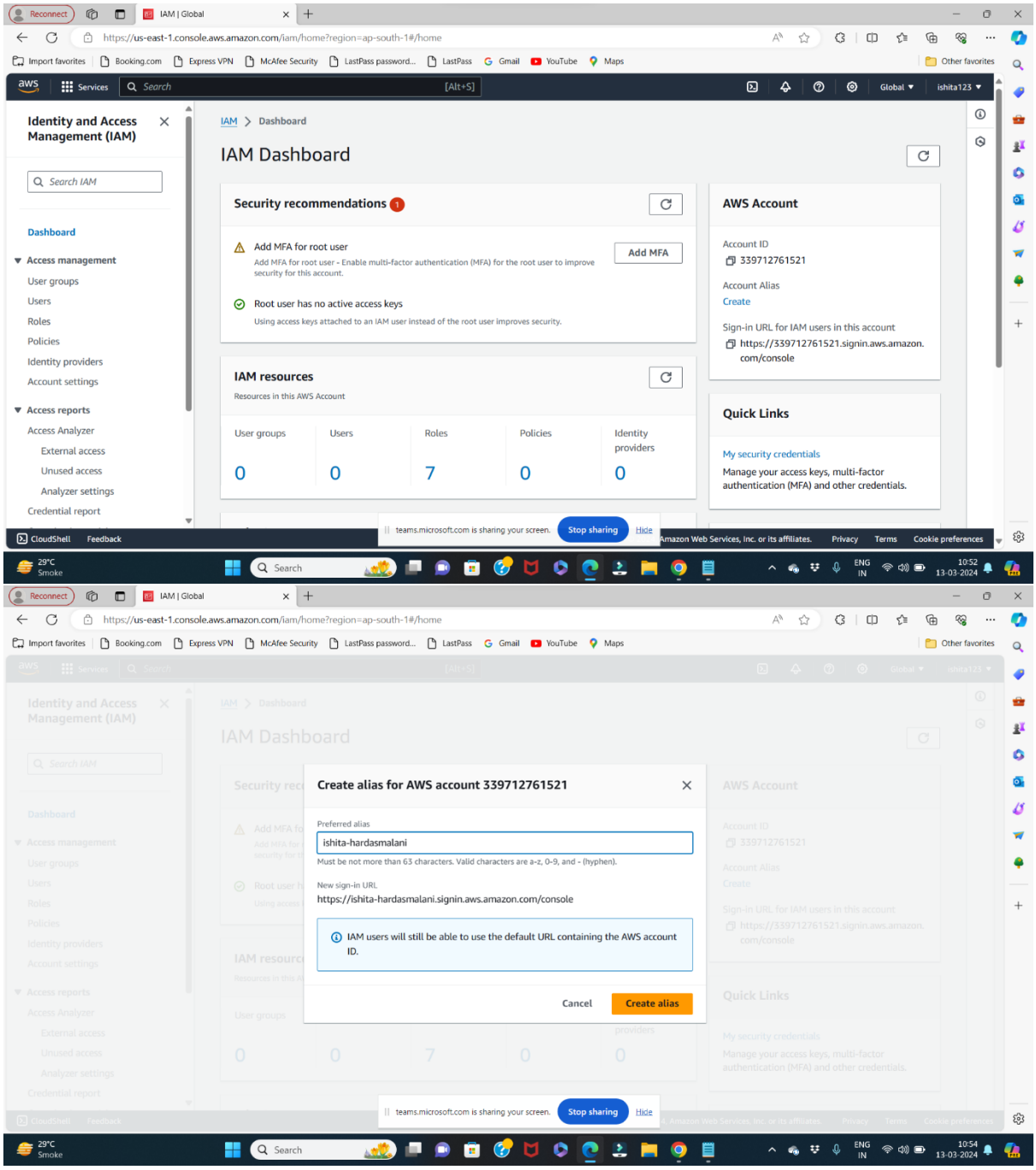
- It helps mitigate the risk of unauthorized access due to compromised passwords or credentials.

- MFA is particularly important for accessing sensitive AWS resources, managing critical infrastructure, or performing administrative tasks within AWS accounts.

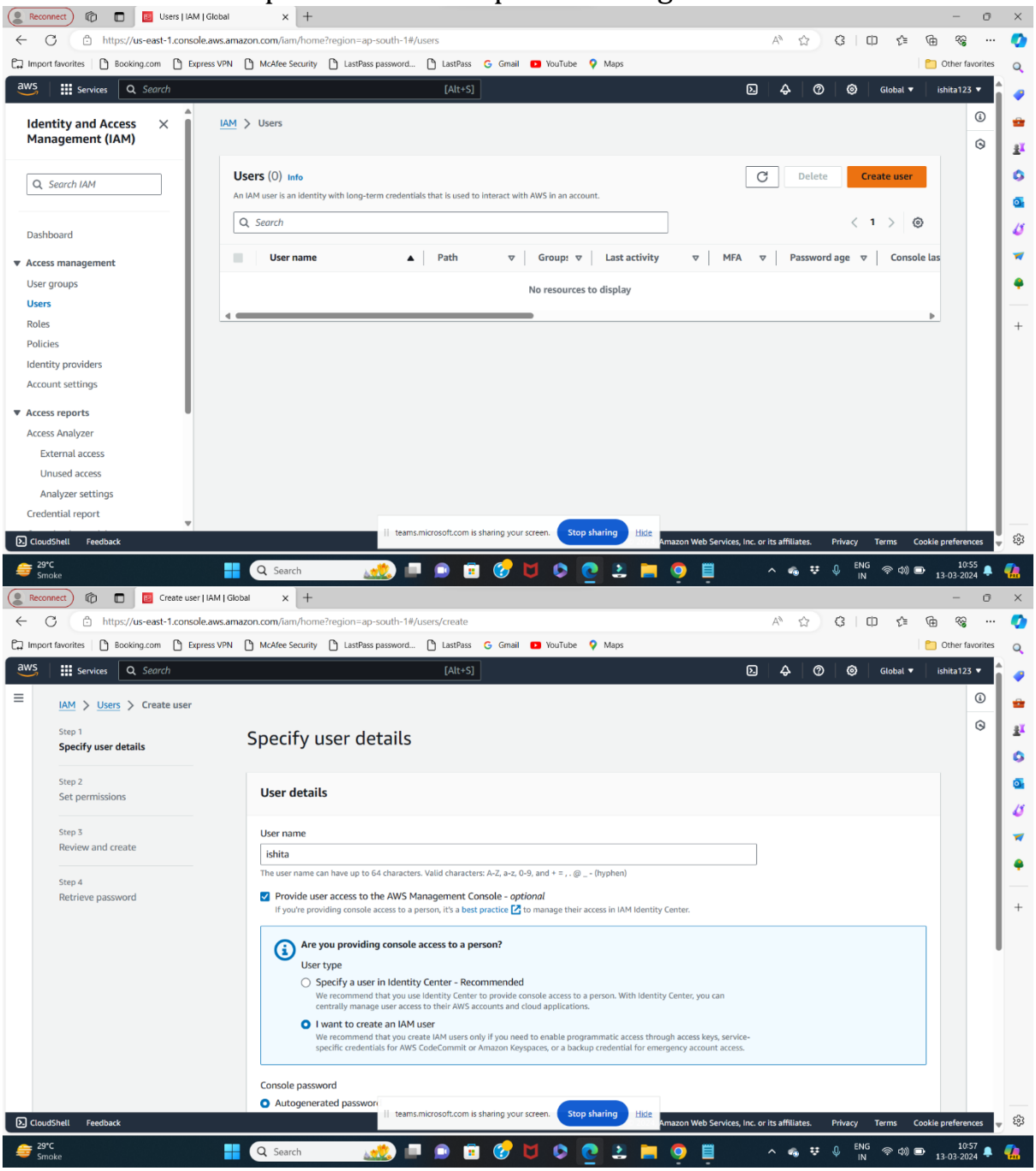
Overall, MFA is a critical security feature in AWS that helps protect against unauthorized access and strengthens the overall security posture of AWS accounts and resources. It is recommended that organizations enable MFA for all IAM users and the root account to enhance security and mitigate the risk of security breaches.

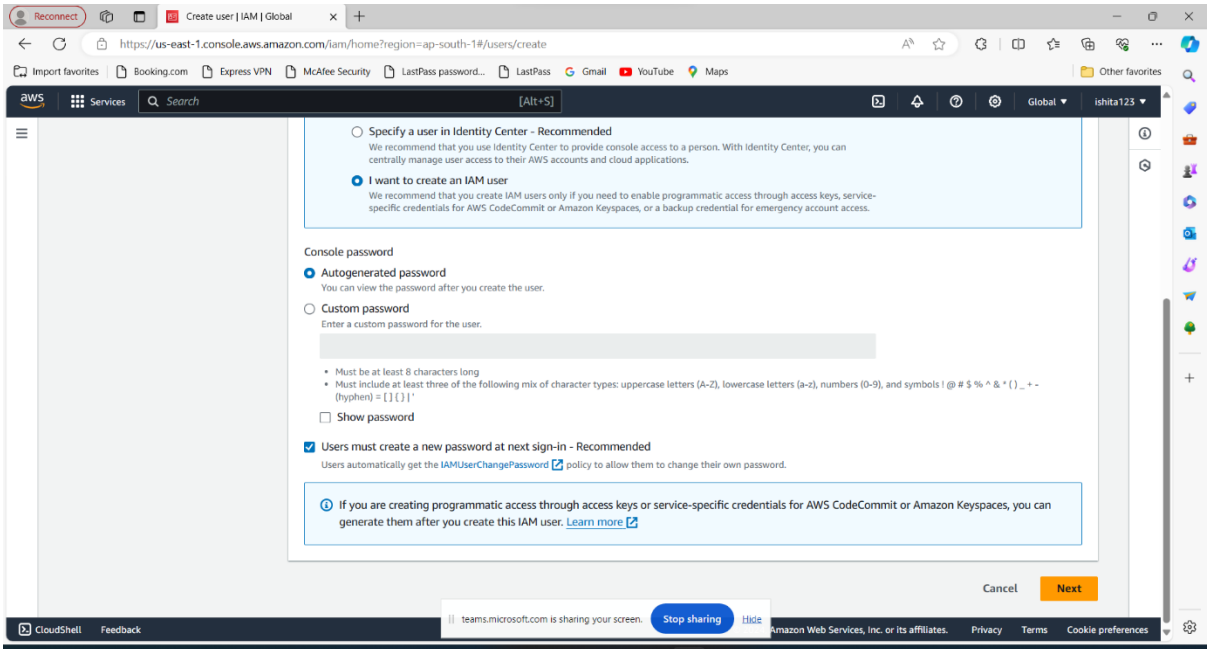
Implementation:

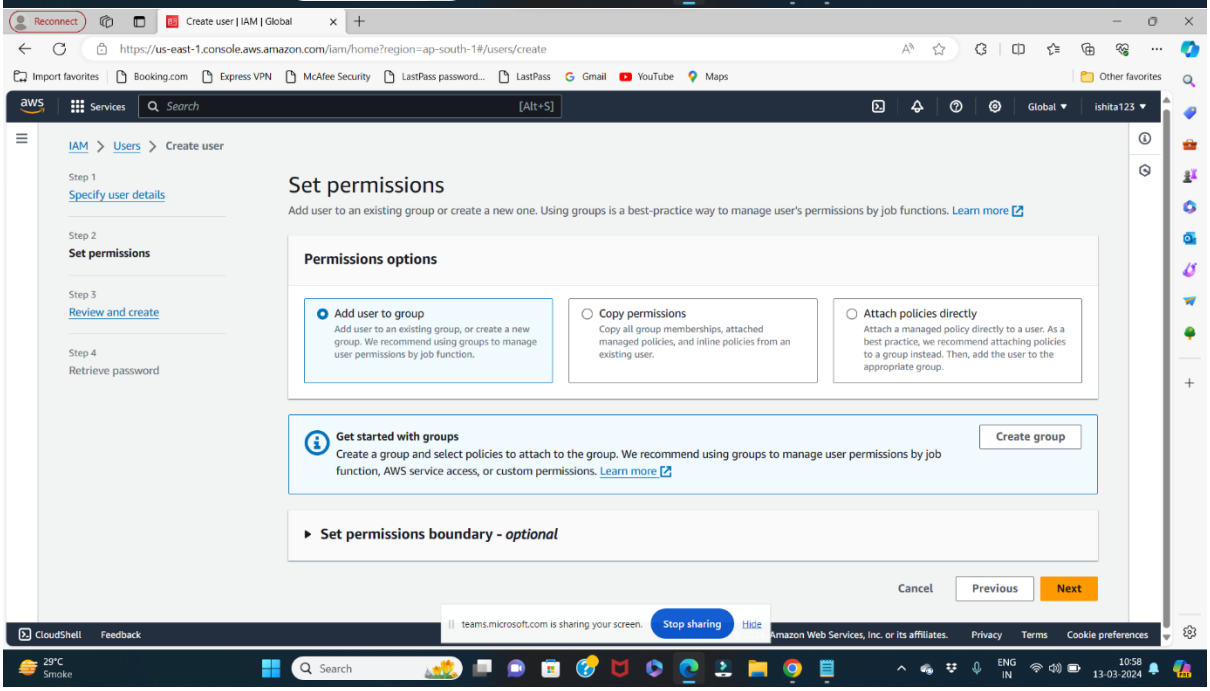
1. IAM dashboard , create alias for root user

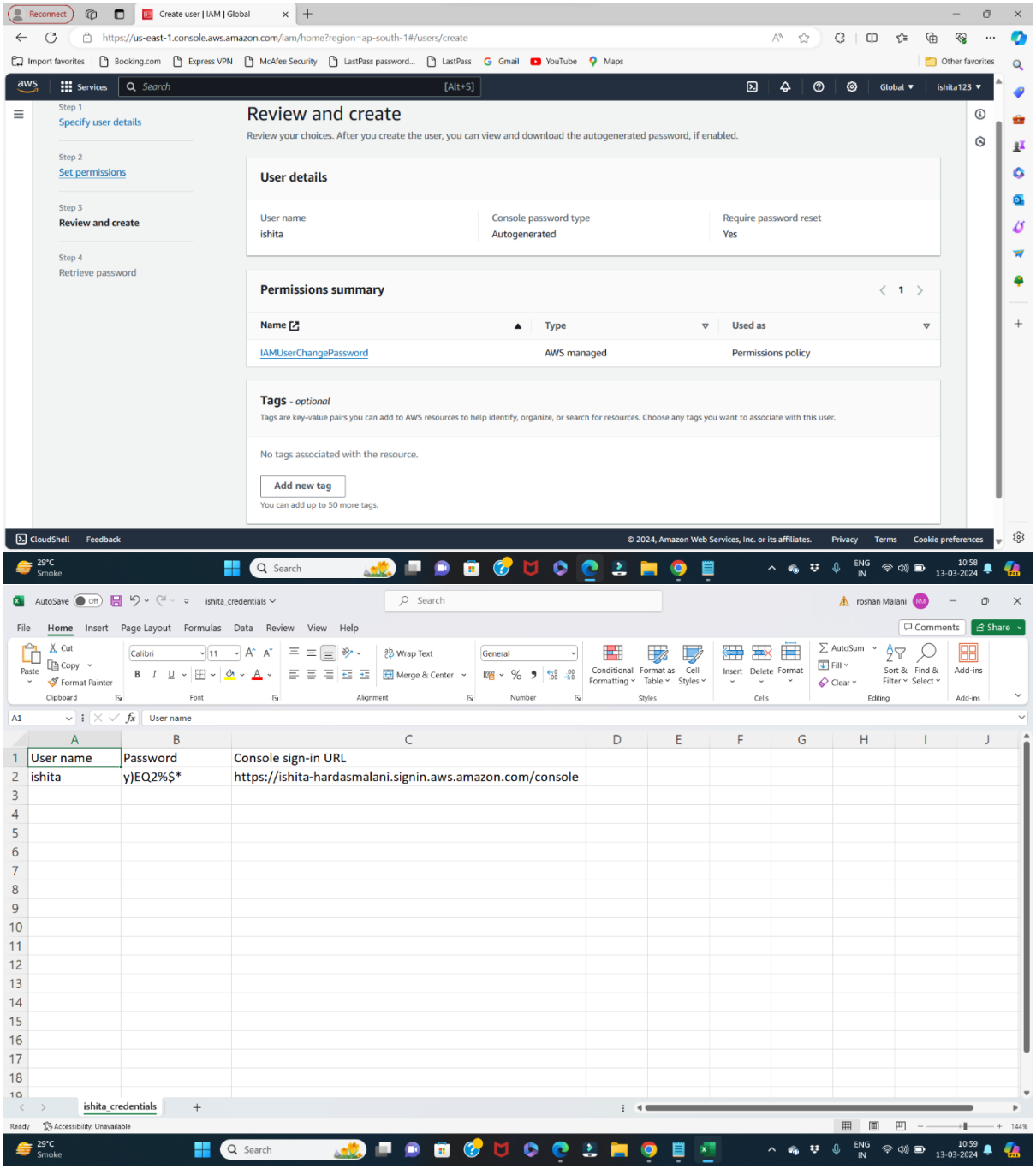


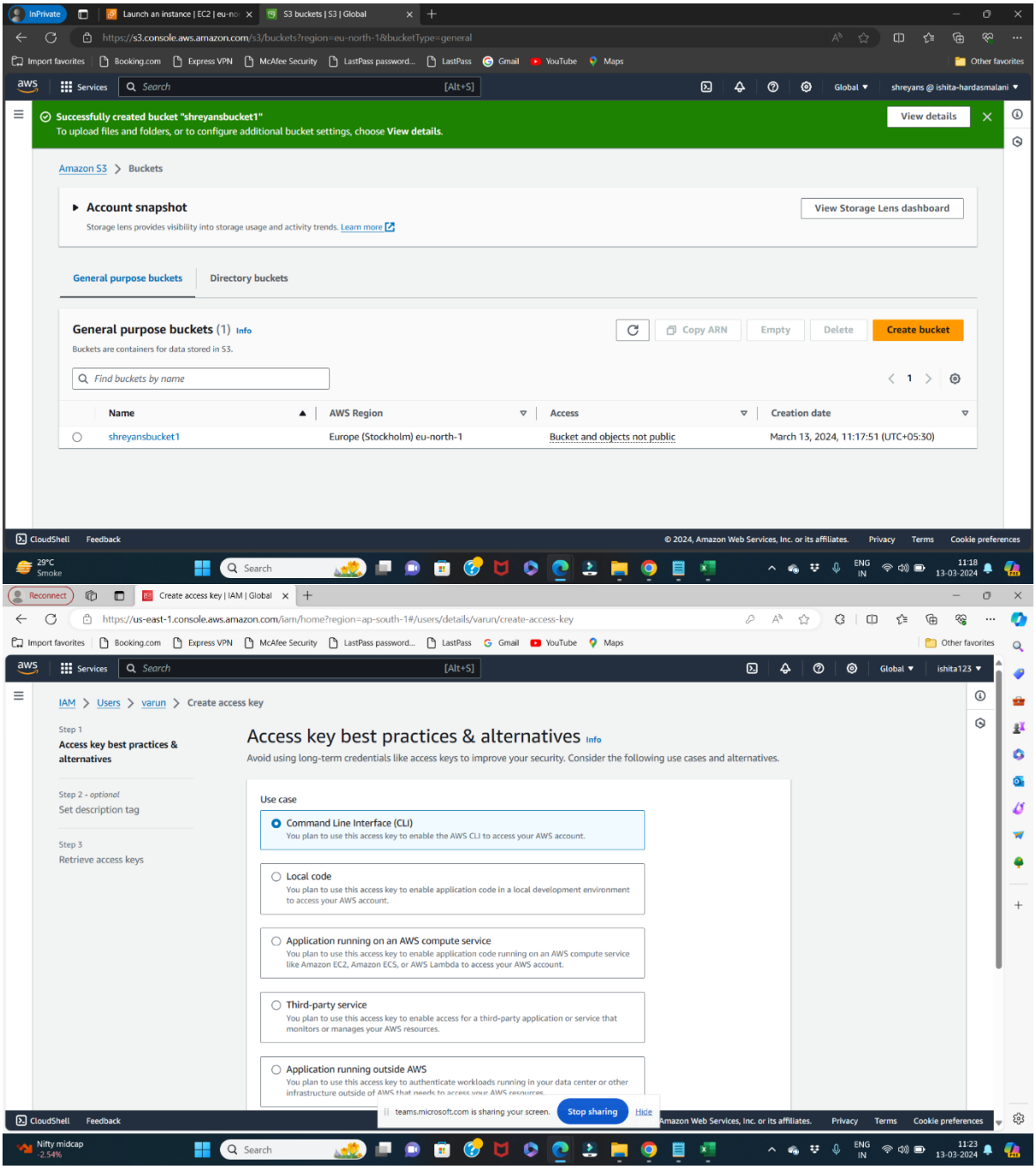
2. Create Users with specific roles and policies assigned



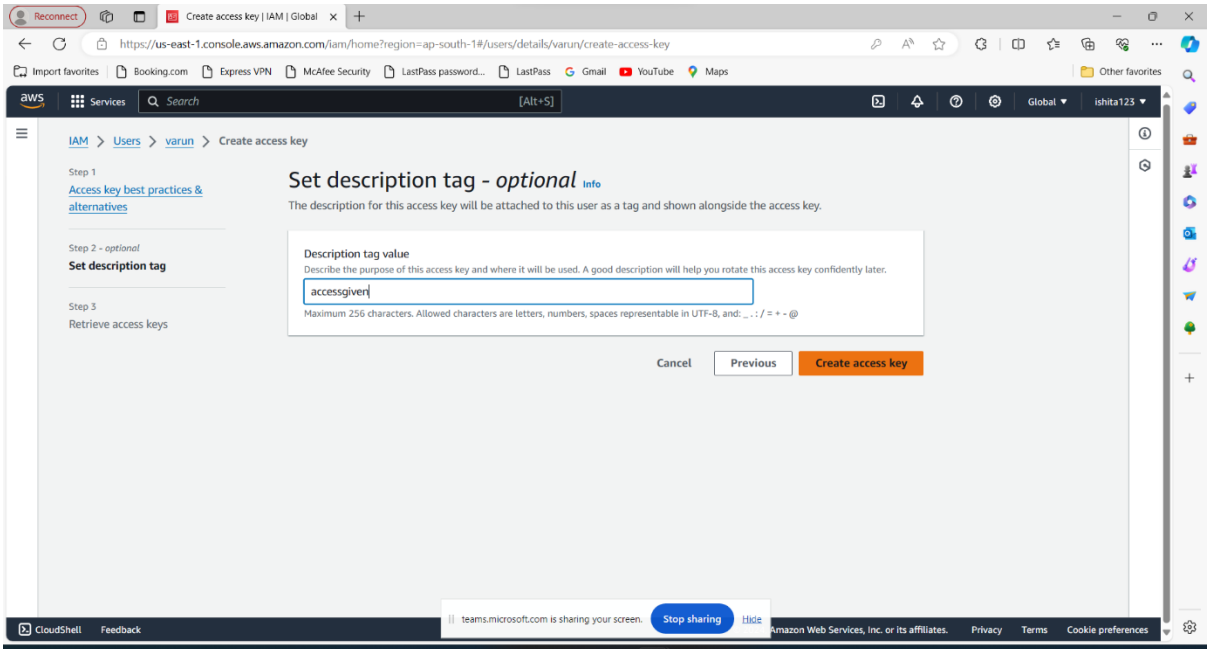

Reconnect
Create user | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
Specify a user 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
CloudShell
Feedback
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Smoke
Search
ENG
IN
10:57
13-03-2024

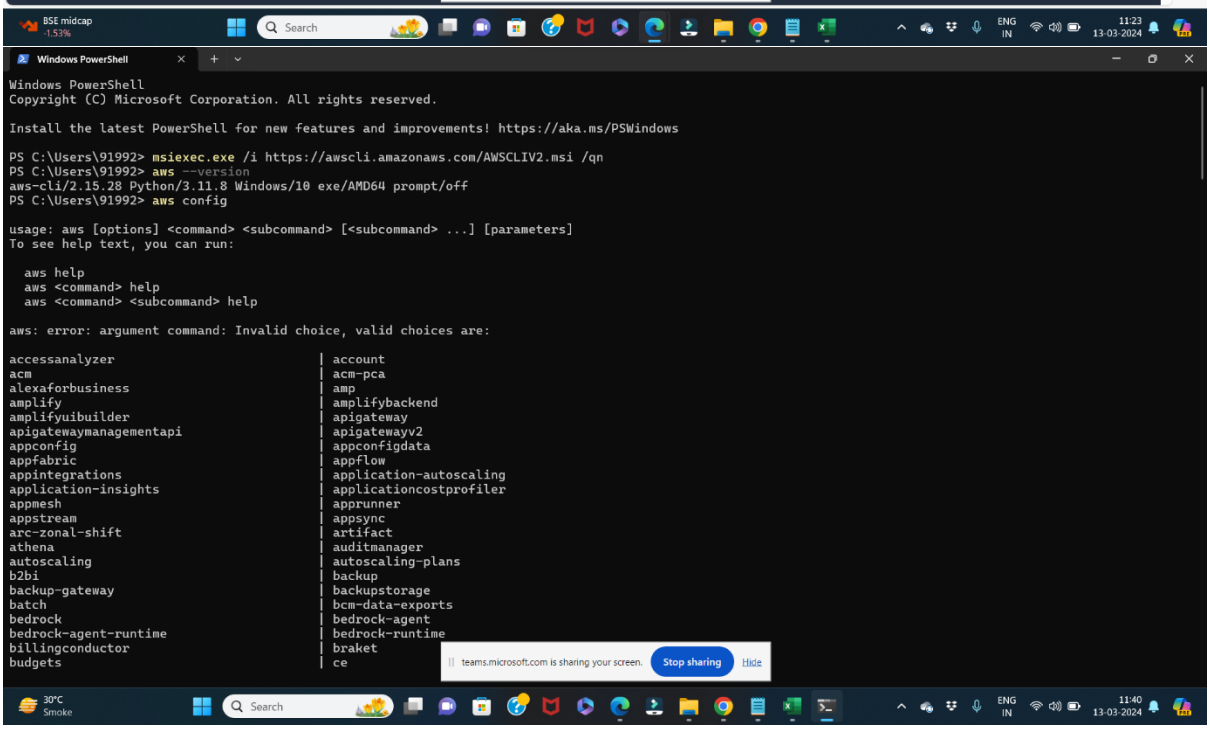

Reconnect
Create user | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
IAM
Users
Create 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
CloudShell
Feedback
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Smoke
Search
ENG
IN
10:58
13-03-2024

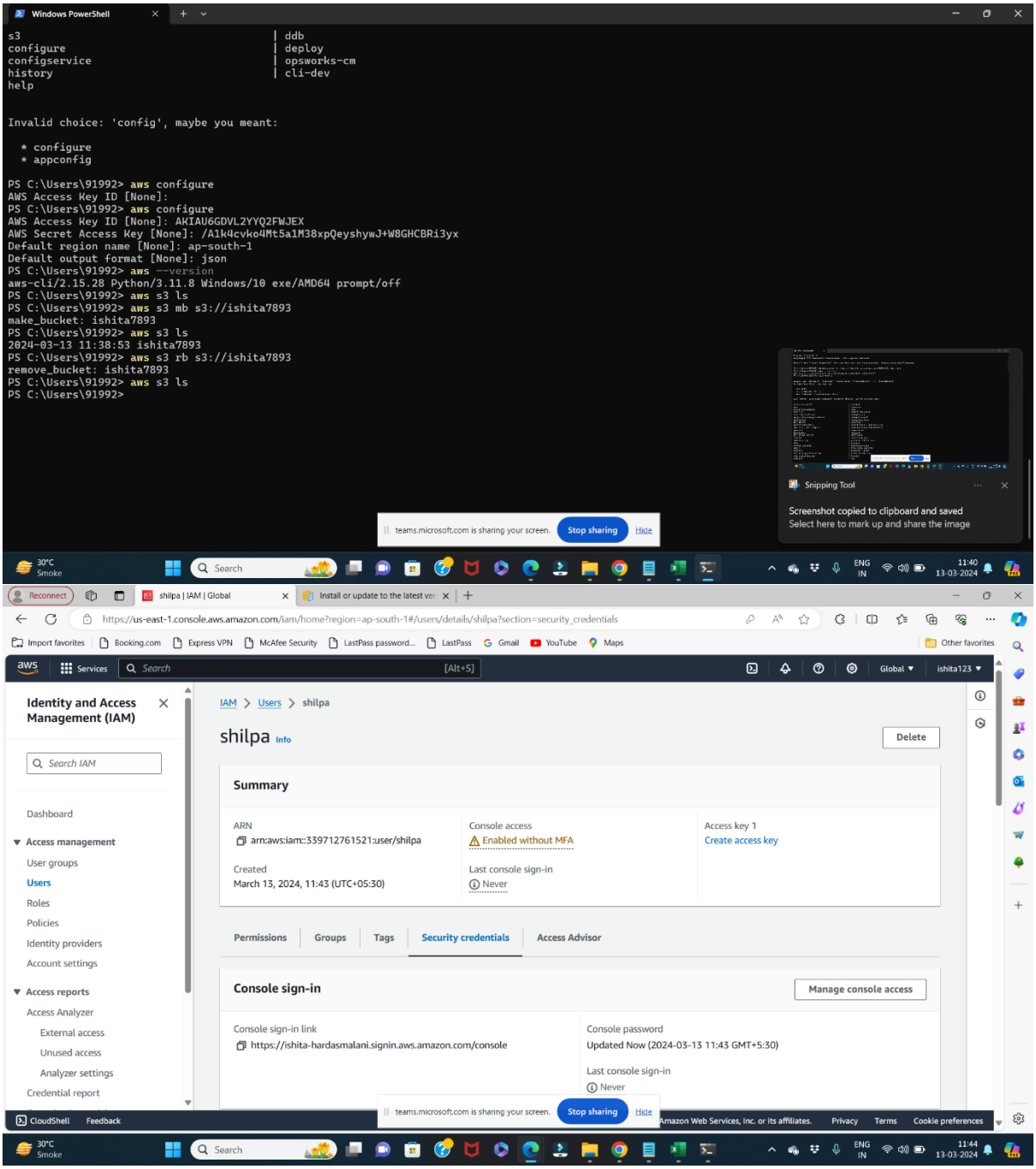

Reconnect
Create user | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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
ishita
Console password type
Autogenerated
Require password reset
Yes
Permissions summary
Name
Type
Used as
IAMUserChangePassword
AWS managed
Permissions policy
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
29°C
Smoke
Search
ENG
IN
10:58
13-03-2024
AutoSave
ishita_credentials
roshan Malani
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Comments
Share
Paste
Cut
Copy
Format Painter
Clipboard
Calibri
11
Font
Wrap Text
Merge & Center
Alignment
General
Number
Conditional Formatting
Format as Table
Cell Styles
Styles
Insert
Delete
Format
Cells
AutoSum
Fill
Clear
Sort & Filter
Find & Select
Editing
Add-ins
A1
User name
A
B
C
D
E
F
G
H
I
J
1
User name
Password
Console sign-in URL
2
ishita
y)EQ2%$*
https://ishita-hardasmalani.signin.aws.amazon.com/console
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
ishita_credentials
Ready
Accessibility: Unavailable
144%
29°C
Smoke
Search
ENG
IN
10:59
13-03-2024

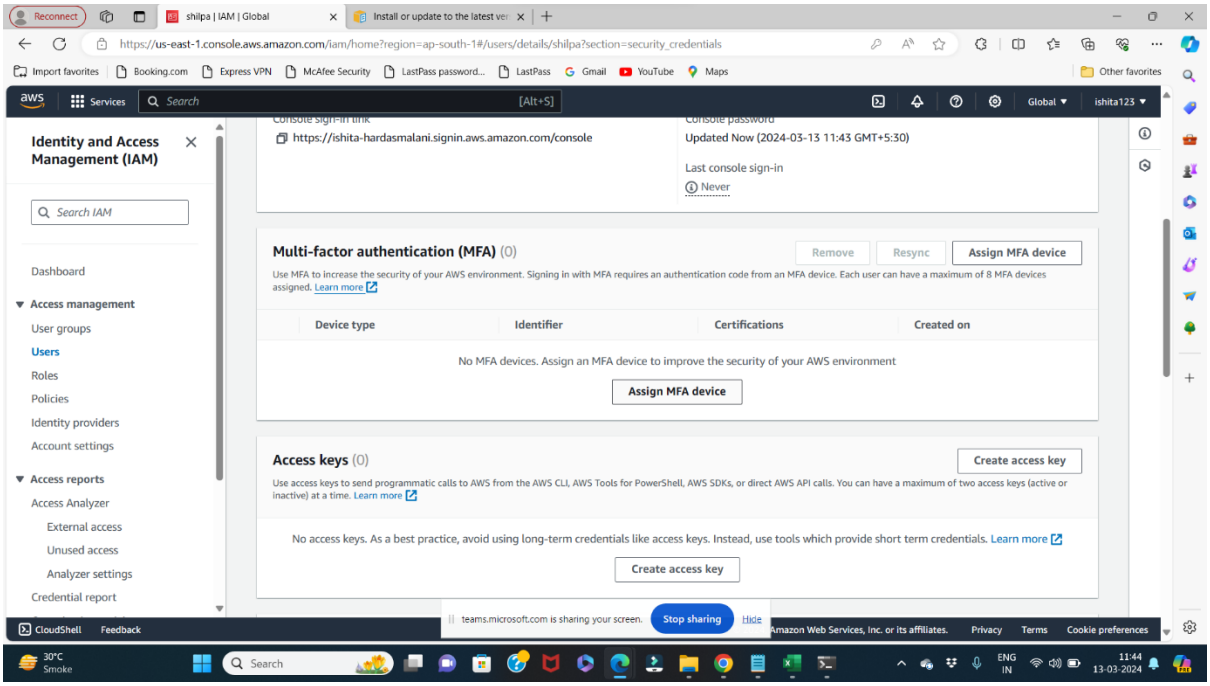

Successfully created bucket "shreyansbucket1"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
shreyansbucket1
Europe (Stockholm) eu-north-1
Bucket and objects not public
March 13, 2024, 11:17:51 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create access key | IAM | Global
IAM > Users > varun > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Access key best practices & alternatives Info
Avoid using long-term credentials like access keys to improve your security. Consider the following use case and alternatives.
Use case
Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.
Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.
Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

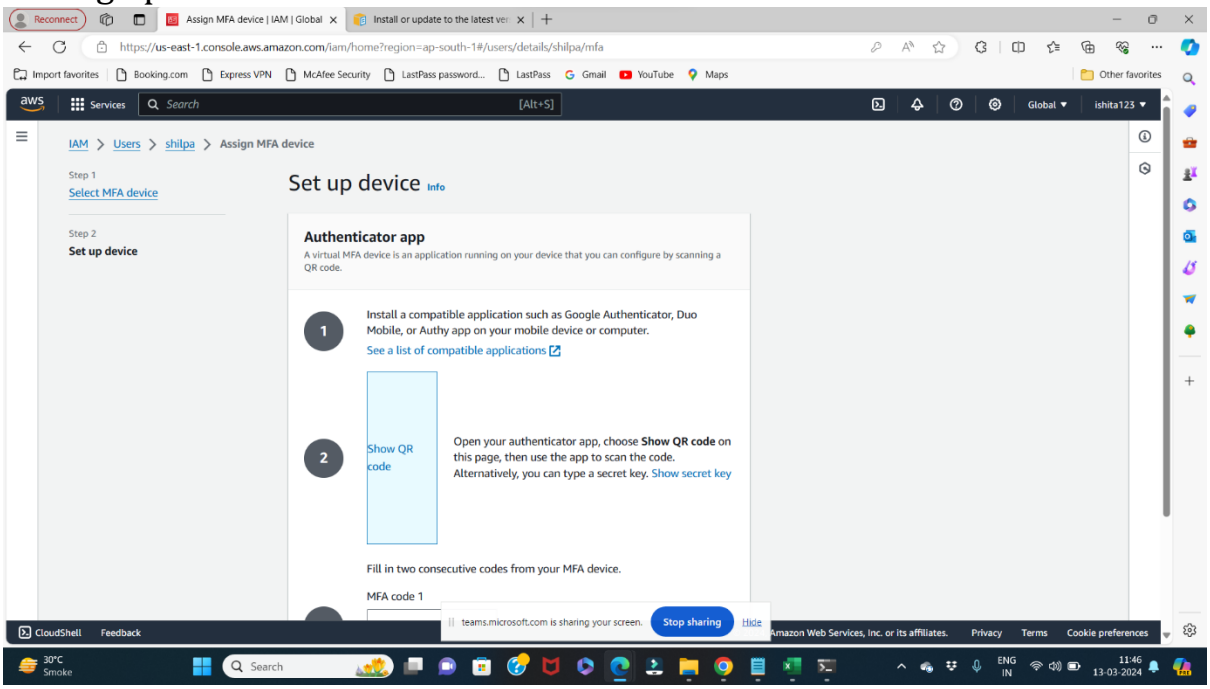

Reconnect
Create access key | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/varun/create-access-key
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
IAM > Users > varun > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Set description tag - optional Info
The description for this access key will be attached to this user as a tag and shown alongside the access key.
Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.
accessgiven
Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @
Cancel
Previous
Create access key
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

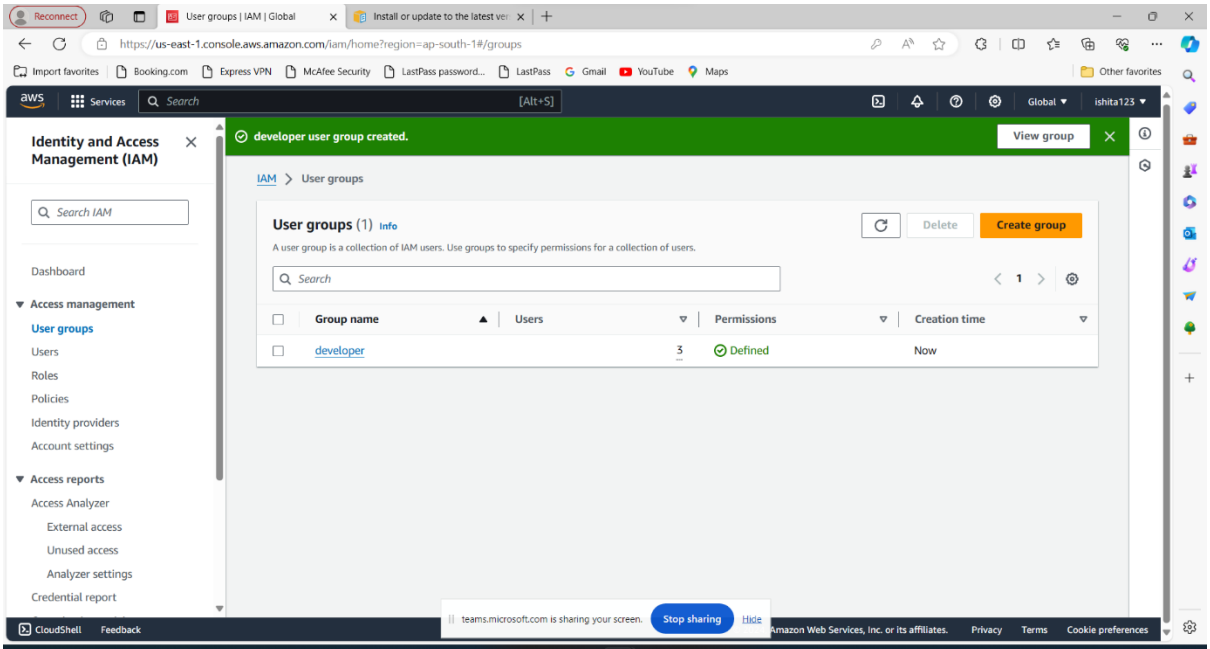

BSE midcap
-1.53%
Search
ENG
IN
11:23
13-03-2024
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\91992> msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi /qn
PS C:\Users\91992> aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
PS C:\Users\91992> aws config
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
aws help
aws <command> help
aws <command> <subcommand> help
aws: error: argument command: Invalid choice, valid choices are:
accessanalyzer | account
acm | acm-pca
alexaforbusiness | amp
amplify | amplifybackend
amplifyuibuilder | apigateway
apigatewaymanagementapi | apigatewayv2
appconfig | appconfigdata
appfabric | appflow
appintegrations | application-autoscaling
application-insights | applicationcostprofiler
appmesh | apprunner
appstream | appsync
arc-zonal-shift | artifact
athena | auditmanager
autoscaling | autoscaling-plans
b2bi | backup
backup-gateway | backupstorage
batch | bcm-data-exports
bedrock | bedrock-agent
bedrock-agent-runtime | bedrock-runtime
billingconductor | braket
budgets | ce
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
30°C
Smoke
Search
ENG
IN
11:40
13-03-2024

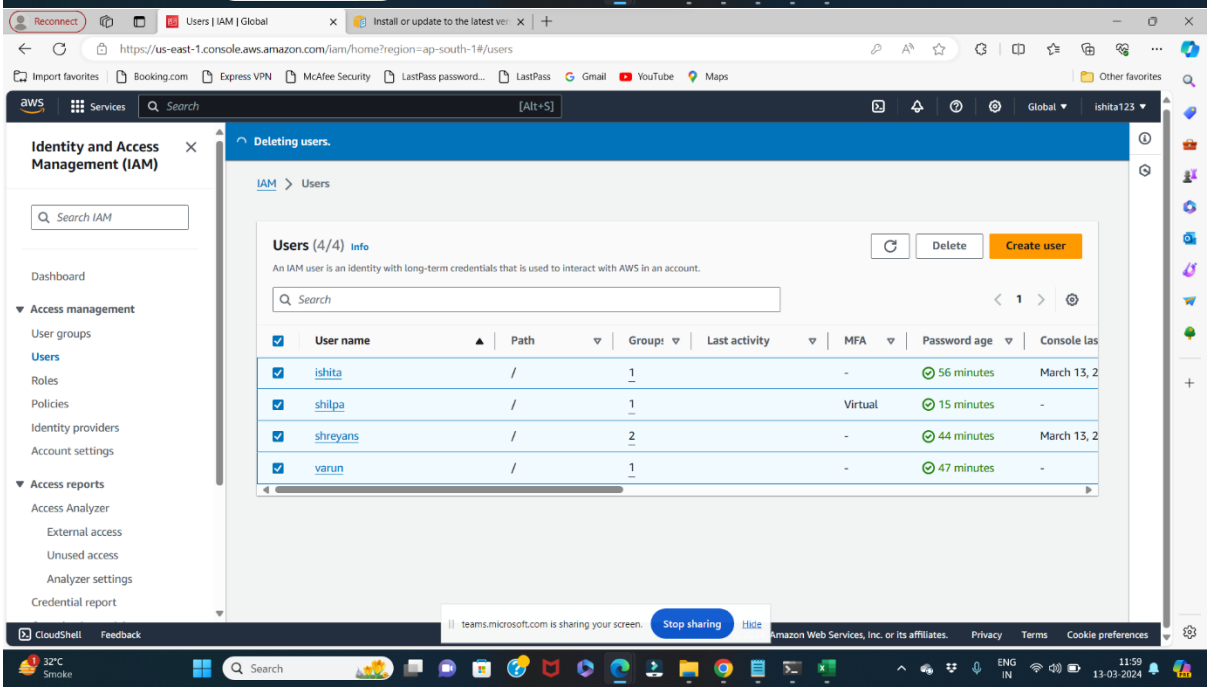

Windows PowerShell
s3 | ddb
configure | deploy
configservice | opsworks-cm
history | cli-dev
help
Invalid choice: 'config', maybe you meant:
* configure
* appconfig
PS C:\Users\91992> aws configure
AWS Access Key ID [None]:
PS C:\Users\91992> aws configure
AWS Access Key ID [None]: AKIAU6GDVL2YYQ2FWJEX
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json
PS C:\Users\91992> aws --version
aws-cli/2.15.28 Python/3.11.8 Windows/10 exe/AMD64 prompt/off
PS C:\Users\91992> aws s3 ls
PS C:\Users\91992> aws s3 mb s3://ishita7893
make_bucket: ishita7893
PS C:\Users\91992> aws s3 ls
2024-03-13 11:38:53 ishita7893
PS C:\Users\91992> aws s3 rb s3://ishita7893
remove_bucket: ishita7893
PS C:\Users\91992> aws s3 ls
PS C:\Users\91992>
Snipping Tool
Screenshot copied to clipboard and saved
Select here to mark up and share the image
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Reconnect
shilpa | IAM | Global
Install or update to the latest ver
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/shilpa?section=security_credentials
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
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
IAM > Users > shilpa
shilpa Info
Delete
Summary
ARN
arn:aws:iam::339712761521:user/shilpa
Console access
Enabled without MFA
Access key 1
Create access key
Created
March 13, 2024, 11:43 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Access Advisor
Console sign-in
Manage console access
Console sign-in link
https://ishita-hardasmalani.signin.aws.amazon.com/console
Console password
Updated Now (2024-03-13 11:43 GMT+5:30)
Last console sign-in
Never
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
30°C
Smoke
Search
ENG
IN
11:40
13-03-2024
11:44
13-03-2024

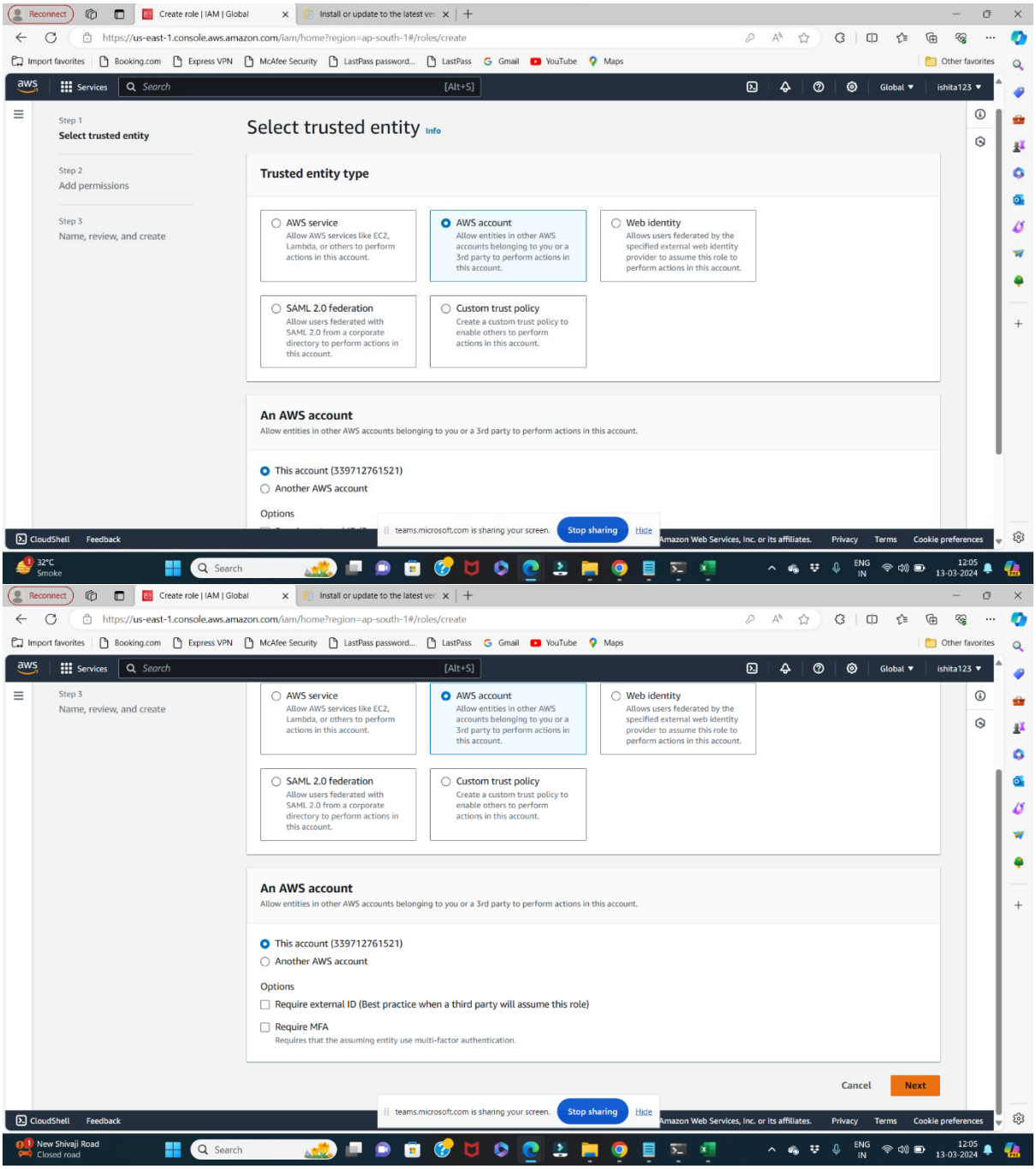


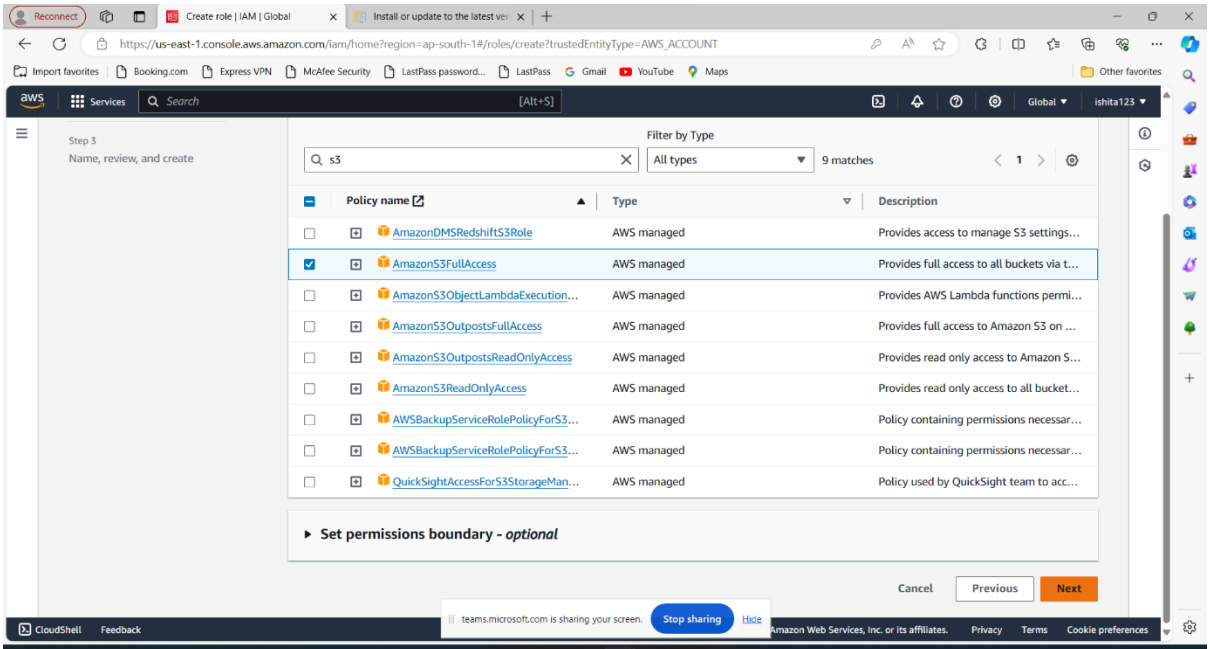
3. Setting up MFA

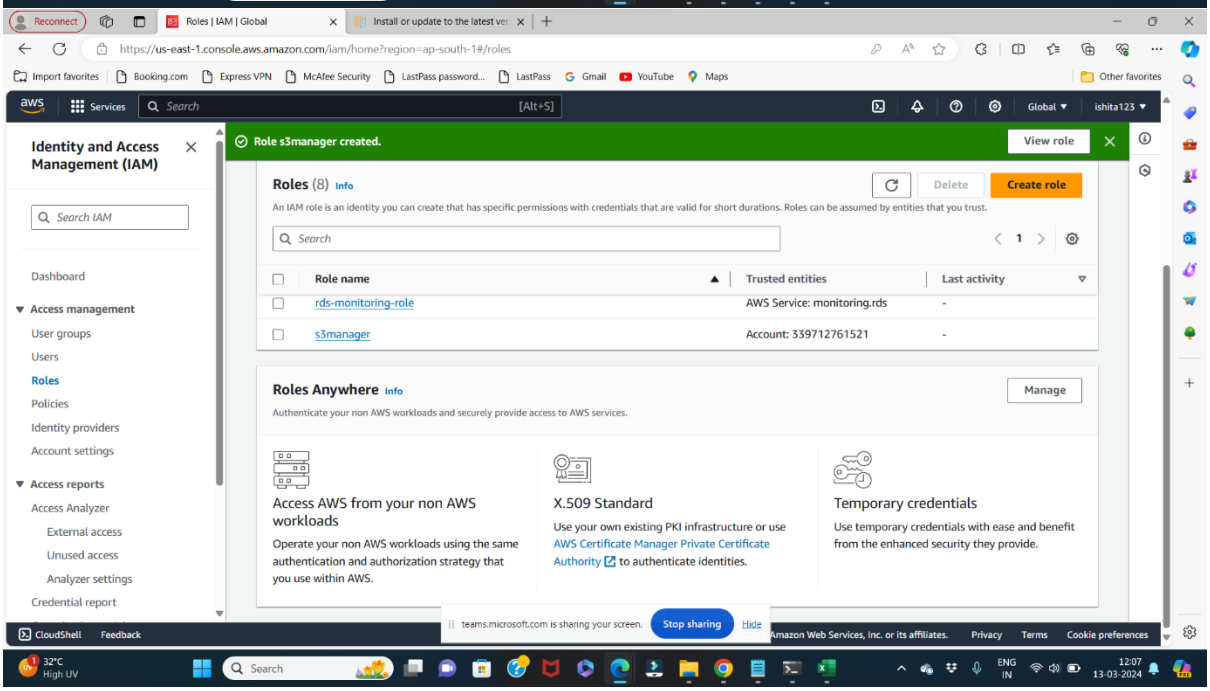


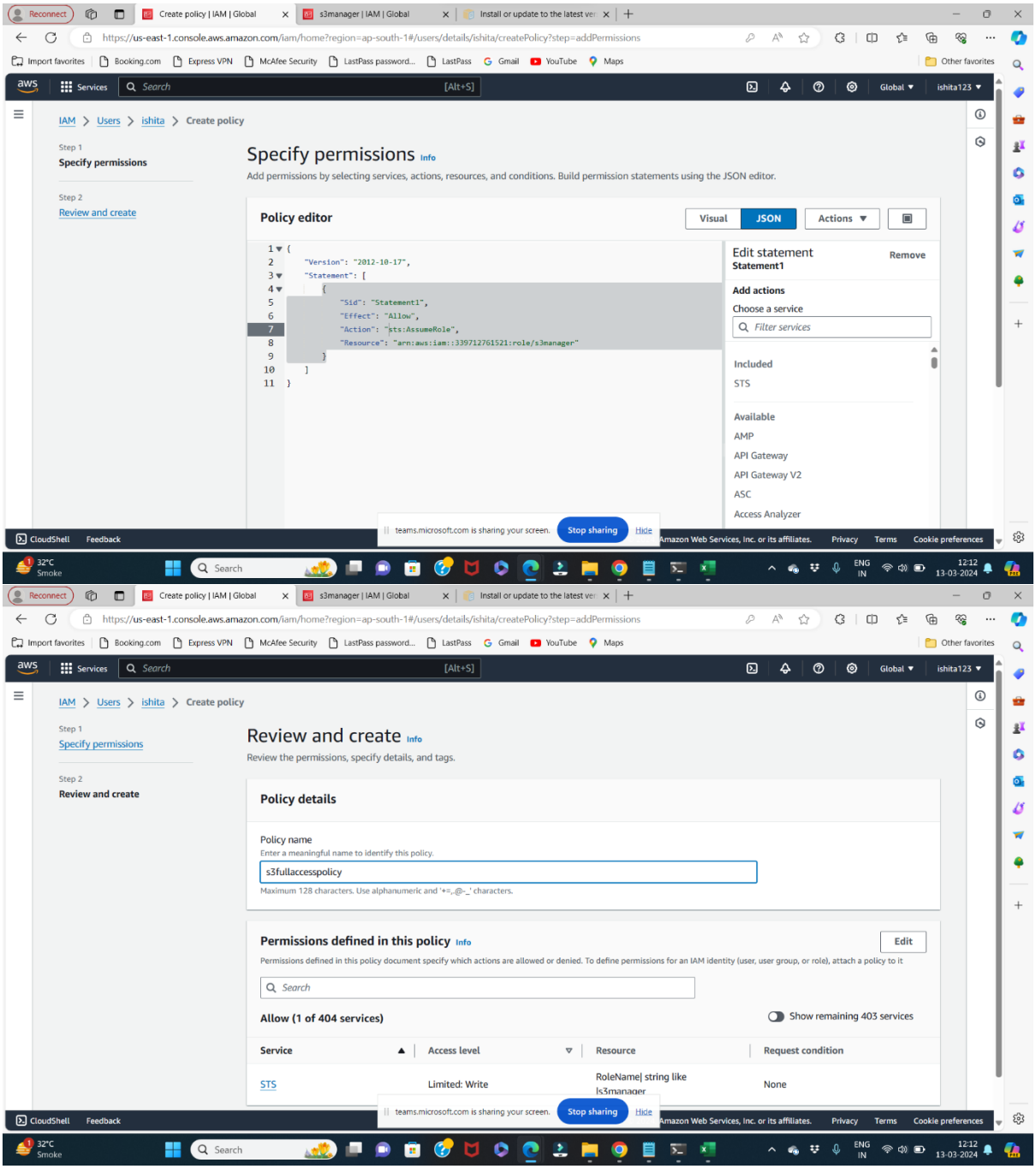

Reconnect
User groups | IAM | Global
Install or update to the latest ver
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
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
developer user group created.
View group
IAM > User groups
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
developer
3
Defined
Now
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
30°C
Smoke
Search
ENG
IN
11:53
13-03-2024


Reconnect
Users | IAM | Global
Install or update to the latest ver
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
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
Deleting users.
IAM > Users
Users (4/4) 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 las
ishita
/
1
-
56 minutes
March 13, 2
shilpa
/
1
Virtual
15 minutes
-
shreyans
/
2
-
44 minutes
March 13, 2
varun
/
1
-
47 minutes
-
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
11:59
13-03-2024

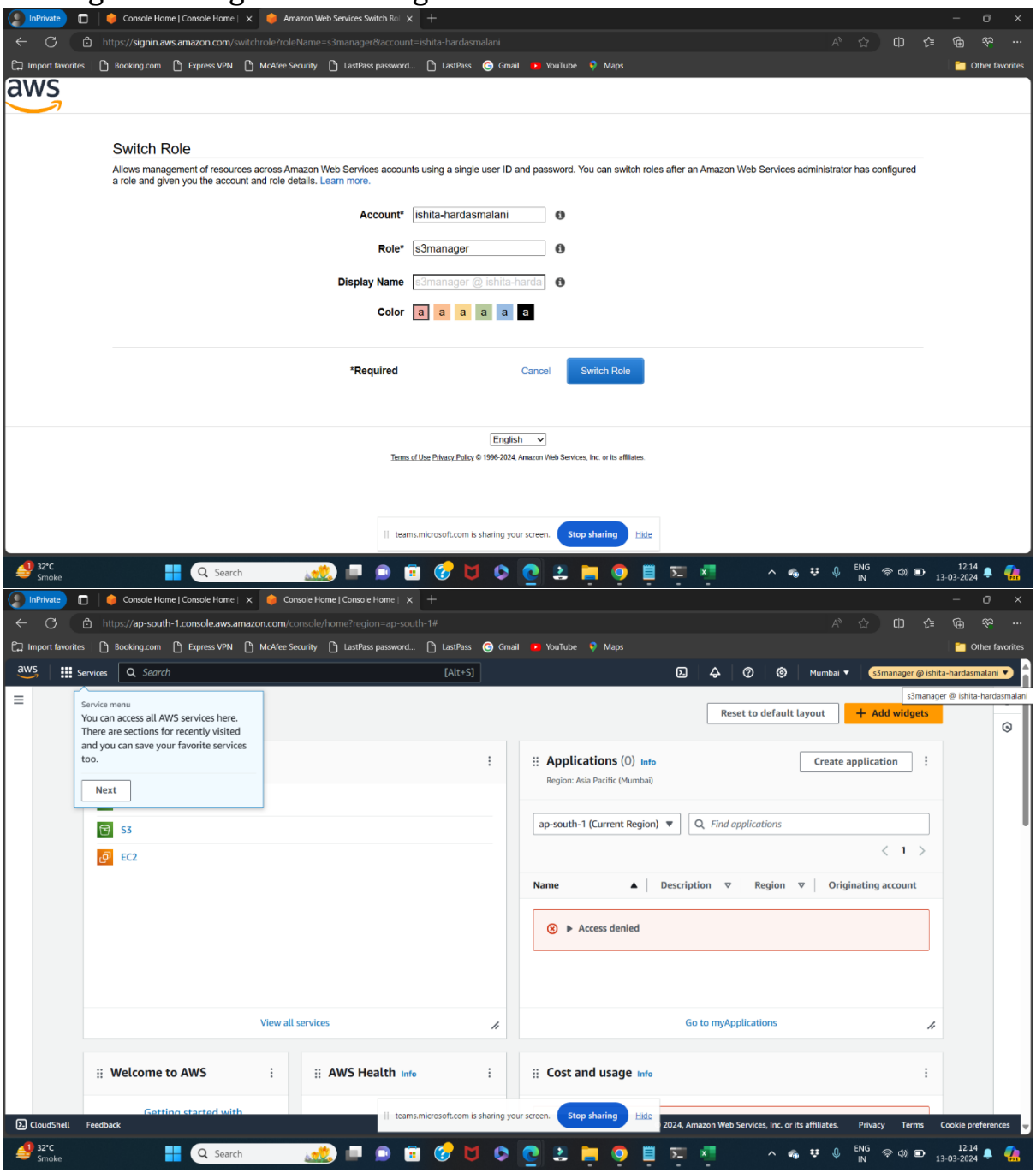

Reconnect
Create role | IAM | Global
Install or update to the latest ver
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
This account (339712761521)
Another AWS account
Options
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
12:05
13-03-2024
Reconnect
Create role | IAM | Global
Install or update to the latest ver
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
Step 3
Name, review, and create
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
This account (339712761521)
Another AWS account
Options
Require external ID (Best practice when a third party will assume this role)
Require MFA
Requires that the assuming entity use multi-factor authentication.
Cancel
Next
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
New Shivaji Road
Closed road
Search
ENG
IN
12:05
13-03-2024

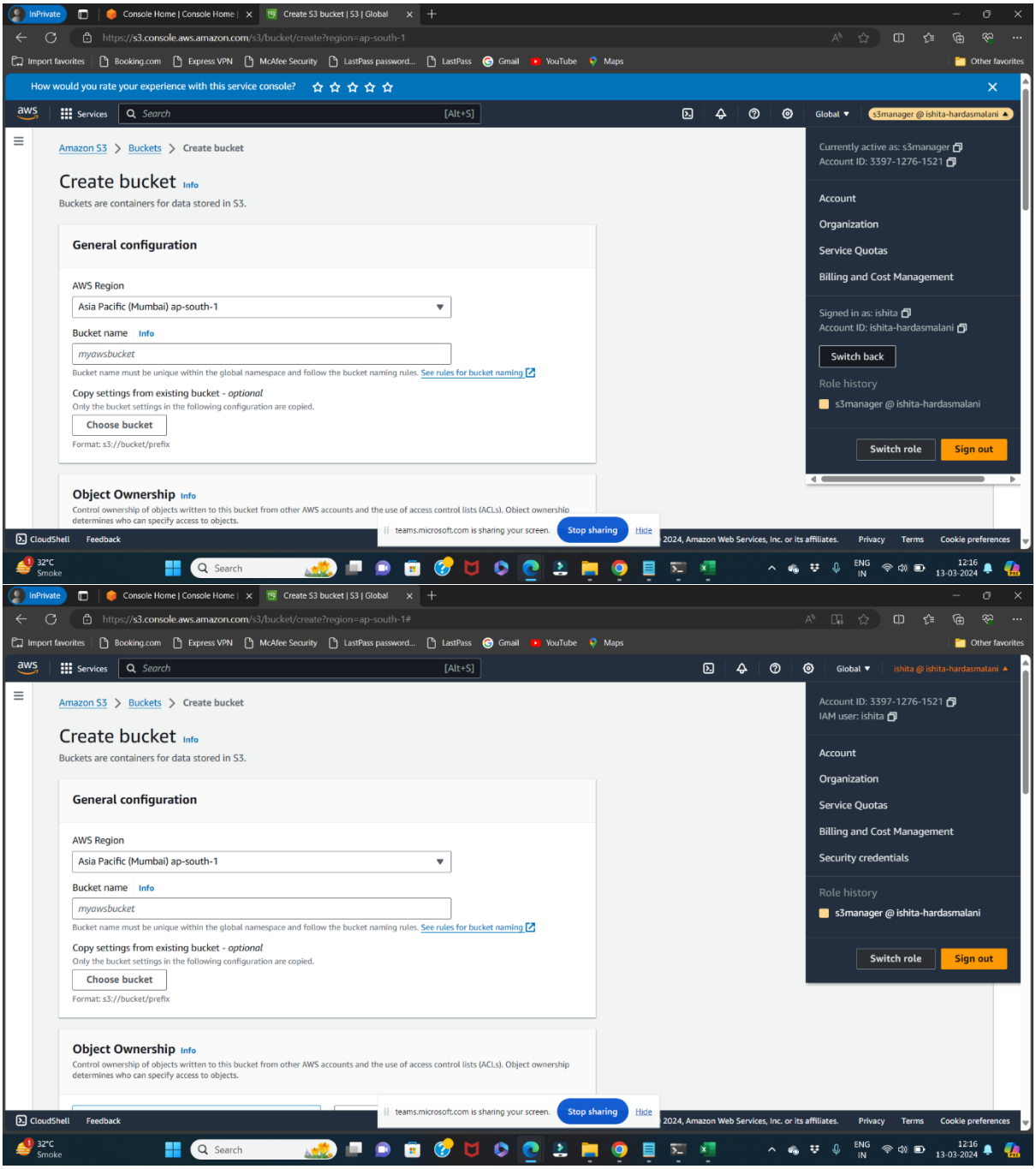

Reconnect
Create role | IAM | Global
Install or update to the latest ver
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_ACCOUNT
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
Step 3
Name, review, and create
Filter by Type
s3
All types
9 matches
1
Policy name
Type
Description
AmazonDMSRedshiftS3Role
AWS managed
Provides access to manage S3 settings...
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via t...
AmazonS3ObjectLambdaExecution...
AWS managed
Provides AWS Lambda functions permi...
AmazonS3OutpostsFullAccess
AWS managed
Provides full access to Amazon S3 on ...
AmazonS3OutpostsReadOnlyAccess
AWS managed
Provides read only access to Amazon S...
AmazonS3ReadOnlyAccess
AWS managed
Provides read only access to all bucket...
AWSBackupServiceRolePolicyForS3...
AWS managed
Policy containing permissions necessar...
AWSBackupServiceRolePolicyForS3...
AWS managed
Policy containing permissions necessar...
QuickSightAccessForS3StorageMan...
AWS managed
Policy used by QuickSight team to acc...
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
New Shivaji Road
Closed road
Search
ENG
IN
12:06
13-03-2024


Reconnect
Roles | IAM | Global
Install or update to the latest ver
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles
Import favorites
Booking.com
Express VPN
McAfee Security
LastPass password...
LastPass
Gmail
YouTube
Maps
Other favorites
aws
Services
Search
[Alt+S]
Global
ishita123
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
Role s3manager created.
View role
Roles (8) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Search
1
Role name
Trusted entities
Last activity
rds-monitoring-role
AWS Service: monitoring.rds
-
s3manager
Account: 339712761521
-
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.
X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.
Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.
CloudShell
Feedback
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
High UV
Search
ENG
IN
12:07
13-03-2024


Create policy | IAM | Global
s3manager | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ishita/createPolicy?step=addPermissions
IAM > Users > ishita > 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": "Statement1",
"Effect": "Allow",
"Action": "sts:AssumeRole",
"Resource": "arn:aws:iam::339712761521:role/s3manager"
}
]
}
Edit statement
Statement1
Remove
Add actions
Choose a service
Filter services
Included
STS
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Privacy
Terms
Cookie preferences
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
s3fullaccesspolicy
Maximum 128 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 404 services)
Show remaining 403 services
Service
Access level
Resource
Request condition
STS
Limited: Write
RoleName| string like
|s3manager
None

4. 4.Using according to roles assigned




InPrivate
Console Home | Console Home
Create S3 bucket | S3 | Global
https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
How would you rate your experience with this service console?
Services
Search
[Alt+S]
Global
s3manager @ ishita-hardasmalani
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket name Info
myawsbucket
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
Currently active as: s3manager
Account ID: 3397-1276-1521
Account
Organization
Service Quotas
Billing and Cost Management
Signed in as: ishita
Account ID: ishita-hardasmalani
Switch back
Role history
s3manager @ ishita-hardasmalani
Switch role
Sign out
CloudShell
Feedback
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
12:16
13-03-2024

InPrivate
Console Home | Console Home
Create S3 bucket | S3 | Global
https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1#
Services
Search
[Alt+S]
Global
ishita @ ishita-hardasmalani
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket name Info
myawsbucket
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
Account ID: 3397-1276-1521
IAM user: ishita
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Role history
s3manager @ ishita-hardasmalani
Switch role
Sign out
CloudShell
Feedback
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
12:16
13-03-2024