Terna Engineering College
Computer Engineering Department
Program: Sem VIII

Course: Cloud Computing Lab (CSL803)

Faculty: Reshma Koli

Experiment No. 7

A.1 Aim: Understand Security of Web Server and demonstration of IAM using own cloud/AWS.

PART B
(PART B: TO BE COMPLETED BY STUDENTS)

Roll No. 50	**Name:** AMEY MAHENDRA THAKUR
Class: BE COMPS B 50	**Batch:** B3
Date of Experiment: 23-02-2022	**Date of Submission:** 23-02-2022
Grade:	

B.1 Question of Curiosity:

Q.1 Explain User Management in cloud computing Detail?

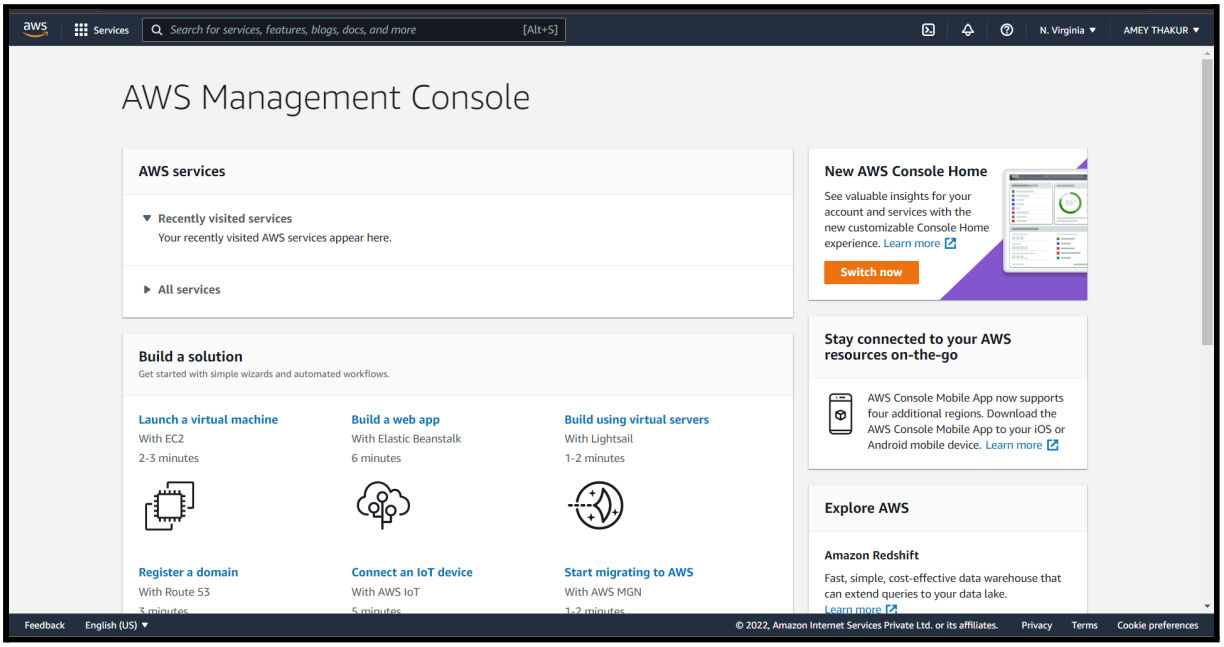
ANS:

- User management describes the ability for administrators to manage user access to various IT resources like systems, devices, applications, storage systems, networks, SaaS services, and more. User management is a core part of any identity and access management (IAM) solution, in particular directory services tools. Controlling and managing user access to IT resources is fundamental security essential for any organization. User management enables admins to control user access and on-board and off-board users to and from IT resources. Subsequently, a directory service will then authenticate, authorize, and audit user access to IT resources based on what the IT admin had dictated.
- Traditionally, user management and authentication services have been grounded with Windows-based on-prem servers, databases, and closed virtual private networks (VPN) through an on-prem identity provider (IdP) such as Microsoft Active Directory. However, recent trends are seeing a shift towards cloud-based identity and access management (IAM), granting administrators even greater control over digital assets. These solutions enable user management over web applications, cloud infrastructure, non-Windows devices, and more leveraging modern protocols such as SAML JIT and SCIM (among others).

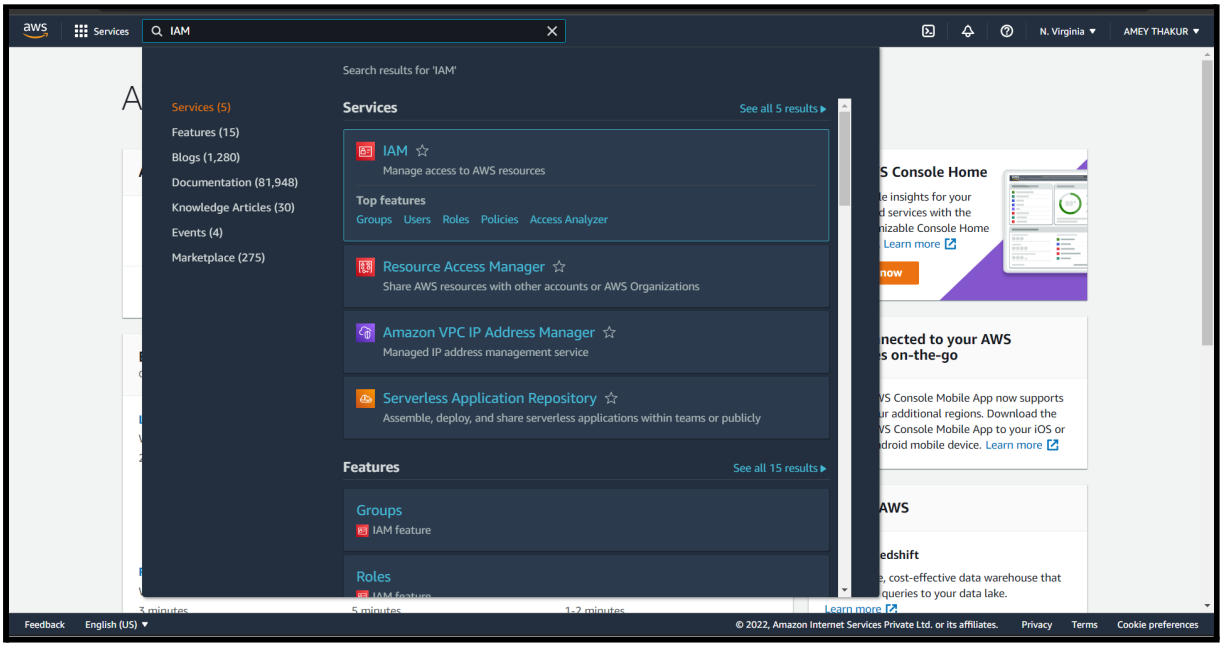
Q.2 Add snapshots for creating IAM user and user groups (using AWS IAM service).
ANS:

Practical Video (AWS IAM Service): https://youtu.be/dnmuv0PC7W8

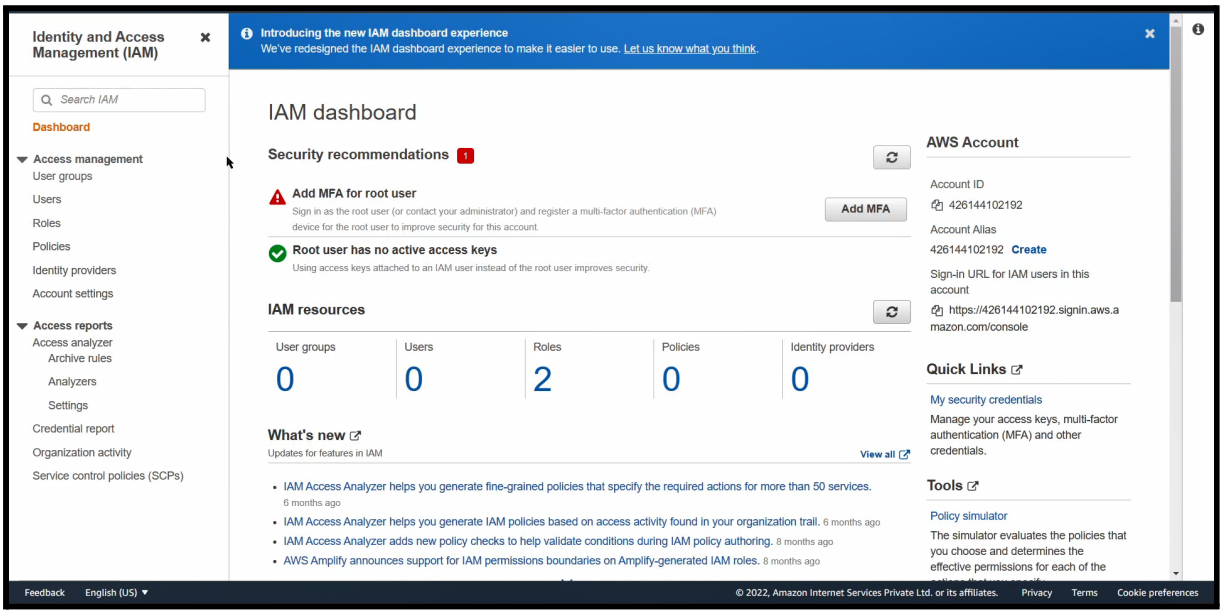
Step 1:



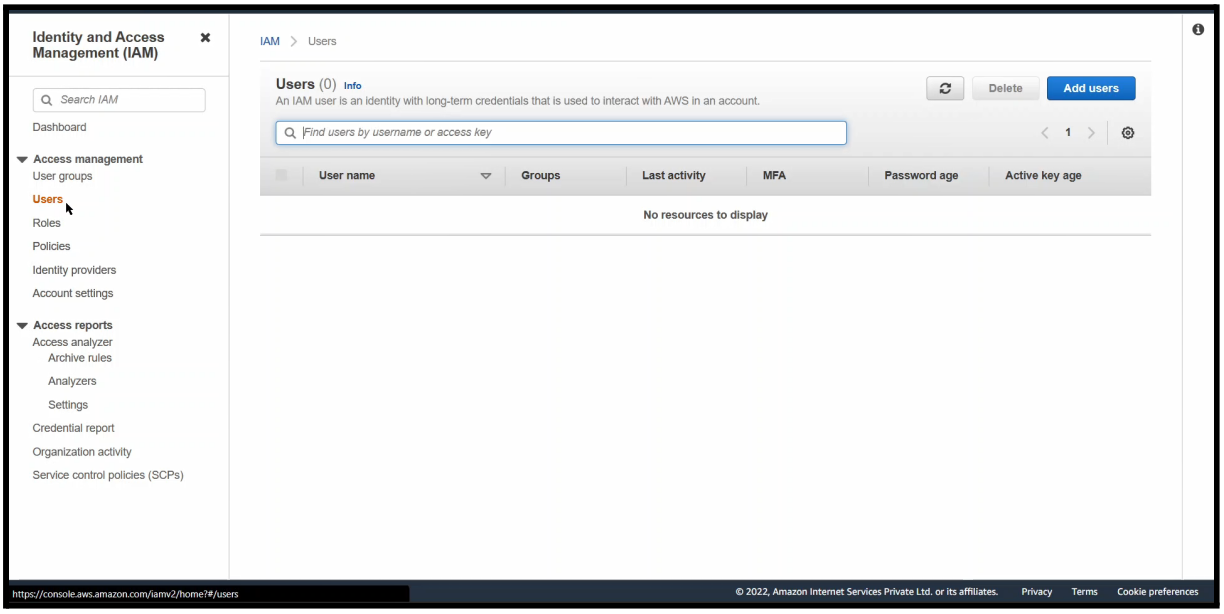
Step 2:



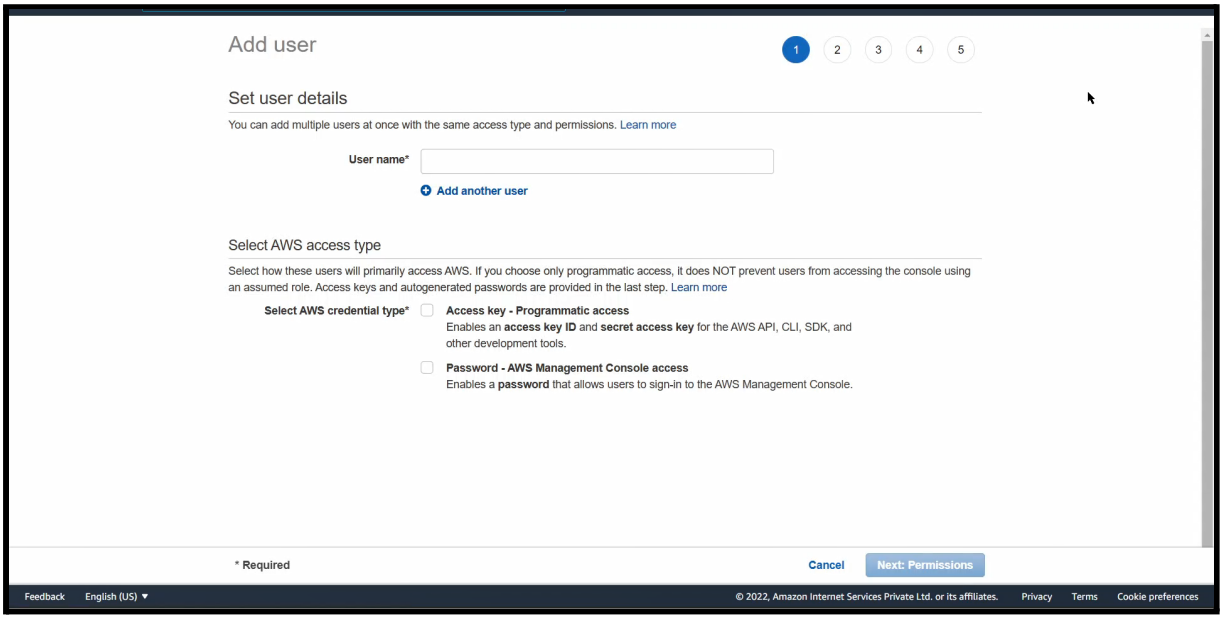
Step 3:


Identity and Access Management (IAM)
Search 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)
Introducing the new IAM dashboard experience
We've redesigned the IAM dashboard experience to make it easier to use. Let us know what you think.
IAM dashboard
Security recommendations 1
Add MFA for root user
Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device 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
User groups 0
Users 0
Roles 2
Policies 0
Identity providers 0
What's new
Updates for features in IAM
View all
IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 6 months ago
IAM Access Analyzer helps you generate IAM policies based on access activity found in your organization trail. 6 months ago
IAM Access Analyzer adds new policy checks to help validate conditions during IAM policy authoring. 8 months ago
AWS Amplify announces support for IAM permissions boundaries on Amplify-generated IAM roles. 8 months ago
AWS Account
Account ID
426144102192
Account Alias
426144102192 Create
Sign-in URL for IAM users in this account
https://426144102192.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

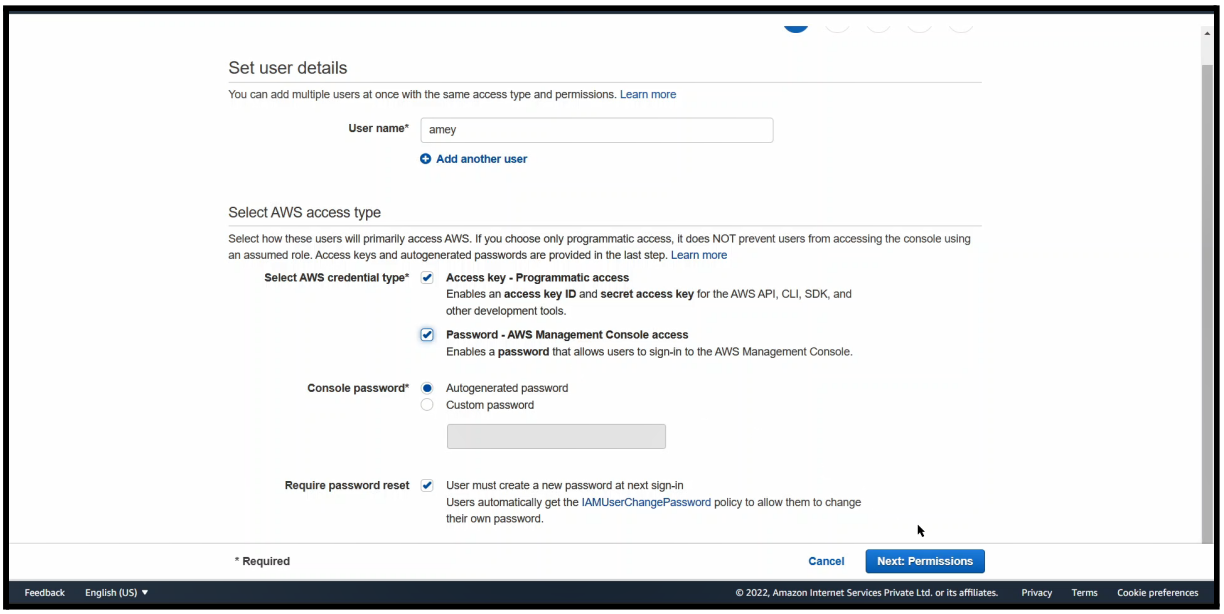
Step 4:


Identity and Access Management (IAM)
Search 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 > 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
Add users
Find users by username or access key
User name
Groups
Last activity
MFA
Password age
Active key age
No resources to display
https://console.aws.amazon.com/iamv2/home?#/users
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

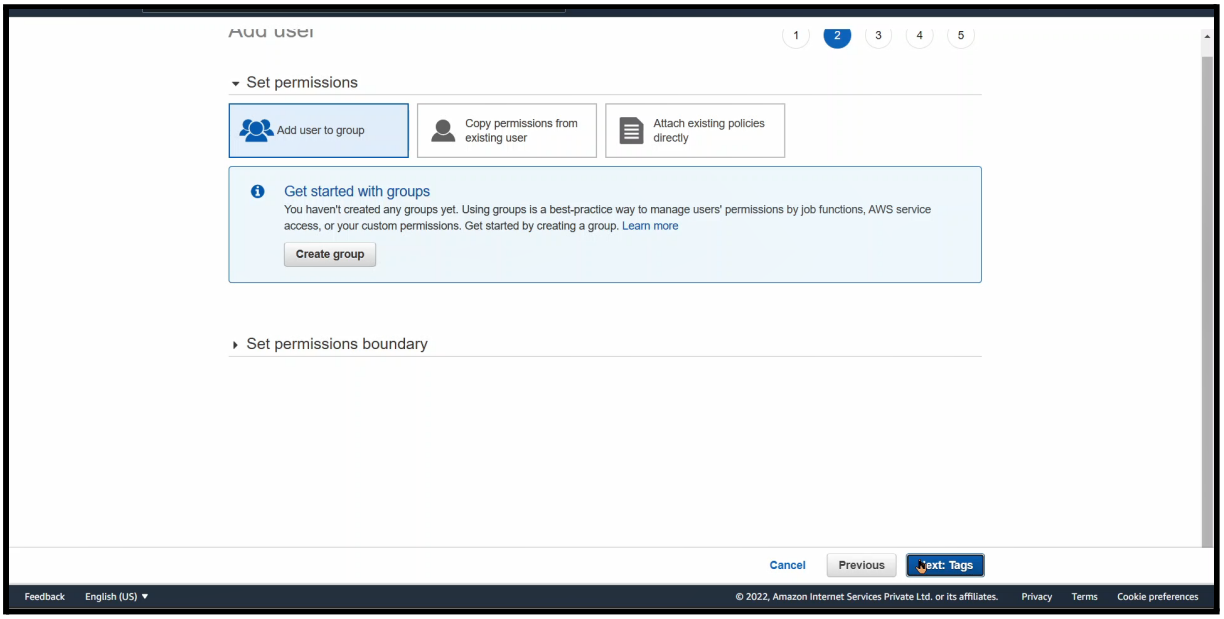
Step 5:


Add user
1 2 3 4 5
Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
Add another user
Select AWS access type
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more
Select AWS credential type*
Access key - Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
Password - AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.
* Required
Cancel
Next: Permissions
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

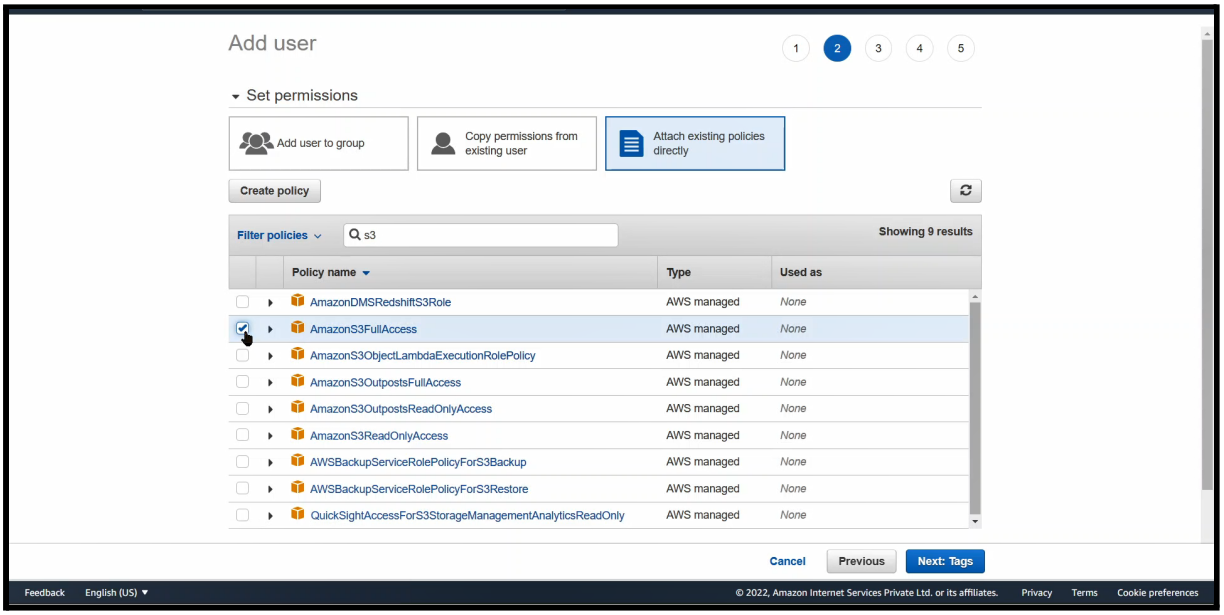
Step 6:


Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
amey
Add another user
Select AWS access type
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more
Select AWS credential type*
Access key - Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
Password - AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.
Console password*
Autogenerated password
Custom password
Require password reset
User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
* Required
Cancel
Next: Permissions
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

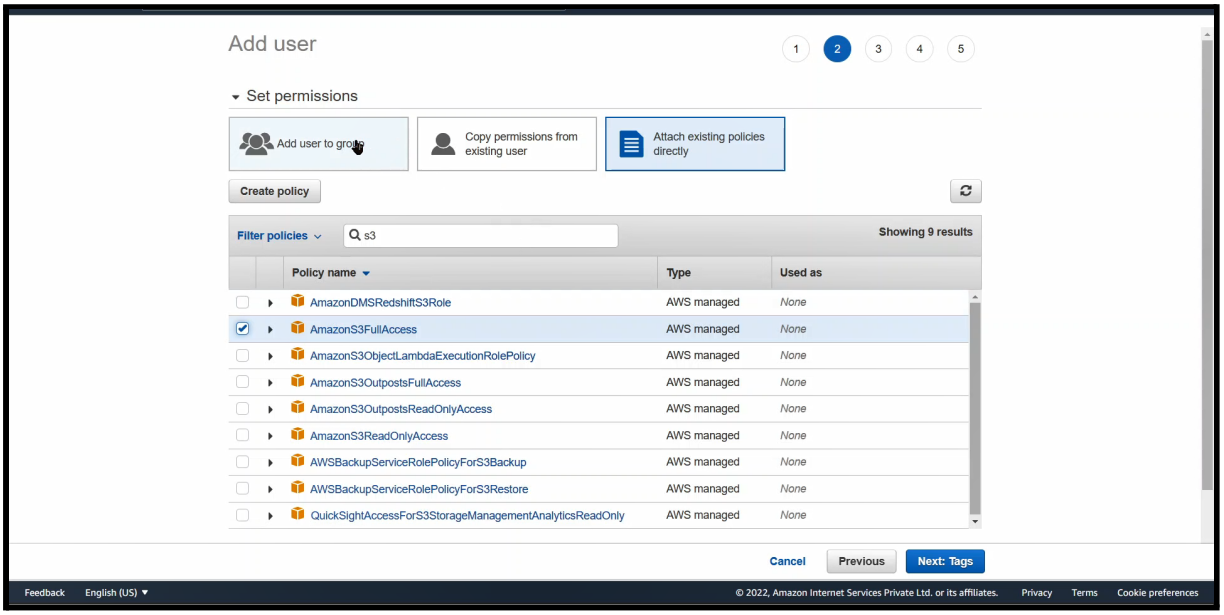
Step 7:


Add user
1 2 3 4 5
Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly
Get started with groups
You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. Learn more
Create group
Set permissions boundary
Cancel
Previous
Next: Tags
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

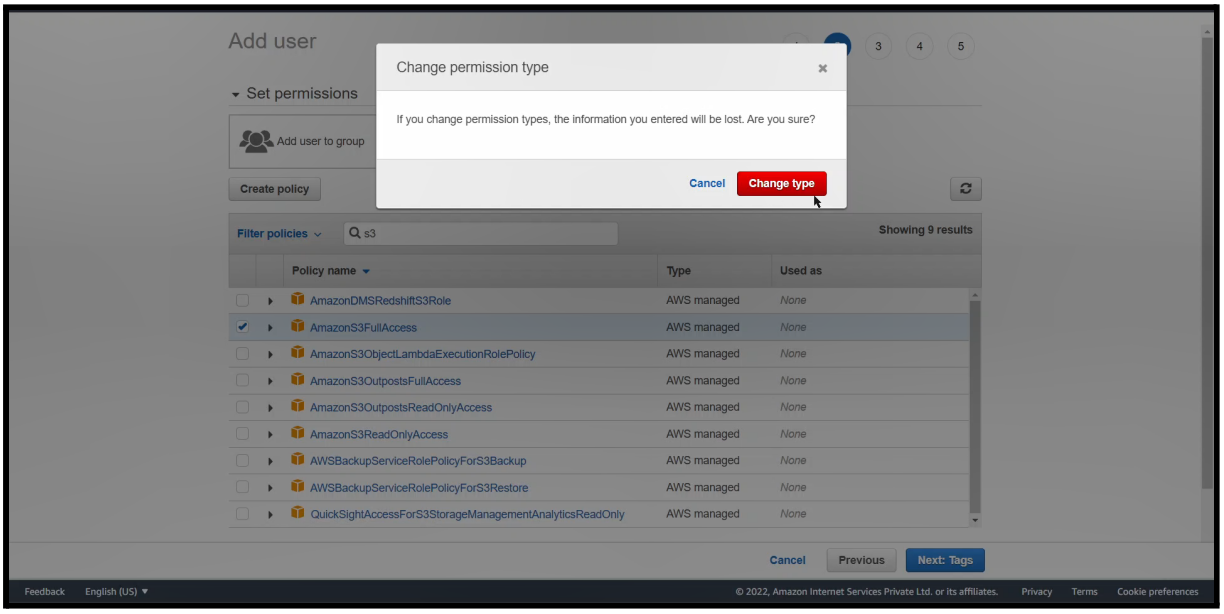
Step 8:


Add user
1 2 3 4 5
Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies
s3
Showing 9 results
Policy name
Type
Used as
AmazonDMSRedshiftS3Role AWS managed None
AmazonS3FullAccess AWS managed None
AmazonS3ObjectLambdaExecutionRolePolicy AWS managed None
AmazonS3OutpostsFullAccess AWS managed None
AmazonS3OutpostsReadOnlyAccess AWS managed None
AmazonS3ReadOnlyAccess AWS managed None
AWSBackupServiceRolePolicyForS3Backup AWS managed None
AWSBackupServiceRolePolicyForS3Restore AWS managed None
QuickSightAccessForS3StorageManagementAnalyticsReadOnly AWS managed None
Cancel
Previous
Next: Tags
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

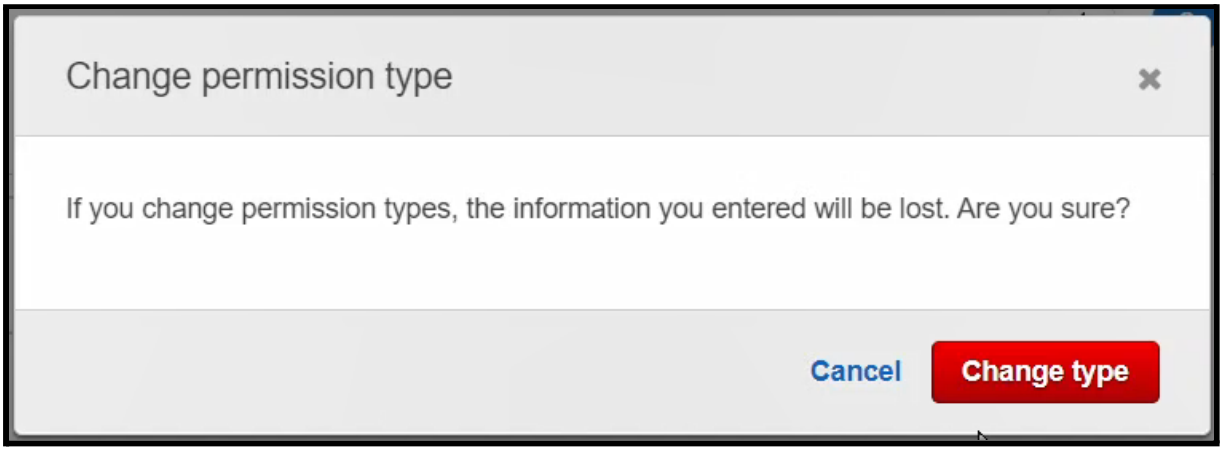
Step 9:



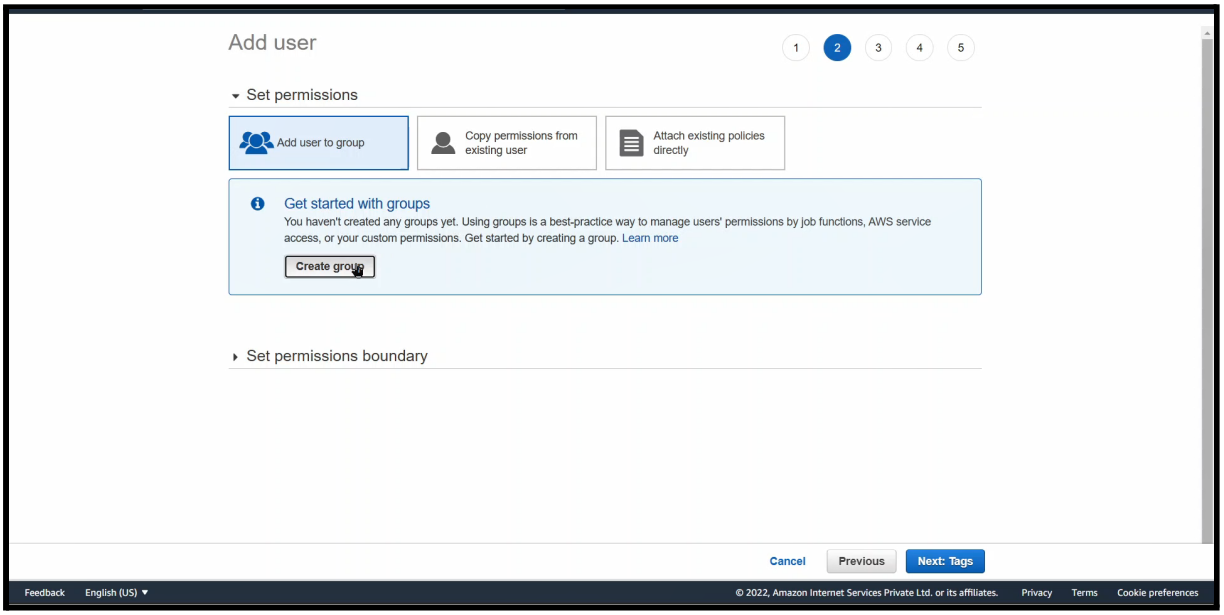
Step 10:



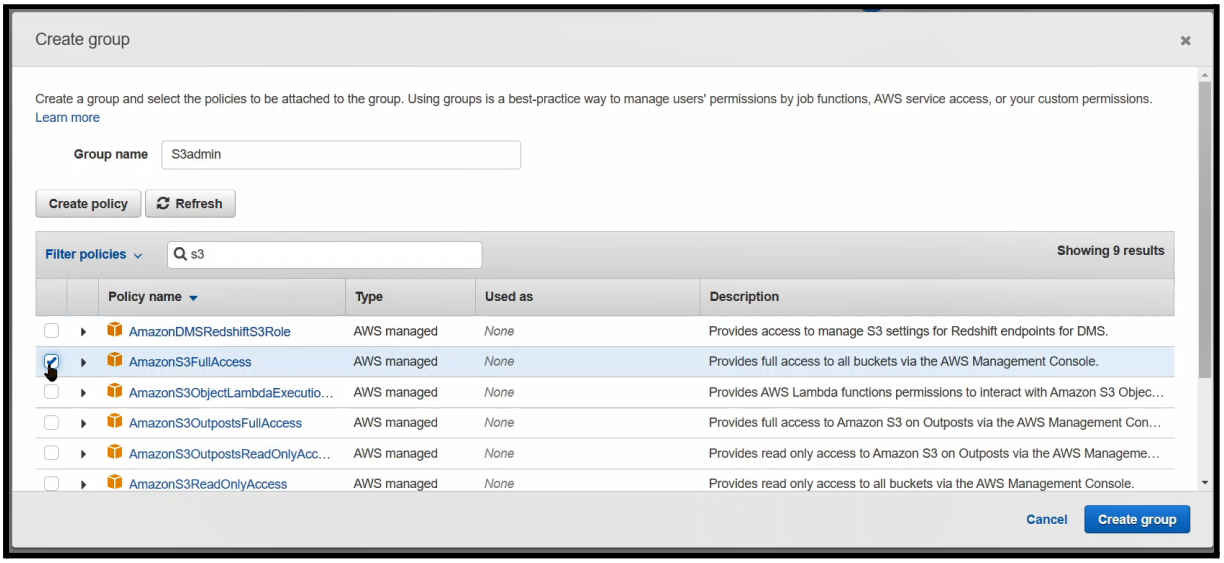
Step 11:



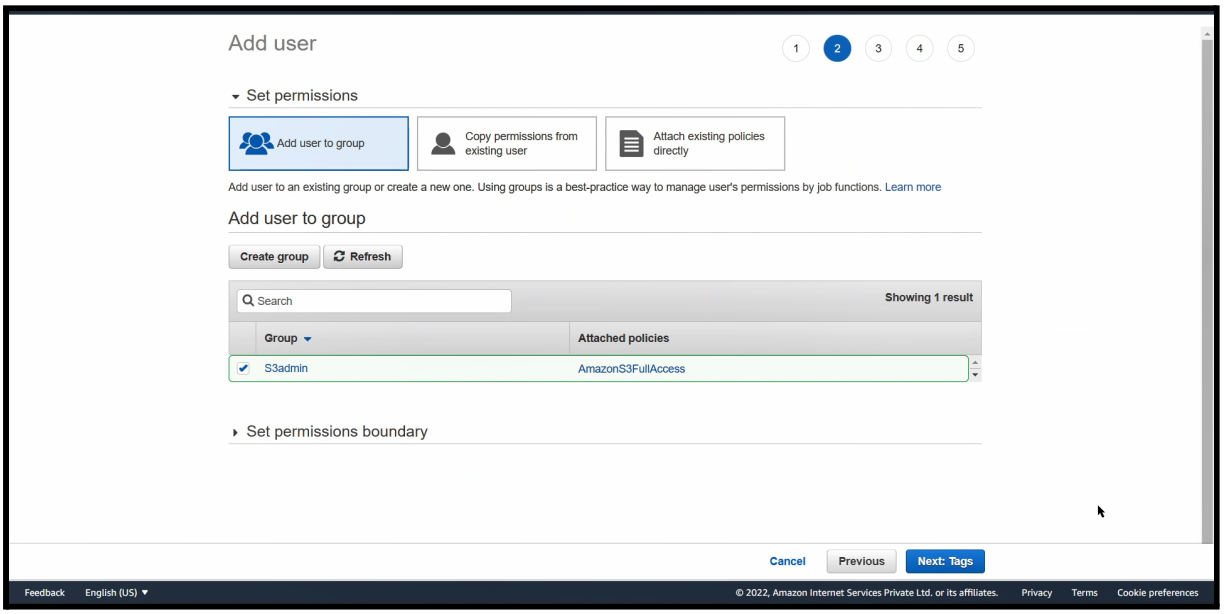
Step 12:



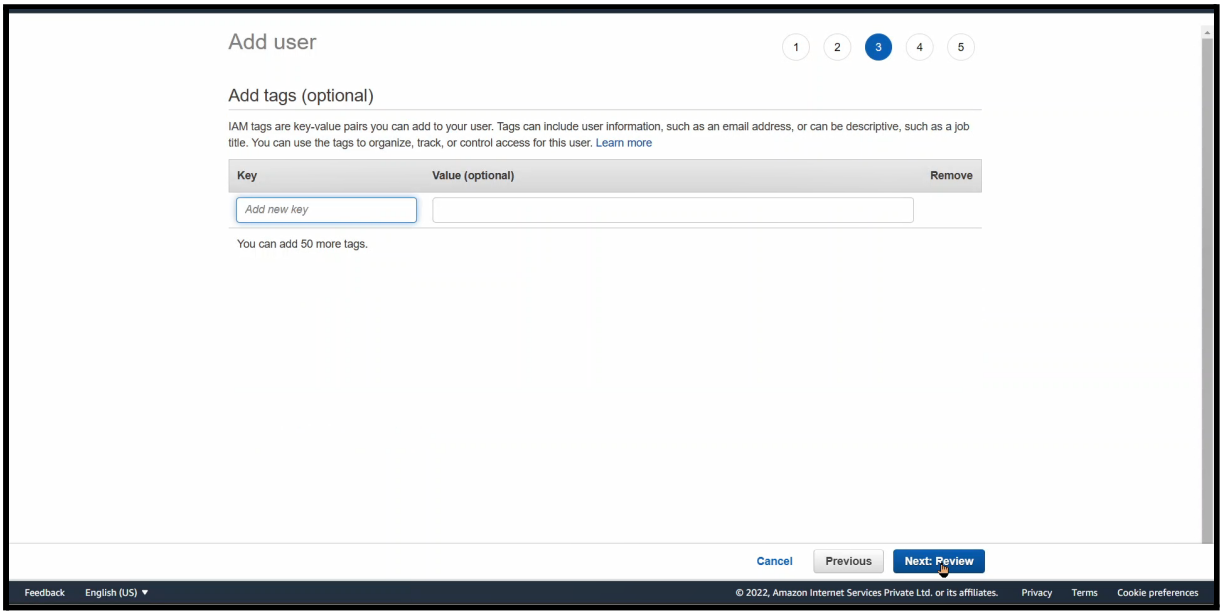
Step 13:



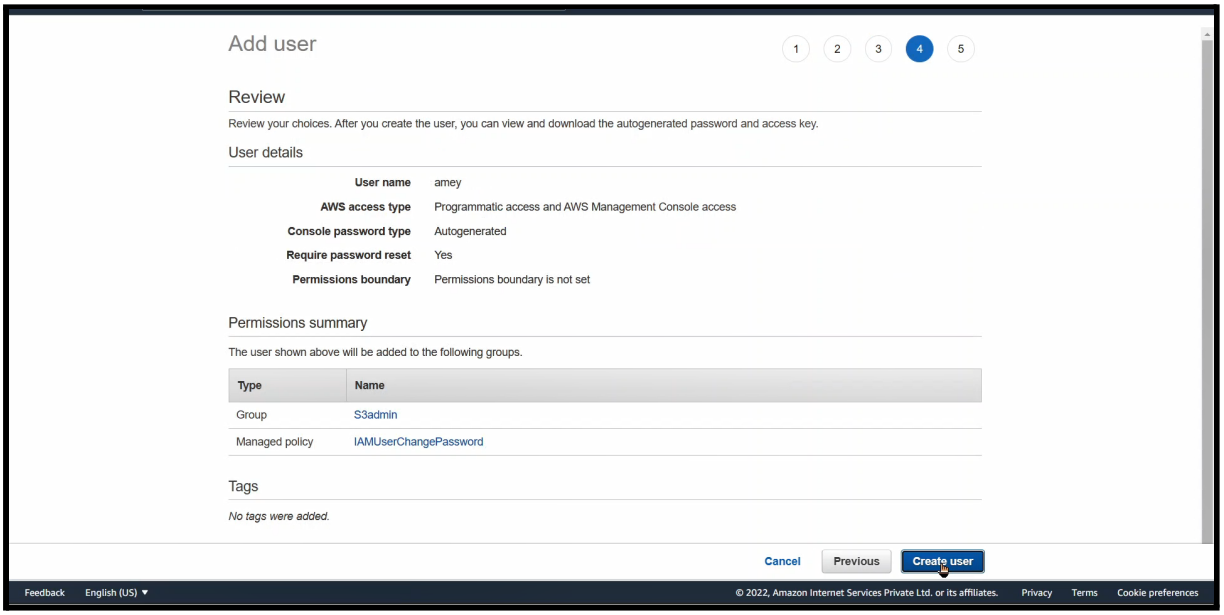
Step 14:



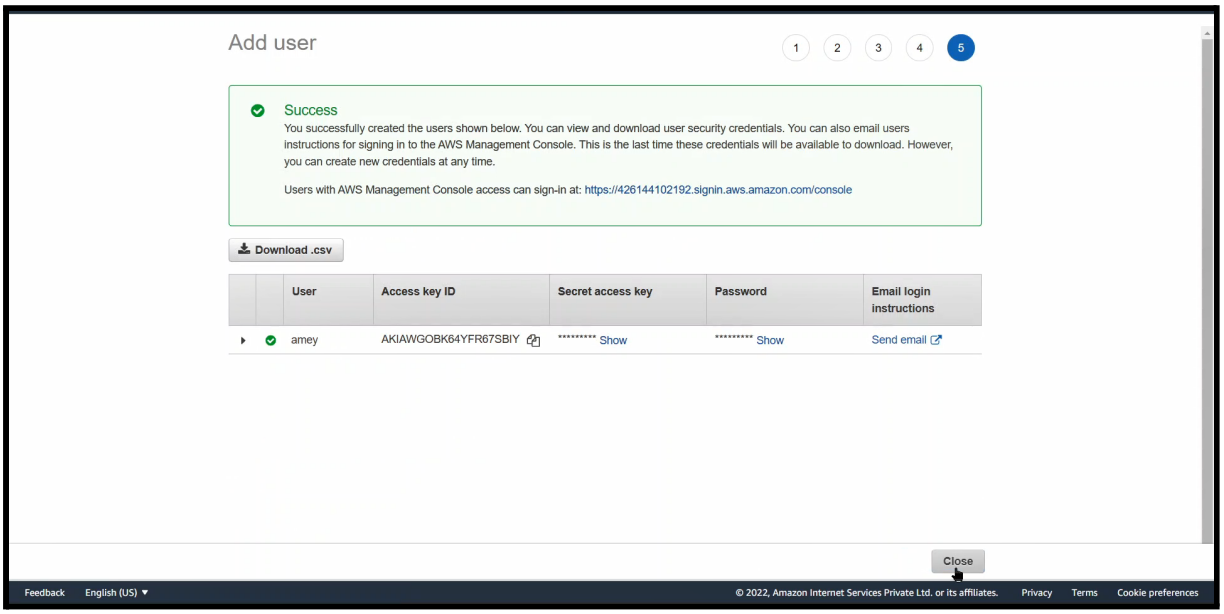
Step 15:



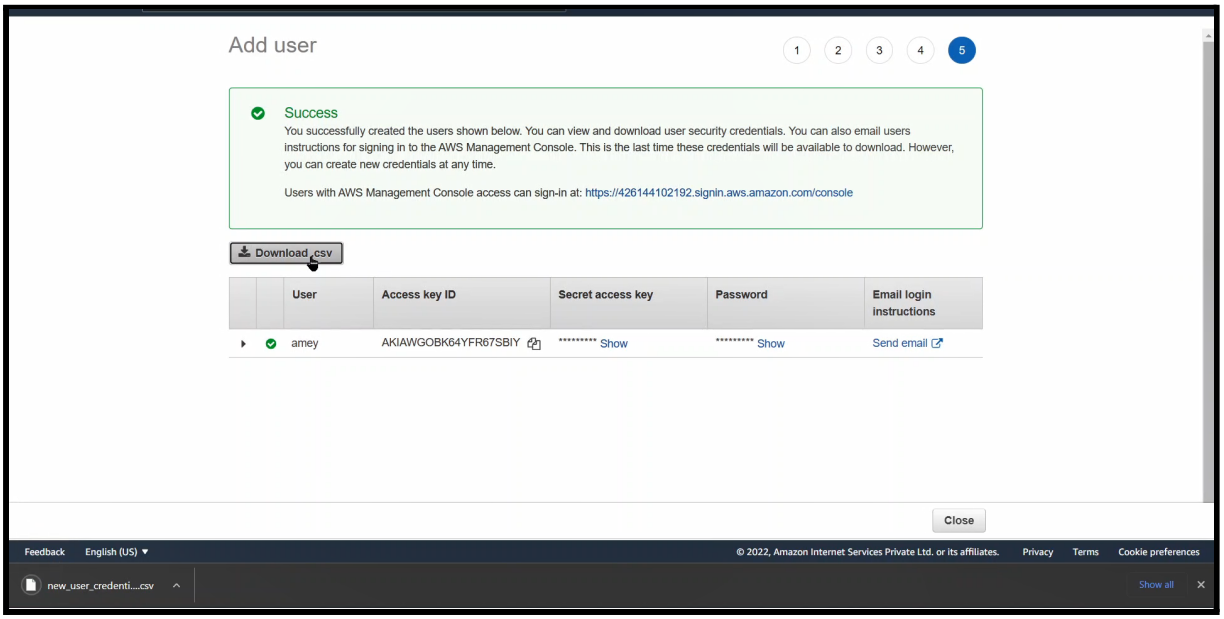
Step 16:



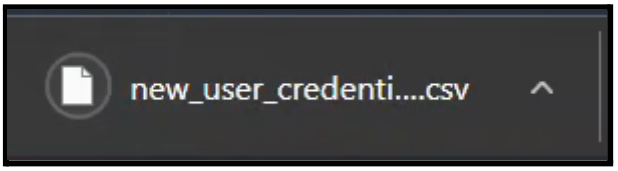
Step 17:



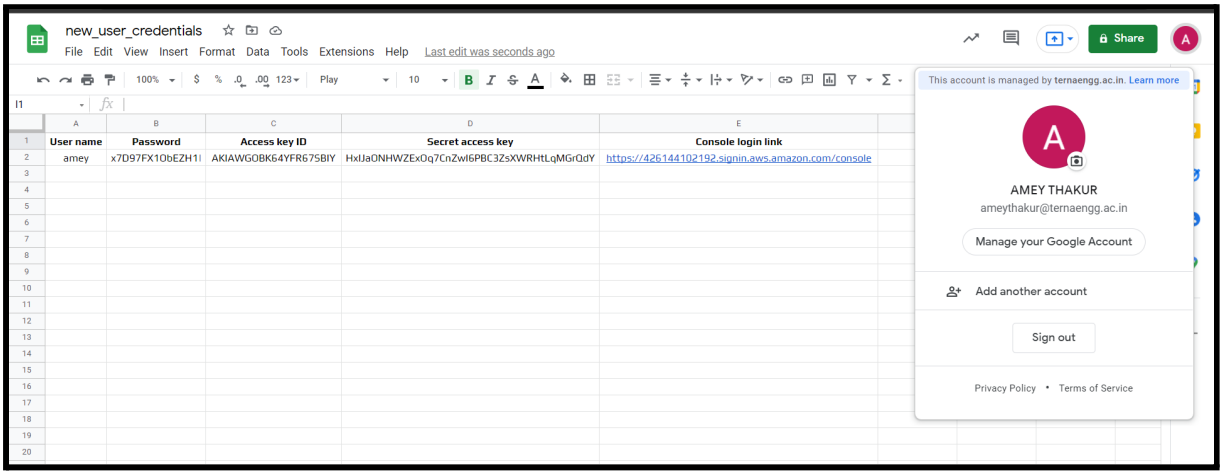
Step 18:



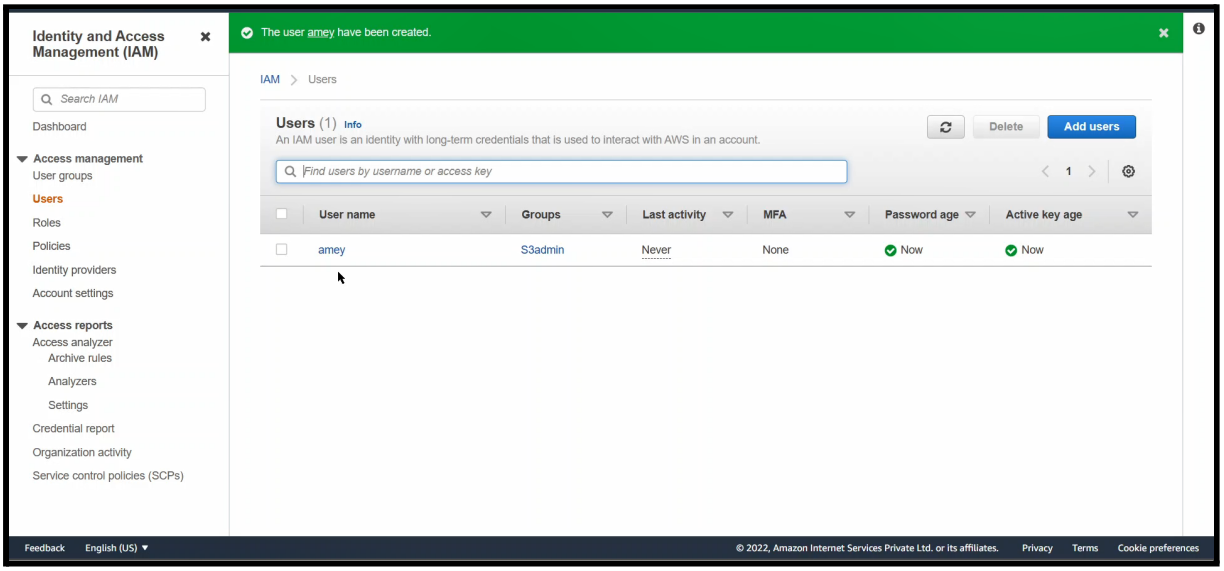
Step 19:



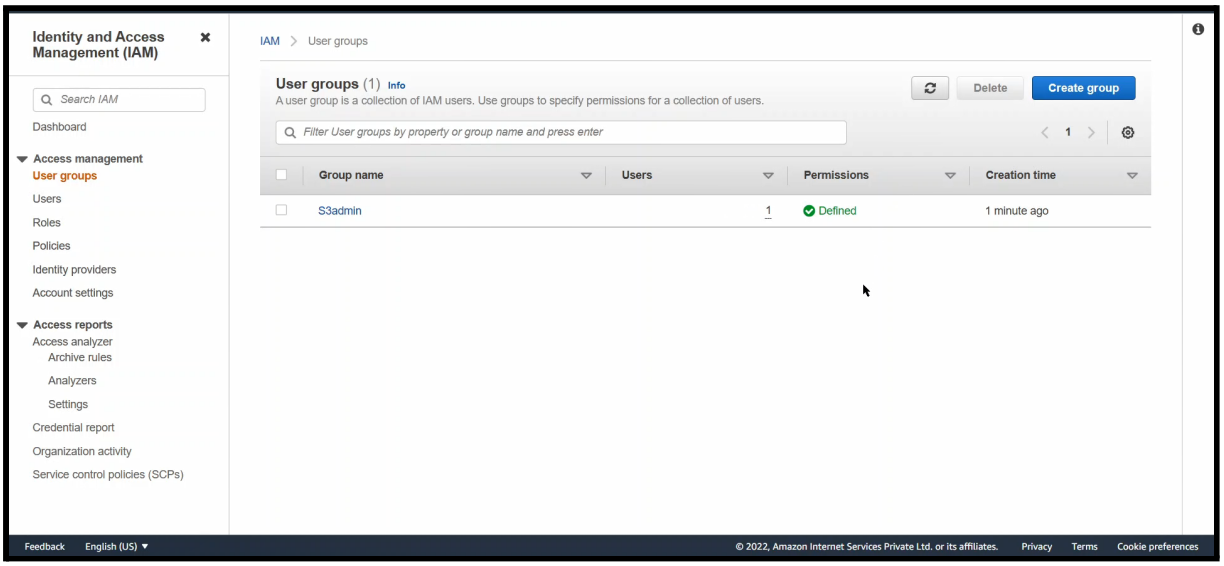
Step 20:



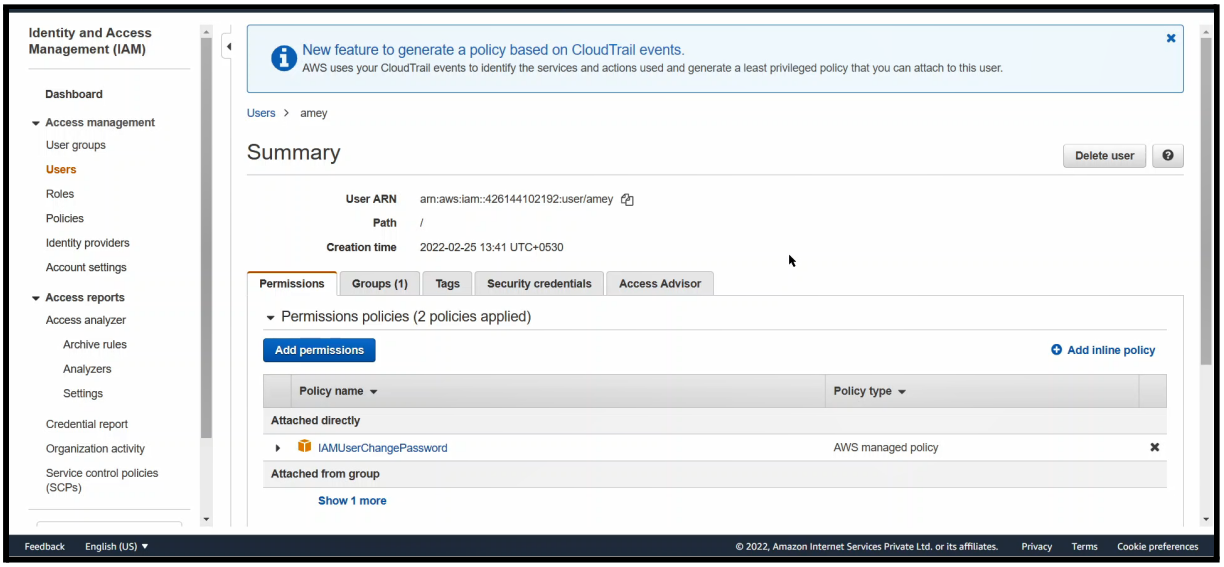
Step 21:



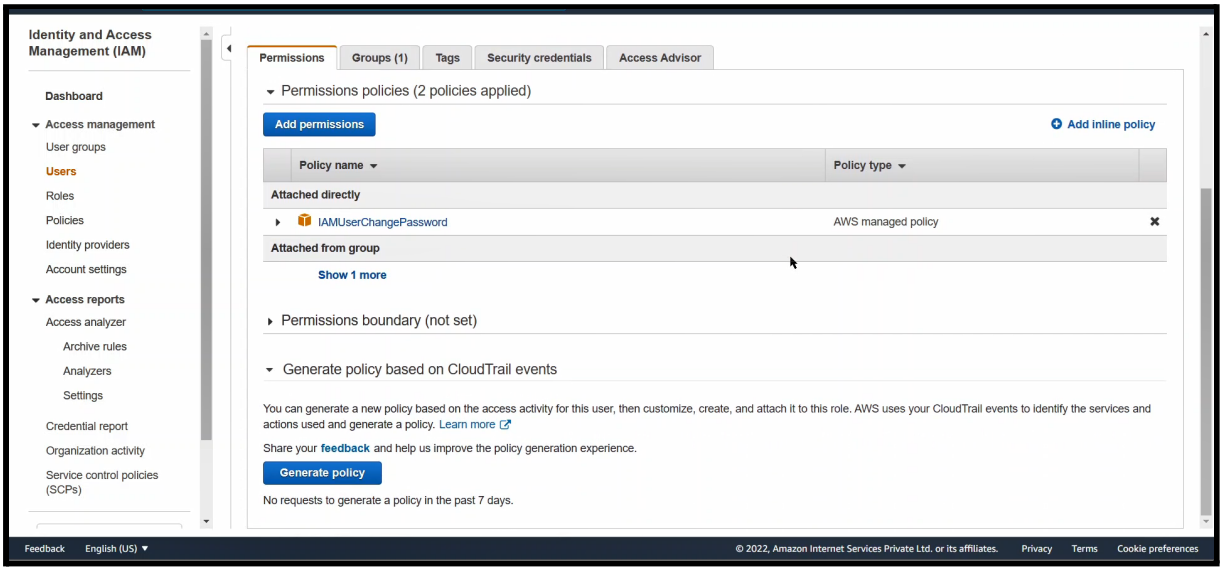
Step 22:



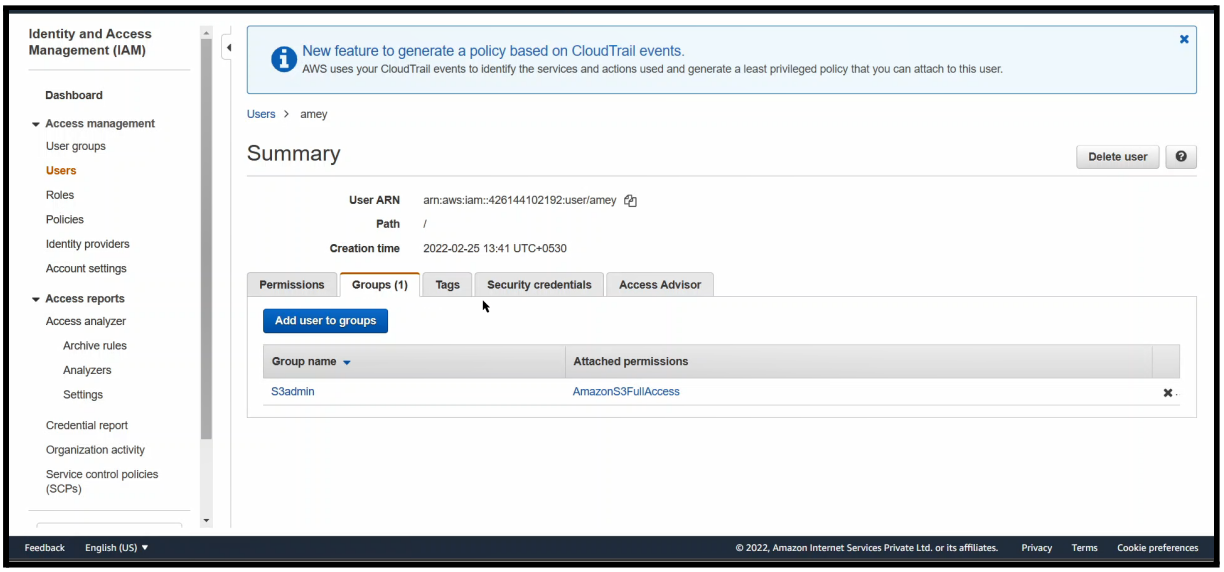
Step 23:



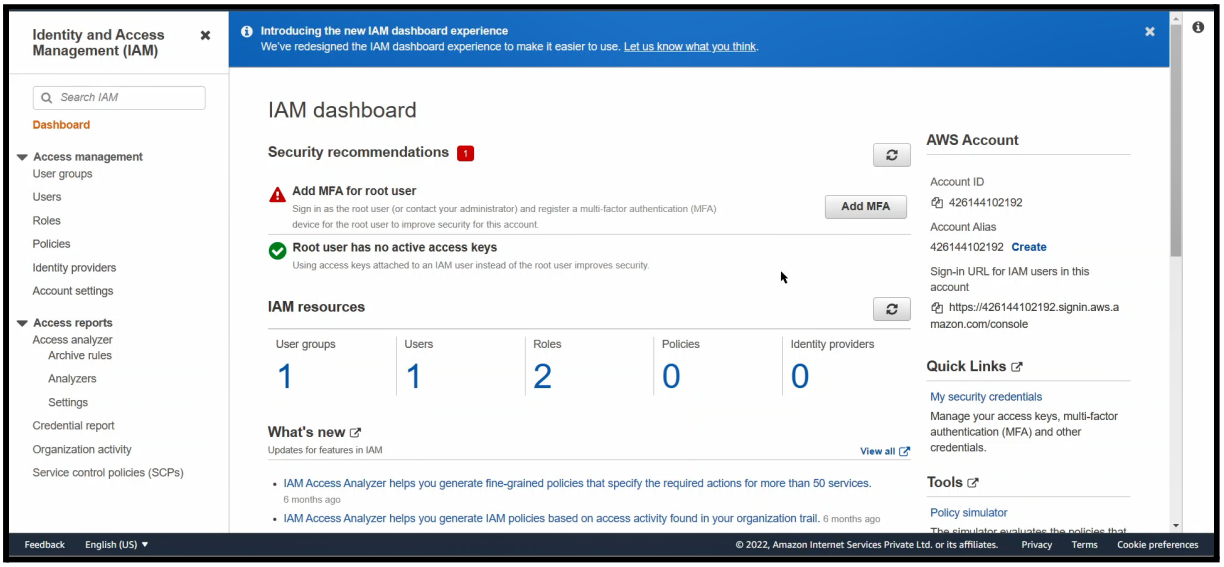
Step 24:



Step 25:



Step 26:



Q.3 Explain various parameters to measure the security of the webserver?

ANS:

1. SSH Keys:

➔ SSH, or secure shell, is an encrypted protocol used to administer and communicate with servers. When working with a server, you'll likely spend most of your time in a terminal session connected to your server through SSH. A more secure alternative to password-based logins, SSH keys use encryption to provide a secure way of logging into your server and are recommended for all users.

➔ With SSH keys, a private and public key pair is created for the purpose of authentication. The private key is kept secret and secure by the user, while the public key can be shared.

2. Firewalls

➔ A firewall is a software or hardware device that controls how services are exposed to the network, and what types of traffic are allowed in and out of a given server or servers. A properly configured firewall will ensure that only services that should be publicly available can be reached from outside your servers or network.

3. VPC Networks

➔ Virtual Private Cloud (VPC) networks are private networks for your infrastructure's resources. VPC networks provide a more secure connection among resources because the network's interfaces are inaccessible from the public internet and other VPC networks in the cloud.

4. VPNs and Private Networking

➔ Private networks are networks that are only available to certain servers or users. A VPN, or virtual private network, is a way to create secure connections between remote computers and present the connection as if it were a local private network. This provides a way to configure your services as if they were on a private network and connect remote servers over secure connections.

B.2 Conclusion:

We have understood the security of Web Server and we have successfully demonstrated how to create IAM Users using our own cloud.