

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:

The screenshot shows the AWS Management Console homepage. At the top, there's a search bar and a navigation bar with options like 'Services', 'N. Virginia', and 'AMEY THAKUR'. The main area is titled 'AWS Management Console' and features sections for 'AWS services' (with 'Recently visited services' and 'All services' options), 'Build a solution' (with options like 'Launch a virtual machine', 'Build a web app', 'Build using virtual servers', 'Register a domain', 'Connect an IoT device', and 'Start migrating to AWS'), and 'Explore AWS' (with a section for 'Amazon Redshift'). On the right side, there are promotional banners for 'New AWS Console Home' and 'Stay connected to your AWS resources on-the-go'.

Step 2:

The screenshot shows the AWS Management Console search results for 'IAM'. The search bar at the top has 'IAM' typed into it. The results are categorized into 'Services' and 'Features'. Under 'Services', there are five items: 'IAM' (Manage access to AWS resources), 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations), 'Amazon VPC IP Address Manager' (Managed IP address management service), and 'Serverless Application Repository' (Assemble, deploy, and share serverless applications within teams or publicly). Under 'Features', there are two items: 'Groups' (IAM feature) and 'Roles' (IAM feature). Each item has a small icon, a name, a star rating, and a brief description. The right side of the screen includes the same promotional banners as the previous screenshot.

Step 3:

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar menu includes options like Dashboard, Access management (User groups, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). A banner at the top says "Introducing the new IAM dashboard experience". The main area has sections for "Security recommendations" (warning about root user MFA and active access keys) and "AWS Account" (Account ID: 426144102192, Account Alias: 426144102192, Create link). Below that is the "IAM resources" section with counts: User groups (0), Users (0), Roles (2), Policies (0), and Identity providers (0). A "What's new" section lists recent updates from the IAM Access Analyzer. On the right, there are "Quick Links" (My security credentials, Policy simulator) and "Tools" (View all).

Step 4:

The screenshot shows the "Users" page under the IAM service. The sidebar menu is identical to the previous screen. The main content area shows a table with one row, indicating "No resources to display". The table has columns for User name, Groups, Last activity, MFA, Password age, and Active key age. A search bar at the top allows finding users by username or access key.

Step 5:

Add user

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*

[+ 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.

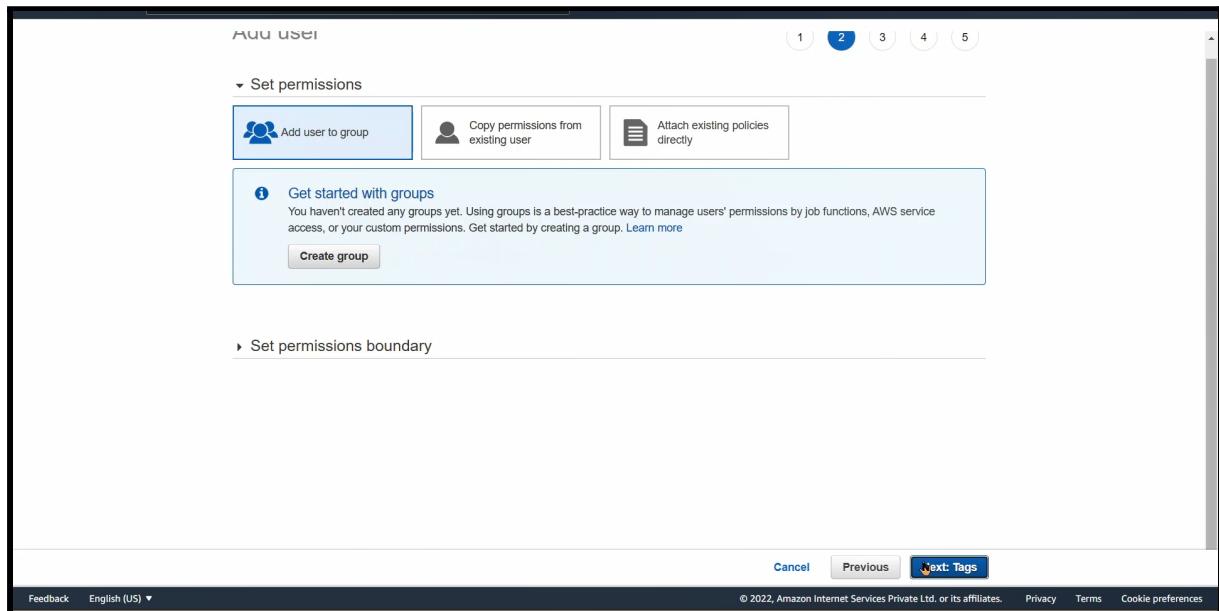
Console password* Autogenerated password
 Custom password

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.

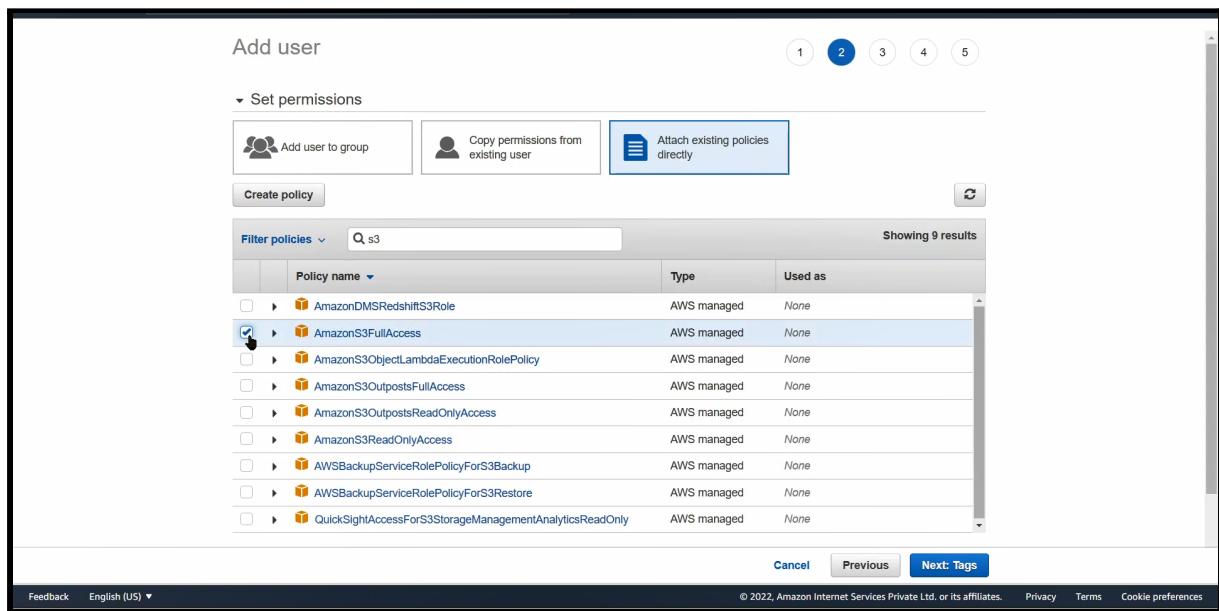
* Required Cancel [Next: Permissions](#)

Feedback English (US) ▾ © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Step 7:



Step 8:



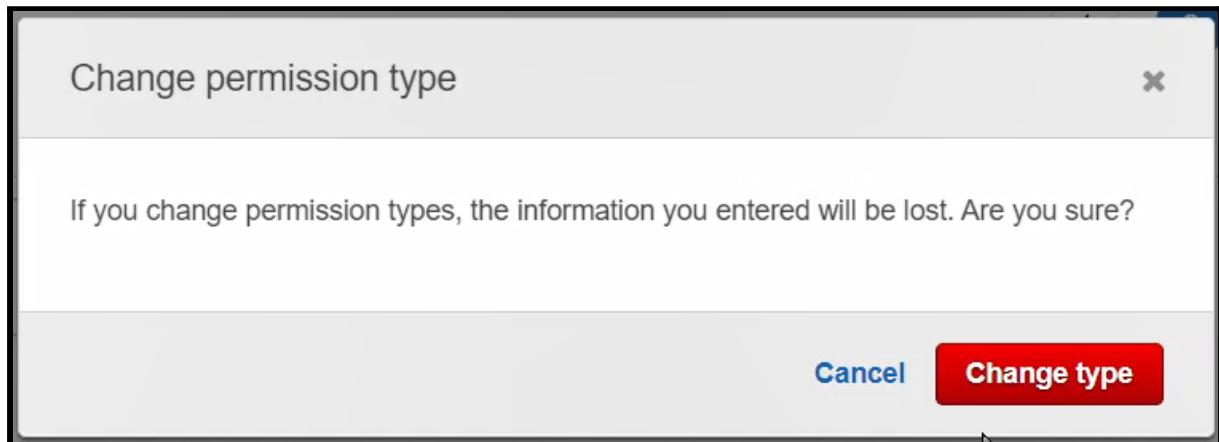
Step 9:

The screenshot shows the 'Add user' wizard at step 9, titled 'Set permissions'. It includes tabs for 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly'. A search bar filters results for 's3'. A modal window is open, showing a list of AWS managed policies with 'AmazonS3FullAccess' selected. The modal has 'Cancel' and 'Next: Tags' buttons.

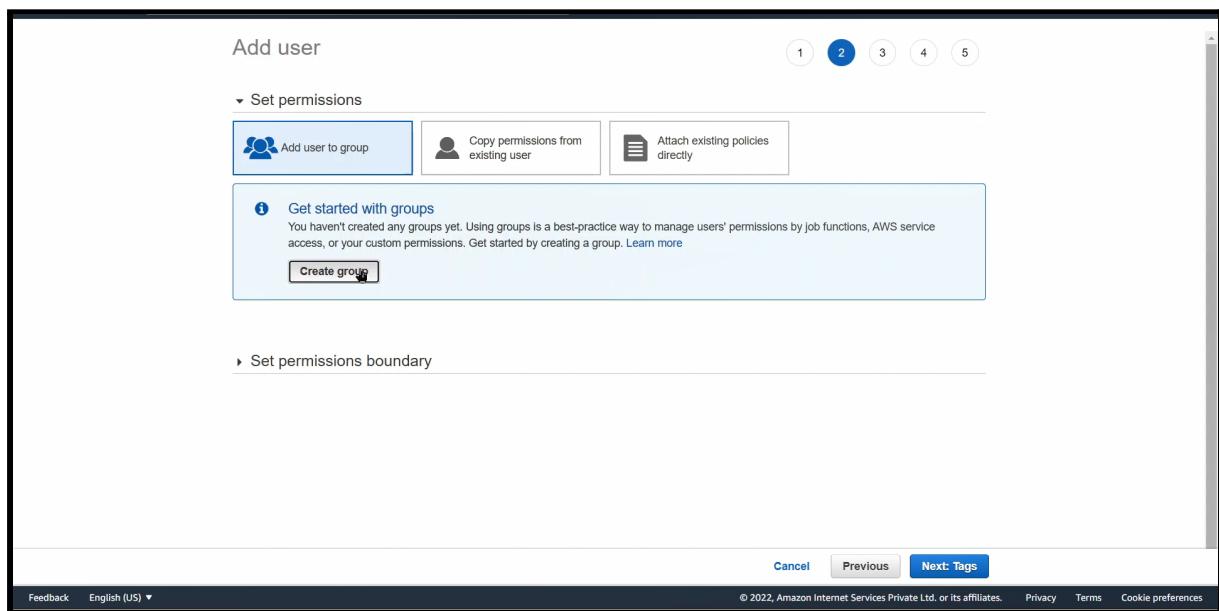
Step 10:

The screenshot shows the 'Add user' wizard at step 10, with a modal dialog titled 'Change permission type'. It asks if changing permission types will lose information and contains 'Cancel' and 'Change type' buttons. The background shows the 'Set permissions' section with 'AmazonS3FullAccess' selected.

Step 11:



Step 12:



Step 13:

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions.

Learn more

Group name: S3admin

Create policy Refresh

Filter policies ▾

Policy name	Type	Used as	Description
AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via the AWS Management Console.
AmazonS3ObjectLambdaExecutionRole	AWS managed	None	Provides AWS Lambda functions permissions to interact with Amazon S3 Object...
AmazonS3OutpostsFullAccess	AWS managed	None	Provides full access to Amazon S3 on Outposts via the AWS Management Con...
AmazonS3OutpostsReadOnlyAccess	AWS managed	None	Provides read only access to Amazon S3 on Outposts via the AWS Manageme...
AmazonS3ReadOnlyAccess	AWS managed	None	Provides read only access to all buckets via the AWS Management Console.

Showing 9 results

Cancel Create group

Step 14:

Add user

1 2 3 4 5

Set permissions

Add user to group Copy permissions from existing user Attach existing policies directly

Add user to group

Create group Refresh

Search Group Attached policies

Group	Attached policies
S3admin	AmazonS3FullAccess

Showing 1 result

Set permissions boundary

Cancel Previous Next: Tags

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Step 15:

The screenshot shows the 'Add tags (optional)' step of the AWS IAM 'Add user' wizard. It includes a table for adding tags, a note about the limit of 50 tags, and navigation buttons for 'Cancel', 'Previous', and 'Next: Review'.

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	<input type="button" value="Remove"/>

You can add 50 more tags.

1 2 3 4 5

Cancel Previous Next: Review

Feedback English (US) ▾ © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Step 16:

The screenshot shows the 'Review' step of the AWS IAM 'Add user' wizard, displaying the user details and permissions summary.

Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	amey
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	S3admin
Managed policy	IAMUserChangePassword

Tags

No tags were added.

1 2 3 4 5

Cancel Previous Create user

Feedback English (US) ▾ © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Step 17:

The screenshot shows the 'Add user' page in the AWS Management Console. A success message box is displayed, stating: 'Success: You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.' Below the message, there is a 'Download .csv' button. A table lists the user details:

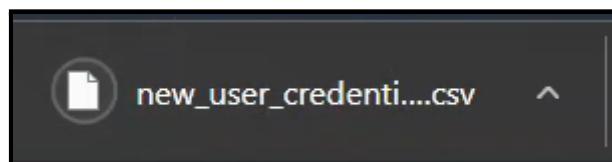
	User	Access key ID	Secret access key	Password	Email login instructions
▶	amey	AKIAWGOBK64YFR67SBIY	***** Show	***** Show	Send email

At the bottom of the page, there are links for Feedback, English (US), © 2022, Amazon Internet Services Private Ltd. or its affiliates., Privacy, Terms, and Cookie preferences.

Step 18:

The screenshot shows the 'Add user' page in the AWS Management Console, identical to Step 17. A success message box is displayed. Below the message, there is a 'Download .csv' button. A download progress bar is visible at the bottom of the screen, indicating that a file named 'new_user_credential....csv' is being downloaded. The file name is partially cut off. At the bottom of the page, there are links for Feedback, English (US), © 2022, Amazon Internet Services Private Ltd. or its affiliates., Privacy, Terms, and Cookie preferences.

Step 19:



Step 20:

A	B	C	D	E
User name	Password	Access key ID	Secret access key	Console login link
amey	x7097FX10bEZH1I	AKIAWGOBK64YFR675BY	HxJJaONHWZEExoq7CnZw6PBC3zsXWRHtLqMGrQdY	https://426144102192.signin.aws.amazon.com/console
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Step 21:

The user amey have been created.

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.

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	amey	S3admin	Never	None	Now	Now

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Step 22:

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation menu is expanded to show 'Access management' under 'User groups'. The main content area displays a table titled 'User groups (1) Info'. The table has columns for Group name, Users, Permissions, and Creation time. One row is listed: 'S3admin' with 'Defined' permissions and created '1 minute ago'. A search bar at the top allows filtering by property or group name.

Step 23:

The screenshot shows the AWS IAM User Summary page for a user named 'amey'. The left sidebar shows the 'Users' section is selected. The main summary table includes fields for User ARN (arn:aws:iam::426144102192:user/amey), Path (/), and Creation time (2022-02-25 13:41 UTC+0530). Below the summary table, the 'Permissions' tab is active, showing two policies applied: 'IAMUserChangePassword' (AWS managed policy). Other tabs include 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor'. A modal window at the top right informs the user about a new feature to generate a policy based on CloudTrail events.

Step 24:

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). The main content area is titled 'Permissions' and shows 'Permissions policies (2 policies applied)'. It includes tabs for 'Add permissions', 'Add inline policy', 'Policy name', and 'Policy type'. A table lists two policies: 'IAMUserChangePassword' (AWS managed policy). Other sections include 'Attached from group', 'Show 1 more', 'Permissions boundary (not set)', and 'Generate policy based on CloudTrail events' (with a note about generating a least privileged policy). A 'Generate policy' button is present. The bottom of the screen shows standard AWS footer links: © 2022, Amazon Internet Services Private Ltd. or its affiliates., Privacy, Terms, and Cookie preferences.

Step 25:

The screenshot shows the AWS IAM 'Users' section. The left sidebar is identical to Step 24. The main content area is titled 'Summary' for the user 'amey'. It displays the User ARN (arn:aws:iam::426144102192:user/amey), Path (/), and Creation time (2022-02-25 13:41 UTC+0530). Below this is a table for 'Attached permissions' under the 'Groups (1)' tab. The table shows one group, 'S3admin', which has 'AmazonS3FullAccess' attached. Other tabs include 'Permissions', 'Tags', 'Security credentials', and 'Access Advisor'. A 'Delete user' button is visible in the top right. A blue info box at the top right of the summary area says: 'New feature to generate a policy based on CloudTrail events. AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.' The bottom of the screen shows standard AWS footer links: © 2022, Amazon Internet Services Private Ltd. or its affiliates., Privacy, Terms, and Cookie preferences.

Step 26:

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there's a navigation sidebar with options like 'Dashboard', 'Access management', 'Access reports', and 'Credential report'. The main area displays 'Security recommendations' with a warning about 'Add MFA for root user' and a note about 'Root user has no active access keys'. Below this is a summary of 'IAM resources': 1 User group, 1 User, 2 Roles, 0 Policies, and 0 Identity providers. A 'What's new' section lists two items from 'IAM Access Analyzer'. To the right, there's an 'AWS Account' section with details like Account ID (426144102192), Account Alias (426144102192), and a sign-in URL. There are also 'Quick Links' and 'Tools' sections.

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.