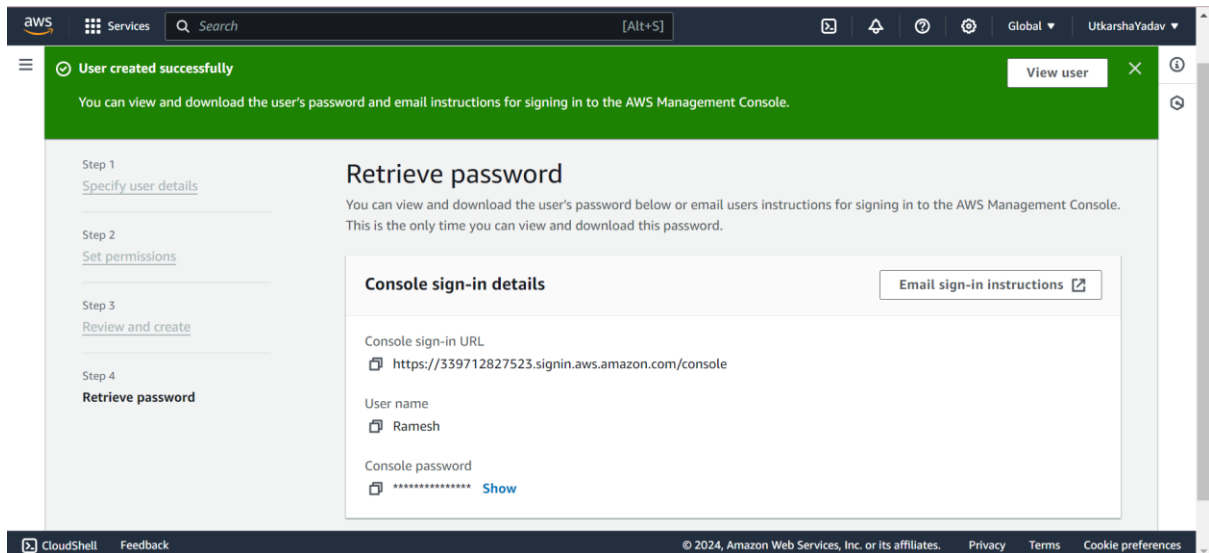


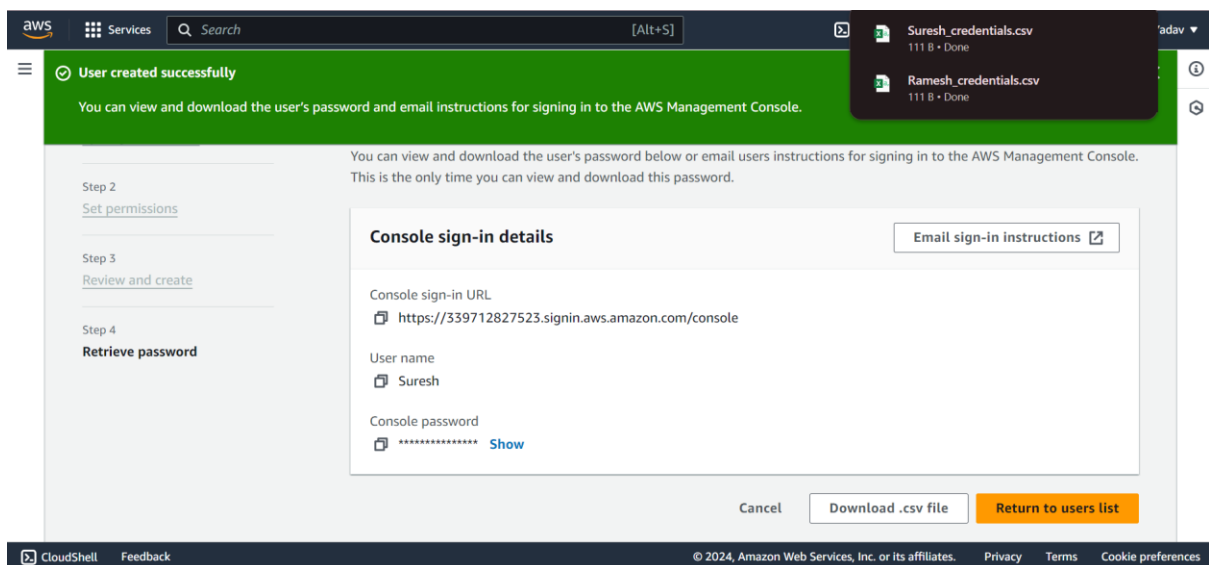
Assignment 7 -Bucket Policy

Go IAM and create to users Ramesh (S3fullaccess) and Suresh (S3Readonlyaccess) and download id password csv file.

Ramesh is created



Suresh is created



Go to S3 and create bucket with ACLs enabled and versioning enabled

The screenshot shows the AWS S3 Buckets console. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and user information. Below the navigation bar, the 'Amazon S3' breadcrumb is followed by 'Buckets'. A banner for 'Account snapshot' is visible. The 'General purpose buckets' tab is selected, showing a list of buckets. One bucket, 'bucketpolicydemocr', is listed with the following details:

Name	AWS Region	IAM Access Analyzer	Creation date
bucketpolicydemocr	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	September 29, 2024, 23:53:56 (UTC+05:30)

Go to bucket configure - permission then go the Bucket policy and click EDIT and go to POLICY GENERATOR

The screenshot shows the 'Bucket policy' configuration page for the bucket 'bucketpolicydemocr'. The page has an 'Edit' button and a 'Delete' button. A blue information box states: 'Public access is blocked because Block Public Access settings are turned on for this bucket. To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access.' Below this, the policy field is empty and displays 'No policy to display.' with a 'Copy' button.

Policy Generator- Select the type of Policy and add users arn whom you want to give access



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal :339712827523:user/Suresh

Use a comma to separate multiple values.

AWS Service

Add bucket arn with/*

Amazon S3

☐ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 3 Action(s) Selected ☐ All Actions ('*')

Amazon Resource Name (ARN) :s3:::bucketpolicydemocrrr/*

ARN should follow the following format: `arn:aws:s3:::{BucketName}/{KeyName}`.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

[Add Statement](#)

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
<ul style="list-style-type: none">arn:aws:iam::339712827523:user/Ramesharn:aws:iam::339712827523:user/Suresh	Allow	<ul style="list-style-type: none">s3:DeleteObjects3:GetObjects3:PutObject	arn:aws:s3:::bucketpolicydemocrrr/*	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#)

[Start Over](#)

Copy this code and paste in bucket policy

