Experiment – 8

Name : Ronak Surve
Subject : CC Lab
Roll No : 64
Date : 16/03/2023

Learning Objective:	To study and Implement Security as a Service on AWS/Azure
Learning Outcome:	Students will be able to understand the Security practices available in public cloud platforms and to demonstrate various Threat detection,
Course Outcome:	CSL605.4
Program Outcome:	1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems. 2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences. 3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations. 4. Conduct investigations of complex problems: Use research based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions. 5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
Bloom's Taxonomy Level:	Apply
Theory:	Security as a Service (SECaaS) refers to the delivery of security solutions and services to organizations as a cloud-based service. This approach allows organizations to outsource theirsecurity needs to third-party providers who specialize in security and can offer more robust and scalable solutions. Here are some examples of SECaaS solutions in terms of IAM, Data Protection, DataDetection, and Infrastructure Protection:

Identity and Access Management (IAM):

IAM is a crucial aspect of security as it ensures that only authorized users can access an organization's resources. Some SECaaS solutions that fall under IAM include:

Single Sign-On (SSO): SSO allows users to log in to multiple applications with a single set ofcredentials, reducing the risk of password fatigue and making it easier for IT administrators tomanage access.

Multi-factor Authentication (MFA): MFA adds an extra layer of security to the authentication process, requiring users to provide additional verification beyond a password. This can includea fingerprint scan, a code sent to a mobile device, or a security token.

Example: Okta is a popular SECaaS provider that offers a range of IAM solutions, includingSSO and MFA.

Data Protection:

Data protection is essential for safeguarding sensitive information and preventing databreaches. Some SECaaS solutions that fall under data protection include:

Encryption: Encryption is the process of converting data into a code that can only be deciphered by authorized parties. This helps to ensure that even if data is intercepted or stolen,it cannot be read by unauthorized users.

Data Loss Prevention (DLP): DLP solutions help organizations prevent accidental orintentional data leaks by monitoring and controlling data access and usage.

Example: Sophos is a SECaaS provider that offers a range of data protection solutions,including encryption and DLP.

Data Detection:

Data detection solutions help organizations identify and respond to security threats in real-time. Some SECaaS solutions that fall under data detection include:

Security Information and Event Management (SIEM): SIEM solutions collect and analyzesecurity data from across an organization's network to identify and respond to security incidents.

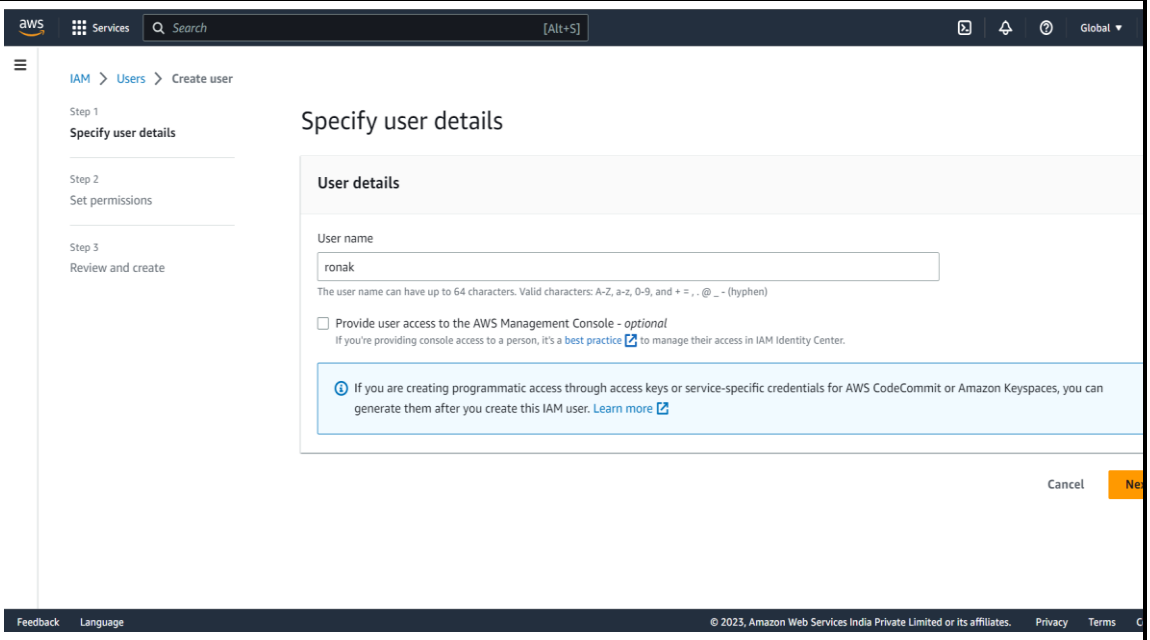
	Intrusion Detection and Prevention Systems (IDPS): IDPS solutions monitor network trafficfor signs of malicious activity and can automatically block or quarantine potential threats. Example: IBM Security is a SECaaS provider that offers a range of data detection solutions,including SIEM and IDPS. Infrastructure Protection: Infrastructure protection solutions help organizations protect their IT infrastructure from cyberthreats. Some SECaaS solutions that fall under infrastructure protection include: Firewall: A firewall is a network security system that monitors and controls incoming andoutgoing network traffic based on predetermined security rules. Distributed Denial of Service (DDoS) Protection: DDoS protection solutions help organizations protect their websites and other online services from DDoS attacks, which canoverload and disrupt online services. Example: Amazon Web Services (AWS) is a SECaaS provider that offers a range of infrastructure protection solutions, including firewall and DDoS protection.
Procedure	To know the Security practices available in public cloud platforms and to demonstrate various Threat detection, Data protection and Infrastructure protection services in AWS and Azure.
Steps	1. Sign in to the AWS Management Console and navigate to the IAM service. 2. In the IAM dashboard, select "Users" from the left-hand menu and click the "Add user"button. 3. Enter a name for the user in the "User name" field. You can also add a description ifdesired. 4. Under "Select AWS access type", choose between "Programmatic access", "AWSManagement Console access", or both. 5. If you choose "Programmatic access", select the checkbox for "Attach existing policiesdirectly". Then, search and select the policies that you want to attach to the user. Policies define the permissions that the user has to access AWS services and resources. 6. If you choose "AWS Management Console access", select the checkbox for "Requirepassword reset" to force the user to create a new password when they first sign in. 7. Click "Next: Tags" to add tags to the user (optional). 8. Click "Next: Review" to review the details of the user.

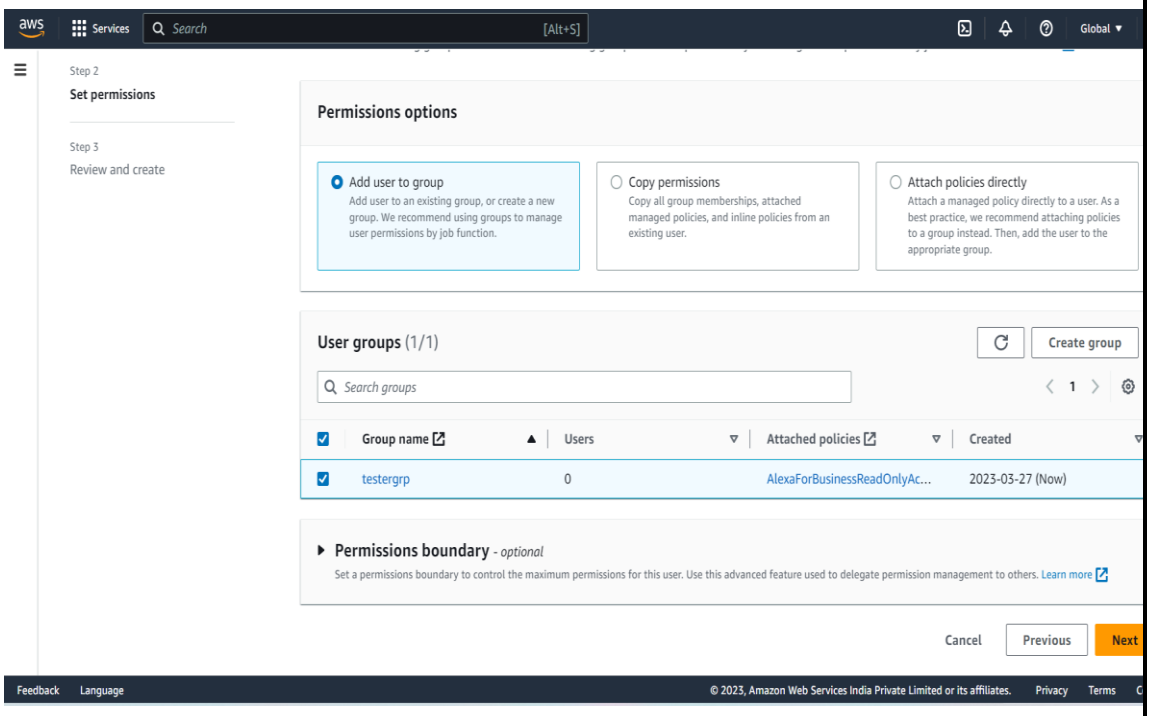
9. Review the information and click "Create user" to create the IAM user.

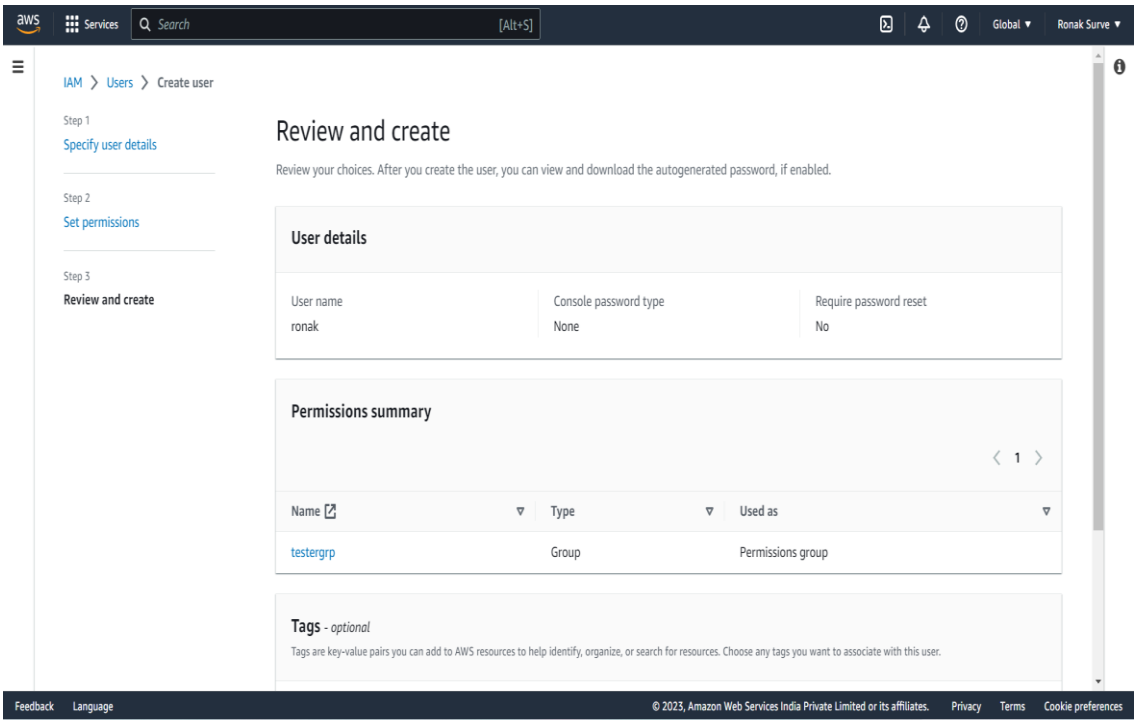
10. After the user is created, you will see a success message with the user's Access key IDand Secret access key. Make sure to download or copy these credentials, as they will not be shown again.

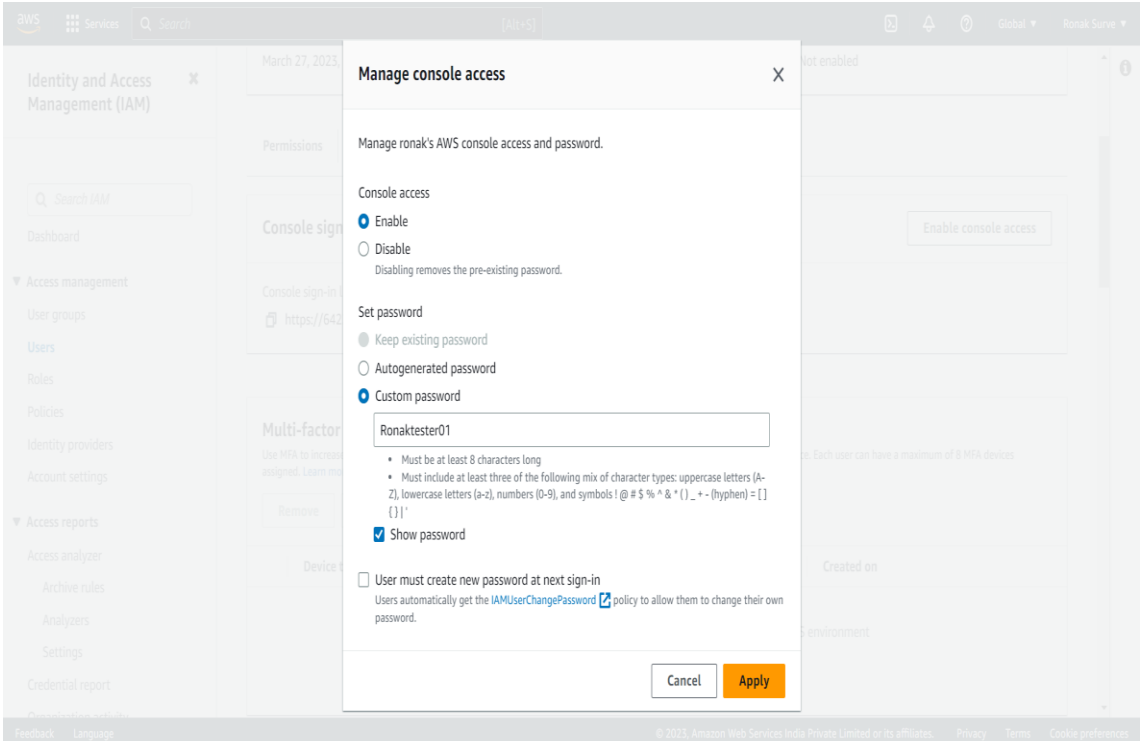
11. You can also choose to send an email invitation to the user to provide them with a linkto set their own password and activate their account

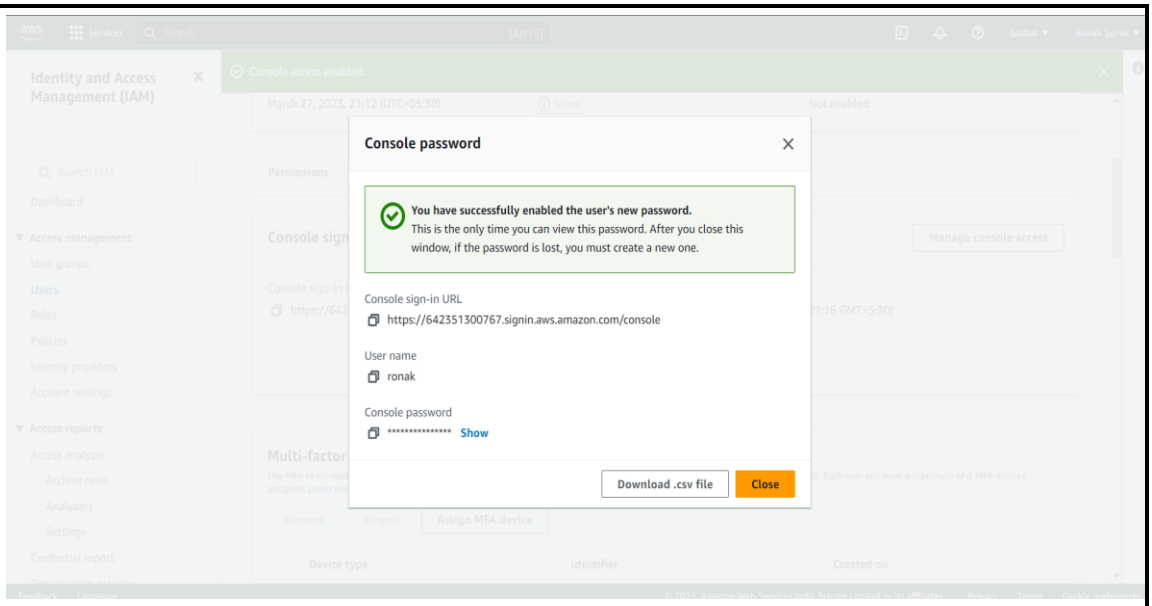
Outcome :

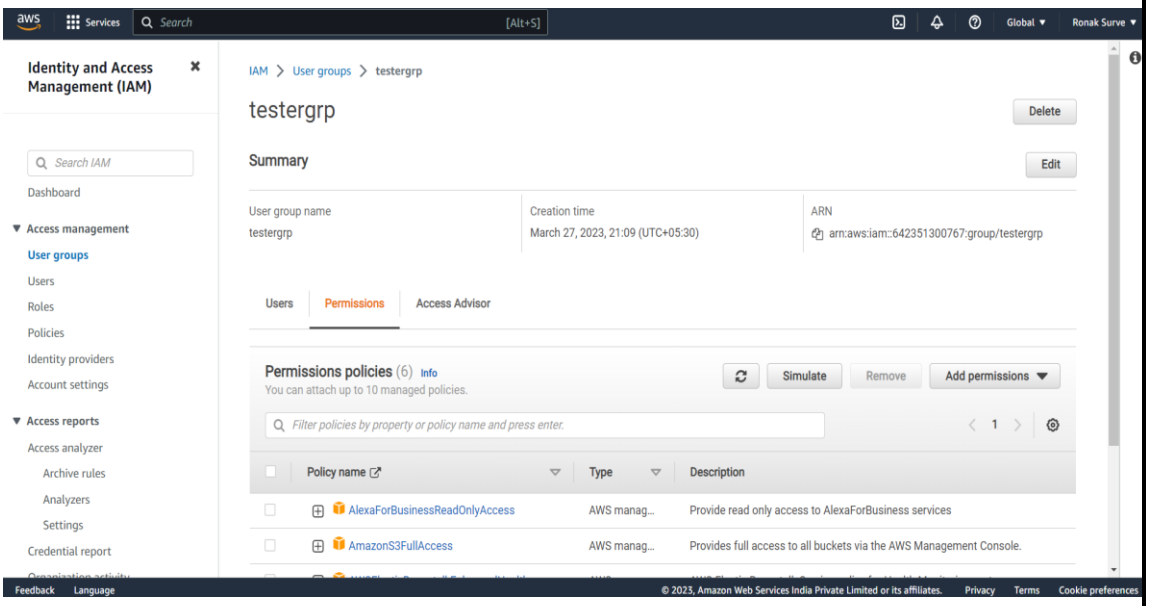


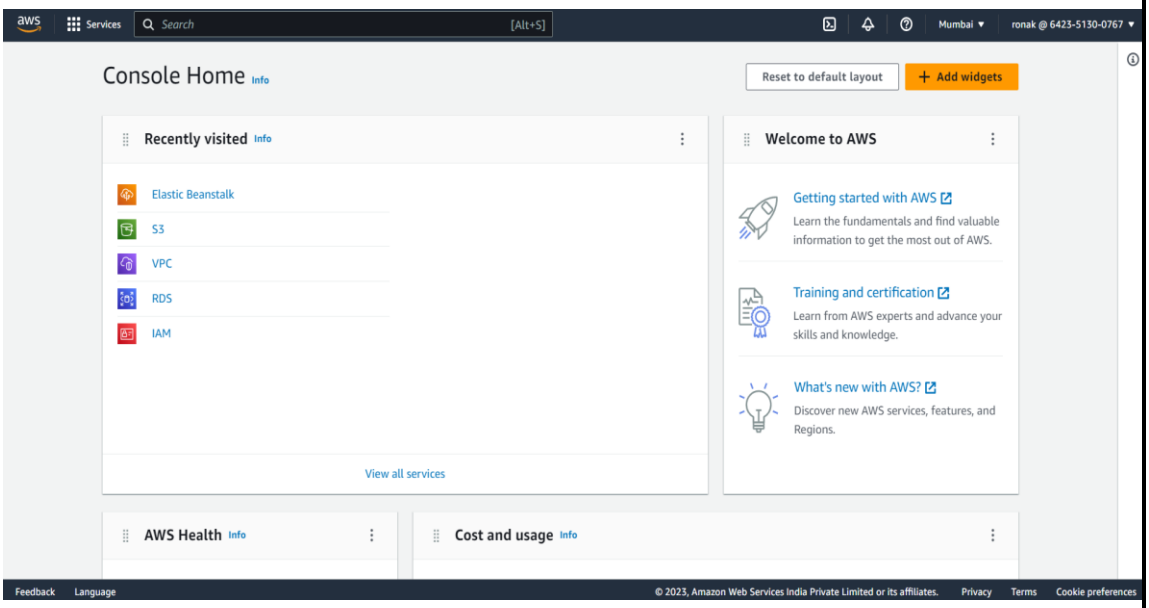


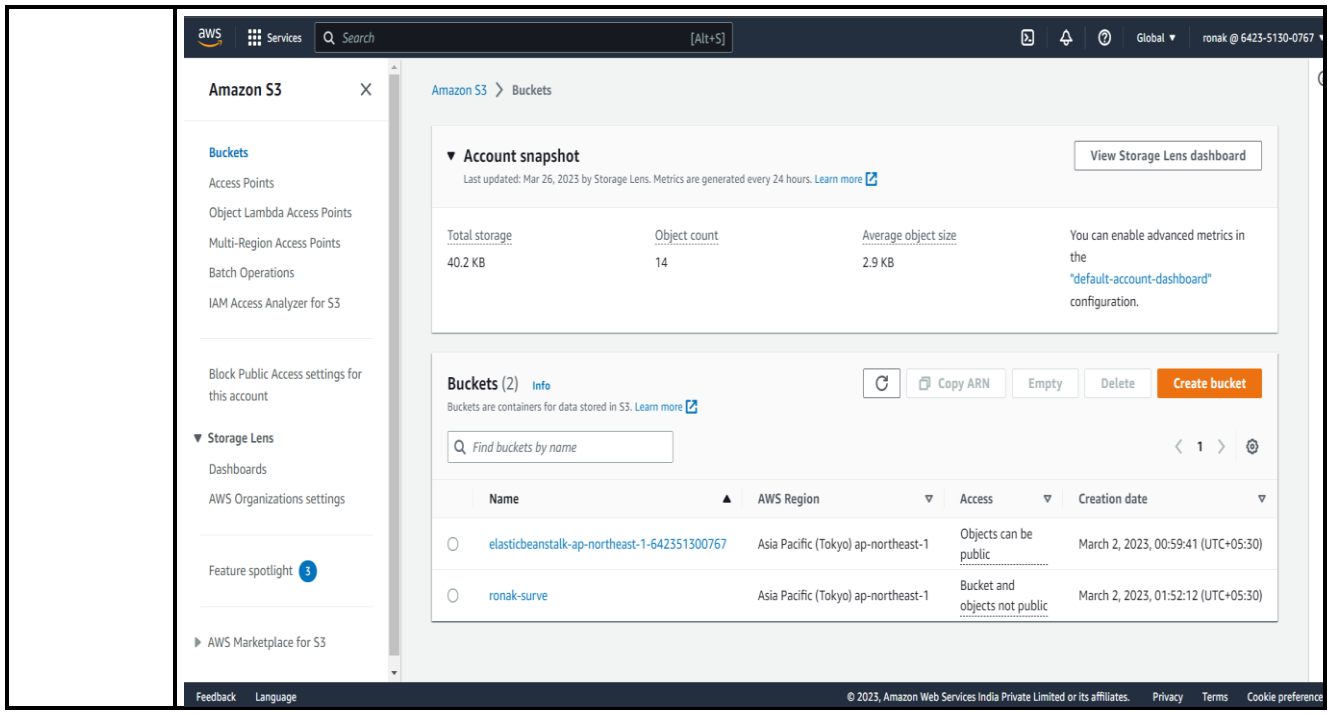

Services
Search
[Alt+S]
Global
Ronak Surve
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
ronak
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
testergrp
Group
Permissions group
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.
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences


Manage console access
Manage ronak's AWS console access and password.
Console access
Enable
Disable
Disabling removes the pre-existing password.
Set password
Keep existing password
Autogenerated password
Custom password
Ronaktester01
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
User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
Cancel
Apply


Console password
You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.
Console sign-in URL
https://642351300767.signin.aws.amazon.com/console
User name
ronak
Console password
Show
Download .csv file
Close


Identity and Access Management (IAM)
IAM > User groups > testergrp
testergrp
Delete
Summary
Edit
User group name
testergrp
Creation time
March 27, 2023, 21:09 (UTC+05:30)
ARN
arn:aws:iam::642351300767:group/testergrp
Users
Permissions
Access Advisor
Permissions policies (6) 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
AlexaForBusinessReadOnlyAccess
AWS manag...
Provide read only access to AlexaForBusiness services
AmazonS3FullAccess
AWS manag...
Provides full access to all buckets via the AWS Management Console.


Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
Elastic Beanstalk
S3
VPC
RDS
IAM
View all services
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
Learn from AWS experts and advance your skills and knowledge.
What's new with AWS?
Discover new AWS services, features, and Regions.
AWS Health Info
Cost and usage Info


aws
Services
Search
[Alt+S]
Global
ronak @ 6423-5130-0767
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
Last updated: Mar 26, 2023 by Storage Lens. Metrics are generated every 24 hours. Learn more
View Storage Lens dashboard
Total storage
40.2 KB
Object count
14
Average object size
2.9 KB
You can enable advanced metrics in the "default-account-dashboard" configuration.
Buckets (2) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
Access
Creation date
elasticbeanstalk-ap-northeast-1-642351300767
Asia Pacific (Tokyo) ap-northeast-1
Objects can be public
March 2, 2023, 00:59:41 (UTC+05:30)
ronak-surve
Asia Pacific (Tokyo) ap-northeast-1
Bucket and objects not public
March 2, 2023, 01:52:12 (UTC+05:30)
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preference

Conclusion :	Successfully created IAM user using AWS.
References:	https://docs.aws.amazon.com/iam/index.html

Rubrics for Assessment

Timely Submission	Submitted after 2 weeks 0	Submitted after deadline 1	On time Submission 2
Understanding	Student is confused about the concept 0	Students has justifiably understood the concept 2	Students is very clear about the concepts 3
Performance	Students has not performed the Experiment 0	Student has performed with help 2	Student has independently performed the experiment 3
Development	Students struggle to provide security. 0	Student can write steps the requirement stated 1	Student can write exceptional steps with his own ideas 2