Name- Aniket Devidas Tayde

Subject- Cloud Computing

Colledge– DY. Patil International University

Task(3)- CLOUD SECURITY IMPLEMENTATION

IMPLEMENT IAM POLICIES, SECURE STORAGE,
AND DATA ENCRYPTION ON A CLOUD PLATFORM.
DELIVERABLE: CONFIGURED SECURITY
POLICIES AND A REPORT DETAILING THE SETUP.

- ## Objective-

To implement and demonstrate security best practices in the cloud using AWS services, including identity and access management, secure data storage, and encryption.

- **Key Components:**

1. IAM:

- Create users/roles
- Apply least privilege policies
- Enable MFA

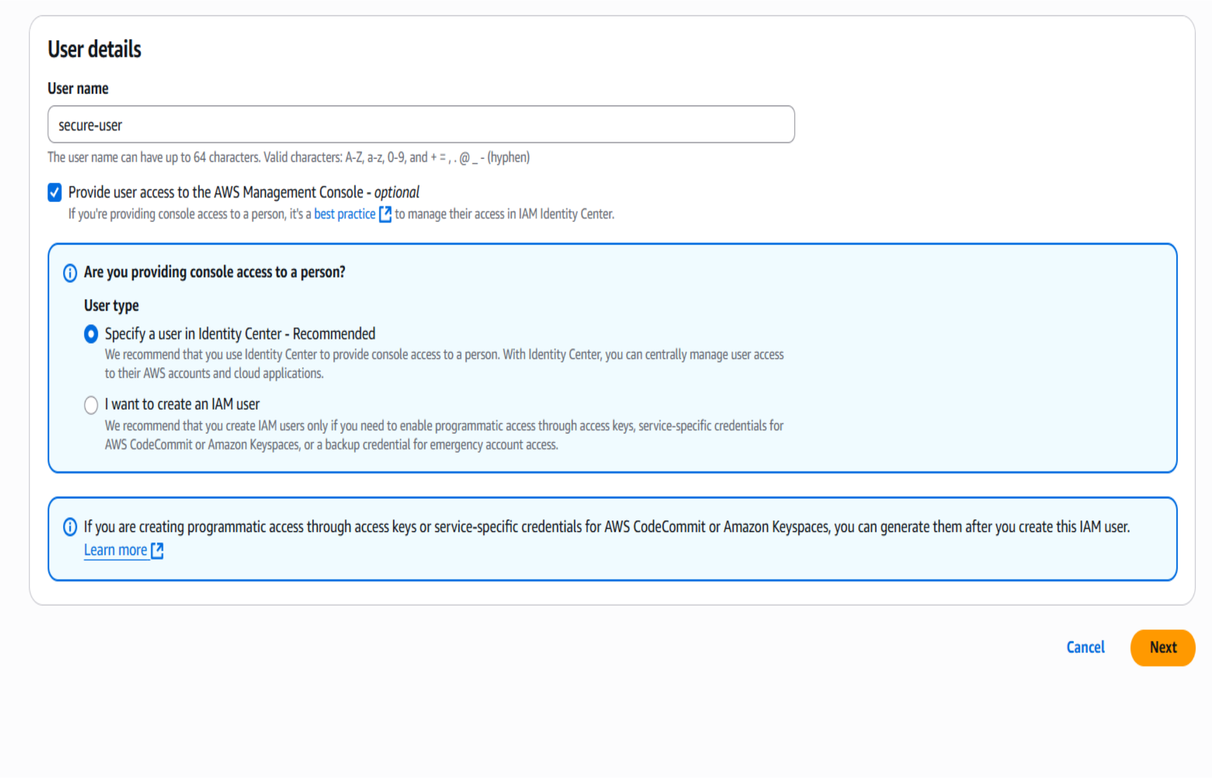
2. Secure Storage (S3):

- Make buckets private
- Use bucket policies/ACLs
- Enable SSE-S3 encryption

3. Encryption:

- Encrypt data at rest (S3)
- Use HTTPS for in-transit data

- **Screenshots After Task Submission-**



User details

User name

secure-user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

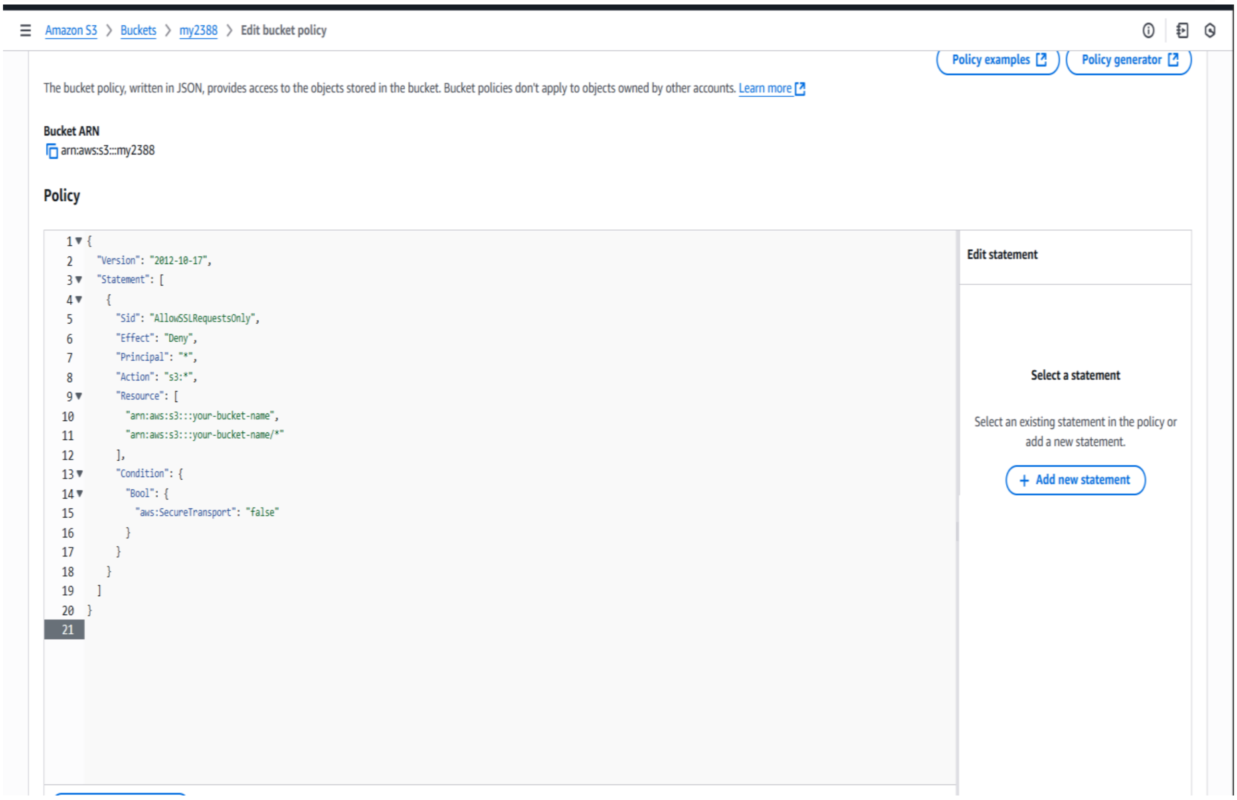
● Specify a user in Identity Center - Recommended

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.

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



The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN

arn:aws:s3:::my2388

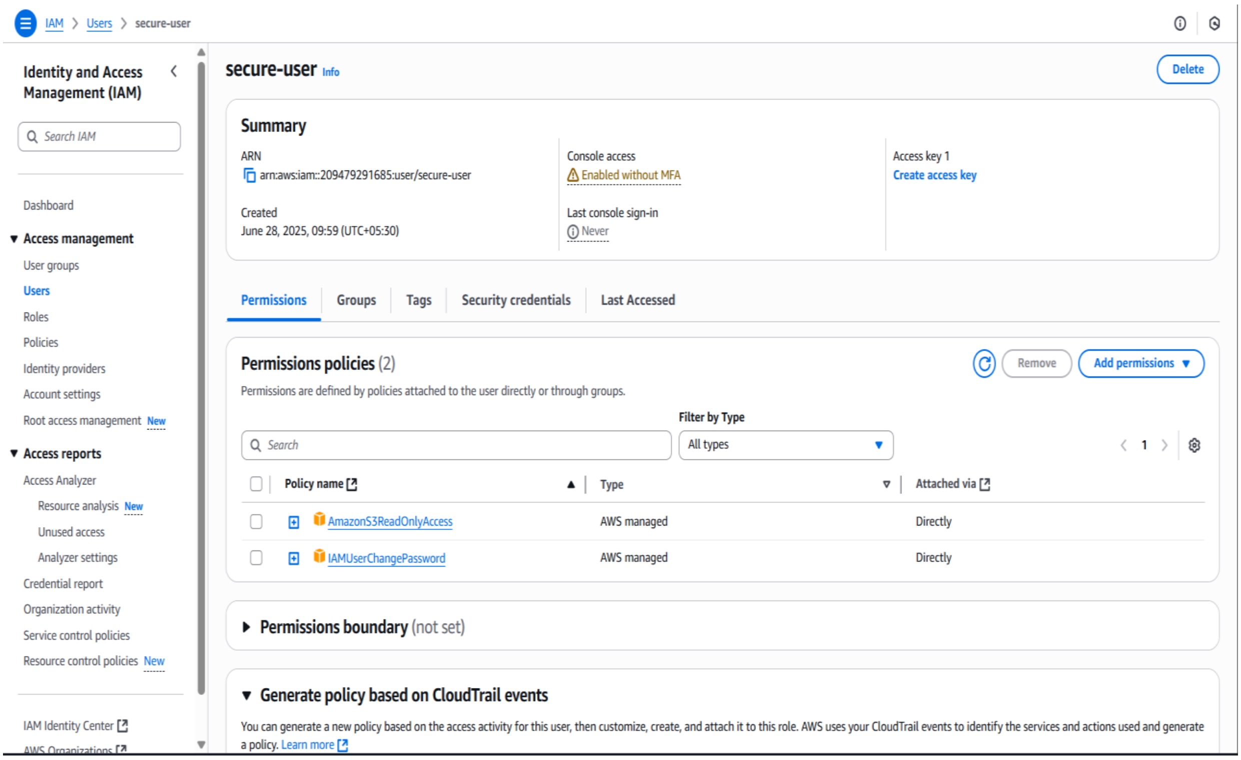
Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::your-bucket-name",
        "arn:aws:s3:::your-bucket-name/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.



secure-user Info

Summary

ARN
arn:aws:iam::209479291685:user/secure-user

Created
June 28, 2025, 09:59 (UTC+05:30)

Console access
⚠ Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

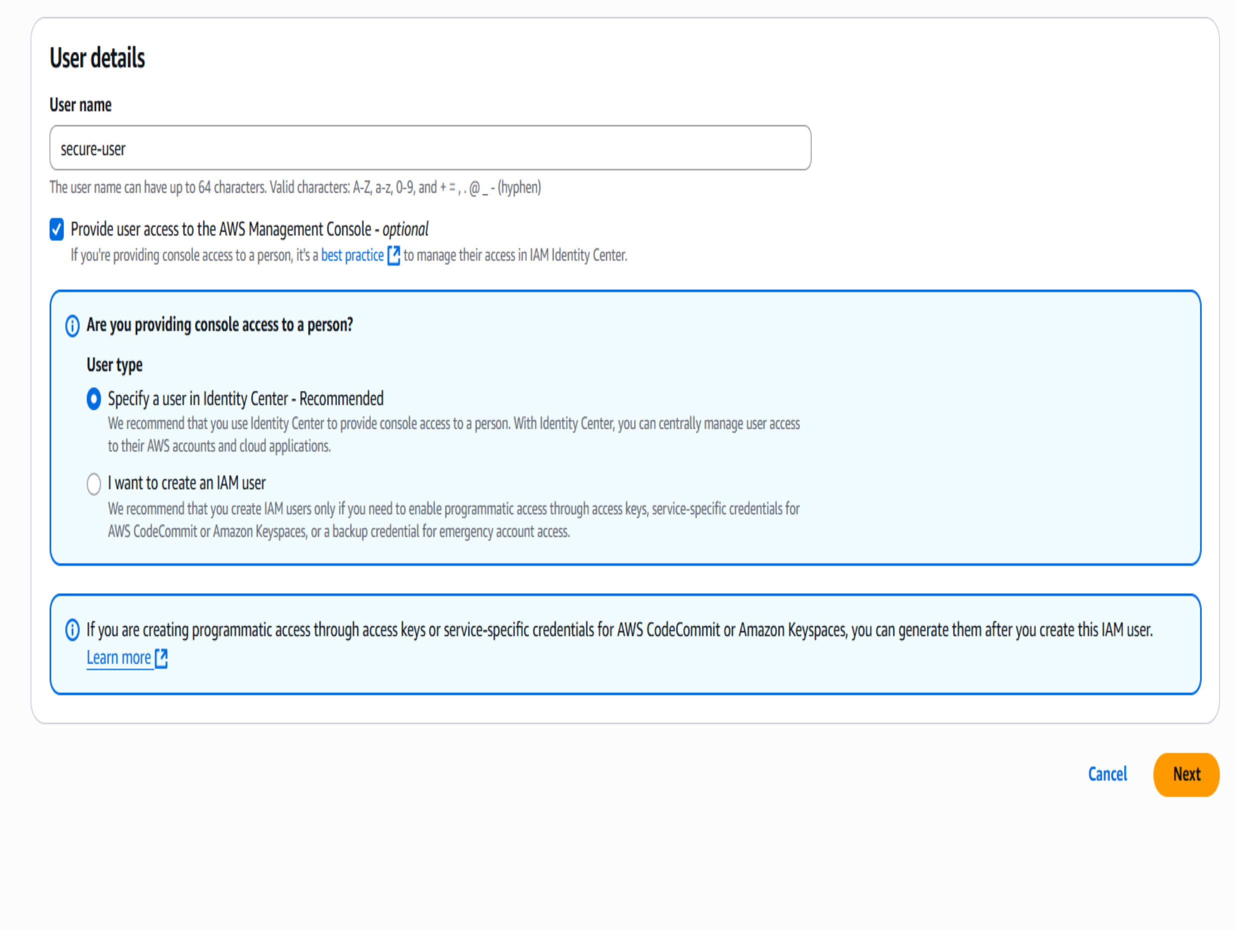
Filter by Type: All types

□	Policy name	Type	Attached via
□	AmazonS3ReadOnlyAccess	AWS managed	Directly
□	IAMUserChangePassword	AWS managed	Directly

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more



User details

User name

secure-user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

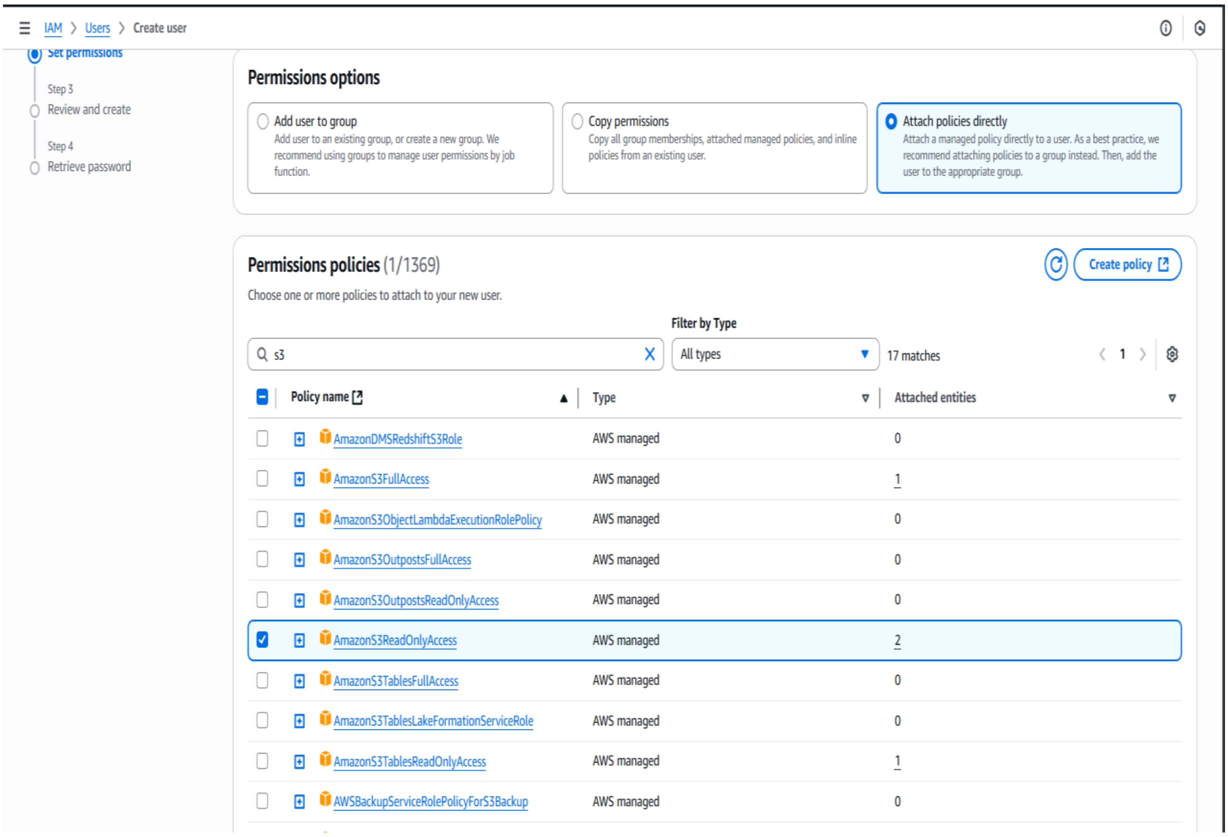
● Specify a user in Identity Center - Recommended

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.

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



● Set permissions

Step 3
○ Review and create

Step 4
○ Retrieve password

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.

Permissions policies (1/1369)

Choose one or more policies to attach to your new user.

Filter by Type

s3 | All types | 17 matches

☐	Policy name	Type	Attached entities
☐	AmazonDMSRedshiftS3Role	AWS managed	0
☐	AmazonS3FullAccess	AWS managed	1
☐	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
☐	AmazonS3OutpostsFullAccess	AWS managed	0
☐	AmazonS3OutpostsReadOnlyAccess	AWS managed	0
☑	AmazonS3ReadOnlyAccess	AWS managed	2
☐	AmazonS3TablesFullAccess	AWS managed	0
☐	AmazonS3TablesLakeFormationServiceRole	AWS managed	0
☐	AmazonS3TablesReadOnlyAccess	AWS managed	1
☐	AWSBackupServiceRolePolicyForS3Backup	AWS managed	0