

Practical-3 Identity Access Management.

Write-up:

Users and Groups

In cloud environments, Users and Groups are essential components in managing and organizing access control.

- Users represent individual identities that require access to resources. They can be employees, contractors, or applications that need permissions to operate in the system. Each user is given a unique identity within the organization, allowing for customized access and permissions.
- Groups are collections of users with similar access needs. Rather than assigning permissions to each user individually, administrators can create groups and assign specific permissions to the group, simplifying management. For example, a "Developers" group might be given permission to deploy applications, while a "Support" group could be restricted to viewing logs and system statuses. Together, Users and Groups allow administrators to streamline access control policies, manage permissions more efficiently, and ensure that only authorized individuals have access to specific resources.

IAM (Identity and Access Management)

IAM (Identity and Access Management) is a critical framework in cloud security that enables organizations to define, manage, and control user access to resources. IAM provides a centralized way to create and manage identities, roles, and policies that specify what level of access each user or application has to resources

The key functions of IAM include:

- Authentication: Verifying that users are who they claim to be, typically via passwords, multi-factor authentication, or single sign-on (SSO).
- Authorization: Granting the correct level of access to authenticated users based on their roles and policies.
- User Management: Creating, modifying, and deleting user accounts as employees join, leave, or change roles within the organization.
- Policy Management: Defining permissions and rules that control what resources users

or groups can access and what actions they can perform.

IAM plays a crucial role in maintaining security and compliance, helping organizations avoid unauthorized access and safeguard sensitive data.

Role of IAM

The Role of IAM extends beyond just assigning access; it serves as the foundation of security and governance within an organization. IAM's responsibilities are essential for:

1. **Enhancing Security:** By ensuring that only authorized individuals or systems can access specific resources, IAM reduces the risk of unauthorized access or data breaches.
2. **Maintaining Compliance:** Many industries require strict access control for regulatory compliance. IAM provides the necessary tools to meet these standards, often with detailed logging and auditing capabilities.
3. **Improving Operational Efficiency:** IAM simplifies access management by using roles and groups, reducing the administrative workload associated with granting and revoking access.
4. **Supporting Scalability:** As organizations grow, IAM makes it easier to manage thousands of users and their permissions across various systems, applications, and resources.

IAM is essential in cloud environments, where resources are highly distributed and continuously scaled, making access control crucial for effective governance and security.

This overview highlights how IAM, along with user and group management, provides a structured approach to managing permissions and protecting sensitive data within an organization.

[Login as root user

Search iam (manage access to aws services)

Go to users write name create user

Giving access:- go to ARN(auto enable console ; what you want to show the user first page

Custom password you can set

Auto by computer

Then after copying the link sign in to I am user

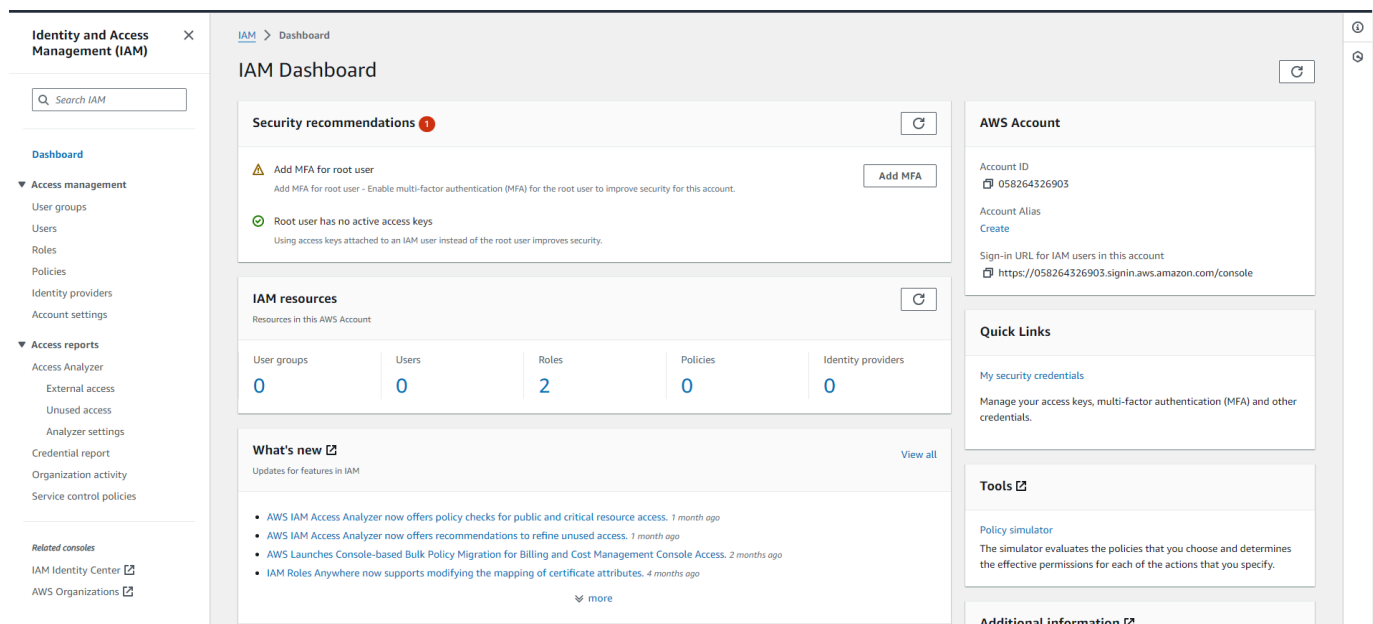
Create policies select service –S3 effect=allow sid name of root user create

go to json

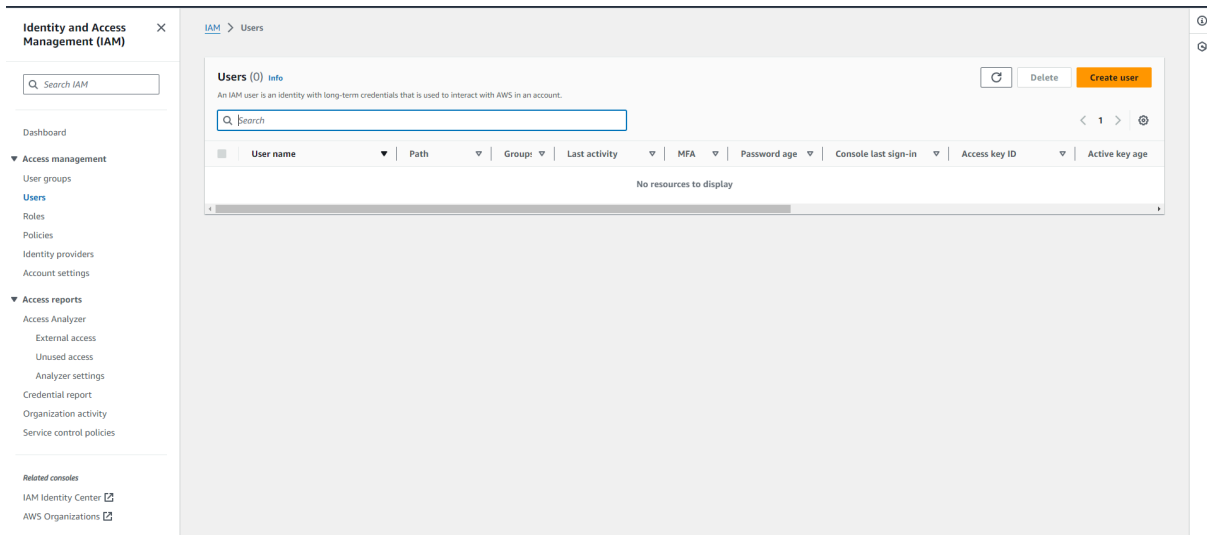
visualise : graphical access select s3 allow all options(*)

root user add permission attach policy search and add permission]

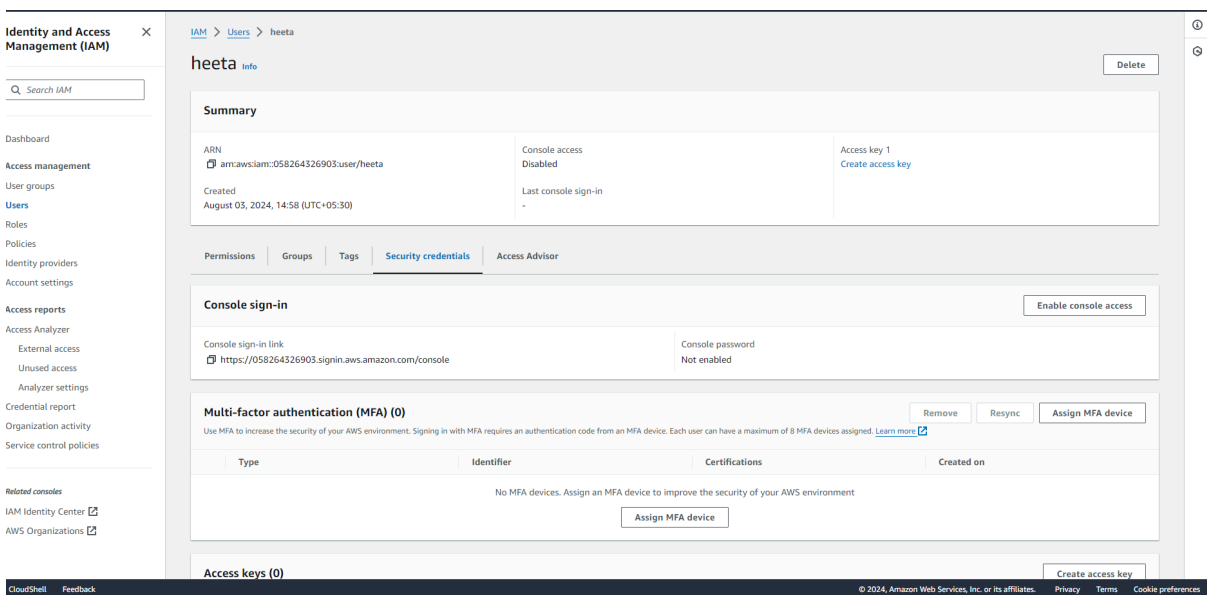
1: Search IAM Identify and manage access on AWS services)



2: Go to users ----> write name--> create user



3: Once the user is created we can create password by two methods: a) autogenerated b) custom. Tap on the user name that you created. Go into the Security credentials and enable console access.



4: Copying the ARN and logging with IAM user

Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)

English

[Terms of Use](#)
[Privacy Policy](#)
© 1999-2024 Amazon Web Services, Inc. or its affiliates.

5: Unless and until the access to delete or update or create the buckets, EC2 is granted the IAM user can't perform those tasks the access is denied .

Reset to default layout

+ Add widgets

Recently visited

No recently visited services

Explore one of these commonly visited AWS services.

[EC2](#) [S3](#) [RDS](#) [Lambda](#)

[View all services](#)

Applications (0)

Region: Europe (Stockholm)

eu-north-1 (Current Region)

Find applications

< 1 >

Name	Description	Region	Originating account
Access denied			

[Go to my Applications](#)

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.

AWS Health

No health data

You don't have permissions to access AWS Health.

Cost and usage

Current month costs

Access denied

Forecasted month end costs

Access denied

Savings opportunities

Access denied

Cost breakdown

Access denied

CloudShell

Feedback

© 2024 Amazon Web Services, Inc. or its affiliates.
[Privacy](#)
[Terms](#)
[Cookie preferences](#)

6: To unable those access we need to create a policy for the same .

Left side of the window comprises of the option policy then create policy .

Once the policy is created attach it to the user name.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM Identity Center

AWS Organizations

IAM > Policies

Policies (1221) info

Actions

Delete

Create policy

Search

Filter by Type

All types

	Policy name	Type	Used as	Description
<input type="radio"/>	AccessAnalyzerServiceRolePolicy	AWS managed	None	-
<input type="radio"/>	AdministratorAccess	AWS managed – job function	None	Provides full access to AWS services an...
<input type="radio"/>	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
<input type="radio"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permis...
<input type="radio"/>	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
<input type="radio"/>	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
<input type="radio"/>	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
<input type="radio"/>	AlexaForBusinessLifeseizeDelegatedAccess...	AWS managed	None	Provide access to Lifeseize AVS devices
<input type="radio"/>	AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	-
<input type="radio"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
<input type="radio"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...
<input type="radio"/>	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/dele...
<input type="radio"/>	AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...
<input type="radio"/>	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to us...
<input type="radio"/>	AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlo...
<input type="radio"/>	AmazonAthenaReadOnlyAccess	AWS managed	None	Provides read only access to Amazon A...

7:Granting permission .change the sid to the user name .

Step 2

Review and create

Policy editor

Visual

JSON

Actions

S3

Allow

All actions

Specify what actions can be performed on specific resources in S3.

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

☒ All S3 actions (s3:*)

Access level

List (Selected 15/15)

Read (Selected 60/60)

Write (Selected 57/57)

Permissions management (Selected 15/15)

Tagging (Selected 12/12)

Warning icon

Dependent permissions not selected.

To grant permissions for the selected resource actions, including additional dependent actions might be required.

- s3:CreateJob requires 1 more action.
- s3:PauseReplication requires 2 more actions.
- s3:PutReplicationConfiguration requires 1 more action.

Resources

Specify resource ARNs for these actions.

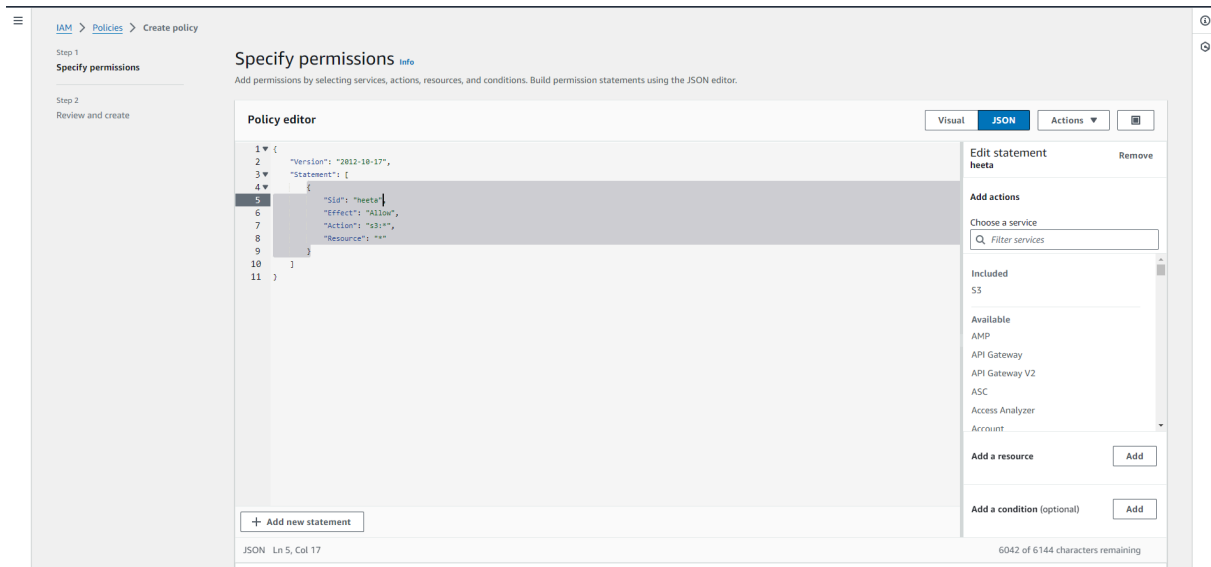
☒ All

Effect

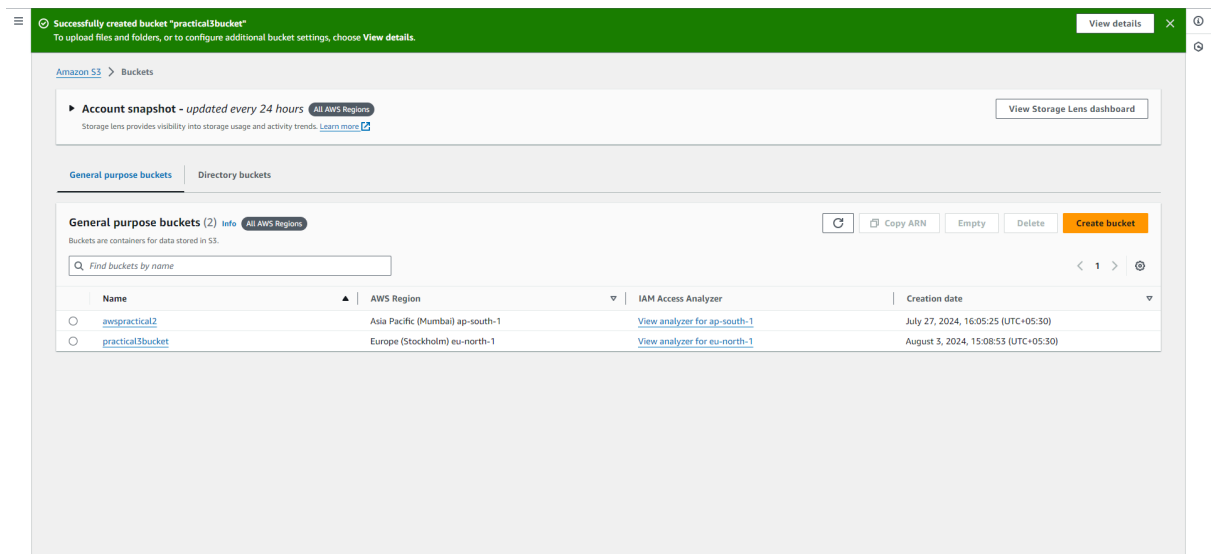
☒ Allow
 ☐ Deny

Expand all

Collapse all



8: Now, the IAM user can successfully create a S3 bucket .



#FOR EC2 . After selecting the policy select ec2 instead of s3 bucket . and do the necessary required changes. Rest all steps are same

Policy attached to 0 entities.

IAM > Policies > Create policy

Step 1

Specify permissions

Step 2

Review and create

Specify permissions

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

EC2

AllowAll actions

Specify what actions can be performed on specific resources in EC2.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

☒ All EC2 actions (ec2:*)

Access level

List (Selected 175/175)

Read (Selected 36/36)

Write (Selected 420/420)

Permissions management (Selected 5/5)

Tagging (Selected 2/2)

Dependent permissions not selected.

To grant permissions for the selected resource actions, including additional dependent actions might be required.

ec2:AssociateInstanceProfile requires 1 more action.

Effect

☒ Allow☐ Deny

Expand all | Collapse all

Modify permissions in heeeta_policy

Step 1

Modify permissions in heeeta_policy

Step 2

Review and save

Modify permissions in heeeta_policy

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "heeta",
6       "Effect": "Allow",
7       "Action": "ec2:*",
8       "Resource": "*"
9     }
10  ]
11 }
```

+ Add new statement

Edit statement heeta

Remove

Add actions

Choose a service

Filter services

Included

EC2

Available

AMP

API Gateway

API Gateway V2

ASC

Access Analyzer

Account

Add a resource

Add

Add a condition (optional)

Add

6041 of 6144 characters remaining

Check for new access

JSON Ln 5, Col 16

Security: 0Errors: 0Warnings: 0Suggestions: 0

EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-0608eab3a160028c0)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Create billing alerts

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance

Learn more

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

Create a new RDS database

Learn more

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

Create EBS snapshot policy

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Manage detailed monitoring

Create Load Balancer

Create an application, network gateway or classic Elastic Load Balancer

Create Load Balancer

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Create AWS budget

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

Manage CloudWatch alarms

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

All states

Connect

Instance state

Actions

Launch Instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	practical3	i-0b08eab3a160028cc	Running	t3.micro	Initializing	User: amzaws	eu-north-1b	ec2-13-60-87-40.eu-no...	13.60.87.40	-

Select an instance