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

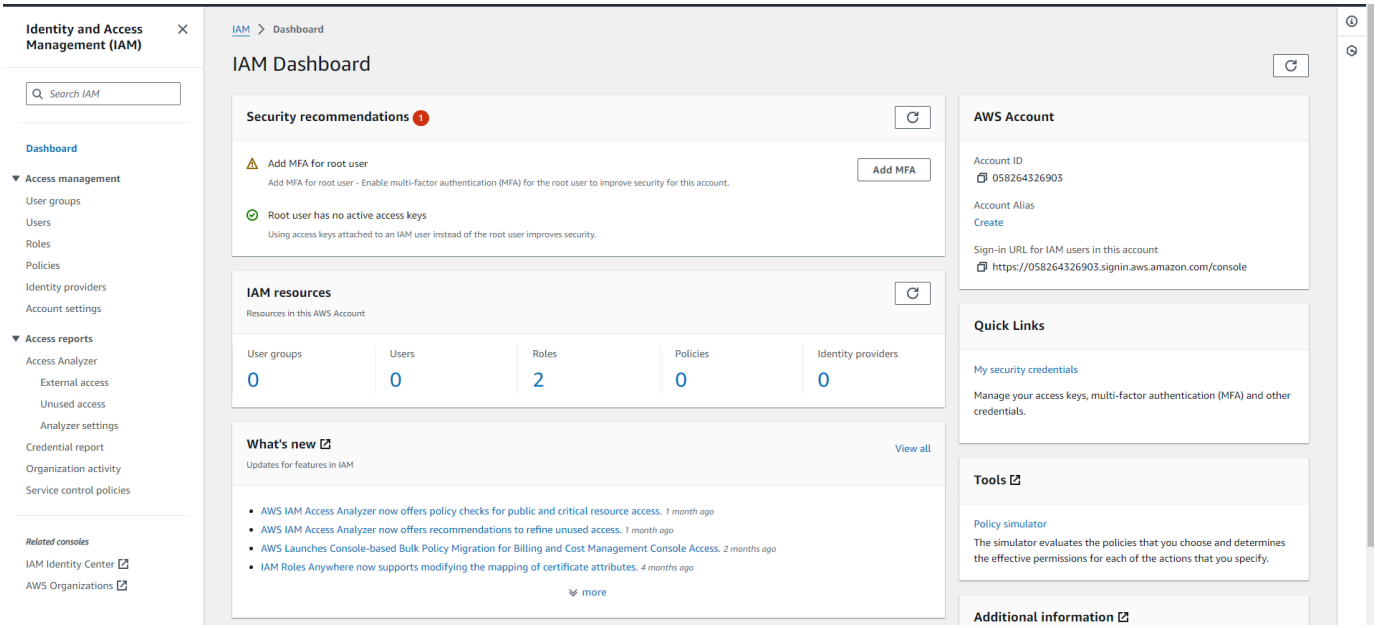
Create policies select service –S3 effect=allow sid name of root user create

go to json

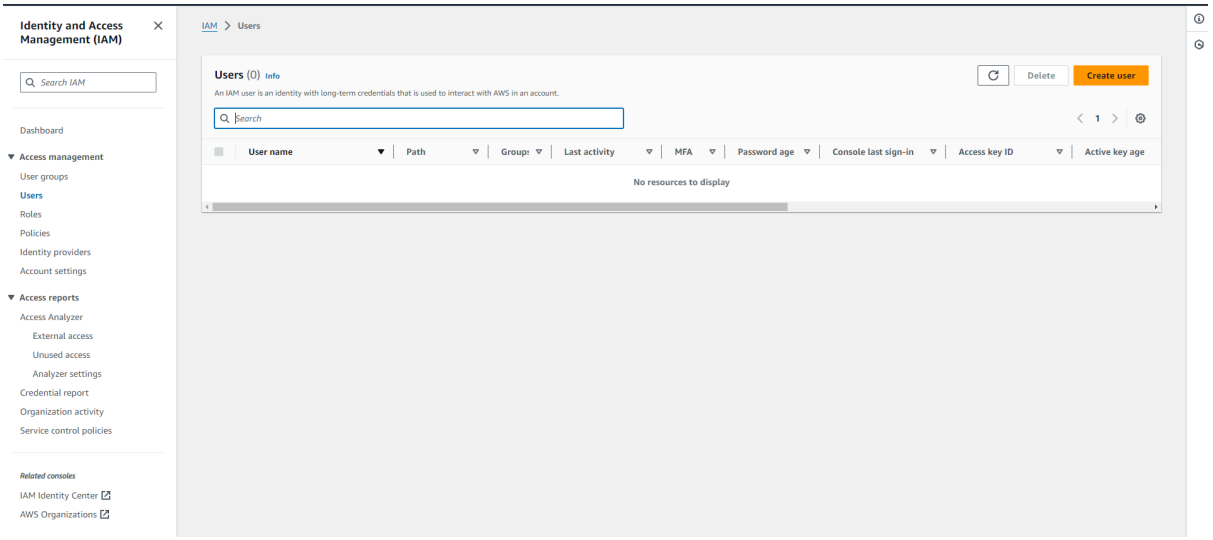
visualise : graphical access select s3 allow all options(*)

root user add permission attach policy search and add permission]

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

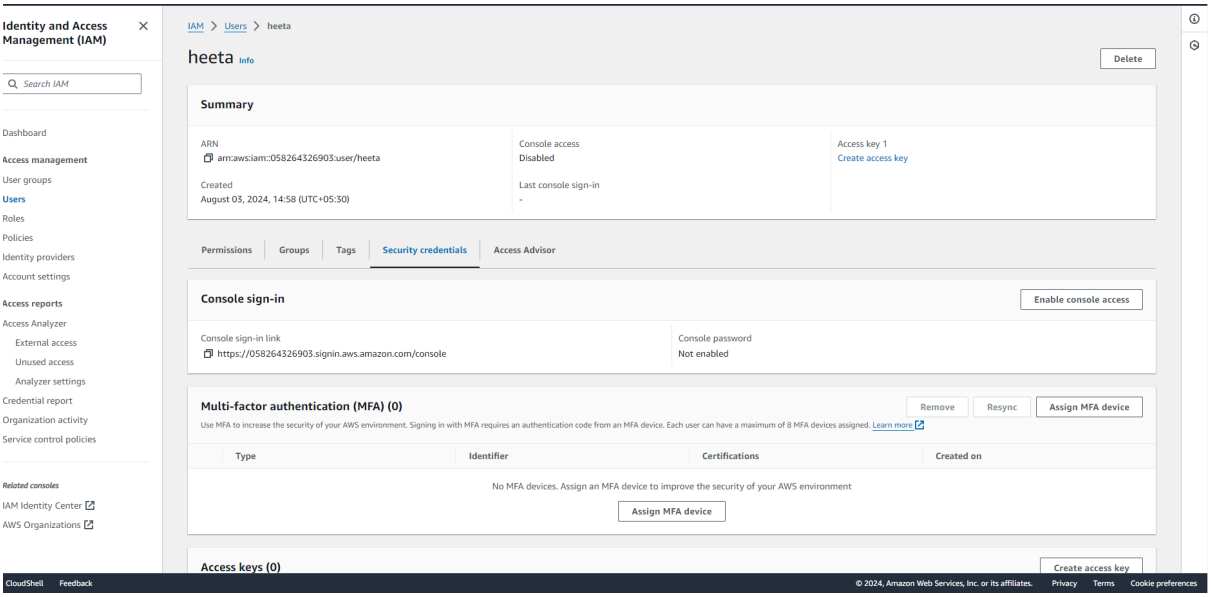


2: Go to users ----> write name--? create user

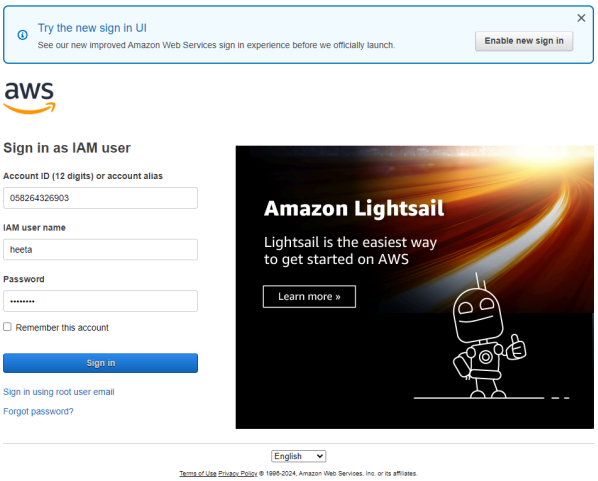


3:**Once the user is created we can create password by two method a)autogenerated b)custom**

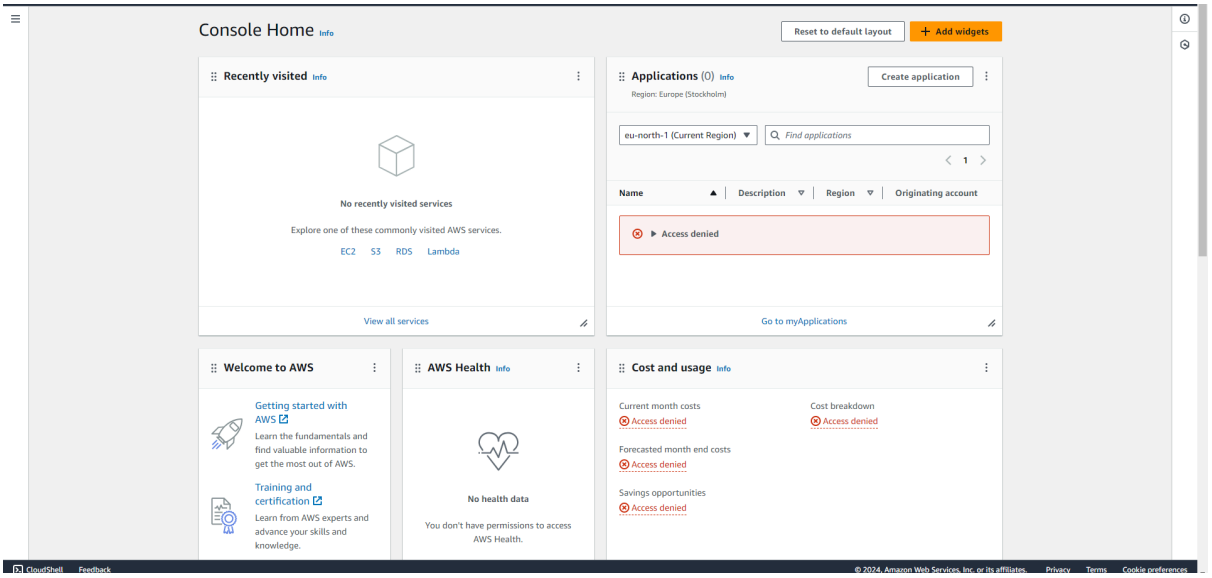
Tap on the user name that you created. Go into the Security credentials and enable console access.



4: Copying the ARN and logging with I AM user



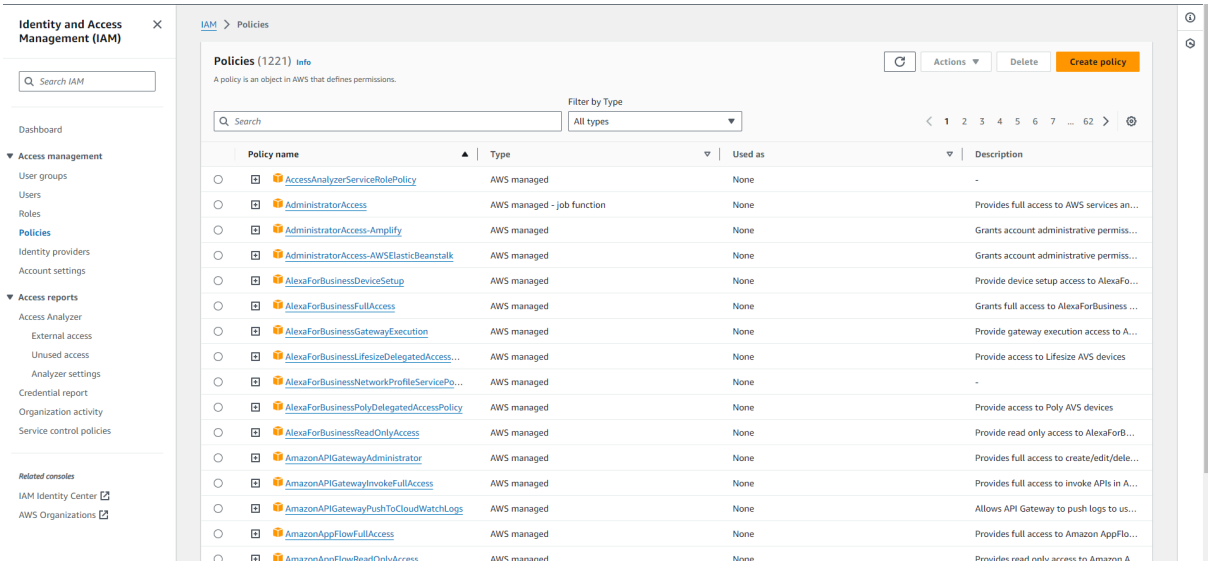
5:Unless and until the access to delete or update or create the buckets,EC2 is granted the IAM user can't perform those tasks the access is denied .



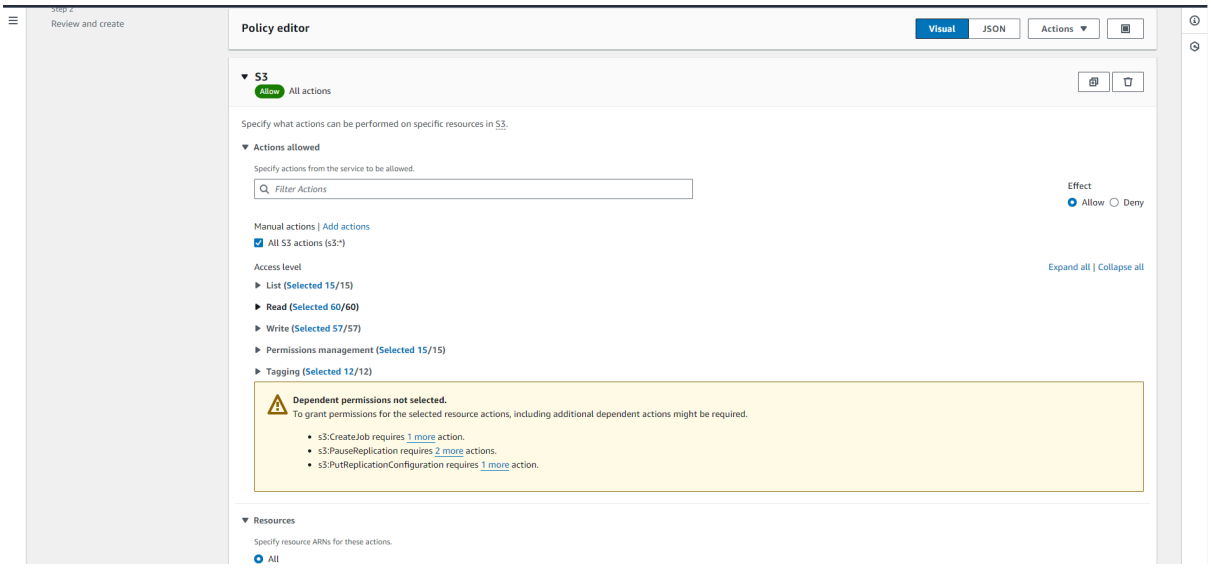
6:To unable those access we need to create a policy for the same .

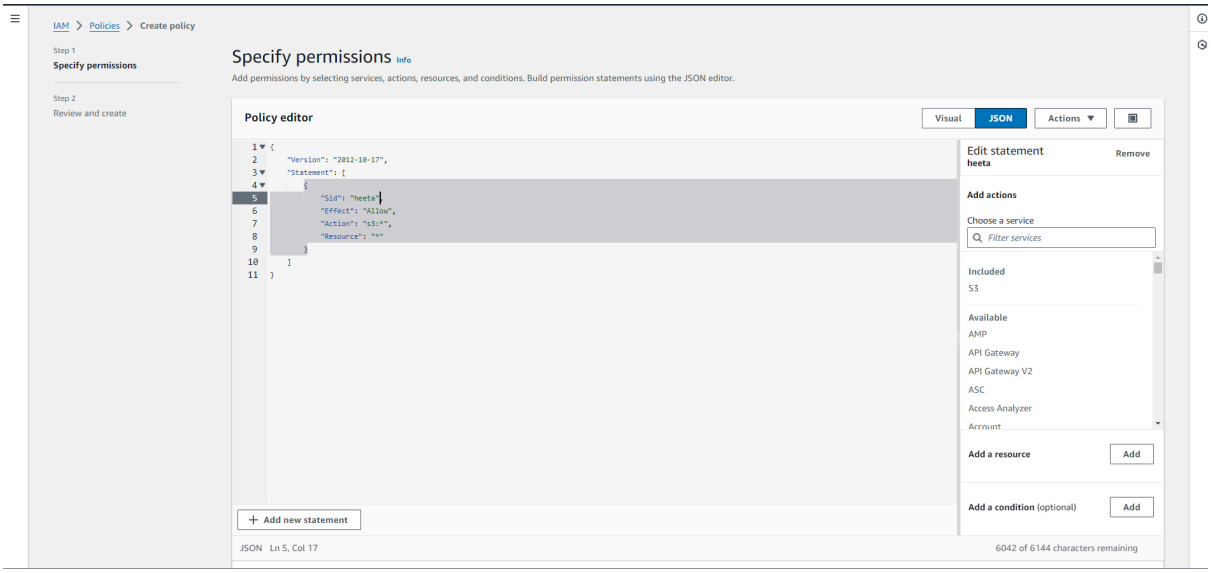
Left side of the window comprises of the option policy then create policy .

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

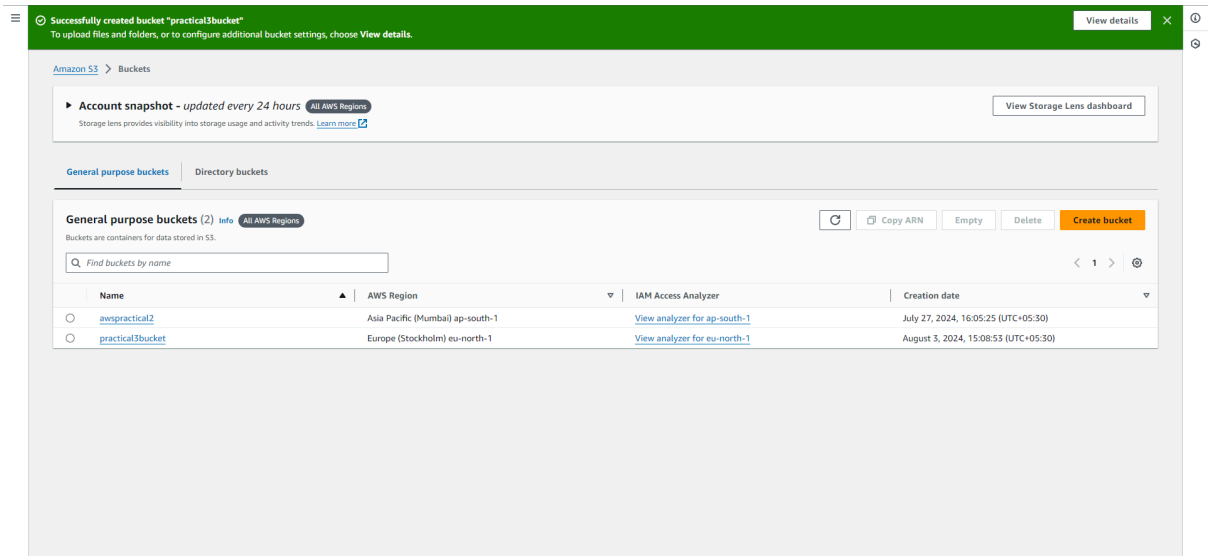


7:Granting permission .change the sid to the user name .

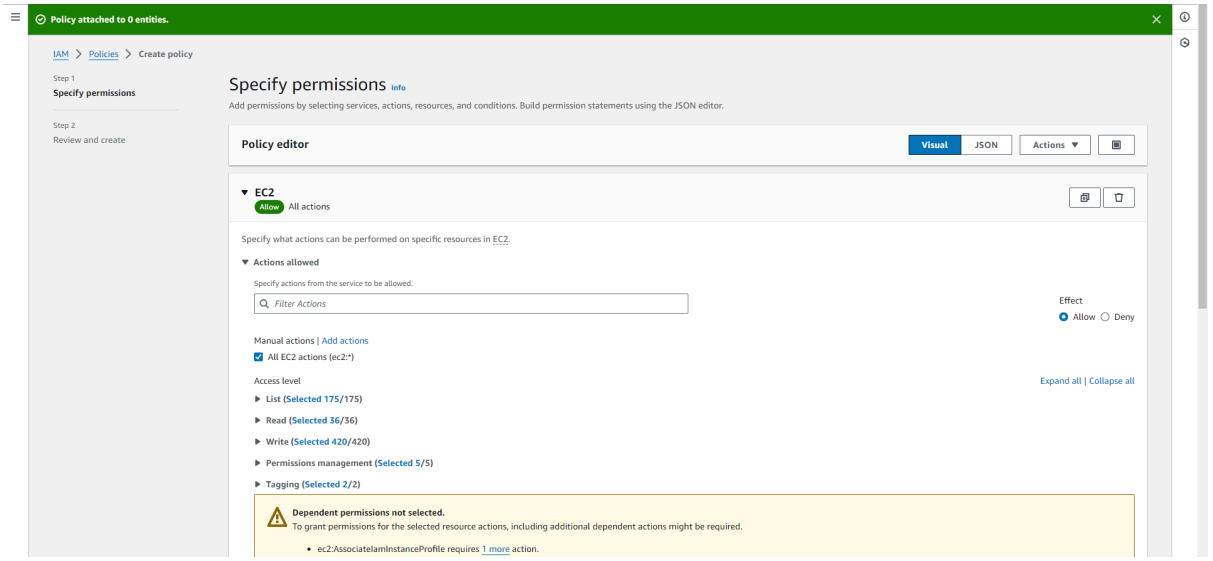


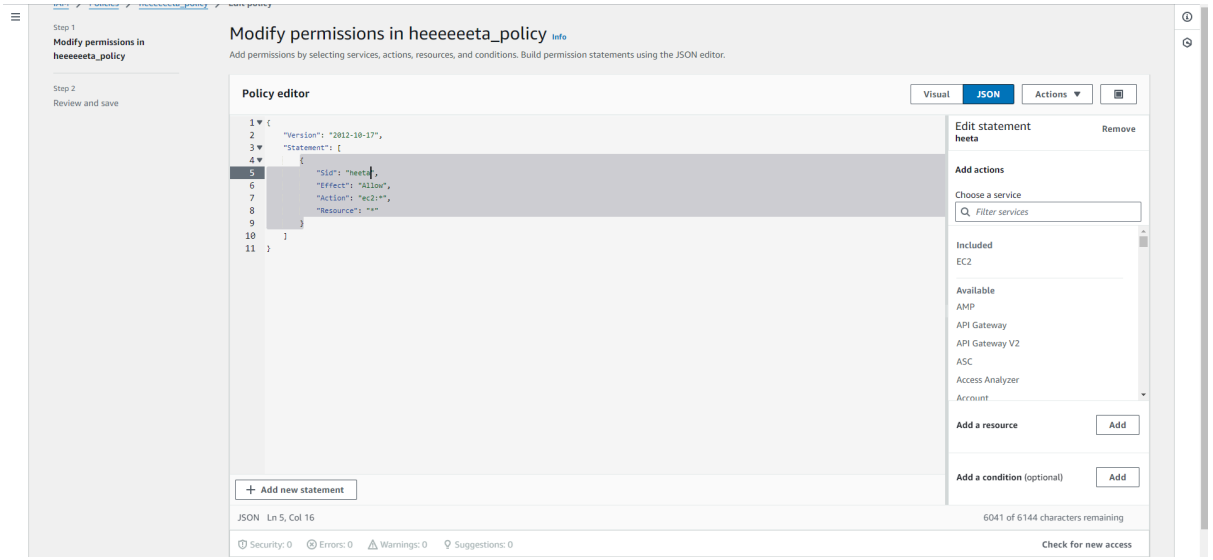


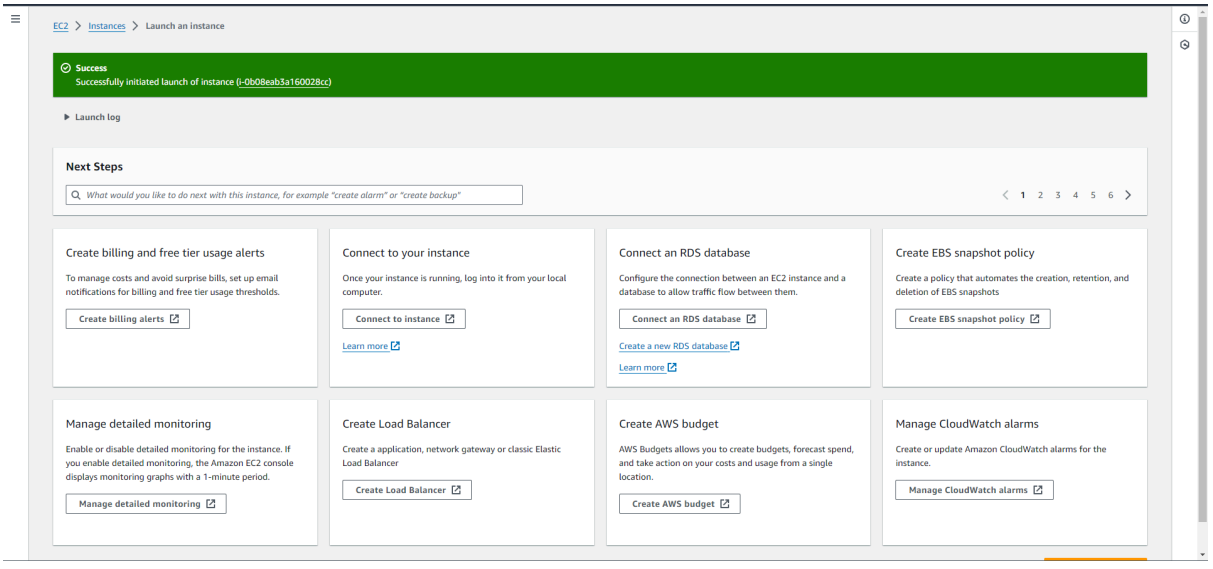
8: Now, the IAM user can successfully create a S3 bucket .

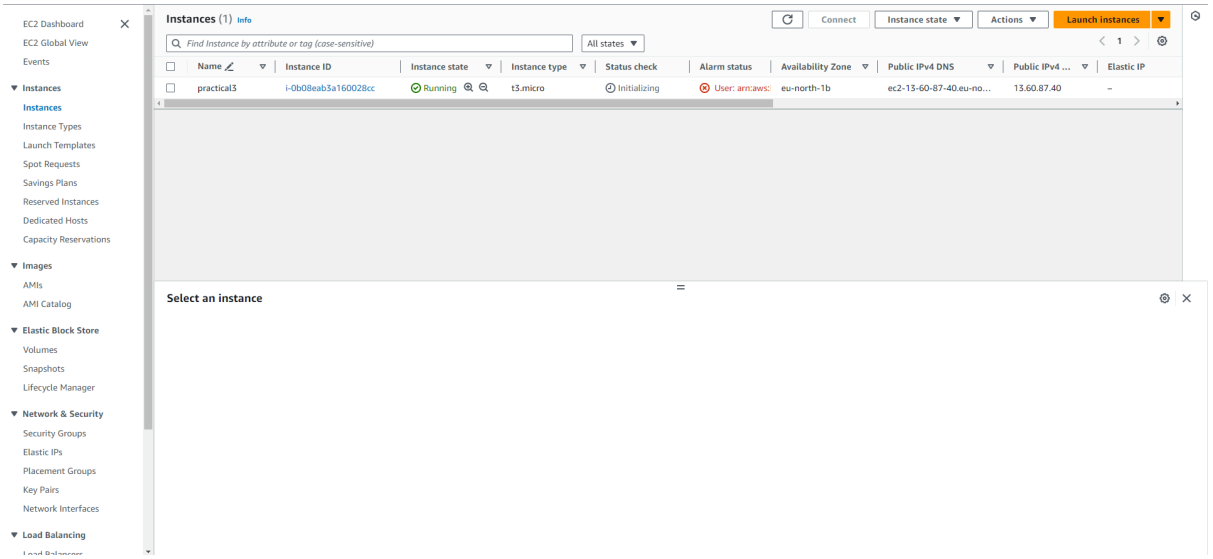


#FOR EC2 . After selecting the policy select ec2 instead of s3 bucket . and do the necessary required changes. Rest all steps are same


Policy attached to 0 entities.
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
EC2
Allow All actions
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All EC2 actions (ec2:*)
Access level
Expand all | Collapse all
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:AssociateIamInstanceProfile requires 1 more action.


Step 1
Modify permissions in heeeeeeta_policy
Step 2
Review and save
Modify permissions in heeeeeeta_policy Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "heeta",
"Effect": "Allow",
"Action": "ec2:*",
"Resource": "*"
}
]
}
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
Add new statement
JSON Ln 5, Col 16
6041 of 6144 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Check for new access


EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0b08eab3a160028cc)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
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 a 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
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
practical3
i-0b08eab3a160028cc
Running
t3.micro
Initializing
eu-north-1b
ec2-13-60-87-40.eu-no...
13.60.87.40
Select an instance