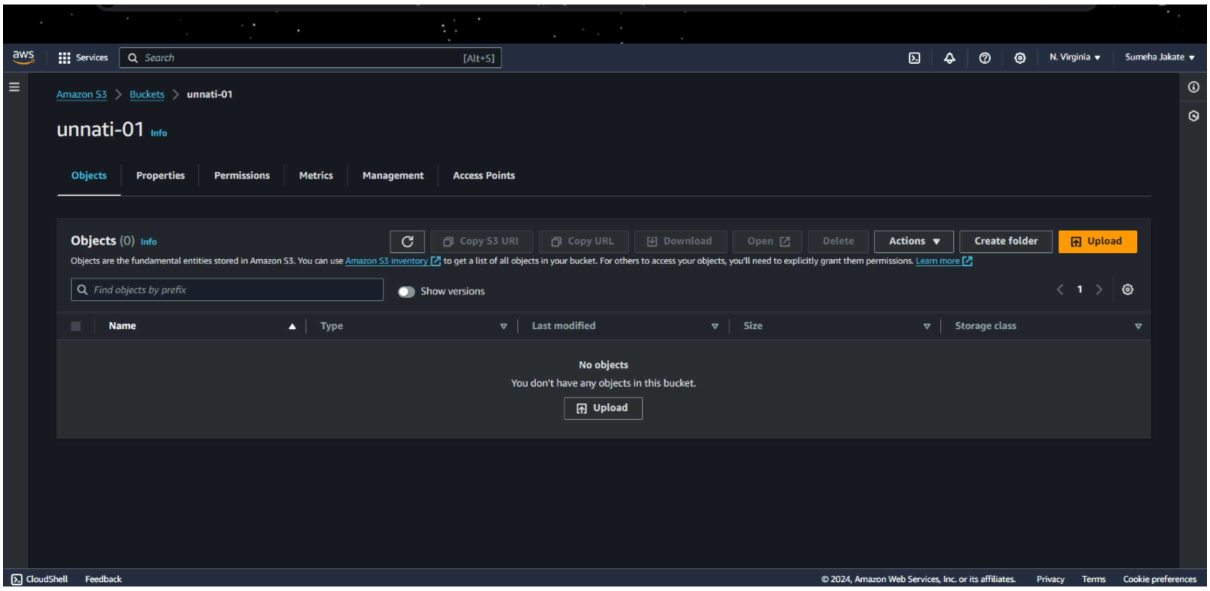
To assign specific permissions in AWS IAM for three users (`user1`, `user2`, and `user3`) with different levels of access to an S3 bucket, follow these steps:

Step 1: Create an S3 Bucket

1. **Create an S3 Bucket**:
   - Open the S3 console.
   - Choose "Create bucket".
   - Enter a unique bucket name.
   - Select a region.
   - Configure other settings as needed.
   - Choose "Create bucket".



Amazon S3 > Buckets > unnati-01

unnati-01 Info

Objects (0) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

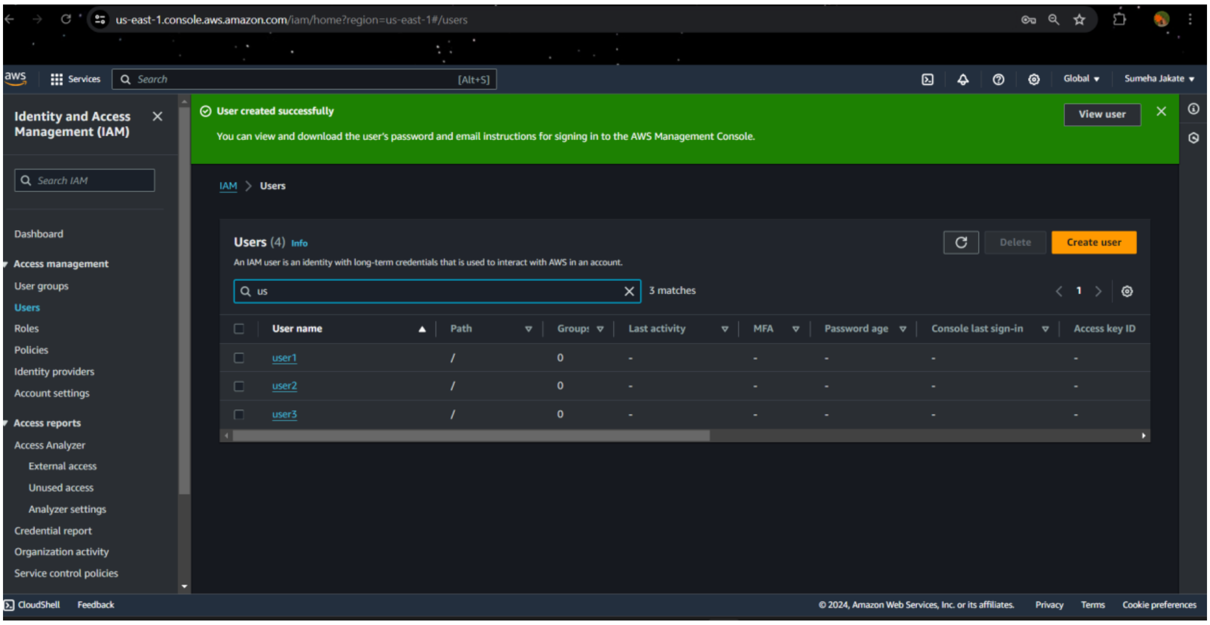
No objects

You don't have any objects in this bucket.

© 2024, Amazon Web Services, Inc. or its affiliates.

Step 2: Create IAM Users

1. **Create IAM Users**:
    - Open the IAM console.
    - In the navigation pane, choose "Users".
    - Choose "Add user".
    - Enter the user names (`user1`, `user2`, and `user3`).
    - Select "AWS Management Console access".
    - Set custom passwords or auto-generated passwords for console access.
    - Choose "Next: Permissions".



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (4)

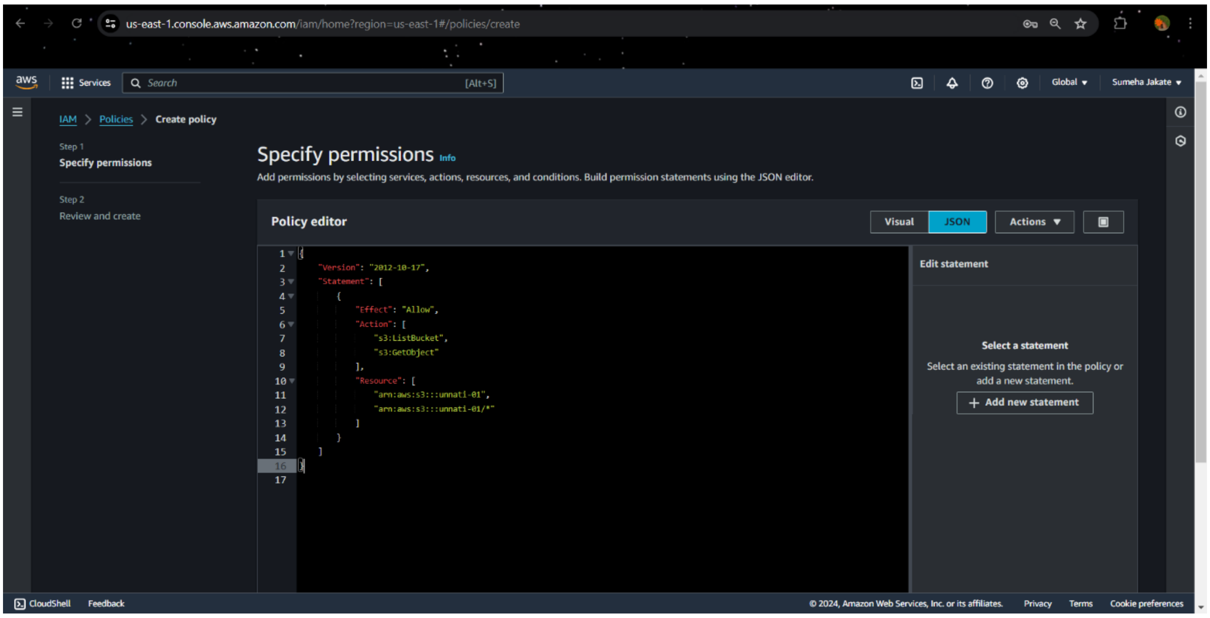
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

3 matches

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
user1	/	0	-	-	-	-	-
user2	/	0	-	-	-	-	-
user3	/	0	-	-	-	-	-

Step 3: Create and Attach Policies

1. **Create a Policy for `user1`:**
   - Open the IAM console.
   - In the navigation pane, choose "Policies".
   - Choose "Create policy".
   - Select the "JSON" tab and enter the following policy for `user1`


us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
aws
Services
Search
[Alt+S]
Global
Sumeha Jakate
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Visual
JSON
Actions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Specify permissions Info

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

Policy editor

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::unnati-01",
                "arn:aws:s3:::unnati-01/*"
            ]
        }
    ]
}
```

Edit statement

Select a statement

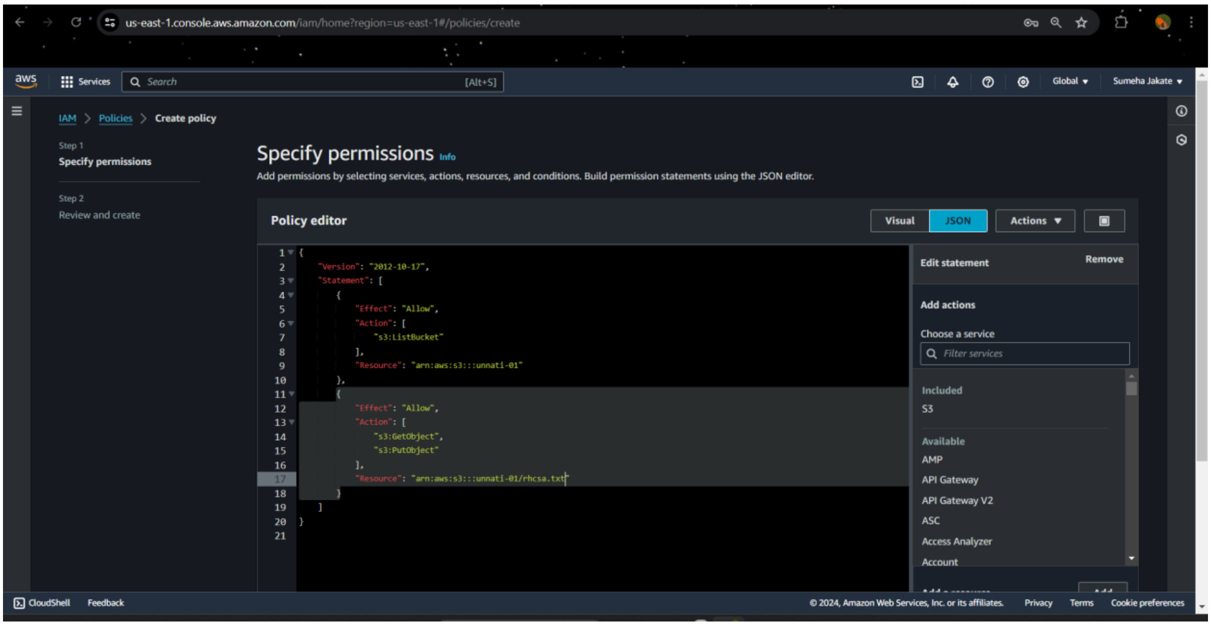
Select an existing statement in the policy or add a new statement.

+ Add new statement

- Choose "Next: Tags", then "Next: Review".
- Enter a name for the policy.
- Choose "Create policy".

2. **Create a Policy for `user2`:**

- Repeat the above steps to create a policy for `user2`



Specify permissions Info

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

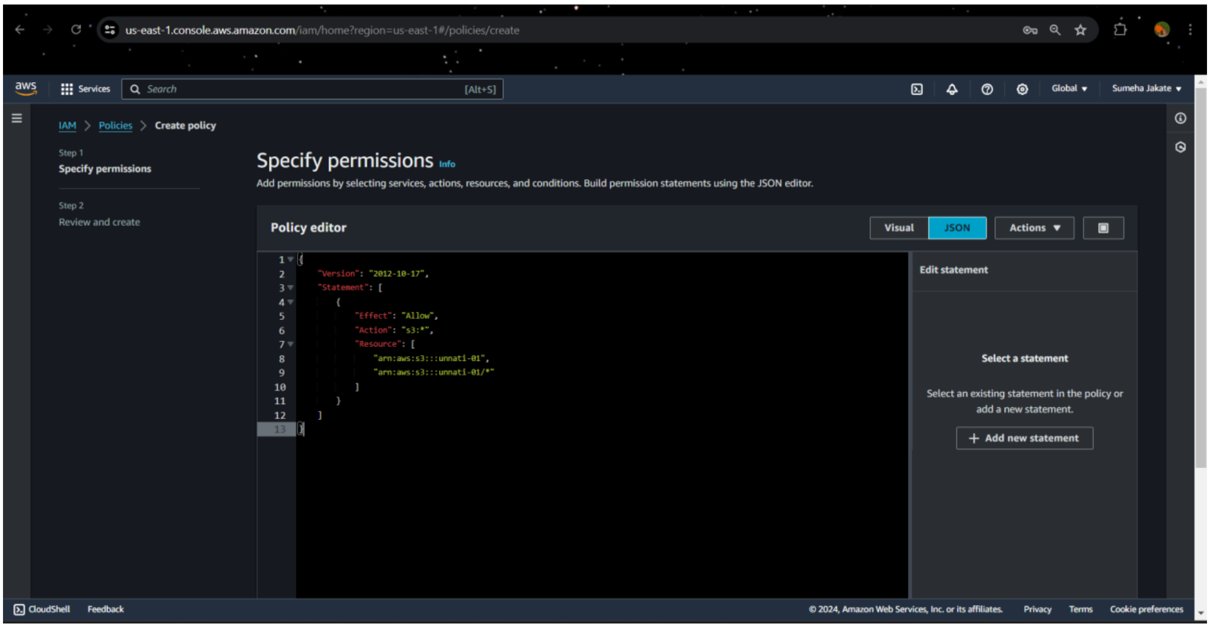
Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::unnati-01"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::unnati-01/rhcsa.txt"
        }
    ]
}
```

- Choose "Next: Tags", then "Next: Review".
- Enter a name for the policy.
- Choose "Create policy"

3. **Create a Policy for `user3`:**

- Repeat the above steps to create a policy for `user3`



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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::unnati-01",
                "arn:aws:s3:::unnati-01/*"
            ]
        }
    ]
}
```

Edit statement

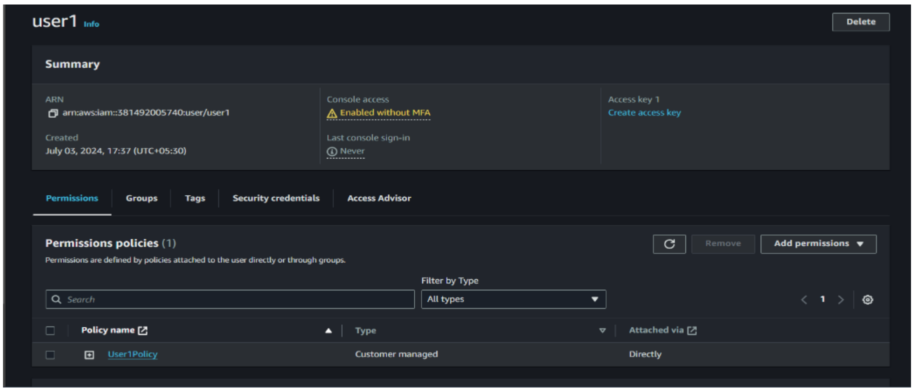
Select a statement

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

- Choose "Next: Tags", then "Next: Review".
- Enter a name for the policy.
- Choose "Create policy".

4. **Attach Policies to Users**:

- Go to the "Users" section in the IAM console.
- Select `user1`, go to the "Permissions" tab, and choose "Add permissions".
- Select "Attach policies directly", find `User1Policy`, and attach it.
- Repeat for `user2` with `User2Policy` and for `user3` with `User3Policy`.



Summary

ARN: arn:aws:iam::381492005740:user/user1

Created: July 03, 2024, 17:37 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: Never

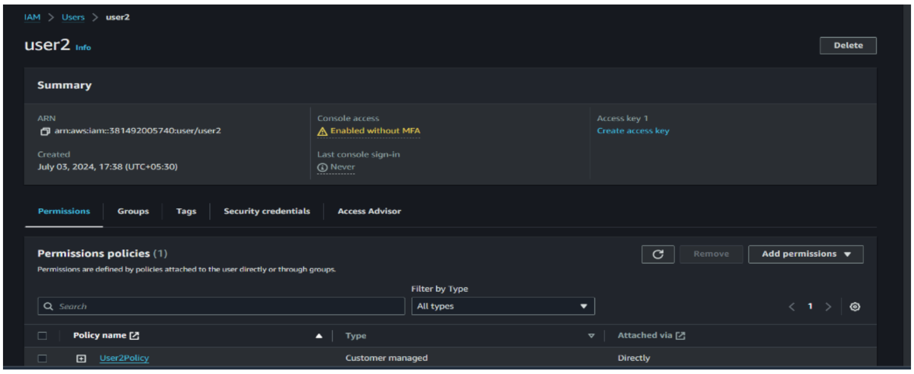
Access key 1: Create access key

Permissions policies (1)

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

Filter by Type: All types

Policy name	Type	Attached via
User1Policy	Customer managed	Directly



Summary

ARN: arn:aws:iam::381492005740:user/user2

Created: July 03, 2024, 17:38 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: Never

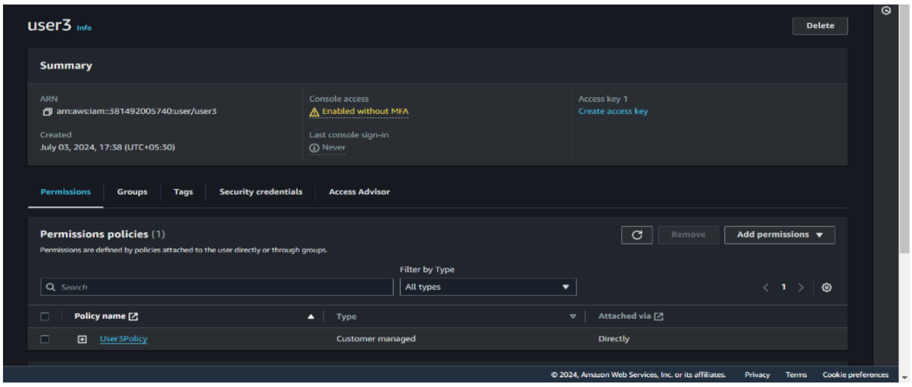
Access key 1: Create access key

Permissions policies (1)

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

Filter by Type: All types

Policy name	Type	Attached via
User2Policy	Customer managed	Directly



Summary

ARN: arn:aws:iam::381492005740:user/user3

Created: July 03, 2024, 17:38 (UTC+05:30)

Console access: Enabled without MFA

Last console sign-in: Never

Access key 1: Create access key

Permissions policies (1)

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

Filter by Type: All types

Policy name	Type	Attached via
User3Policy	Customer managed	Directly

© 2024, Amazon Web Services, Inc. or its affiliates.

Step 4: Verify Permissions

1. **Login as `user1`:**
   - Use the AWS Management Console login link and credentials for `user1`.
   - Go to the S3 console and verify that `user1` can list the bucket and read objects.

2. **Login as `user2`:**
   - Use the AWS Management Console login link and credentials for `user2`.
   - Go to the S3 console and verify that `user2` can list the bucket, read, and write the specific object.

3. **Login as `user3`:**
   - Use the AWS Management Console login link and credentials for `user3`.
   - Go to the S3 console and verify that `user3` has all permissions for the bucket.

By following these steps, you will have created an S3 bucket, configured IAM users, attached the appropriate policies, and verified their permissions.