Lesson 03 Demo 03

Using IAM Roles to Access S3 Bucket

Objective: To securely access Amazon S3 (Simple Storage Service) buckets from an EC2 instance using IAM (Identity and Access Management) roles

Tools required: AWS Lab

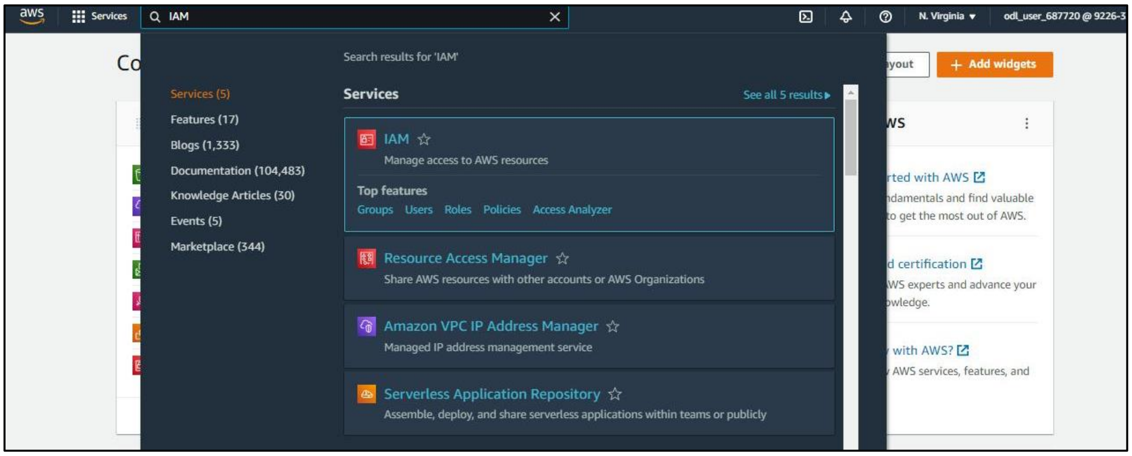
Prerequisites: Create an EC2 instance named S3

Steps to be followed:

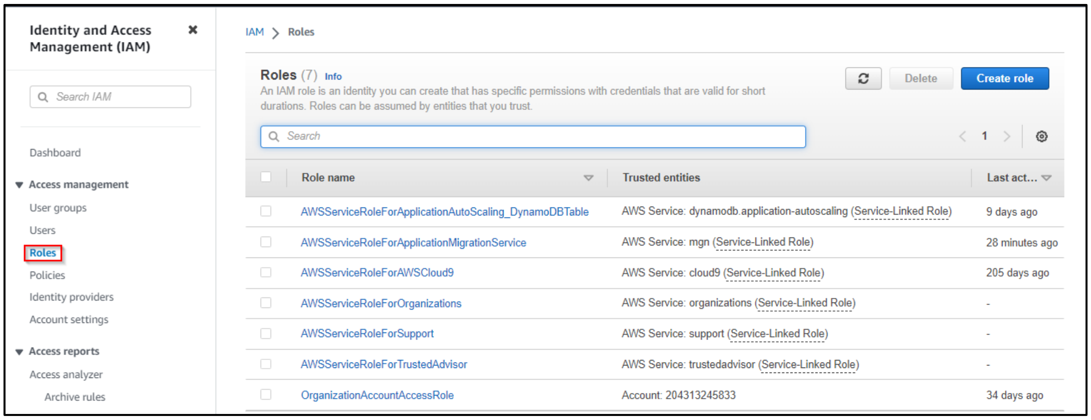
1. Create an IAM role
2. Connect IAM Profile to EC2
3. Validate access to the S3 bucket

Step 1: Create an IAM role

1.1 On the AWS management console, search and select **IAM**



1.2 Navigate to **Roles,** and click on the **Create role** button



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

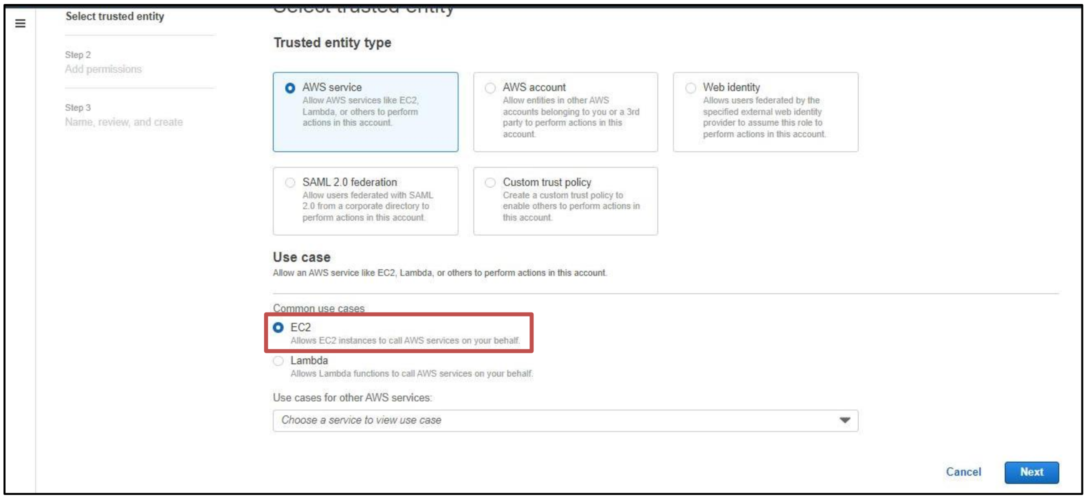
IAM > Roles

Roles (7) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last act...
□	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-autoscaling (Service-Linked Role)	9 days ago
□	AWSServiceRoleForApplicationMigrationService	AWS Service: mgn (Service-Linked Role)	28 minutes ago
□	AWSServiceRoleForAWSCloud9	AWS Service: cloud9 (Service-Linked Role)	205 days ago
□	AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	-
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
□	OrganizationAccountAccessRole	Account: 204313245833	34 days ago

1.3 Choose AWS service, select **EC2**, and click **Next**



Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

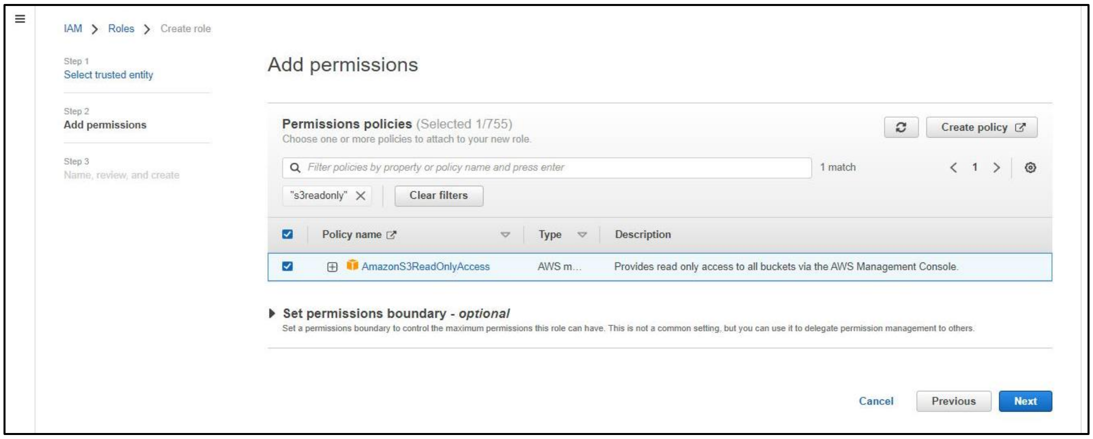
● EC2
Allows EC2 instances to call AWS services on your behalf.

○ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

1.4 Search and select **AmazonS3ReadOnlyAccess**, and proceed by clicking **Next**



Add permissions

Permissions policies (Selected 1/755)

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

Filter policies by property or policy name and press enter

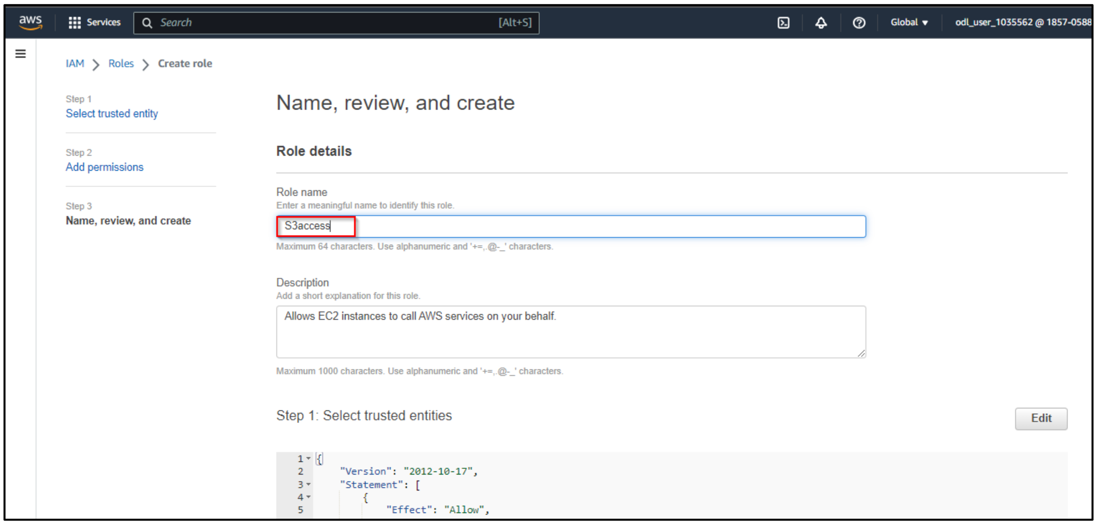
"s3readonly"

☑	Policy name	Type	Description
☑	⊞ AmazonS3ReadOnlyAccess	AWS m...	Provides read only access to all buckets via the AWS Management Console.

Set permissions boundary - *optional*

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

1.5 Input the role name, and click **Create role**



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

S3access

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

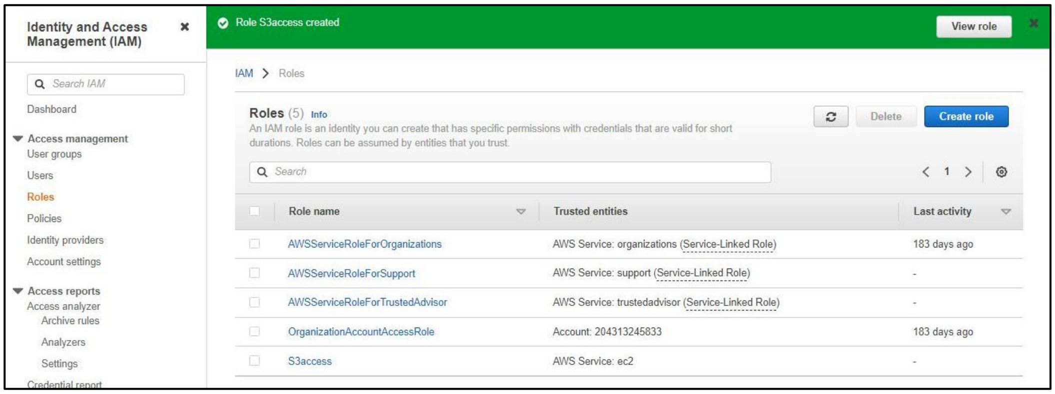
Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```



Role S3access created

Roles (5) Info

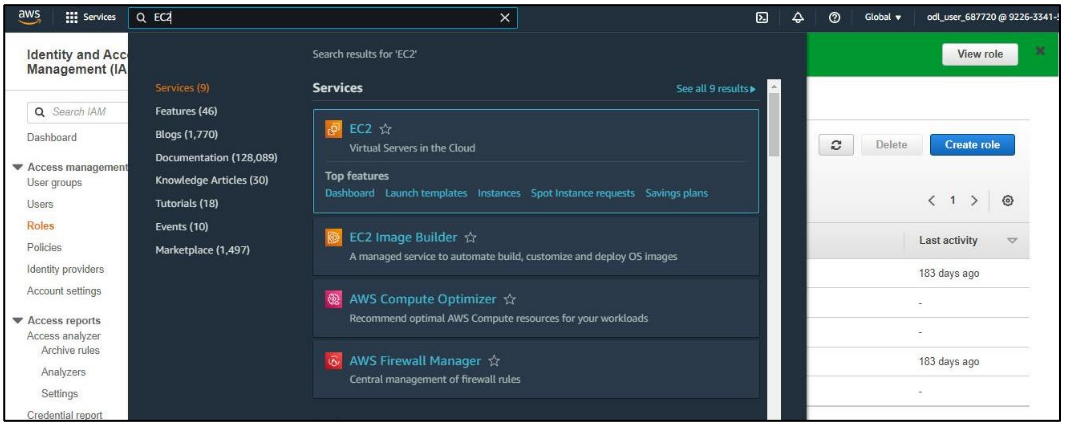
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	183 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
OrganizationAccountAccessRole	Account: 204313245833	183 days ago
S3access	AWS Service: ec2	-

The IAM role is successfully created.

Step 2: Connect IAM Profile to EC2

2.1 Navigate to the **EC2** console



Search results for 'EC2'

Services

See all 9 results ▸

EC2 ☆
Virtual Servers in the Cloud

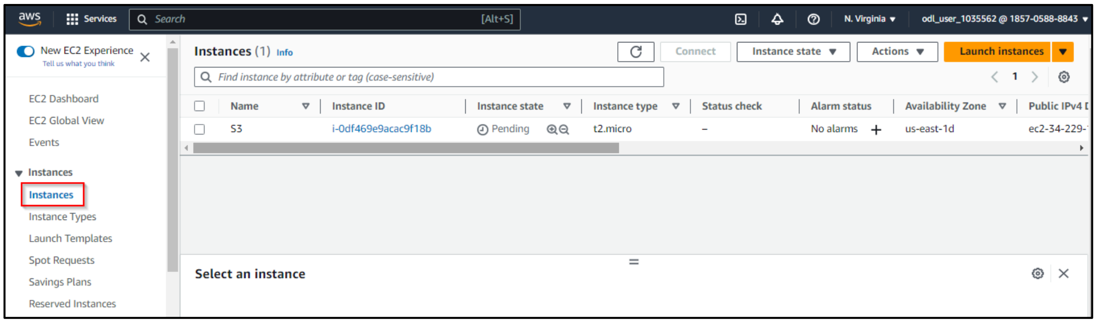
Top features
Dashboard Launch templates Instances Spot Instance requests Savings plans

EC2 Image Builder ☆
A managed service to automate build, customize and deploy OS images

AWS Compute Optimizer ☆
Recommend optimal AWS Compute resources for your workloads

AWS Firewall Manager ☆
Central management of firewall rules

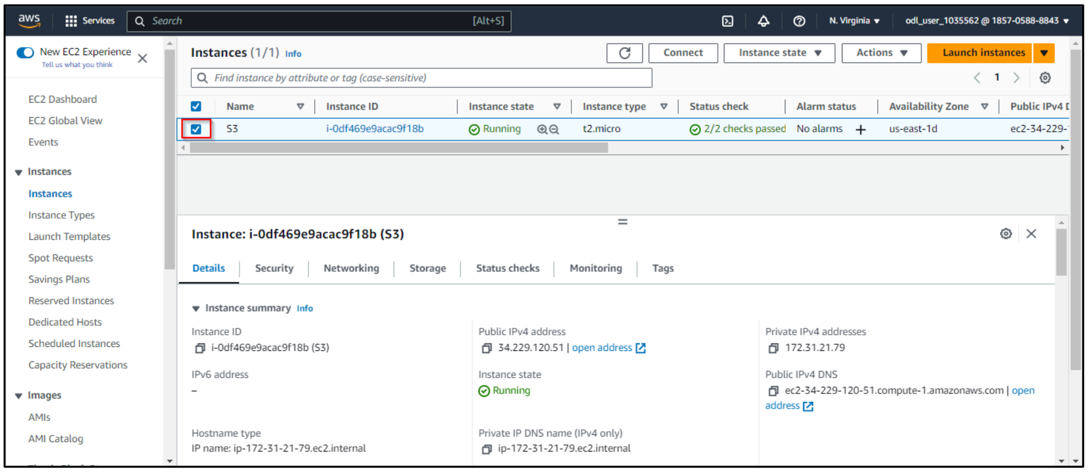
2.2 Click on **Instances** and launch a new instance named **S3**



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
□	S3	i-0df469e9acac9f18b	Pending	t2.micro	–	No alarms +	us-east-1d	ec2-34-229-

For creating instances, refer to previous demos.

2.3 Select the **S3** instance



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
☑	S3	i-0df469e9acac9f18b	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1d	ec2-34-229-

Instance: i-0df469e9acac9f18b (S3)

Instance ID
i-0df469e9acac9f18b (S3)

Public IPv4 address
34.229.120.51 | open address

Private IPv4 addresses
172.31.21.79

IPv6 address
–

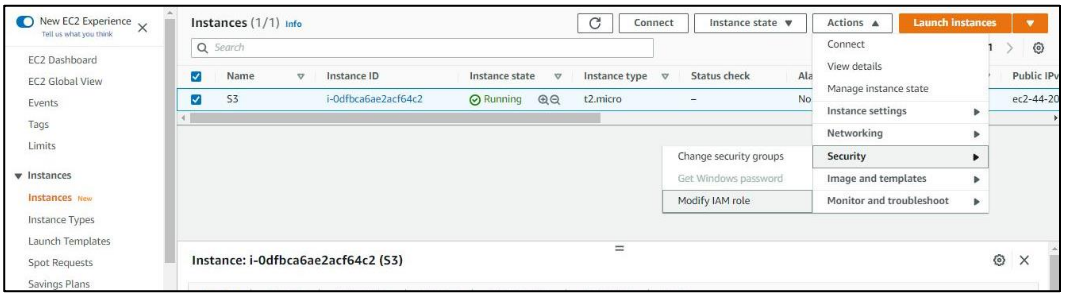
Instance state
Running

Public IPv4 DNS
ec2-34-229-120-51.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-172-31-21-79.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-21-79.ec2.internal

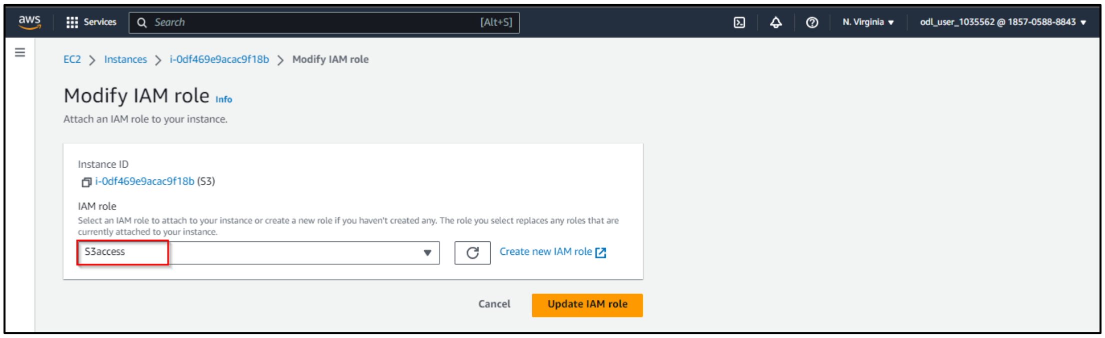
2.4 Under **Actions**, choose **Security** and click **Modify IAM role**



☑	Name	Instance ID	Instance state	Instance type	Status check	Ala	Public IPv
☑	S3	i-0dfbca6ae2acf64c2	Running	t2.micro	–	No	ec2-44-20

Instance: i-0dfbca6ae2acf64c2 (S3)

2.5 In the IAM role section, select the previously created role, and click **Update IAM role**


aws
Services
Search [Alt+S]
N. Virginia
odl_user_1035562 @ 1857-0588-8843
EC2 > Instances > i-0df469e9acac9f18b > Modify IAM role
Info
Create new IAM role
Cancel
Update IAM role

Modify IAM role

Attach an IAM role to your instance.

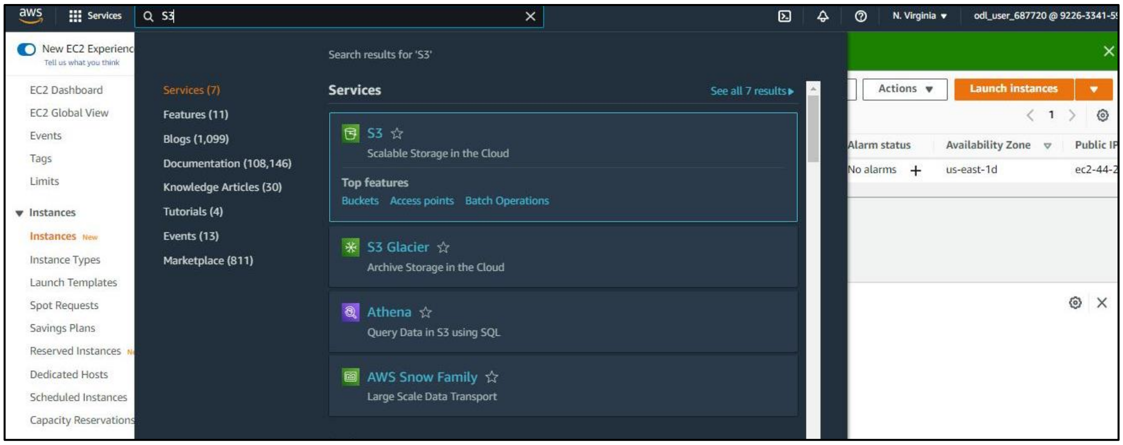
Instance ID
i-0df469e9acac9f18b (S3)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

S3access

Step 3: Validate access to the S3 bucket

3.1 Navigate to the **S3** console



Search results for 'S3'

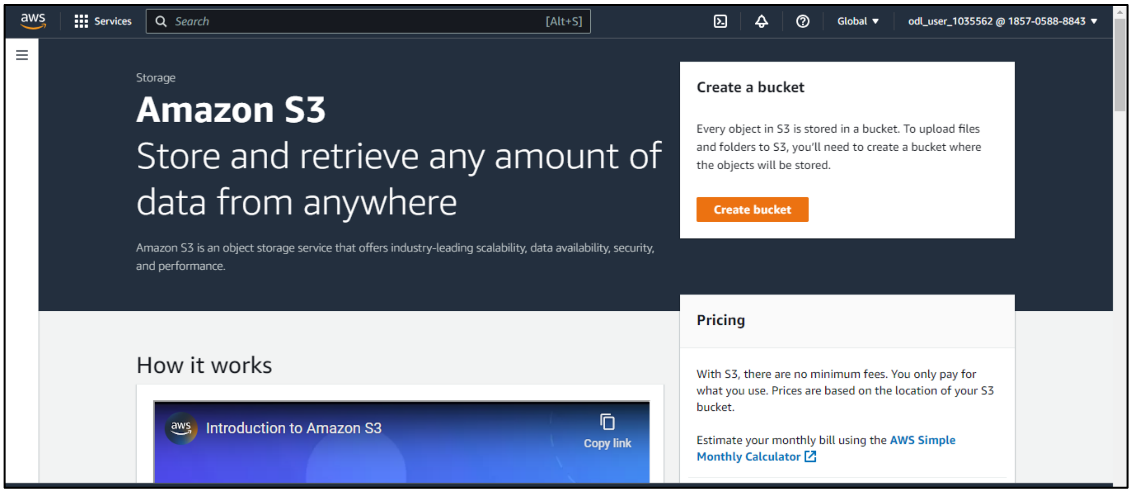
S3 — Scalable Storage in the Cloud

S3 Glacier — Archive Storage in the Cloud

Athena — Query Data in S3 using SQL

AWS Snow Family — Large Scale Data Transport

3.2 Click on **Create bucket**



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

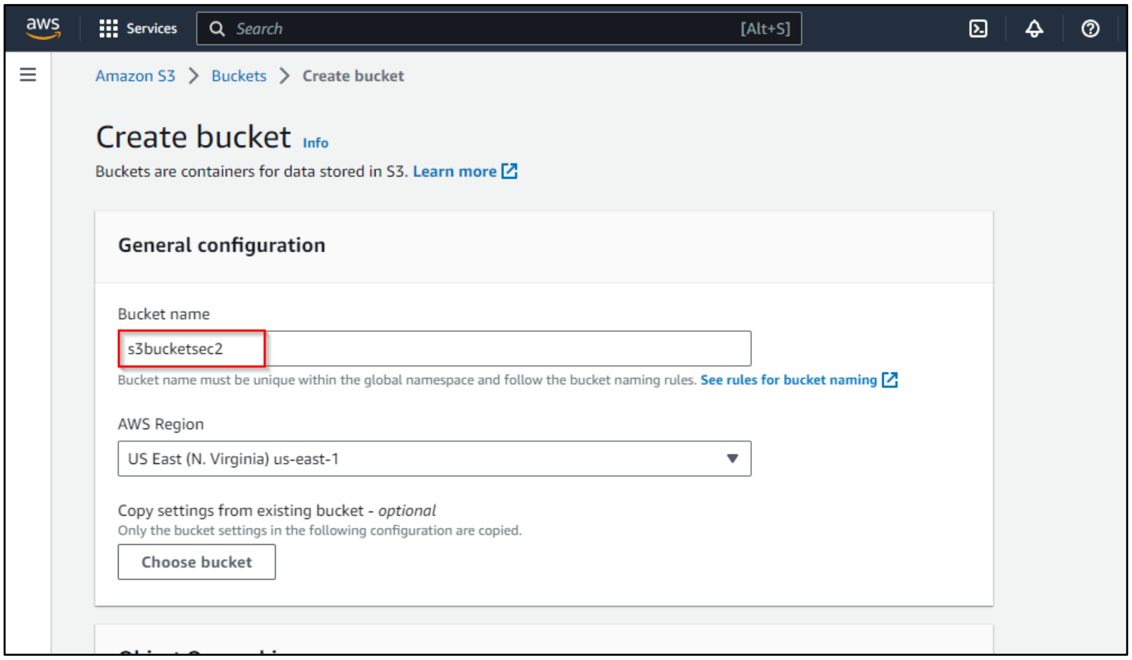
Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the **AWS Simple Monthly Calculator**

How it works

3.3 Name the bucket **s3bucketsec2,** and click on **Create bucket**



Create bucket

Buckets are containers for data stored in S3. **Learn more**

General configuration

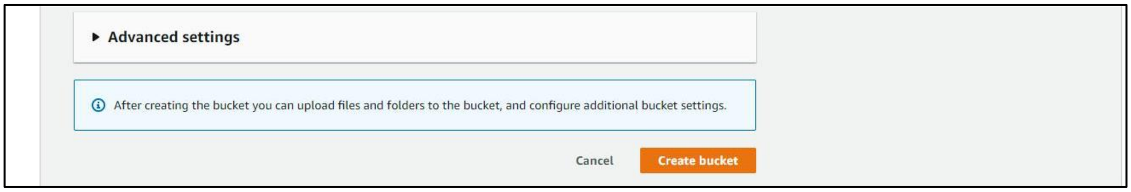
Bucket name: s3bucketsec2

Bucket name must be unique within the global namespace and follow the bucket naming rules. **See rules for bucket naming**

AWS Region: US East (N. Virginia) us-east-1

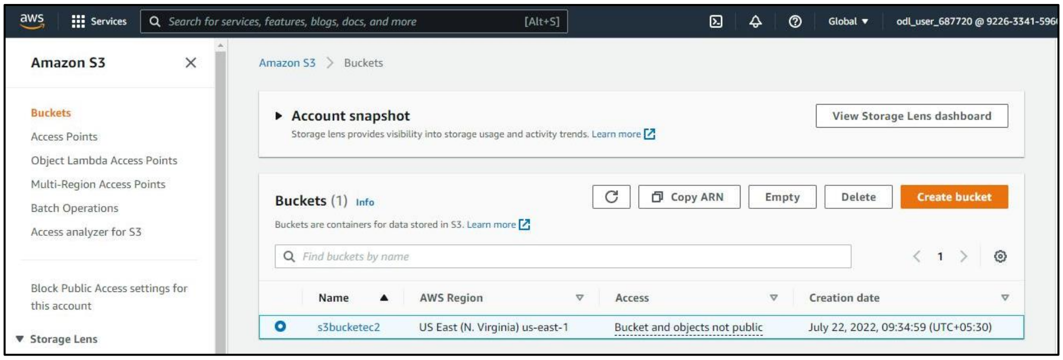
Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.



After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

3.4 Select the S3 bucket to verify


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
odl_user_687720 @ 9226-3341-596
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Amazon S3 > Buckets
View Storage Lens dashboard
Copy ARN
Empty
Delete
Create bucket
Find buckets by name

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

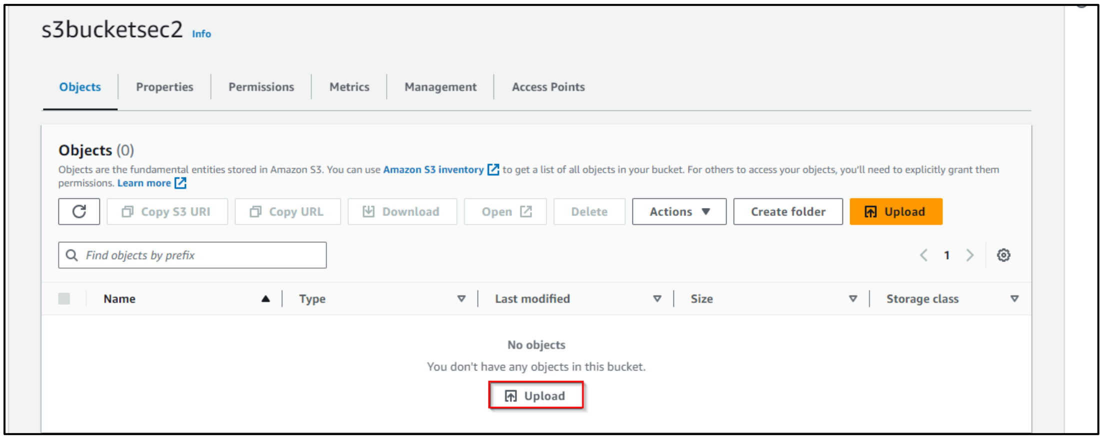
Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
s3bucketec2	US East (N. Virginia) us-east-1	Bucket and objects not public	July 22, 2022, 09:34:59 (UTC+05:30)

Note: Upload a **.txt** file to the S3 bucket.

3.5 Click on **Upload**

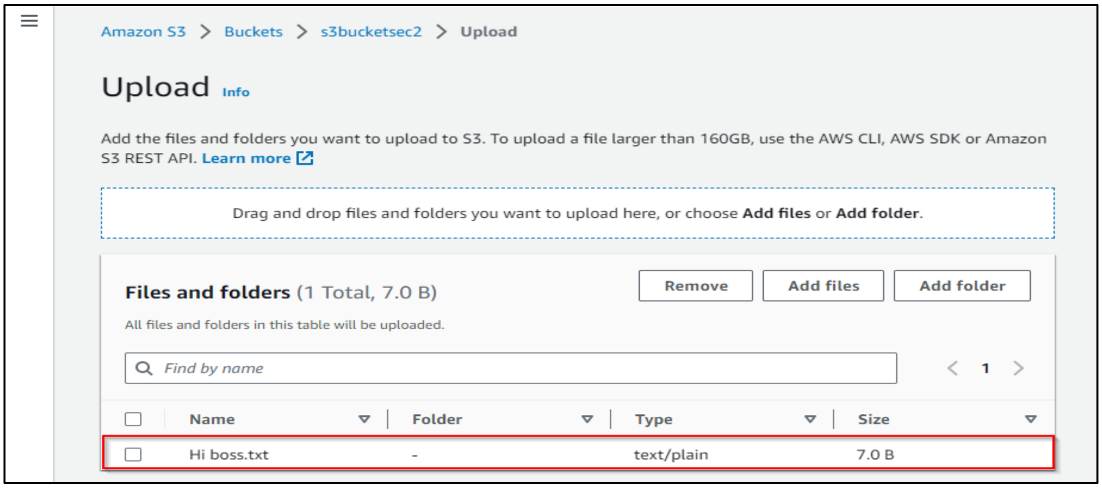


Objects (0)

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.



Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

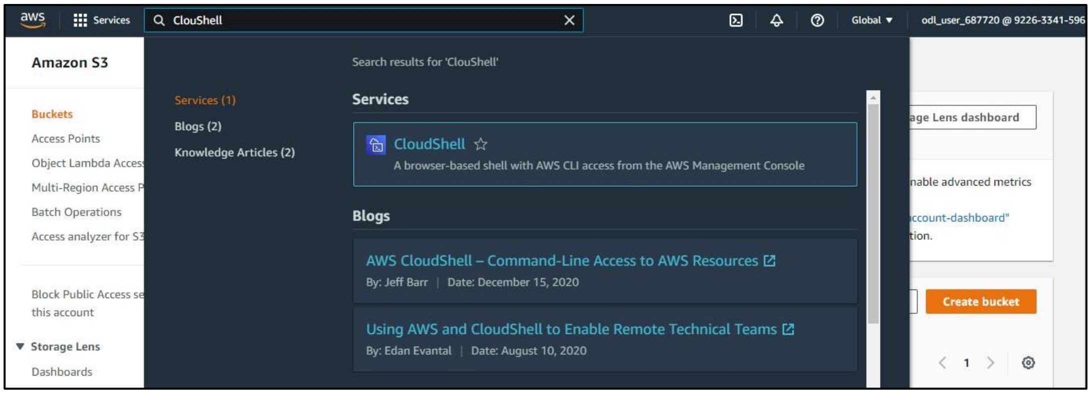
Files and folders (1 Total, 7.0 B)

All files and folders in this table will be uploaded.

Name	Folder	Type	Size
Hi boss.txt	-	text/plain	7.0 B

The file is uploaded successfully.

3.6 In the **IAM** dashboard, search and select **CloudShell**



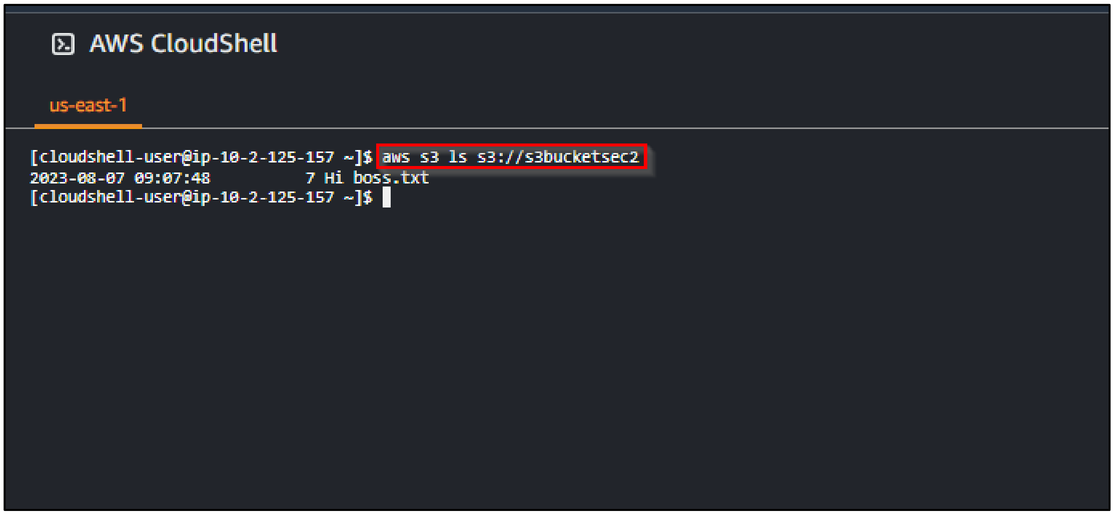
A browser-based shell with AWS CLI access from the AWS Management Console

AWS CloudShell – Command-Line Access to AWS Resources
By: Jeff Barr | Date: December 15, 2020

Using AWS and CloudShell to Enable Remote Technical Teams
By: Edan Evantal | Date: August 10, 2020

3.7 Enter the following command:

aws s3 ls s3://s3bucketec2



```
[cloudshell-user@ip-10-2-125-157 ~]$ aws s3 ls s3://s3bucketsec2
2023-08-07 09:07:48          7 Hi boss.txt
[cloudshell-user@ip-10-2-125-157 ~]$
```

Note: Replace **s3bucketsec2** with your bucket name

By following these steps, you have demonstrated how an EC2 instance can securely access S3 services using IAM roles.