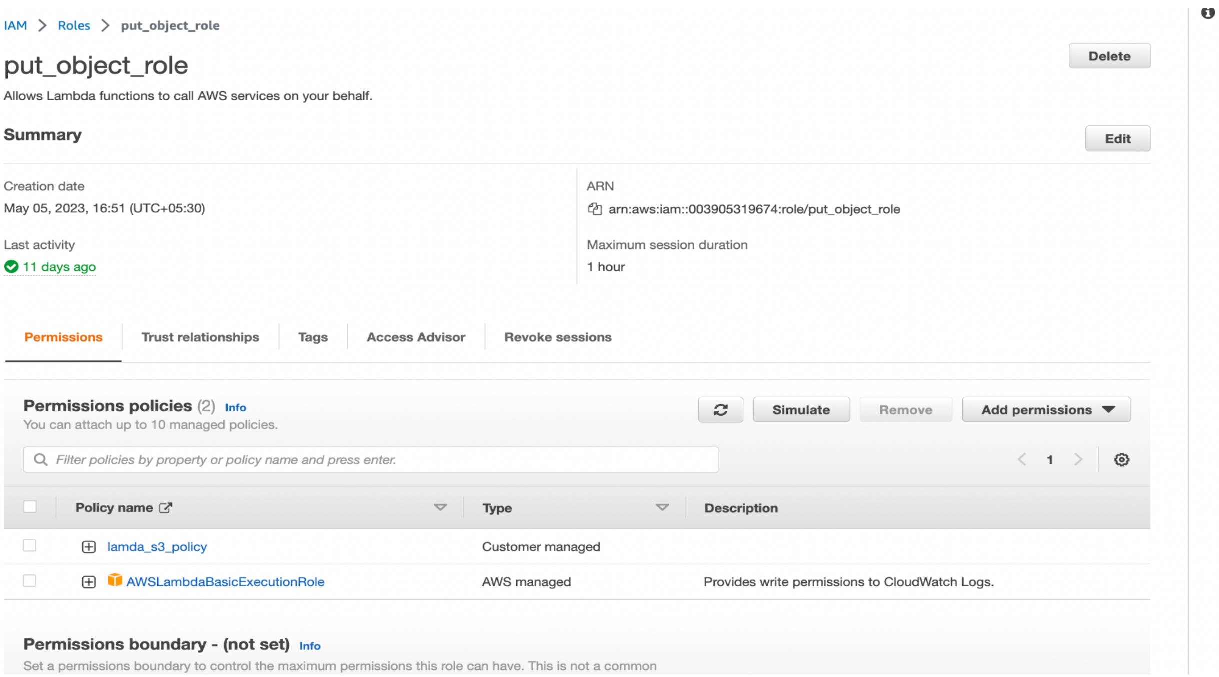
TASK - 1

1. Create an IAM role with S3 full access.

- Search IAM in AWS Console.
- Under the Access Management section click on the Roles section.
- Click on Create Role and select AWS Service and EC2.



IAM > Roles > put_object_role

put_object_role

Allows Lambda functions to call AWS services on your behalf.

Summary

Creation date
May 05, 2023, 16:51 (UTC+05:30)

ARN
arn:aws:iam::003905319674:role/put_object_role

Last activity
✓ 11 days ago

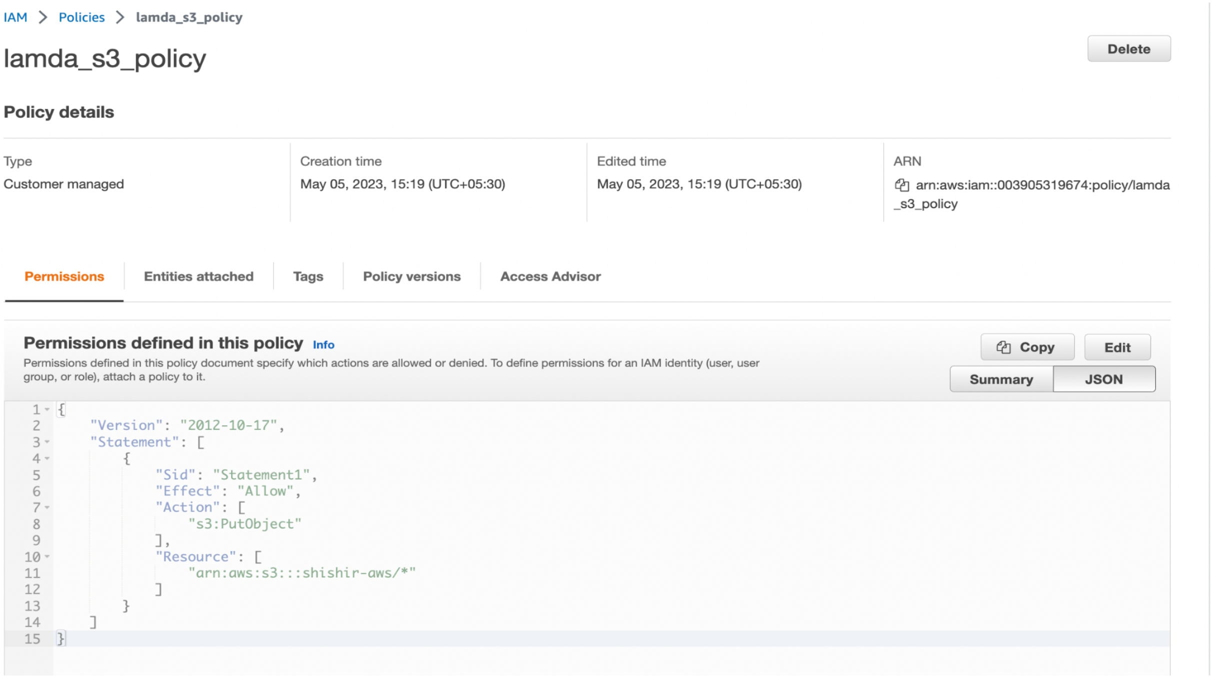
Maximum session duration
1 hour

Permissions policies (2) Info
You can attach up to 10 managed policies.

□	Policy name	Type	Description
□	lamda_s3_policy	Customer managed	
□	AWSLambdaBasicExecutionRole	AWS managed	Provides write permissions to CloudWatch Logs.

Permissions boundary - (not set) Info
Set a permissions boundary to control the maximum permissions this role can have. This is not a common

- In lambda_s3_policy, attach put object permission for your bucket.
- Add your role name and click on create role



IAM > Policies > lamda_s3_policy

lamda_s3_policy

Policy details

Type
Customer managed

Creation time
May 05, 2023, 15:19 (UTC+05:30)

Edited time
May 05, 2023, 15:19 (UTC+05:30)

ARN
arn:aws:iam::003905319674:policy/lamda_s3_policy

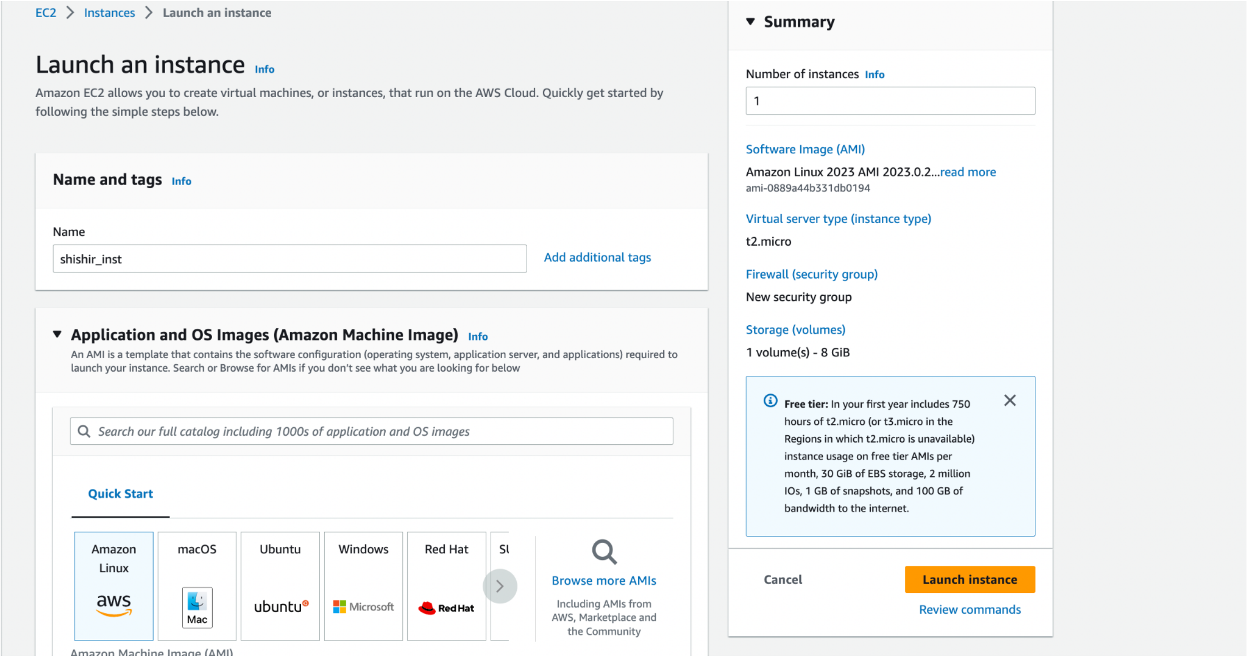
Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::shishir-aws/*"
            ]
        }
    ]
}
```

2. Create an EC2 instance with the above role.

- Search EC2 in AWS Console and click on Launch Instance.
- Give the name of your instance and select the below configuration.
- Under advance details select the IAM role created and launch the instance



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: shishir_inst

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Summary

Number of instances Info: 1

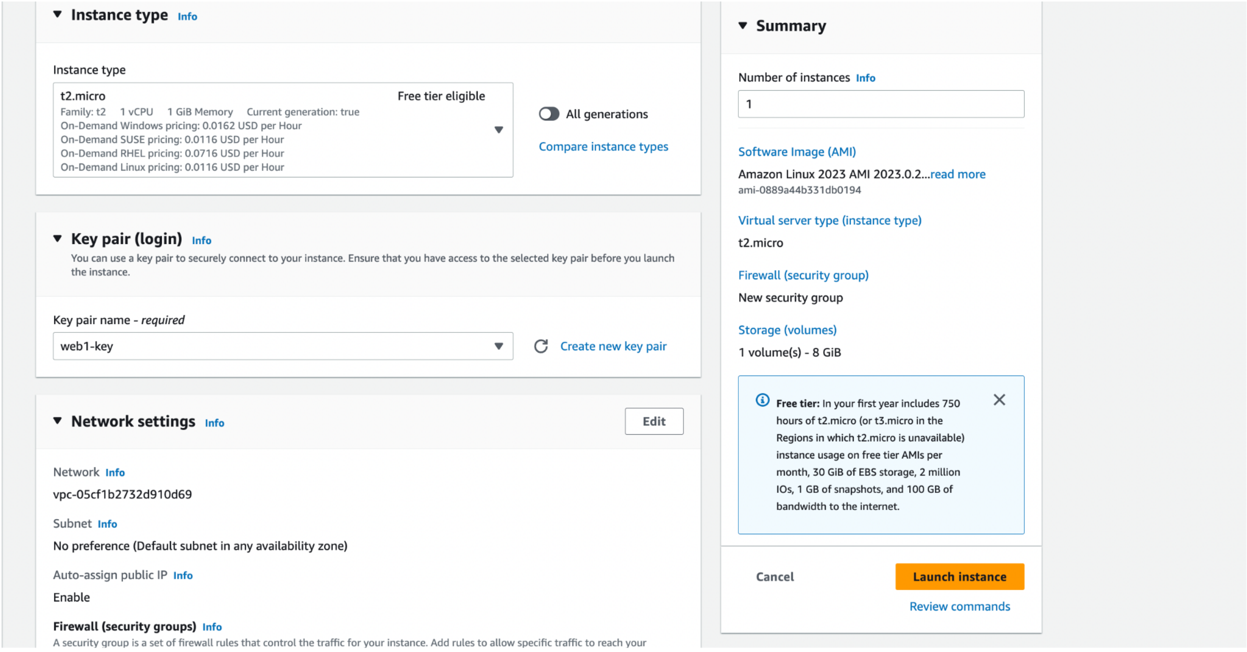
Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...read more
ami-0889a44b331db0194

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



Instance type Info

Instance type: t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: web1-key

Network settings Info

Network Info: vpc-05cf1b2732d910d69

Subnet Info: No preference (Default subnet in any availability zone)

Auto-assign public IP Info: Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your

Summary

Number of instances Info: 1

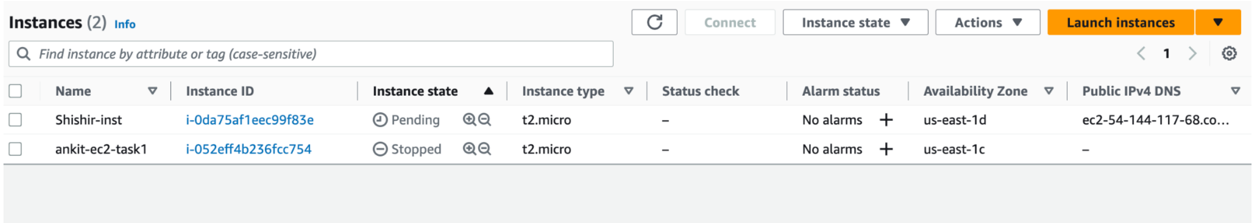
Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...read more
ami-0889a44b331db0194

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



Instances (2) Info

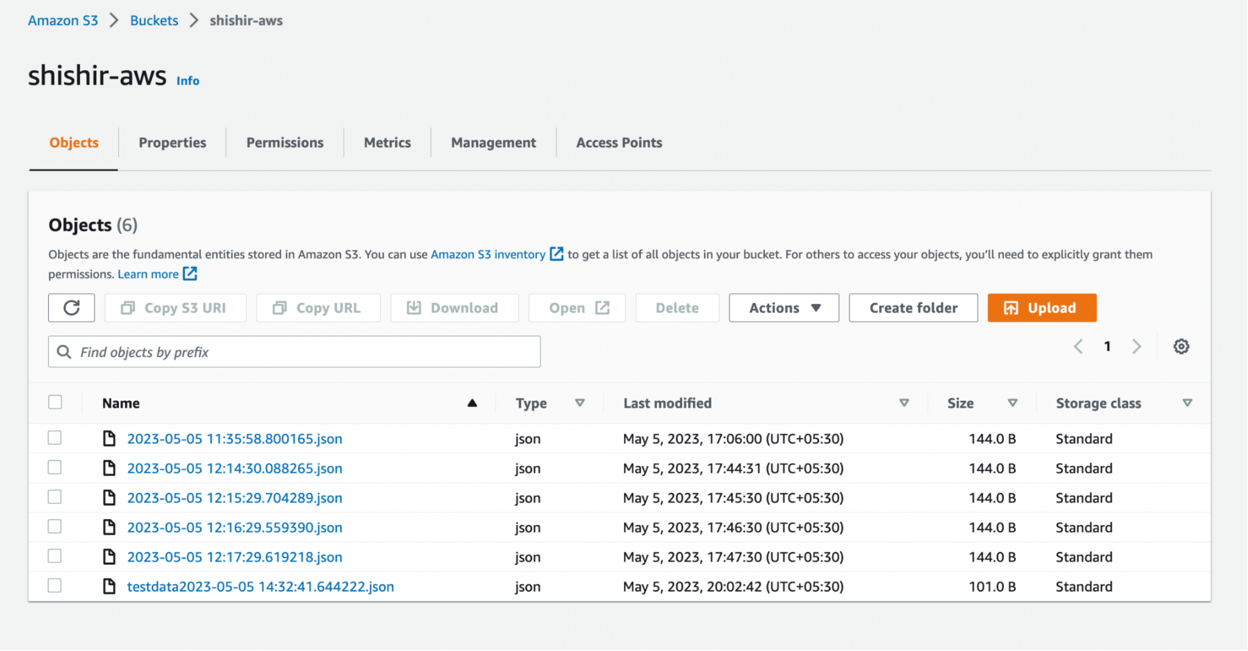
Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Shishir-inst	i-0da75af1eec99f83e	Pending	t2.micro	–	No alarms	us-east-1d	ec2-54-144-117-68.co…
ankit-ec2-task1	i-052eff4b236fcc754	Stopped	t2.micro	–	No alarms	us-east-1c	–

3. Create a bucket from AWS CLI

- Open your terminal and type aws configure.
- Type your access key ID and password and type your region name.
- Type the below command and mention your unique bucket name and your region.

CLI COMMAND: aws s3api create-bucket –bucket shishir-aws –region us-east-1



Objects (6)

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

□	Name ▲	Type	Last modified	Size	Storage class
□	2023-05-05 11:35:58.800165.json	json	May 5, 2023, 17:06:00 (UTC+05:30)	144.0 B	Standard
□	2023-05-05 12:14:30.088265.json	json	May 5, 2023, 17:44:31 (UTC+05:30)	144.0 B	Standard
□	2023-05-05 12:15:29.704289.json	json	May 5, 2023, 17:45:30 (UTC+05:30)	144.0 B	Standard
□	2023-05-05 12:16:29.559390.json	json	May 5, 2023, 17:46:30 (UTC+05:30)	144.0 B	Standard
□	2023-05-05 12:17:29.619218.json	json	May 5, 2023, 17:47:30 (UTC+05:30)	144.0 B	Standard
□	testdata2023-05-05 14:32:41.644222.json	json	May 5, 2023, 20:02:42 (UTC+05:30)	101.0 B	Standard