Multiple Choice Questions (MCQs) - Answers Kobi Kuzi

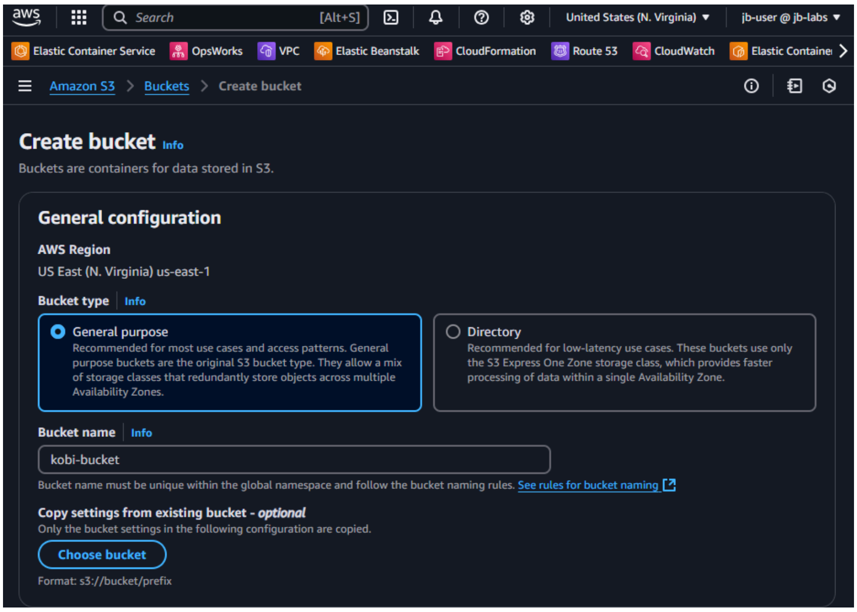
1. C
2. A
3. C
4. A
5. B
6. A
7. A
8. B
9. B
10. C
11. A
12. AWS Landing Zone is a well-architected, multi-account AWS environment that is scalable and secure. They help using the Multi-Account framework which provides the highest level of resource and security isolation.
13. AWS WAF protects web applications from common attacks using a set of rules for inbound and outbound to create a more safe usage for our web application.
14. AWS Snowball is a hardware which can contain large sets of data which we want to transfer (210 TB of usable storage capacity) .
15. The key differences between AWS Backup and snapshot is that AWS Backup is a comprehensive and flexible copy of your cloud workloads. On the other end snapshots are a point in time copy of our cloud workload(usually a copy of an EBS of a certain EC2). snapshots are more complex to maintain and more costly.
16. AWS Shield responds to dedicated DDoS attacks by creating, evaluating and deploying a custom AWS WAF set of rules.
17. Both are used to connect multiple VPCs. VPC Peering is a connection between two VPCs that enables you to route traffic between them privately. On the other end AWS Transit Gateway is a fully managed service that connects VPCs and On-Premises networks through a central hub without relying on numerous point-to-point connections or Transit VPC.
18. AWS Step Functions is a visual workflow service that helps developers use AWS services to build distributed applications, automate processes, orchestrate microservices, and create data and machine learning (ML) pipelines. One of the ways it helps developers with workflow automation is iterate over and process large data-sets.

19. The AWS Control Tower takes away the hustle of setting up different teams. With the AWS control tower, you can set up a landing zone, a multi-account environment for simpler migration. AWS Control Tower uses other services such as Organizations, Service Catalog, and Config which helps with managing teams, users, etc.
20. AWS Outposts rack is a fully managed service that extends AWS infrastructure, services, APIs, and tools on premises for a truly consistent hybrid experience. The significance is to automatically translate high volumes of user-generated content, such as social media feed stories, profile descriptions, and comments, in real time. Set up a consistent hybrid cloud architecture to process data on premises due to cost, size, bandwidth, or timing constraints. Control where your applications run and where your data resides. Maintain data control on premises to meet legal, industry, or contractual requirements. Support on-premises hybrid cloud migration of applications with local system interdependencies or applications with data residency requirements.
21. EBS: high performance, per-instance block storage. EFS: scalable file storage for multiple EC2 instances. S3: object storage for complex queries and archived data.

Section 2: Hands-on UI-Based Questions

1. S3 Bucket Configuration:

To create an S3 with enabling Bucket version all you need to do is to enable it (could enable after the creation of the the S3 bucket)



Create bucket

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name

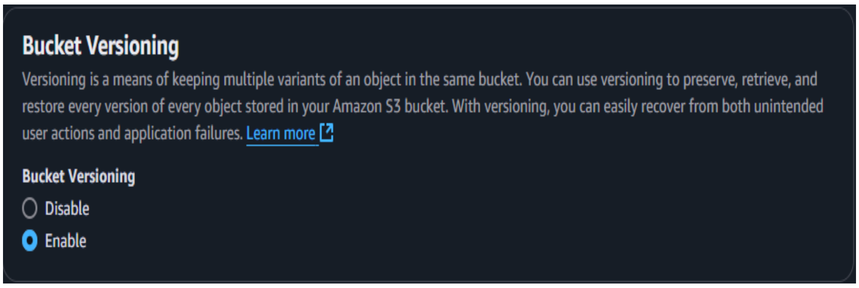
kobi-bucket

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

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

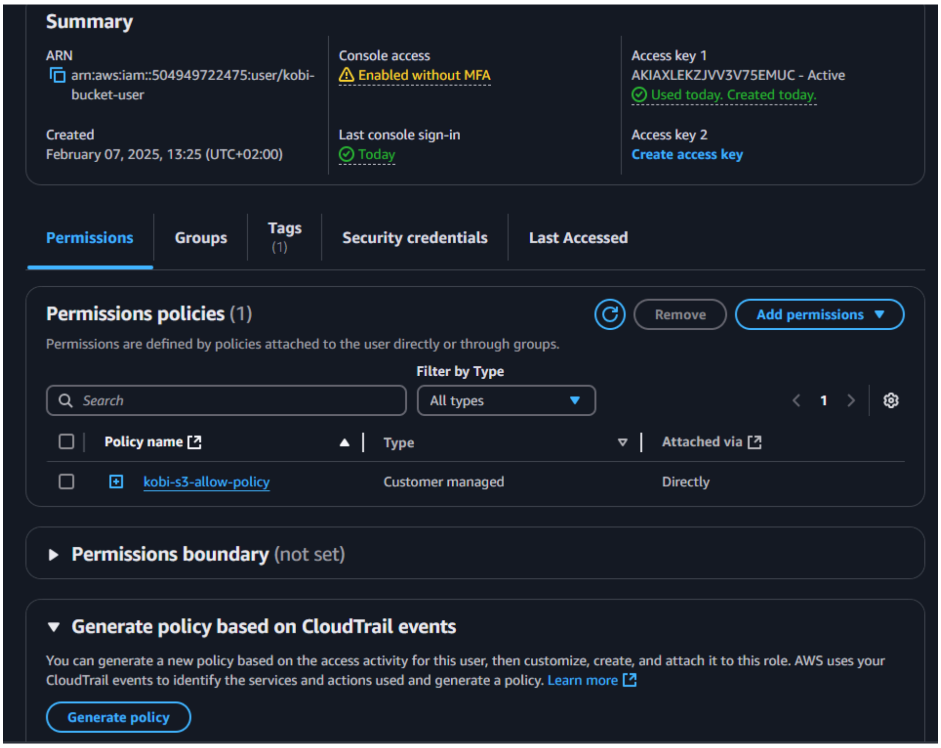
Bucket Versioning

○ Disable

● Enable

IAM policy created after the IAM user:

Created an IAM user named kobi-bucket-user and the policy named kobi-s3-allow-policy shown under where i give access to Get, Put, Delete of certain objects and gives the user the possibilities to watch only his buckets.



Summary

ARN
arn:aws:iam::504949722475:user/kobi-bucket-user

Created
February 07, 2025, 13:25 (UTC+02:00)

Console access
Enabled without MFA

Last console sign-in
Today

Access key 1
AKIAXLEKZJVV3V75EMUC - Active
Used today. Created today.

Access key 2
Create access key

Permissions policies (1)

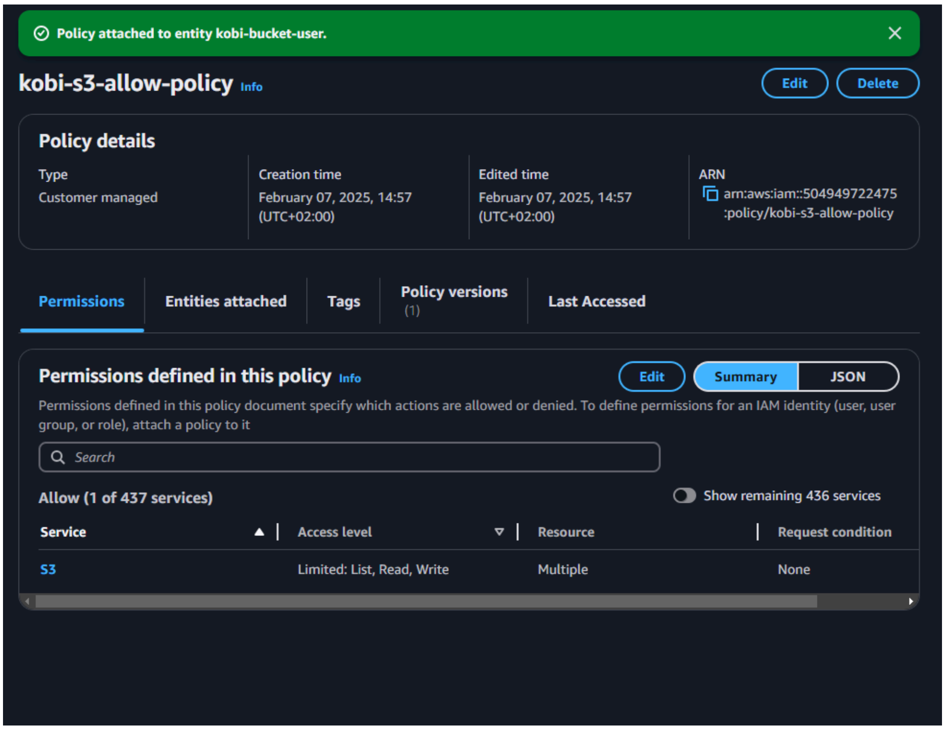
Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type	Attached via
□	kobi-s3-allow-policy	Customer managed	Directly

▶ **Permissions boundary** (not set)

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more



Policy attached to entity kobi-bucket-user.

kobi-s3-allow-policy

Policy details

Type	Creation time	Edited time	ARN
Customer managed	February 07, 2025, 14:57 (UTC+02:00)	February 07, 2025, 14:57 (UTC+02:00)	arn:aws:iam::504949722475:policy/kobi-s3-allow-policy

Permissions defined in this policy

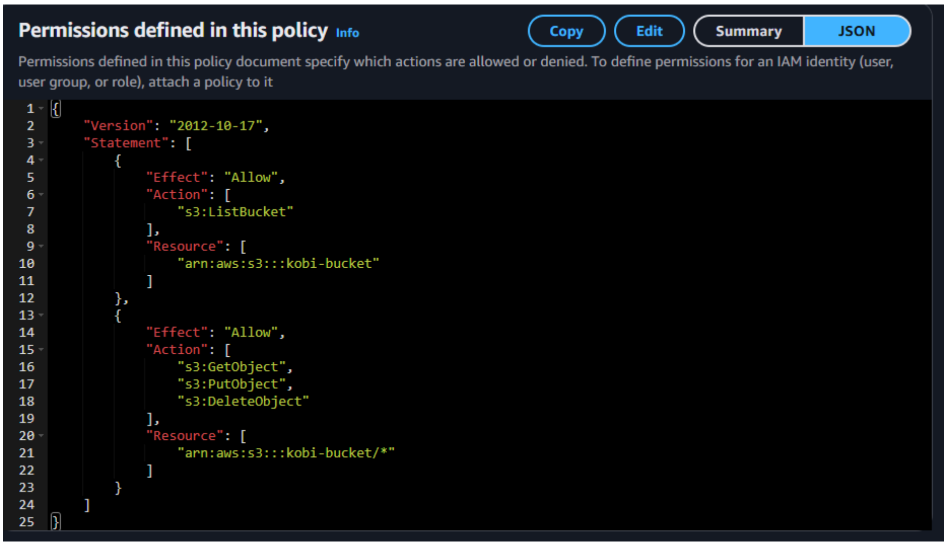
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 437 services)

Show remaining 436 services

Service	Access level	Resource	Request condition
S3	Limited: List, Read, Write	Multiple	None

The bucket policy for traffic which allows the same as the user AMI policies:

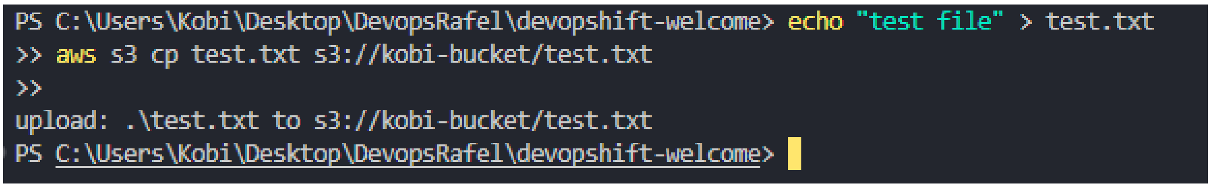


Permissions defined in this policy

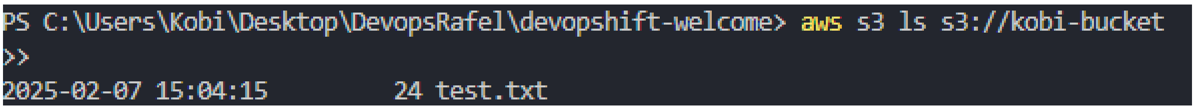
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::kobi-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::kobi-bucket/*"
            ]
        }
    ]
}
```

Showing an Addition of a new file to my bucket using the aws cli:

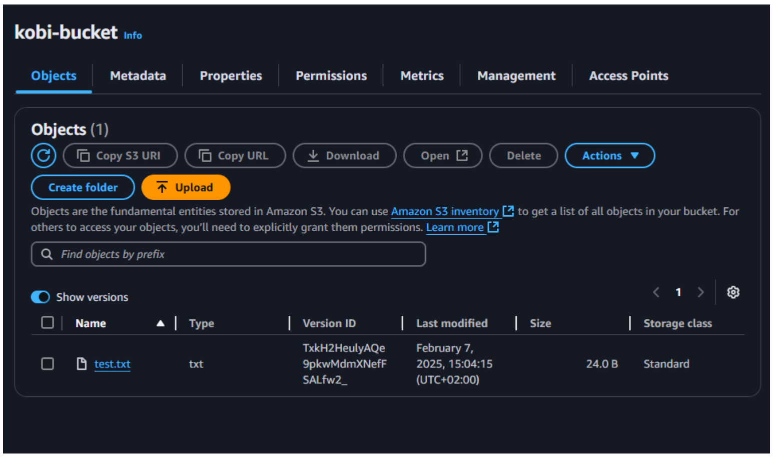


```
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> echo "test file" > test.txt
>> aws s3 cp test.txt s3://kobi-bucket/test.txt
>>
upload: .\test.txt to s3://kobi-bucket/test.txt
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome>
```



```
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> aws s3 ls s3://kobi-bucket
>>
2025-02-07 15:04:15         24 test.txt
```

in AWS UI:

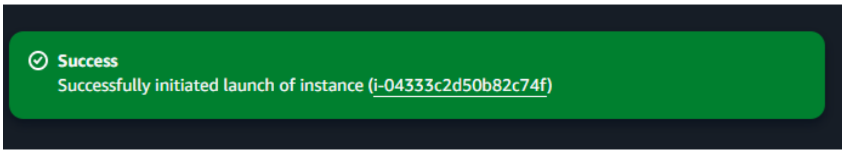


Objects (1)

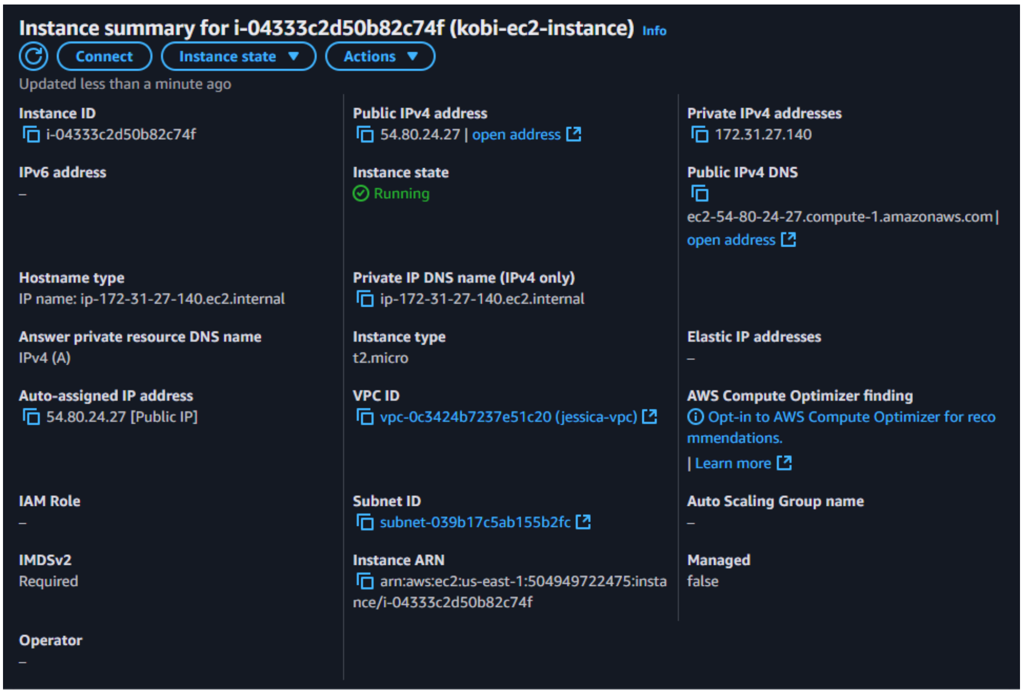
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Version ID	Last modified	Size	Storage class
□	test.txt	txt	TxkH2HeulyAQe9pkwMdmXNefFSALfw2_	February 7, 2025, 15:04:15 (UTC+02:00)	24.0 B	Standard

2. Launch an EC2 Instance:



Success
Successfully initiated launch of instance (i-04333c2d50b82c74f)



Instance summary for i-04333c2d50b82c74f (kobi-ec2-instance)

Updated less than a minute ago

Instance ID
i-04333c2d50b82c74f

IPv6 address
–

Hostname type
IP name: ip-172-31-27-140.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
54.80.24.27 [Public IP]

IAM Role
–

IMDSv2
Required

Operator
–

Public IPv4 address
54.80.24.27 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-27-140.ec2.internal

Instance type
t2.micro

VPC ID
vpc-0c3424b7237e51c20 (jessica-vpc)

Subnet ID
subnet-039b17c5ab155b2fc

Instance ARN
arn:aws:ec2:us-east-1:504949722475:instance/i-04333c2d50b82c74f

Private IPv4 addresses
172.31.27.140

Public IPv4 DNS
ec2-54-80-24-27.compute-1.amazonaws.com | open address

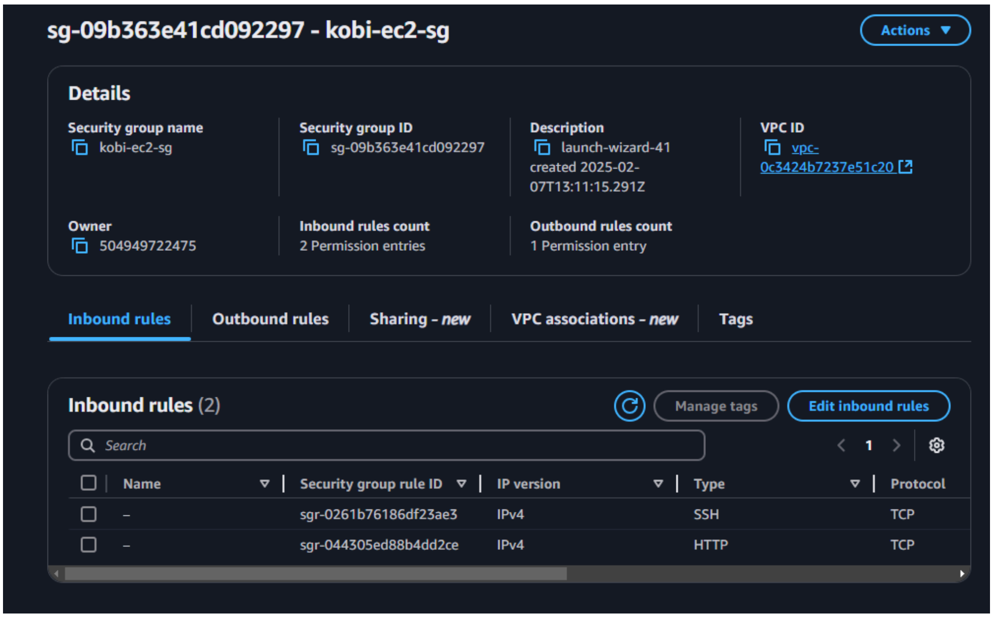
Elastic IP addresses
–

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

Managed
false

the security group named kobi-ec2-sg:



sg-09b363e41cd092297 - kobi-ec2-sg

Details

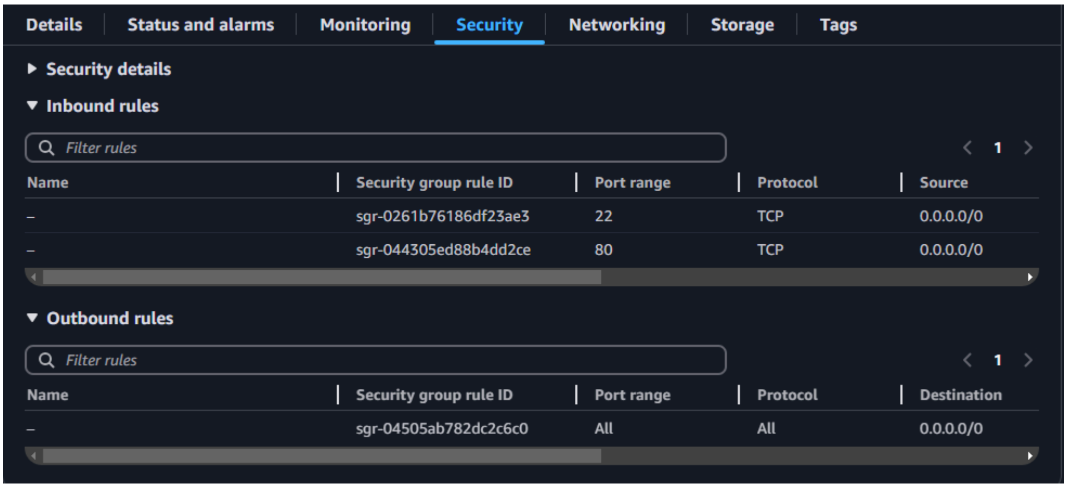
Security group name	Security group ID	Description	VPC ID
kobi-ec2-sg	sg-09b363e41cd092297	launch-wizard-41 created 2025-02-07T13:11:15.291Z	vpc-0c3424b7237e51c20

Owner	Inbound rules count	Outbound rules count
504949722475	2 Permission entries	1 Permission entry

Inbound rules (2)

☐	Name	Security group rule ID	IP version	Type	Protocol
☐	–	sgr-0261b76186df23ae3	IPv4	SSH	TCP
☐	–	sgr-044305ed88b4dd2ce	IPv4	HTTP	TCP

Security group rules inside my own instance:



▶ Security details

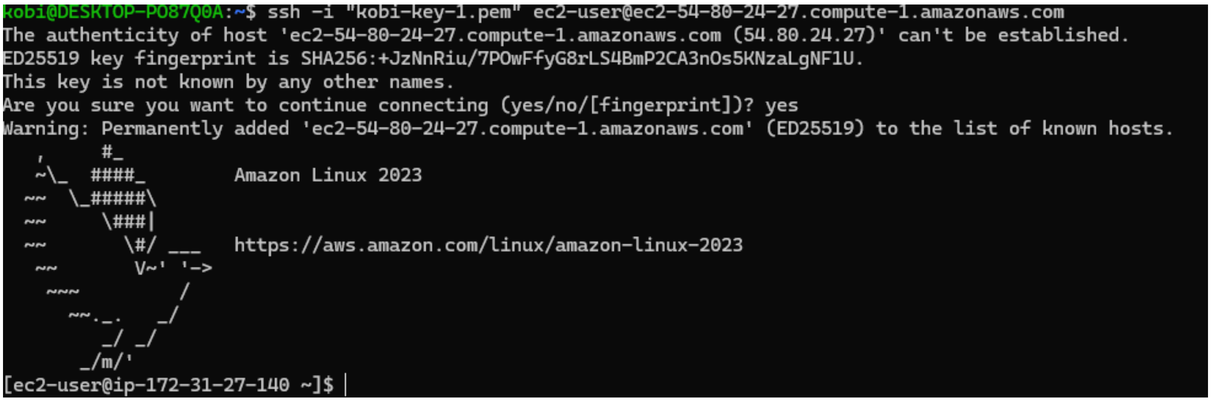
▼ Inbound rules

Name	Security group rule ID	Port range	Protocol	Source
–	sgr-0261b76186df23ae3	22	TCP	0.0.0.0/0
–	sgr-044305ed88b4dd2ce	80	TCP	0.0.0.0/0

▼ Outbound rules

Name	Security group rule ID	Port range	Protocol	Destination
–	sgr-04505ab782dc2c6c0	All	All	0.0.0.0/0

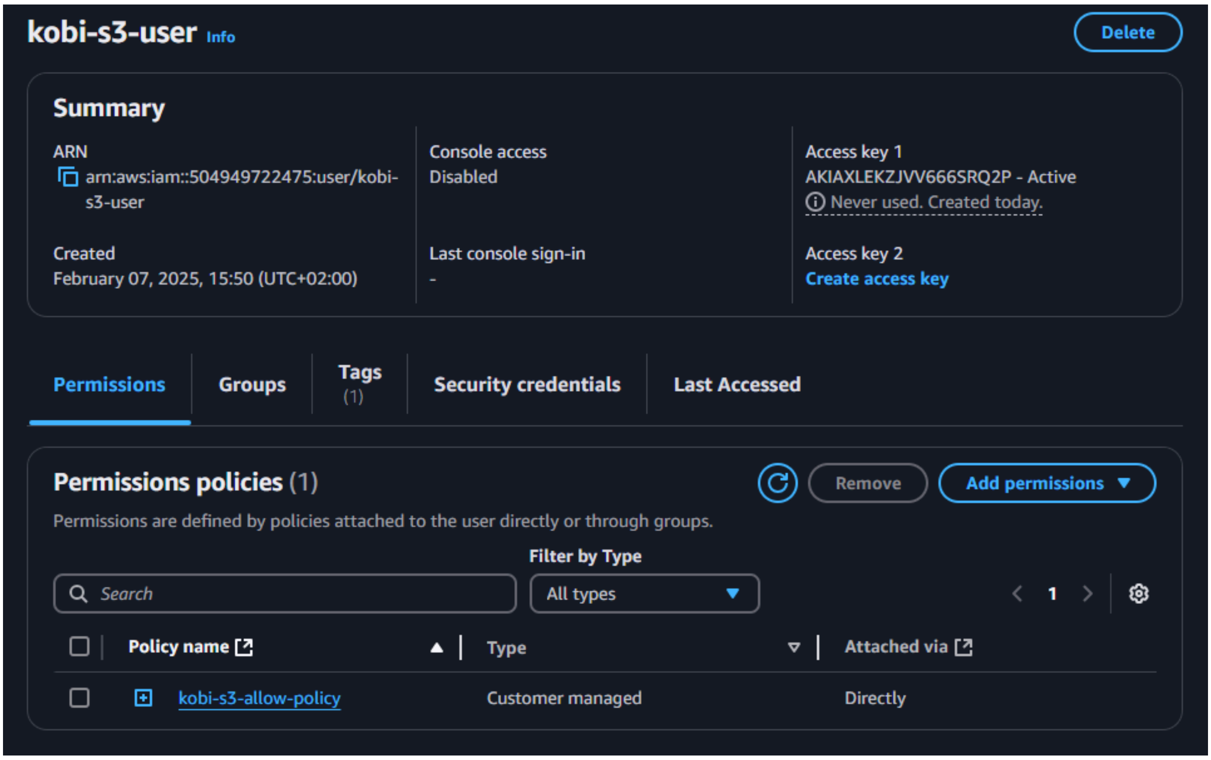
Using SSH to log in the machine:



```
kobi@DESKTOP-PO87Q0A:~$ ssh -i "kobi-key-1.pem" ec2-user@ec2-54-80-24-27.compute-1.amazonaws.com
The authenticity of host 'ec2-54-80-24-27.compute-1.amazonaws.com (54.80.24.27)' can't be established.
ED25519 key fingerprint is SHA256:+JzNnRiu/7POwFfyG8rLS4BmP2CA3nOs5KNzaLgNF1U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-80-24-27.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-27-140 ~]$ |
```

3. Configure an IAM User with S3 Access:

Because we already created a new user we will create another new one named kobi-s3-user and attach the Policy we already created in step one to this user to:



Summary

ARN
arn:aws:iam::504949722475:user/kobi-s3-user

Console access
Disabled

Access key 1
AKIAXLEKZJVV666SRQ2P - Active
Never used. Created today.

Created
February 07, 2025, 15:50 (UTC+02:00)

Last console sign-in
-

Access key 2
Create access key

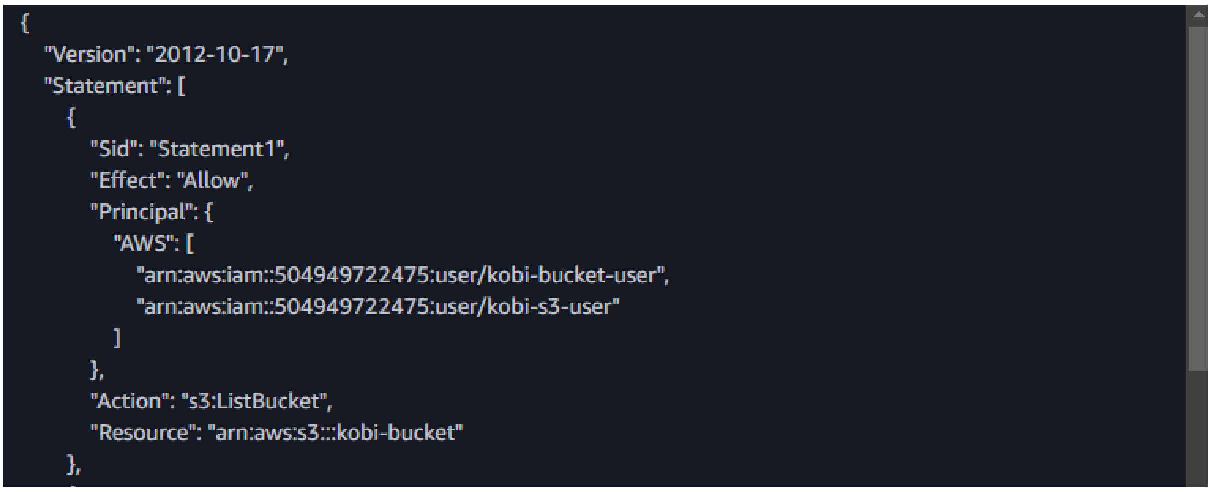
Permissions policies (1)

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

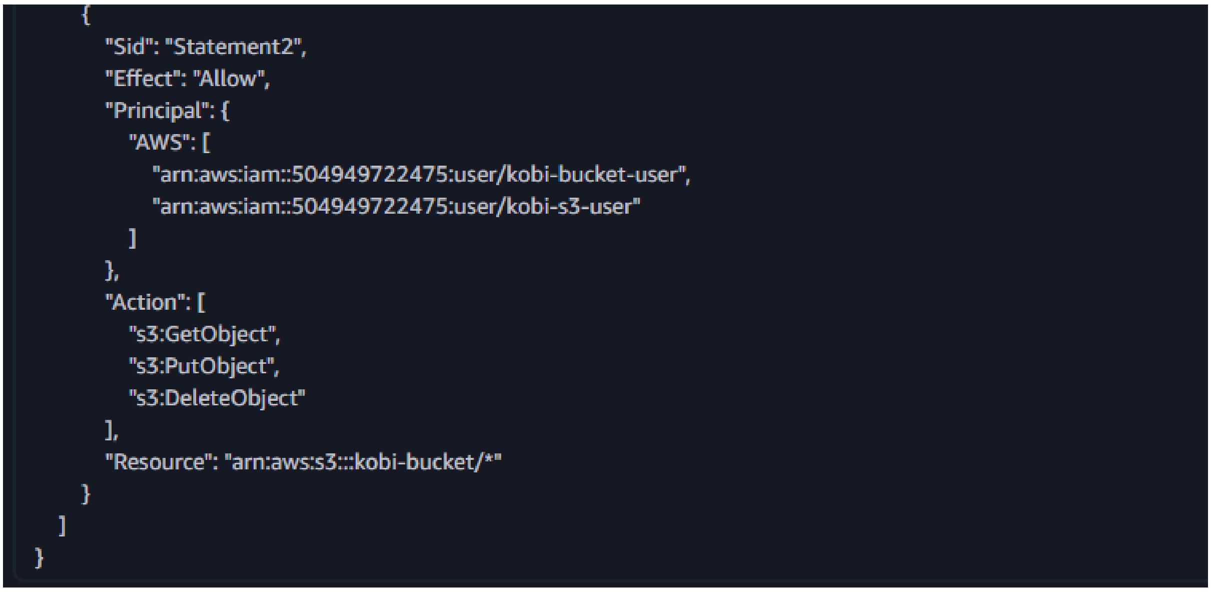
Filter by Type

□	Policy name	Type	Attached via
□	kobi-s3-allow-policy	Customer managed	Directly

We will update the new S3 bucket policy to allow the new user to do the same actions as the other user we created in Step 1:

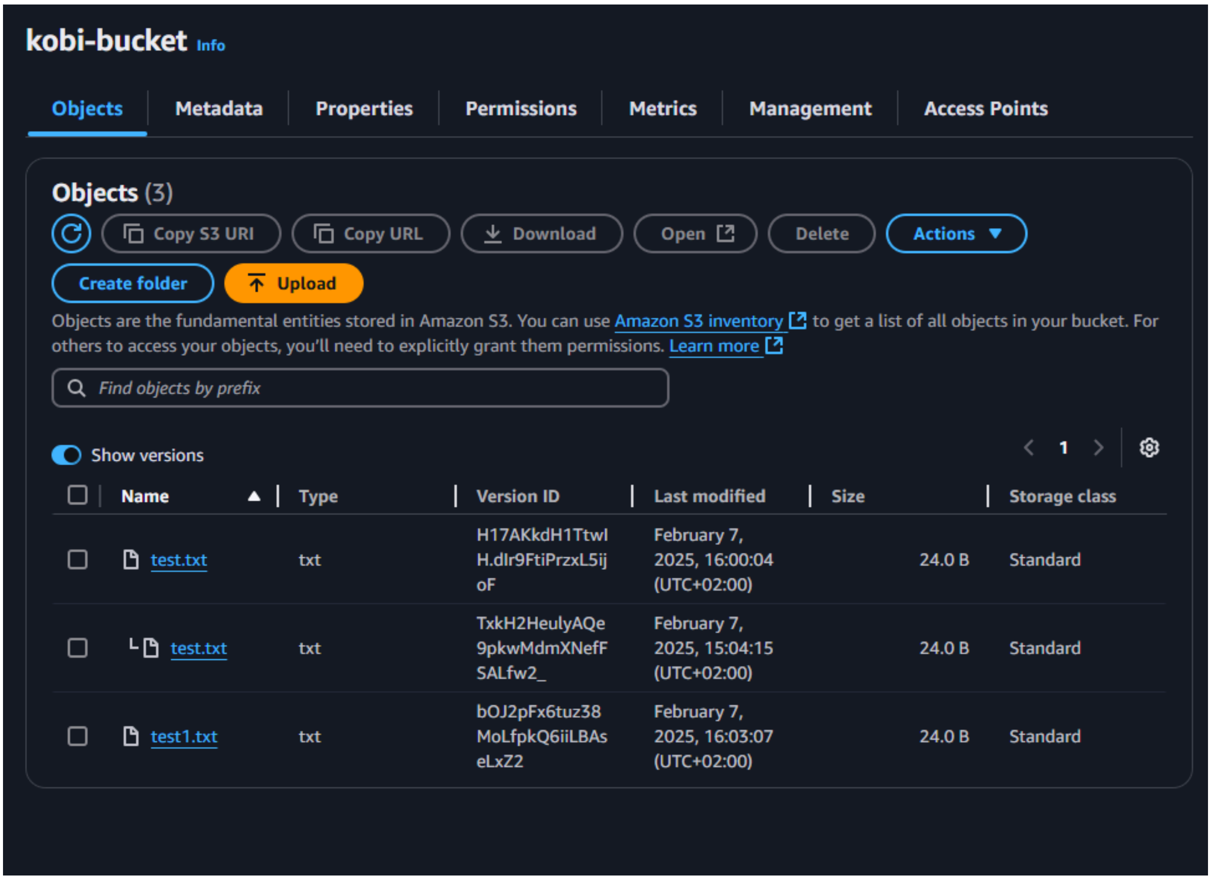


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::504949722475:user/kobi-bucket-user",
          "arn:aws:iam::504949722475:user/kobi-s3-user"
        ]
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::kobi-bucket"
    },
```



```
      {
        "Sid": "Statement2",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::504949722475:user/kobi-bucket-user",
            "arn:aws:iam::504949722475:user/kobi-s3-user"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:PutObject",
          "s3:DeleteObject"
        ],
        "Resource": "arn:aws:s3:::kobi-bucket/*"
      }
    ]
  }
```

we can see we inserted 2 different files using the new user through our aws cli:

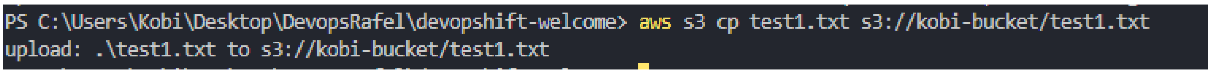


Objects (3)

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

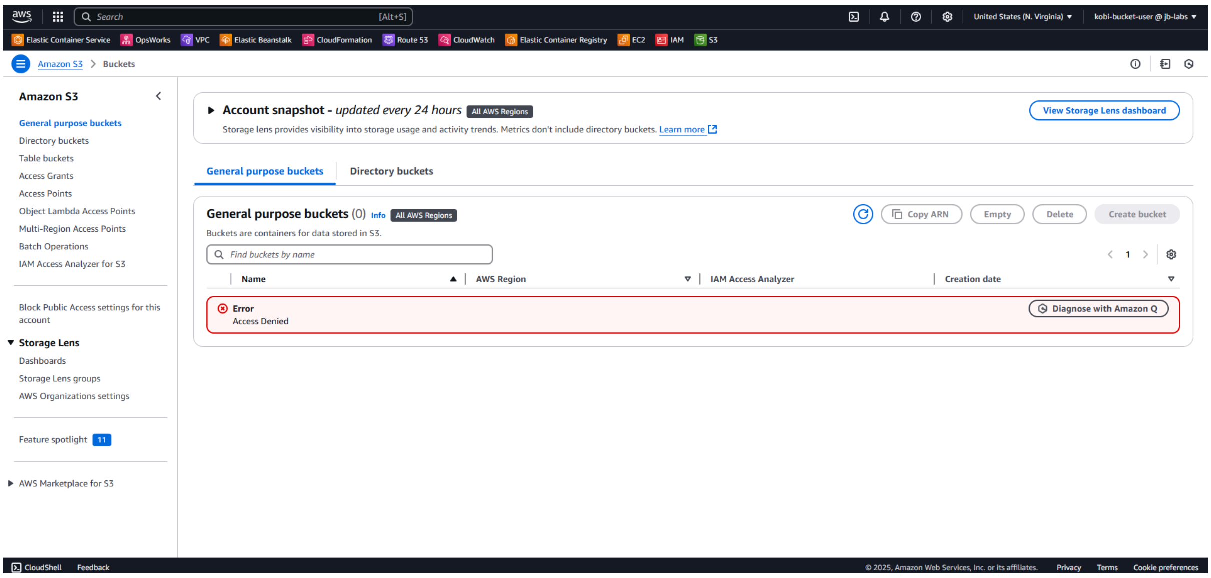
□	Name	Type	Version ID	Last modified	Size	Storage class
□	test.txt	txt	H17AKkdH1TtwlH.dlr9FtiPrzxL5ijoF	February 7, 2025, 16:00:04 (UTC+02:00)	24.0 B	Standard
□	└ test.txt	txt	TxkH2HeulyAQe9pkwMdmXNefFSALfw2_	February 7, 2025, 15:04:15 (UTC+02:00)	24.0 B	Standard
□	test1.txt	txt	bOJ2pFx6tuz38MoLfpkQ6iiLBAseLxZ2	February 7, 2025, 16:03:07 (UTC+02:00)	24.0 B	Standard

To Verify we have the correct permissions we can log in to the user using the UI or use the cred to try and upload/delete an object from the bucket in this example I added to kobi-bucket another text file named test1.txt



```
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> aws s3 cp test1.txt s3://kobi-bucket/test1.txt
upload: .\test1.txt to s3://kobi-bucket/test1.txt
```

we can see that if we try to use our user (kobi-bucket-user) and see our all of our s3 buckets it is not possible:



Account snapshot - *updated every 24 hours* All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more

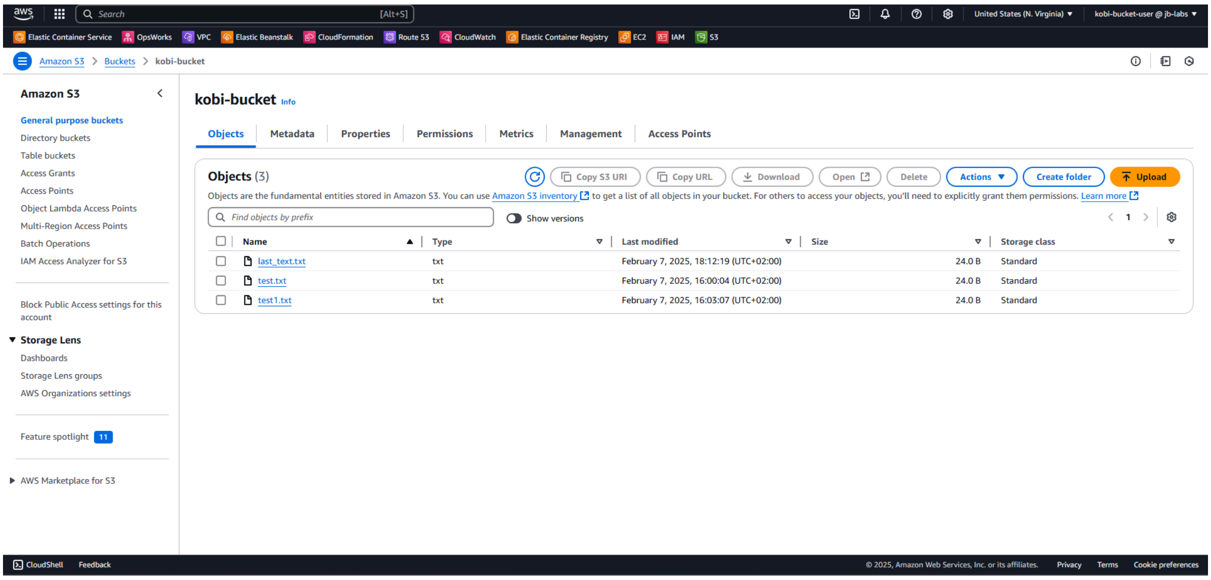
General purpose buckets (0) Info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date

Error
Access Denied

But if we want to see a certain bucket (our bucket named kobi-bucket) we could see him using this url (https://us-east-1.console.aws.amazon.com/s3/buckets/kobi-bucket?region=us-east-1&tab=objects&bucketType=general):



kobi-bucket Info

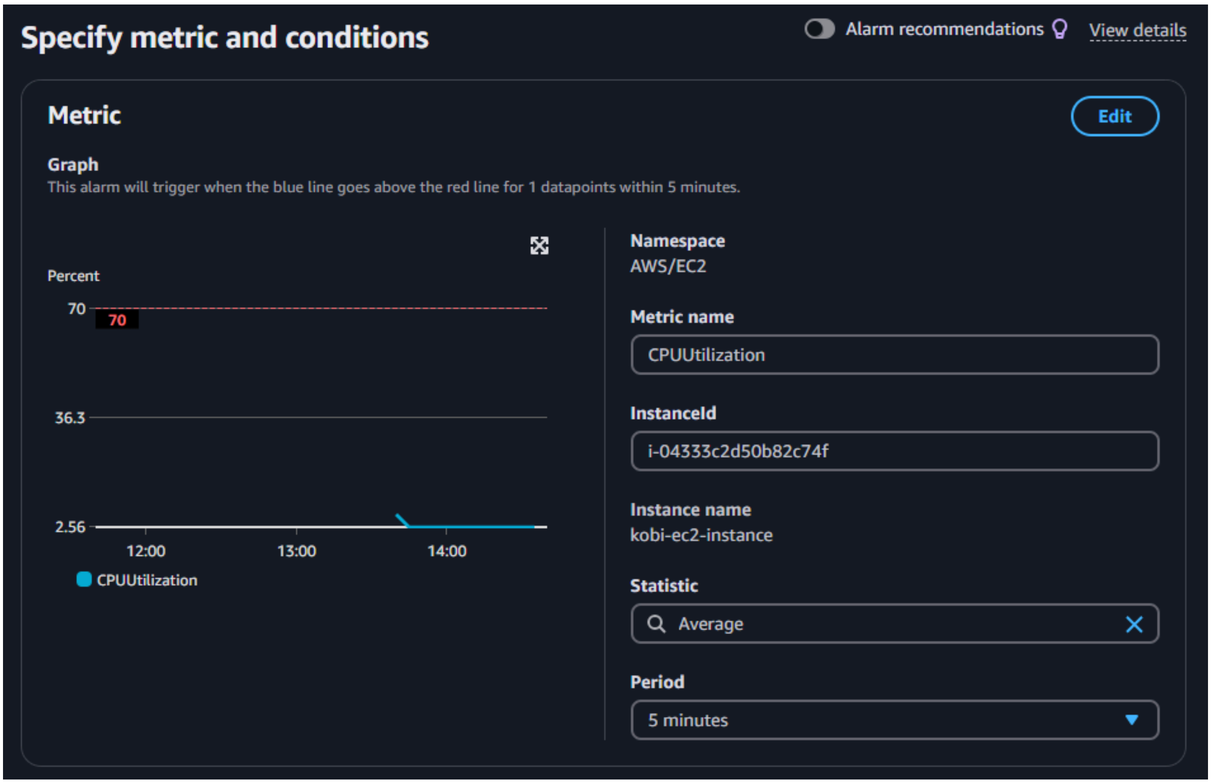
Objects (3)

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
□	last_text.txt	txt	February 7, 2025, 18:12:19 (UTC+02:00)	24.0 B	Standard
□	test.txt	txt	February 7, 2025, 16:00:04 (UTC+02:00)	24.0 B	Standard
□	test1.txt	txt	February 7, 2025, 16:03:07 (UTC+02:00)	24.0 B	Standard

4. Set Up a CloudWatch Alarm:

in this section i created an alarm named kobi-high-cpu-alarms which will perform an action of sending a notification to my email using the topic "kobi-ec2-topic-alarm" whenever our cpu usage is over 70% for five min



Specify metric and conditions

Alarm recommendations View details

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Namespace
AWS/EC2

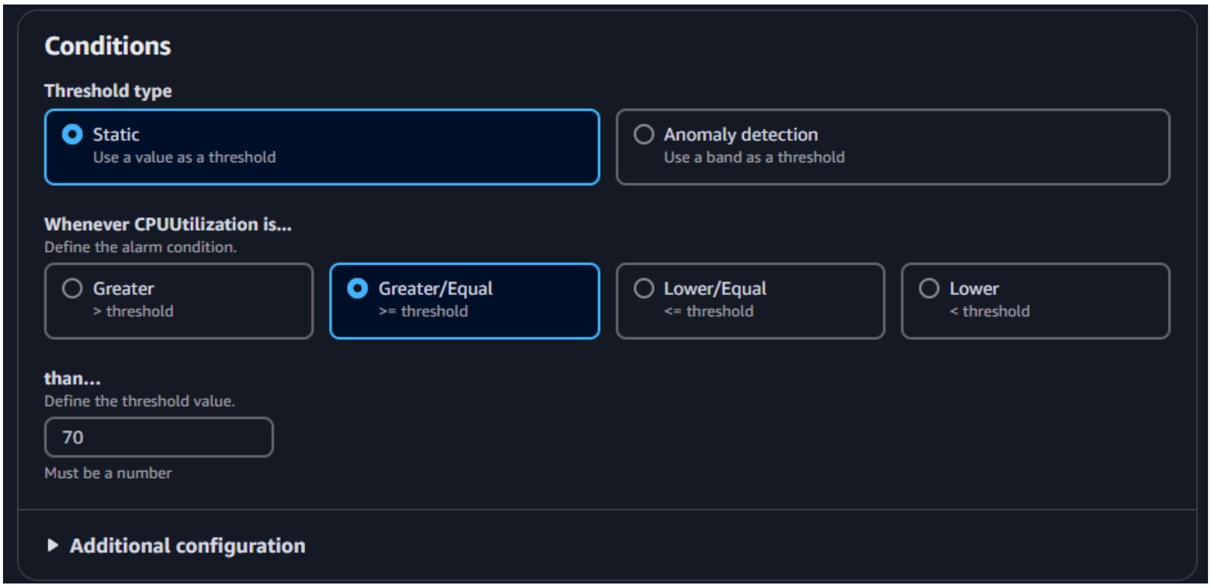
Metric name
CPUUtilization

InstanceId
i-04333c2d50b82c74f

Instance name
kobi-ec2-instance

Statistic
Average

Period
5 minutes



Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

○ Greater
> threshold

● Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

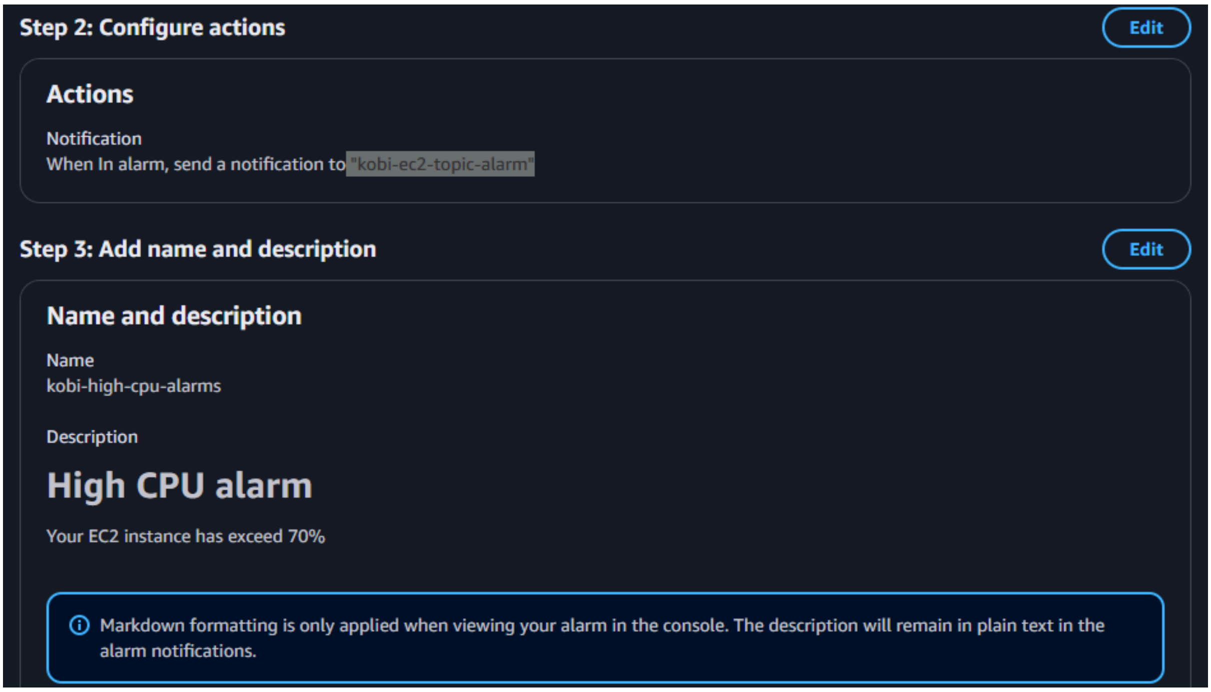
○ Lower
< threshold

than...
Define the threshold value.

70

Must be a number

▸ **Additional configuration**



Step 2: Configure actions

Actions

Notification
When In alarm, send a notification to "kobi-ec2-topic-alarm"

Step 3: Add name and description

Name and description

Name
kobi-high-cpu-alarms

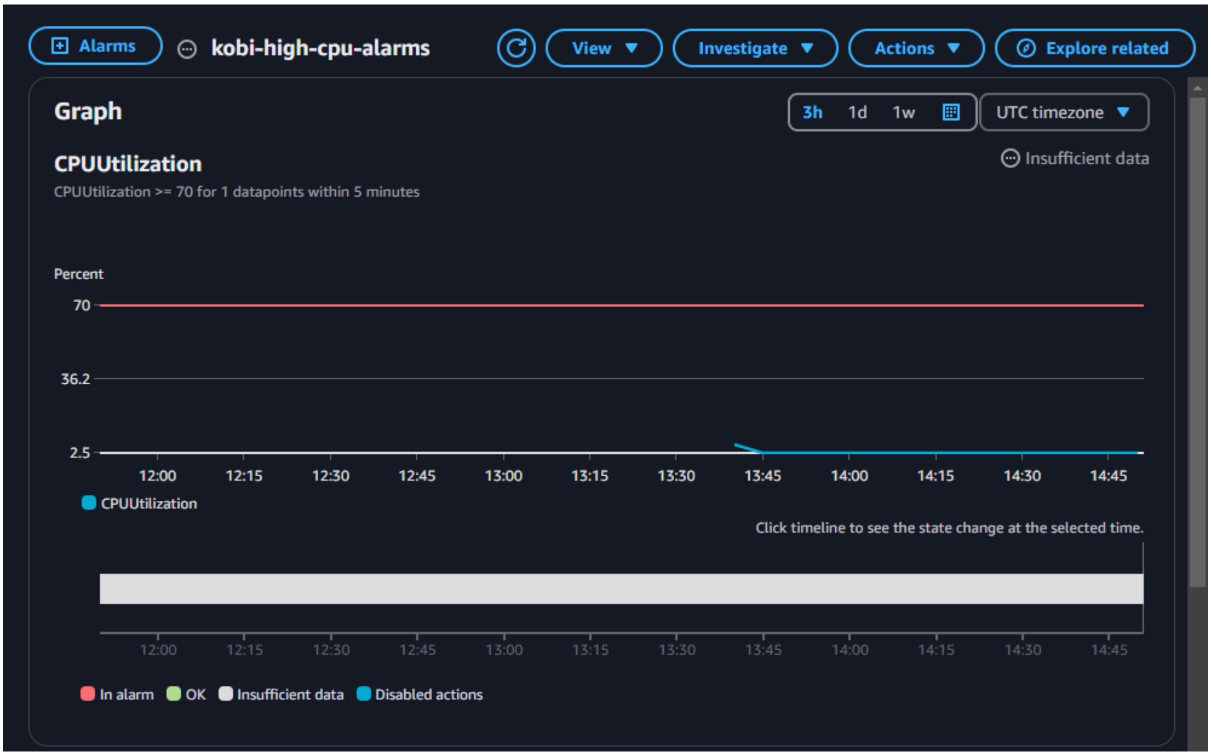
Description

High CPU alarm

Your EC2 instance has exceed 70%

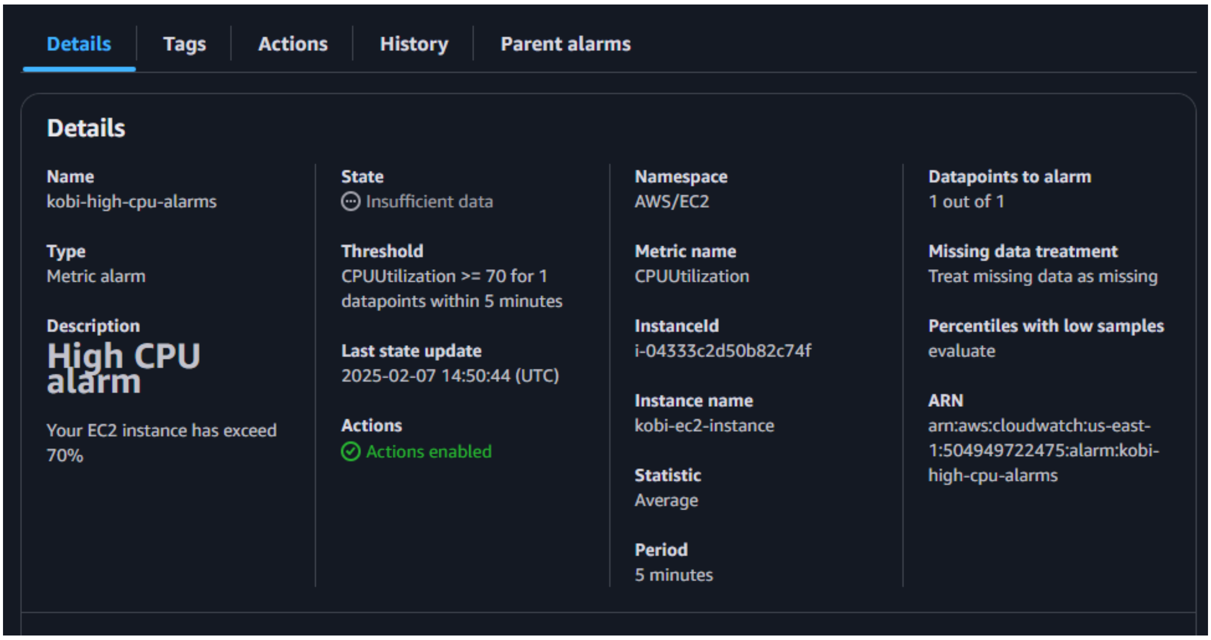
ⓘ Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

The Alarm:



CPUUtilization >= 70 for 1 datapoints within 5 minutes

Click timeline to see the state change at the selected time.



Details

Name
kobi-high-cpu-alarms

Type
Metric alarm

Description
High CPU alarm

Your EC2 instance has exceed 70%

State
⊙ Insufficient data

Threshold
CPUUtilization >= 70 for 1 datapoints within 5 minutes

Last state update
2025-02-07 14:50:44 (UTC)

Actions
✓ Actions enabled

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-04333c2d50b82c74f

Instance name
kobi-ec2-instance

Statistic
Average

Period
5 minutes

Datapoints to alarm
1 out of 1

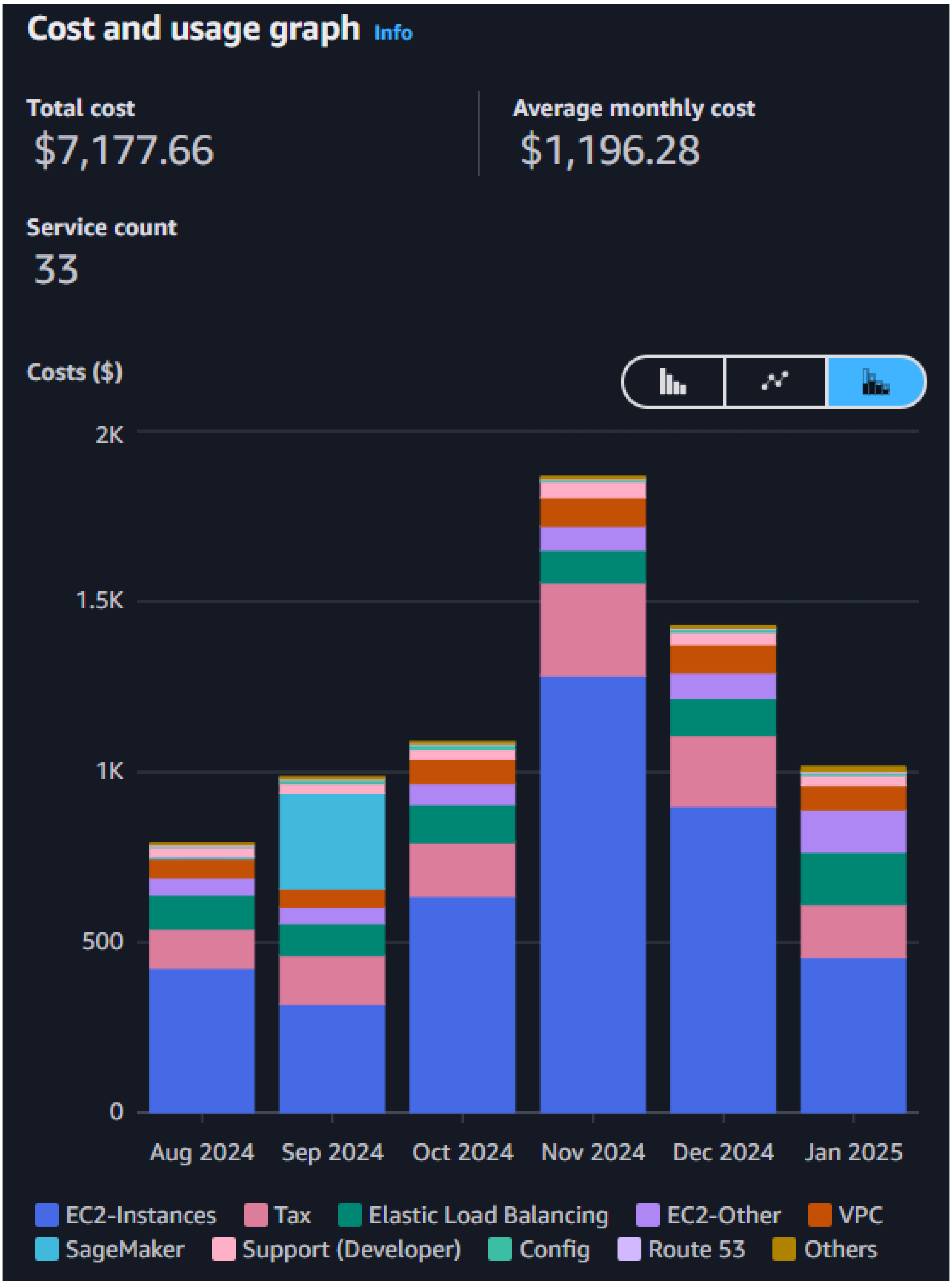
Missing data treatment
Treat missing data as missing

Percentiles with low samples
evaluate

ARN
arn:aws:cloudwatch:us-east-1:504949722475:alarm:kobi-high-cpu-alarms

5. Identify AWS Billing Costs:

The cost usage graph will show us all of our user cost and avg cost for this month, we can use the report params filters to filter usage by certain services like EC2, S3, etc or by users, region or instance type. We can change the type of the metric showed to us the times of which we want to evaluate and the dimensions:



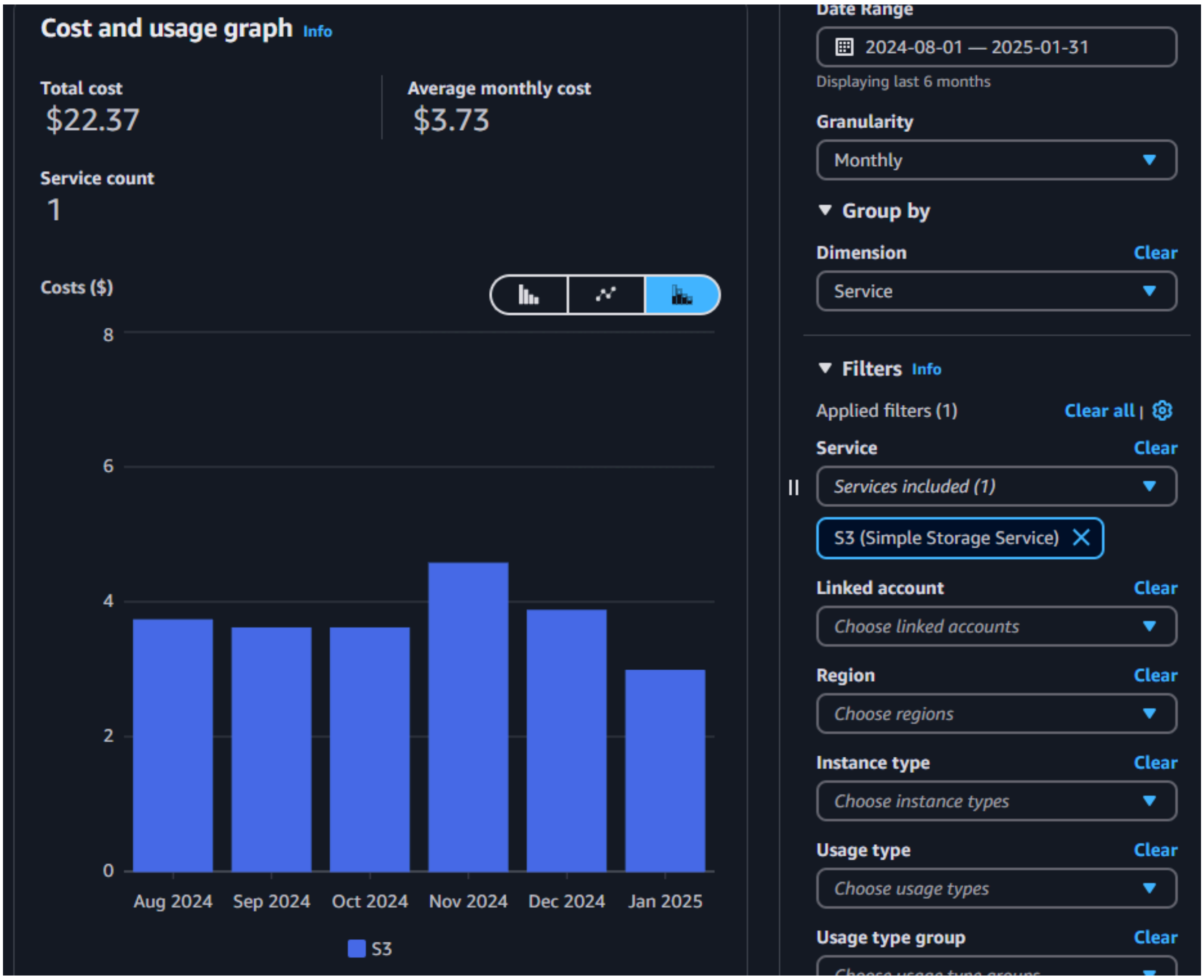
Cost and usage graph Info

Total cost
$7,177.66

Average monthly cost
$1,196.28

Service count
33

filtering the billing by usage of S3 service only:



Cost and usage graph Info

Total cost
$22.37

Average monthly cost
$3.73

Service count
1

Date Range
2024-08-01 — 2025-01-31
Displaying last 6 months

Granularity
Monthly

▼ Group by

Dimension Clear
Service

▼ Filters Info

Applied filters (1) Clear all

Service Clear
Services included (1)
S3 (Simple Storage Service) ✕

Linked account Clear
Choose linked accounts

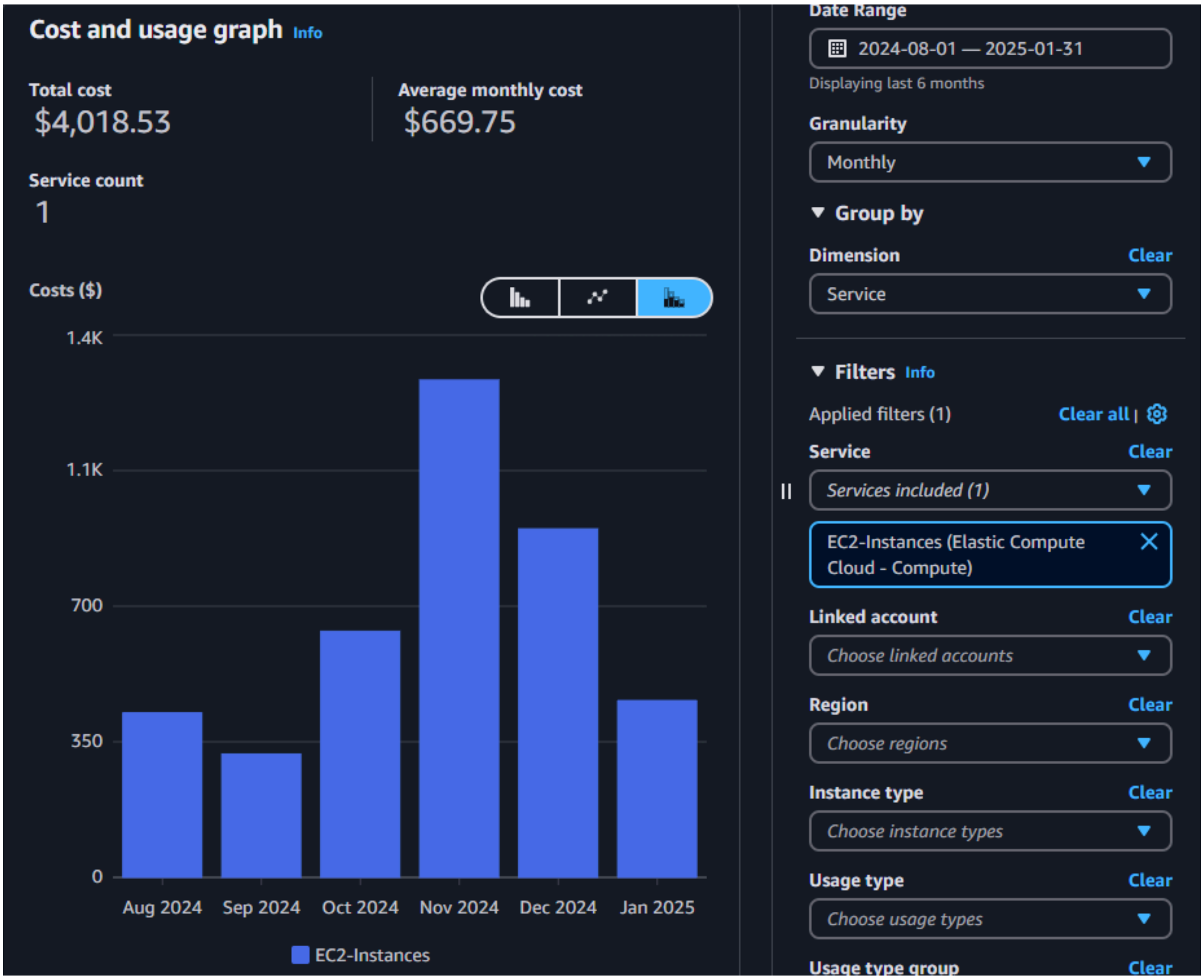
Region Clear
Choose regions

Instance type Clear
Choose instance types

Usage type Clear
Choose usage types

Usage type group Clear
Choose usage type groups

Showing the costs based on EC2 instances only:



Cost and usage graph Info

Total cost
$4,018.53

Average monthly cost
$669.75

Service count
1

Date Range
2024-08-01 — 2025-01-31
Displaying last 6 months

Granularity
Monthly

Group by

Dimension Clear
Service

Filters Info

Applied filters (1) Clear all

Service Clear
Services included (1)
EC2-Instances (Elastic Compute Cloud - Compute)

Linked account Clear
Choose linked accounts

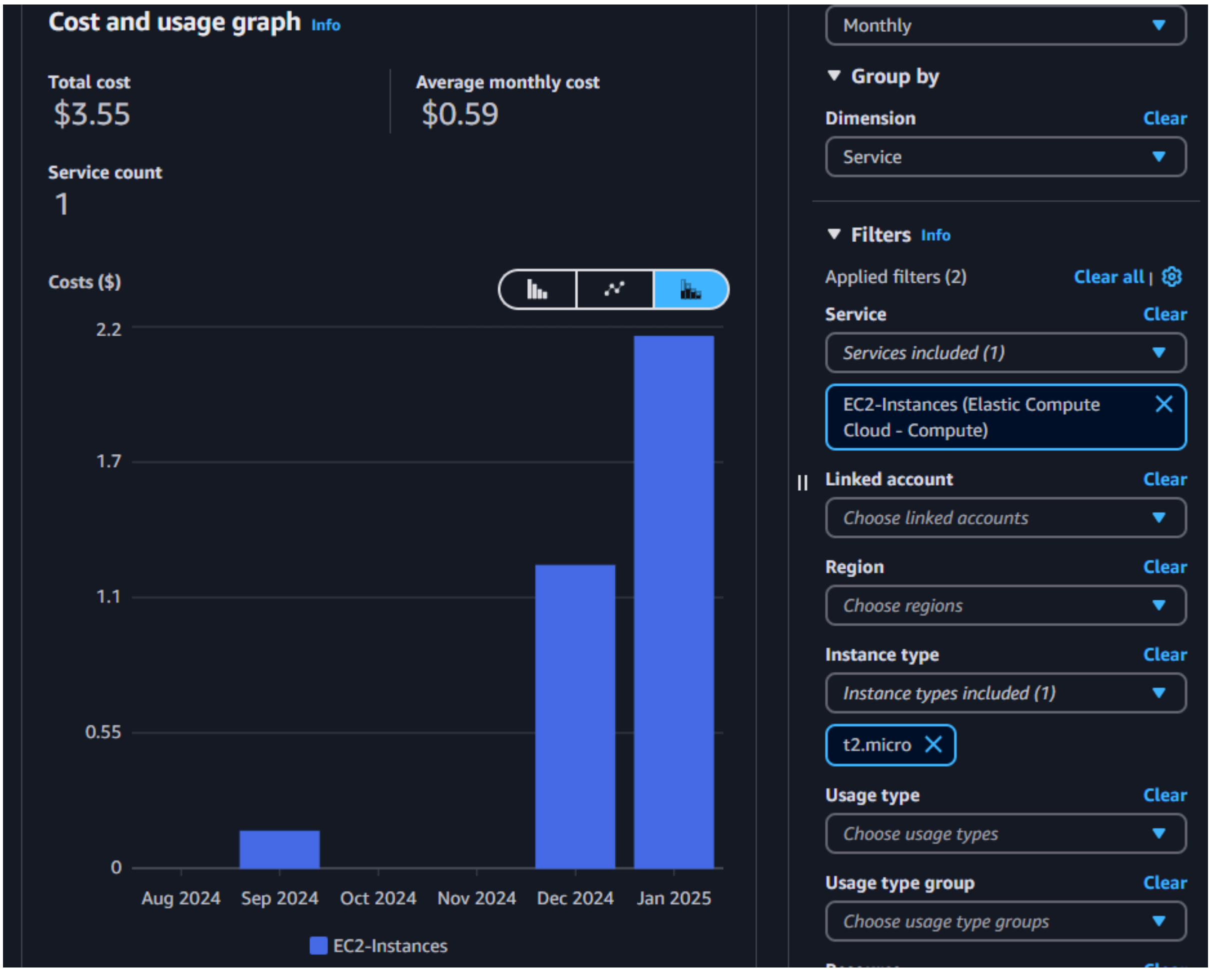
Region Clear
Choose regions

Instance type Clear
Choose instance types

Usage type Clear
Choose usage types

Usage type group Clear

and showing by EC2 instances which uses t2.micro:



Cost and usage graph Info

Total cost
$3.55

Average monthly cost
$0.59

Service count
1

Monthly

Group by

Dimension: Service

Filters Info

Applied filters (2)

Service: Services included (1)

EC2-Instances (Elastic Compute Cloud - Compute)

Linked account: Choose linked accounts

Region: Choose regions

Instance type: Instance types included (1)

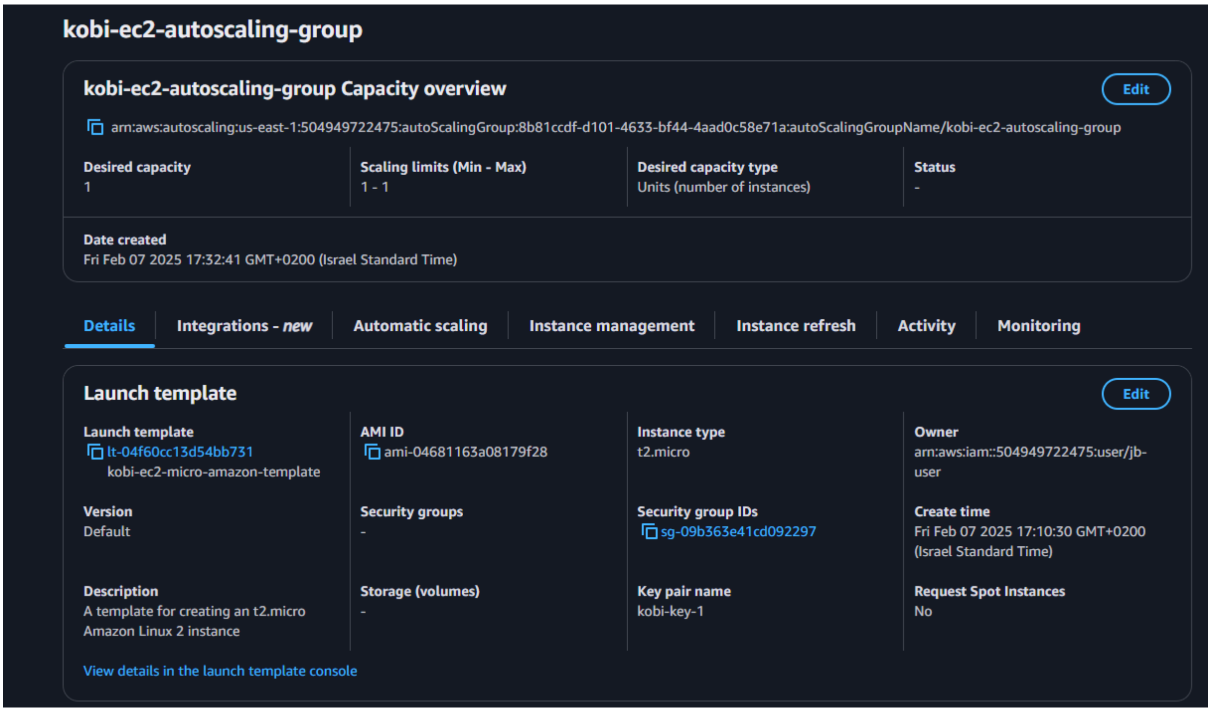
t2.micro

Usage type: Choose usage types

Usage type group: Choose usage type groups

Section 3: Hands-on advanced:

1. Deploy an Auto Scaling Group with a Single EC2 Instance:



kobi-ec2-autoscaling-group

kobi-ec2-autoscaling-group Capacity overview

arn:aws:autoscaling:us-east-1:504949722475:autoScalingGroup:8b81ccdf-d101-4633-bf44-4aad0c58e71a:autoScalingGroupName/kobi-ec2-autoscaling-group

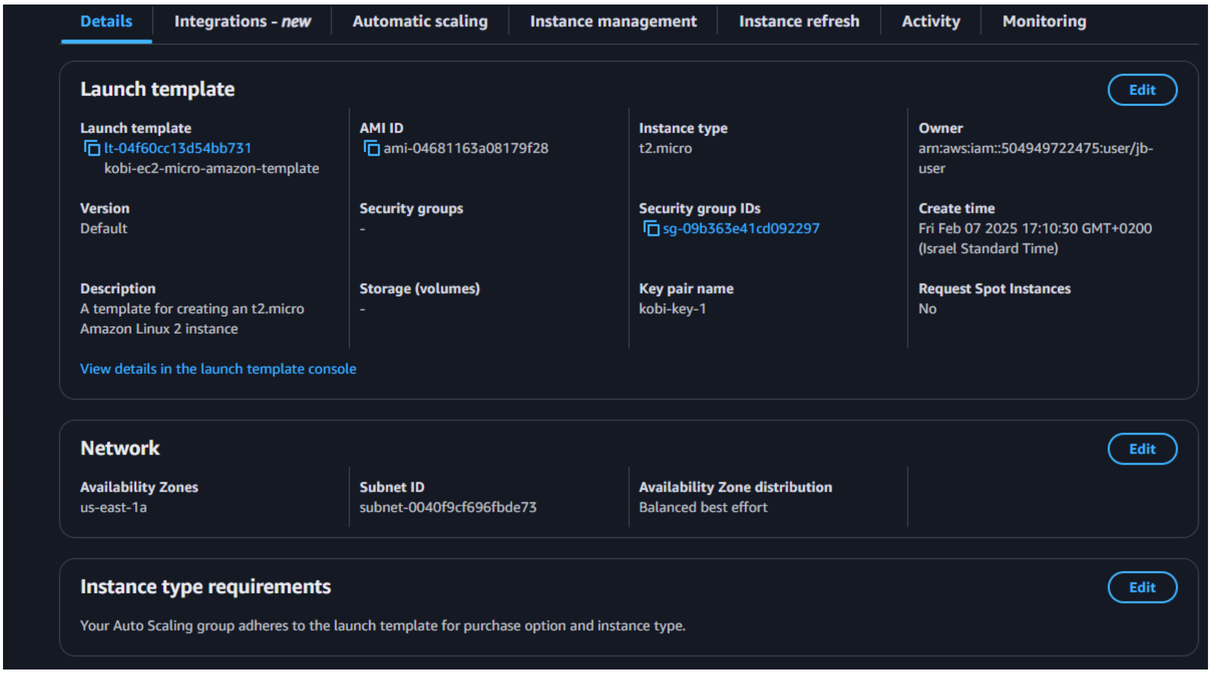
Desired capacity	Scaling limits (Min - Max)	Desired capacity type	Status
1	1 - 1	Units (number of instances)	-

Date created
Fri Feb 07 2025 17:32:41 GMT+0200 (Israel Standard Time)

Launch template

Launch template lt-04f60cc13d54bb731 kobi-ec2-micro-amazon-template	**AMI ID** ami-04681163a08179f28	**Instance type** t2.micro	**Owner** arn:aws:iam::504949722475:user/jb-user
Version Default	**Security groups** -	**Security group IDs** sg-09b363e41cd092297	**Create time** Fri Feb 07 2025 17:10:30 GMT+0200 (Israel Standard Time)
Description A template for creating an t2.micro Amazon Linux 2 instance	**Storage (volumes)** -	**Key pair name** kobi-key-1	**Request Spot Instances** No

View details in the launch template console



Launch template

Launch template lt-04f60cc13d54bb731 kobi-ec2-micro-amazon-template	**AMI ID** ami-04681163a08179f28	**Instance type** t2.micro	**Owner** arn:aws:iam::504949722475:user/jb-user
Version Default	**Security groups** -	**Security group IDs** sg-09b363e41cd092297	**Create time** Fri Feb 07 2025 17:10:30 GMT+0200 (Israel Standard Time)
Description A template for creating an t2.micro Amazon Linux 2 instance	**Storage (volumes)** -	**Key pair name** kobi-key-1	**Request Spot Instances** No

View details in the launch template console

Network

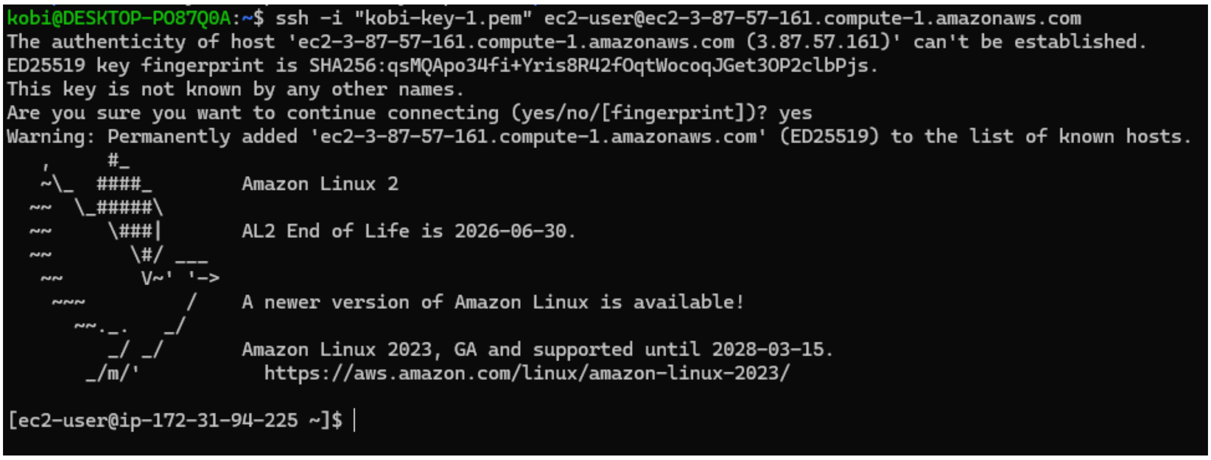
Availability Zones	Subnet ID	Availability Zone distribution
us-east-1a	subnet-0040f9cf696fbde73	Balanced best effort

Instance type requirements

Your Auto Scaling group adheres to the launch template for purchase option and instance type.

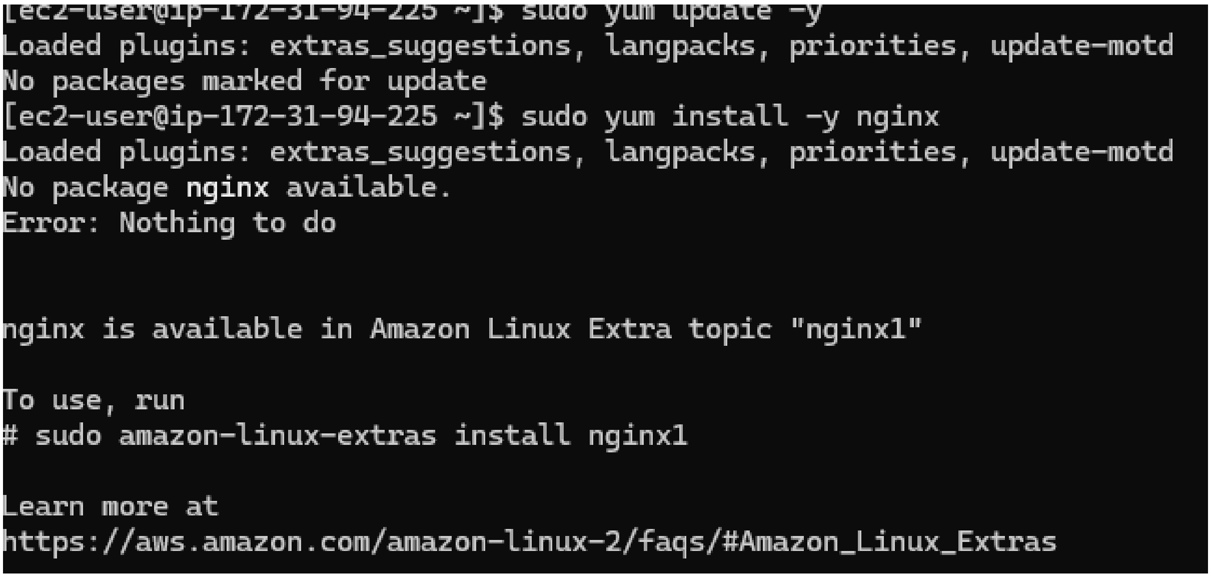
2. Connect to the EC2 Instance and Install Nginx:

Connecting via SSH:



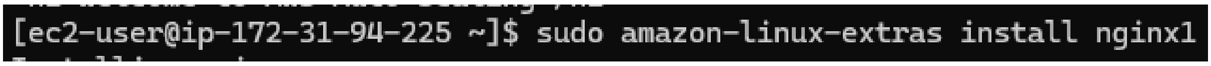
```
kobi@DESKTOP-PO87Q0A:~$ ssh -i "kobi-key-1.pem" ec2-user@ec2-3-87-57-161.compute-1.amazonaws.com
The authenticity of host 'ec2-3-87-57-161.compute-1.amazonaws.com (3.87.57.161)' can't be established.
ED25519 key fingerprint is SHA256:qsMQApo34fi+Yris8R42fOqtWocoqJGet3OP2clbPjs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-87-57-161.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2026-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-172-31-94-225 ~]$ |
```

Running the commands given to us in the file:



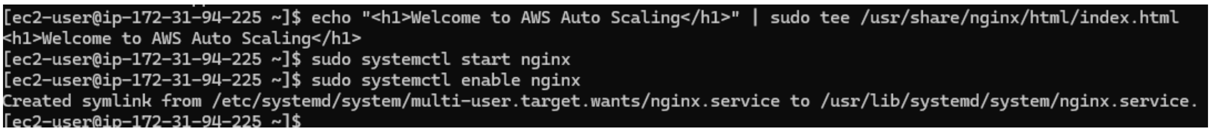
```
[ec2-user@ip-172-31-94-225 ~]$ sudo yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No packages marked for update
[ec2-user@ip-172-31-94-225 ~]$ sudo yum install -y nginx
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No package nginx available.
Error: Nothing to do


nginx is available in Amazon Linux Extra topic "nginx1"

To use, run
# sudo amazon-linux-extras install nginx1

Learn more at
https://aws.amazon.com/amazon-linux-2/faqs/#Amazon_Linux_Extras
```

running a new command cause “sudo yum install -y nginx” was not working:



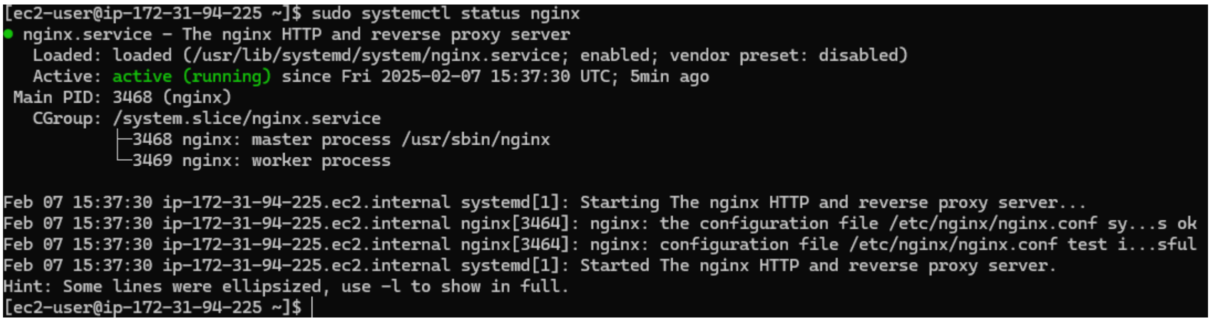
```
[ec2-user@ip-172-31-94-225 ~]$ sudo amazon-linux-extras install nginx1
```

Running the following commands:



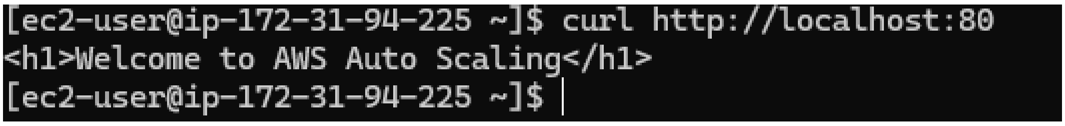
```
[ec2-user@ip-172-31-94-225 ~]$ echo "<h1>Welcome to AWS Auto Scaling</h1>" | sudo tee /usr/share/nginx/html/index.html
<h1>Welcome to AWS Auto Scaling</h1>
[ec2-user@ip-172-31-94-225 ~]$ sudo systemctl start nginx
[ec2-user@ip-172-31-94-225 ~]$ sudo systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.
[ec2-user@ip-172-31-94-225 ~]$
```

Showing the nginx service is up and running:



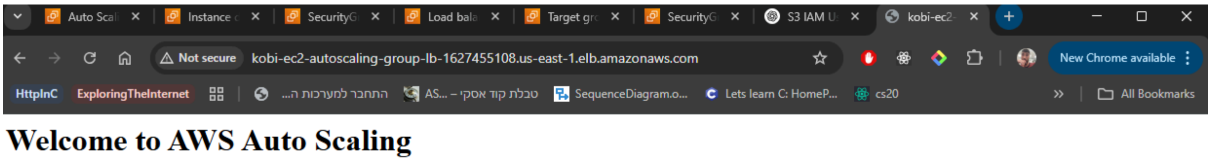
```
[ec2-user@ip-172-31-94-225 ~]$ sudo systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2025-02-07 15:37:30 UTC; 5min ago
 Main PID: 3468 (nginx)
   CGroup: /system.slice/nginx.service
           ├─3468 nginx: master process /usr/sbin/nginx
           └─3469 nginx: worker process

Feb 07 15:37:30 ip-172-31-94-225.ec2.internal systemd[1]: Starting The nginx HTTP and reverse proxy server...
Feb 07 15:37:30 ip-172-31-94-225.ec2.internal nginx[3464]: nginx: the configuration file /etc/nginx/nginx.conf sy...s ok
Feb 07 15:37:30 ip-172-31-94-225.ec2.internal nginx[3464]: nginx: configuration file /etc/nginx/nginx.conf test i...sful
Feb 07 15:37:30 ip-172-31-94-225.ec2.internal systemd[1]: Started The nginx HTTP and reverse proxy server.
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-172-31-94-225 ~]$
```

curl command:



```
[ec2-user@ip-172-31-94-225 ~]$ curl http://localhost:80
<h1>Welcome to AWS Auto Scaling</h1>
[ec2-user@ip-172-31-94-225 ~]$
```

3. Access the Web Page via the Load Balancer:

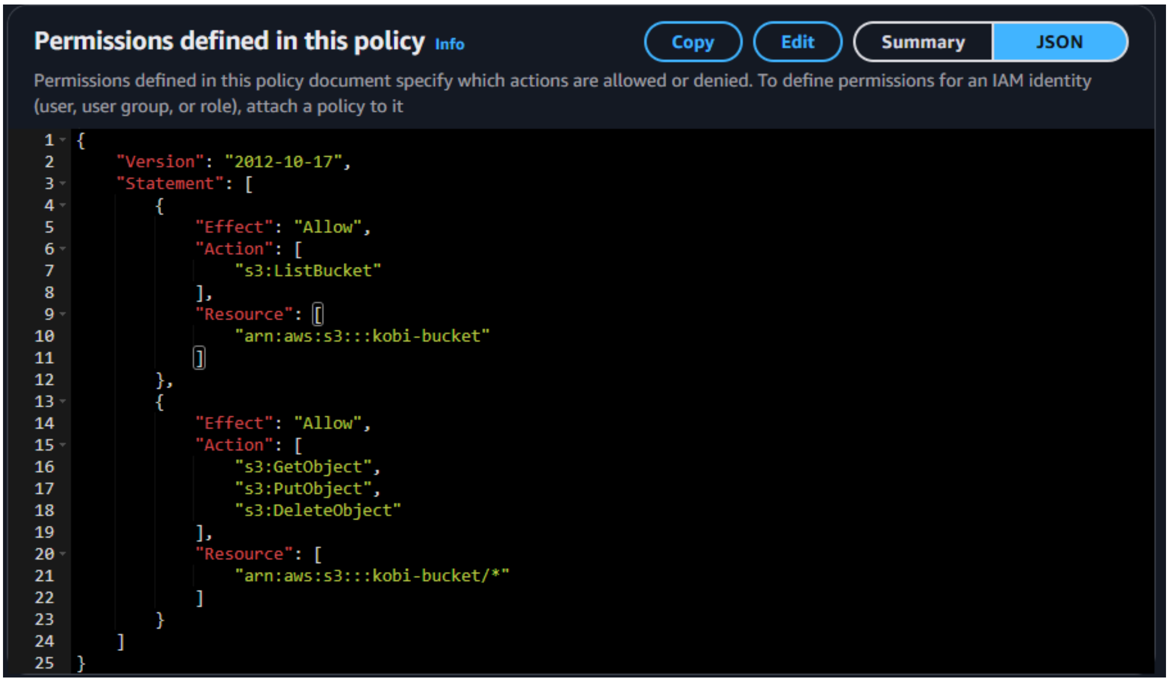


kobi-ec2-autoscaling-group-lb-1627455108.us-east-1.elb.amazonaws.com

Welcome to AWS Auto Scaling

IAM User Setup for S3 Access:

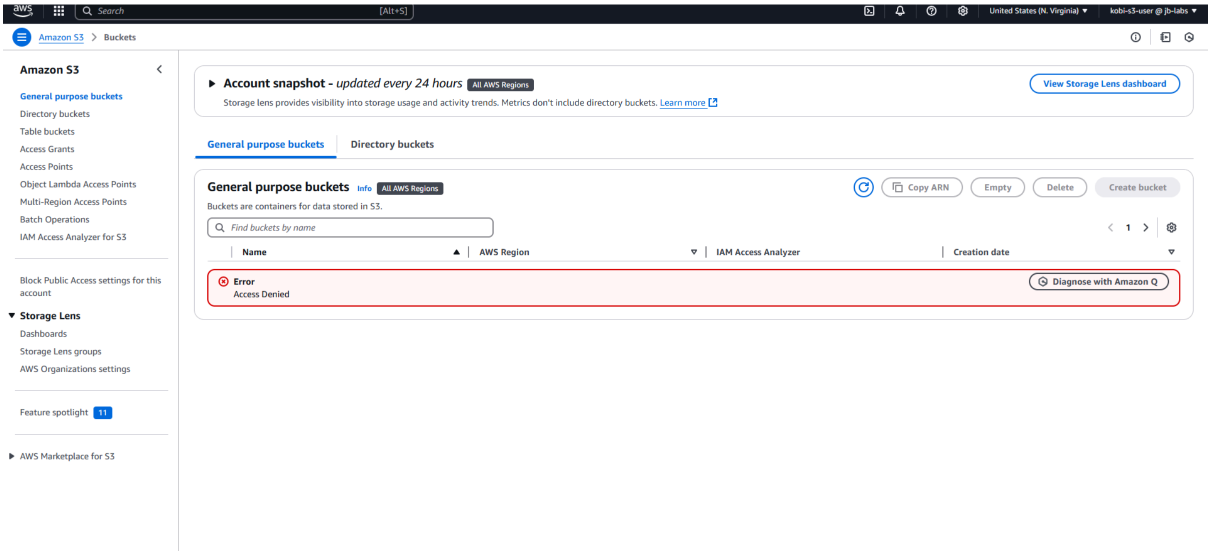
The user policy permission:



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": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::kobi-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::kobi-bucket/*"
            ]
        }
    ]
}
```

trying to access all buckets will result in permission denied:



Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more

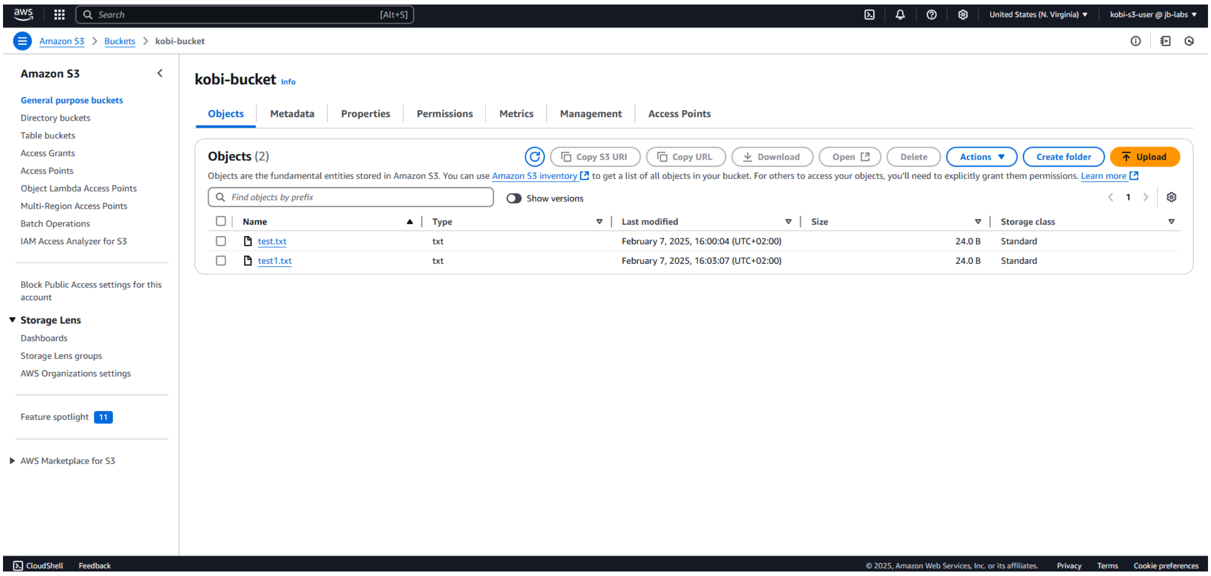
General purpose buckets Info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date

Error
Access Denied

but trying a specific bucket (in this case my own bucket named kobi-bucket) will work connect via this url (https://us-east-1.console.aws.amazon.com/s3/buckets/kobi-bucket?region=us-east-1&tab=objects&bucketType=general):

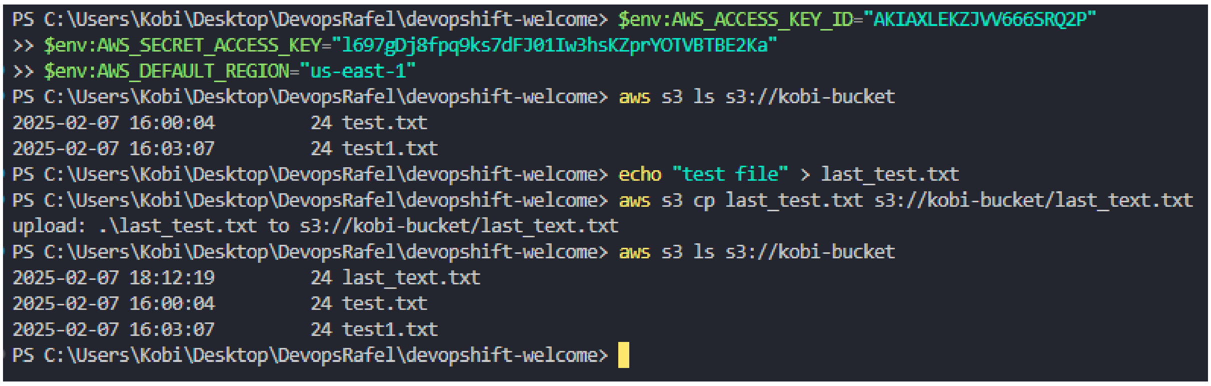


Objects (2)

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

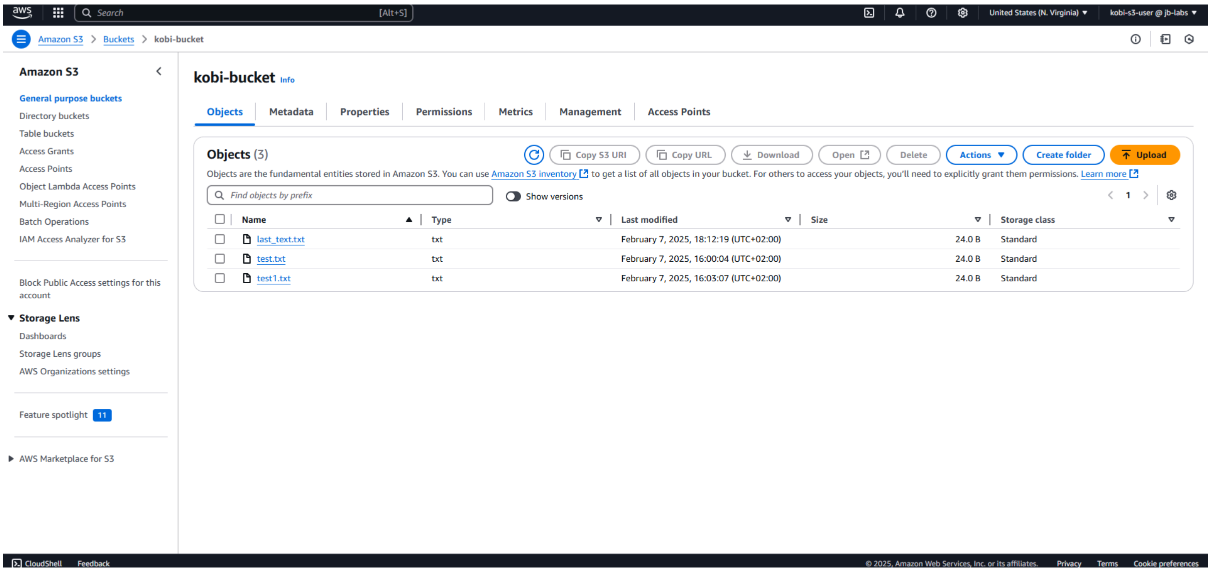
	Name	Type	Last modified	Size	Storage class
□	test.txt	txt	February 7, 2025, 16:00:04 (UTC+02:00)	24.0 B	Standard
□	test1.txt	txt	February 7, 2025, 16:03:07 (UTC+02:00)	24.0 B	Standard

Using aws sdk to see the user can update and see the certain bucket he is attached to:



```
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> $env:AWS_ACCESS_KEY_ID="AKIAXLEKZJVV666SRQ2P"
>> $env:AWS_SECRET_ACCESS_KEY="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"
>> $env:AWS_DEFAULT_REGION="us-east-1"
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> aws s3 ls s3://kobi-bucket
2025-02-07 16:00:04         24 test.txt
2025-02-07 16:03:07         24 test1.txt
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> echo "test file" > last_test.txt
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> aws s3 cp last_test.txt s3://kobi-bucket/last_text.txt
upload: .\last_test.txt to s3://kobi-bucket/last_text.txt
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome> aws s3 ls s3://kobi-bucket
2025-02-07 18:12:19         24 last_text.txt
2025-02-07 16:00:04         24 test.txt
2025-02-07 16:03:07         24 test1.txt
PS C:\Users\Kobi\Desktop\DevopsRafel\devopshift-welcome>
```

after the addition of the new file through the ui:



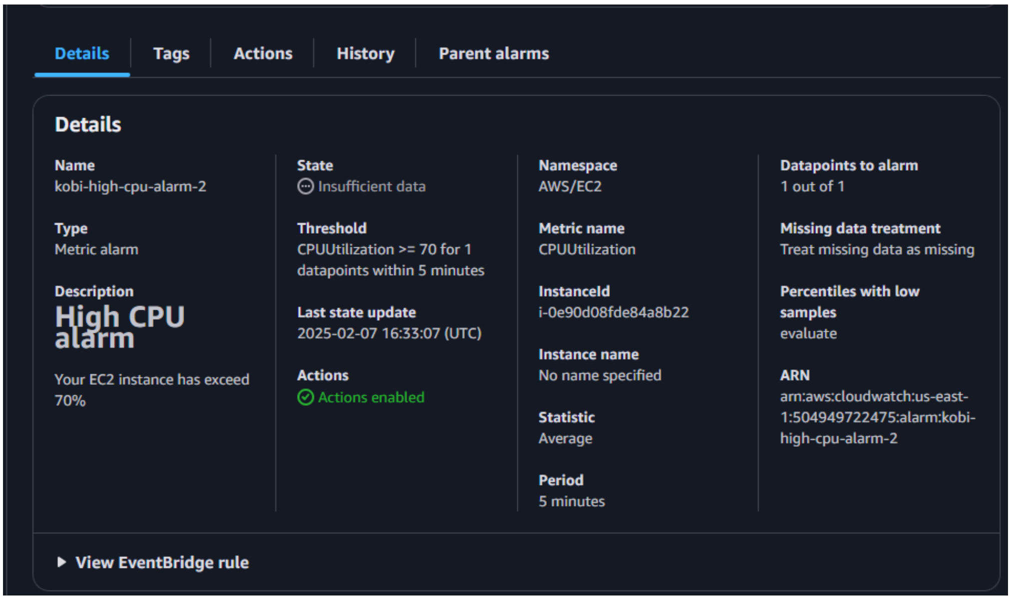
kobi-bucket

Objects (3)

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
□	last_text.txt	txt	February 7, 2025, 18:12:19 (UTC+02:00)	24.0 B	Standard
□	test.txt	txt	February 7, 2025, 16:00:04 (UTC+02:00)	24.0 B	Standard
□	test1.txt	txt	February 7, 2025, 16:03:07 (UTC+02:00)	24.0 B	Standard

5. Create a CloudWatch Alarm for CPU Usage:



Details

Name
kobi-high-cpu-alarm-2

Type
Metric alarm

Description
High CPU alarm

Your EC2 instance has exceed 70%

State
Insufficient data

Threshold
CPUUtilization >= 70 for 1 datapoints within 5 minutes

Last state update
2025-02-07 16:33:07 (UTC)

Actions
Actions enabled

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-0e90d08fde84a8b22

Instance name
No name specified

Statistic
Average

Period
5 minutes

Datapoints to alarm
1 out of 1

Missing data treatment
Treat missing data as missing

Percentiles with low samples
evaluate

ARN
arn:aws:cloudwatch:us-east-1:504949722475:alarm:kobi-high-cpu-alarm-2