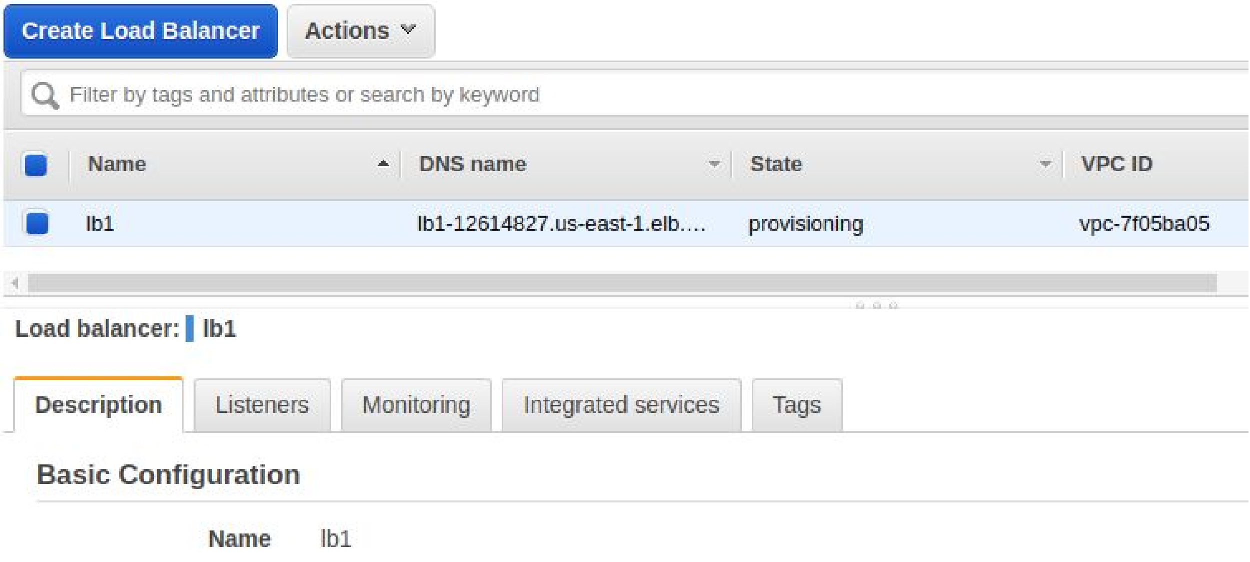
ASSESSMENT - 15

S3, Route 53 & DNS

TO THE NEW

1) **Create a private hosted zone named "ttn-internal.com" attached to the default vpc. and created a cname record "myloadbalance.ttn-internal.com" for any load balancer pointed to its dns. Do reverse lookup for the record from any instance of the vpc and share the result.**

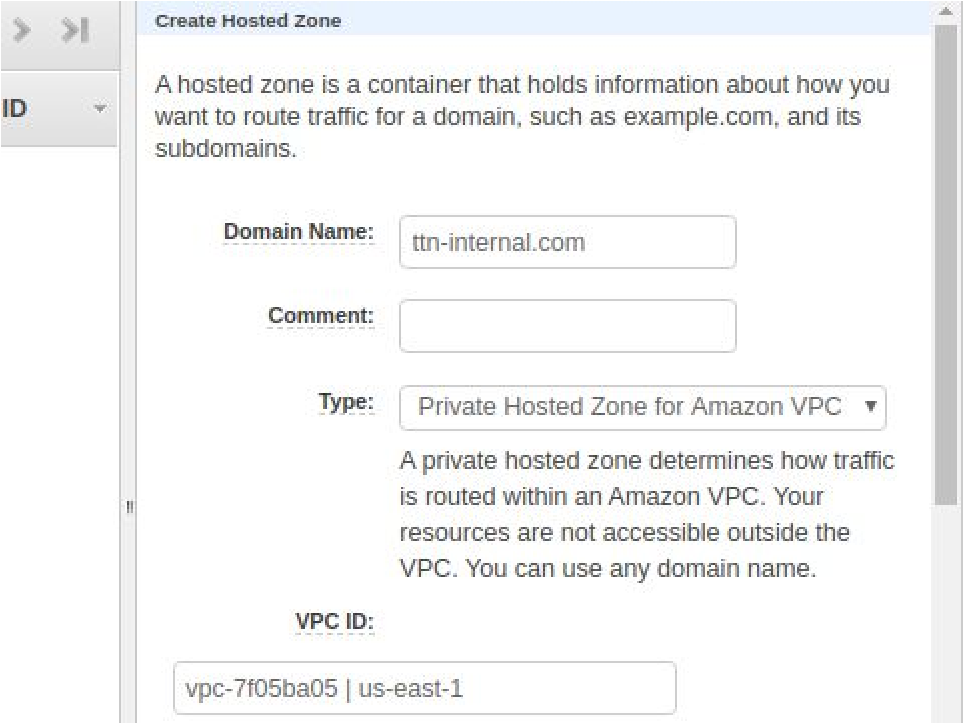


Name	DNS name	State	VPC ID
lb1	lb1-12614827.us-east-1.elb....	provisioning	vpc-7f05ba05

Load balancer: lb1

Basic Configuration

Name lb1



Create Hosted Zone

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain Name: ttn-internal.com

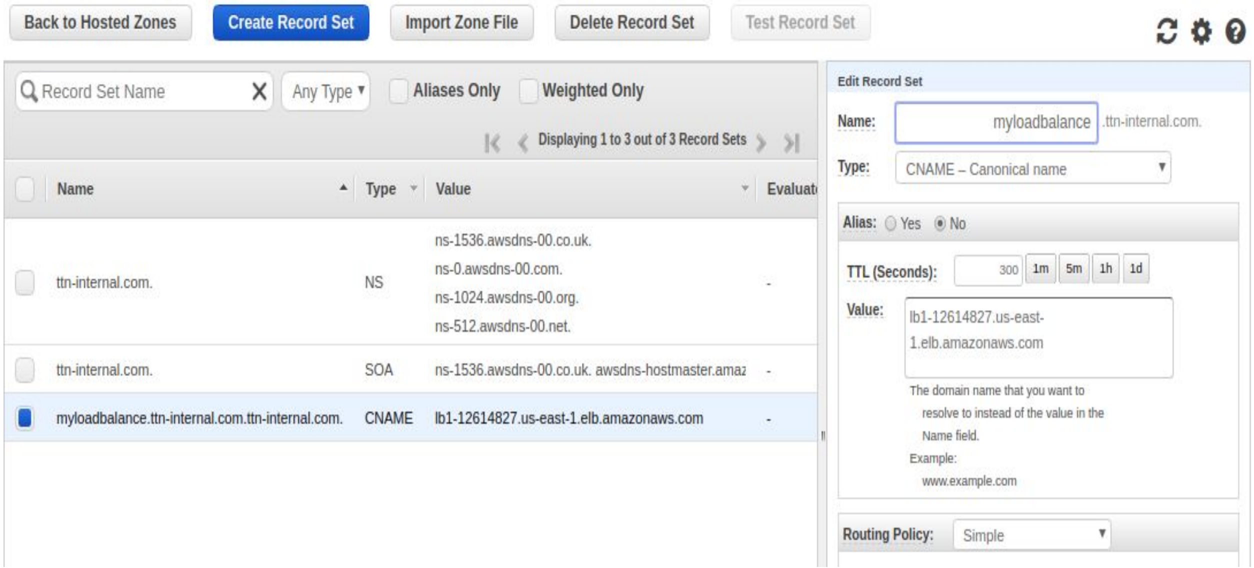
Comment:

Type: Private Hosted Zone for Amazon VPC

A private hosted zone determines how traffic is routed within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any domain name.

VPC ID:

vpc-7f05ba05 | us-east-1



Name	Type	Value	Evaluat
ttn-internal.com.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-
ttn-internal.com.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz	-
myloadbalance.ttn-internal.com.ttn-internal.com.	CNAME	lb1-12614827.us-east-1.elb.amazonaws.com	-

Edit Record Set

Name: myloadbalance .ttn-internal.com.

Type: CNAME – Canonical name

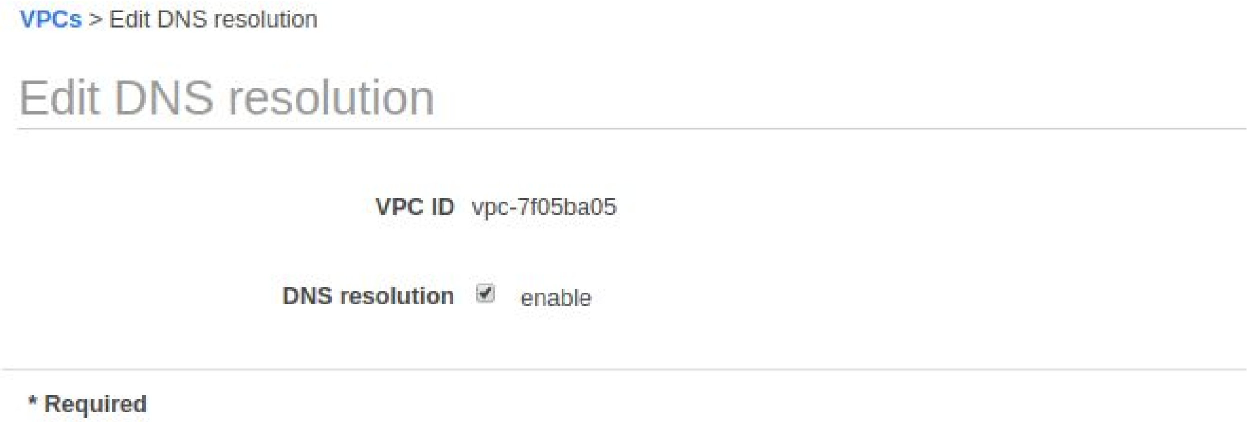
Alias: ○ Yes ● No

TTL (Seconds): 300 1m 5m 1h 1d

Value: lb1-12614827.us-east-1.elb.amazonaws.com

The domain name that you want to resolve to instead of the value in the Name field.
Example:
www.example.com

Routing Policy: Simple

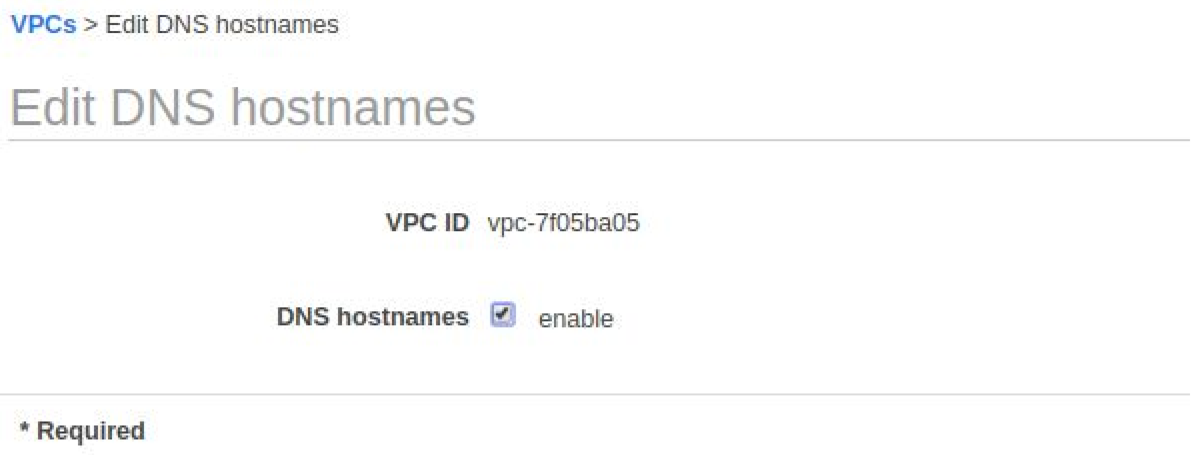

VPCs > Edit DNS resolution

Edit DNS resolution

VPC ID vpc-7f05ba05

DNS resolution ☑ enable

* Required



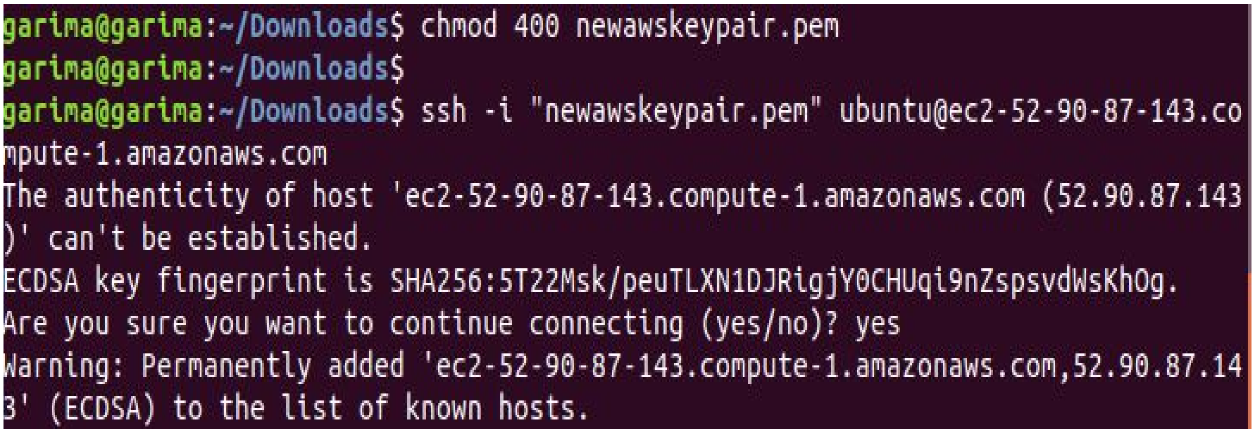
VPCs > Edit DNS hostnames

Edit DNS hostnames

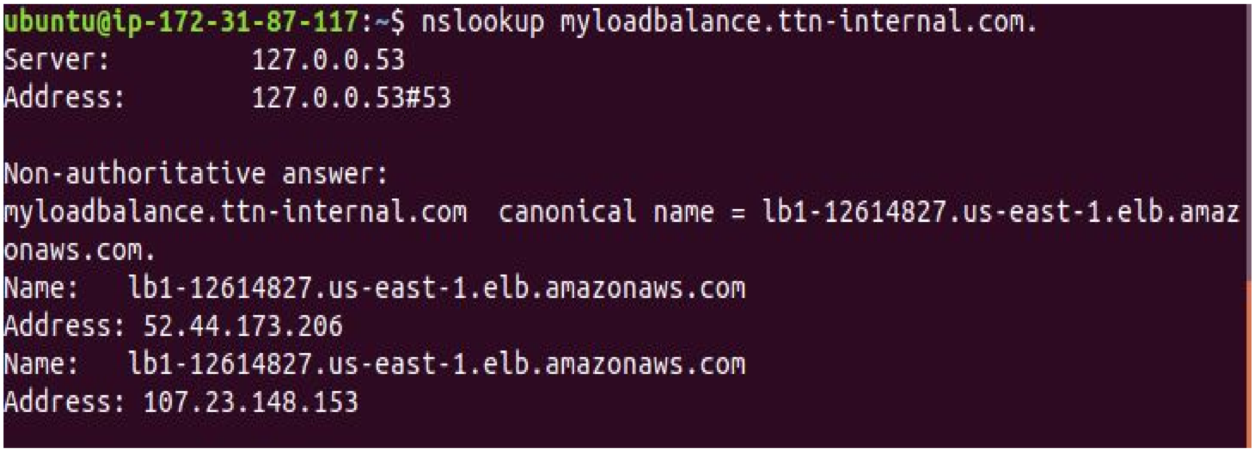
VPC ID vpc-7f05ba05

DNS hostnames ☑ enable

* Required



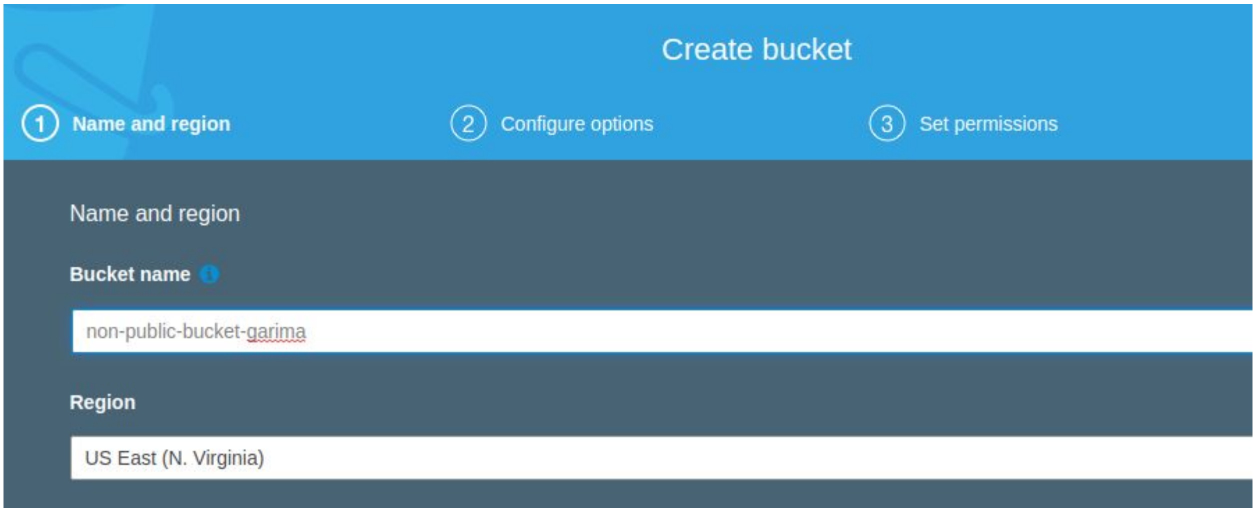
```
garima@garima:~/Downloads$ chmod 400 newawskeypair.pem
garima@garima:~/Downloads$
garima@garima:~/Downloads$ ssh -i "newawskeypair.pem" ubuntu@ec2-52-90-87-143.co
mpute-1.amazonaws.com
The authenticity of host 'ec2-52-90-87-143.compute-1.amazonaws.com (52.90.87.143
)' can't be established.
ECDSA key fingerprint is SHA256:5T22Msk/peuTLXN1DJRigjY0CHUqi9nZspsvdWsKhOg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-52-90-87-143.compute-1.amazonaws.com,52.90.87.14
3' (ECDSA) to the list of known hosts.
```



```
ubuntu@ip-172-31-87-117:~$ nslookup myloadbalance.ttn-internal.com.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
myloadbalance.ttn-internal.com  canonical name = lb1-12614827.us-east-1.elb.amaz
onaws.com.
Name:   lb1-12614827.us-east-1.elb.amazonaws.com
Address: 52.44.173.206
Name:   lb1-12614827.us-east-1.elb.amazonaws.com
Address: 107.23.148.153
```

2) Create a non-public S3 bucket and give appropriate permissions to a server to download objects from the bucket but not to put or delete anything in it.



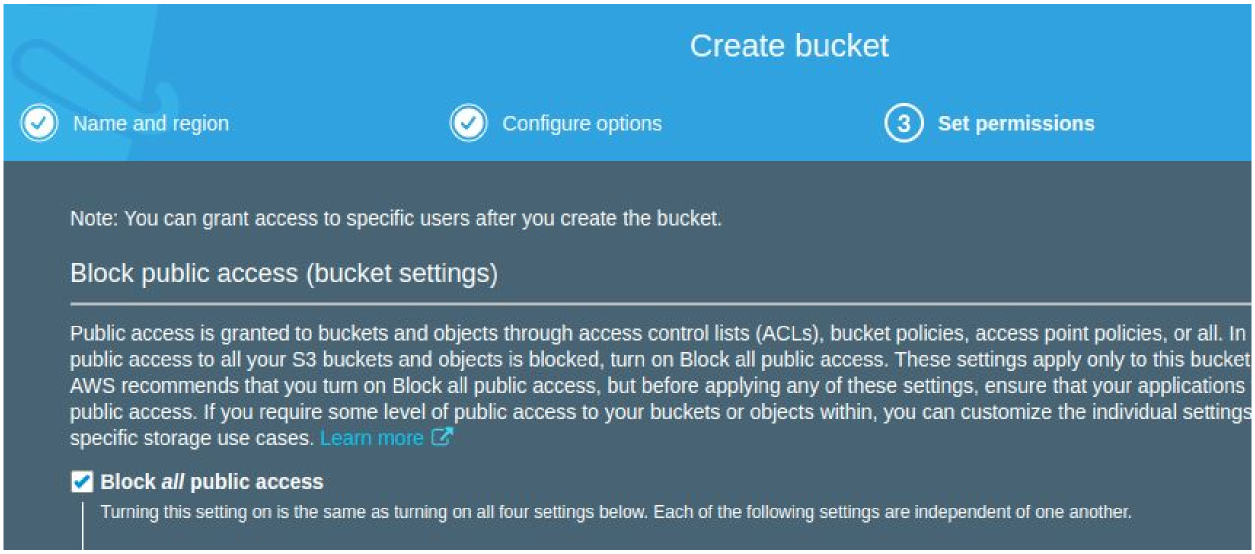
Name and region

Bucket name

non-public-bucket-garima

Region

US East (N. Virginia)



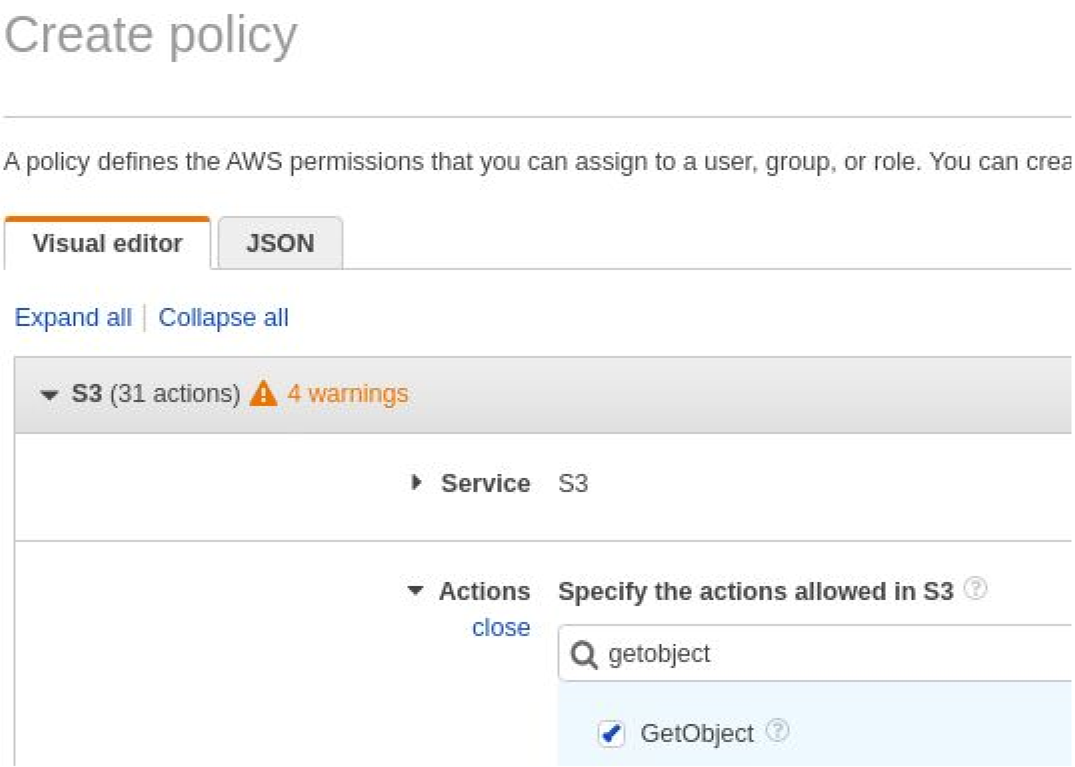
Note: You can grant access to specific users after you create the bucket.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings specific storage use cases. Learn more

☑ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can crea

▼ **S3** (31 actions) ⚠ 4 warnings

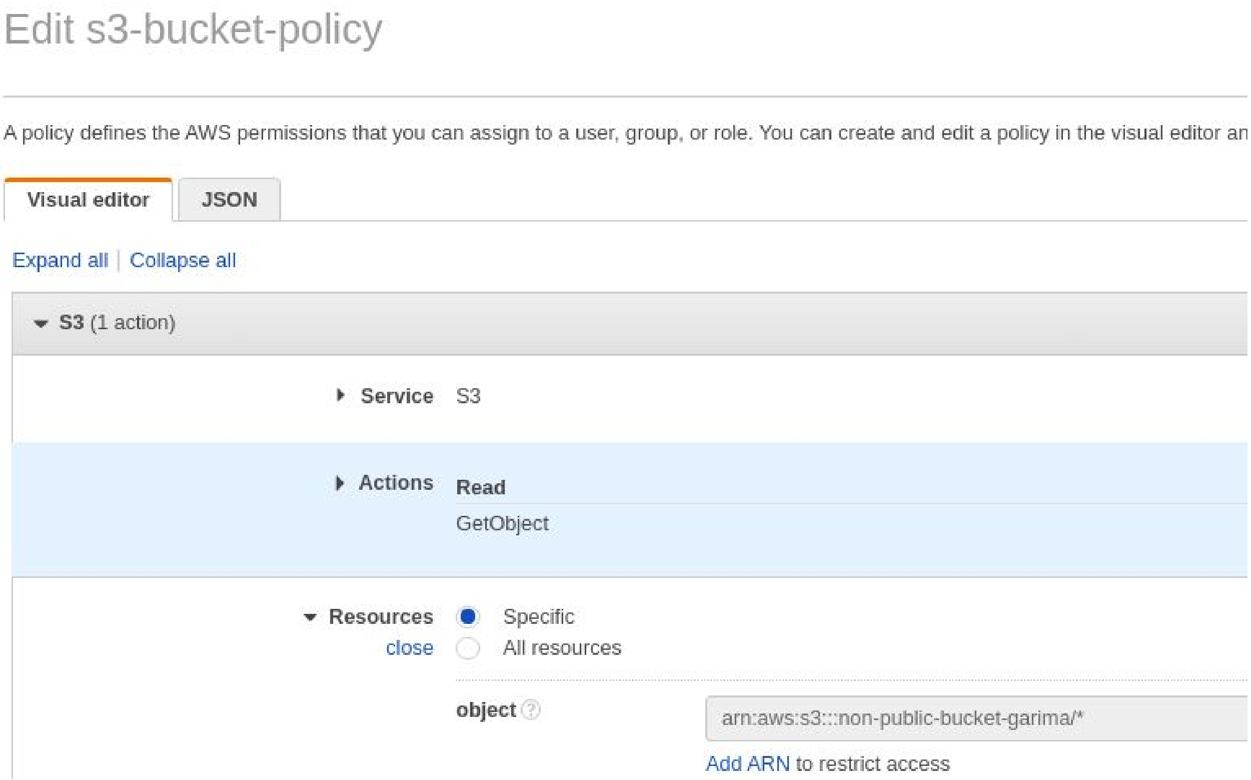
▶ **Service** S3

▼ **Actions** close

Specify the actions allowed in S3

getobject

☑ GetObject



Edit s3-bucket-policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor an

S3 (1 action)

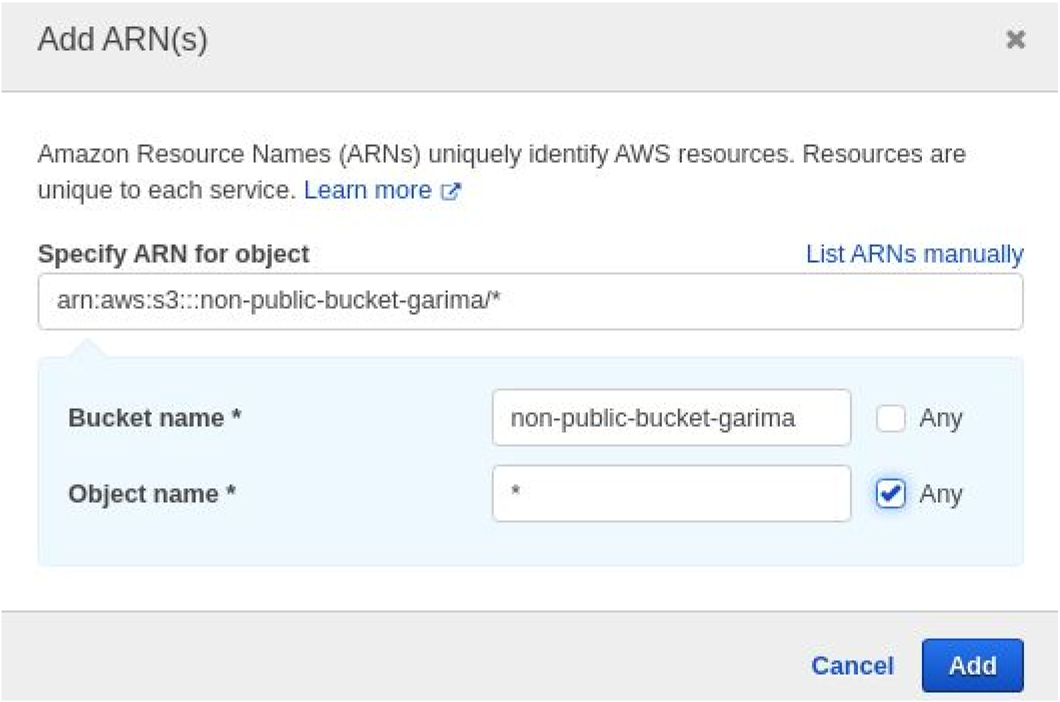
Service S3

Actions Read
GetObject

Resources ● Specific
close ○ All resources

object arn:aws:s3:::non-public-bucket-garima/*

Add ARN to restrict access



Add ARN(s)

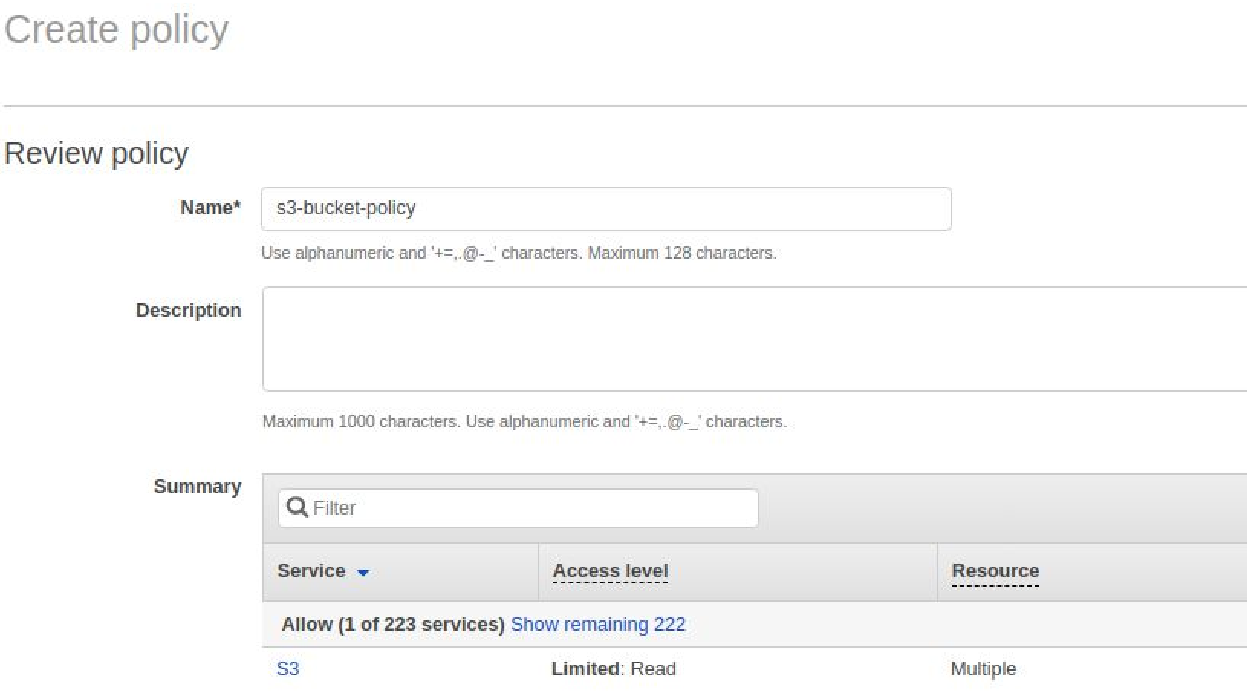
Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for object

arn:aws:s3:::non-public-bucket-garima/*

Bucket name * non-public-bucket-garima □ Any

Object name * * ☑ Any



Create policy

Review policy

Name* s3-bucket-policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

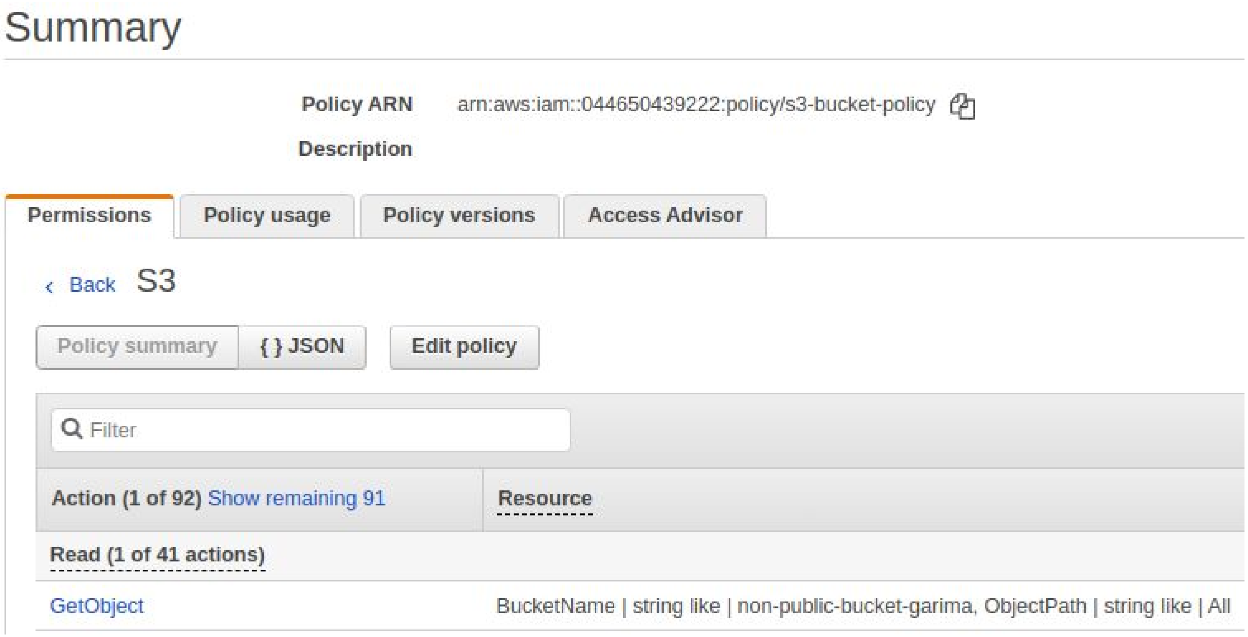
Description

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

Summary

Filter

Service	Access level	Resource
Allow (1 of 223 services) Show remaining 222		
S3	**Limited**: Read	Multiple

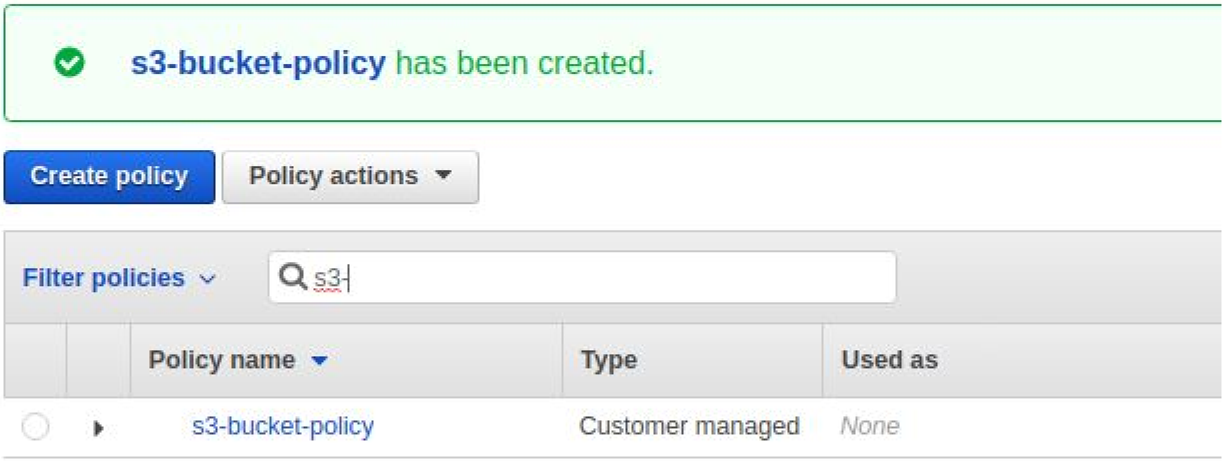


Summary

Policy ARN arn:aws:iam::044650439222:policy/s3-bucket-policy

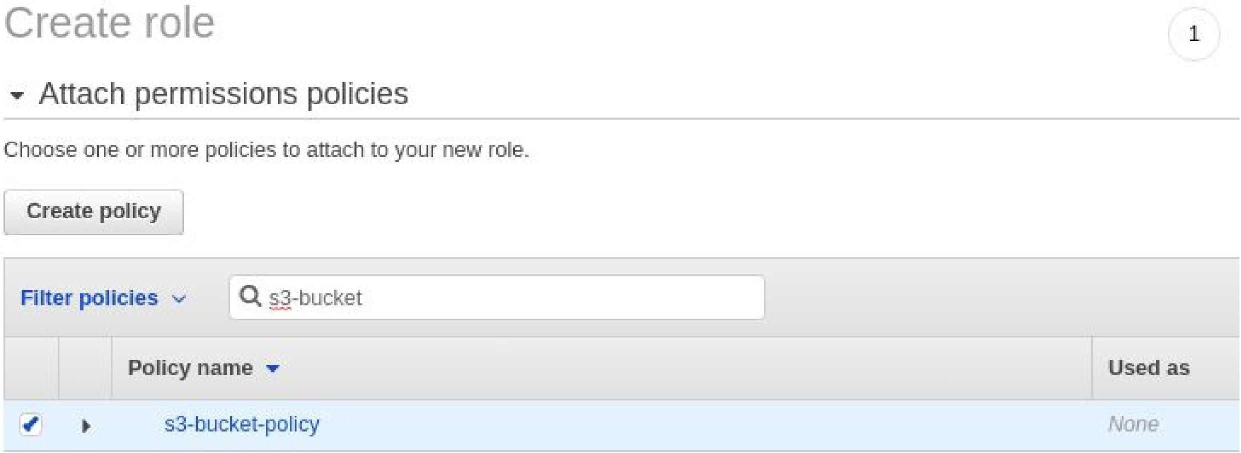
Description

Action (1 of 92) Show remaining 91	Resource
Read (1 of 41 actions)	
GetObject	BucketName | string like | non-public-bucket-garima, ObjectPath | string like | All



s3-bucket-policy has been created.

		Policy name ▼	Type	Used as
○	▸	s3-bucket-policy	Customer managed	None

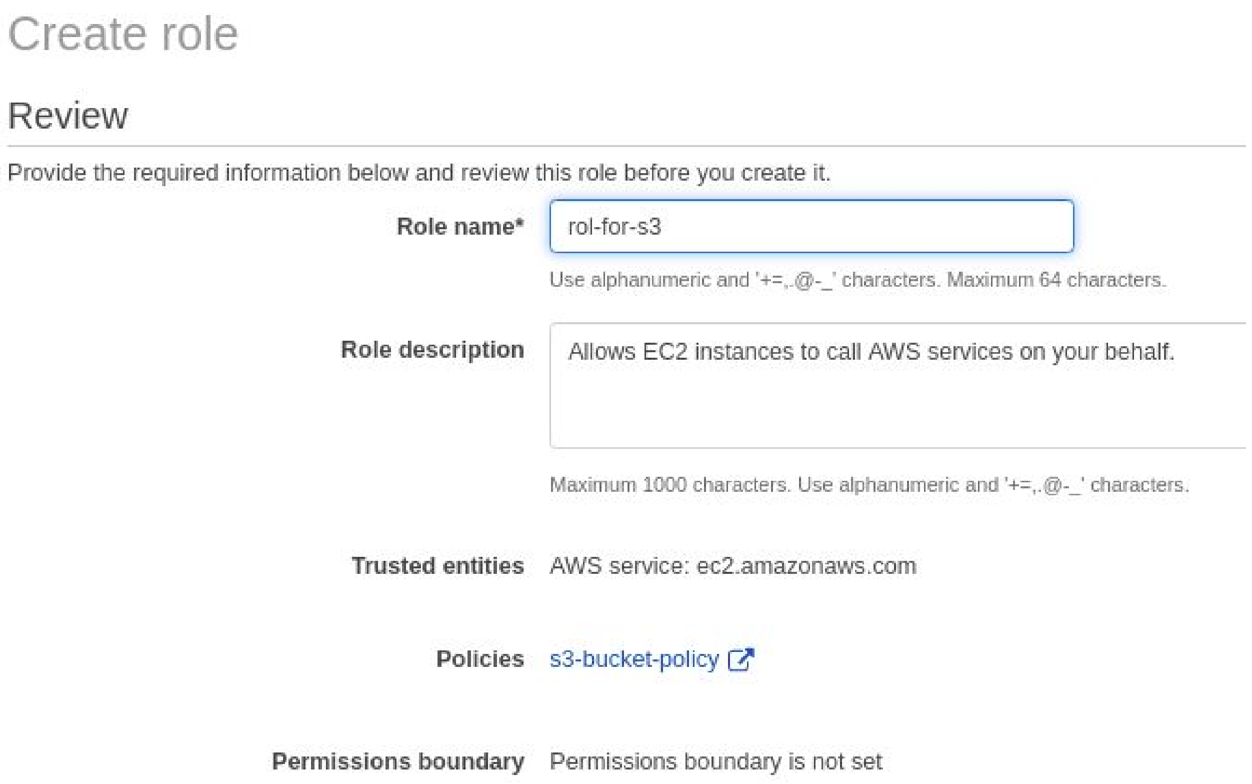


Create role

▾ Attach permissions policies

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

		Policy name ▼	Used as
☑	▸	s3-bucket-policy	None



Create role

Review

Provide the required information below and review this role before you create it.

Role name*: rol-for-s3

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

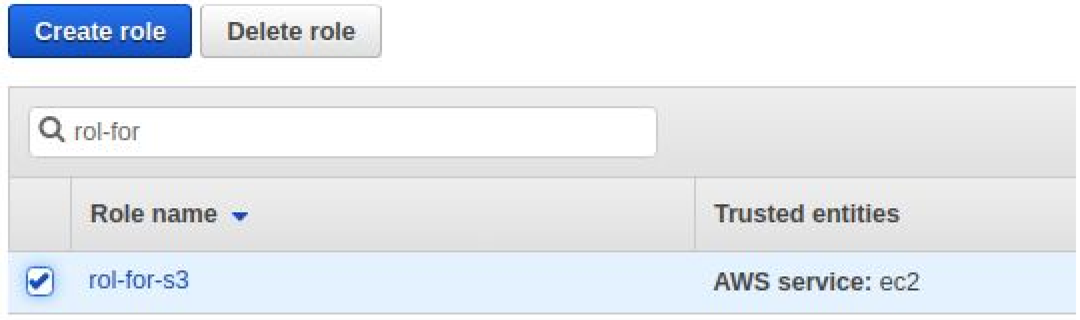
Role description: Allows EC2 instances to call AWS services on your behalf.

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

Trusted entities: AWS service: ec2.amazonaws.com

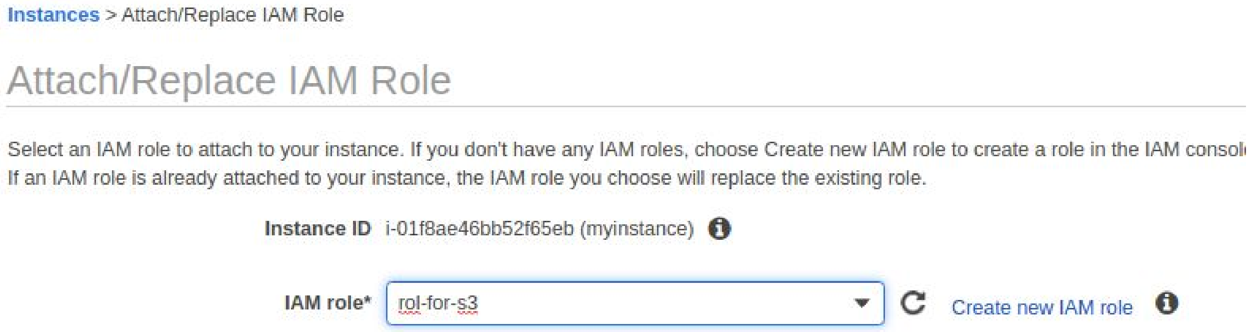
Policies: s3-bucket-policy

Permissions boundary: Permissions boundary is not set



rol-for

	Role name	Trusted entities
☑	rol-for-s3	**AWS service:** ec2



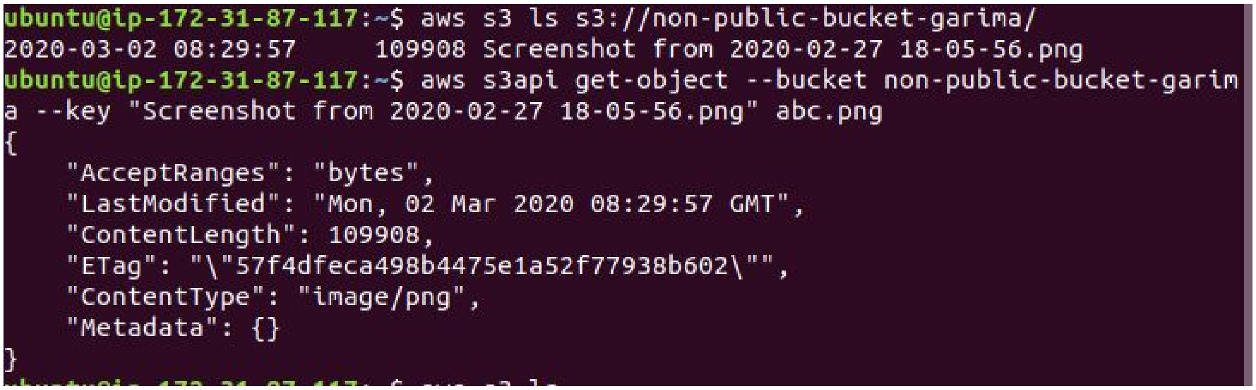
Instances > Attach/Replace IAM Role

Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM consol
If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID: i-01f8ae46bb52f65eb (myinstance)

IAM role*: rol-for-s3



```
ubuntu@ip-172-31-87-117:~$ aws s3 ls s3://non-public-bucket-garima/
2020-03-02 08:29:57     109908 Screenshot from 2020-02-27 18-05-56.png
ubuntu@ip-172-31-87-117:~$ aws s3api get-object --bucket non-public-bucket-garim
a --key "Screenshot from 2020-02-27 18-05-56.png" abc.png
{
    "AcceptRanges": "bytes",
    "LastModified": "Mon, 02 Mar 2020 08:29:57 GMT",
    "ContentLength": 109908,
    "ETag": "\"57f4dfeca498b4475e1a52f77938b602\"",
    "ContentType": "image/png",
    "Metadata": {}
}
ubuntu@ip-172-31-87-117:~$ aws s3 ls
```