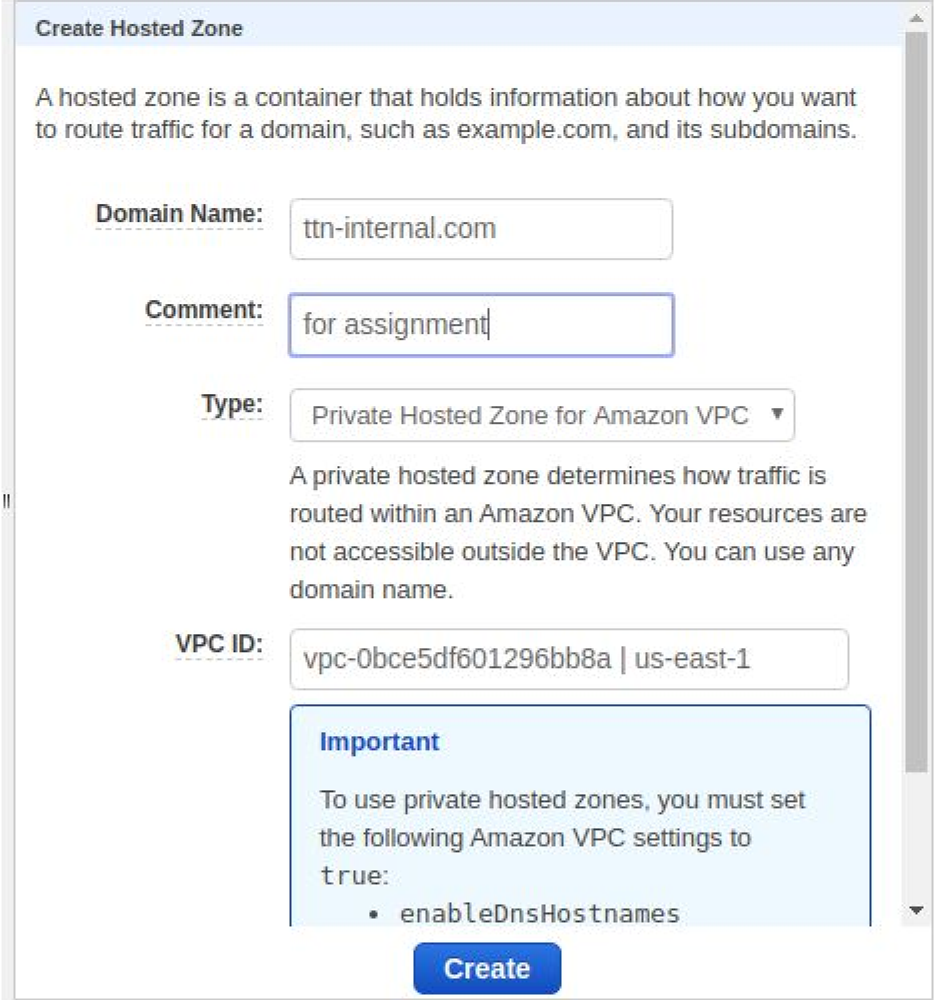
1) create a private hosted zone named "ttn-internal.com" attached to the default vpc. and created a cname record "myloadbalance.ttn-internal.com" for any load balancer pointed to its dns. Do reverse lookup for the record from any instance of the vpc and share the resul



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: for assignment

Type: Private Hosted Zone for Amazon VPC

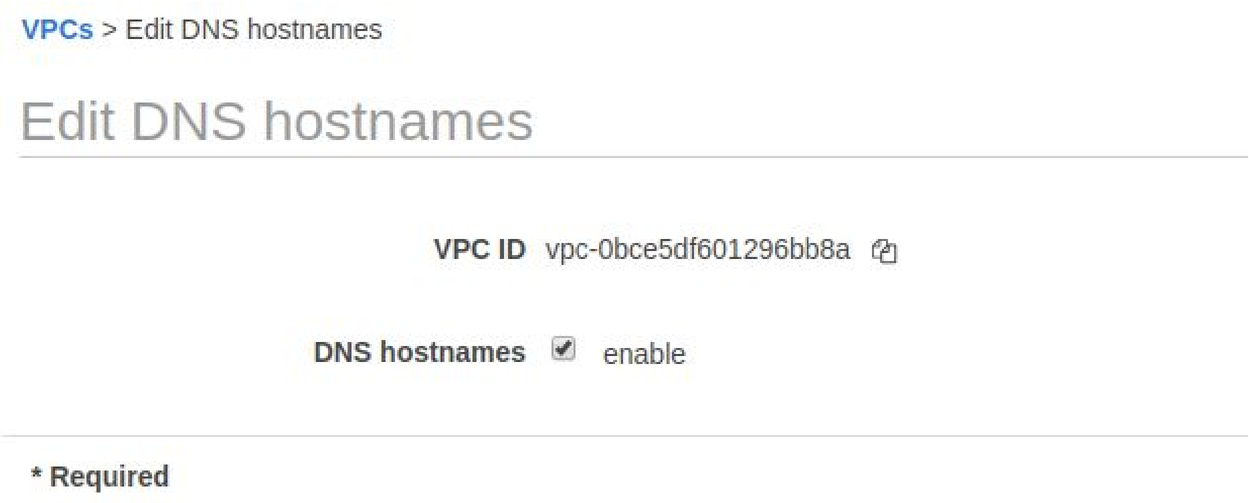
A private hosted zone determines how traffic is routed within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any domain name.

VPC ID: vpc-0bce5df601296bb8a | us-east-1

Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`



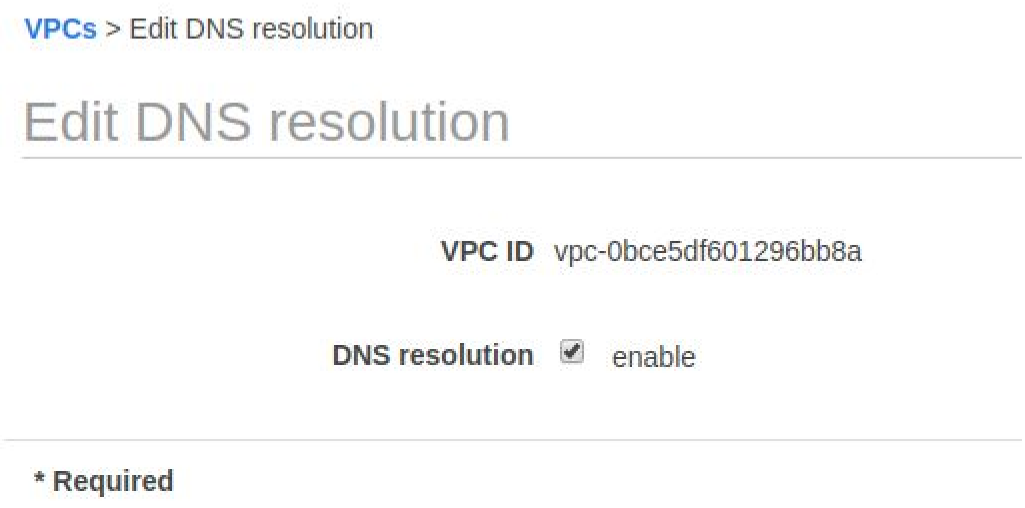
VPCs > Edit DNS hostnames

Edit DNS hostnames

VPC ID vpc-0bce5df601296bb8a

DNS hostnames ☑ enable

* Required



VPCs > Edit DNS resolution

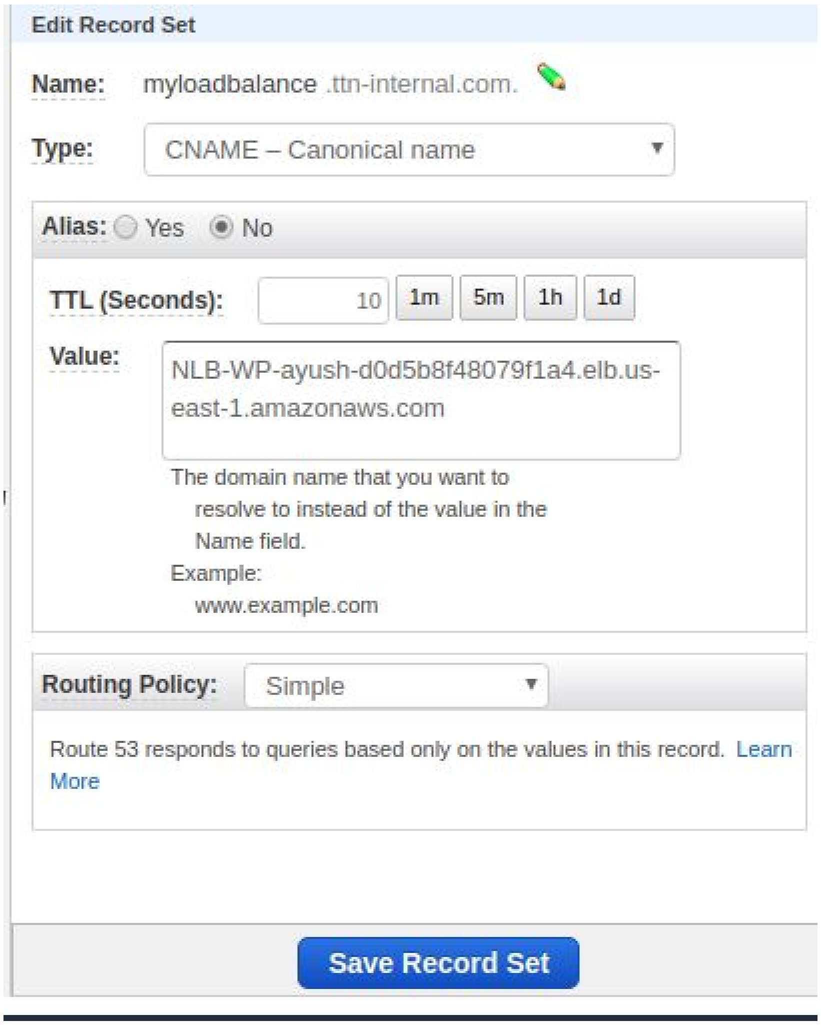
Edit DNS resolution

VPC ID vpc-0bce5df601296bb8a

DNS resolution ☑ enable

* Required

\



Edit Record Set

Name: myloadbalance .ttn-internal.com.

Type: CNAME – Canonical name

Alias: ○ Yes ● No

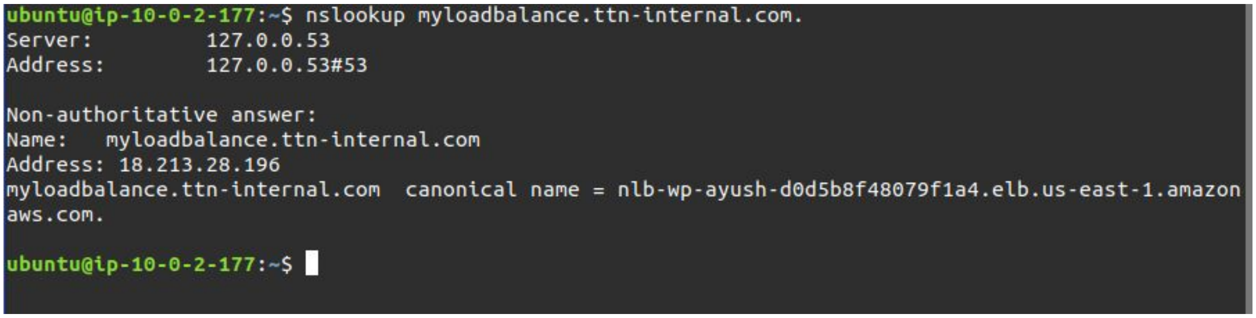
TTL (Seconds): 10

Value: NLB-WP-ayush-d0d5b8f48079f1a4.elb.us-east-1.amazonaws.com

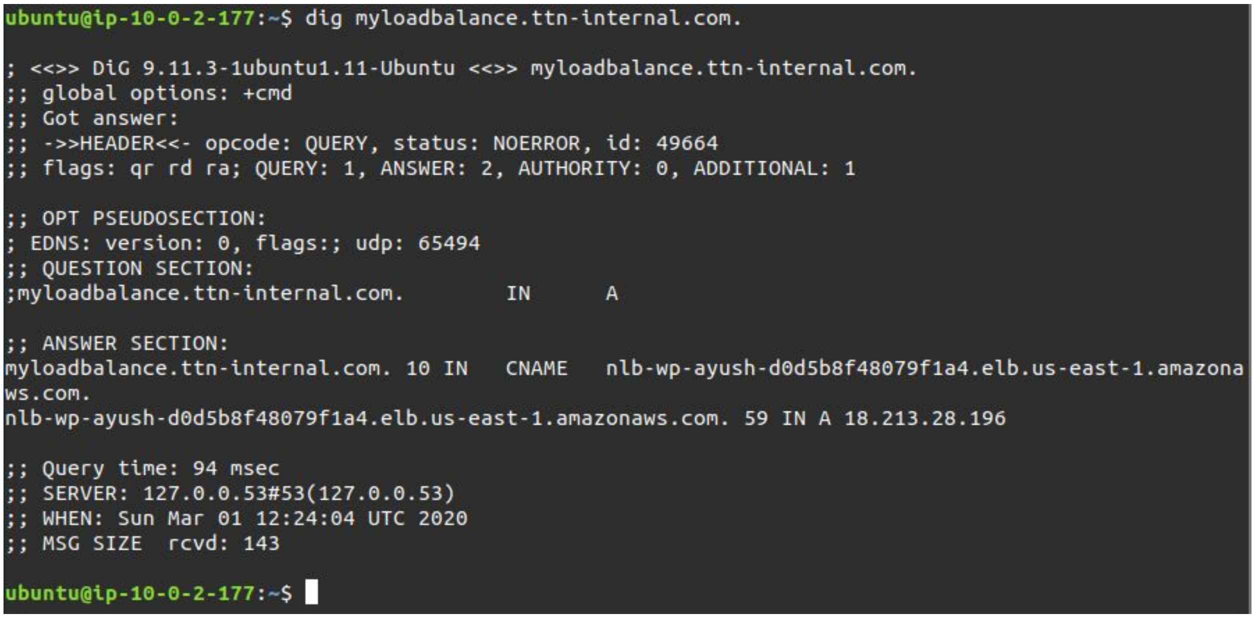
The domain name that you want to resolve to instead of the value in the Name field.
Example:
www.example.com

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

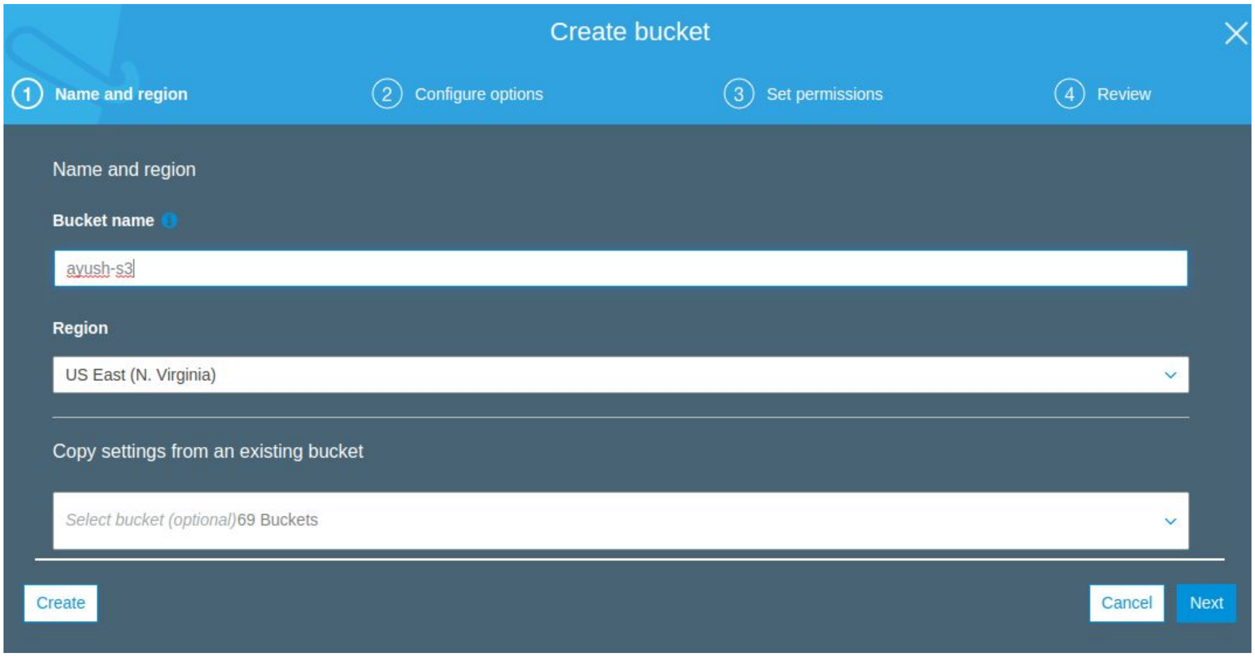


```
ubuntu@ip-10-0-2-177:~$ nslookup myloadbalance.ttn-internal.com.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   myloadbalance.ttn-internal.com
Address: 18.213.28.196
myloadbalance.ttn-internal.com  canonical name = nlb-wp-ayush-d0d5b8f48079f1a4.elb.us-east-1.amazon
aws.com.

ubuntu@ip-10-0-2-177:~$ 
```



```
ubuntu@ip-10-0-2-177:~$ dig myloadbalance.ttn-internal.com.

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> myloadbalance.ttn-internal.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49664
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;myloadbalance.ttn-internal.com.        IN      A

;; ANSWER SECTION:
myloadbalance.ttn-internal.com. 10 IN   CNAME   nlb-wp-ayush-d0d5b8f48079f1a4.elb.us-east-1.amazona
ws.com.
nlb-wp-ayush-d0d5b8f48079f1a4.elb.us-east-1.amazonaws.com. 59 IN A 18.213.28.196

;; Query time: 94 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Mar 01 12:24:04 UTC 2020
;; MSG SIZE  rcvd: 143

ubuntu@ip-10-0-2-177:~$ 
```

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

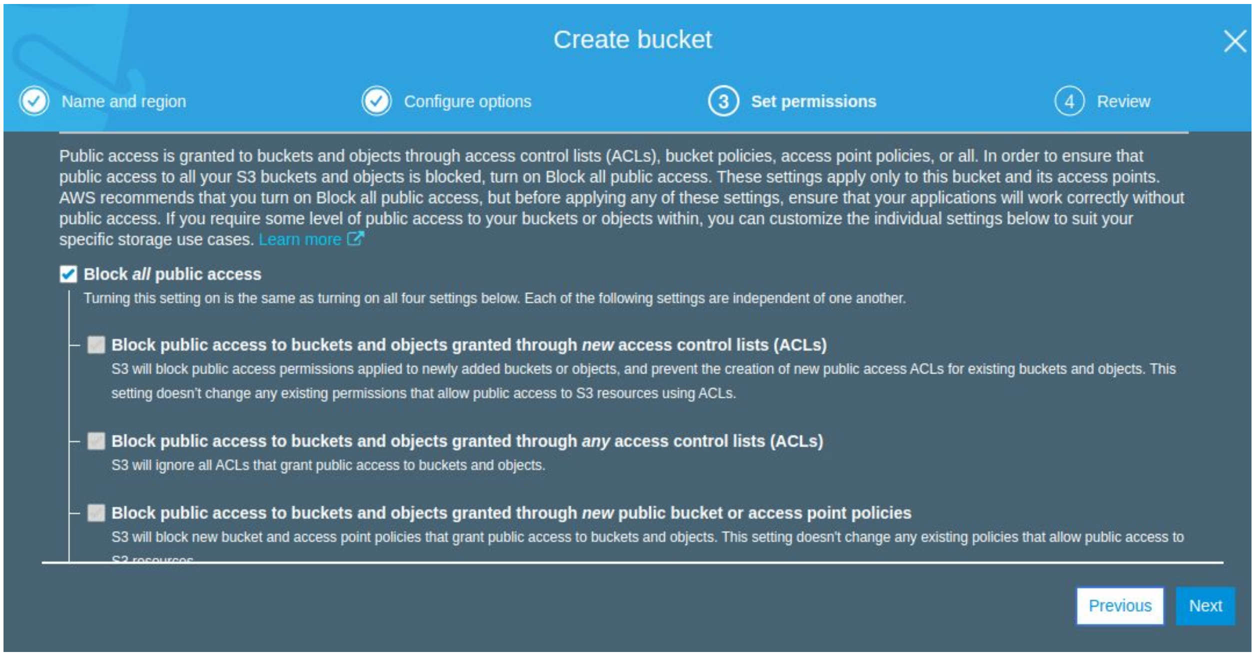
ayush-s3

Region

US East (N. Virginia)

Copy settings from an existing bucket

Select bucket (optional) 69 Buckets

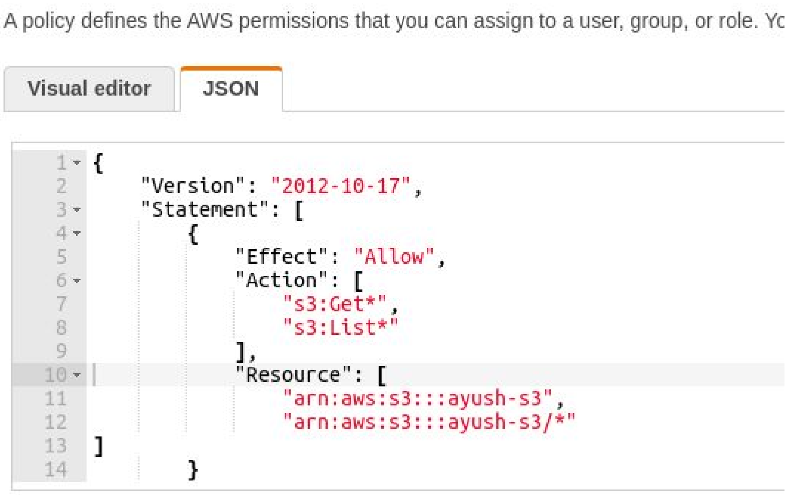


Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

☑ **Block *all* public access**

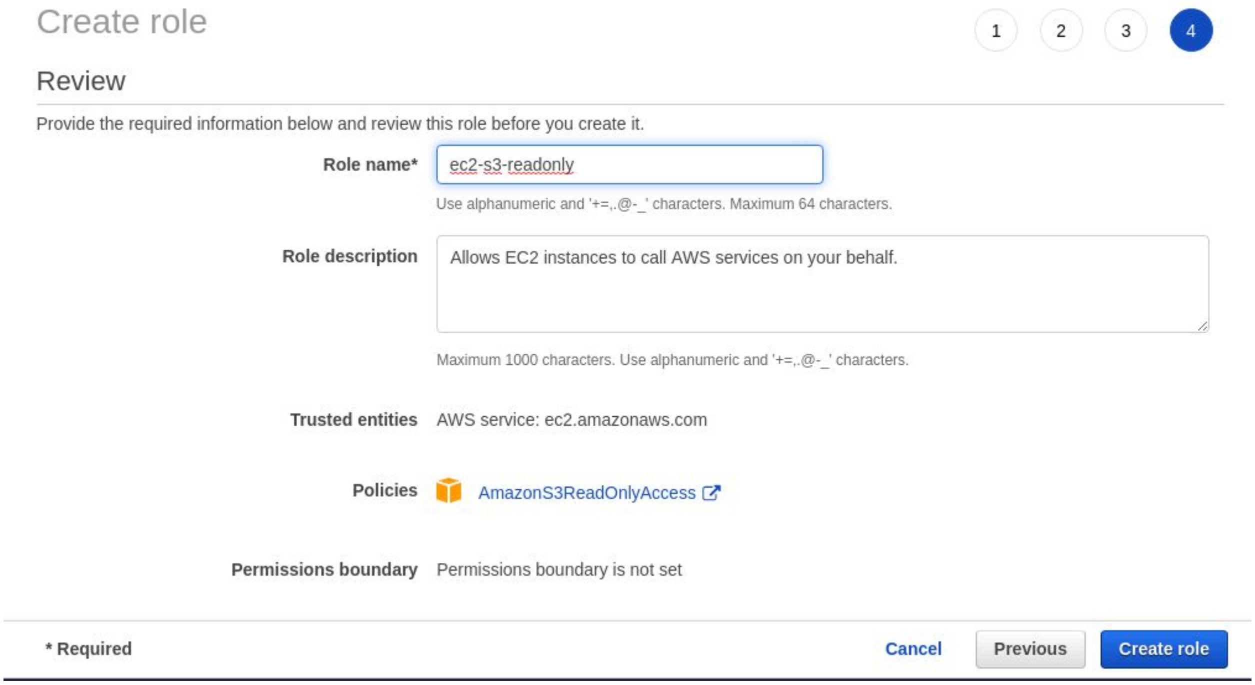
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources



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

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



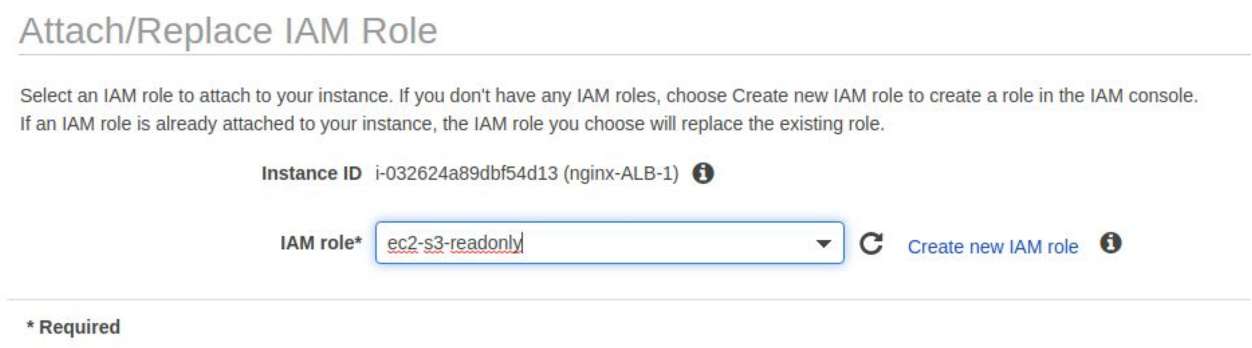
Create role

Review

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

Role name*	ec2-s3-readonly 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	AmazonS3ReadOnlyAccess
Permissions boundary	Permissions boundary is not set

* Required

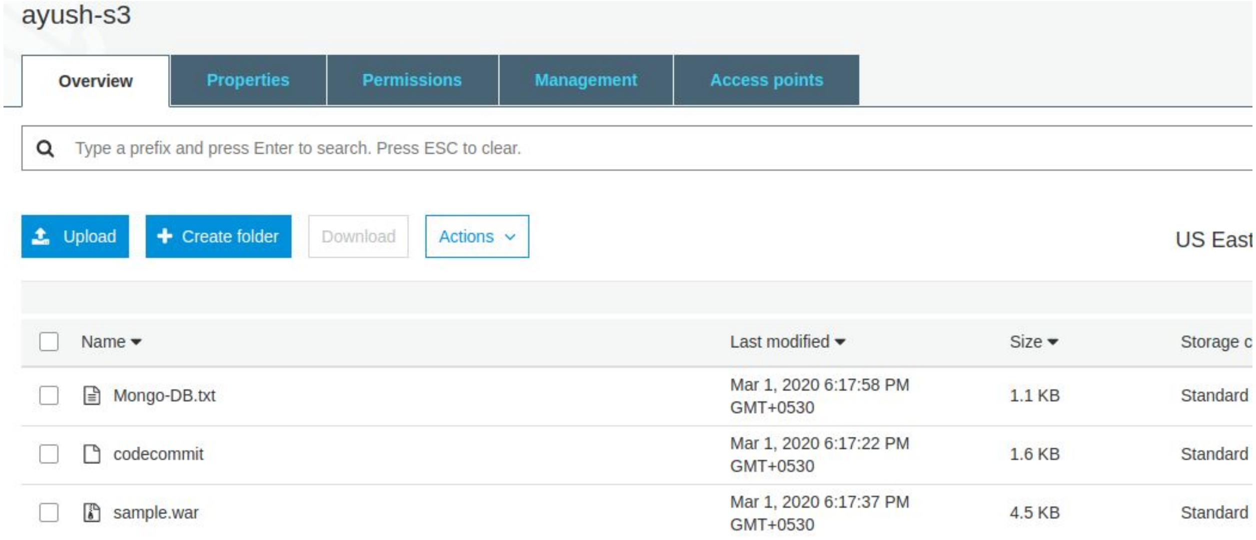


Attach/Replace IAM Role

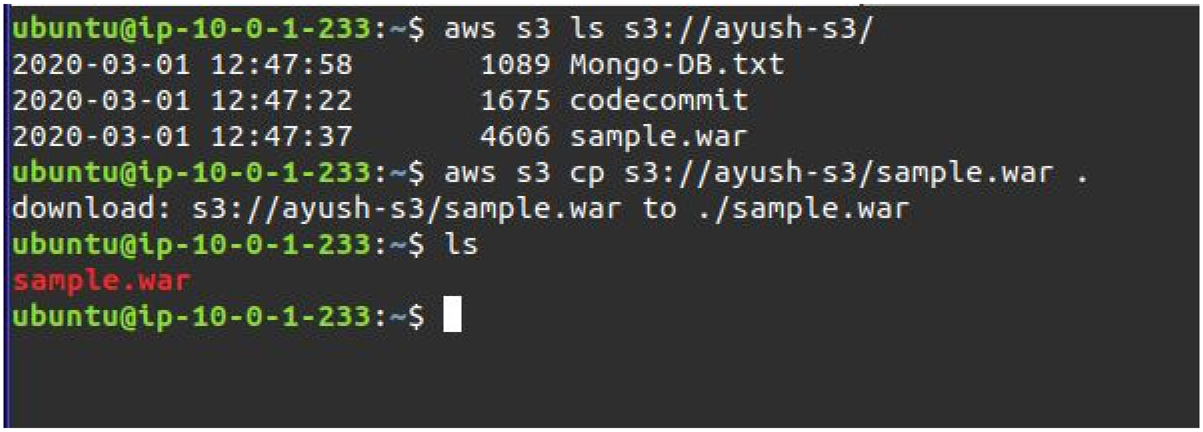
Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID	i-032624a89dbf54d13 (nginx-ALB-1)
IAM role*	ec2-s3-readonly

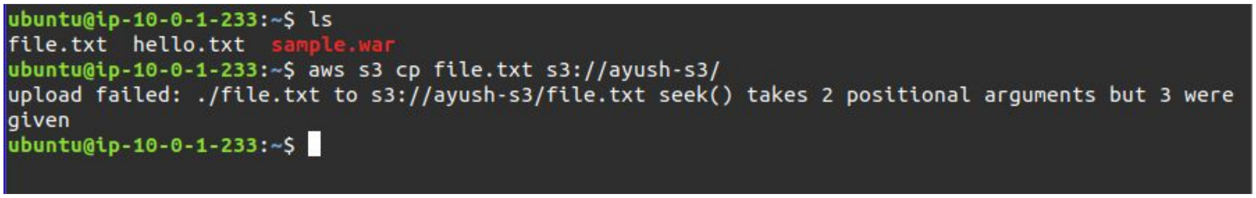
* Required



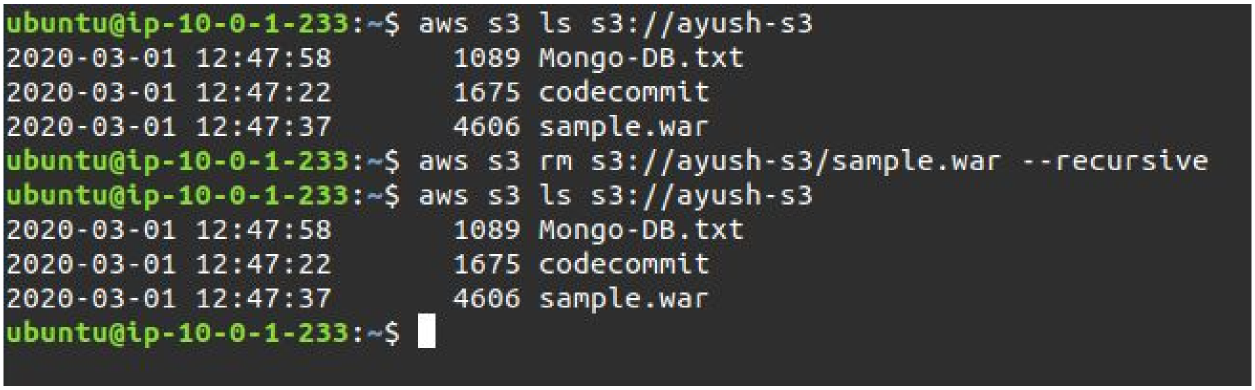
□	Name	Last modified	Size	Storage c
□	Mongo-DB.txt	Mar 1, 2020 6:17:58 PM GMT+0530	1.1 KB	Standard
□	codecommit	Mar 1, 2020 6:17:22 PM GMT+0530	1.6 KB	Standard
□	sample.war	Mar 1, 2020 6:17:37 PM GMT+0530	4.5 KB	Standard



```
ubuntu@ip-10-0-1-233:~$ aws s3 ls s3://ayush-s3/
2020-03-01 12:47:58       1089 Mongo-DB.txt
2020-03-01 12:47:22       1675 codecommit
2020-03-01 12:47:37       4606 sample.war
ubuntu@ip-10-0-1-233:~$ aws s3 cp s3://ayush-s3/sample.war .
download: s3://ayush-s3/sample.war to ./sample.war
ubuntu@ip-10-0-1-233:~$ ls
sample.war
ubuntu@ip-10-0-1-233:~$
```



```
ubuntu@ip-10-0-1-233:~$ ls
file.txt  hello.txt  sample.war
ubuntu@ip-10-0-1-233:~$ aws s3 cp file.txt s3://ayush-s3/
upload failed: ./file.txt to s3://ayush-s3/file.txt seek() takes 2 positional arguments but 3 were
given
ubuntu@ip-10-0-1-233:~$
```



```
ubuntu@ip-10-0-1-233:~$ aws s3 ls s3://ayush-s3
2020-03-01 12:47:58       1089 Mongo-DB.txt
2020-03-01 12:47:22       1675 codecommit
2020-03-01 12:47:37       4606 sample.war
ubuntu@ip-10-0-1-233:~$ aws s3 rm s3://ayush-s3/sample.war --recursive
ubuntu@ip-10-0-1-233:~$ aws s3 ls s3://ayush-s3
2020-03-01 12:47:58       1089 Mongo-DB.txt
2020-03-01 12:47:22       1675 codecommit
2020-03-01 12:47:37       4606 sample.war
ubuntu@ip-10-0-1-233:~$
```