

Session : S3, Route 53 & DNS

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.

Filter by tags and attributes or search by keyword				
1 to 1 of 1				
Name	DNS name	State	VPC ID	Availability
Jay-ALB	Jay-ALB-2008596953.us-east-1.elb.amazonaws.com	active	vpc-0da5f25424642658b	us-east-1

ARN	arn:aws:elasticloadbalancing:us-east-1:187632318301:loadbalancer/app/Jay-ALB/79f7b52525f82b4e
DNS name	Jay-ALB-2008596953.us-east-1.elb.amazonaws.com (A Record)
State	active
Type	application
Scheme	internet-facing
IP address type	ipv4

Edit IP address type

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:

Comment:

Type:

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:

Important

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

- enableDnsHostnames

Create

☐ Aliases Only
☐ Weighted Only

<< < Displaying 1 to 3 out of 3 Record Sets > >

Name	Type	Value	Eva
ttn3.internal.com.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-
ttn3.internal.com.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz	-
myloadbalancejay.ttn3.internal.com.	CNAME	Jay-ALB-2008596953.us-east-1.elb.amazonaws.cor	-

Edit Record Set

Name: myloadbalancejay.ttn3.internal.com.

Type: CNAME – Canonical name

Alias: ☐ Yes ☒ No

TTL (Seconds):

Value: Jay-ALB-2008596953.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

Route 53 responds to queries based only on the values in this record. [Learn More](#)

```
ubuntu@ip-10-0-1-249:~$ sudo dig myloadbalancejay.ttn3.internal.com

;; <<>> DiG 9.11.3-1ubuntu1.1-Ubuntu <<>> myloadbalancejay.ttn3.internal.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36261
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;myloadbalancejay.ttn3.internal.com. IN A

;; ANSWER SECTION:
myloadbalancejay.ttn3.internal.com. 60 IN CNAME jay-alb-2008596953.us-east-1.elb.amazonaws.com.
jay-alb-2008596953.us-east-1.elb.amazonaws.com. 59 IN A 54.236.73.61
jay-alb-2008596953.us-east-1.elb.amazonaws.com. 59 IN A 52.20.113.45

;; Query time: 80 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Mar 02 18:04:30 UTC 2020
;; MSG SIZE rcvd: 152

ubuntu@ip-10-0-1-249:~$ curl myloadbalancejay.ttn3.internal.com
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
  body {
    width: 35em;
    margin: 0 auto;
    font-family: Tahoma, Verdana, Arial, sans-serif;
  }

```

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

S3 buckets

Q aks

+ Create bucket

Edit public access settings

Empty

Delete

☐ Bucket name ▼

Access ⓘ ▼

☐ aks-piv-buc

Bucket and objects

☒ akshaybuck1

Bucket and objects

akshaybuck1

Copy Bucket ARN

Properties

Events	0 Active notifications
Versioning	Enabled
MFA delete	Disabled
Logging	Disabled
Static web hosting	Disabled
Tags	0 Tags
Requester pays	Disabled
Object lock	Disabled
Transfer acceleration	Disabled

Permissions

Owner	nitin.bhadoria
Block public access	Enabled
Bucket policy	No
Access control list	1 Grantees

Expand all | Collapse all

▼ S3 (1 action)

Clone Remove

► Service

S3

► Actions

Read

GetObject

▼ Resources

☒ Specific

☐ All resources

close

object ?

arn:aws:s3:::akshaybuck1/*

EDIT

+

☐ Any

Add ARN to restrict access

► Request conditions

Specify request conditions (optional)

+ Add additional permissions

Summary

Delete role

Role ARN	arn:aws:iam::187632318301:role/Jay-S3-role
Role description	Allows EC2 instances to call AWS services on your behalf. Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/Jay-S3-role
Path	/
Creation time	2020-03-02 23:53 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions

Trust relationships

Tags (3)

Access Advisor

Revoke sessions

▼ Permissions policies (1 policy applied)

Attach policies

[+ Add inline policy](#)

Policy name ▼	Policy type ▼	
▶ Jay-S3-policy	Managed policy	✕

Add permissions to Jay-Alice

1

2

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy



Filter policies ▼		Q Jay		Showing 4 results	
	Policy name ▼	Type	Used as		
<input type="checkbox"/>	▶ Jay-Assume-Role	Customer managed	Permissions policy (1)		
<input type="checkbox"/>	▶ Jay-DBAdmin-policy	Customer managed	Permissions policy (1)		
<input type="checkbox"/>	▶ Jay-Dev-Policy	Customer managed	Permissions policy (2)		
<input checked="" type="checkbox"/>	▶ Jay-S3-policy	Customer managed	Permissions policy (1)		

Cancel

Next: Review

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-0b5a1e96e0c9d54e6 (Akshay)

IAM role* Jay-S3-role

[Create new IAM role](#)

* Required

Cancel

Apply

```
ubuntu@ip-172-31-228-111:~$ aws s3 ls
```

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied

```
ubuntu@ip-172-31-228-111:~$ aws s3api get-object --bucket akshaybuck1 --key "VPC .pdf" jay.pdf
```

```
{
  "AcceptRanges": "bytes",
  "LastModified": "Wed, 26 Feb 2020 18:42:11 GMT",
  "ContentLength": 882990,
  "ETag": "\"00bf80b575650c4de649cf7bfe0549e3\"",
  "VersionId": "943sdeqjUei0N_wJMXFrnPzLu_ncyEJj",
  "ContentType": "application/octet-stream",
  "Metadata": {}
}
```

```
ubuntu@ip-172-31-228-111:~$ █
```