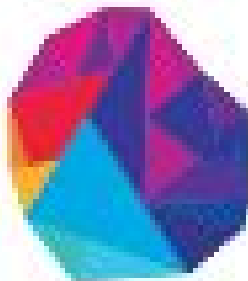


ASSESSMENT ON S3, ROUTE53 AND DNS

**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.

STEP 1: Create a load balancer

Create Load Balancer Actions						
Filter by tags and attributes or search by keyword						
	Name	DNS name	State	VPC ID	Availability Zones	Type
	Q1route53lb	Q1route53lb-549966066.us-...	provisioning	vpc-94ab21ee	us-east-1c, us-east-1a, ...	application

STEP 2: Attach the instance to load balancer in vpc(default)

Step 6: Review

Please review the load balancer details before continuing

Load balancer	
Name	Q1route53lb
Scheme	internet-facing
Listeners	Port:80 - Protocol:HTTP
IP address type	ipv4
VPC	vpc-94ab21ee
Subnets	subnet-6784fa00, subnet-f59edbdb, subnet-4ff4fa05, subnet-e592e9b9, subnet-af028091, subnet-94a8989b
Tags	
Security groups	
Security groups	sg-95ce75d3
Routing	
Target group	New target group
Target group name	route53Tg
Port	80
Target type	instance
Protocol	HTTP
Health check protocol	HTTP
Path	/
Health check port	traffic port
Healthy threshold	5

STEP 3: Create a private Hosted Zone named "ttn-internal.com" in Route53

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:

Diksha Tomar

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-94ab21ee | us-east-1

Important

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

- enableDnsHostnames
- enableDnsSupport

Back to Hosted Zones

Create Record Set

Import Zone File

Delete Record Set

Test Record Set

Q	Record Set Name	X	Any Type ▾	<input type="checkbox"/> Aliases Only	<input type="checkbox"/> Weighted Only	⏪ ⏩	Displaying 1 to 2 out of 2 Record Sets	⏪ ⏩
<input type="checkbox"/>	Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Region	W
<input checked="" type="checkbox"/>	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.	-	-	172800		
<input type="checkbox"/>	ttn-internal.com.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz	-	-	900		

STEP 4: Enable DNS Resolution in VPC

Create VPC Actions ^

Filter by tags keyword

Name	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
default	available	172.31.0....	-	dopt-7f8eba04

- Delete VPC
- Edit CIDRs
- Create Default VPC
- Create flow log
- Edit DHCP options set
- Edit DNS resolution
- Edit DNS hostnames
- Add/Edit Tags

VPCs > Edit DNS resolution

Edit DNS resolution

VPC ID vpc-94ab21ee

DNS resolution ☒ enable

* Required

STEP 5: EnableDNS Hostname in VPC

VPCs > Edit DNS hostnames

Edit DNS hostnames

VPC ID vpc-94ab21ee

DNS hostnames ☒ enable

* Required

STEP 6: Route53 > Create Record Set

[Back to Hosted Zones](#)

[Create Record Set](#)

Create Record Set

Name:

myloadbalance.ttn-internal.com.

Type:

CNAME – Canonical name

Alias:

☐ Yes ☒ No

TTL (Seconds):

3001m5m1h1d

Value:

Q1route53lb-549966066.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](#)

STEP 7: SSH into your instance and then run nslookup command

*nslookup (name server lookup) is a tool used to perform DNS lookups in Linux. It is used to display DNS details, such as the IP address of a particular computer, the MX records for a domain or the NS servers of a domain.

```
ubuntu@ip-172-31-93-142:~$ 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 = q1route53lb-549966066.us-east-1
.elb.amazonaws.com.
Name:   q1route53lb-549966066.us-east-1.elb.amazonaws.com
Address: 54.175.84.243
Name:   q1route53lb-549966066.us-east-1.elb.amazonaws.com
Address: 52.200.152.194

ubuntu@ip-172-31-93-142:~$
```

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.

STEP 1: Create a S3 bucket with no public access

The screenshot shows the AWS S3 Buckets console. At the top, there's a search bar and a 'Discover the console' link. Below that, there are buttons for '+ Create bucket', 'Edit public access settings', 'Empty', and 'Delete'. A summary shows '1 Buckets' and '1 Regions'. A table lists the buckets:

Bucket name	Access	Region	Date created
<input type="checkbox"/> nonpublics3diksha	Bucket and objects not public	US East (N. Virginia)	Mar 2, 2020 2:20:00 PM GMT+0530

STEP 2: Create a policy

The screenshot shows the 'Create policy' page in the AWS IAM console. It has two tabs: 'Visual editor' (selected) and 'JSON'. A description states: '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 and using JSON. [Learn more](#)'. There's an 'Import managed policy' link. Below, there are 'Expand all' and 'Collapse all' links. The policy configuration is as follows:

- S3 (1 action)**: Clone | Remove
- Service**: S3
- Actions**: Read, GetObject
- Resources**: Specific (selected), All resources (unselected). A search bar shows 'arn:aws:s3::nonpublics3diksha/*' with an 'EDIT' button and a checkbox for 'Any'. A link 'Add ARN to restrict access' is below.
- Request conditions**: Specify request conditions (optional)

Create policy

1

2

Review policy

Name* nopublics3_diksha_policy

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

Description only allowed to download

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

Summary

Q Filter

Service ▾

Access level

Resource

Request condition

Allow (1 of 223 services) [Show remaining 222](#)

S3

Limited: Read

BucketName | string like |
nopublics3diksha, ObjectPath | string
like | All

None

Edit nopublics3_diksha_policy

1

2

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 and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

[Expand all](#) | [Collapse all](#)

▼ S3 (1 action)

[Clone](#) [Remove](#)

► Service S3

► Actions Read

GetObject

► Resources arn:aws:s3:::nopublics3diksha/*

► Request conditions [Specify request conditions \(optional\)](#)

STEP 3: Create a role and attach the above policy

Roles > Nopublic_s3_diksha

Summary

Delete role

Role ARN `arn:aws:iam::200332499555:role/Nopublic_s3_diksha` [🔗](#)
Role description Allows EC2 instances to call AWS services on your behalf. | [Edit](#)
Instance Profile ARNs `arn:aws:iam::200332499555:instance-profile/Nopublic_s3_diksha` [🔗](#)
Path /
Creation time 2020-03-02 15:20 UTC+0530
Last activity Not accessed in the tracking period
Maximum CLI/API session duration 1 hour [Edit](#)

Permissions

Trust relationships

Tags (2)

Access Advisor

Revoke sessions

▼ Permissions policies (1 policy applied)

Attach policies

➕ Add inline policy

Policy name ▼	Policy type ▼	
▶ npublics3_diksha_policy	Managed policy	✕

▶ Permissions boundary (not set)

STEP 4: Attach it to your instance

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Purpose	Instance ID	Instance Type	Availability Zone	Instance State
<input checked="" type="checkbox"/>	Nopublic_s3_diksha_instance	Attaching role nopublic_s3 to it	i-01349819dc49397fd	t2.micro	us-east-1d	running

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 console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-01349819dc49397fd (Nopublic_s3_diksha_instance) [i](#)

IAM role* [↻](#) [Create new IAM role](#) [i](#)

* Required

STEP 5: Is into your s3 bucket. You will see that access is denied

```
ubuntu@ip-172-31-36-78:~$ aws s3 ls s3://nonpublic3diksha/
```

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

```
ubuntu@ip-172-31-36-78:~$
```


STEP 6: Download the object from that bucket and you will be allowed to do so.

```
ubuntu@ip-172-31-36-78:~$ aws s3api get-object --bucket nonpublics3diksha --key "giphy.gif" giphy
{
  "AcceptRanges": "bytes",
  "LastModified": "Mon, 02 Mar 2020 10:08:53 GMT",
  "ContentLength": 2046036,
  "ETag": "\"1fdf64e2ede6f751fd668788a6900b6d\"",
  "ContentType": "image/gif",
  "Metadata": {}
}
ubuntu@ip-172-31-36-78:~$
```