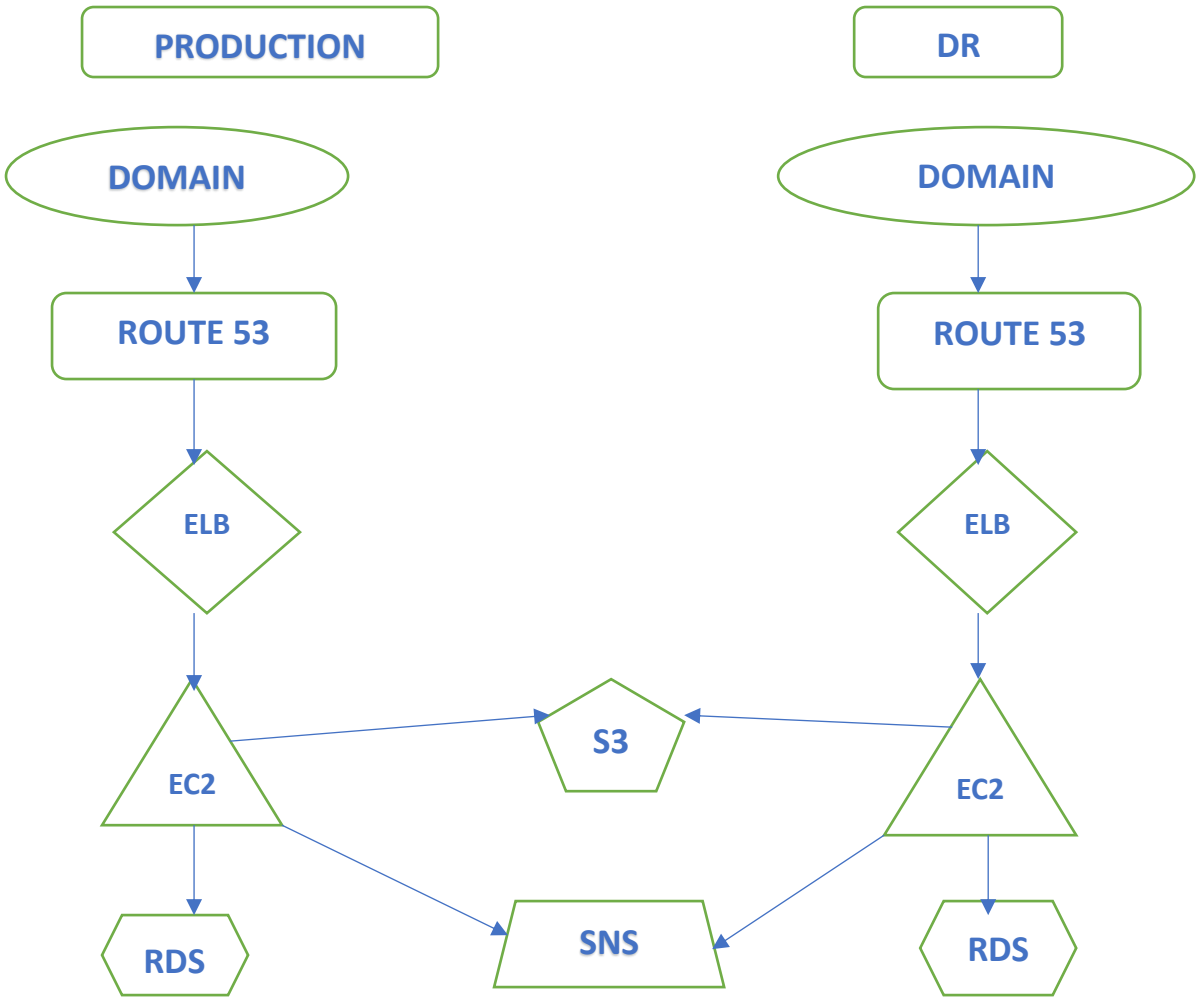
# AWS PROJECT

## IMPLEMENTING SAME REGION DISASTER RECOVERY IN ACTIVE PASSIVE FAILOVER POLICY

Project details:

In this project, I had done backup and restore the primary environment for the AWS cloud infrastructure in same region disaster recovery for active passive failover routing policy and give alert email notification for any ec2 instance state is changed for production environment.

Project Architecture:




Steps to build this project:

Step 1: Create a Secure Socket Layer certificate in amazon certificate manager.

Step 2: Create a hosted zone in Route 53 and attached to the domain.

Step 3: Create a subnet group and database in RDS.

Step 4: Create an IAM role for ec2 instance.

Step 5: To launch an ec2 instance for production and DR server.

Step 6: Create a classic load balancer for production and DR server.

Step 7: Mapping with load balancer in route 53 for create failover records.

Step 8: ACM certificate mapping with load balancer.

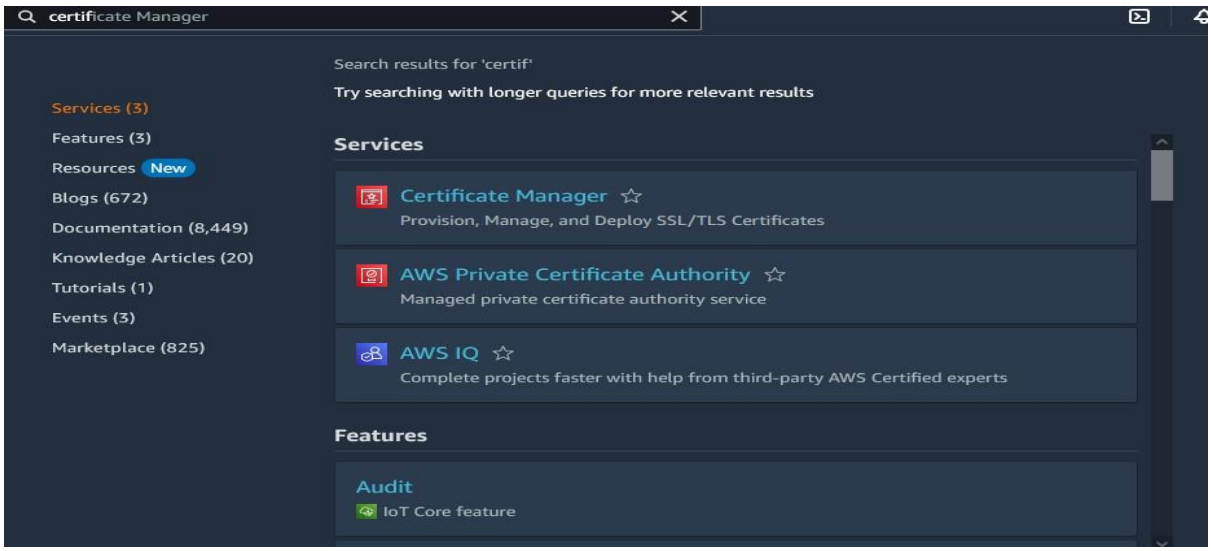
Step 9: Create a S3 bucket and Synchronuos the production and DR server.

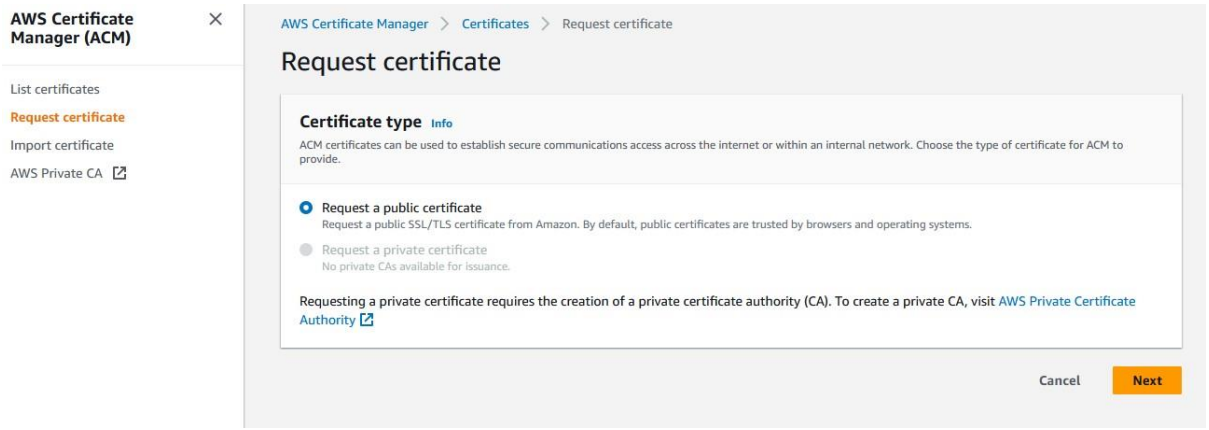
Step 10: Create alert notification for ec2 instance state change (SNS,AMAZON EVENTBRIDGE RULE).

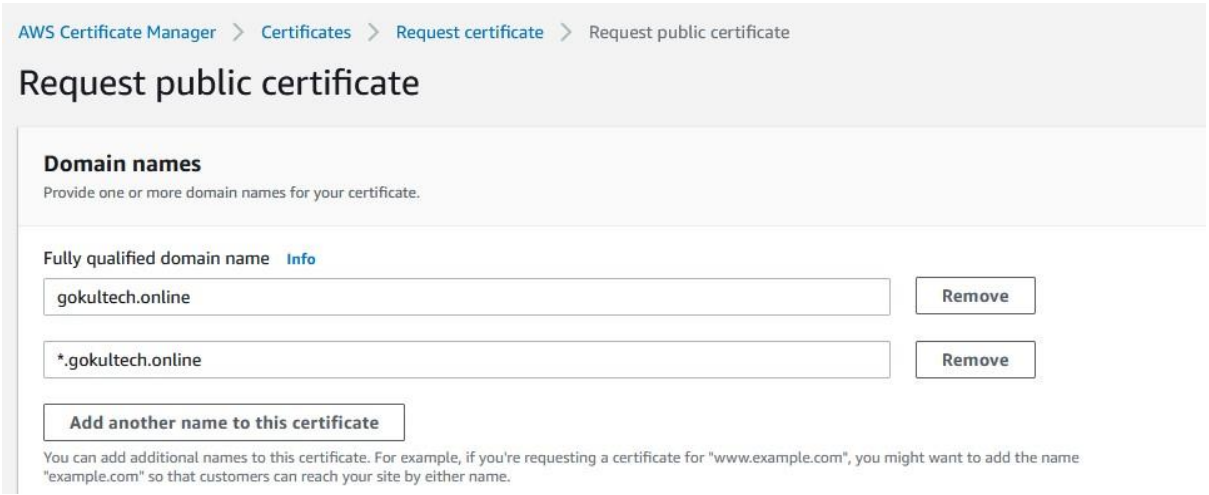
Detailed Explanations in project:

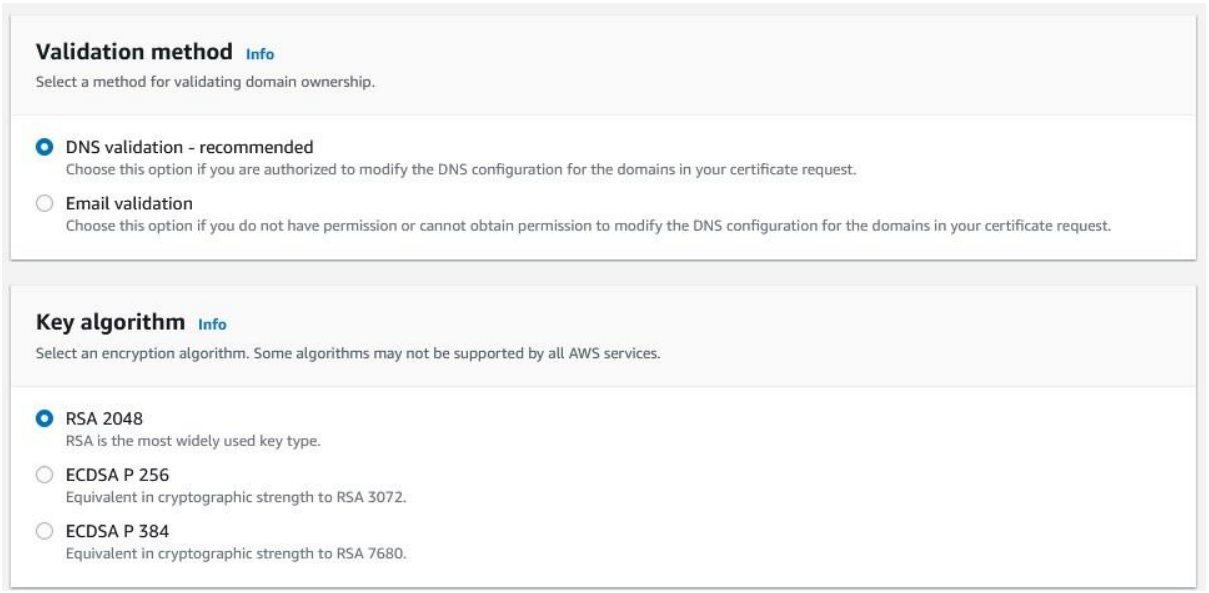
Step 1: Create a Secure Socket Layer certificate in amazon certificate manager.

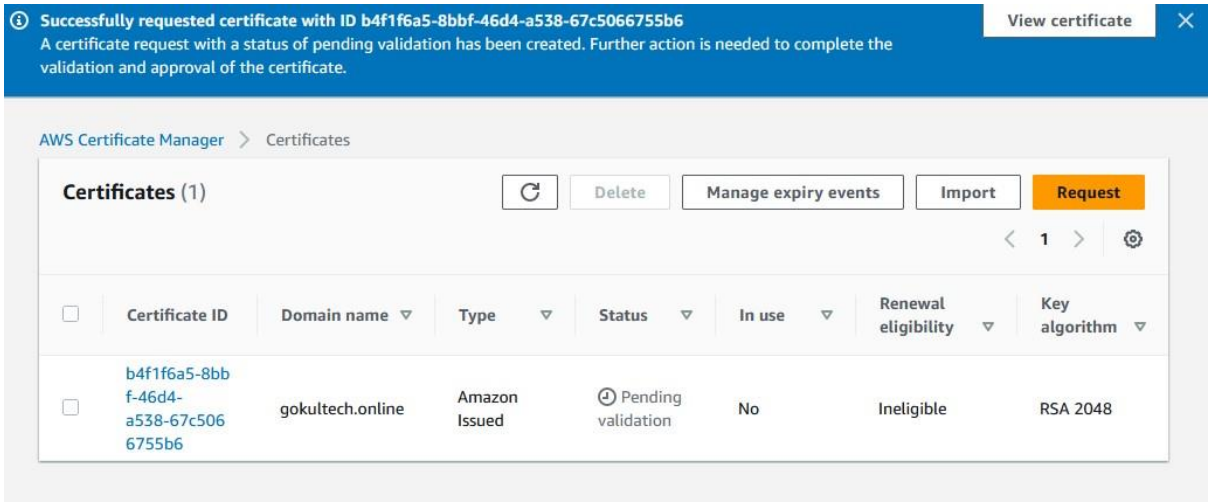
Go to ACM → request a certificate → enter the details → request. Then the status is pending validation → create set record for certificate → select certificate id → scroll down → create record for route 53 → then create records → wait 30 minutes for certificate issued.

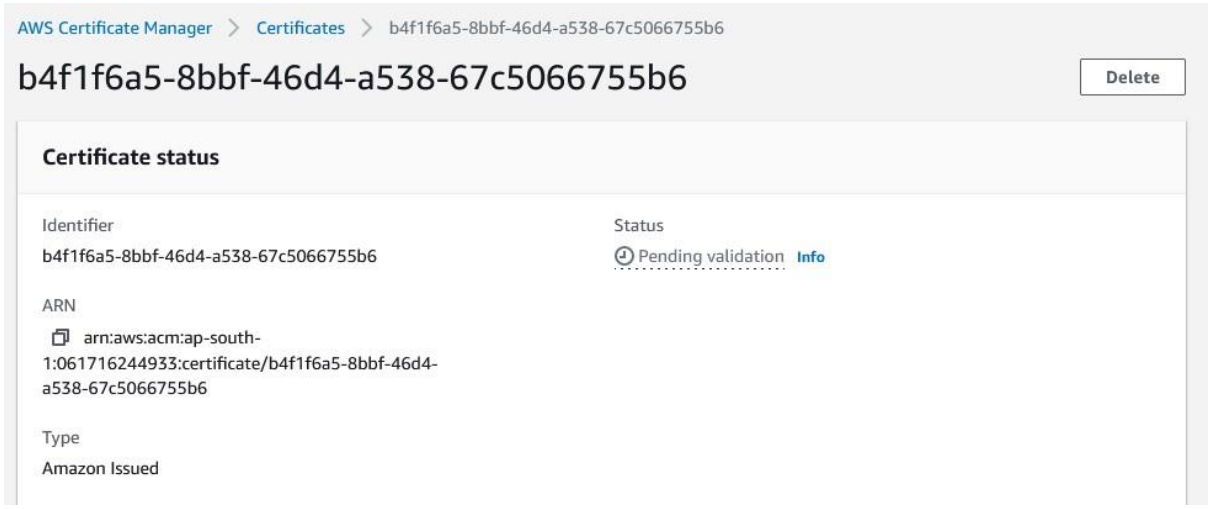


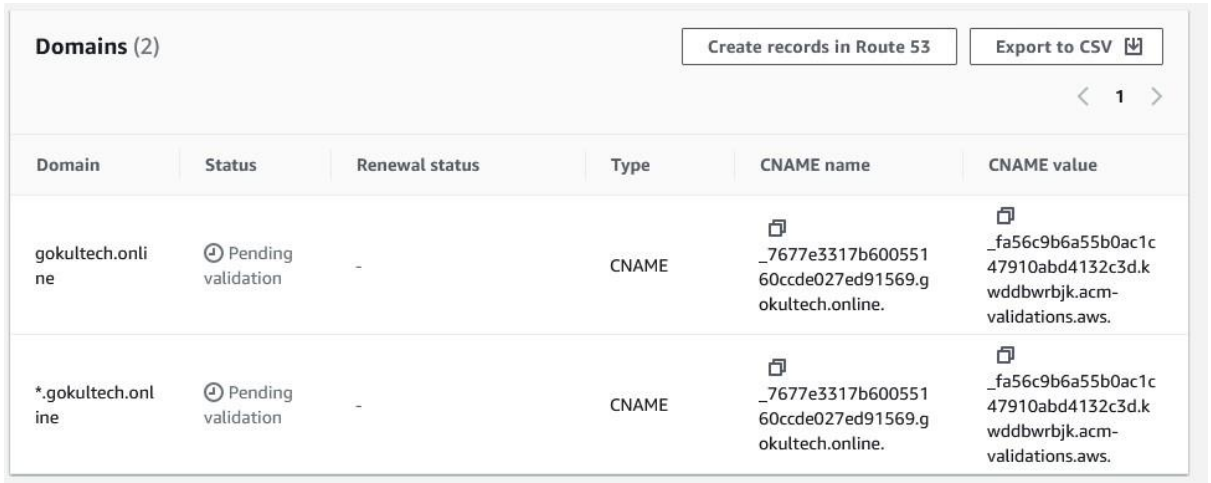


AWS Certificate Manager (ACM)
List certificates
Request certificate
Import certificate
AWS Private CA
AWS Certificate Manager > Certificates > Request certificate
Request certificate
Certificate type Info
ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for ACM to provide.
Request a public certificate
Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.
Request a private certificate
No private CAs available for issuance.
Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit AWS Private Certificate Authority
Cancel
Next

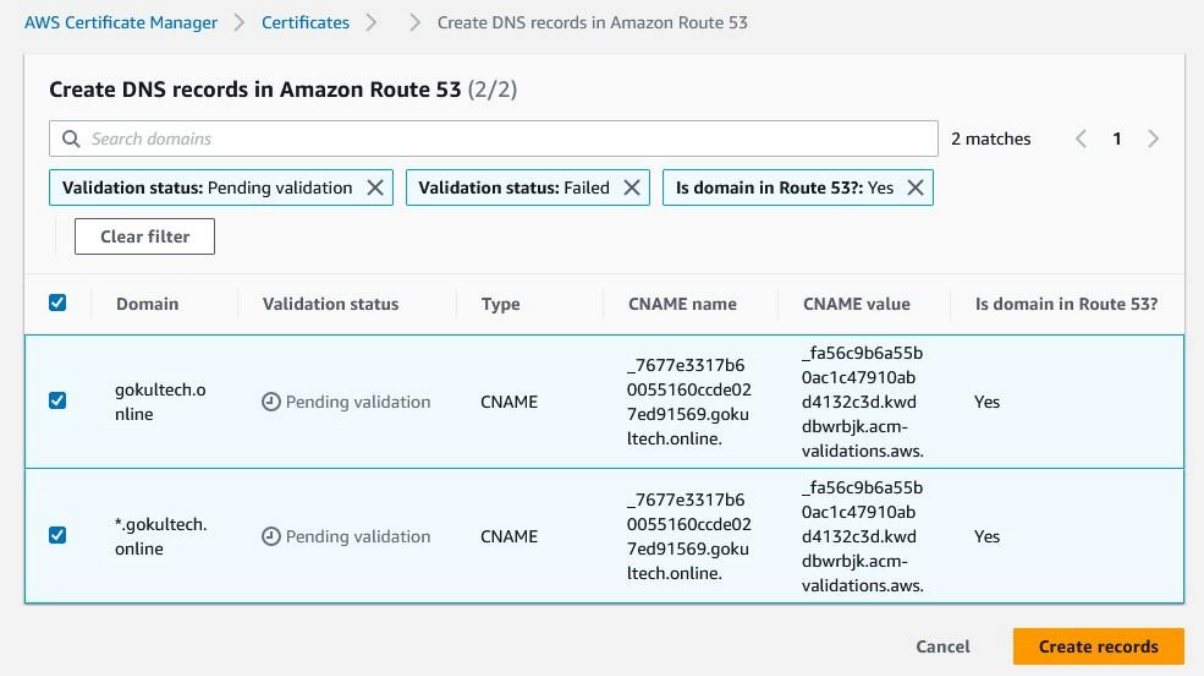

AWS Certificate Manager > Certificates > Request certificate > Request public certificate
Request public certificate
Domain names
Provide one or more domain names for your certificate.
Fully qualified domain name Info
gokultech.online
Remove
*.gokultech.online
Remove
Add another name to this certificate
You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

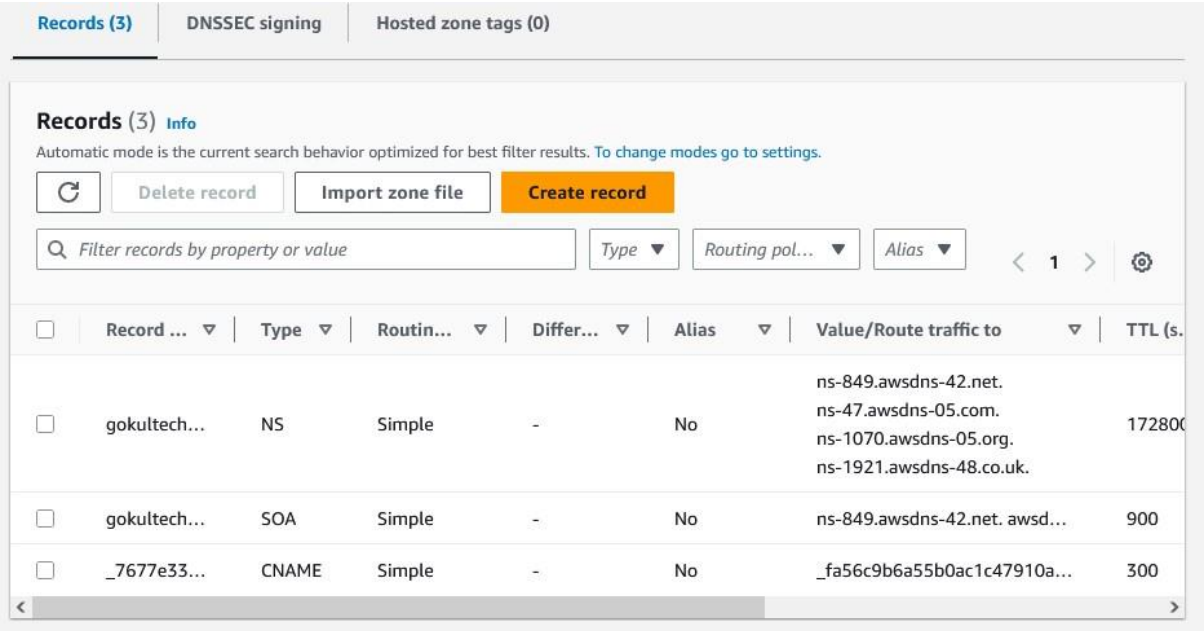

Validation method Info
Select a method for validating domain ownership.
DNS validation - recommended
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.
Email validation
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.
Key algorithm Info
Select an encryption algorithm. Some algorithms may not be supported by all AWS services.
RSA 2048
RSA is the most widely used key type.
ECDSA P 256
Equivalent in cryptographic strength to RSA 3072.
ECDSA P 384
Equivalent in cryptographic strength to RSA 7680.


Successfully requested certificate with ID b4f1f6a5-8bbf-46d4-a538-67c5066755b6
A certificate request with a status of pending validation has been created. Further action is needed to complete the validation and approval of the certificate.
View certificate
AWS Certificate Manager > Certificates
Certificates (1)
Delete
Manage expiry events
Import
Request
1
Certificate ID
Domain name
Type
Status
In use
Renewal eligibility
Key algorithm
b4f1f6a5-8bbf-46d4-a538-67c5066755b6
gokultech.online
Amazon Issued
Pending validation
No
Ineligible
RSA 2048


AWS Certificate Manager > Certificates > b4f1f6a5-8bbf-46d4-a538-67c5066755b6
b4f1f6a5-8bbf-46d4-a538-67c5066755b6
Delete
Certificate status
Identifier
b4f1f6a5-8bbf-46d4-a538-67c5066755b6
Status
Pending validation
Info
ARN
arn:aws:acm:ap-south-1:061716244933:certificate/b4f1f6a5-8bbf-46d4-a538-67c5066755b6
Type
Amazon Issued


Domains (2)
Create records in Route 53
Export to CSV
1
Domain
Status
Renewal status
Type
CNAME name
CNAME value
gokultech.online
Pending validation
-
CNAME
_7677e3317b60055160ccde027ed91569.gokultech.online.
_fa56c9b6a55b0ac1c47910abd4132c3d.kwddbwrbjk.acm-validations.aws.
*.gokultech.online
Pending validation
-
CNAME
_7677e3317b60055160ccde027ed91569.gokultech.online.
_fa56c9b6a55b0ac1c47910abd4132c3d.kwddbwrbjk.acm-validations.aws.



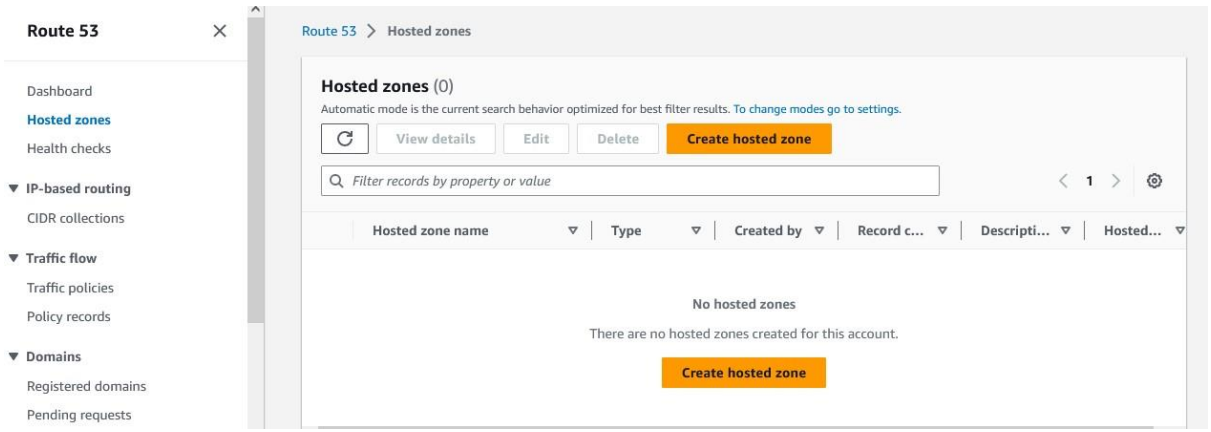




Step 2: Create a hosted zone in Route 53 and attached to the domain.

Go to Route 53 → create hosted zone → enter domain name → create. Then NS and SOA records will be created.

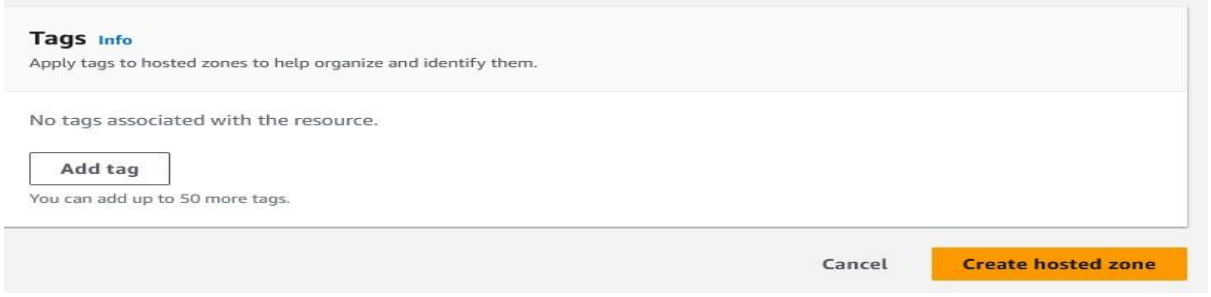
Next name server will be attached to domain.

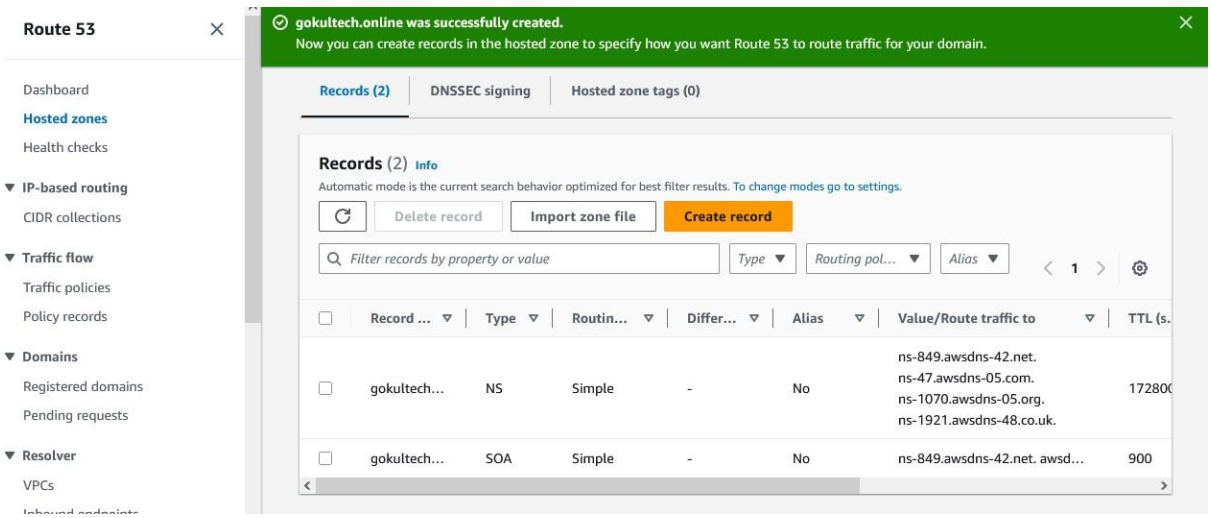
Go to Domain provider (hostinger) → manage → dns name server → change name server → copy and paste name server → save.

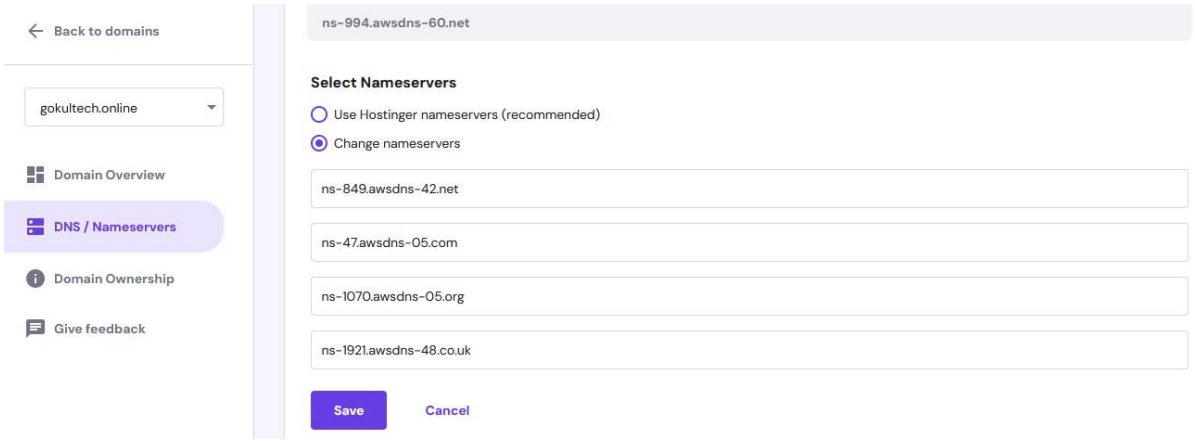

Route 53
Dashboard
Hosted zones
Health checks
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Route 53 > Hosted zones
Hosted zones (0)
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
View details
Edit
Delete
Create hosted zone
Filter records by property or value
Hosted zone name
Type
Created by
Record c...
Descripti...
Hosted...
No hosted zones
There are no hosted zones created for this account.
Create hosted zone

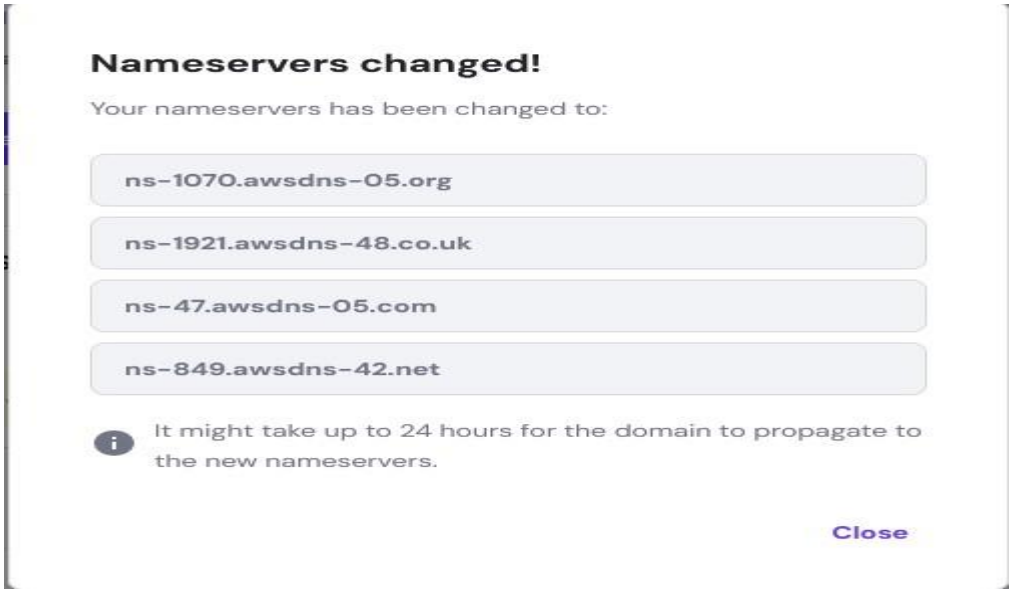

Route 53 > Hosted zones > Create hosted zone
Create hosted zone Info
Hosted zone configuration
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.
Domain name Info
This is the name of the domain that you want to route traffic for.
gokultech.online
Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [ \ ] ^ _ ` { | } . ~
Description - optional Info
This value lets you distinguish hosted zones that have the same name.
The hosted zone is used for...
The description can have up to 256 characters. 0/256


Type Info
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.
Public hosted zone
A public hosted zone determines how traffic is routed on the internet.
Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.


Tags Info
Apply tags to hosted zones to help organize and identify them.
No tags associated with the resource.
Add tag
You can add up to 50 more tags.
Cancel
Create hosted zone


Route 53
Dashboard
Hosted zones
Health checks
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Resolver
VPCs
gokultech.online was successfully created.
Now you can create records in the hosted zone to specify how you want Route 53 to route traffic for your domain.
Records (2)
DNSSEC signing
Hosted zone tags (0)
Records (2) Info
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Delete record
Import zone file
Create record
Filter records by property or value
Type
Routing pol...
Alias
Record ...
Type
Routin...
Differ...
Alias
Value/Route traffic to
TTL (s.
gokultech...
NS
Simple
-
No
ns-849.awsdns-42.net.
ns-47.awsdns-05.com.
ns-1070.awsdns-05.org.
ns-1921.awsdns-48.co.uk.
gokultech...
SOA
Simple
-
No
ns-849.awsdns-42.net. awsd...
900

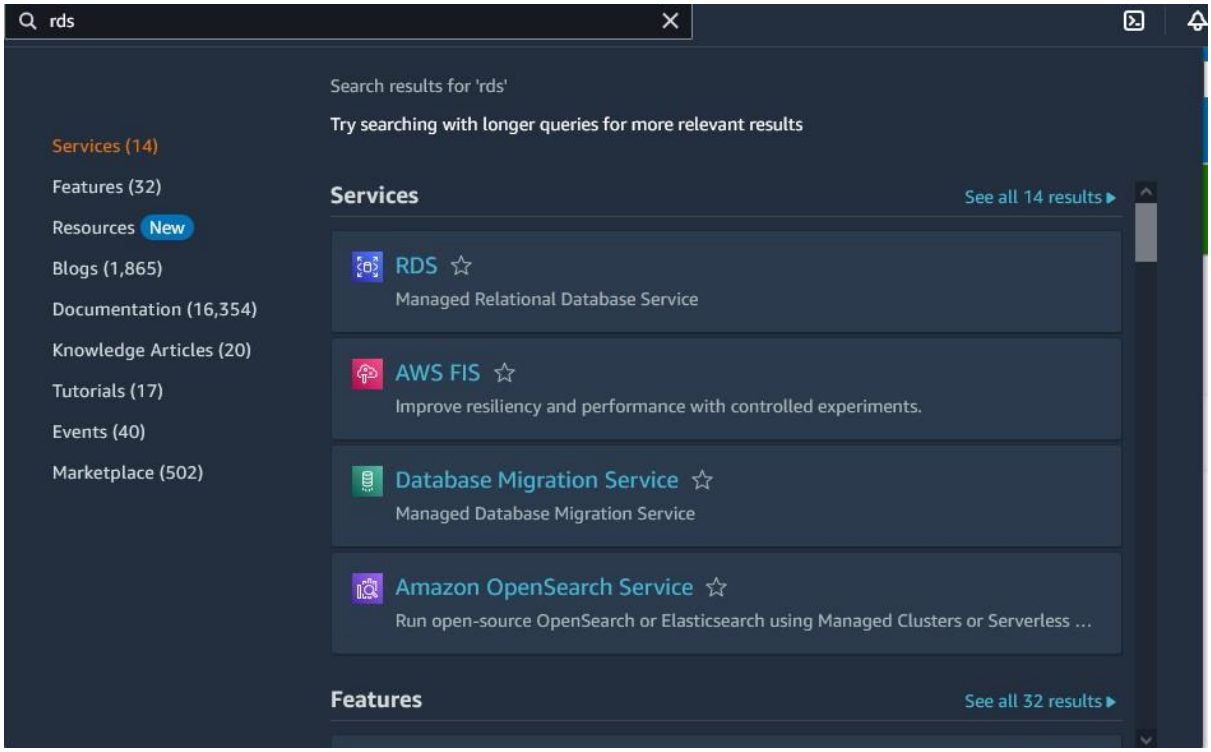


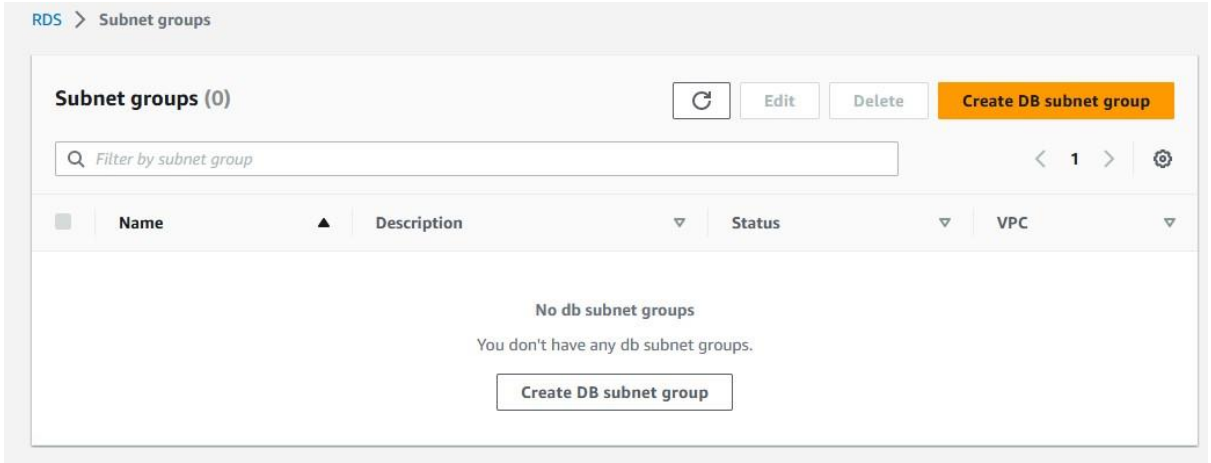




Step 3: Create a subnet group and database in RDS.

Go to RDS → subnet group → create → enter the group name, select vpc,select subnet and availability zone → create db subnet.

Create a production and DR database: select database → create → enter the name, engine community → enter user name and password → create database for both production and DR.


rds
Search results for 'rds'
Try searching with longer queries for more relevant results
Services (14)
Features (32)
Resources New
Blogs (1,865)
Documentation (16,354)
Knowledge Articles (20)
Tutorials (17)
Events (40)
Marketplace (502)
Services
See all 14 results
RDS
Managed Relational Database Service
AWS FIS
Improve resiliency and performance with controlled experiments.
Database Migration Service
Managed Database Migration Service
Amazon OpenSearch Service
Run open-source OpenSearch or Elasticsearch using Managed Clusters or Serverless ...
Features
See all 32 results


RDS > Subnet groups
Subnet groups (0)
Edit
Delete
Create DB subnet group
Filter by subnet group
1
Name
Description
Status
VPC
No db subnet groups
You don't have any db subnet groups.
Create DB subnet group

RDS > Subnet groups > Create DB subnet group

# Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

## Subnet group details

Name

You won't be able to modify the name after your subnet group has been created.

myprodsubnet

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

myprodsubnet

VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

vpc-0c00de5a272d681c8

## Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

*Choose an availability zone*

ap-south-1a ✕ ap-south-1b ✕ ap-south-1c ✕

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

*Select subnets*

subnet-09509f28b8049ea43 (172.31.32.0/20) ✕

subnet-0c01776e4151b5a05 (172.31.0.0/20) ✕

subnet-0661762305c51ffc3 (172.31.16.0/20) ✕

For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.

## Subnets selected (3)

| Availability zone | Subnet ID | CIDR block |
|---|---|---|
| ap-south-1a | subnet-09509f28b8049ea43 | 172.31.32.0/20 |
| ap-south-1b | subnet-0c01776e4151b5a05 | 172.31.0.0/20 |
| ap-south-1c | subnet-0661762305c51ffc3 | 172.31.16.0/20 |

RDS > Subnet groups

**Subnet groups (2)** Edit Delete Create DB subnet group

Filter by subnet group 1

| Name | Description | Status | VPC |
|---|---|---|---|
| mydrsubnet | mydrsubnet | Complete | vpc-0c00de5a272d681c8 |
| myprodsubnet | myprodsubnet | Complete | vpc-0c00de5a272d681c8 |

RDS > Create database

# Create database

## Choose a database creation method Info

- (●) **Standard create**
  You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- ( ) **Easy create**
  Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine type Info

- Aurora (MySQL Compatible)
- Aurora (PostgreSQL Compatible)
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft SQL Server

Edition

MySQL Community

Engine Version

MySQL 5.7.39

MySQL engine versions earlier than 8.0.17 don't support the newest m6g or r6g generation instance classes.

## Templates

Choose a sample template to meet your use case.

- **Production**
  Use defaults for high availability and fast, consistent performance.
- **Dev/Test**
  This instance is intended for development use outside of a production environment.
- **Free tier**
  Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. Info

## Settings

DB instance identifier Info

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

proddb

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username Info

Type a login ID for the master user of your DB instance.

proddba

1 to 16 alphanumeric characters. First character must be a letter.

☐ Manage master credentials in AWS Secrets Manager

Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
Learn more

Master password Info

••••••••••

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

Confirm master password Info

••••••••••

## Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class Info

- Standard classes (includes m classes)
- Memory optimized classes (includes r and x classes)
- Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps

Include previous generation classes

## Connectivity Info

### Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

- (●) **Don't connect to an EC2 compute resource**
  Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.
- ( ) **Connect to an EC2 compute resource**
  Set up a connection to an EC2 compute resource for this database.

### Network type Info

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

- (●) **IPv4**
  Your resources can communicate only over the IPv4 addressing protocol.
- ( ) **Dual-stack mode**
  Your resources can communicate over IPv4, IPv6, or both.

### Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-0c00de5a272d681c8)
3 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change its VPC.

### DB subnet group Info

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

myprodsubnet
3 Subnets, 3 Availability Zones

### Public access Info

- ( ) **Yes**
  RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- (●) **No**
  RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

### VPC security group (firewall) Info

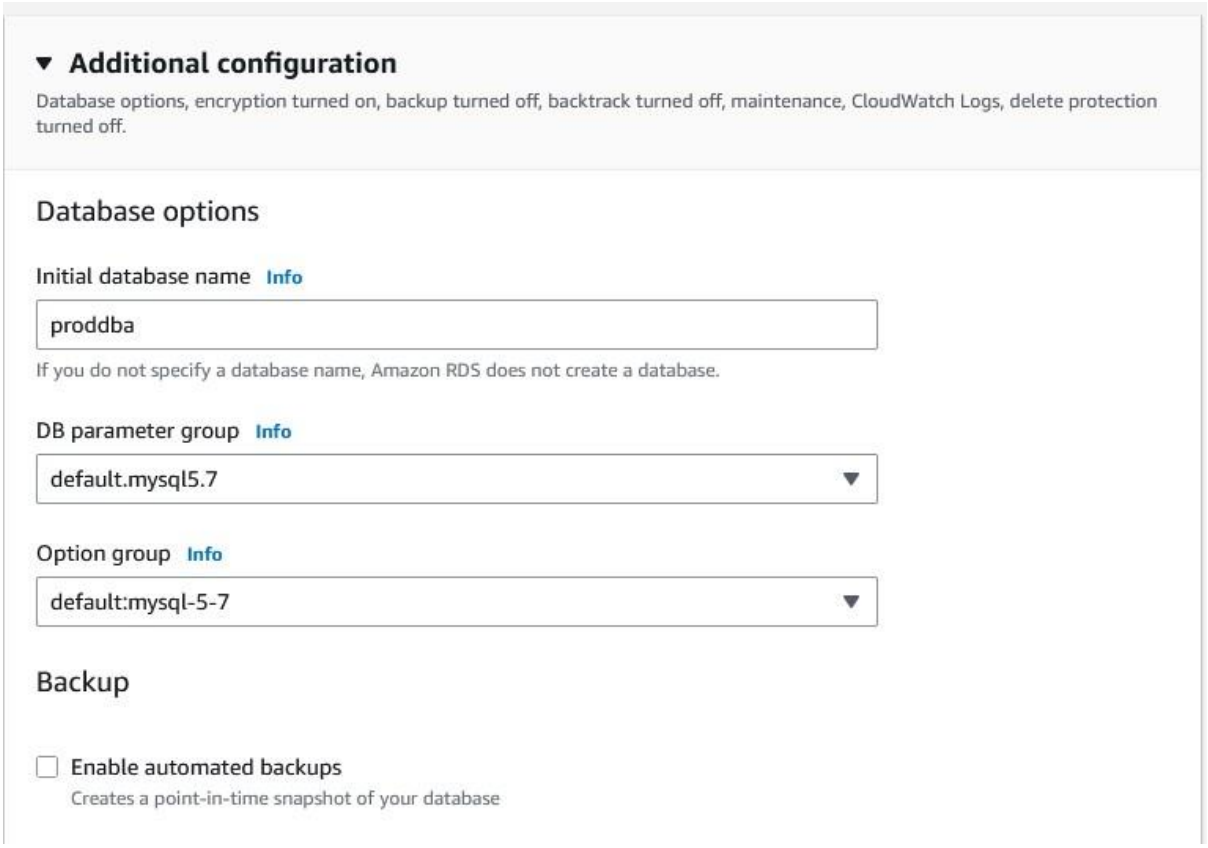
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

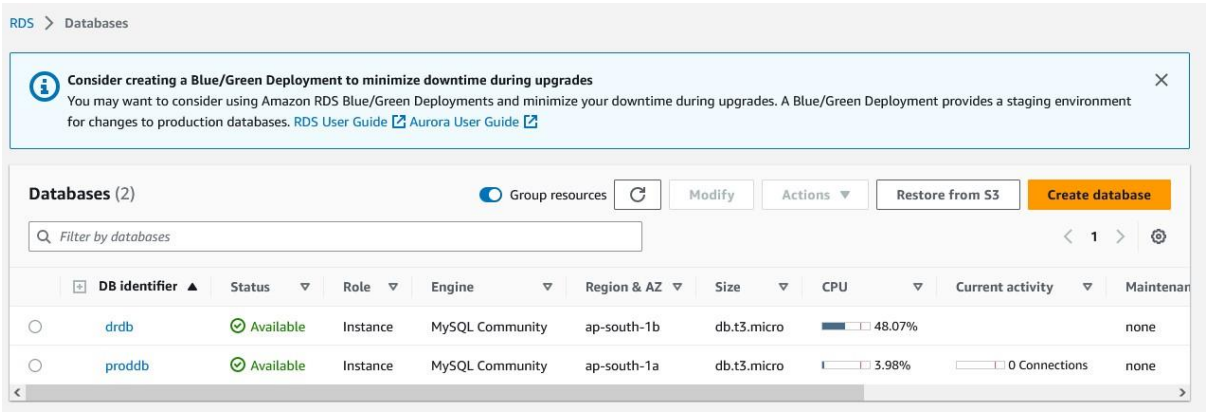
- (●) **Choose existing**
  Choose existing VPC security groups
- ( ) **Create new**
  Create new VPC security group

### Existing VPC security groups

*Choose one or more options*

launch-wizard-1 ×




Step 4: Create an IAM role for ec2 instance.

Go to IAM → role → create new role → aws service ec2 and S3 → create role.

Step 5: To launch an ec2 instance for production and DR server.

Go to EC2 → instance → launch instance for both with bash scripts given below to add user date for instance launch.

Bash script to deploy wordpress app:

==========

#!/bin/bash

yum install httpd php-mysql -y

amazon-linux-extras install -y php7.3

cd /var/www/html

echo "healthy" > healthy.html

wget https://wordpress.org/latest.tar.gz

tar -xzf latest.tar.gz

cp -r wordpress/* /var/www/html/

rm -rf wordpress

rm -rf latest.tar.gz

chmod -R 755 wp-content

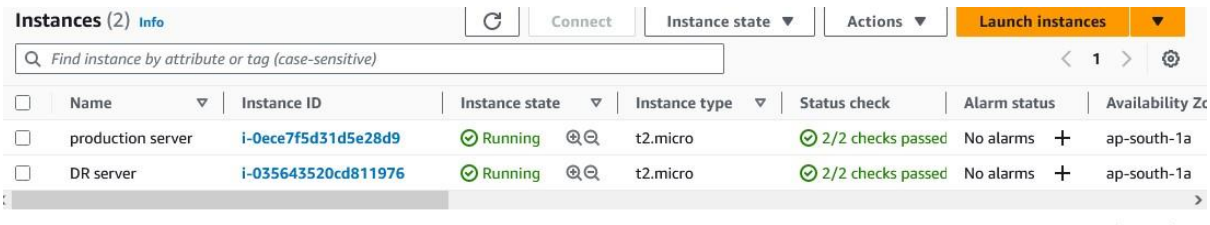
chown -R apache:apache wp-content

wget https://s3.amazonaws.com/bucketforwordpresslab-donotdelete/htaccess.txt

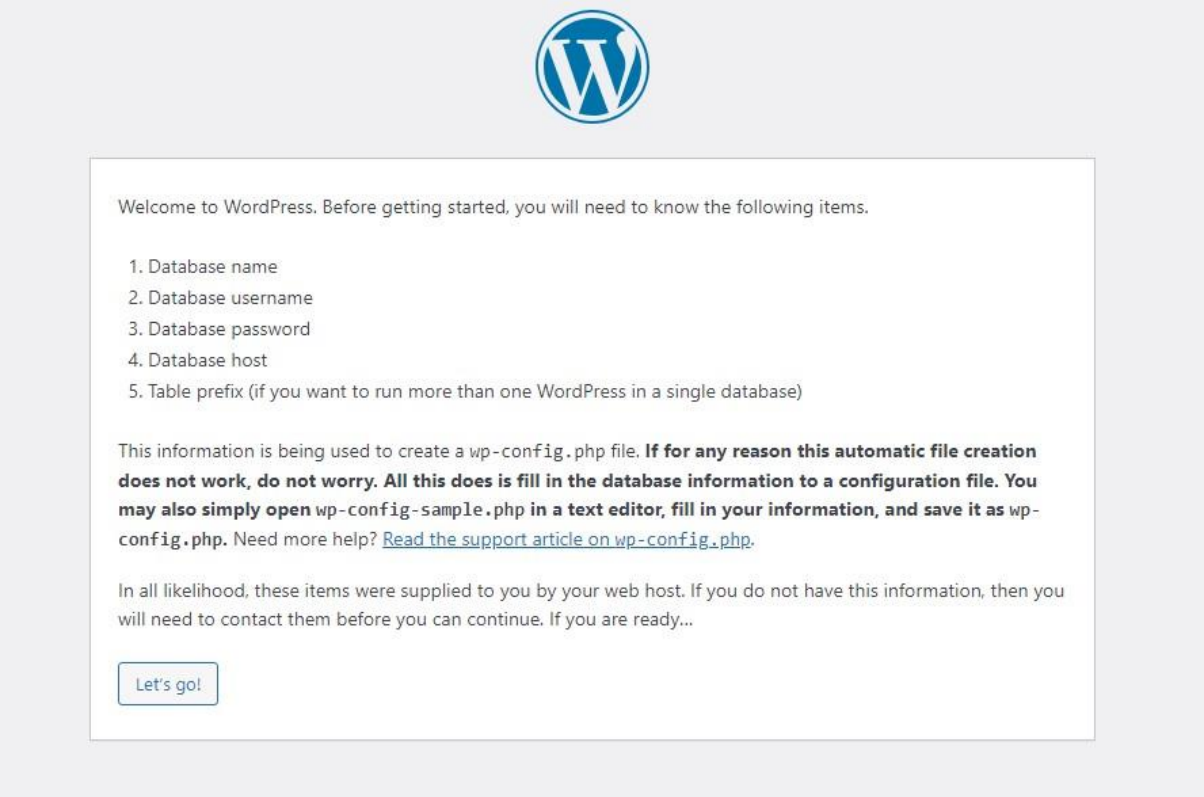
mv htaccess.txt .htaccess

chkconfig httpd on

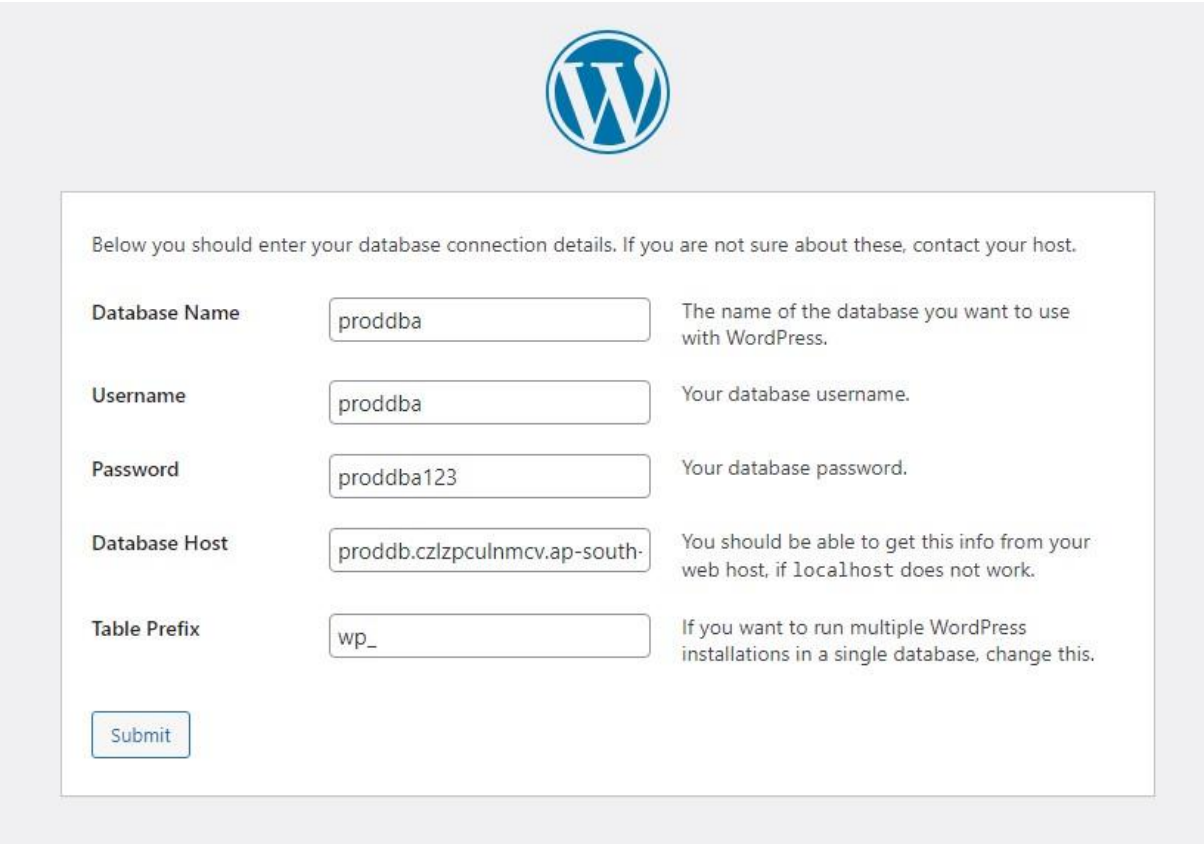
service httpd start



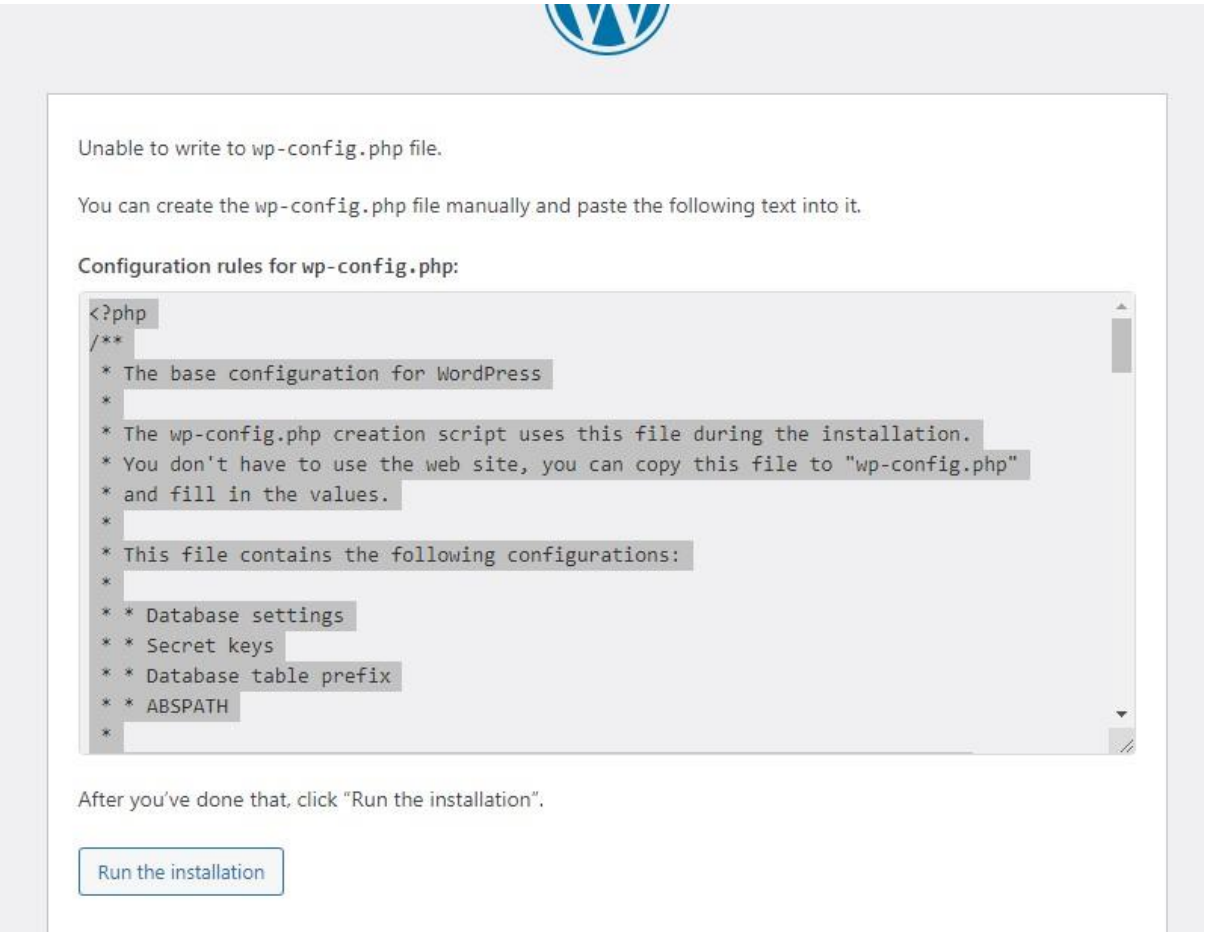

Next to check the browser with public ip for production server.




Click lets go  next page will show and enter the database details.




Click submit go to next page

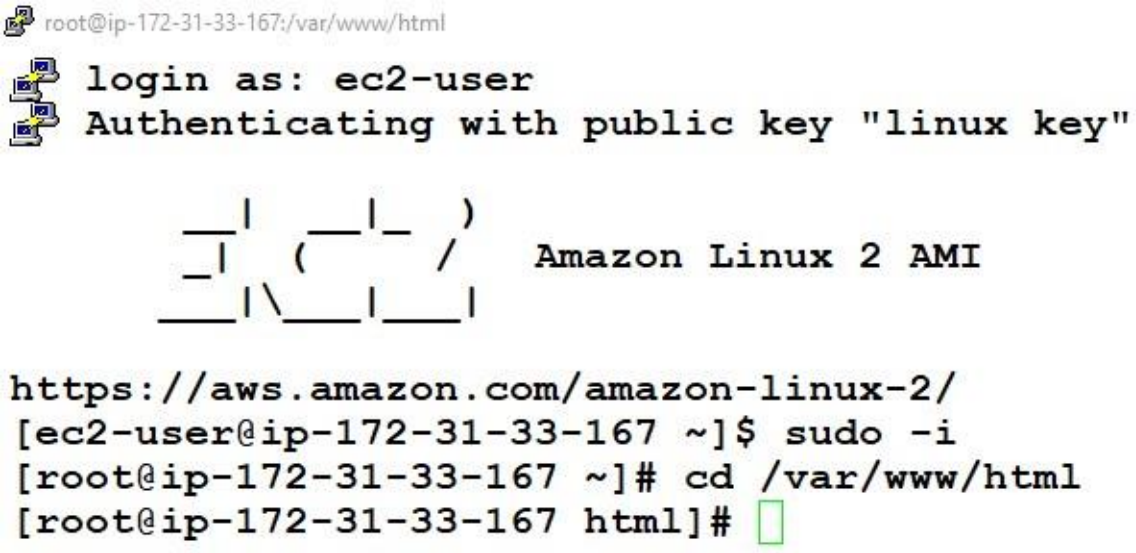



To log in production server through putty

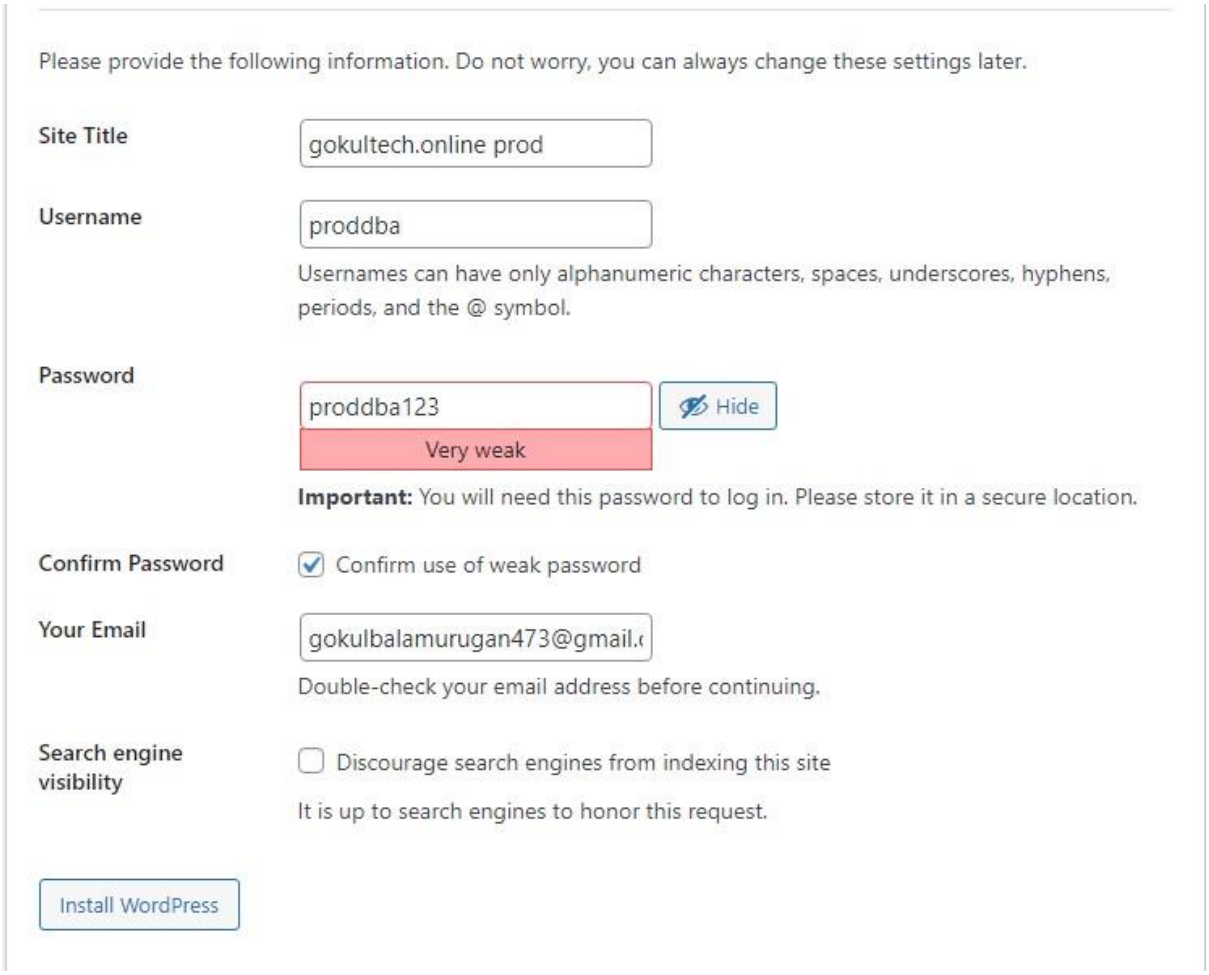
sudo -i

cd /var/www/html

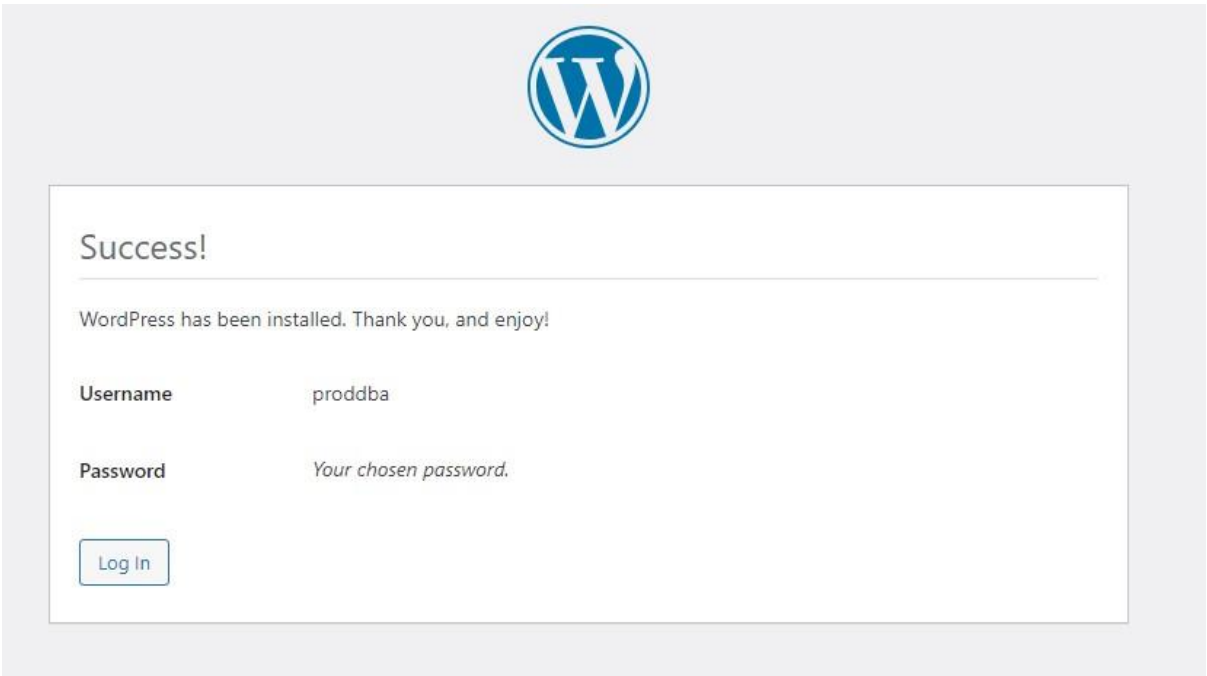
vi wp-config.php → copy and paste the above config file in wp-config.php.



Then run the installation




Click install word press




Repeat the same steps for DR SERVER.

Login the production wordpress

Select post → edit → update


Login the DR wordpress

Select post → edit → update


To check the browser with public ip for both production and DR server.

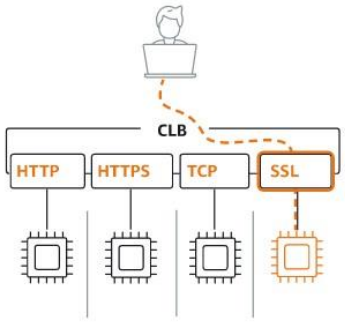


Step 6: Create a classic load balancer for production and DR server.

Go to EC2 →select load balancer → create classic load balancer → enter basic configuration → network mapping → health check → add instance → create load balancer.

▼ Classic Load Balancer - *previous generation*

## Classic Load Balancer Info




Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network.

Create

## Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

myprodlb

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | Info

Scheme can't be changed after the load balancer is created.

- (•) Internet-facing
  An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more
- ( ) Internal
  An internal load balancer routes requests from clients to targets using private IP addresses.

## Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your network settings.

VPC | Info

Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are available for selection. The selected VPC cannot be changed after the load balancer is created. When selecting a VPC for your load balancer, ensure each subnet has a CIDR block with at least a /27 bitmask and at least 8 free IP addresses. Learn more

-
vpc-0c00de5a272d681c8
IPv4: 172.31.0.0/16

Mappings | Info

The load balancer routes traffic only to targets in the selected Availability Zones. We recommend enabling multiple Availability Zones to increase the fault tolerance of your application. For each Availability Zone enabled, you must choose one subnet. It is possible to create the load balancer with just one Availability Zone and corresponding subnet, and you can enable additional Availability Zones after the load balancer is created. It is also possible to update the subnet for an Availability Zone after the load balancer is created, but this process has some requirements. Zones that are not supported by the load balancer or VPC can't be selected.

☑ **ap-south-1a (aps1-az1)**

Subnet

subnet-09509f28b8049ea43

IPv4 address

Assigned by AWS

## Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

launch-wizard-1 sg-0c03c344046b4329f
VPC: vpc-0c00de5a272d681c8

## Listeners and routing Info

A listener is a process that checks for connection requests using the protocol and port you configure. The settings you define for a listener determine how the load balancer routes requests to its registered targets.

Listener HTTP:80 | Instance HTTP:80 | Remove

| Listener protocol | Listener port | Instance protocol | Instance port |
|---|---|---|---|
| HTTP | 80 (1-65535) | HTTP | 80 (1-65535) |

## Health checks Info

Your load balancer automatically performs health checks to test the availability of all registered instances. Health checks send ping requests to instances using the specified protocol, port, and path. Traffic is only routed to instances that meet the healthy threshold specified in your health check settings. Instances that do not respond to the health checks are considered unhealthy and stop receiving traffic until meeting the healthy threshold.

Ping target

The health check ping is sent using the protocol and port you specify. If using HTTP/HTTPS protocol, you must also provide the destination path.

| Ping Protocol | Ping Port | Ping Path |
|---|---|---|
| HTTP | 80 (1-65535) | /healthy.html |

Advanced health check settings

## Instances (1)

You can add instances to register as targets of the load balancer. Alternatively, after your load balancer is created, you can add it to an Amazon EC2 Auto Scaling group to ensure you maintain the correct number of instances to handle the load for your application. For maximum fault tolerance, we recommend maintaining approximately equivalent numbers of instances in each Availability Zone.

Remove | Add instances

Filter resources by property or value

1

| Instance ID | Name | State | Security groups |
|---|---|---|---|
| i-0ece7f5d31d5e28d9 | production server | Running | launch-wizard-1 |

## Attributes

Creating your load balancer using the console gives you the opportunity specify additional features at launch. You can also find and adjust these settings in the load balancer's "Attributes" section after your load balancer is created.

- [x] Enable cross-zone load balancing

With cross-zone load balancing, each load balancer node for your Classic Load Balancer distributes requests evenly across the registered instances in all enabled Availability Zones. If cross-zone load balancing is disabled, each load balancer node distributes requests evenly across the registered instances in its Availability Zone only. Classic Load Balancers created with the API or CLI have cross-zone load balancing disabled by default. After you create a Classic Load Balancer, you can enable or disable cross-zone load balancing at any time.

- [x] Enable connection draining

Applicable to targets that are deregistering, this feature allows existing connections to complete (during a specified draining interval) before reporting the instance as deregistered. Learn more

EC2 | Load balancers | myprodlb

Load balancer: myprodlb

Description | Instances | Health check | Listeners | Monitoring | Tags | Migration

**Connection Draining:** Enabled, 300 seconds (Edit)

Edit Instances

| Instance ID | Name | Availability Zone | Status | Actions |
|---|---|---|---|---|
| i-0ece7f5d31d5e28d9 | production server | ap-south-1a | InService | Remove from Load Balancer |

EC2 | Load balancers | mydrlb

Load balancer: mydrlb

Description | Instances | Health check | Listeners | Monitoring | Tags | Migration

**Connection Draining:** Enabled, 300 seconds (Edit)

Edit Instances

| Instance ID | Name | Availability Zone | Status | Actions |
|---|---|---|---|---|
| i-035643520cd811976 | DR server | ap-south-1a | InService | Remove from Load Balancer |

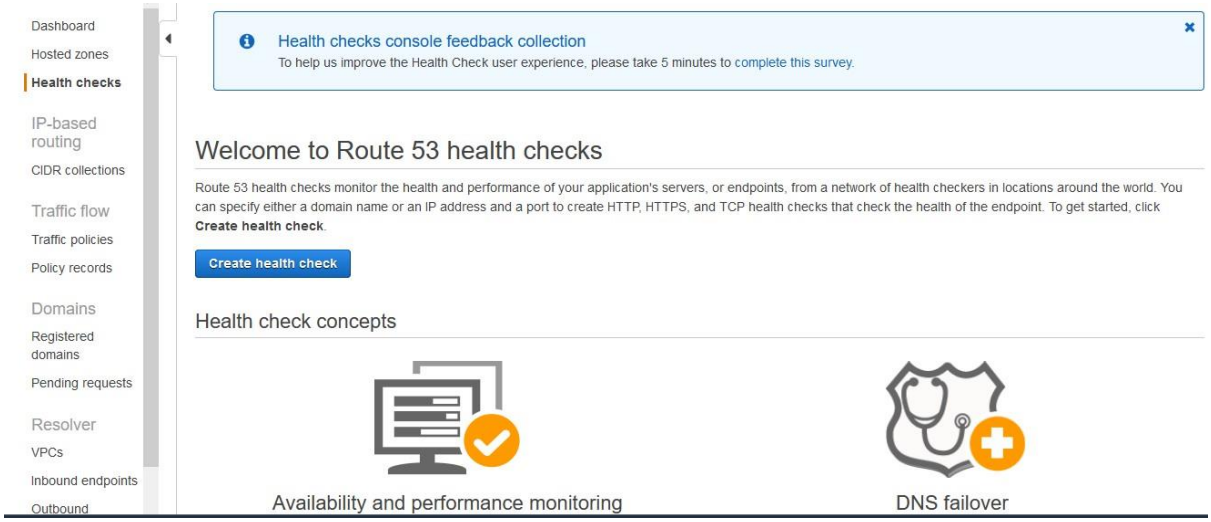
Edit Availability Zones

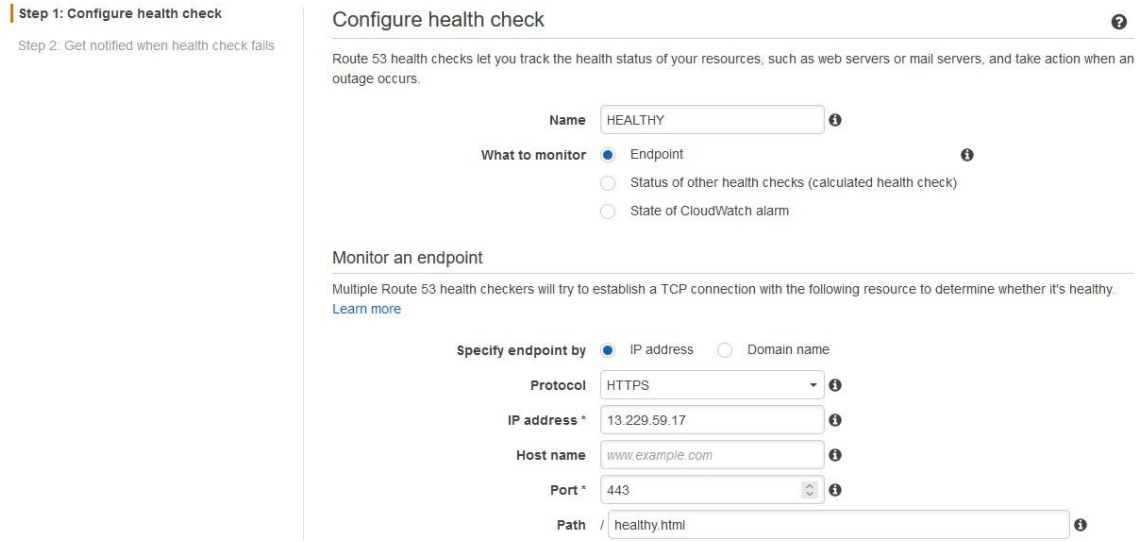
| Availability Zone | Subnet ID | Subnet CIDR | Instance Count | Healthy? | Actions |
|---|---|---|---|---|---|
| ap-south-1c | subnet-0661762305c51ffc3 | 172.31.16.0/20 | 0 | No (Availability Zone contains no healthy targets) | Remove from Load Balancer |
| ap-south-1b | subnet-0c01776e4151b5a05 | 172.31.0.0/20 | 0 | No (Availability Zone contains no healthy targets) | Remove from Load Balancer |
| ap-south-1a | subnet-09509f28b8049ea43 | 172.31.32.0/20 | 1 | Yes | Remove from Load Balancer |

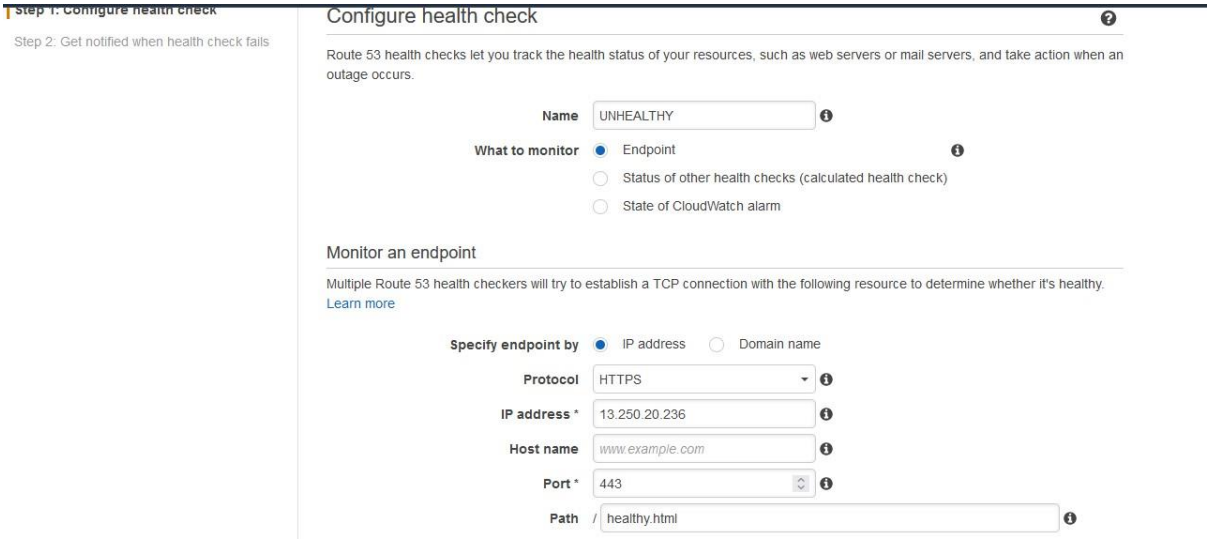
Step 7: Mapping with load balancer in route 53 for create failover records.

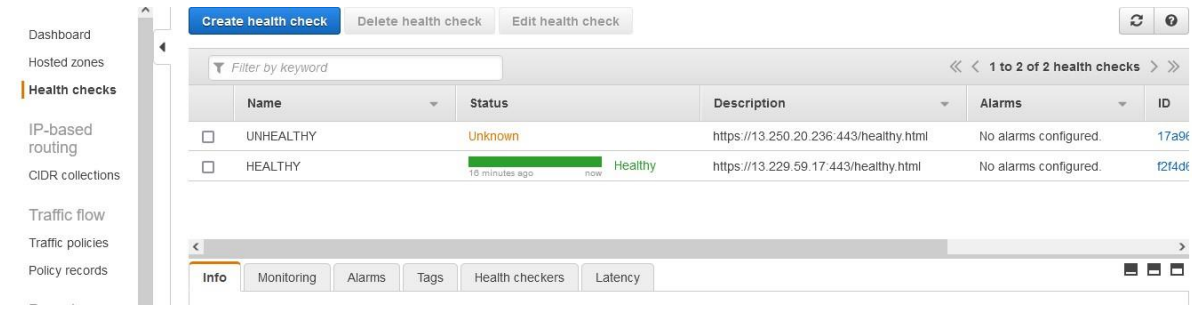
create a record for failover routing policy

Go to route 53 → create health check for healthy and unhealthy → configure health → create.






Once created health check then create a record for failover routing policy

Select hosted zone → create a new record → select route alias → select routing policy type → create a primary and secondary resource

Record name Info

subdomain

gokultech.online

Keep blank to create a record for the root domain.

Record type Info

A – Routes traffic to an IPv4 address and some AWS resources

Alias

Route traffic to Info

Alias to Application and Classic Load Balancer

Asia Pacific (Singapore) [ap-southeast-1]

dualstack.myprodlb-802371561.ap-southeast-1.elb.amazonaws.com

Alias hosted zone ID: Z1LMS91P8CMLE5

Routing policy Info

Failover

Failover record type

Primary

Health check ID Info

f2f4d6c6-c704-4c90-b307-6e5ffc88a4f4

Evaluate target health

Yes

Record ID Info

healthy

Record name Info

dr

.gokultech.online

Keep blank to create a record for the root domain.

Record type Info

A – Routes traffic to an IPv4 address and some AWS resources

Alias

Route traffic to Info

Alias to Application and Classic Load Balancer

Asia Pacific (Singapore) [ap-southeast-1]

dualstack.mydrlb-1116617684.ap-southeast-1.elb.amazonaws.com

Alias hosted zone ID: Z1LMS91P8CMLE5

Routing policy Info

Failover

Failover record type

Secondary

Health check ID - *optional* Info

17a9677b-a74c-4fa3-9698-5a00f79c02c7

Evaluate target health

Yes

Record ID Info

unhealthy

**Record for gokultech.online was successfully created.**

Route 53 propagates your changes to all of the Route 53 authoritative DNS servers within 60 seconds. Use "View status" button to check propagation status.

View status

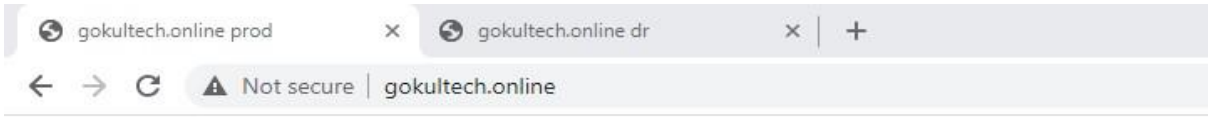
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

Delete record | Import zone file | Create record

Filter records by property or value | Type | Routing pol... | Alias | 1

| Record ... | Type | Routin... | Differ... | Alias | Value/Route traffic to | TTL (s... | Health ... | Evalua... |
|---|---|---|---|---|---|---|---|---|
| gokultech... | A | Simple | - | Yes | dualstack.myprodlb-812751... | - | - | Yes |
| gokultech... | NS | Simple | - | No | ns-849.awsdns-42.net. ns-47.awsdns-05.com. ns-1070.awsdns-05.org. ns-1921.awsdns-48.co.uk. | 172800 | - | - |
| gokultech... | SOA | Simple | - | No | ns-849.awsdns-42.net. awsd... | 900 | - | - |
| _7677e33... | CNAME | Simple | - | No | _fa56c9b6a55b0ac1c47910a... | 300 | - | - |
| dr.gokulte... | A | Simple | - | Yes | dualstack.mydrlb-20825510... | - | - | Yes |

To check the browser with domain name for both server. This not secure.




gokultech.online prod

# Mindblown: a blog about p

## HI THIS MY PRODUCTION SERVER!

Welcome to gokultech prod. This is your first post. Edit or delete it, then start writing!


gokultech.online dr

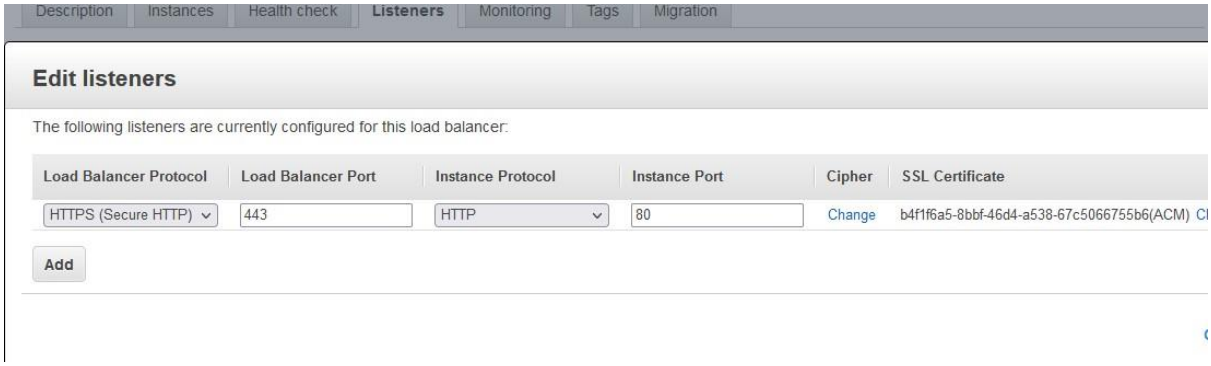
# Mindblown: a blog abo

## HI THIS IS MY DR SERVER!

Welcome to gokultech dr. This is your first post. Edit or delete it, then start writing!

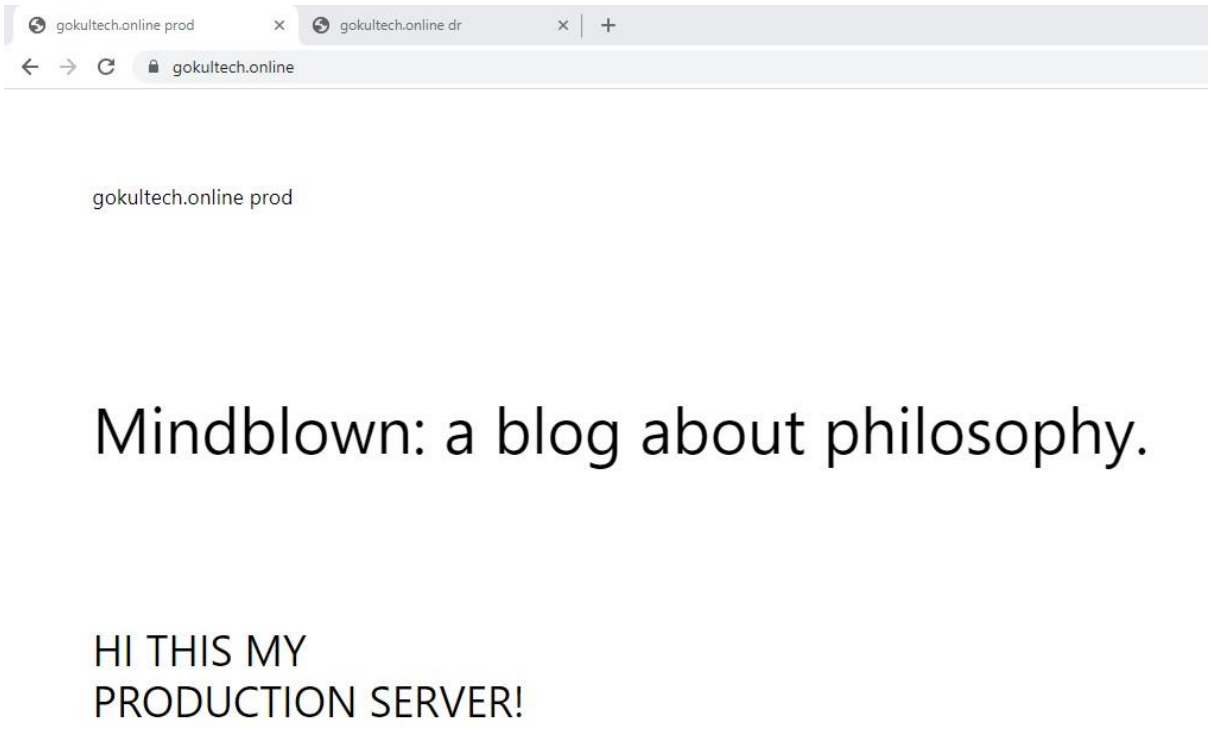
Step 8: ACM certificate mapping with load balancer for secure connection in website.

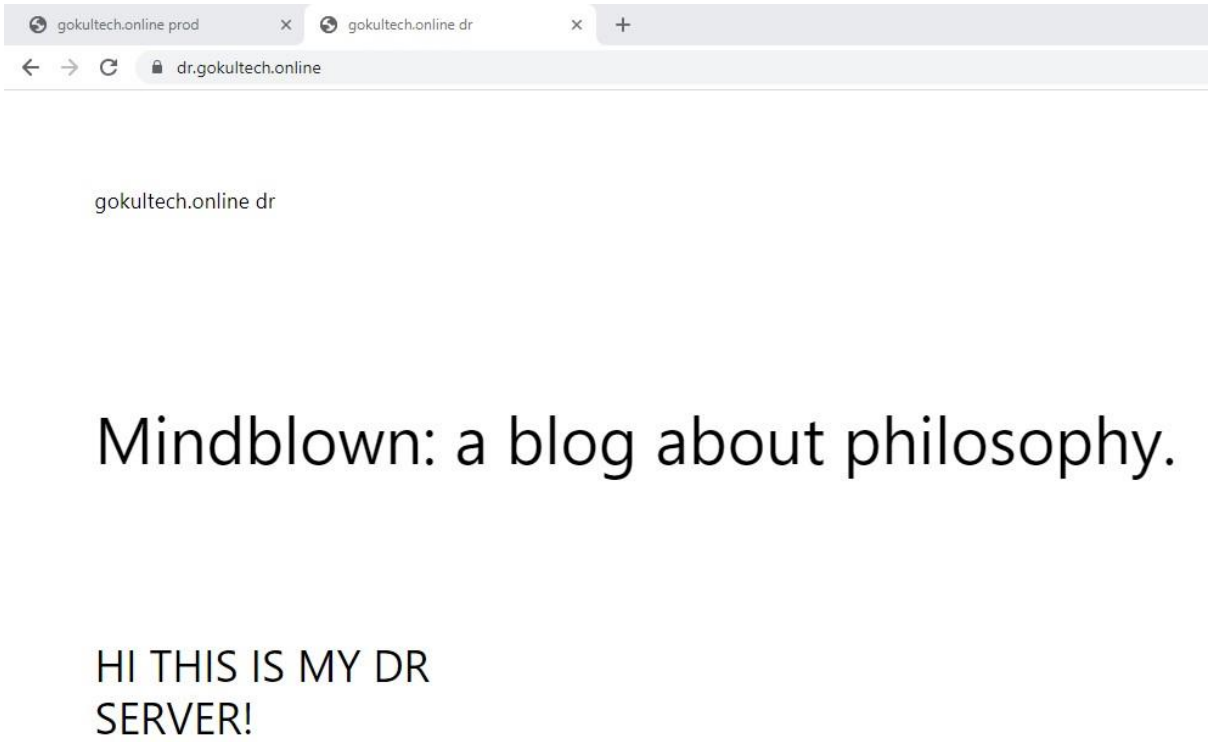
Go to EC2 → select load balancer → click load balancer name → select listener → edit → select HTTPS → change → give ssl certificate for domain → save for both load balancer.




To check the browser with domain in secure

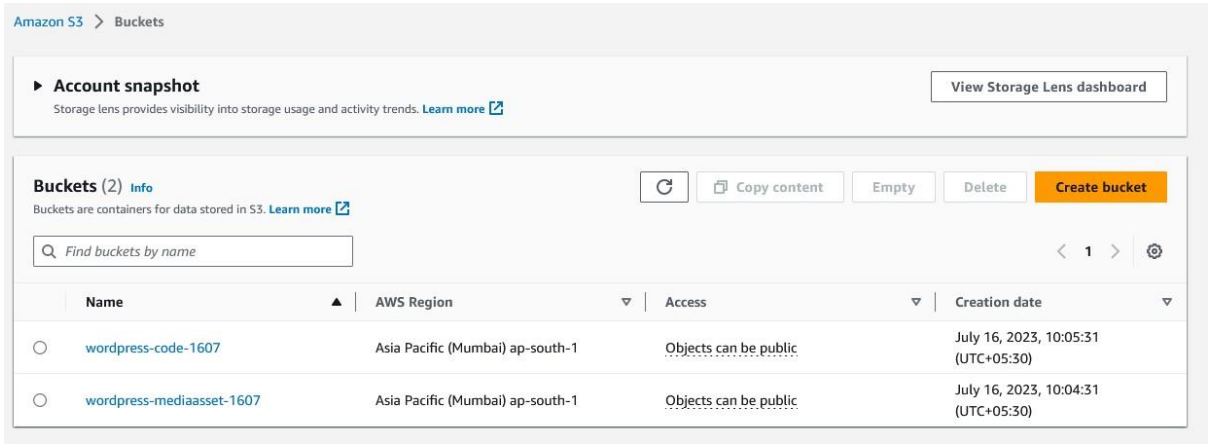
Eg: https://example.online → this is for example






Step 9: Create a S3 bucket and Synchronuos the production and DR server.

Go to S3 → create two buckets → acl enabled → give public access → create bucket.




Step 10: Login the production server through putty

Create cron job expression

crontab -l → list the cron job

crontab -e → edit cron job

*/2 * * * * aws s3 sync --delete /var/www/html/wp-content/uploads s3://wordpress-mediaasset-0811

*/2 * * * * aws s3 sync --delete /var/www/html/ s3://wordpress-code-0811

```
root@ip-172-31-33-167:/
*/2 * * * * aws s3 sync --delete /var/www/html/wp-content/uploads s3://wordpress-mediaasset-0811
*/2 * * * * aws s3 sync --delete /var/www/html/ s3://wordpress-code-0811
~
~
~
```

```
root@ip-172-31-33-167:/
login as: ec2-user
Authenticating with public key "linux key"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-33-167 ~]$ sudo -i
[root@ip-172-31-33-167 ~]# cd /var/www/html
[root@ip-172-31-33-167 html]# vi wp-config.php
[root@ip-172-31-33-167 html]# cd ..
[root@ip-172-31-33-167 www]# cd ..
[root@ip-172-31-33-167 var]# cd ..
[root@ip-172-31-33-167 /]# crontab -l
no crontab for root
[root@ip-172-31-33-167 /]# crontab -e
no crontab for root - using an empty one
crontab: installing new crontab
[root@ip-172-31-33-167 /]#
```

Login DR server through putty

Create cron job expression

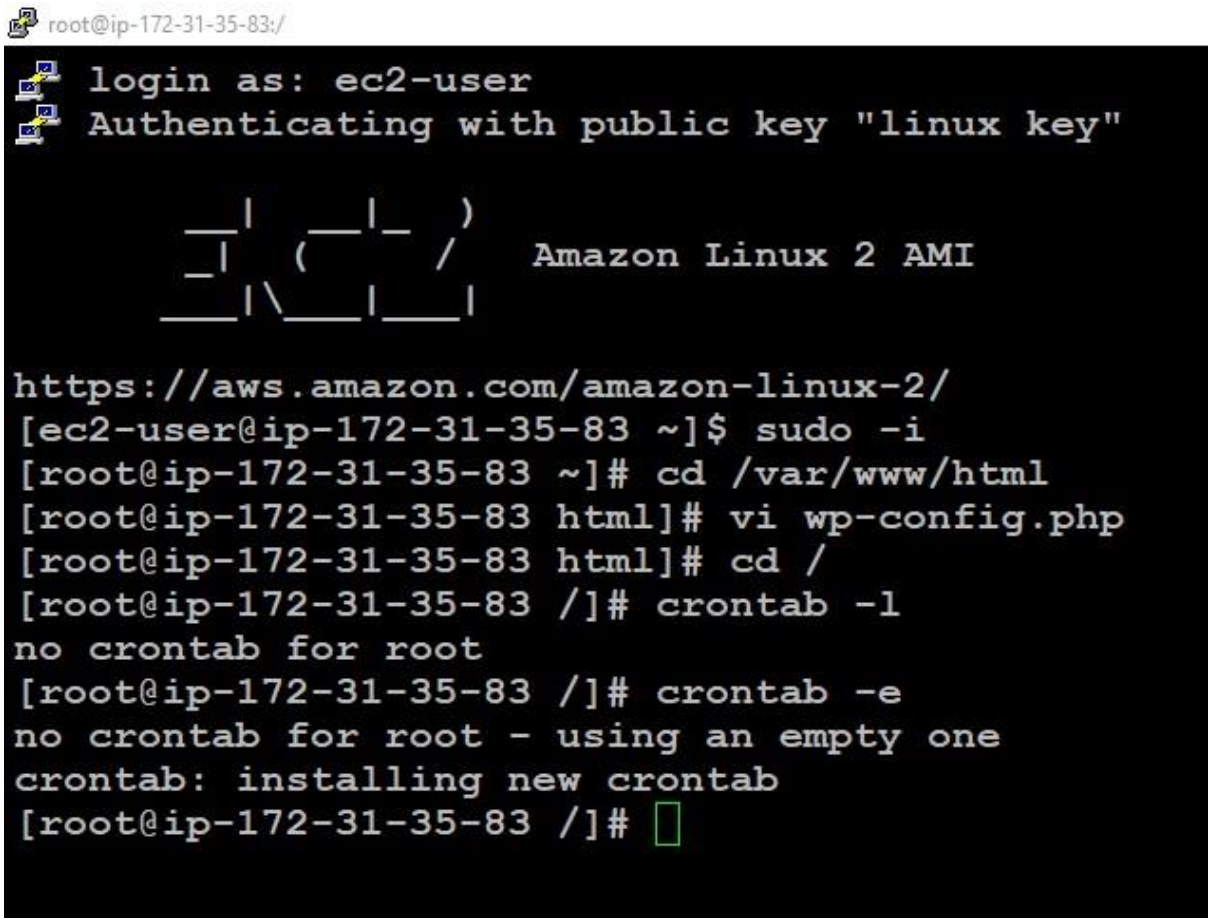
crontab -l → list the cron job

crontab -e → edit cron job

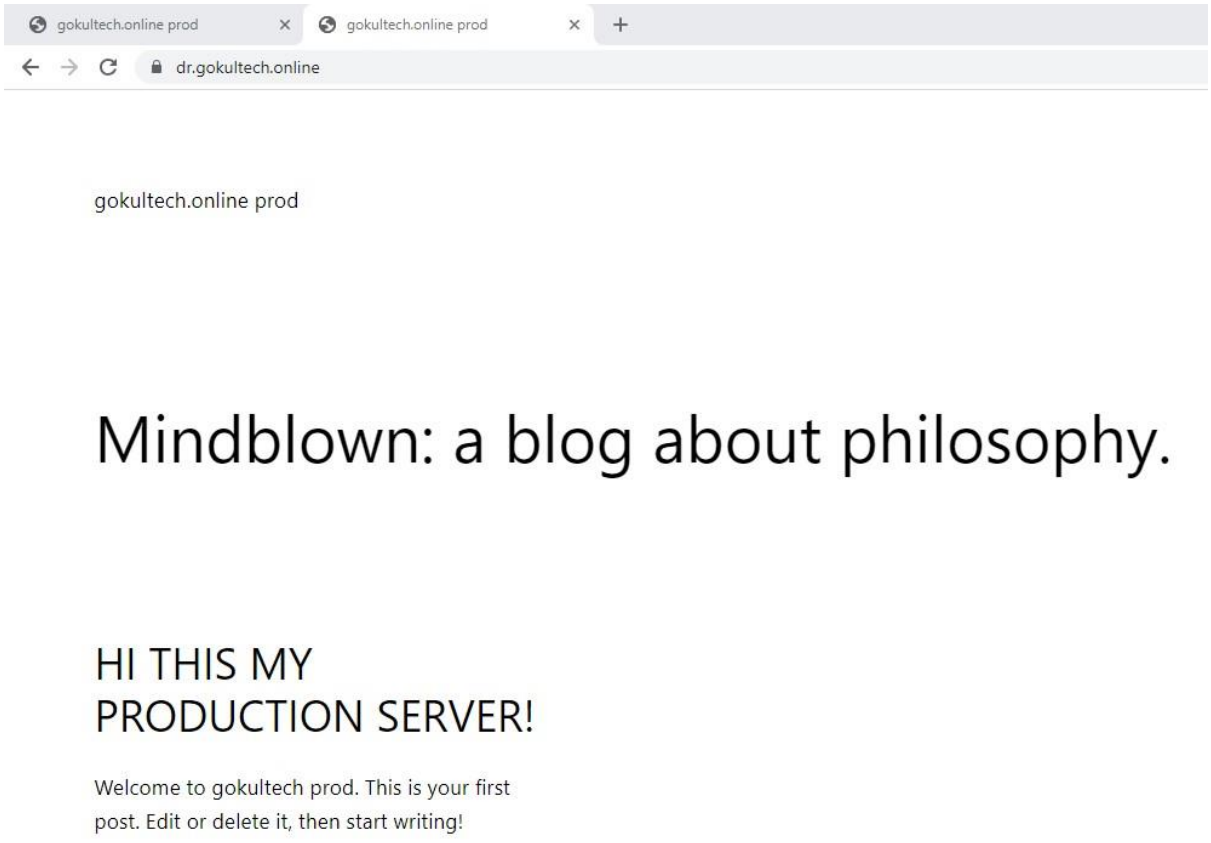
*/2 * * * * aws s3 sync --delete s3://wordpress-mediaasset-0811 /var/www/html/wp-content/uploads

*/2 * * * * aws s3 sync --delete s3://wordpress-code-0811 /var/www/html/

```
root@ip-172-31-35-83:/
*/2 * * * *  aws s3 sync --delete  s3://wordpress-mediaasset-0811 /var/www/html/wp-content/uploads
*/2 * * * *  aws s3 sync --delete  s3://wordpress-code-0811 /var/www/html/
~
~
```

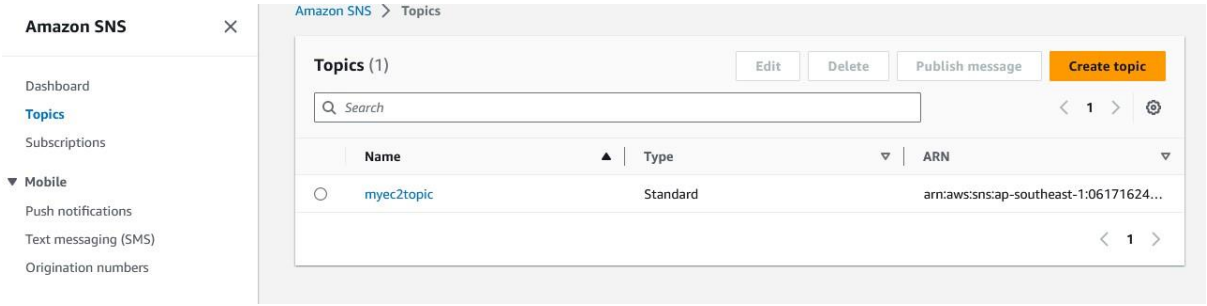


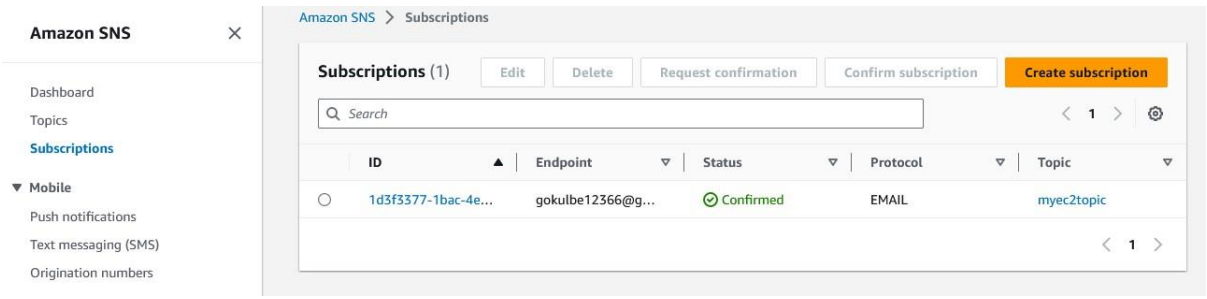

Check browser

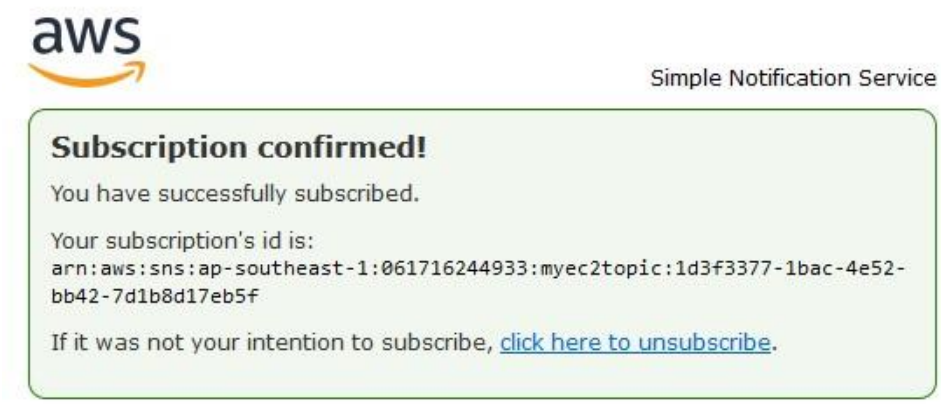


Step 11: create alert notification for ec2 instance stopped

Go to SNS → create topic → create subscription

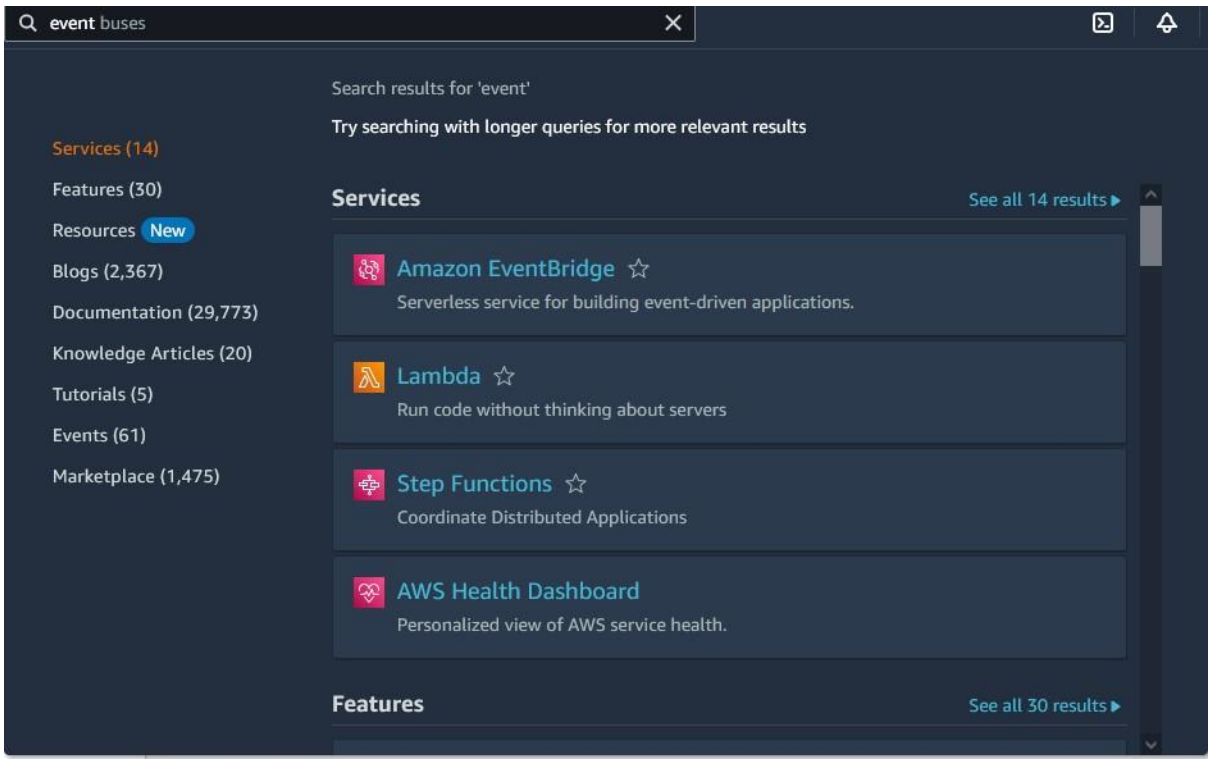


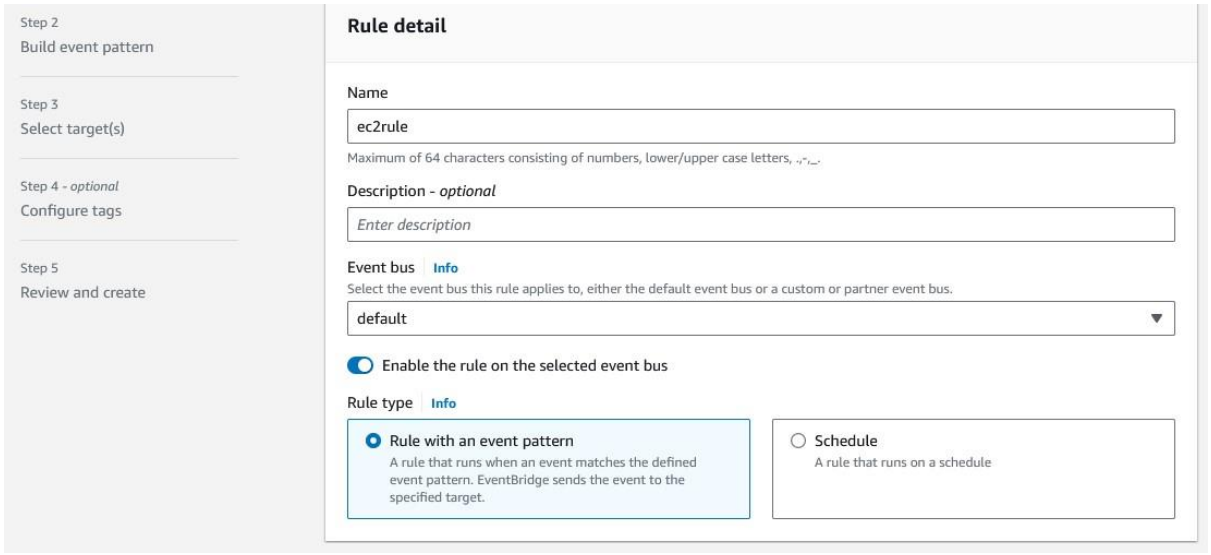




Step 12: create eventbridge rule for ec2 instance state change

Go to eventbridge → create rule → enter rule details → build event pattern → select target → addition setting → change input transform and templates →create rule.


event buses
Search results for 'event'
Try searching with longer queries for more relevant results
Services (14)
Features (30)
Resources New
Blogs (2,367)
Documentation (29,773)
Knowledge Articles (20)
Tutorials (5)
Events (61)
Marketplace (1,475)
Services
See all 14 results
Amazon EventBridge
Serverless service for building event-driven applications.
Lambda
Run code without thinking about servers
Step Functions
Coordinate Distributed Applications
AWS Health Dashboard
Personalized view of AWS service health.
Features
See all 30 results


Step 2
Build event pattern
Step 3
Select target(s)
Step 4 - optional
Configure tags
Step 5
Review and create
Rule detail
Name
ec2rule
Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.
Description - optional
Enter description
Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default
Enable the rule on the selected event bus
Rule type Info
Rule with an event pattern
A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
Schedule
A rule that runs on a schedule

## Event pattern Info

Event source
AWS service or EventBridge partner as source

AWS services

AWS service
The name of the AWS service as the event source

EC2

Event type
The type of events as the source of the matching pattern

EC2 Instance State-change Notification

- ○ Any state
- ◉ Specific state(s)

- ◉ Any instance
- ○ Specific instance Id(s)

Event pattern
Event pattern, or filter to match the events

```
{
  "source": ["aws.ec2"],
  "detail-type": ["EC2 Instance State-change Notificati
}
```

Copy | Test pattern | Edit pattern

## Target 1

Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

- ○ EventBridge event bus
- ○ EventBridge API destination
- ◉ AWS service

Select a target Info
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

SNS topic

Topic

myec2topic

▶ Additional settings

## Target input transformer

You can customize the text from an event before EventBridge passes the event to the target of a rule. Using the input transformer in the console or the API, you define variables that use JSON path to reference values in the original event source. You can define up to 100 variables, assigning each a value from the input. Then you can use those variables in the Input Template as <variable-name>.

### Input path

The Input Path defined as key-value pairs is used to define variables. You use JSON path to reference items in your event and store those values in variables. For instance, you could create an Input Path to reference values in the event.

```
{"instance-id":"$.detail.instance-id",
 "state":"$.detail.state",
 "time":"$.time",
 "region":"$.region",
 "account":"$.account"}
```

## Configure input transformer

Copy | {} Prettify

### Template

The Input Template is a template for the information you want to pass to your target. You can create a template that passes either a string or JSON to the target.

```
:ance <instance-id> on account <account> in the AWS Region <region> has changed to <state>."
```

**Rules** (1) | Delete | Enable | Edit | CloudFormation Template | Create rule

Find rules | Any status | 1 ...

| Name | Status | Type | Description |
|---|---|---|---|
| ec2rule | Enabled | Standard | - |

When ec2 instance state is changed to give alert message

**AWS Notifications** <no-reply@sns.amazonaws.com> 11:51 AM (0 minutes ago)

to me

"At 2023-07-17T06:21:58Z, the status of your EC2 instance i-016c47dcf0e681b77 on account 061716244933 in the AWS Region ap-southeast-1 has changed to stopped."

...

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.ap-southeast-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:ap-southeast-1:061716244933:myec2topic:1d3f3377-1bac-4e52-bb42-7d1b8d17eb5f&Endpoint=gokulbe12366@gmail.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support