Institut TIC de Barcelona
Consorci d'Educació de Barcelona
Generalitat de Catalunya
Ajuntament de Barcelona

ITICBCN

Carla Cuéllar Franco

Plan de Implementación de WordPress de Alta Disponibilidad en AWS

Introducción

Estrategia de implementación (3 horas)

Fase 1: Infraestructura base (45 minutos)

- Crear VPC con subredes públicas y privadas
- Configurar grupos de seguridad
- Configurar EFS para almacenamiento compartido

Fase 2: Base de datos (30 minutos)

- Implementar RDS Multi-AZ con MySQL
- Configurar grupos de seguridad y backups

Fase 3: Balanceador de carga (30 minutos)

- Crear Application Load Balancer
- Configurar health checks y SSL mediante ACM

Fase 4: Auto Scaling y WordPress (45 minutos)

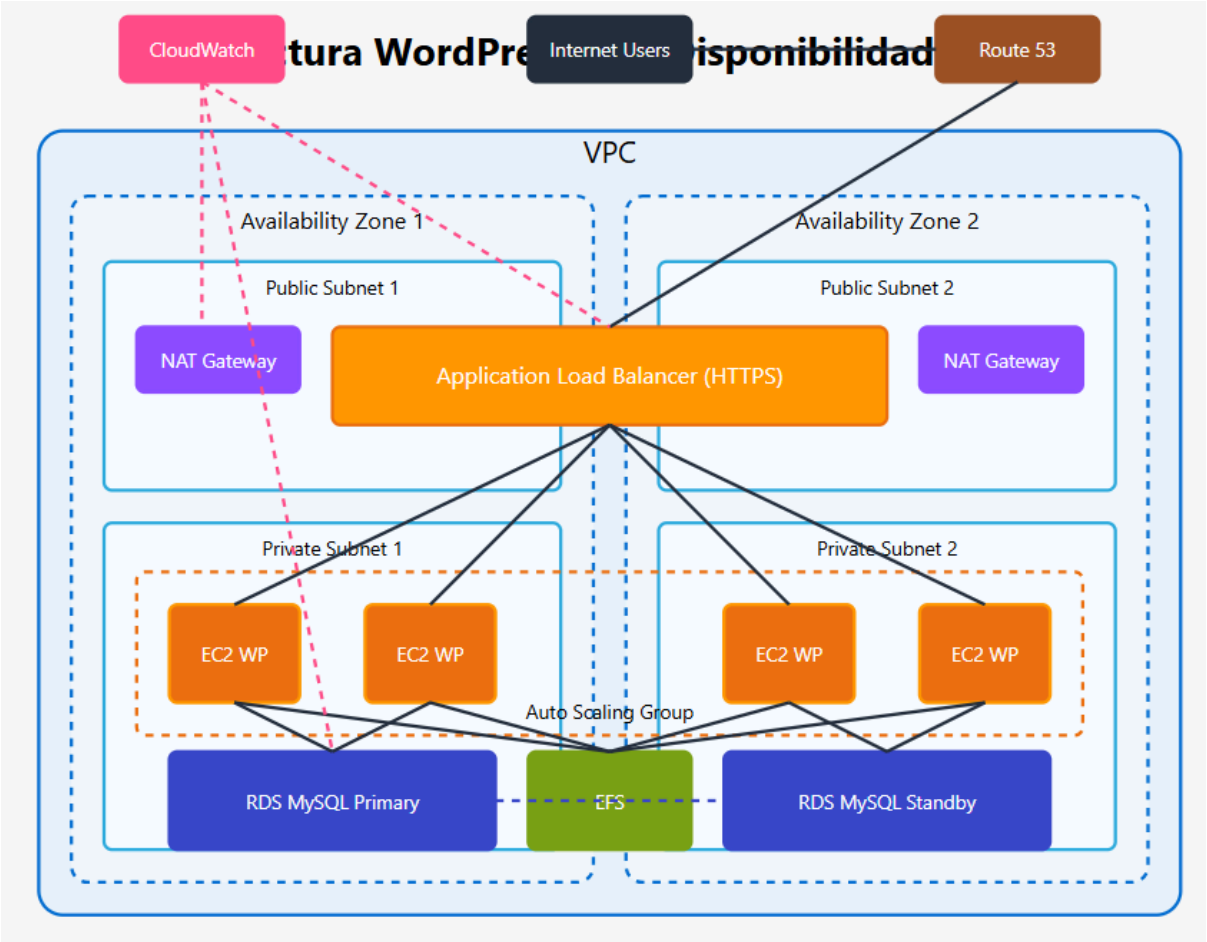
- Crear plantilla de lanzamiento con Ubuntu
- Configurar script de inicio para WordPress
- Implementar grupo de Auto Scaling

Fase 5: Monitorización y pruebas (30 minutos)

- Configurar CloudWatch y alarmas
- Verificar el funcionamiento de WordPress

- Probar escalabilidad

Diagrama de arquitectura



Justificación del diseño

Esta arquitectura es ideal para un WordPress de alta disponibilidad y escalabilidad por las siguientes razones:

Redundancia y tolerancia a fallos:

- Múltiples zonas de disponibilidad protegen contra fallos de infraestructura.
- RDS Multi-AZ proporciona alta disponibilidad para la base de datos.
- El sistema puede seguir funcionando incluso si una zona completa falla.

Escalabilidad:

- Auto Scaling permite aumentar o reducir automáticamente la capacidad según la demanda.
- Las instancias EC2 se distribuyen en varias zonas de disponibilidad.
- EFS proporciona almacenamiento compartido que crece según sea necesario.

Rendimiento optimizado:

- El Application Load Balancer distribuye el tráfico de manera eficiente.
- Las instancias en subredes privadas están protegidas de acceso directo.
- NAT Gateways permiten a las instancias privadas acceder a Internet para actualizaciones.

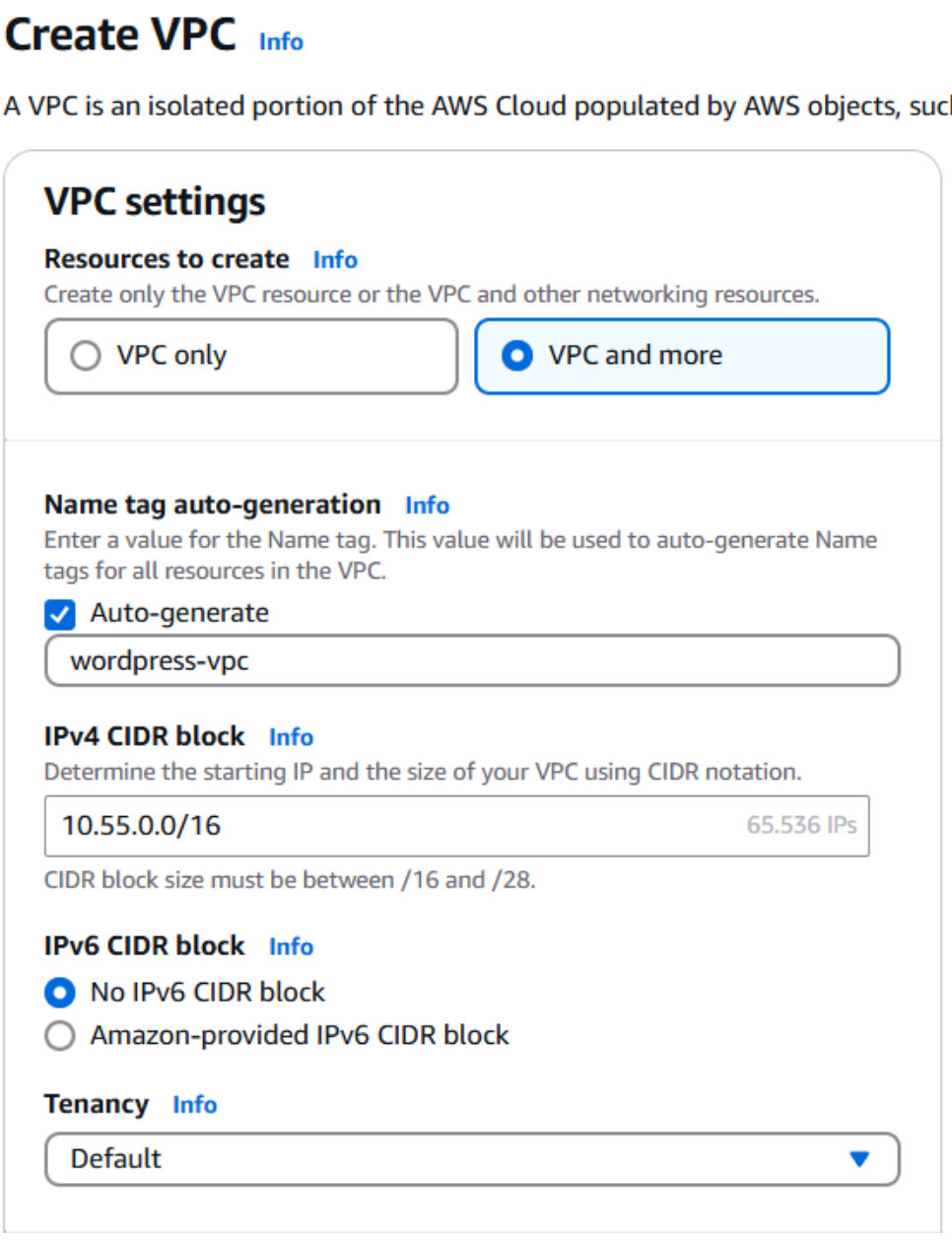
Seguridad:

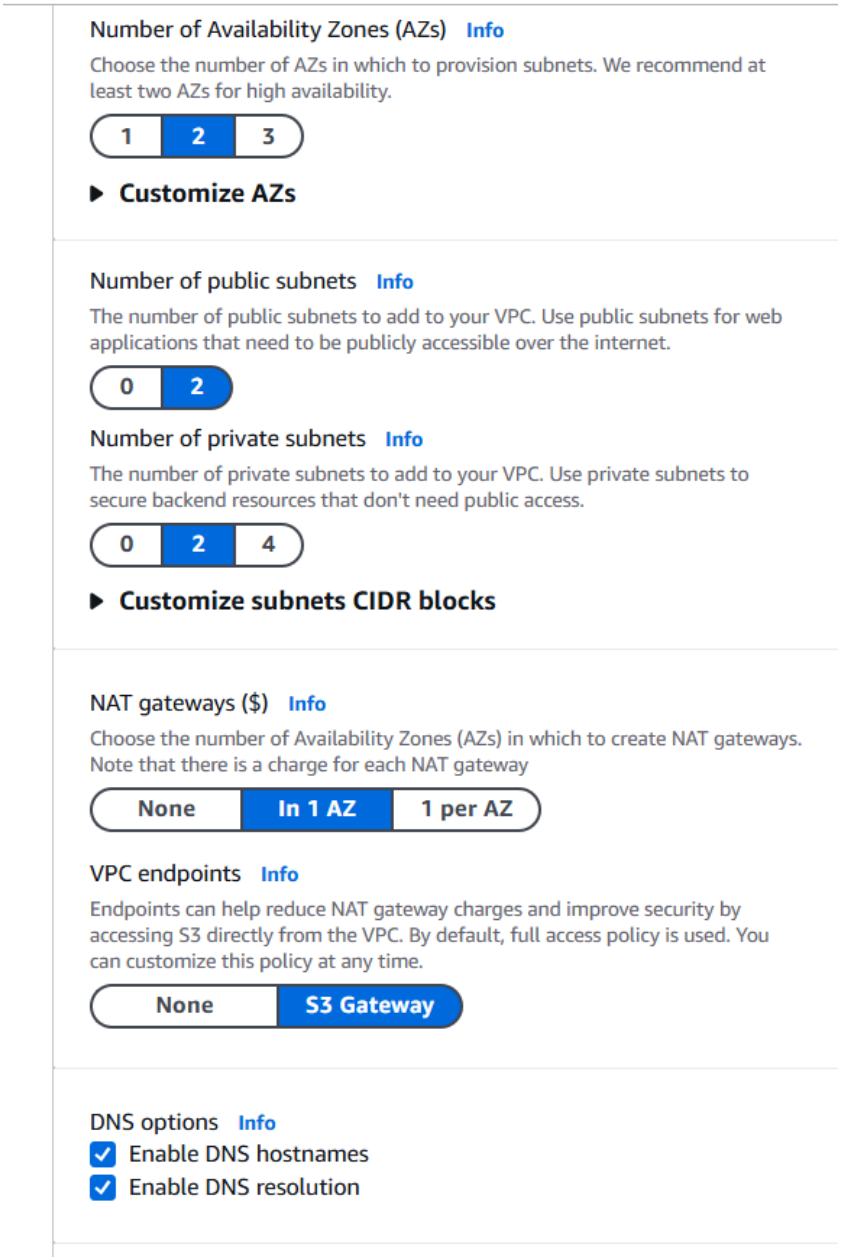
- HTTPS en el ALB mediante AWS Certificate Manager.
- Subredes privadas para componentes críticos.
- Grupos de seguridad restrictivos.

Implementación paso a paso

Fase 1: Infraestructura base

1.1. Crear VPC y subredes

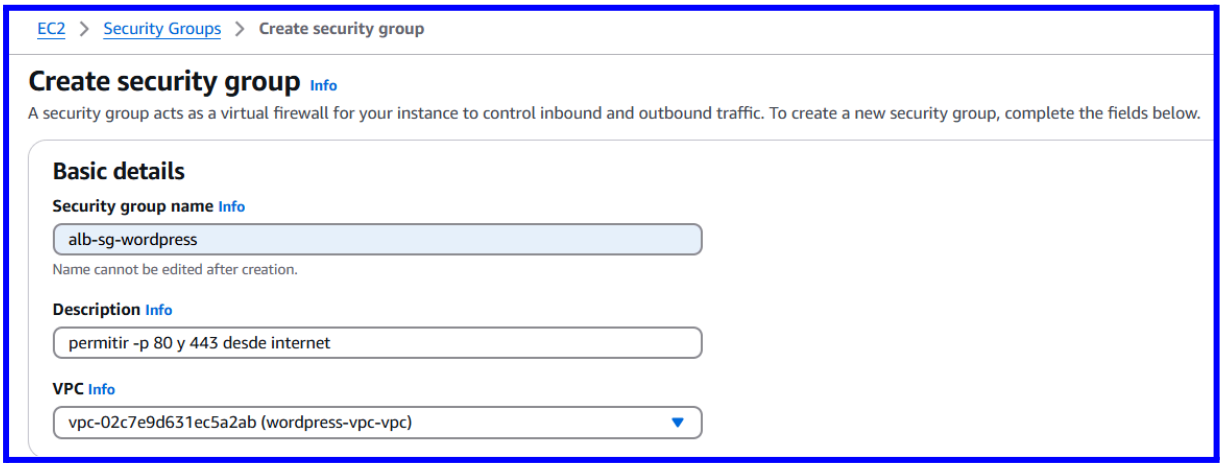


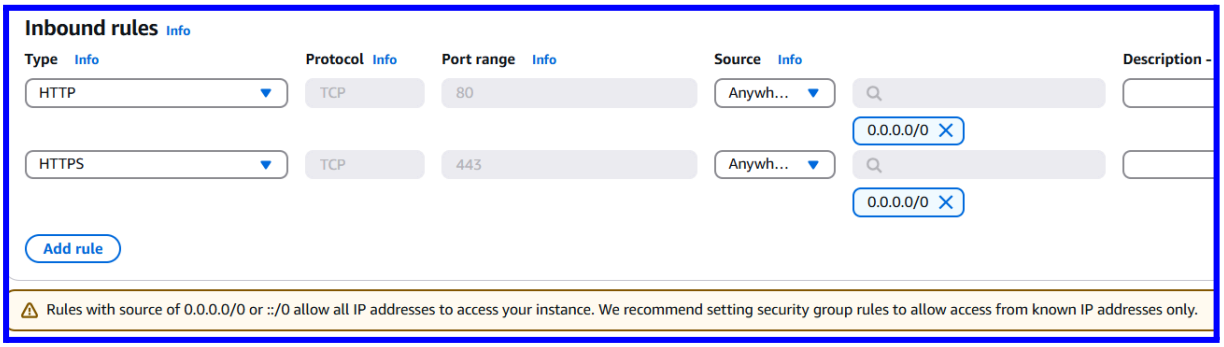


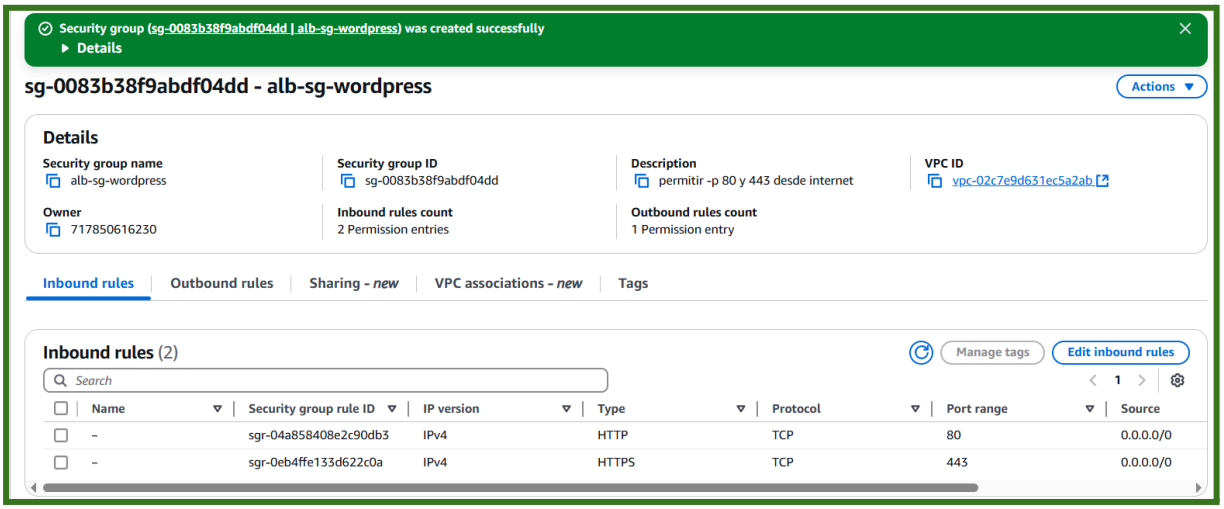
Esto creará 2 subredes pub para el alb y 2 subredes priv para las ec2. Tablas de rutas configuradas. IGW y NGW para tráfico saliente desde las subredes privadas.

1.2. Configurar grupos de seguridad

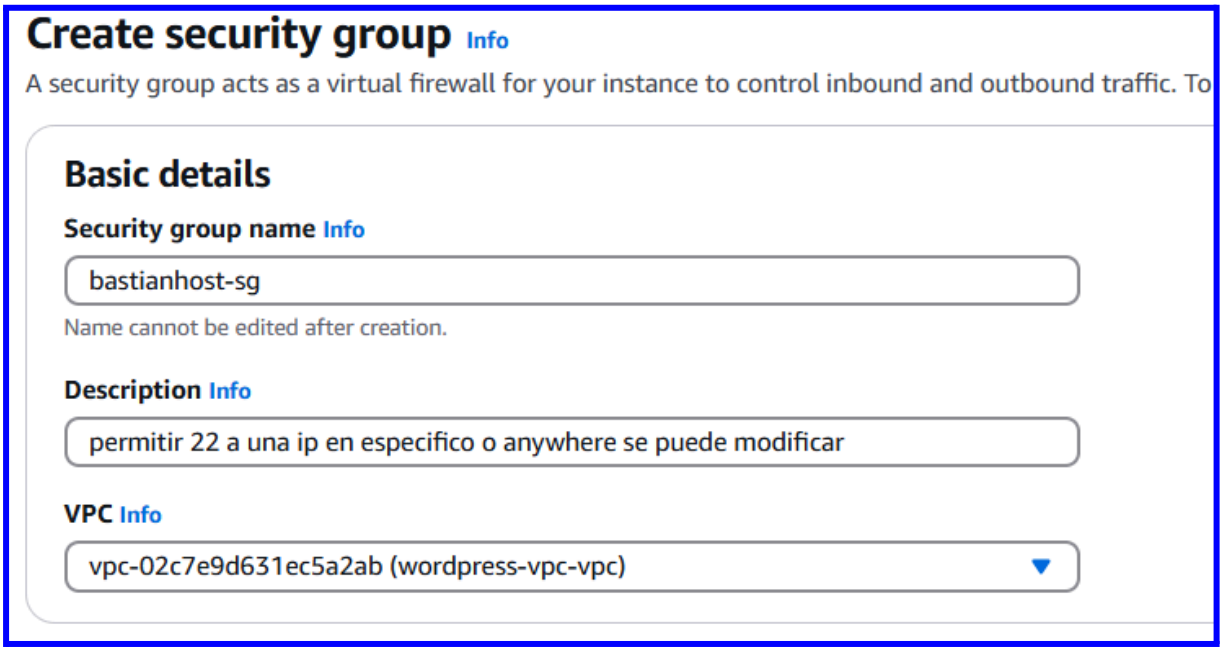
alb-sg-wordpress

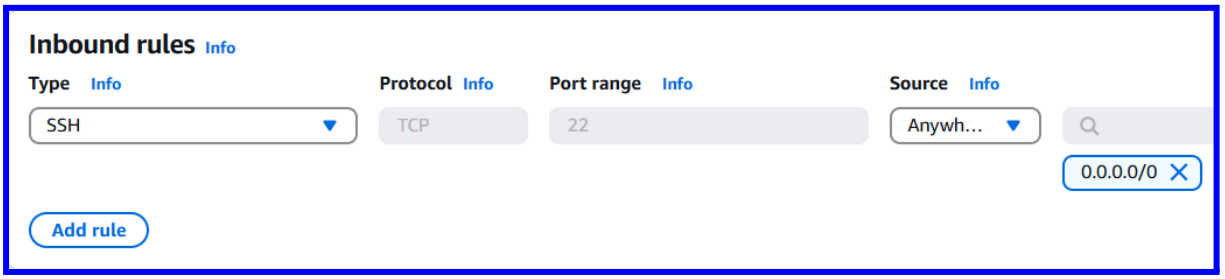


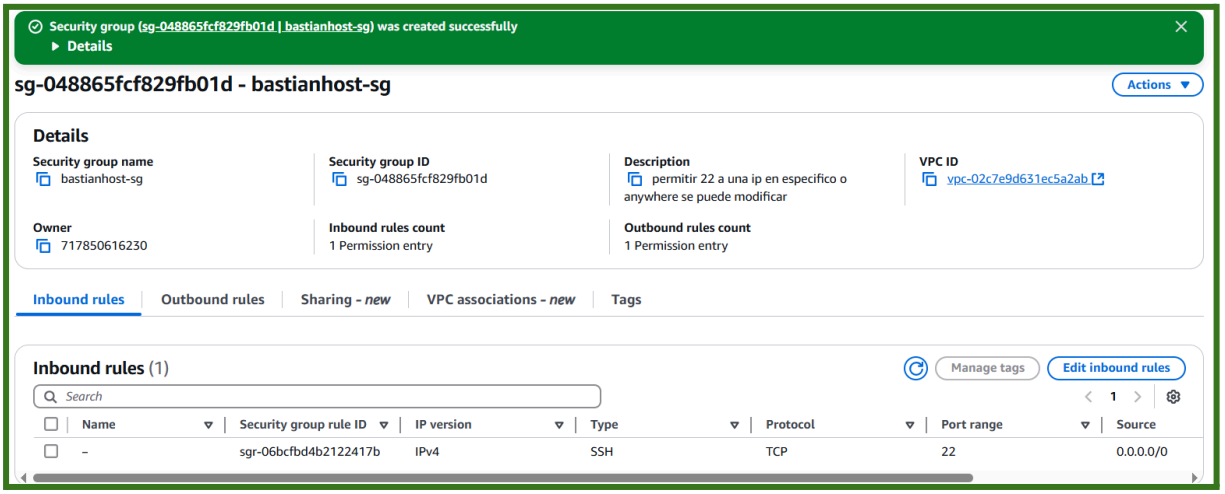




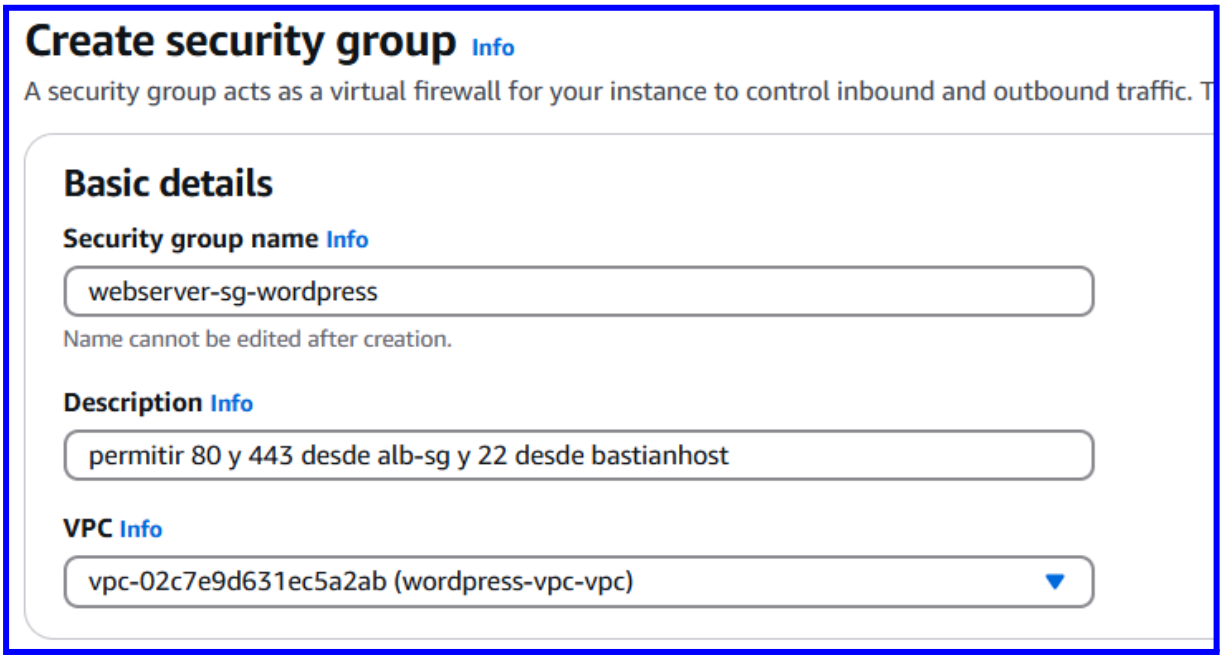
bastianhost-sg

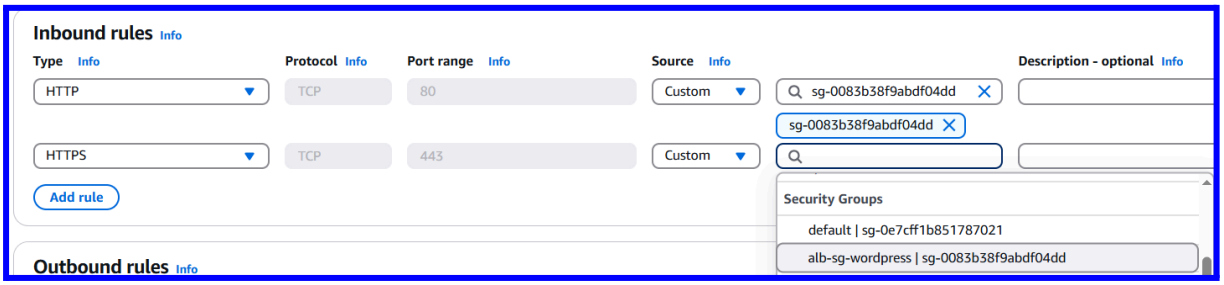




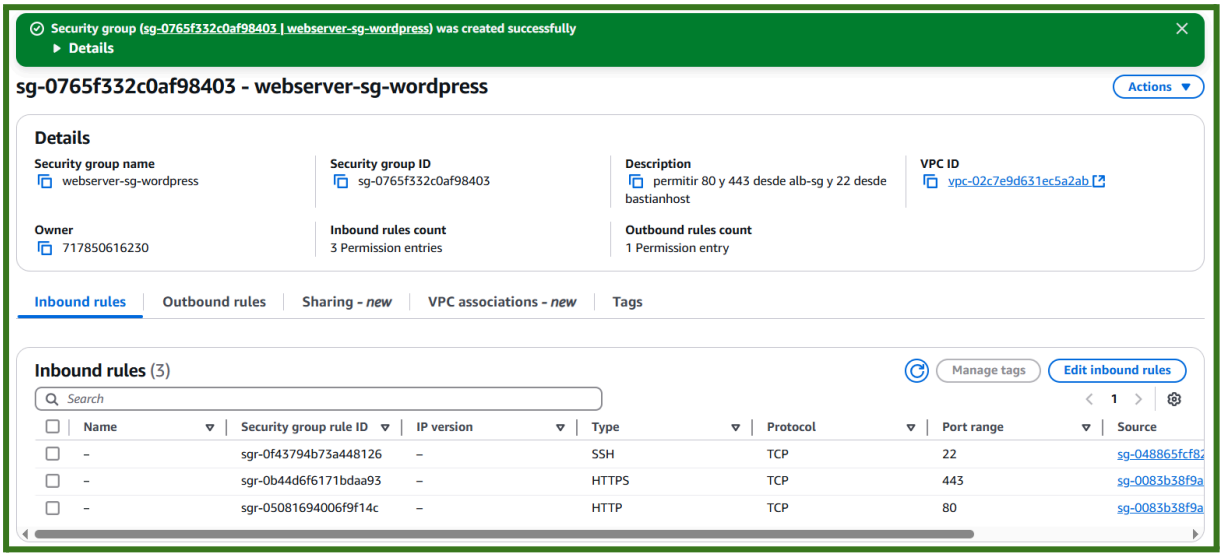


webserver-sg-wordpress

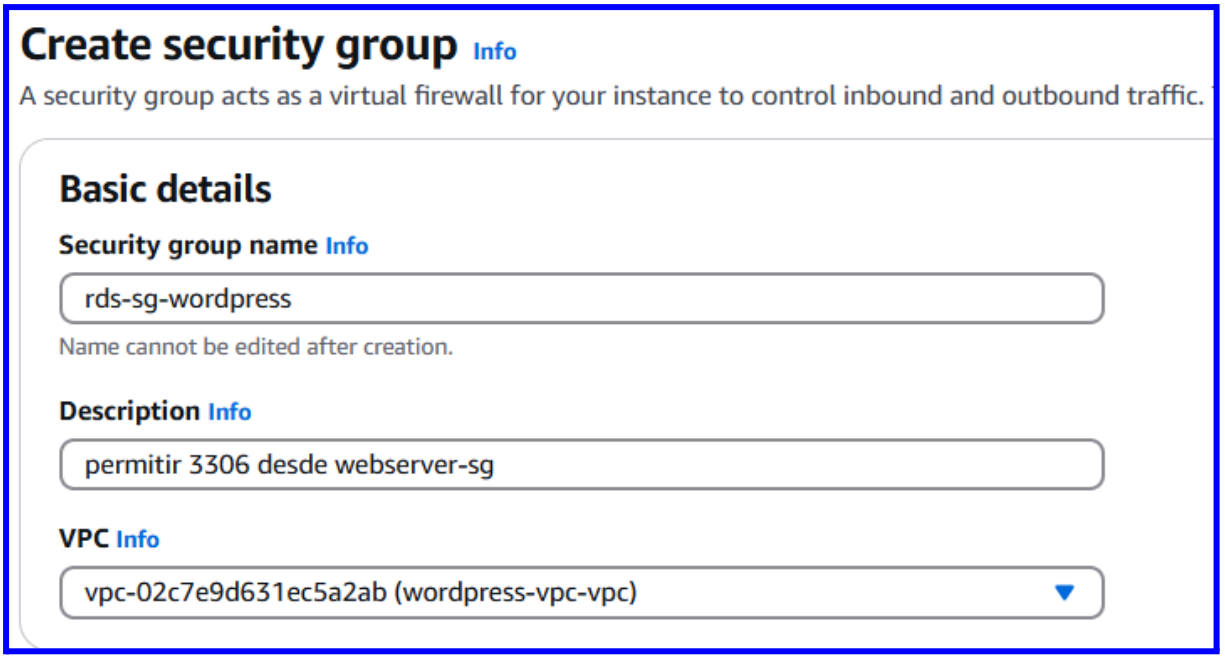


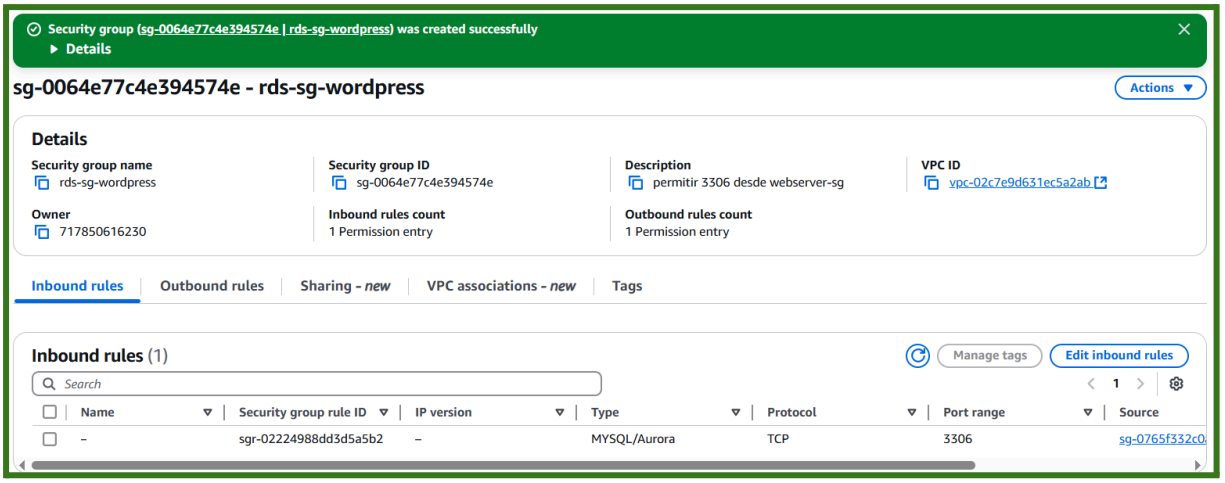



Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
HTTP
TCP
80
Custom
sg-0083b38f9abdf04dd
HTTPS
TCP
443
Custom
sg-0083b38f9abdf04dd
SSH
TCP
22
Custom
alb-sg-wordpress | sg-0083b38f9abdf04dd
bastianhost-sg | sg-048865fcf829fb01d
Add rule

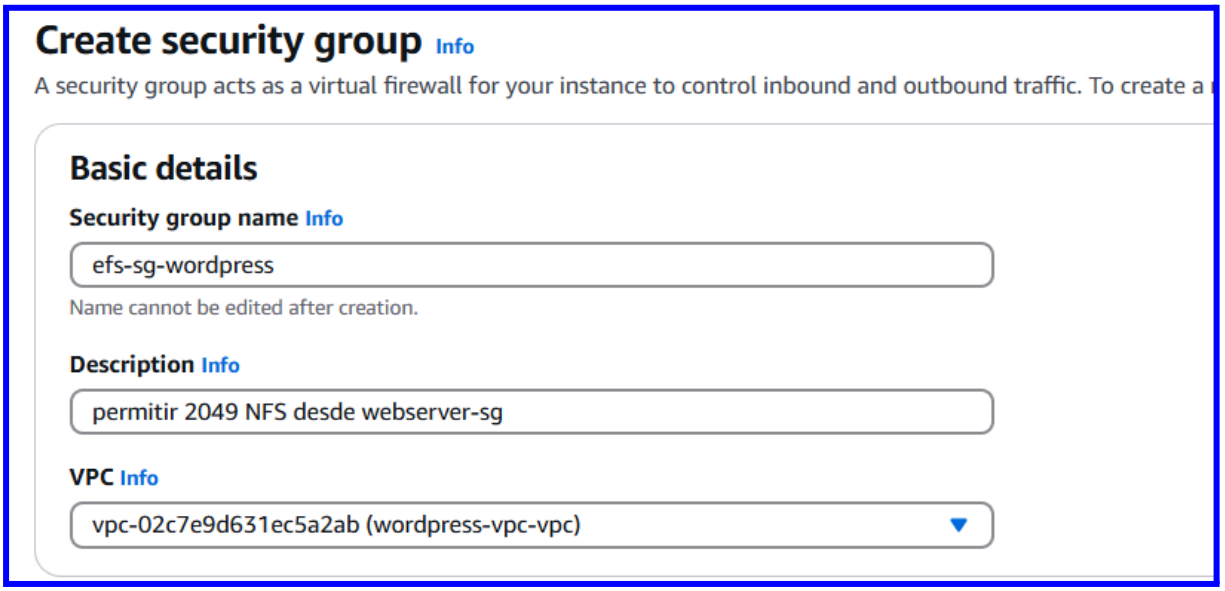

Security group (sg-0765f332c0af98403 | webserver-sg-wordpress) was created successfully
Details
sg-0765f332c0af98403 - webserver-sg-wordpress
Actions
Details
Security group name
webserver-sg-wordpress
Security group ID
sg-0765f332c0af98403
Description
permitir 80 y 443 desde alb-sg y 22 desde bastianhost
VPC ID
vpc-02c7e9d631ec5a2ab
Owner
717850616230
Inbound rules count
3 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (3)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
Source
sgr-0f43794b73a448126
SSH
TCP
22
sgr-0b44d6f6171bdaa93
HTTPS
TCP
443
sgr-05081694006f9f14c
HTTP
TCP
80

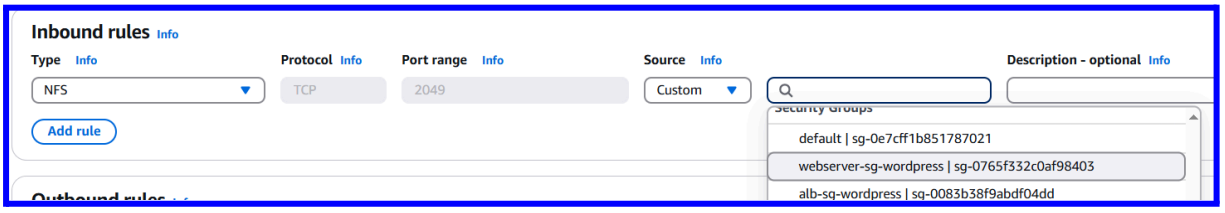
rds-sg-wordpress

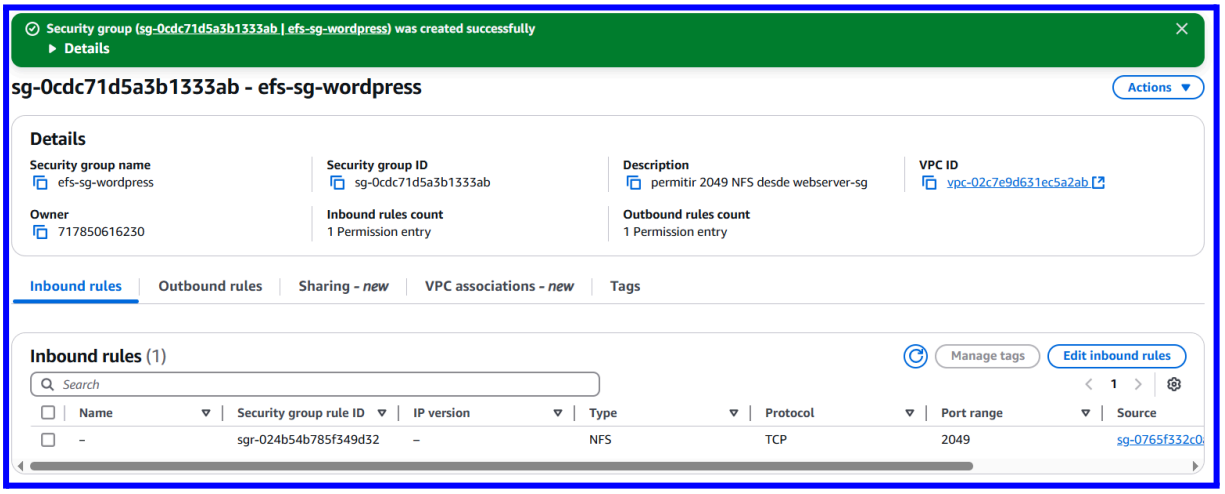




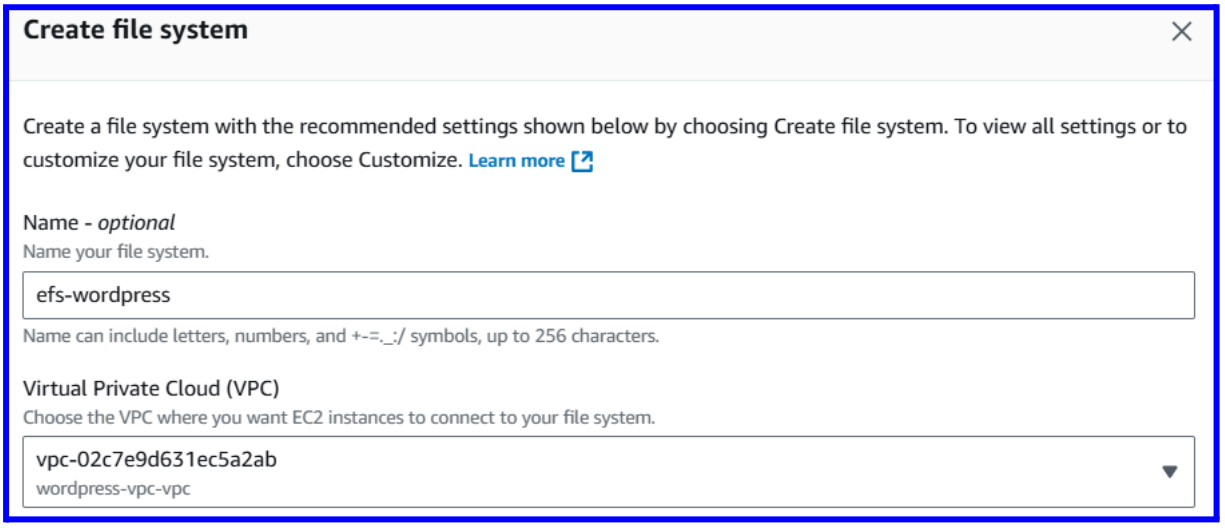
efs-sg-wordpress



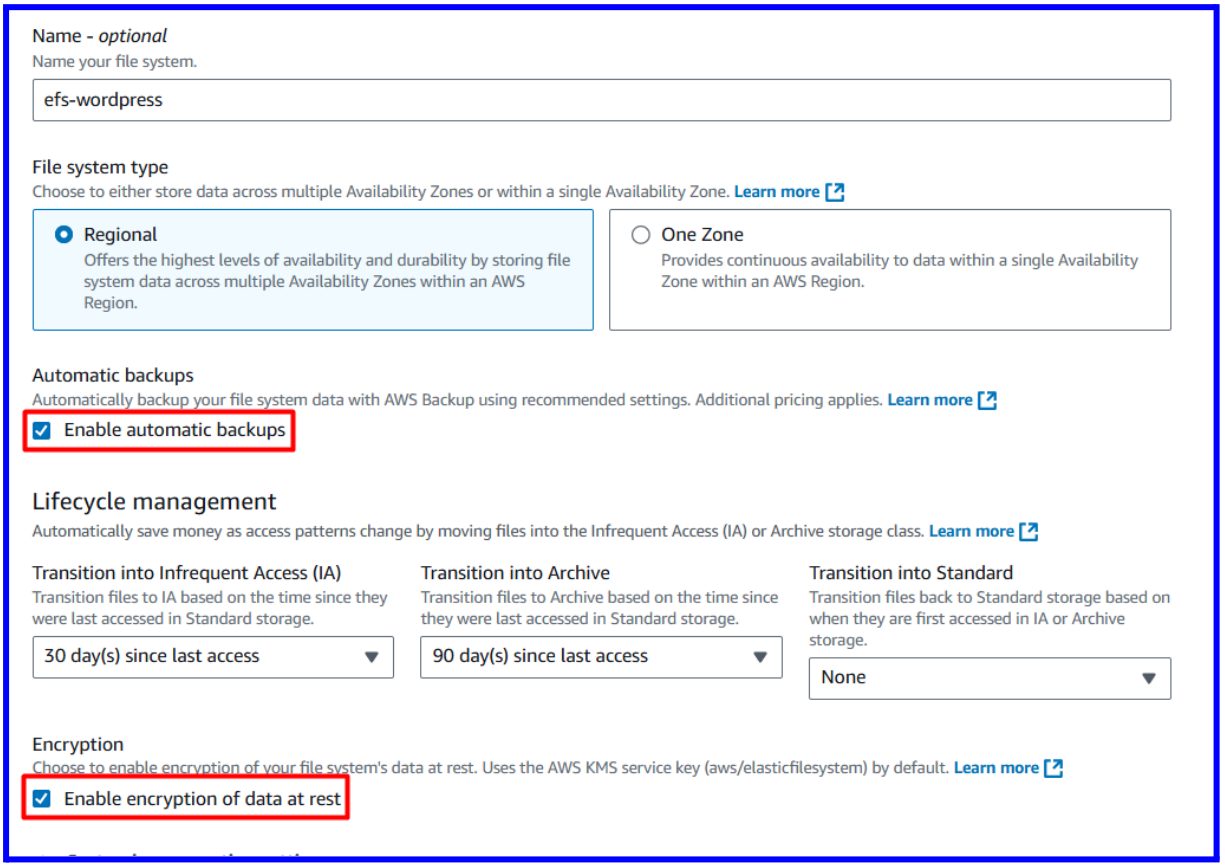


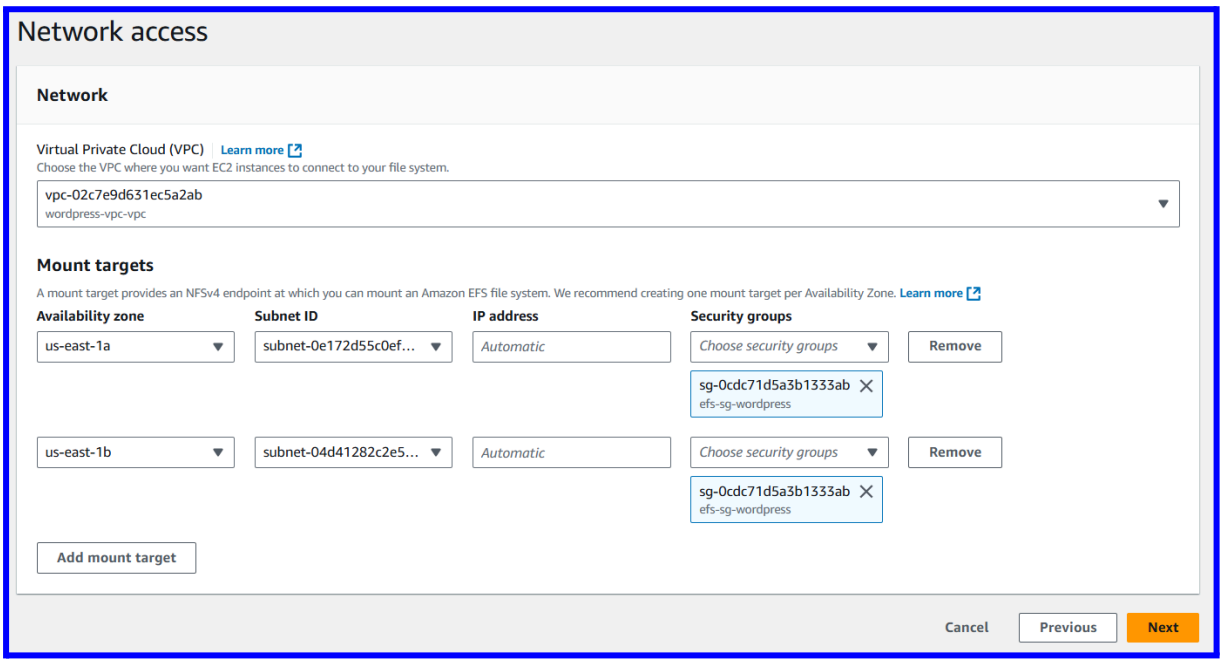


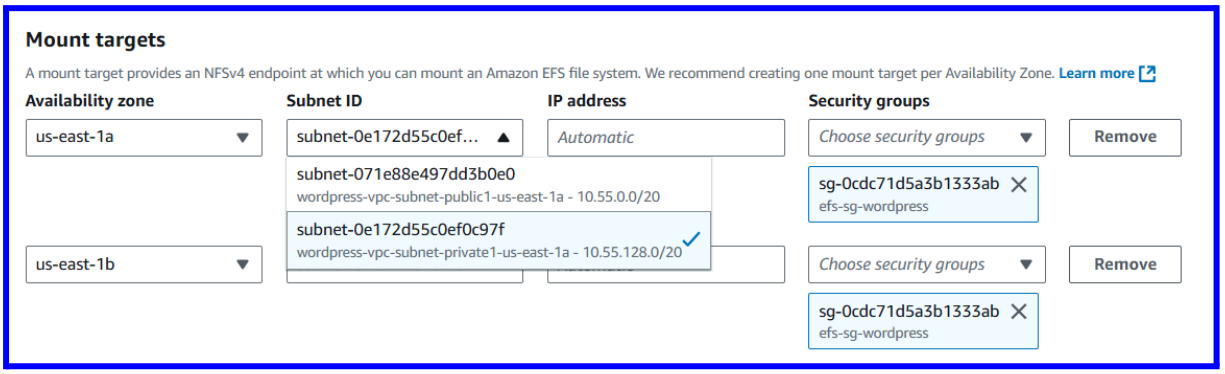
1.3. Configurar EFS para almacenamiento compartido

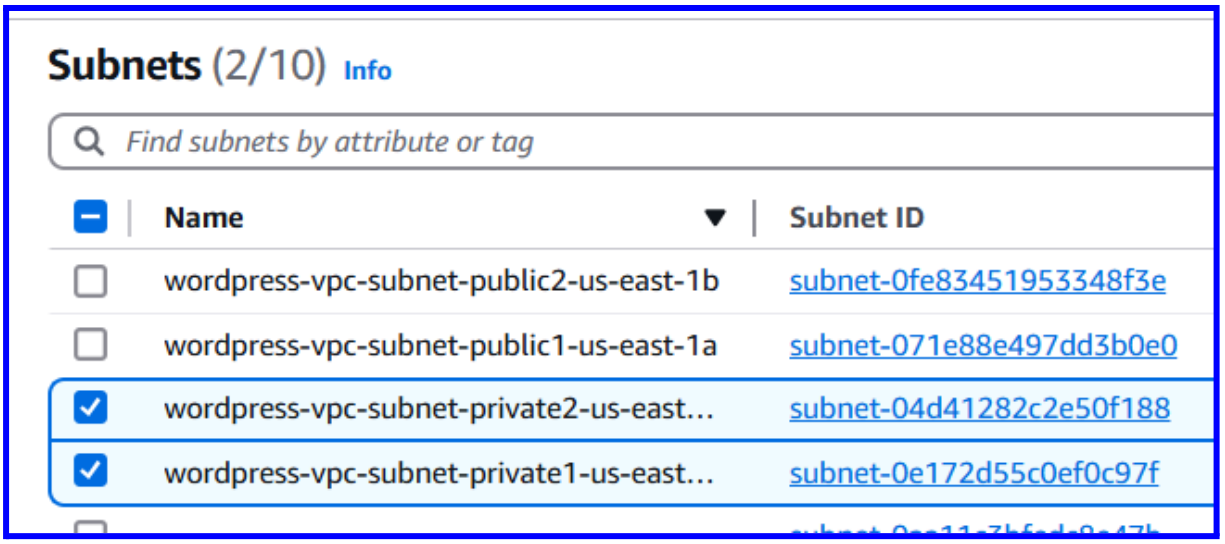


CUSTOMIZER

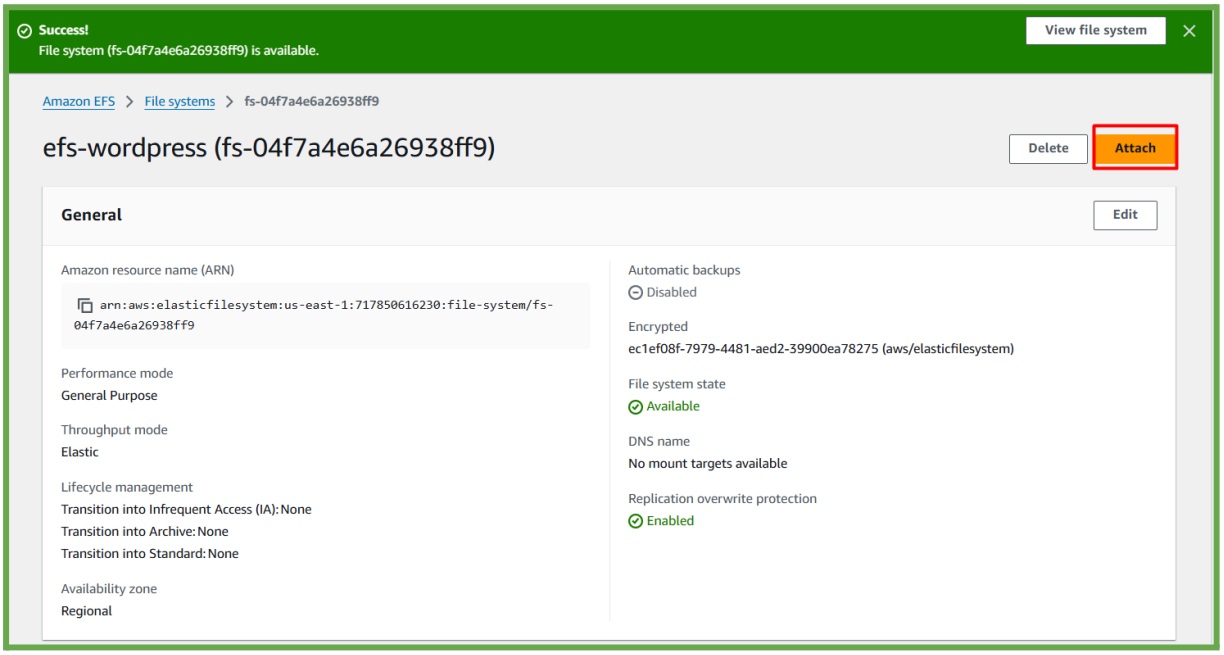






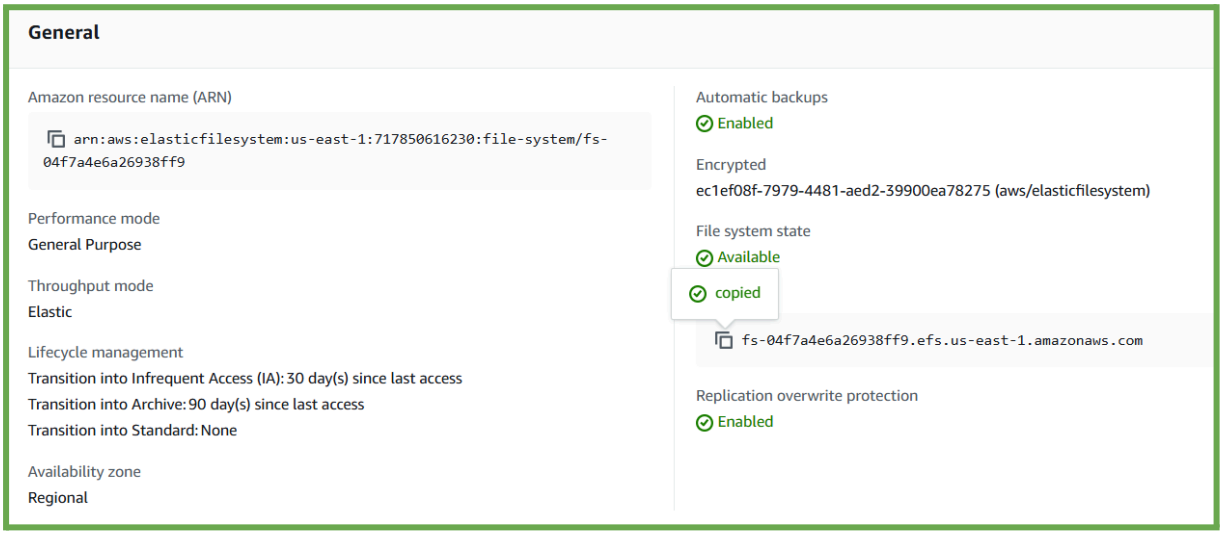


Crear mount targets en las **subredes privadas** de ambas AZs



COPY dns name

`fs-04f7a4e6a26938ff9.efs.us-east-1.amazonaws.com`



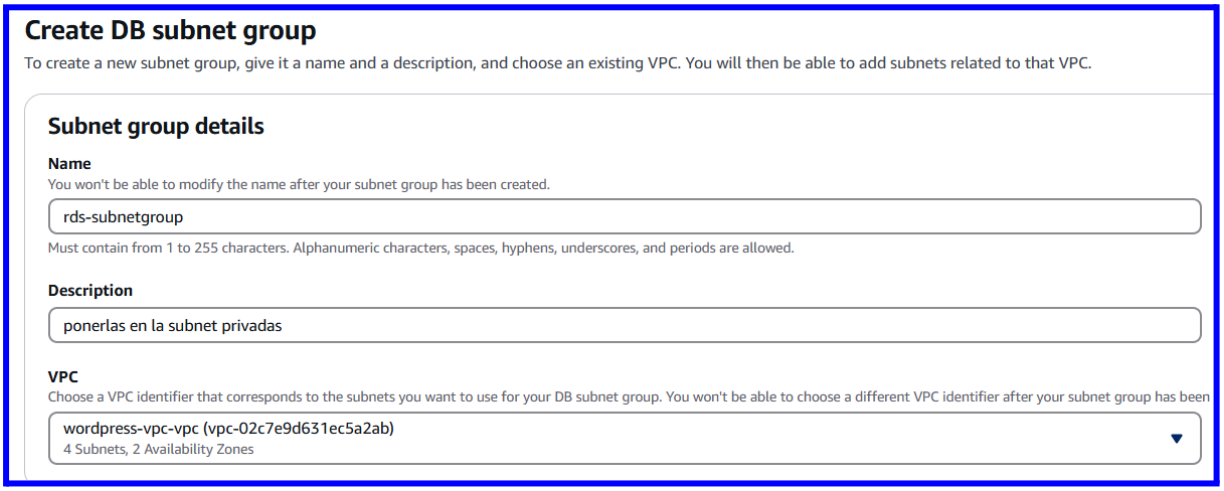
DNS NAME EFS

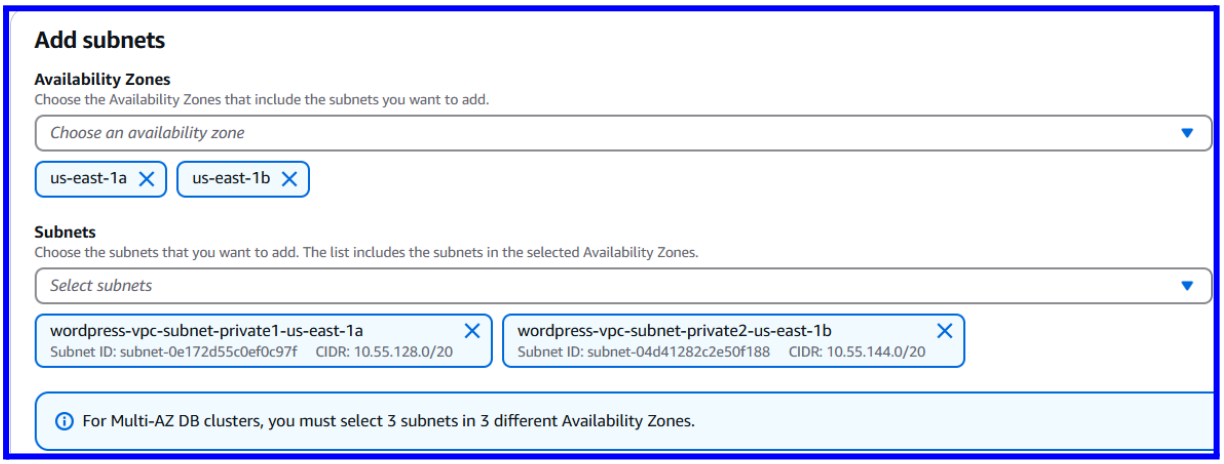
fs-04f7a4e6a26938ff9.efs.us-east-1.amazonaws.com

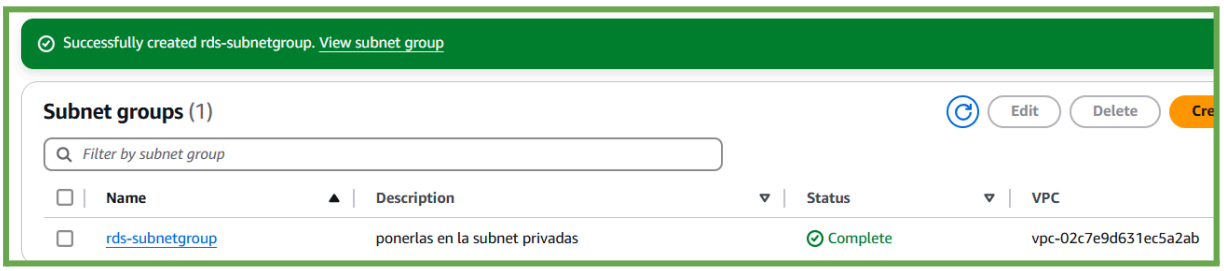
Fase 2: Base de datos

2.1. Implementar RDS Multi-AZ

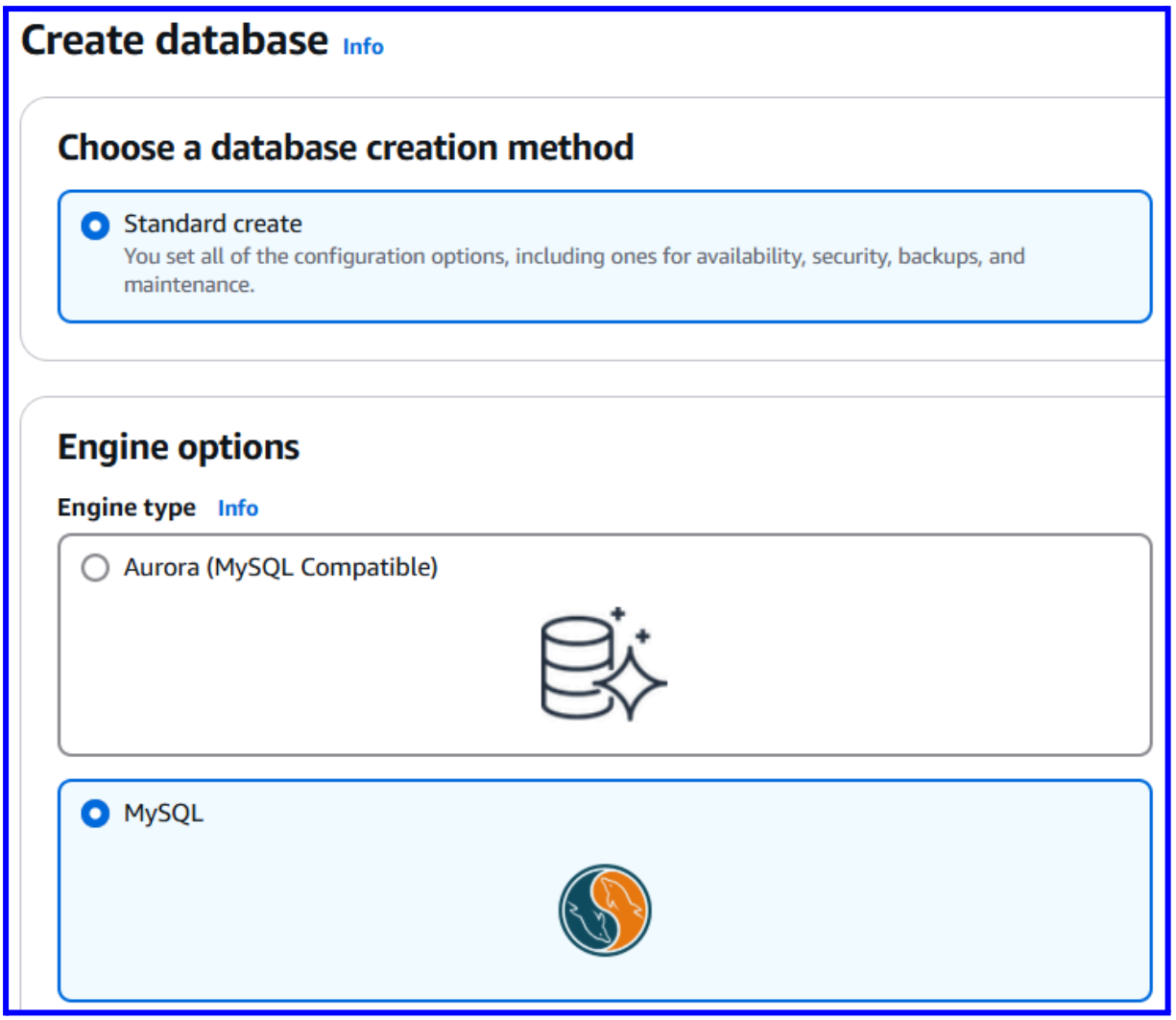
DB subnet group

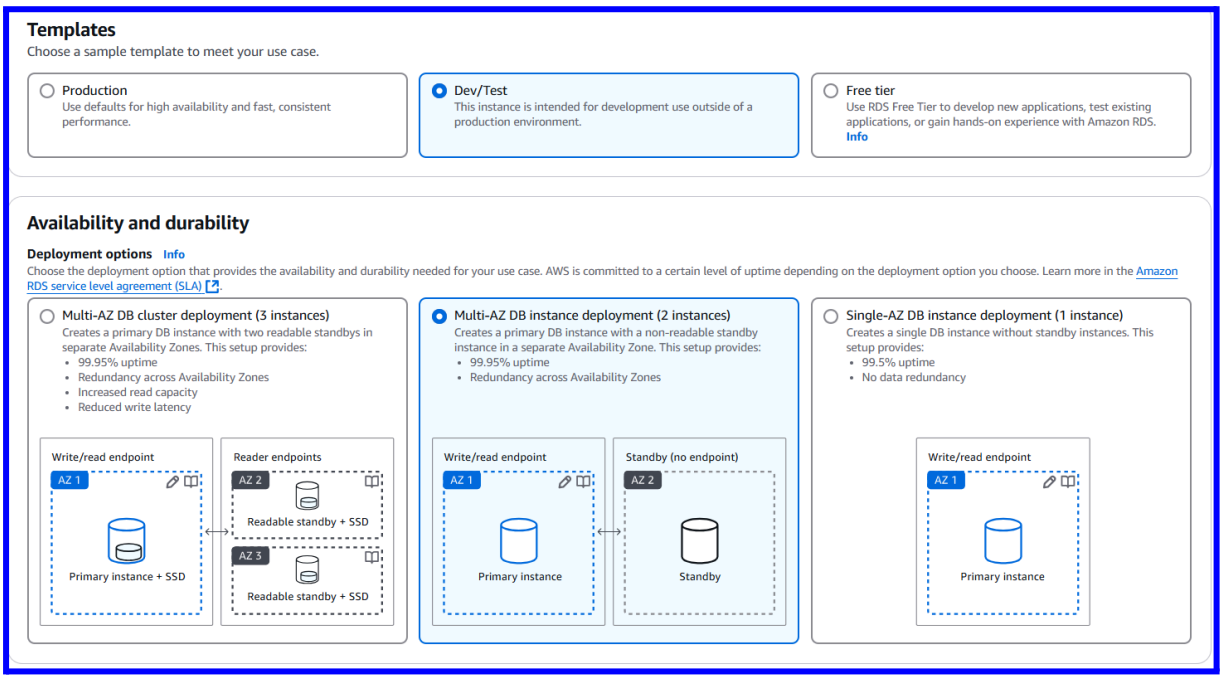


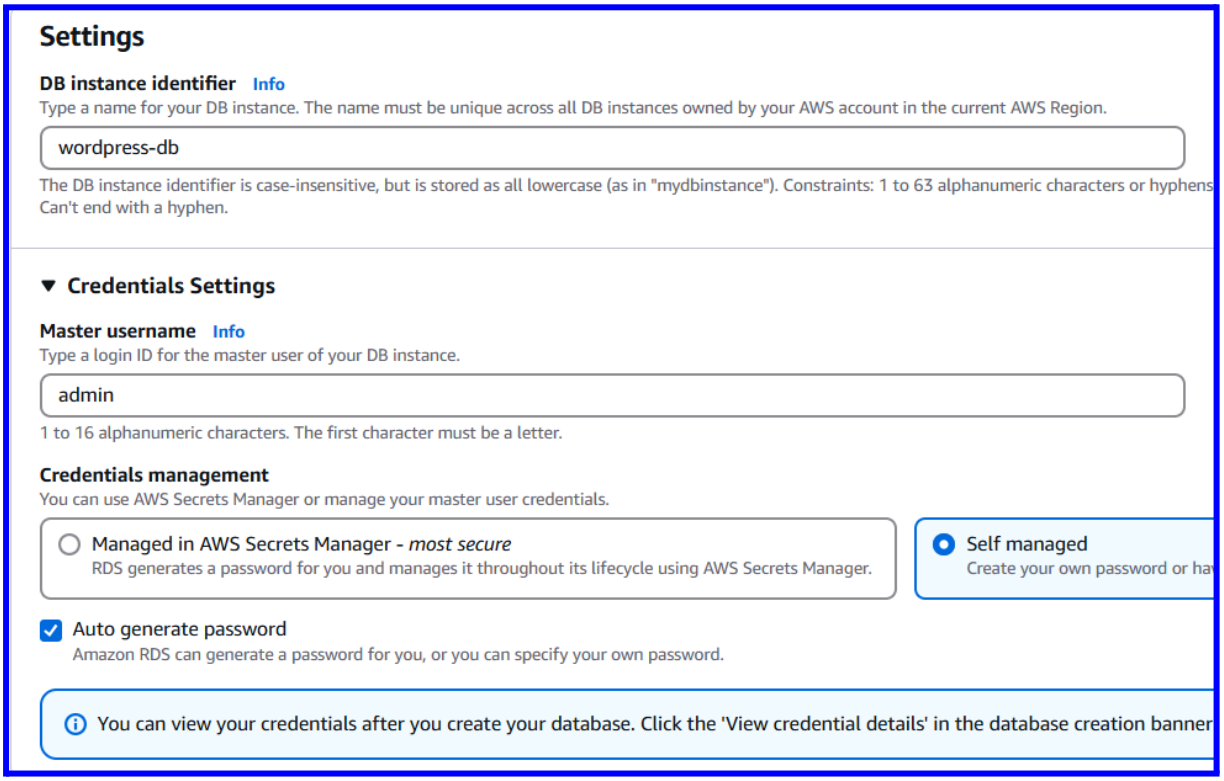


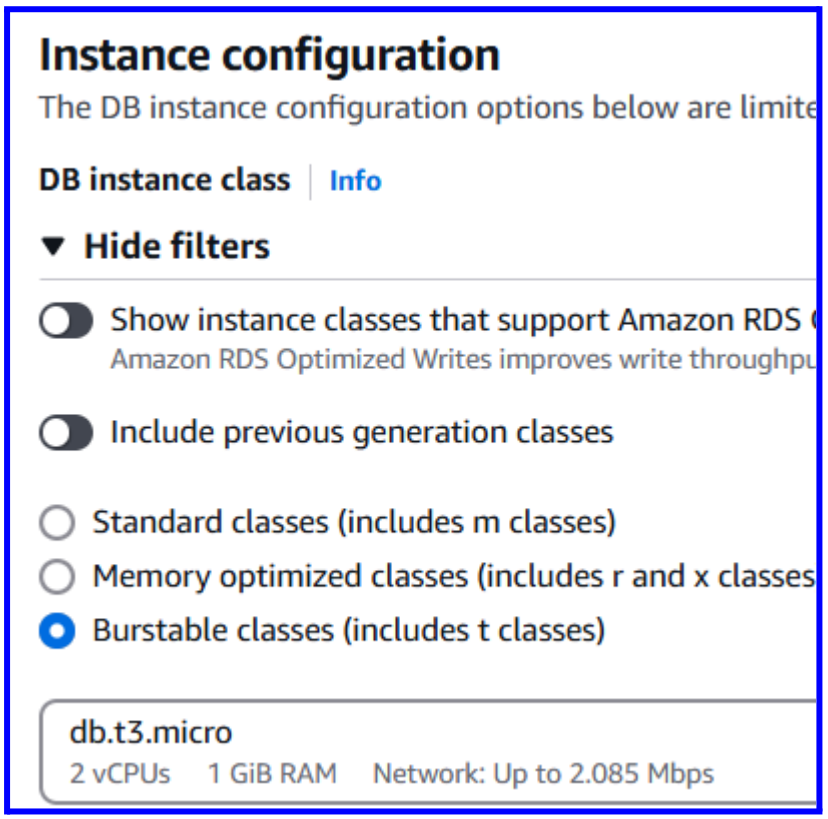


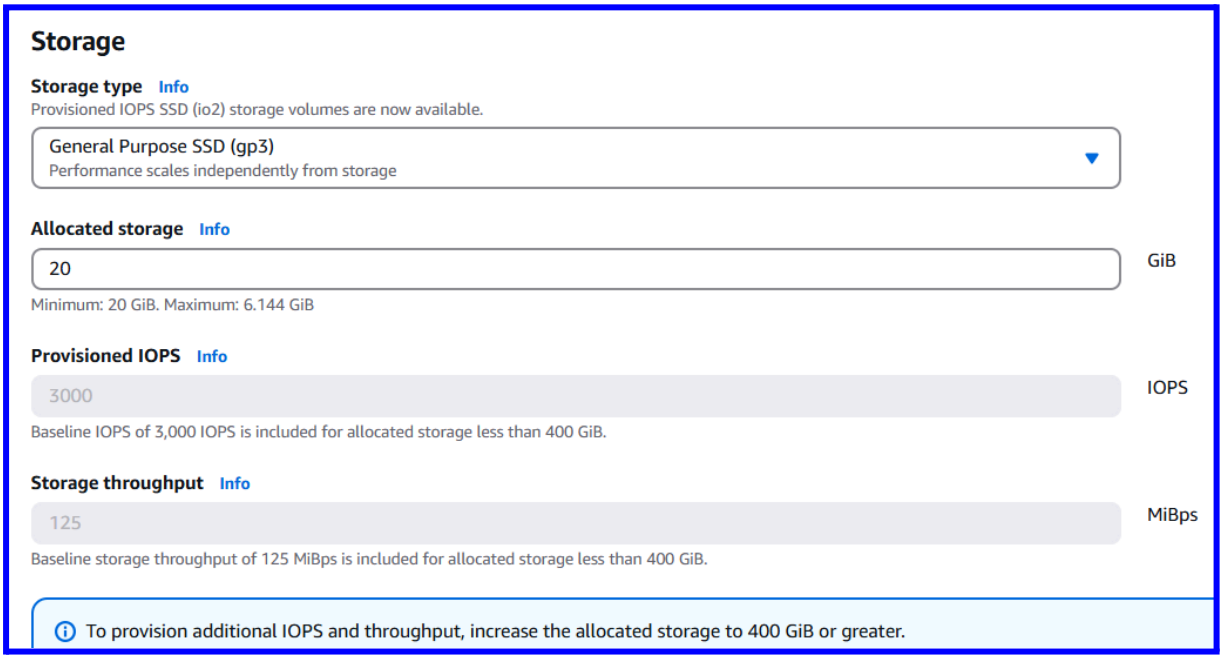
CREATE DB

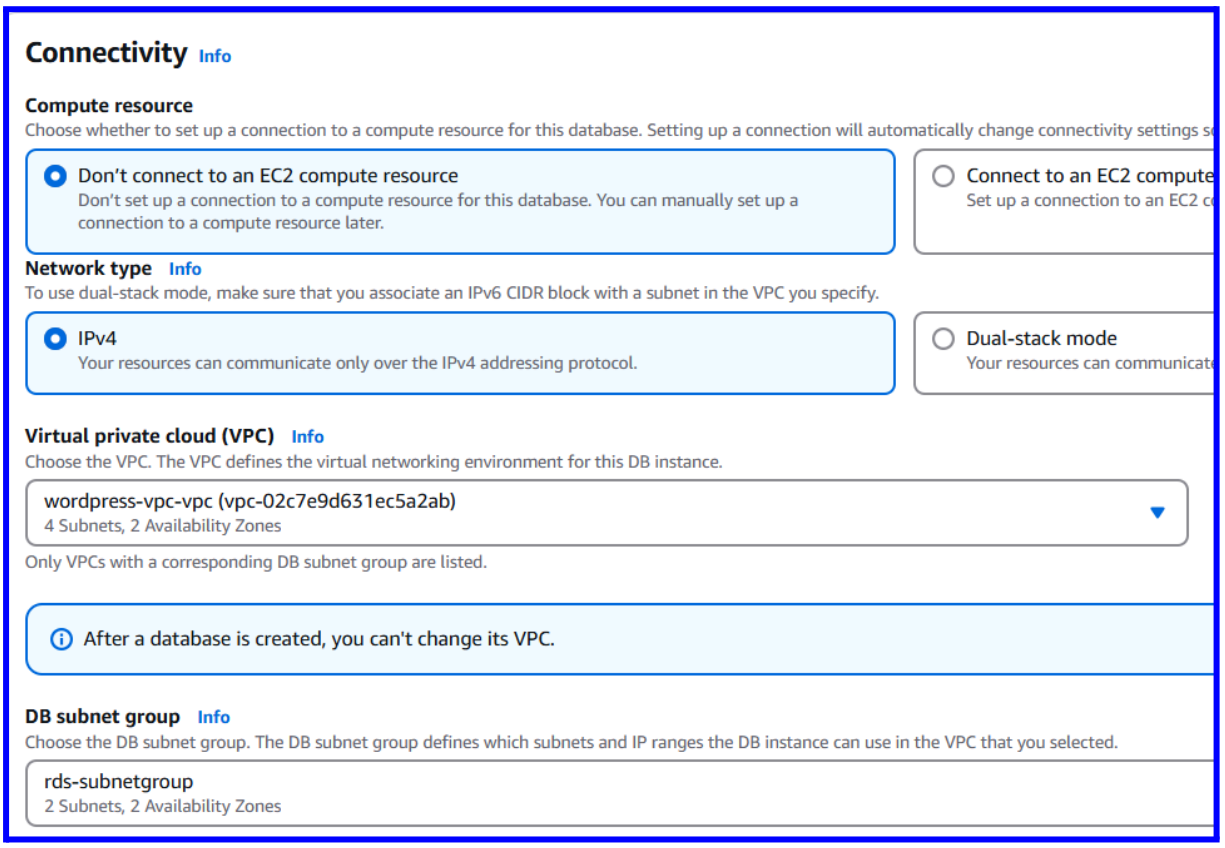

Create database Info
Choose a database creation method
Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.
Engine options
Engine type Info
Aurora (MySQL Compatible)
MySQL

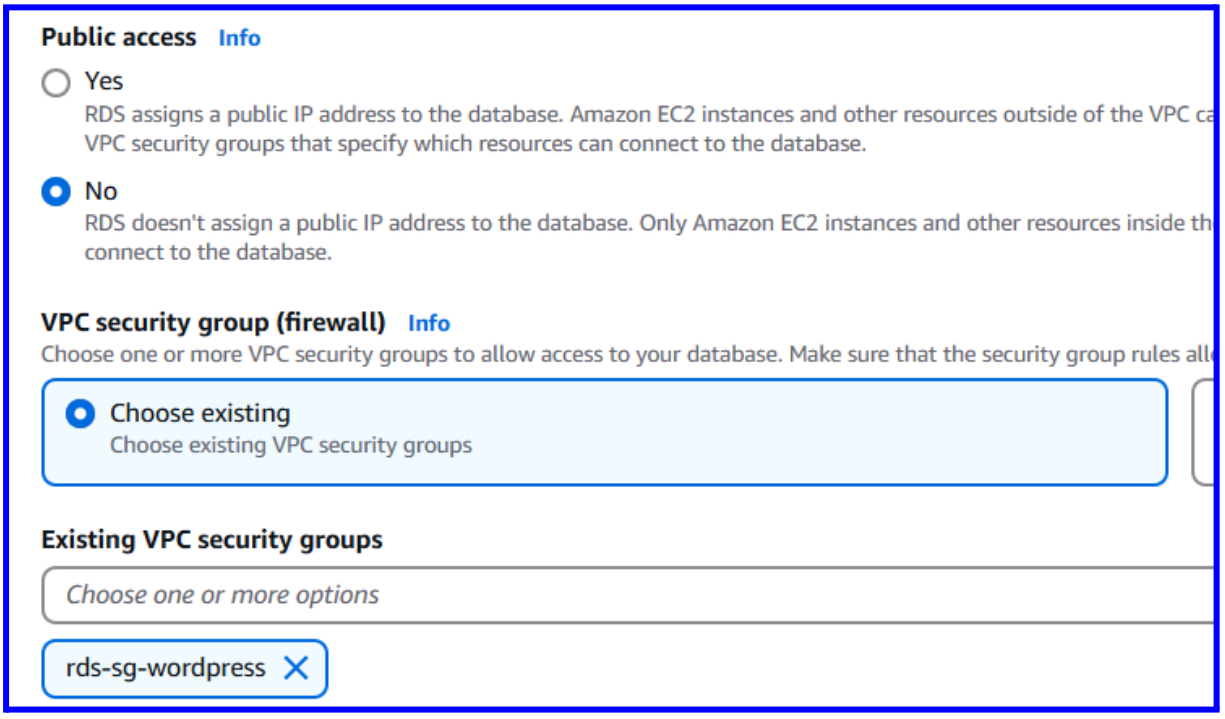

Templates
Choose a sample template to meet your use case.
Production
Use defaults for high availability and fast, consistent performance.
Dev/Test
This instance is intended for development use outside of a production environment.
Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
Info
Availability and durability
Deployment options Info
Choose the deployment option that provides the availability and durability needed for your use case. AWS is committed to a certain level of uptime depending on the deployment option you choose. Learn more in the Amazon RDS service level agreement (SLA).
Multi-AZ DB cluster deployment (3 instances)
Creates a primary DB instance with two readable standbys in separate Availability Zones. This setup provides:
99.95% uptime
Redundancy across Availability Zones
Increased read capacity
Reduced write latency
Write/read endpoint
AZ 1
Primary instance + SSD
Reader endpoints
AZ 2
Readable standby + SSD
AZ 3
Readable standby + SSD
Multi-AZ DB instance deployment (2 instances)
Creates a primary DB instance with a non-readable standby instance in a separate Availability Zone. This setup provides:
99.95% uptime
Redundancy across Availability Zones
Write/read endpoint
AZ 1
Primary instance
Standby (no endpoint)
AZ 2
Standby
Single-AZ DB instance deployment (1 instance)
Creates a single DB instance without standby instances. This setup provides:
99.5% uptime
No data redundancy
Write/read endpoint
AZ 1
Primary instance

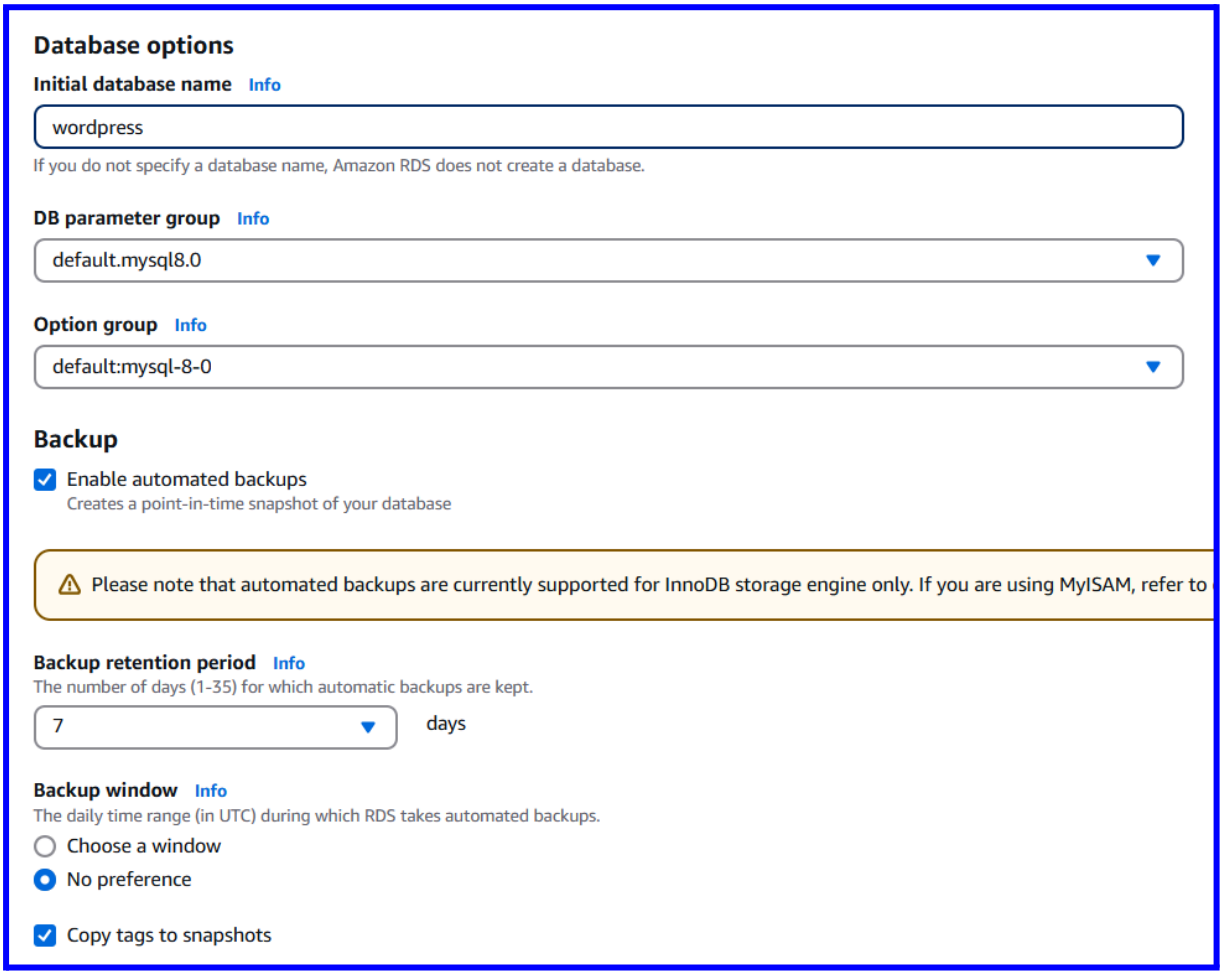

Settings
DB instance identifier Info
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.
wordpress-db
The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens
Can't end with a hyphen.
Credentials Settings
Master username Info
Type a login ID for the master user of your DB instance.
admin
1 to 16 alphanumeric characters. The first character must be a letter.
Credentials management
You can use AWS Secrets Manager or manage your master user credentials.
Managed in AWS Secrets Manager - most secure
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.
Self managed
Create your own password or ha
Auto generate password
Amazon RDS can generate a password for you, or you can specify your own password.
You can view your credentials after you create your database. Click the 'View credential details' in the database creation banner

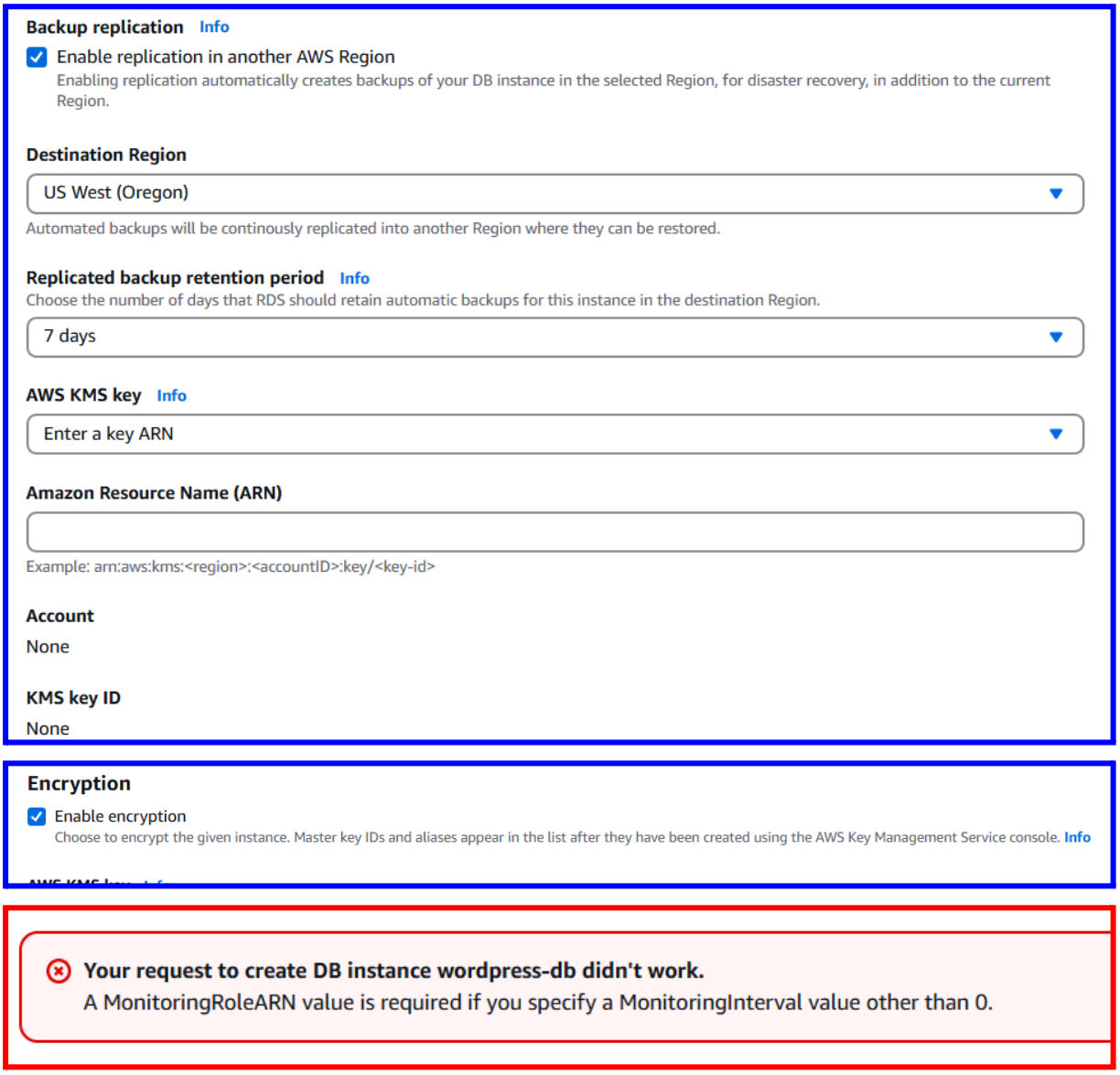

Instance configuration
The DB instance configuration options below are limite
DB instance class
Info
Hide filters
Show instance classes that support Amazon RDS
Amazon RDS Optimized Writes improves write throughpu
Include previous generation classes
Standard classes (includes m classes)
Memory optimized classes (includes r and x classes
Burstable classes (includes t classes)
db.t3.micro
2 vCPUs
1 GiB RAM
Network: Up to 2.085 Mbps


Storage
Storage type
Info
Provisioned IOPS SSD (io2) storage volumes are now available.
General Purpose SSD (gp3)
Performance scales independently from storage
Allocated storage
Info
20
GiB
Minimum: 20 GiB. Maximum: 6.144 GiB
Provisioned IOPS
Info
3000
IOPS
Baseline IOPS of 3,000 IOPS is included for allocated storage less than 400 GiB.
Storage throughput
Info
125
MiBps
Baseline storage throughput of 125 MiBps is included for allocated storage less than 400 GiB.
To provision additional IOPS and throughput, increase the allocated storage to 400 GiB or greater.

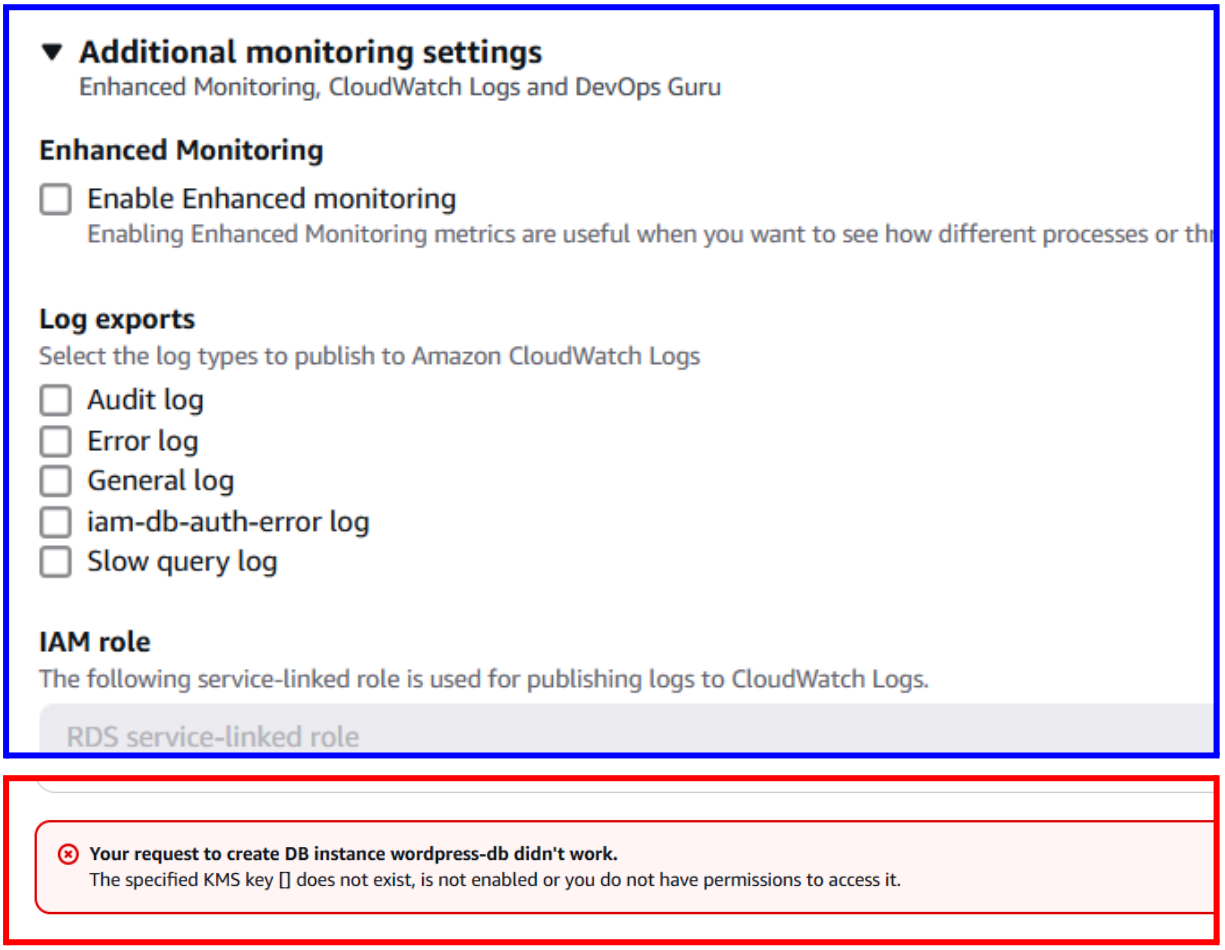

Connectivity Info
Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings s
Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.
Connect to an EC2 compute
Set up a connection to an EC2 c
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 communicat
Virtual private cloud (VPC) Info
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.
wordpress-vpc-vpc (vpc-02c7e9d631ec5a2ab)
4 Subnets, 2 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.
rds-subnetgroup
2 Subnets, 2 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 ca
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 th
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 all
Choose existing
Choose existing VPC security groups
Existing VPC security groups
Choose one or more options
rds-sg-wordpress


Database options
Initial database name Info
wordpress
If you do not specify a database name, Amazon RDS does not create a database.
DB parameter group Info
default.mysql8.0
Option group Info
default:mysql-8-0
Backup
Enable automated backups
Creates a point-in-time snapshot of your database
Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to
Backup retention period Info
The number of days (1-35) for which automatic backups are kept.
7
days
Backup window Info
The daily time range (in UTC) during which RDS takes automated backups.
Choose a window
No preference
Copy tags to snapshots



Problema: El error indica que necesitas un rol de IAM para habilitar Enhanced Monitoring.
Causa: No has configurado un rol de IAM adecuado para Enhanced Monitoring.
Solución recomendada: Desactiva Enhanced Monitoring para evitar errores relacionados con IAM.



Problema: Este error indica que al intentar crear la instancia de RDS, AWS está solicitando un AWS KMS (Key Management Service) key para habilitar la encriptación de la base de datos , pero no se ha proporcionado una clave válida o no se tiene permisos para acceder a ella.

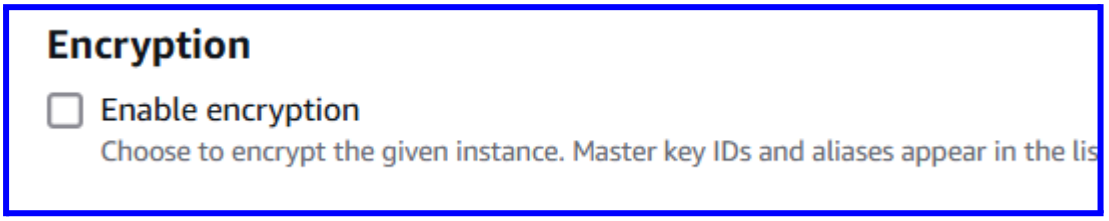
Causa: Encriptación habilitada lo que significa encriptar los datos de la base de datos.
KMS Key requerida: Para habilitar la encriptación, necesitamos proporcionar una clave KMS válida. Esta clave debe:

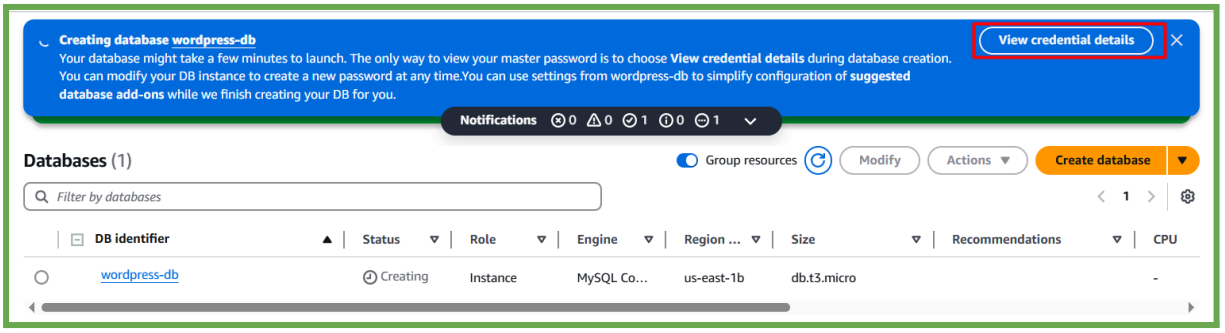
- Existir en tu cuenta de AWS.
- Estar habilitada.
- Ser accesible por el servicio RDS.

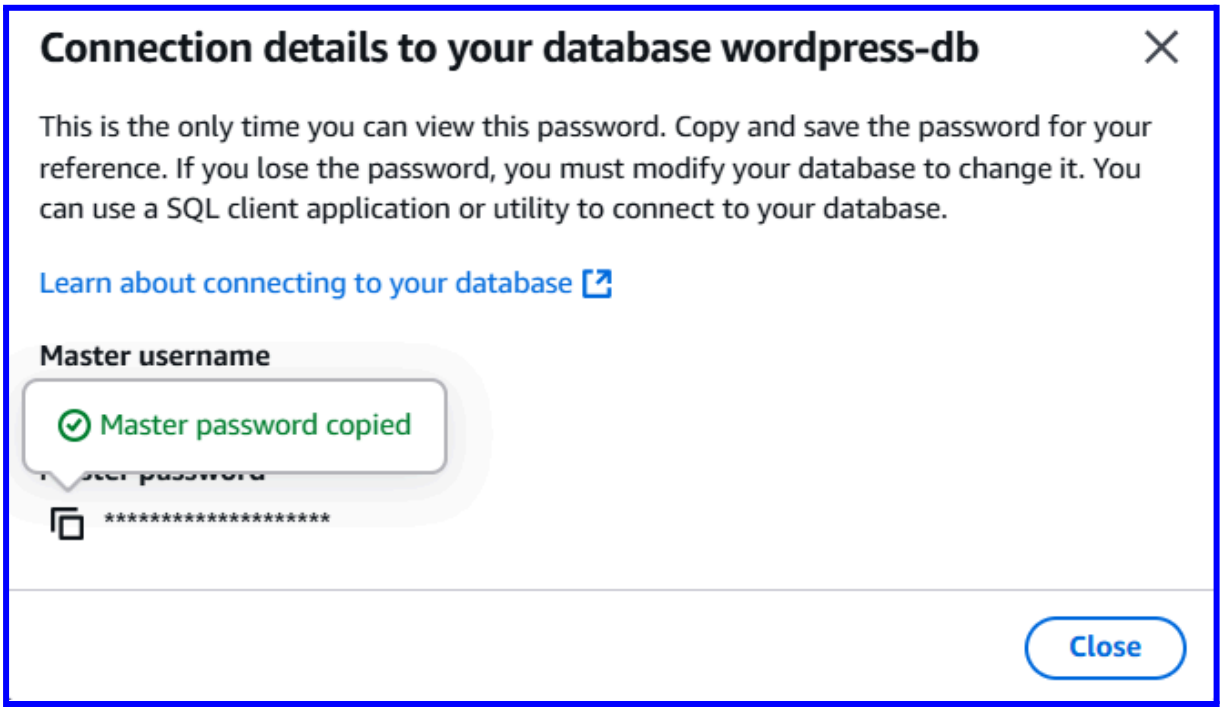
Restricciones de IAM: Dado que tenemos una cuenta de AWS Academy (no se puede crear ni modificar roles o claves KMS), es probable que:

- No hayamos proporcionado una clave KMS válida.
- No tengamos permisos para acceder a las claves KMS disponibles en tu cuenta.

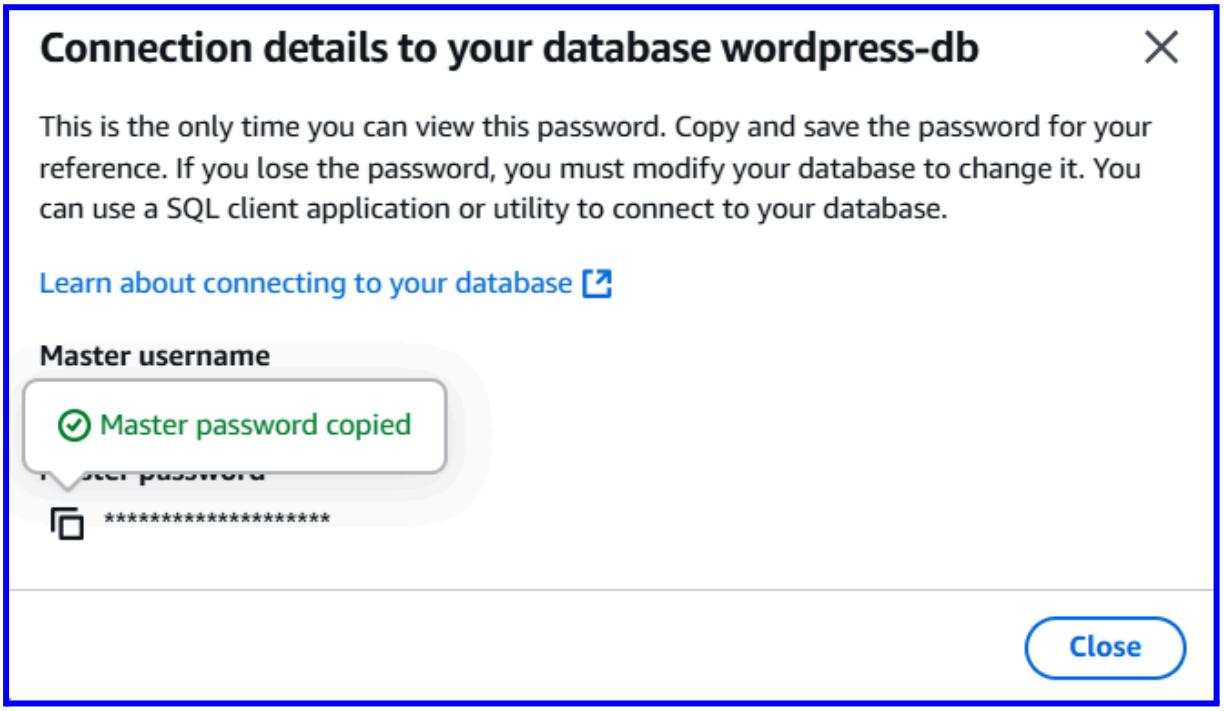
Solución recomendada: Desactivar Enhanced Monitoring para evitar errores relacionados con IAM.
La encriptación de la base de datos es una característica adicional que aumenta la seguridad al cifrar los datos en reposo. Sin embargo, no es estrictamente necesaria para el funcionamiento básico de WordPress.
Si queremos implementar encriptación en el futuro, podremos hacerlo cuando tengamos acceso completo a IAM y KMS.







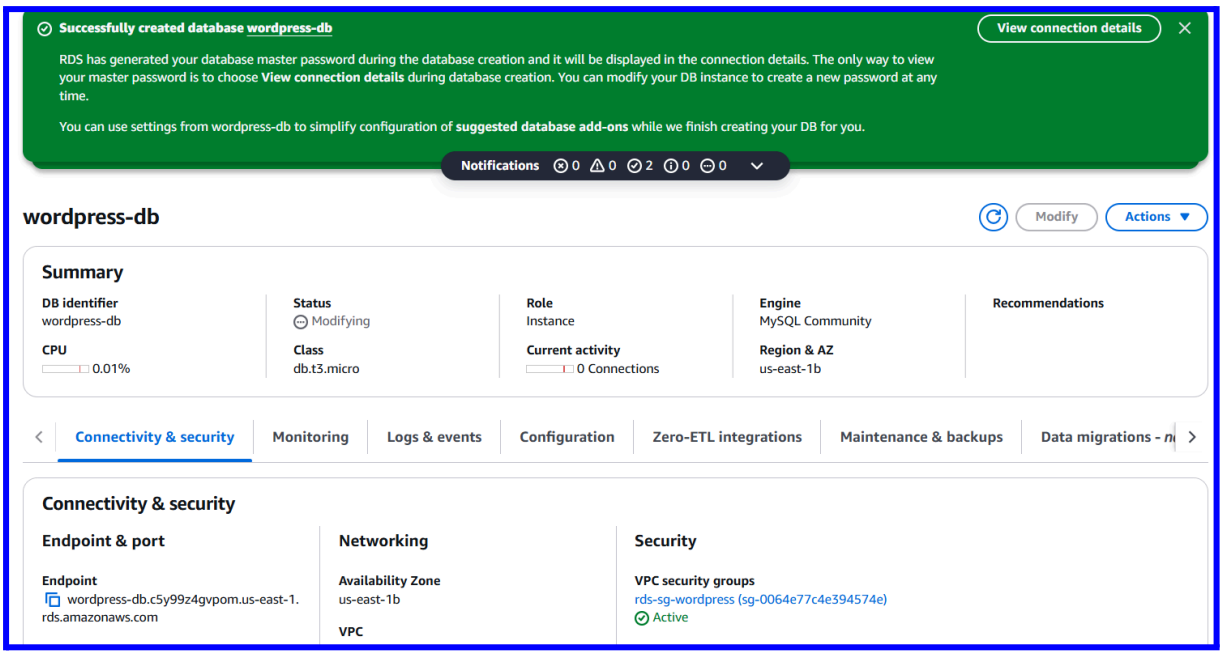
Copy password



RDS PASSWORD

rtPsvolOgO7Ar8KV4oYy

Esperamos unos minutos para que se cree la base de datos:



Copiamos el endpoint:

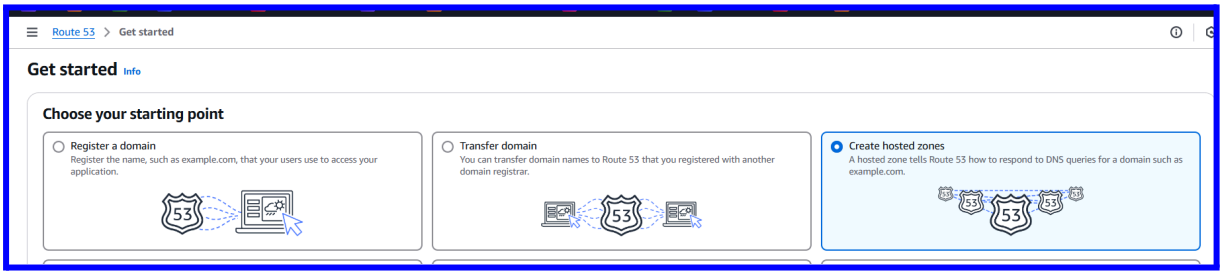
RDS ENDPOINT

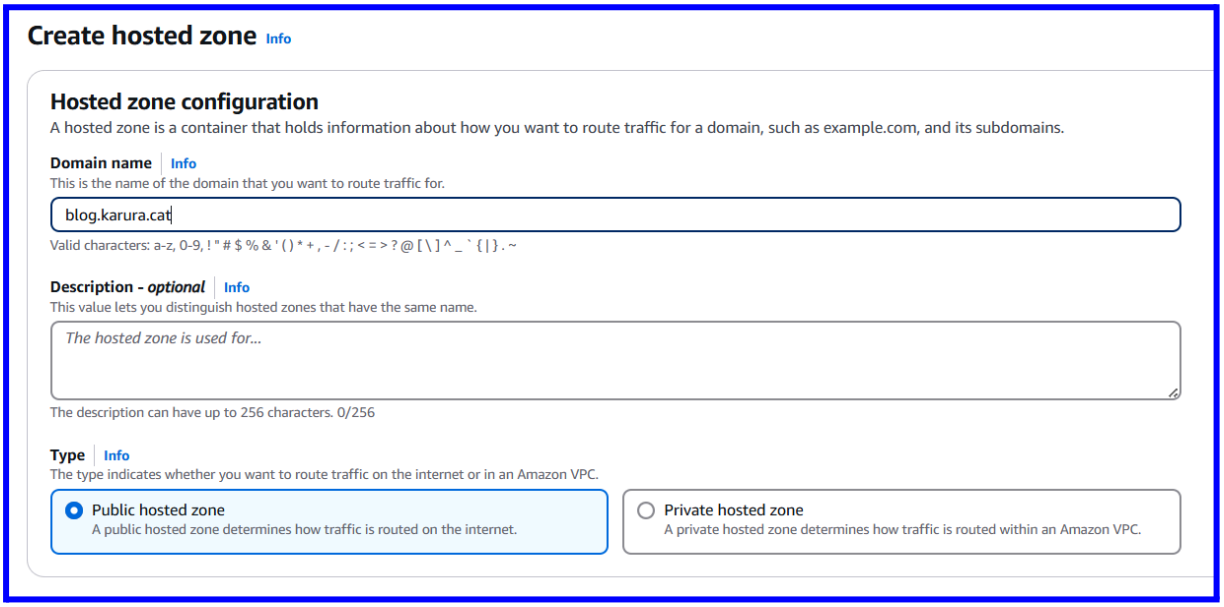
wordpress-db.c5y99z4gvpom.us-east-1.rds.amazonaws.com

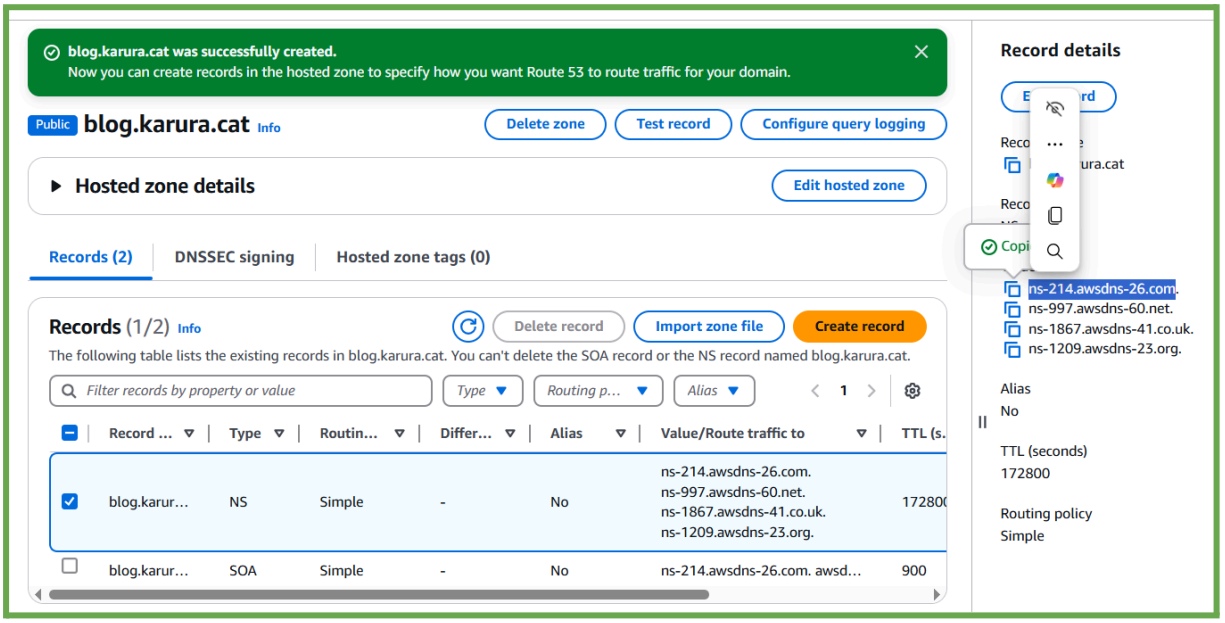
Fase 3: Balanceador de carga

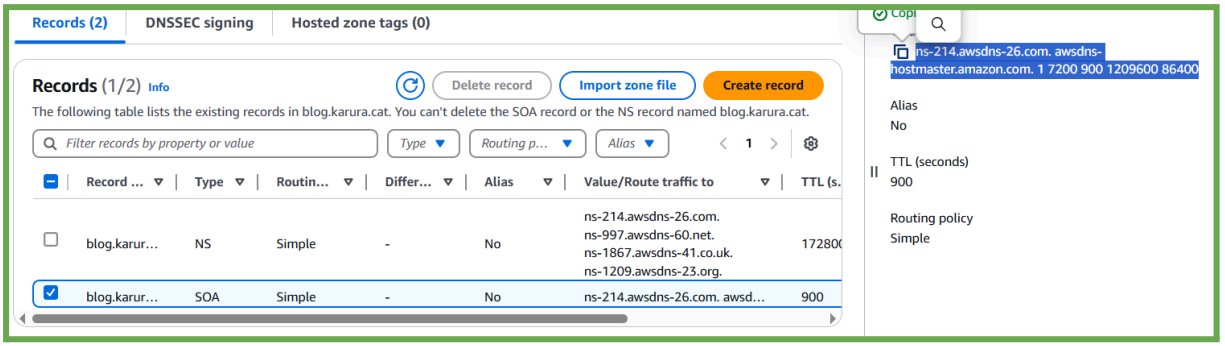
3.1. Crear certificado SSL

CREAR HOSTED ZONE en ROUTE 53





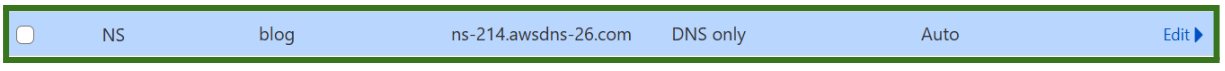




COPY SOA ns-214.awsdns-26.com

ns-214.awsdns-26.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

CLOUDFLARE



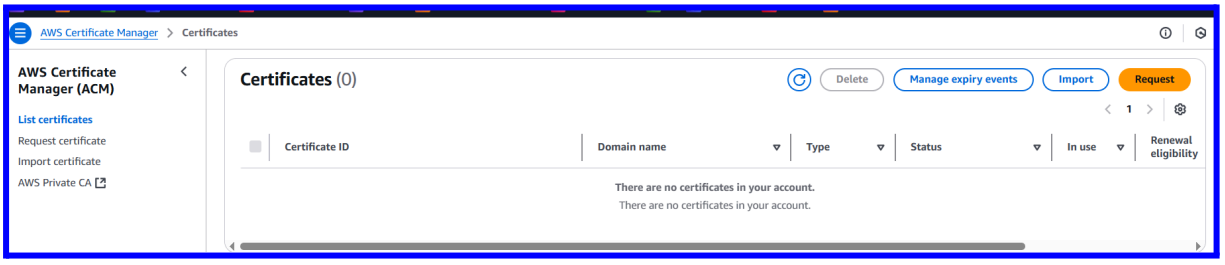
Comprobación:
https://www.diggui.com/


DiG GUI
DiG Web Interface
Dig Command Manual
Record type
NS
Hostname or IP address
blog.karura.cat
Name server
Authoritative
TLD (top-level domain)
Public DNS
8.8.8.8 - Google Public DNS
Specify
More DNS Server...
EDNS Client Subnet (optional)
My IP address
1.2.3.4 or 1.2.3.0/24
Dig options
Tips
Restore Default
tcp Default ON OFF
transport Default IPv4 IPv6
mapped Default ON OFF
nssearch Default ON OFF
trace Default ON OFF
recurse Default ON OFF
edns Default ON OFF
dnssec Default ON OFF
subnet Default ON OFF
cookie Default ON OFF
all Default ON OFF
cmd Default ON OFF
question Default ON OFF
answer Default ON OFF
authority Default ON OFF
additional Default ON OFF
comments Default ON OFF
stats Default ON OFF
multiline Default ON OFF
short Default ON OFF
Output options
Restore Default
Colorize output
Sort alphabetically
Show command
Compare result
DiG Lookup
Reset

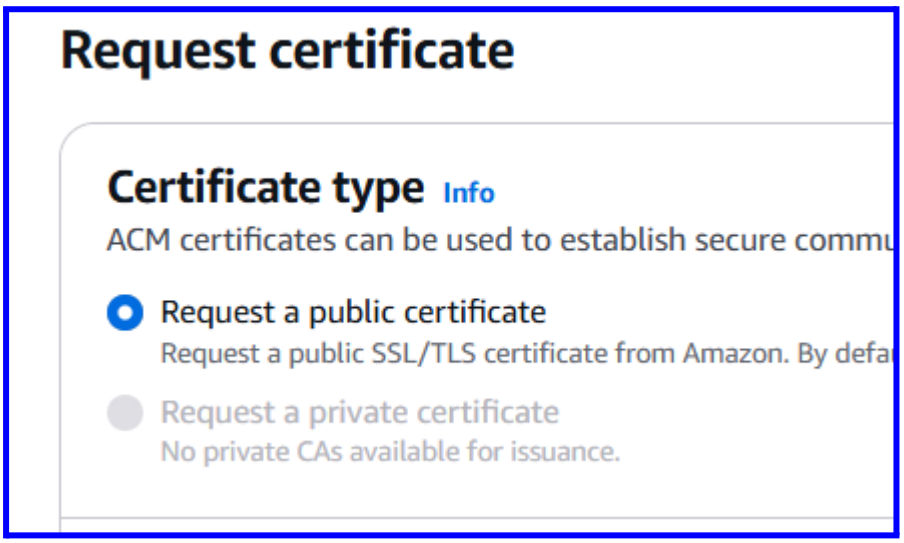
NS:blog.karura.cat@8.8.8.8

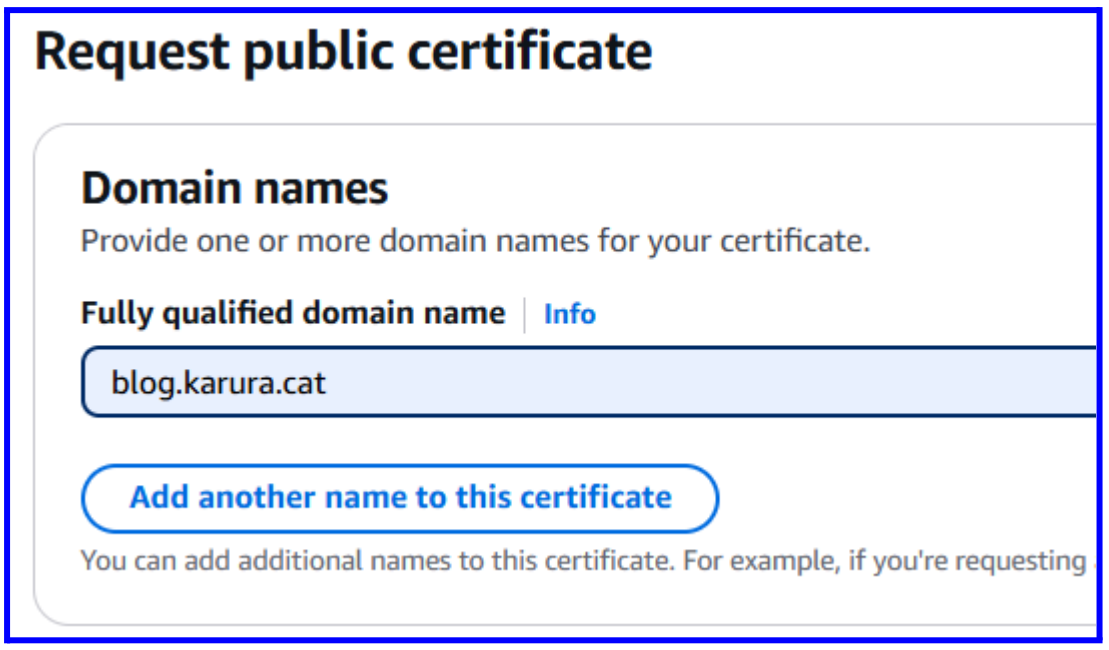
```
; <<>> DiG diggui.com <<>> @8.8.8.8 blog.karura.cat NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 574
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;blog.karura.cat.               IN      NS

;; ANSWER SECTION:
blog.karura.cat.        21410   IN      NS      ns-997.awsdns-60.net.
blog.karura.cat.        21410   IN      NS      ns-214.awsdns-26.com.
blog.karura.cat.        21410   IN      NS      ns-1867.awsdns-41.co.uk.
blog.karura.cat.        21410   IN      NS      ns-1209.awsdns-23.org.

;; Query time: 7 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Apr 27 12:21:53 UTC 2025
;; MSG SIZE  rcvd: 184
```

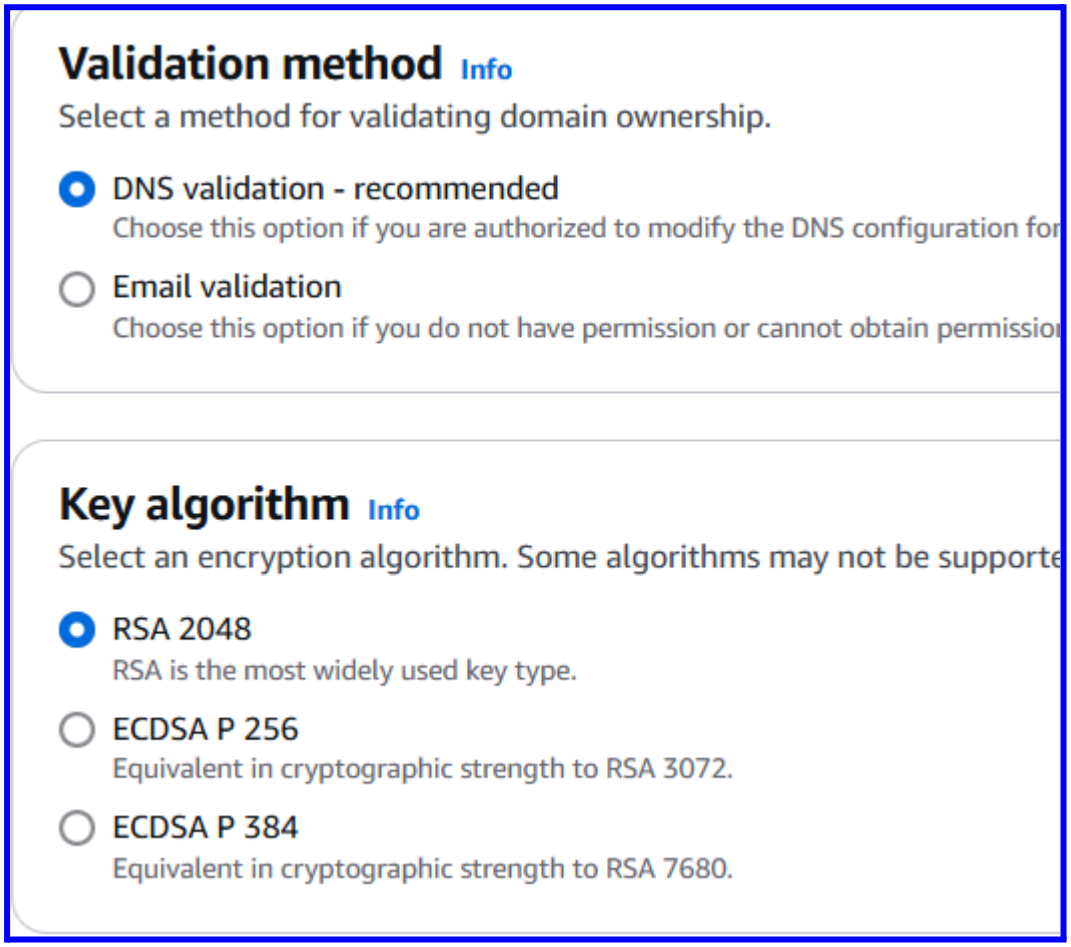
AWS Certificate Manager

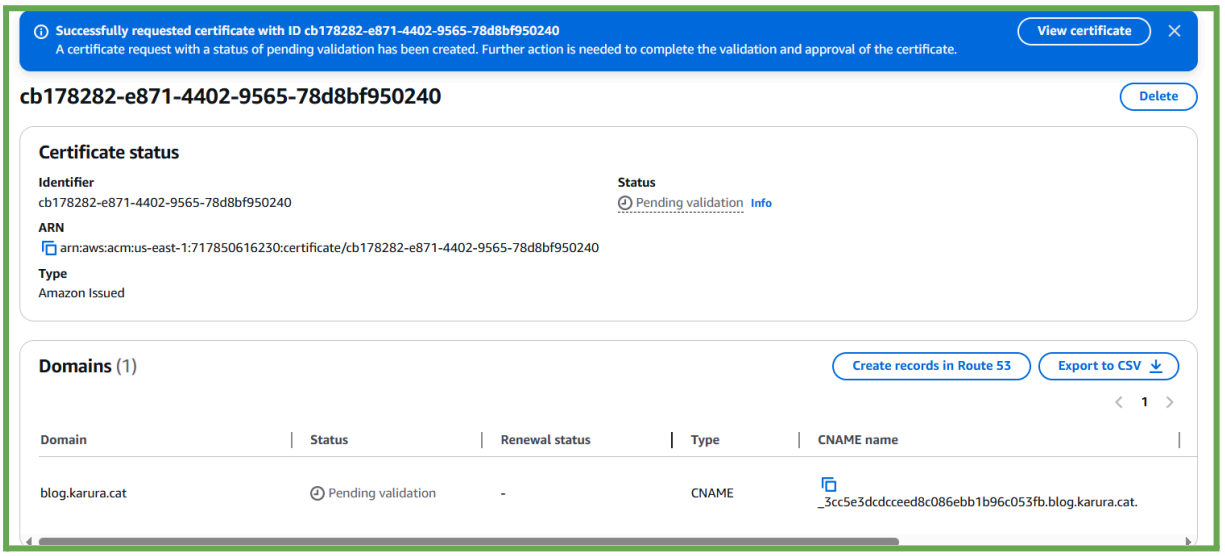


Request

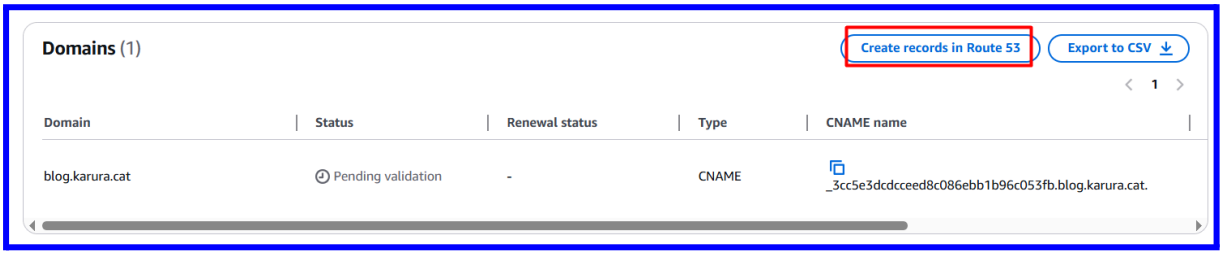

Request certificate
Certificate type Info
ACM certificates can be used to establish secure commu
Request a public certificate
Request a public SSL/TLS certificate from Amazon. By defa
Request a private certificate
No private CAs available for issuance.

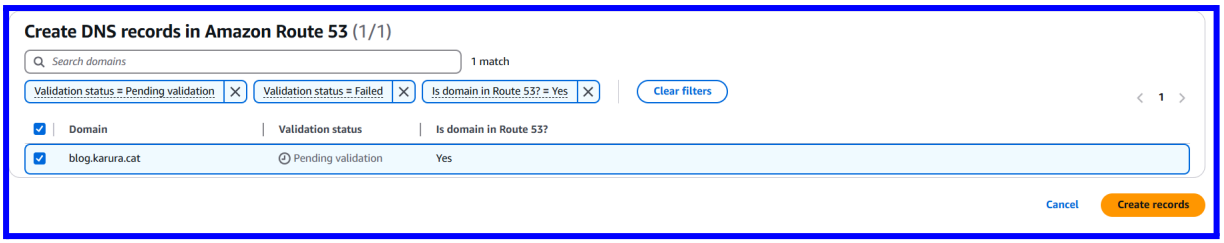

Request public certificate
Domain names
Provide one or more domain names for your certificate.
Fully qualified domain name Info
blog.karura.cat
Add another name to this certificate
You can add additional names to this certificate. For example, if you're requesting

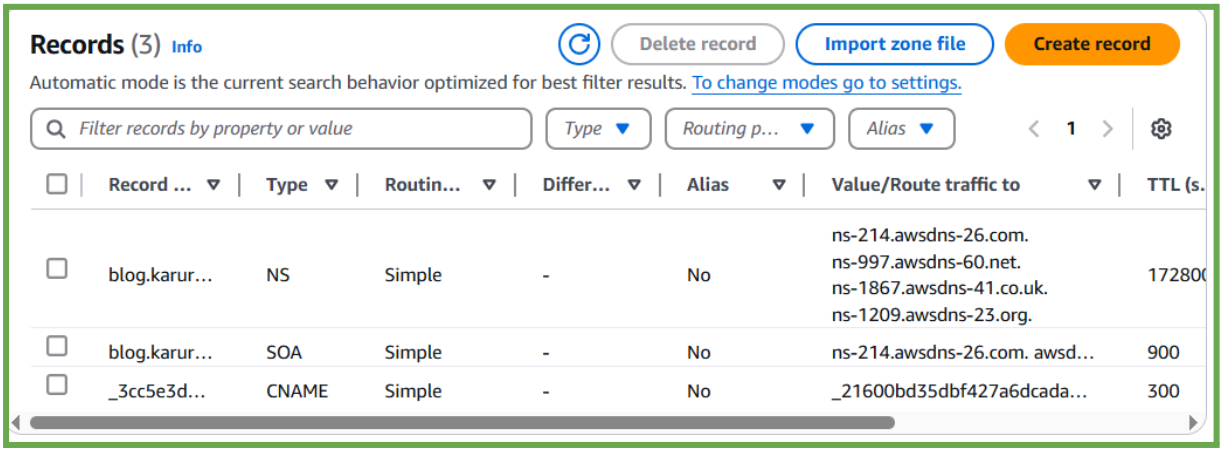




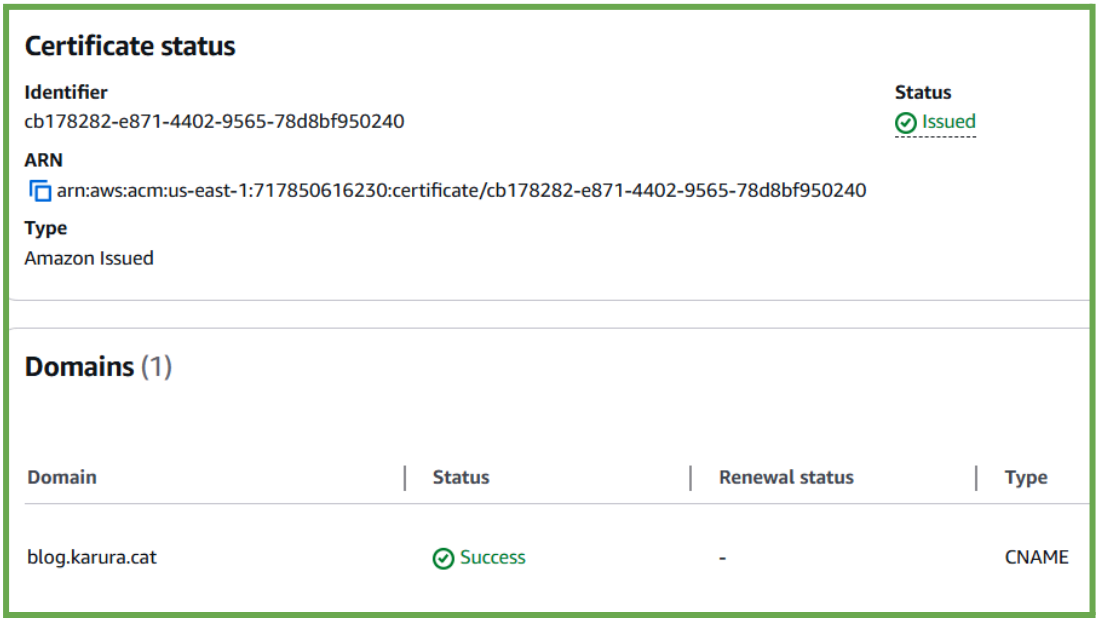
Validar el certificado:



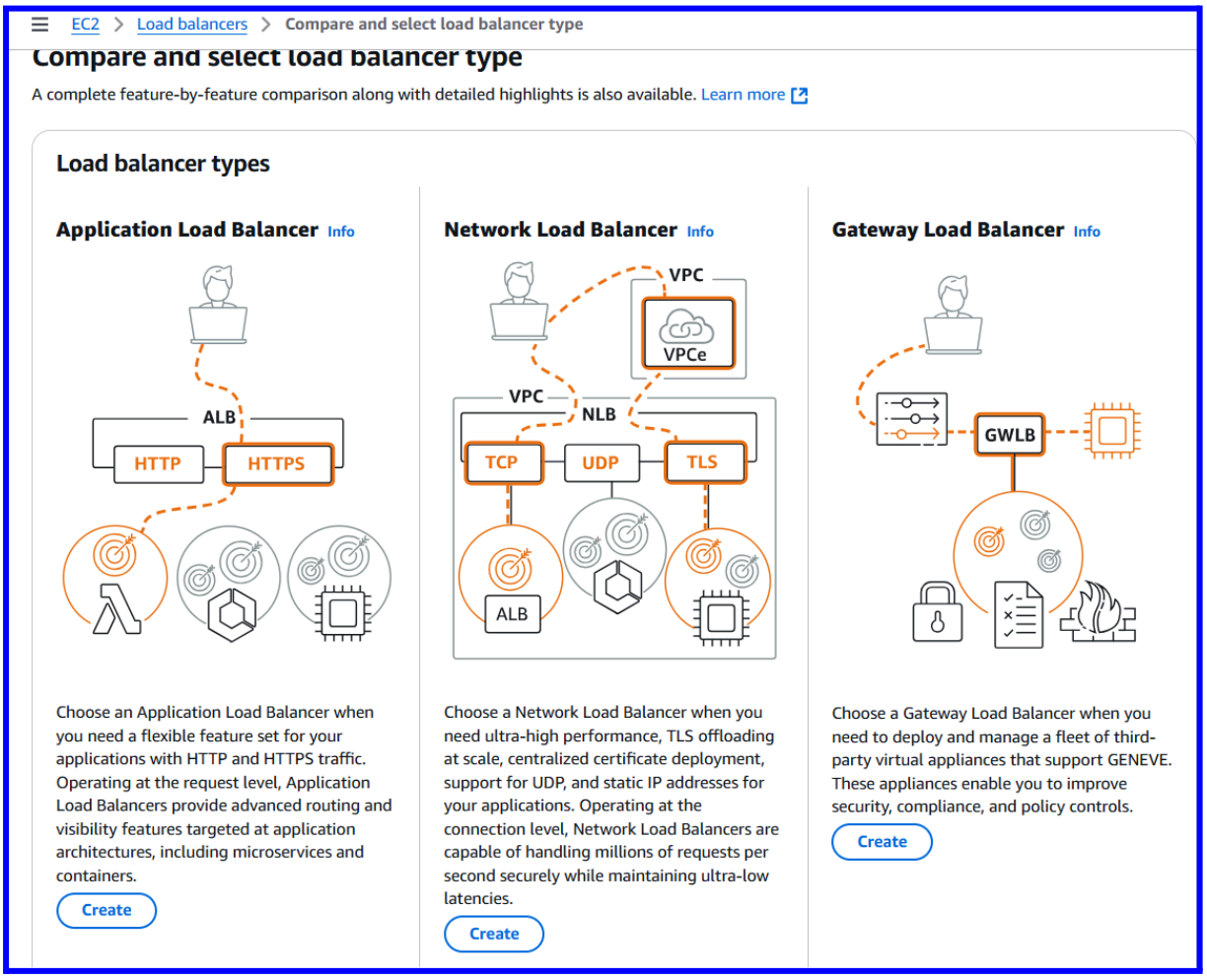


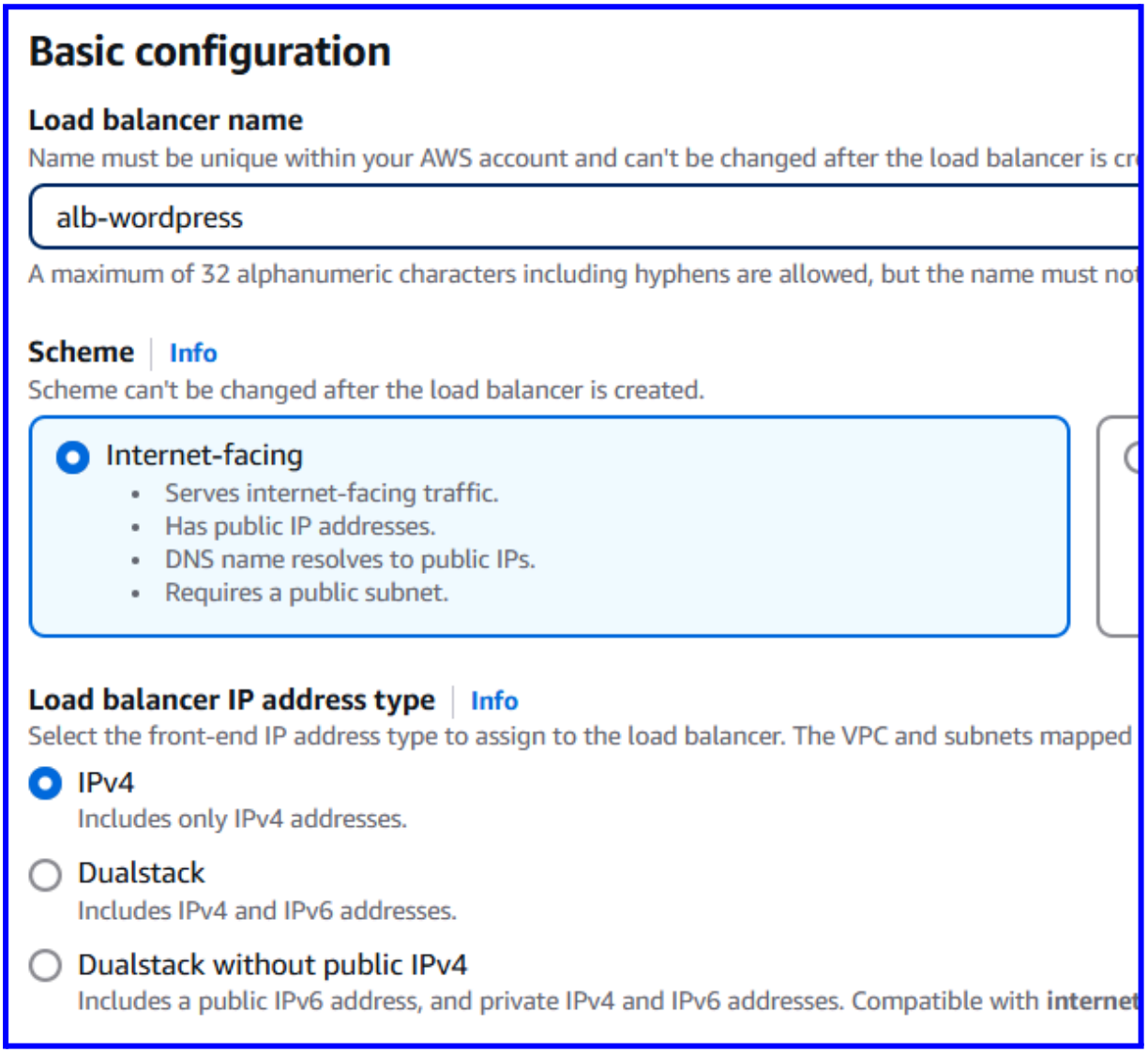


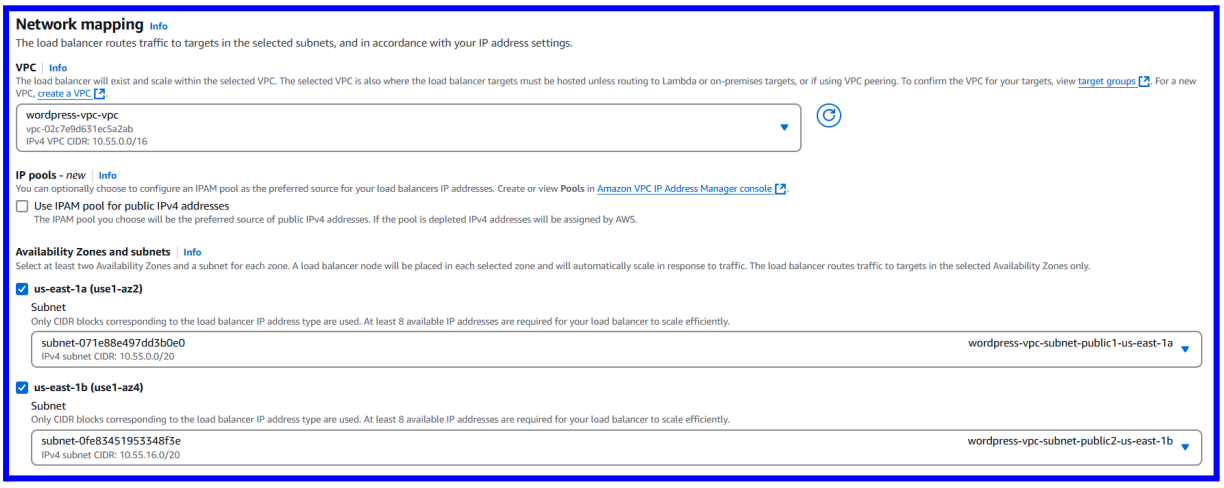
Comprobación:



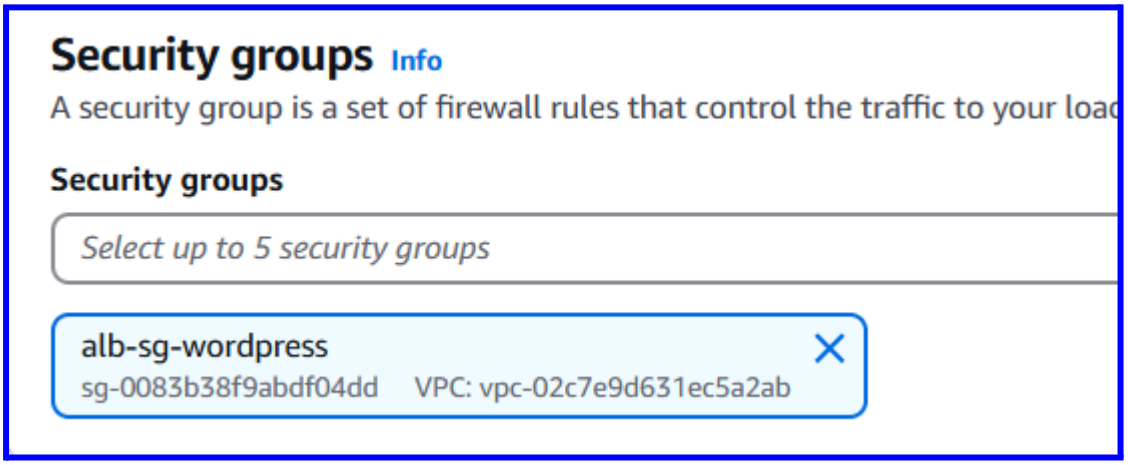
3.2. Crear Application Load Balancer

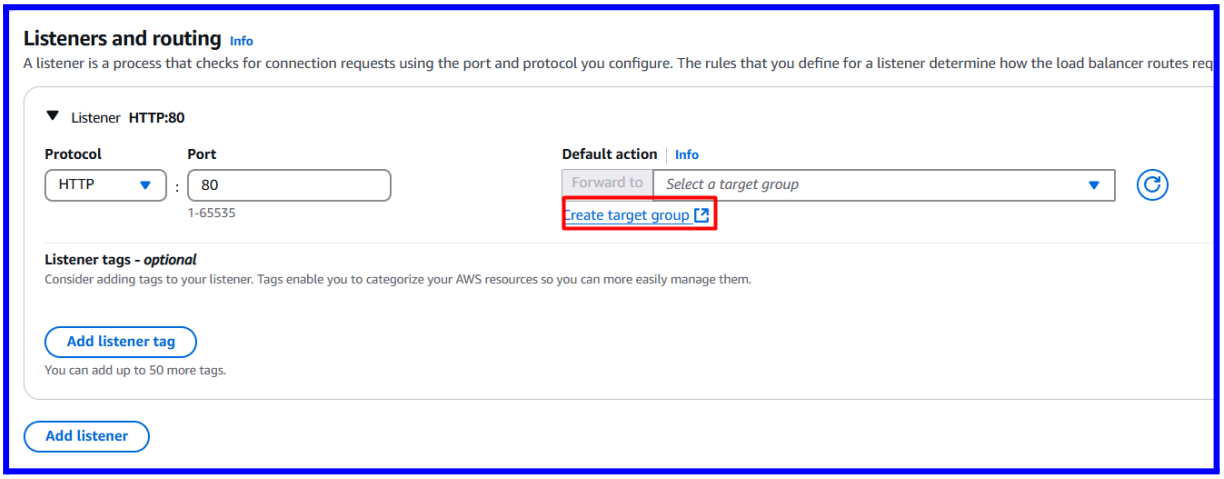



Basic configuration
Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is cr
alb-wordpress
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not
Scheme | Info
Scheme can't be changed after the load balancer is created.
Internet-facing
Serves internet-facing traffic.
Has public IP addresses.
DNS name resolves to public IPs.
Requires a public subnet.
Load balancer IP address type | Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped
IPv4
Includes only IPv4 addresses.
Dualstack
Includes IPv4 and IPv6 addresses.
Dualstack without public IPv4
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with internet

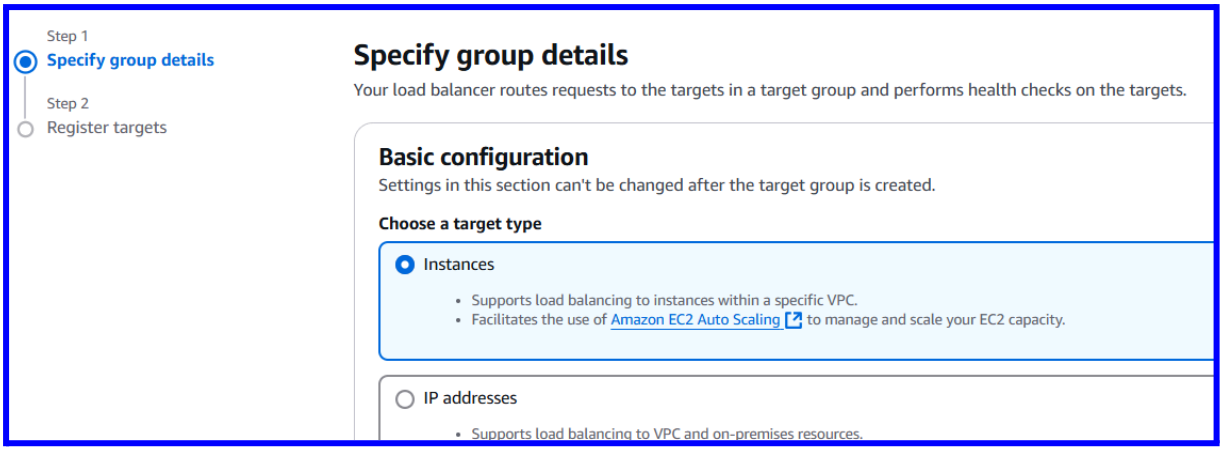

Network mapping Info
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.
VPC | Info
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups. For a new VPC, create a VPC.
wordpress-vpc-vpc
vpc-02c7e9d631ec5a2ab
IPv4 VPC CIDR: 10.55.0.0/16
IP pools - new | Info
You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in Amazon VPC IP Address Manager console.
Use IPAM pool for public IPv4 addresses
The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.
Availability Zones and subnets | Info
Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.
us-east-1a (use1-az2)
Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.
subnet-071e88e497dd3b0e0
IPv4 subnet CIDR: 10.55.0.0/20
wordpress-vpc-subnet-public1-us-east-1a
us-east-1b (use1-az4)
Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.
subnet-0fe83451953348f3e
IPv4 subnet CIDR: 10.55.16.0/20
wordpress-vpc-subnet-public2-us-east-1b

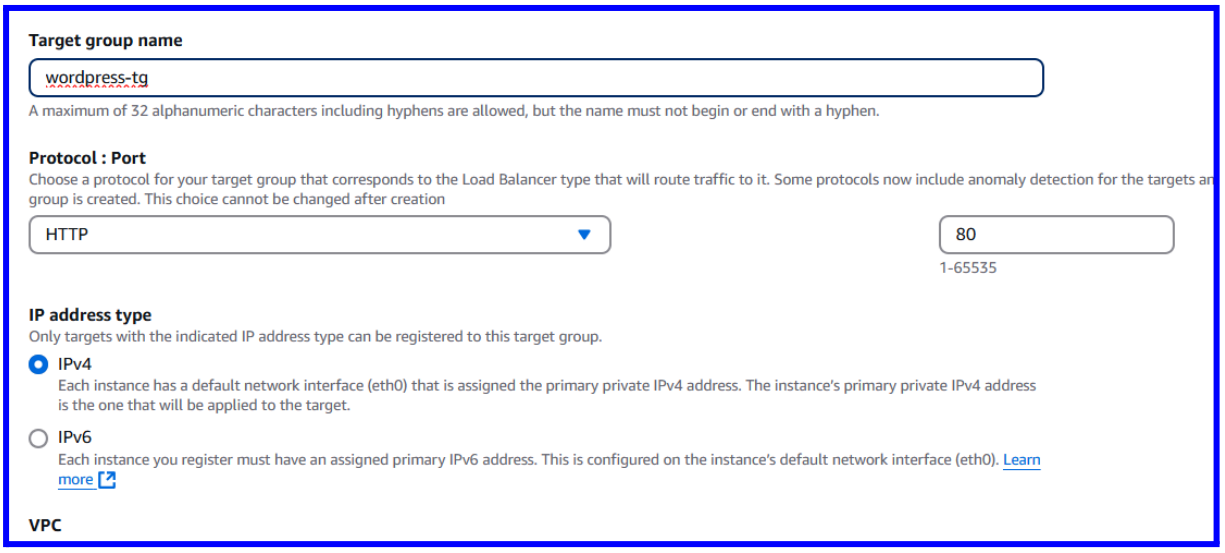
ALB está en las subnet públicas.

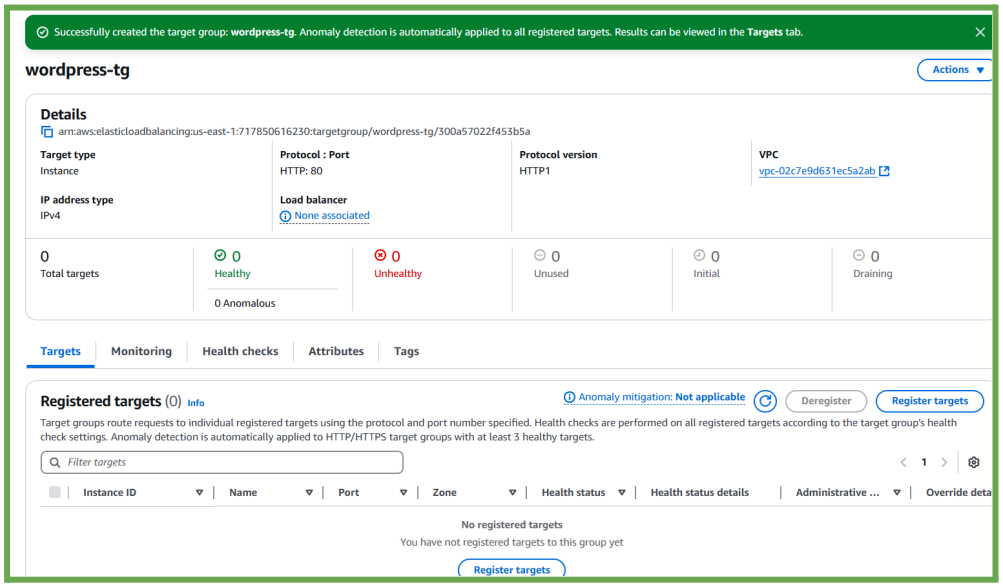




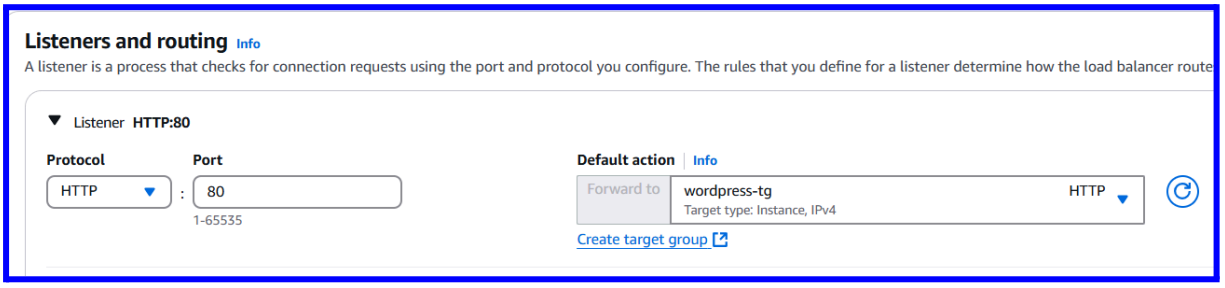
TARGET GROUP

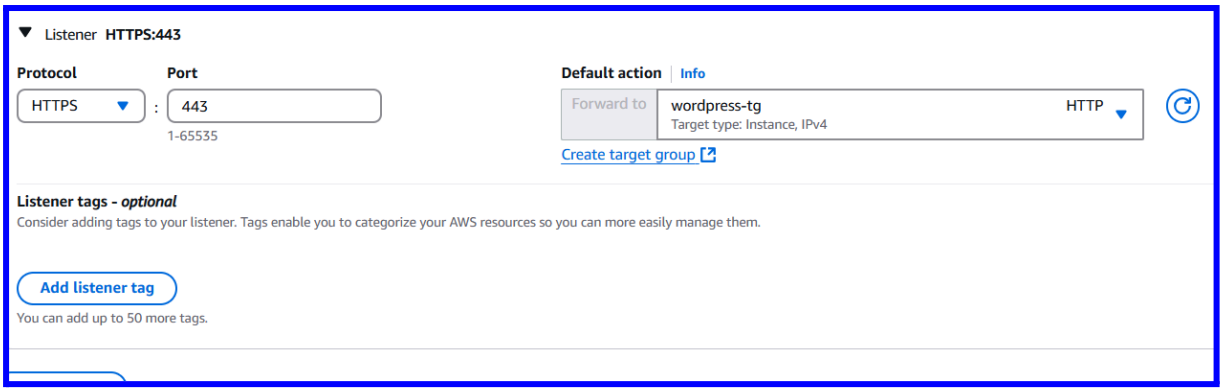


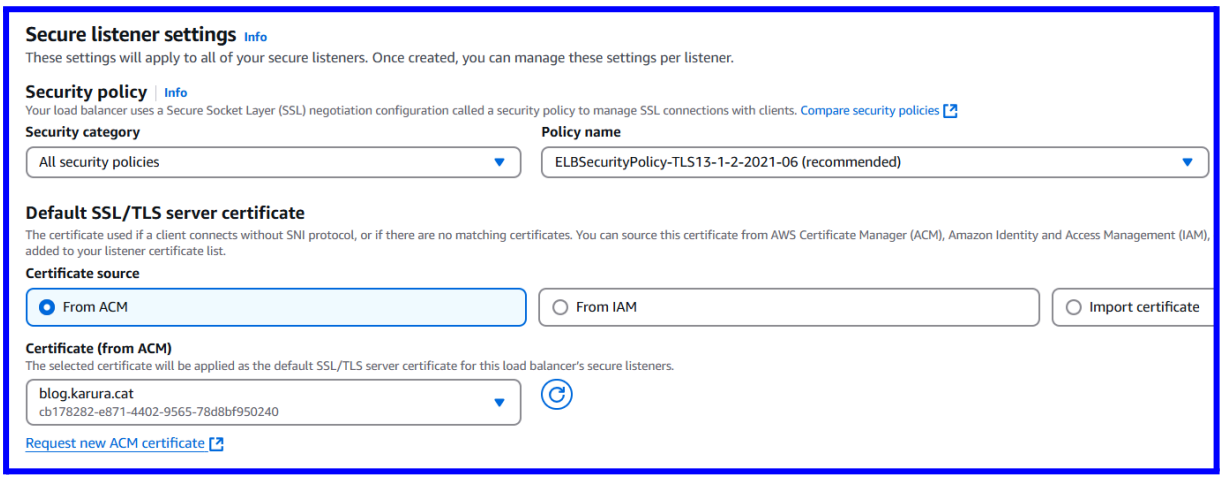


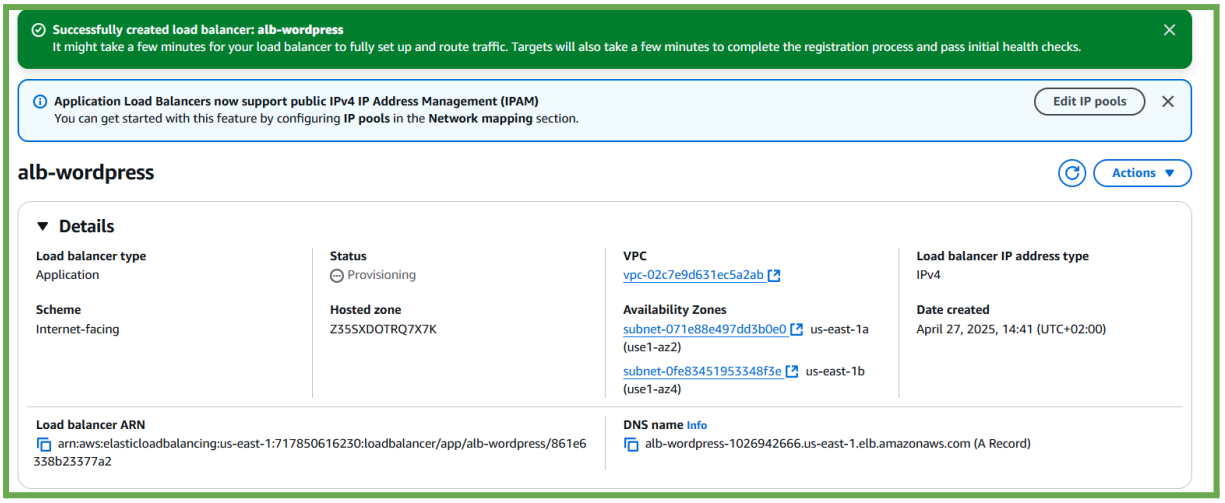


Seguimos con alb



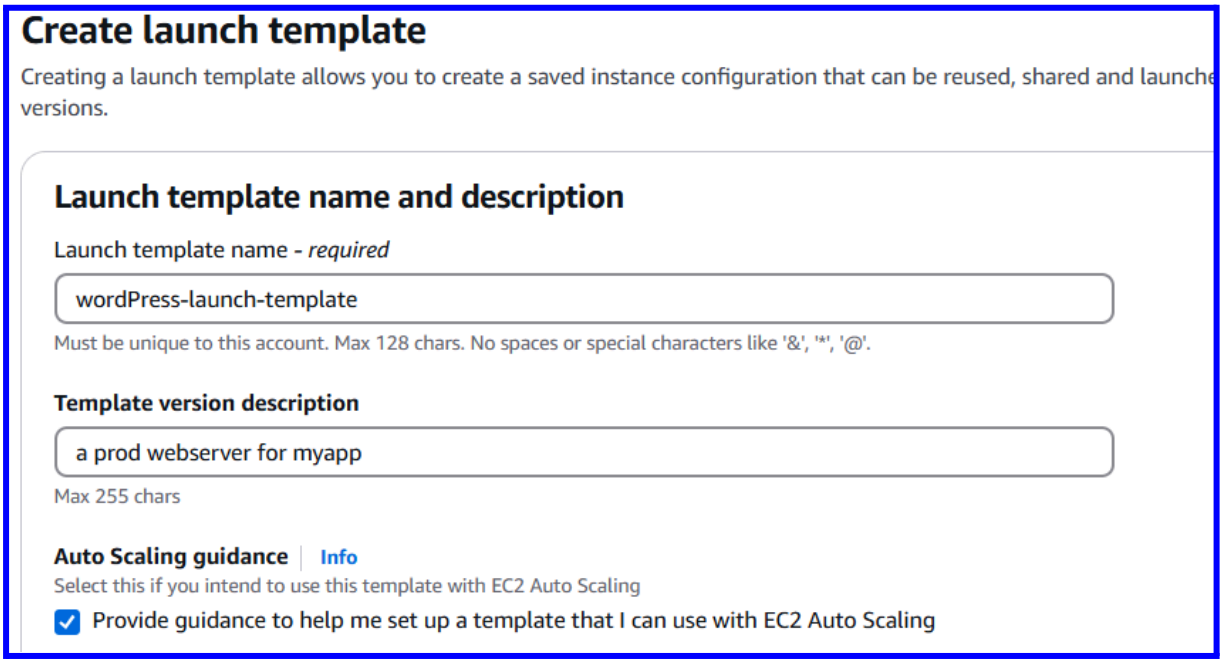


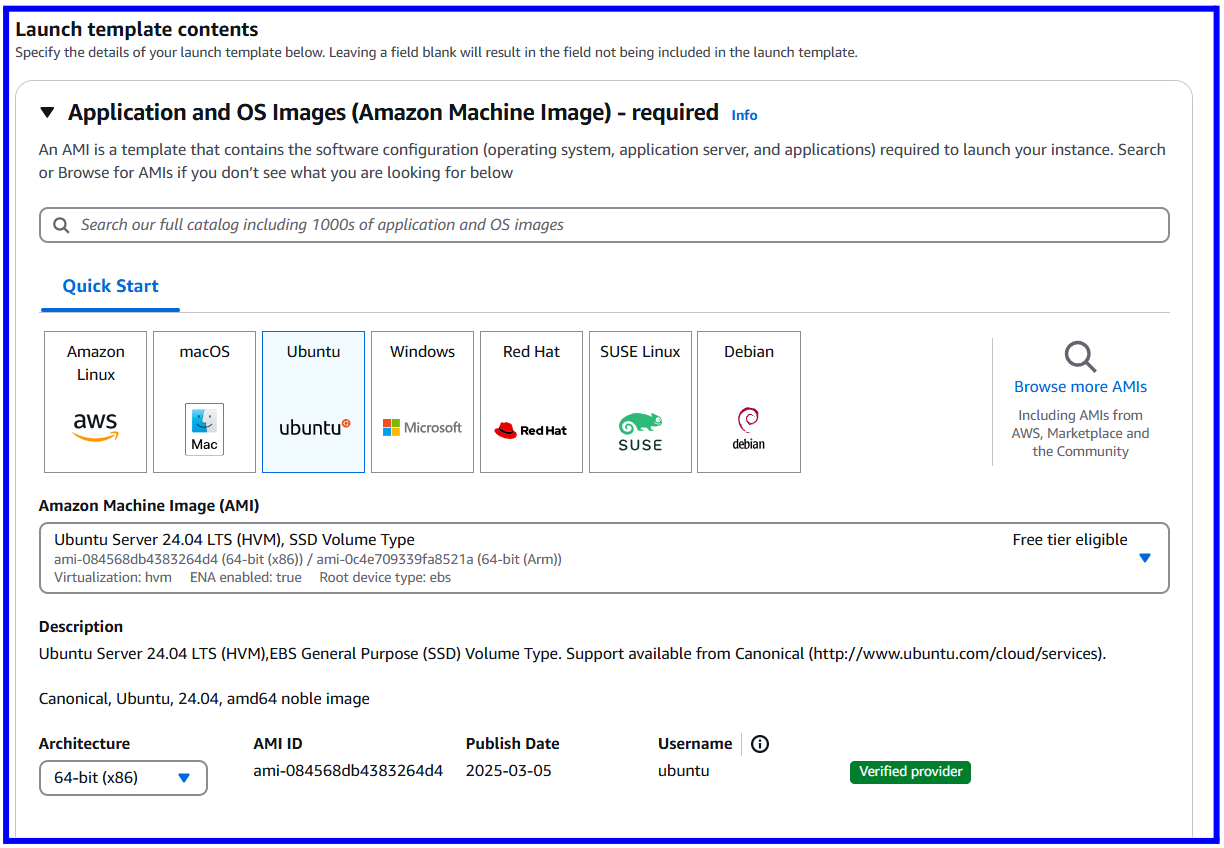

Secure listener settings Info
These settings will apply to all of your secure listeners. Once created, you can manage these settings per listener.
Security policy Info
Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. Compare security policies
Security category
All security policies
Policy name
ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)
Default SSL/TLS server certificate
The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), added to your listener certificate list.
Certificate source
From ACM
From IAM
Import certificate
Certificate (from ACM)
The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.
blog.karura.cat
cb178282-e871-4402-9565-78d8bf950240
Request new ACM certificate

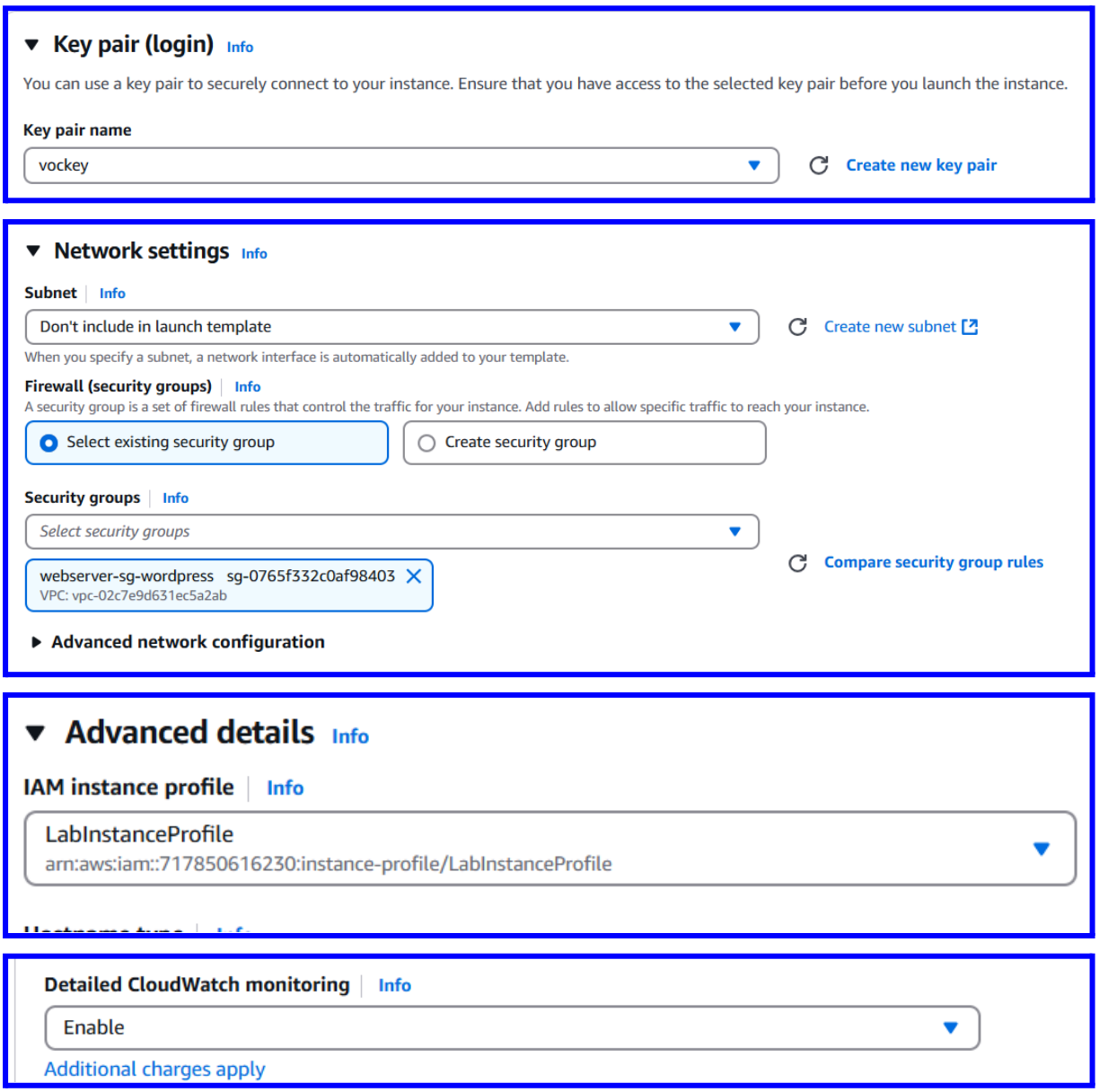

Successfully created load balancer: alb-wordpress
It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.
Application Load Balancers now support public IPv4 IP Address Management (IPAM)
You can get started with this feature by configuring IP pools in the Network mapping section.
Edit IP pools
alb-wordpress
Actions
Details
Load balancer type
Application
Status
Provisioning
VPC
vpc-02c7e9d631ec5a2ab
Load balancer IP address type
IPv4
Scheme
Internet-facing
Hosted zone
Z35SXDOTRQ7X7K
Availability Zones
subnet-071e88e497dd3b0e0 us-east-1a (use1-az2)
subnet-0fe83451953348f3e us-east-1b (use1-az4)
Date created
April 27, 2025, 14:41 (UTC+02:00)
Load balancer ARN
arn:aws:elasticloadbalancing:us-east-1:717850616230:loadbalancer/app/alb-wordpress/861e6338b23377a2
DNS name Info
alb-wordpress-1026942666.us-east-1.elb.amazonaws.com (A Record)

Fase 4: Auto Scaling y WordPress

4.1. Crear plantilla de lanzamiento





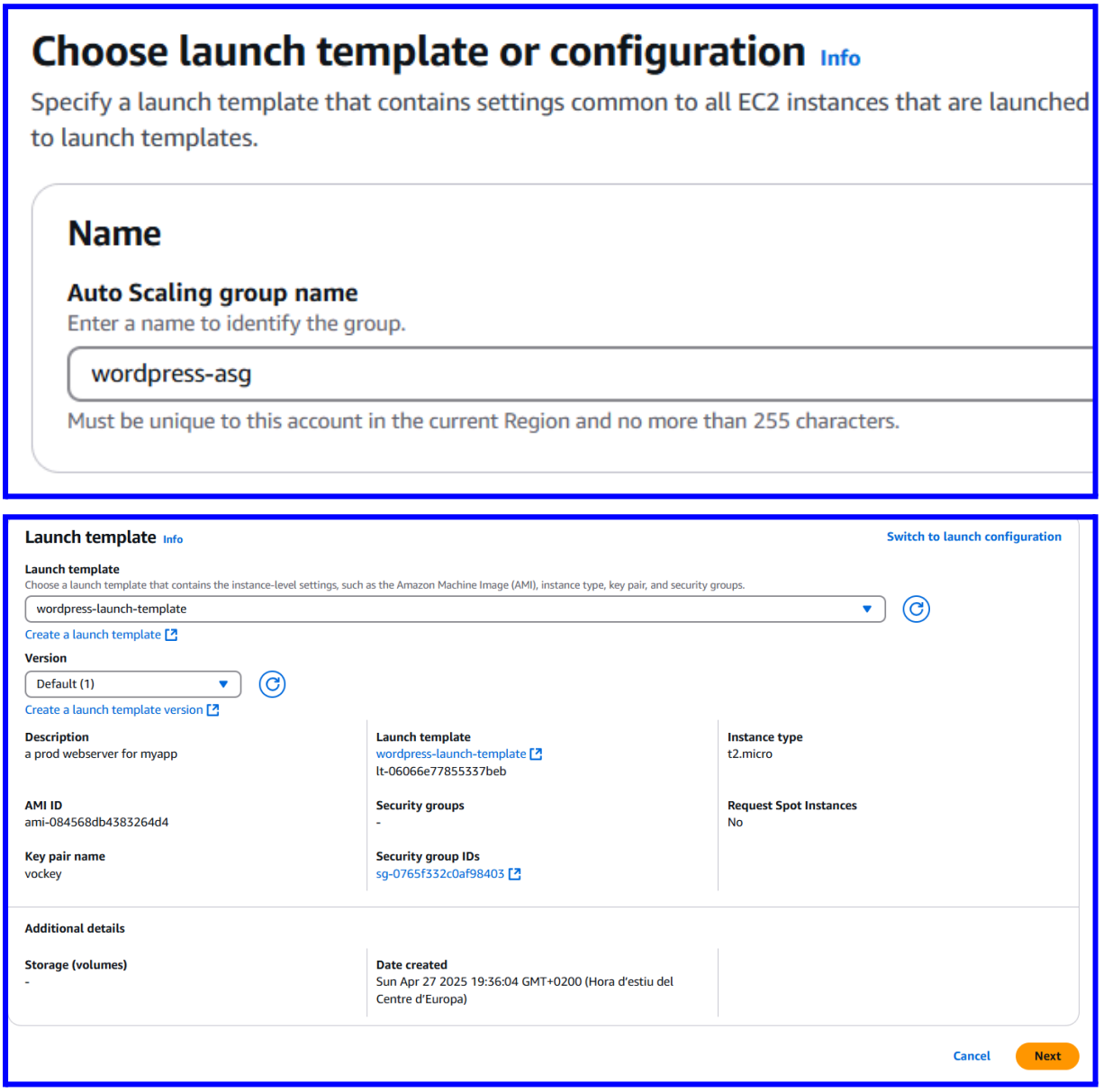



```
#!/bin/bash

# Actualizar el sistema
apt-get update -y
apt-get upgrade -y

# Instalar paquetes necesarios
apt-get install -y apache2 php php-mysql php-gd php-curl php-mbstring php-xml
php-imagick php-zip php-json libapache2-mod-php nfs-common
```

```
# Instalar la CLI de AWS (opcional, solo si necesitas interactuar con otros servicios AWS)
apt-get install -y awscli

# Obtener metadatos de la instancia para el nombre de host
INSTANCE_ID=$(curl -s http://169.254.169.254/latest/meta-data/instance-id)
HOSTNAME="wordpress-$INSTANCE_ID"
hostnamectl set-hostname "$HOSTNAME"

# Crear directorio para EFS
mkdir -p /var/www/html/wp-content

# Montar EFS para contenido compartido
# Asegúrate de reemplazar "fs-XXXXXXXXXXX.efs.us-east-1.amazonaws.com" con tu DNS de EFS real
EFS_DNS="fs-04f7a4e6a26938ff9.efs.us-east-1.amazonaws.com"
mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2 "$EFS_DNS":/ /var/www/html/wp-content

# Añadir entrada en fstab para montaje automático
echo "$EFS_DNS:/ /var/www/html/wp-content nfs4 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,_netdev 0 0" >> /etc/fstab

# Descargar WordPress
cd /tmp
wget https://wordpress.org/latest.tar.gz
tar -xzf latest.tar.gz
cp -a /tmp/wordpress/. /var/www/html/
rm -rf /tmp/wordpress /tmp/latest.tar.gz

# Configurar WordPress
cp /var/www/html/wp-config-sample.php /var/www/html/wp-config.php

# Reemplazar valores en wp-config.php
DB_NAME="wordpress"
DB_USER="admin"
```

```
DB_PASSWORD="rtPsvolOgO7Ar8KV4oYy"
DB_HOST="wordpress-db.c5y99z4gvpom.us-east-1.rds.amazonaws.com"

sed -i "s/database_name_here/$DB_NAME/" /var/www/html/wp-config.php
sed -i "s/username_here/$DB_USER/" /var/www/html/wp-config.php
sed -i "s/password_here/$DB_PASSWORD/" /var/www/html/wp-config.php
sed -i "s/localhost/$DB_HOST/" /var/www/html/wp-config.php

# Generar claves únicas para seguridad
SALT=$(curl -s https://api.wordpress.org/secret-key/1.1/salt/)
STRING='put your unique phrase here'
printf '%s\n' "g/$STRING/d" a "$SALT" . w | ed -s /var/www/html/wp-config.php

# Configurar permisos
chown -R www-data:www-data /var/www/html/
chmod -R 755 /var/www/html/

# Reiniciar Apache
systemctl restart apache2
```

4.2. Crear grupo de Auto Scaling


Choose launch template or configuration Info
Specify a launch template that contains settings common to all EC2 instances that are launched
to launch templates.
Name
Auto Scaling group name
Enter a name to identify the group.
wordpress-asg
Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info
Switch to launch configuration
Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.
wordpress-launch-template
Create a launch template
Version
Default (1)
Create a launch template version
Description
a prod webserver for myapp
Launch template
wordpress-launch-template
lt-06066e77855337beb
Instance type
t2.micro
AMI ID
ami-084568db4383264d4
Security groups
-
Request Spot Instances
No
Key pair name
vockey
Security group IDs
sg-0765f332c0af98403
Additional details
Storage (volumes)
-
Date created
Sun Apr 27 2025 19:36:04 GMT+0200 (Hora d'estiu del Centre d'Europa)
Cancel
Next

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-02c7e9d631ec5a2ab (wordpress-vpc-vpc)
10.55.0.0/16

Create a VPC

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

us-east-1a | subnet-0e172d55c0ef0c97f (wordpress-vpc-subnet-private1-us-east-1a)
10.55.128.0/20

us-east-1b | subnet-04d41282c2e50f188 (wordpress-vpc-subnet-private2-us-east-1b)
10.55.144.0/20

Create a subnet

Availability Zone distribution - *new*
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

- (●) Balanced best effort
  If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.
- ( ) Balanced only
  If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

Cancel | Skip to review | Previous | Next

Integrate with other services - *optional* Info

Use a load balancer to distribute network traffic across multiple servers. Enable service-to-service communications with VPC Lattice. Shift resources away from impaired Availability Zones with zona shift. You can also customize health check replacements and monitoring.

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

- ( ) No load balancer
  Traffic to your Auto Scaling group will not be fronted by a load balancer.
- (●) Attach to an existing load balancer
  Choose from your existing load balancers.
- ( ) Attach to a new load balancer
  Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

- (●) Choose from your load balancer target groups
  This option allows you to attach Application, Network, or Gateway Load Balancers.
- ( ) Choose from Classic Load Balancers

Existing load balancer target groups
Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

wordpress-tg | HTTP
Application Load Balancer: alb-wordpress

VPC Lattice integration options Info

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach

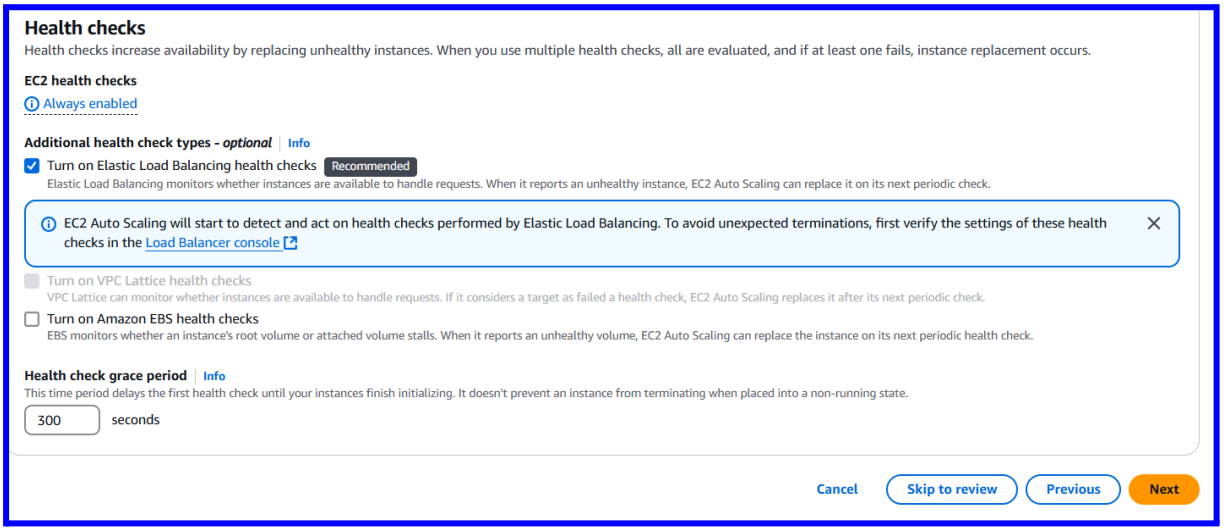
- (●) No VPC Lattice service
  VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.
- ( ) Attach to VPC Lattice service
  Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

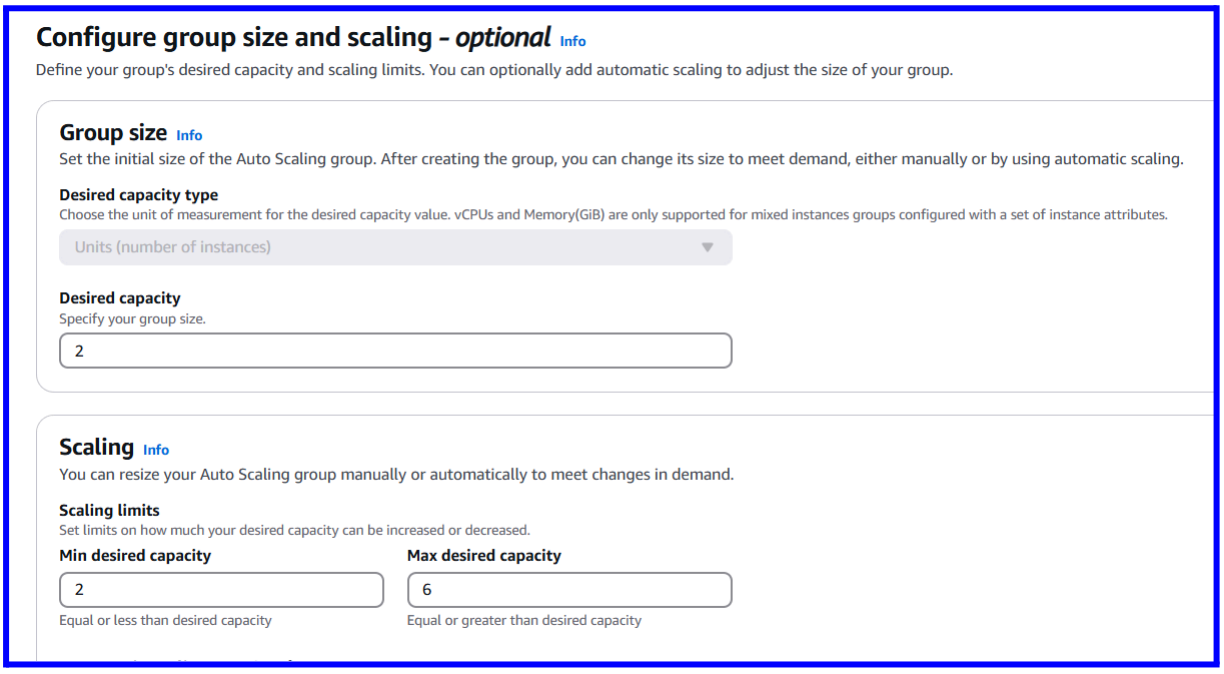
Create new VPC Lattice service

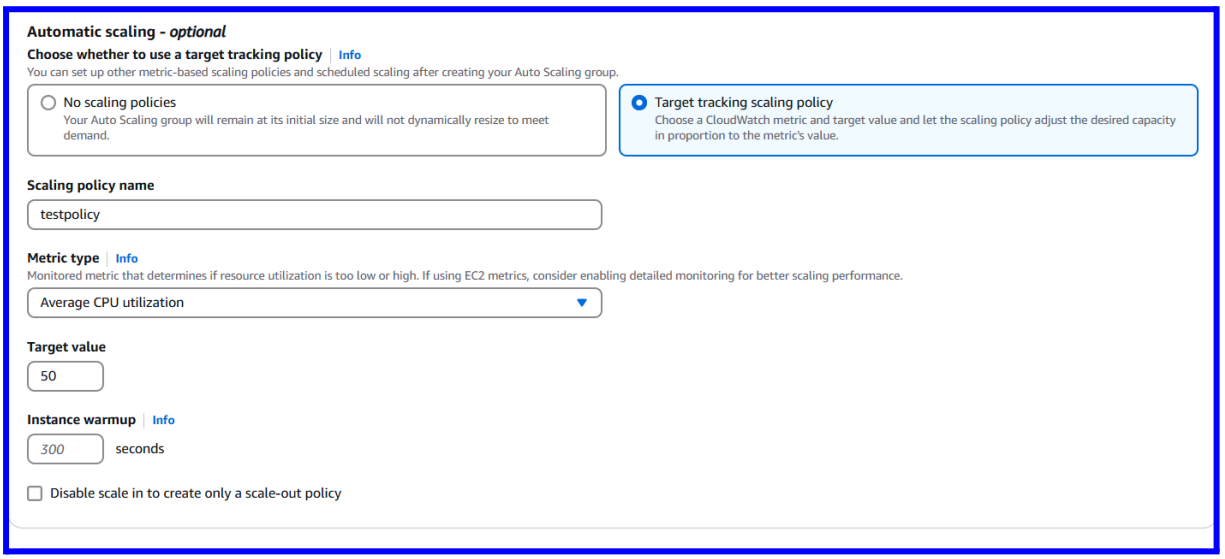
Application Recovery Controller (ARC) zonal shift - *new* Info

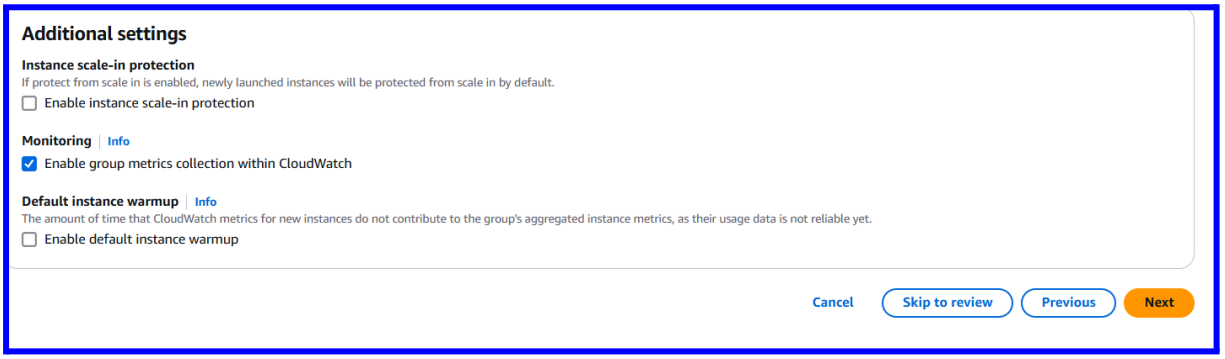
During an Availability Zone impairment, target instance launches towards other healthy Availability Zones.

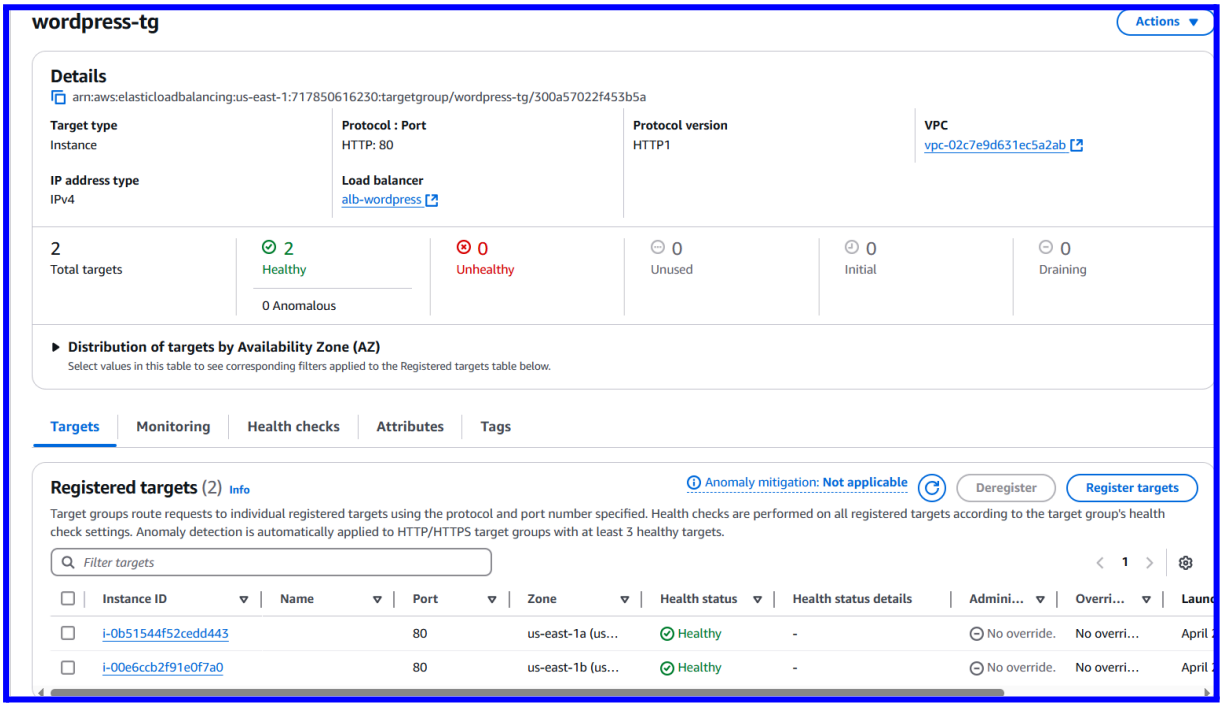
☐ Enable zonal shift
New instance launches will be retargeted towards healthy Availability Zones until the zonal shift is canceled.


Health checks
Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.
EC2 health checks
Always enabled
Additional health check types - optional | Info
Turn on Elastic Load Balancing health checks Recommended
Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.
EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. To avoid unexpected terminations, first verify the settings of these health checks in the Load Balancer console
Turn on VPC Lattice health checks
VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.
Turn on Amazon EBS health checks
EBS monitors whether an instance's root volume or attached volume stalls. When it reports an unhealthy volume, EC2 Auto Scaling can replace the instance on its next periodic health check.
Health check grace period | Info
This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.
300
seconds
Cancel
Skip to review
Previous
Next


Configure group size and scaling - optional Info
Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.
Group size Info
Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.
Desired capacity type
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.
Units (number of instances)
Desired capacity
Specify your group size.
2
Scaling Info
You can resize your Auto Scaling group manually or automatically to meet changes in demand.
Scaling limits
Set limits on how much your desired capacity can be increased or decreased.
Min desired capacity
2
Equal or less than desired capacity
Max desired capacity
6
Equal or greater than desired capacity



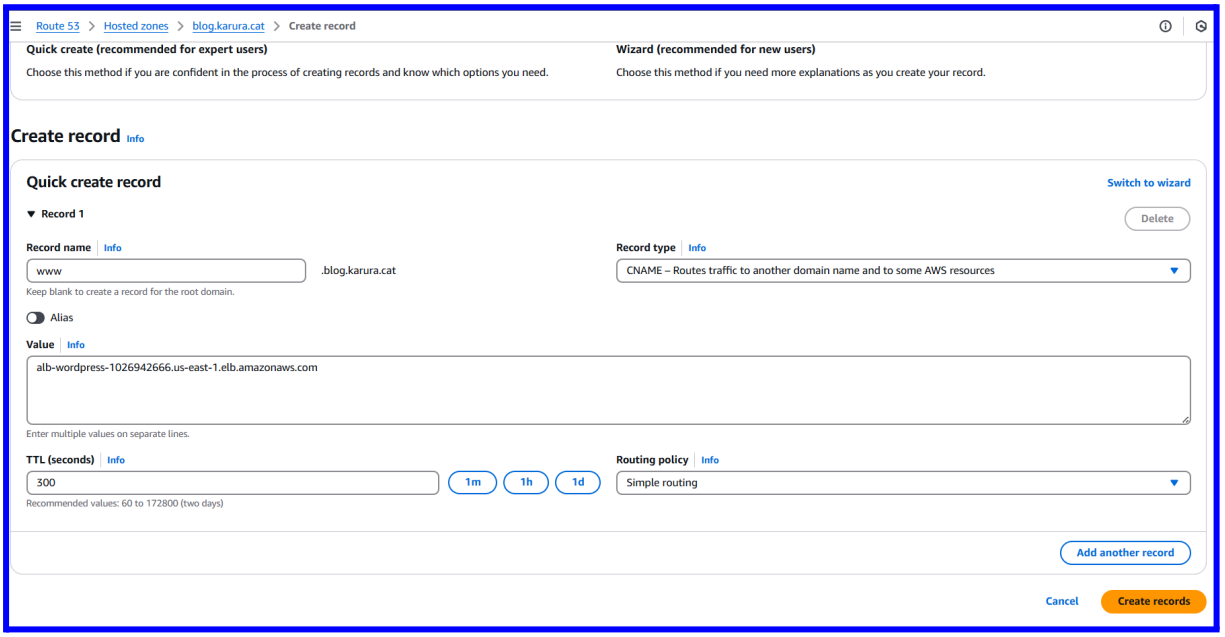


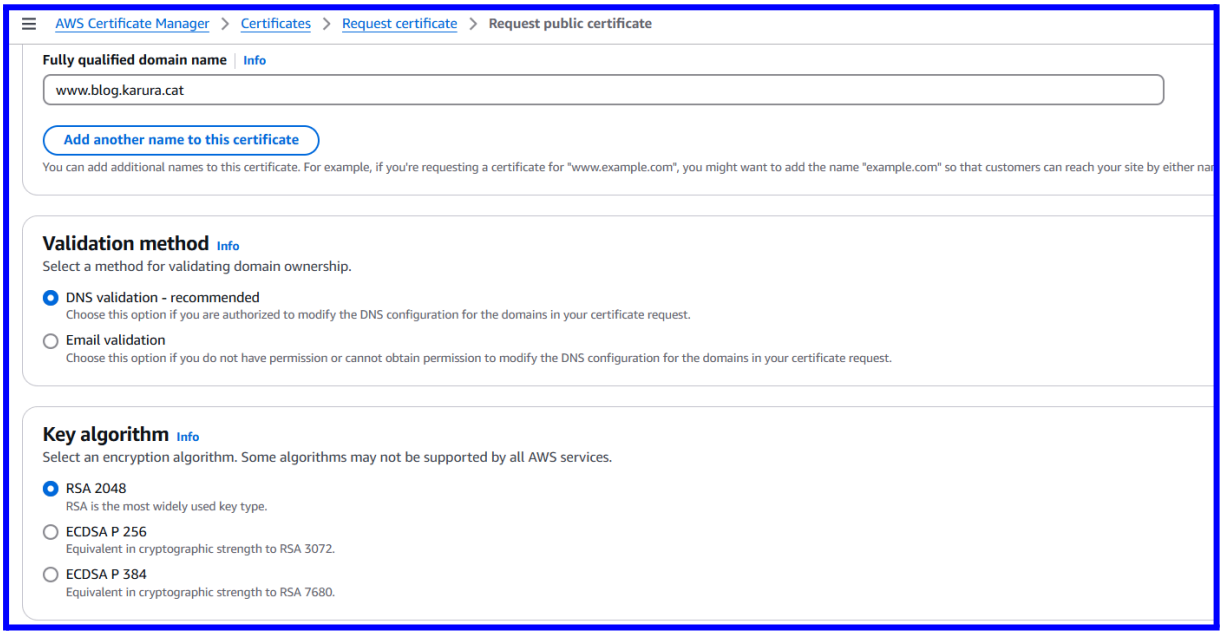


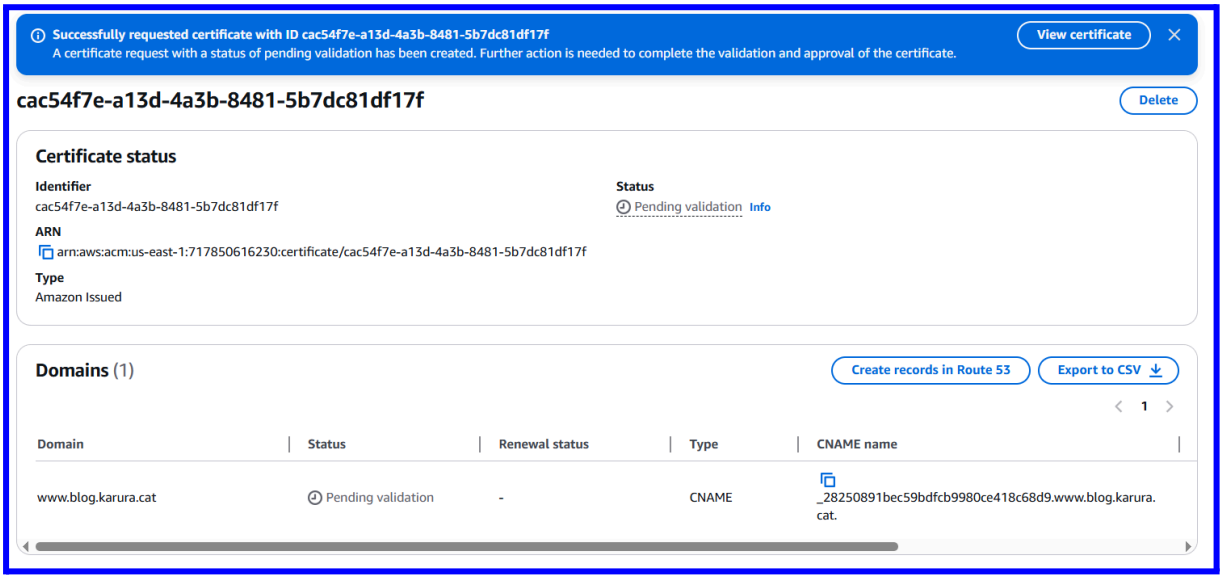
Fase 5: Monitorización y pruebas

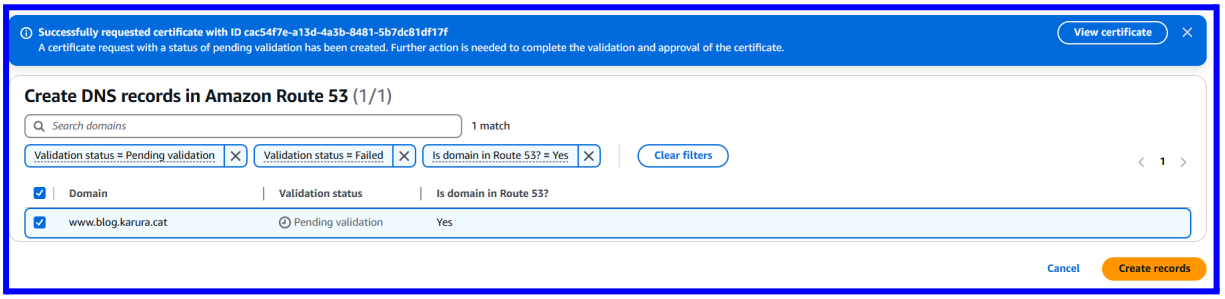
5.1. Configurar CloudWatch

5.3. Configurar Route 53 (para asociar el ALB)


Route 53 > Hosted zones > blog.karura.cat > Create record
Quick create (recommended for expert users)
Choose this method if you are confident in the process of creating records and know which options you need.
Wizard (recommended for new users)
Choose this method if you need more explanations as you create your record.
Create record Info
Quick create record
Switch to wizard
Record 1
Delete
Record name Info
www
.blog.karura.cat
Keep blank to create a record for the root domain.
Record type Info
CNAME – Routes traffic to another domain name and to some AWS resources
Alias
Value Info
alb-wordpress-1026942666.us-east-1.elb.amazonaws.com
Enter multiple values on separate lines.
TTL (seconds) Info
300
1m
1h
1d
Recommended values: 60 to 172800 (two days)
Routing policy Info
Simple routing
Add another record
Cancel
Create records


AWS Certificate Manager > Certificates > Request certificate > Request public certificate
Fully qualified domain name Info
www.blog.karura.cat
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 na
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 cac54f7e-a13d-4a3b-8481-5b7dc81df17f
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
cac54f7e-a13d-4a3b-8481-5b7dc81df17f
Delete
Certificate status
Identifier
cac54f7e-a13d-4a3b-8481-5b7dc81df17f
Status
Pending validation Info
ARN
arn:aws:acm:us-east-1:717850616230:certificate/cac54f7e-a13d-4a3b-8481-5b7dc81df17f
Type
Amazon Issued
Domains (1)
Create records in Route 53
Export to CSV
1
Domain
Status
Renewal status
Type
CNAME name
www.blog.karura.cat
Pending validation
-
CNAME
_28250891bec59bdfcb9980ce418c68d9.www.blog.karura.cat.


Successfully requested certificate with ID cac54f7e-a13d-4a3b-8481-5b7dc81df17f
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
Create DNS records in Amazon Route 53 (1/1)
Search domains
1 match
Validation status = Pending validation
Validation status = Failed
Is domain in Route 53? = Yes
Clear filters
1
Domain
Validation status
Is domain in Route 53?
www.blog.karura.cat
Pending validation
Yes
Cancel
Create records

VERIFICAMOS:

NS:www.blog.karura.cat@8.8.8.8

```
; <<>> DiG diggui.com <<>> @8.8.8.8 www.blog.karura.cat NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49250
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.blog.karura.cat.           IN      NS

;; ANSWER SECTION:
www.blog.karura.cat.    286     IN      CNAME   alb-wordpress-1026942666.us-east-1.elb.amazonaws.com.

;; AUTHORITY SECTION:
us-east-1.elb.amazonaws.com. 46 IN      SOA     ns-1119.awsdns-11.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 60

;; Query time: 6 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Apr 27 18:26:56 UTC 2025
;; MSG SIZE  rcvd: 196
```

cac54f7e-a13d-4a3b-8481-5b7dc81df17f — Delete

Certificate status

Identifier	**Status**
cac54f7e-a13d-4a3b-8481-5b7dc81df17f	Issued

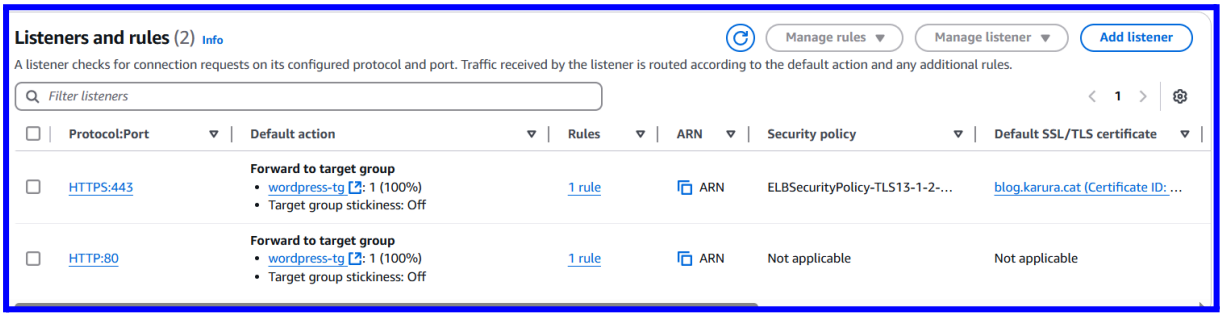
ARN
arn:aws:acm:us-east-1:717850616230:certificate/cac54f7e-a13d-4a3b-8481-5b7dc81df17f

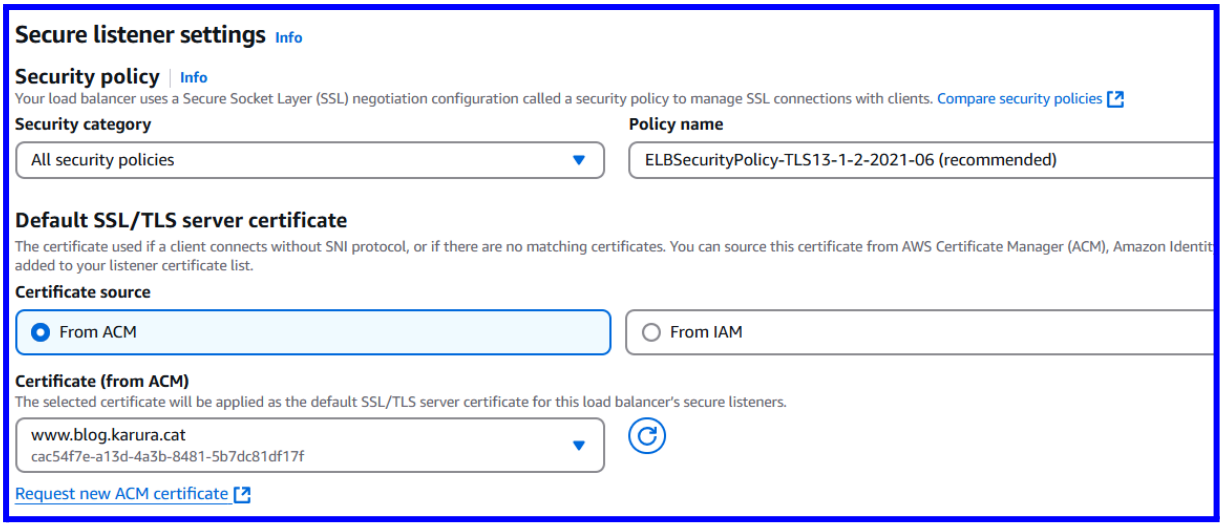
Type
Amazon Issued

Domains (1) — Create records in Route 53 | Export to CSV

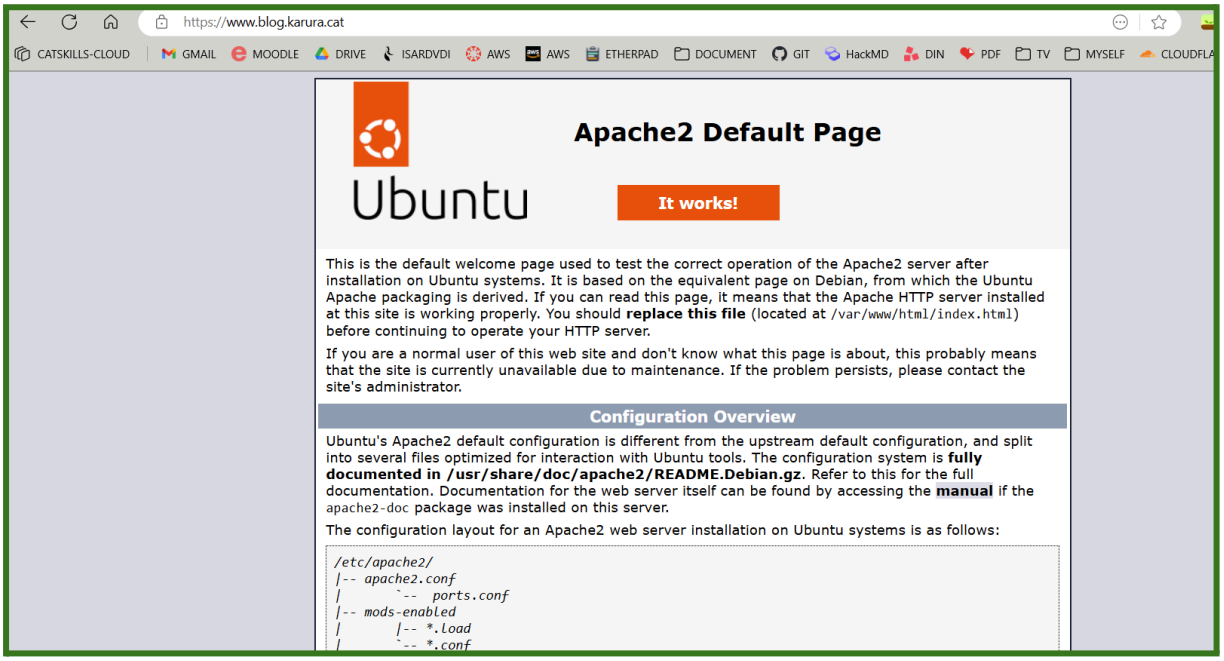
Domain	Status	Renewal status	Type	CNAME name
www.blog.karura.cat	Success	-	CNAME	_28250891bec59bdfcb9980ce418c68d9.www.blog.karura.cat.

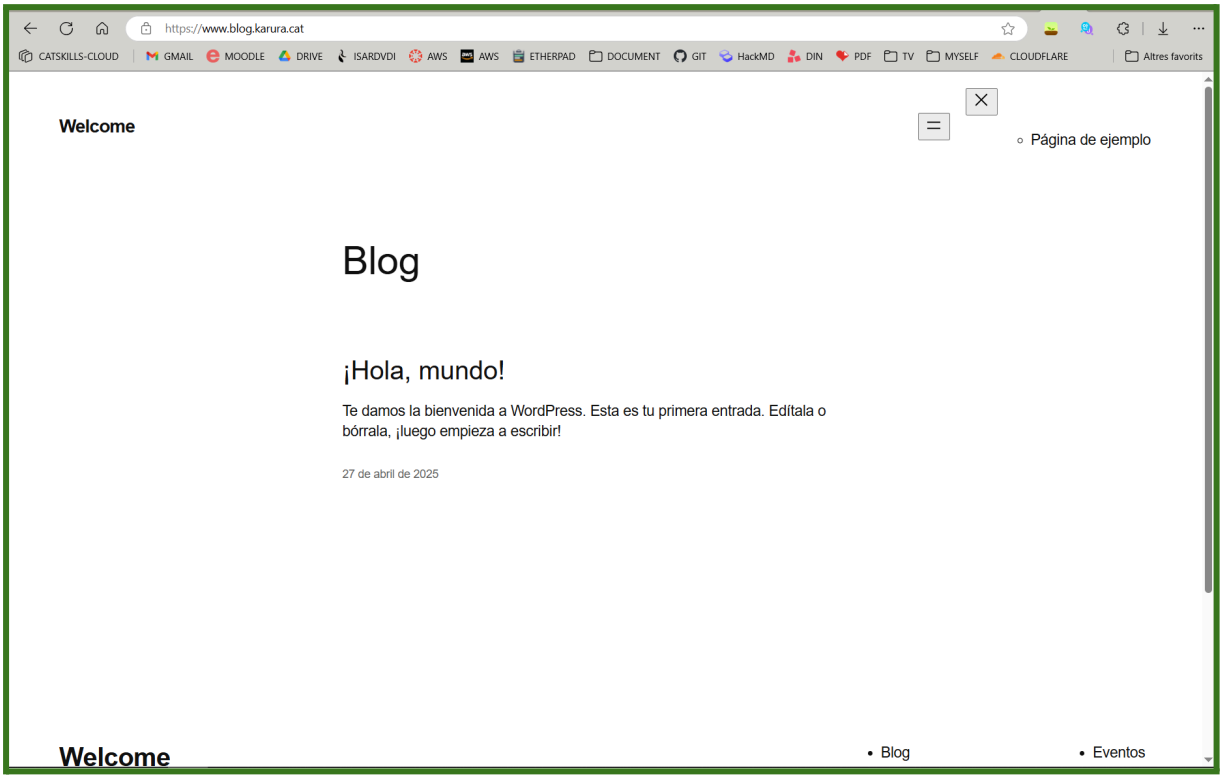
EDITAMOS

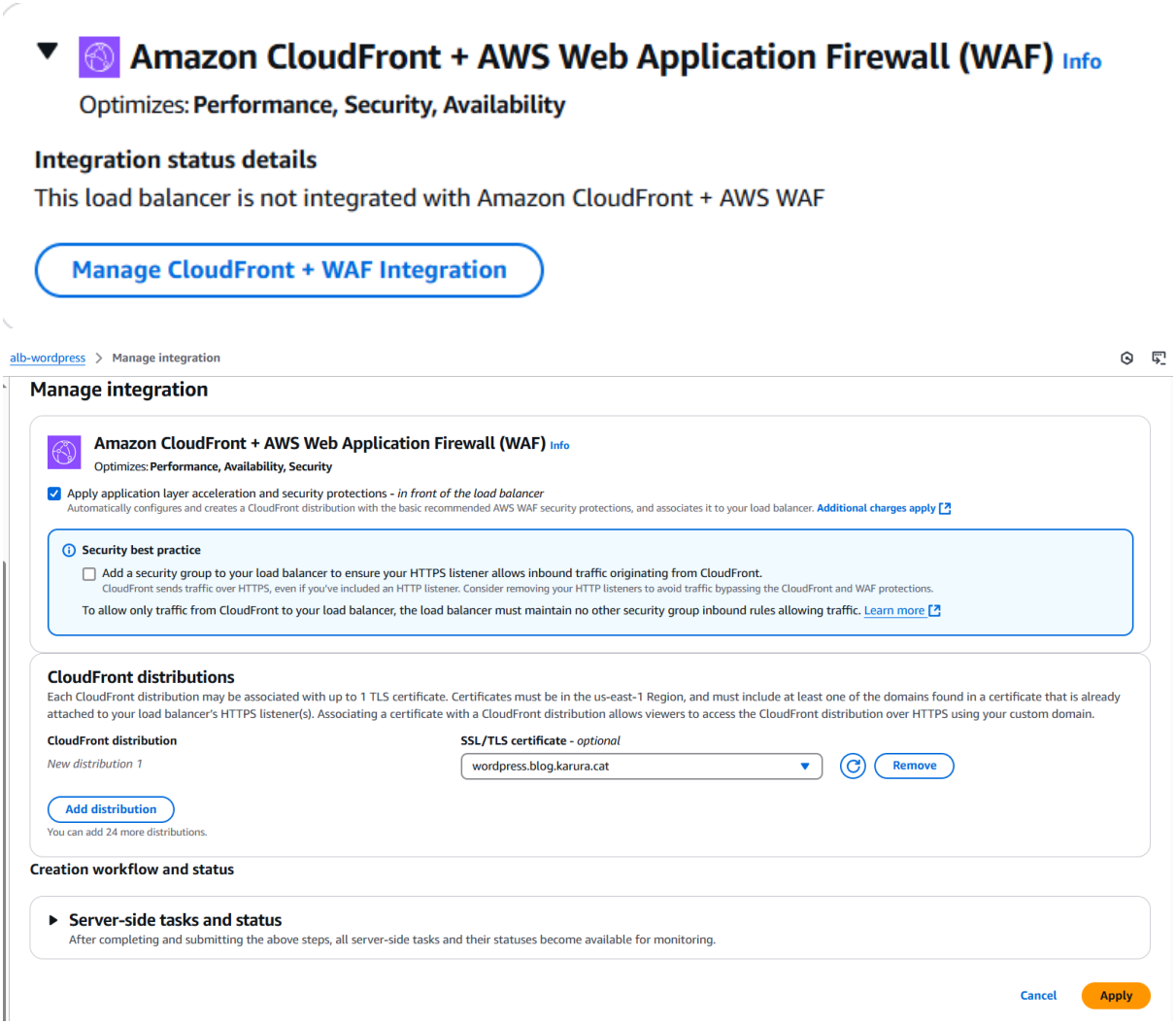




www.blog.karura.cat


https://www.blog.karura.cat
Apache2 Default Page
Ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf


https://www.blog.karura.cat
Welcome
Página de ejemplo
Blog
¡Hola, mundo!
Te damos la bienvenida a WordPress. Esta es tu primera entrada. Edítala o bórrala, ¡luego empieza a escribir!
27 de abril de 2025
Welcome
Blog
Eventos


Amazon CloudFront + AWS Web Application Firewall (WAF) Info
Optimizes: Performance, Security, Availability
Integration status details
This load balancer is not integrated with Amazon CloudFront + AWS WAF
Manage CloudFront + WAF Integration
alb-wordpress > Manage integration
Manage integration
Amazon CloudFront + AWS Web Application Firewall (WAF) Info
Optimizes: Performance, Availability, Security
Apply application layer acceleration and security protections - in front of the load balancer
Automatically configures and creates a CloudFront distribution with the basic recommended AWS WAF security protections, and associates it to your load balancer. Additional charges apply
Security best practice
Add a security group to your load balancer to ensure your HTTPS listener allows inbound traffic originating from CloudFront.
CloudFront sends traffic over HTTPS, even if you've included an HTTP listener. Consider removing your HTTP listeners to avoid traffic bypassing the CloudFront and WAF protections.
To allow only traffic from CloudFront to your load balancer, the load balancer must maintain no other security group inbound rules allowing traffic. Learn more
CloudFront distributions
Each CloudFront distribution may be associated with up to 1 TLS certificate. Certificates must be in the us-east-1 Region, and must include at least one of the domains found in a certificate that is already attached to your load balancer's HTTPS listener(s). Associating a certificate with a CloudFront distribution allows viewers to access the CloudFront distribution over HTTPS using your custom domain.
CloudFront distribution
SSL/TLS certificate - optional
New distribution 1
wordpress.blog.karura.cat
Remove
Add distribution
You can add 24 more distributions.
Creation workflow and status
Server-side tasks and status
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.
Cancel
Apply

Nofunciona


AWS Web Application Firewall (WAF) Info
Optimizes: Security


AWS Web Application Firewall (WAF) Info
Optimizes: Security
Integrated

Creació d'una còpia de seguretat del CMS a S3

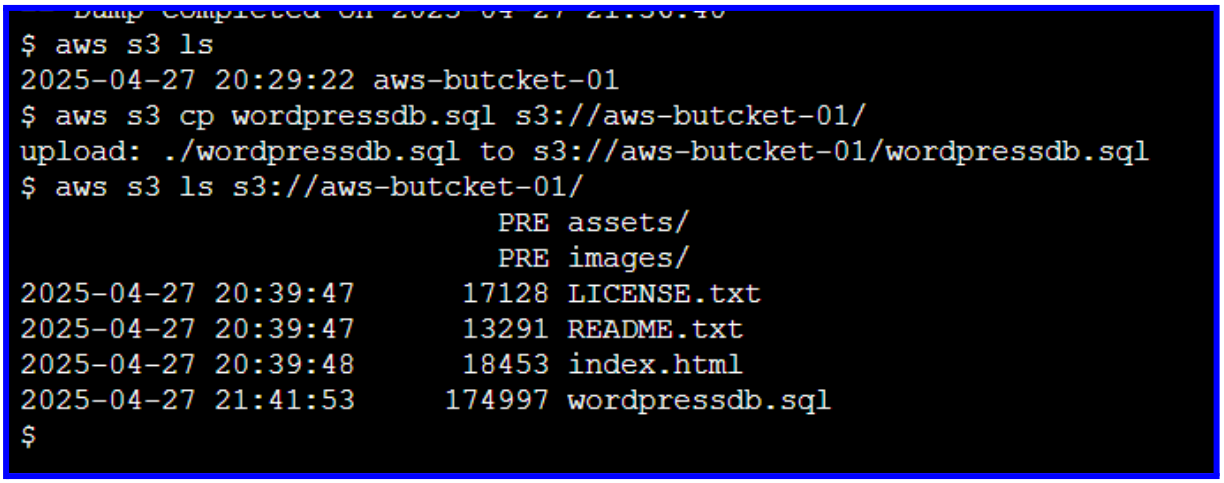
sudo mysqldump -u admin -p -h wordpress-db.c5y99z4gvpom.us-east-1.rds.amazonaws.com > wordpressdb.sql

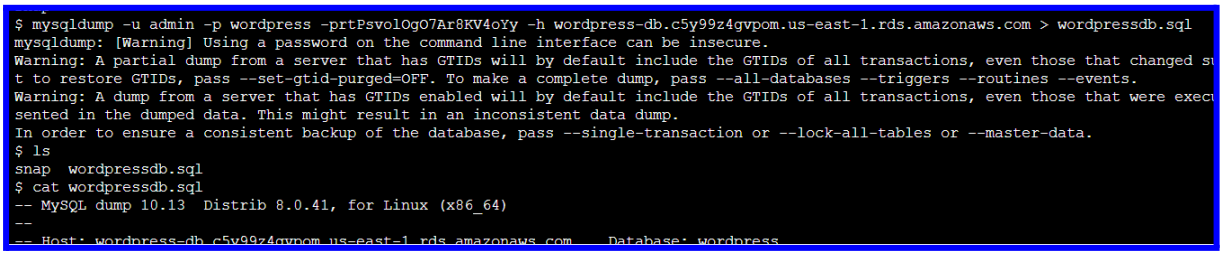
rtPsvolOgO7Ar8KV4oYy
mysql -u admin -p -h wordpress-db.c5y99z4gvpom.us-east-1.rds.amazonaws.com

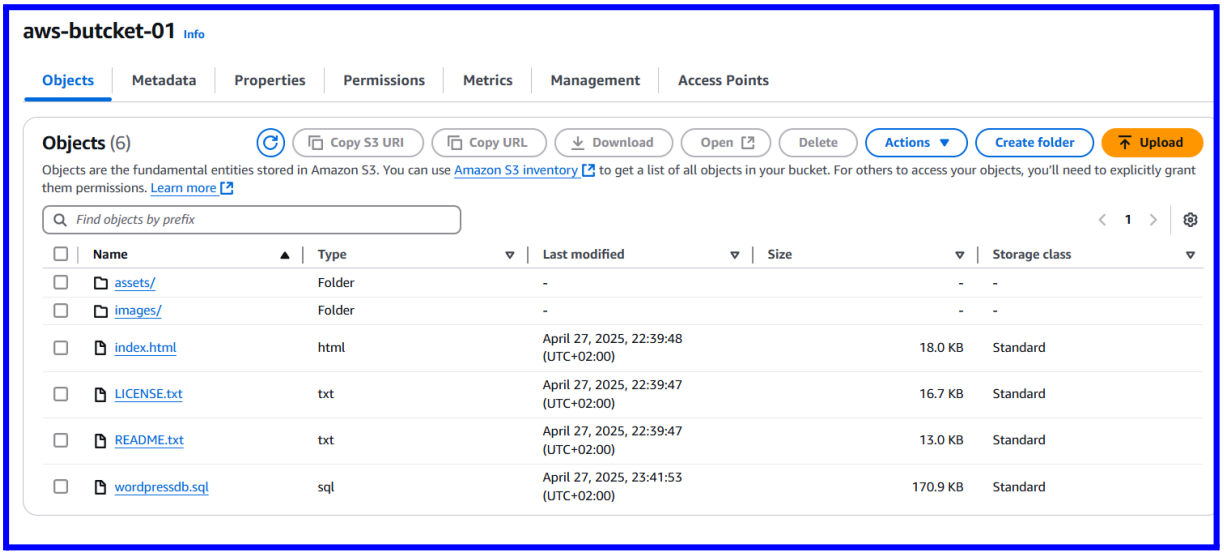
mysqldump -u admin -p wordpress -prtPsvolOgO7Ar8KV4oYy -h wordpress-db.c5y99z4gvpom.us-east-1.rds.amazonaws.com > wordpressdb.sql

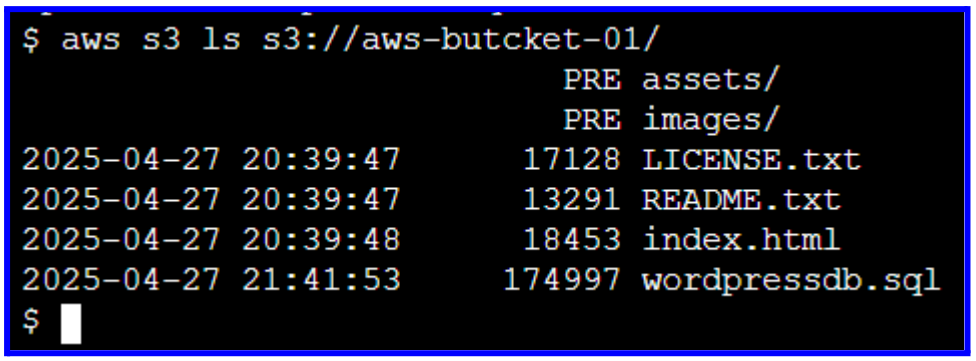
aws s3 cp wordpressdb.sql s3://aws-butcket-01/

aws s3 ls s3://aws-butcket-01/









Creació d'una còpia de seguretat del CMS a S3

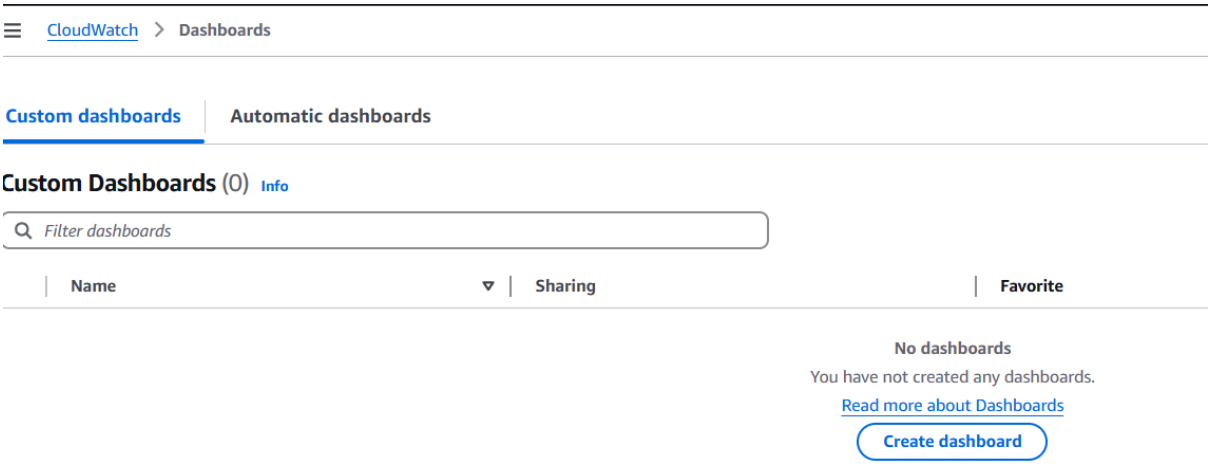
Monitorización y Alarmas

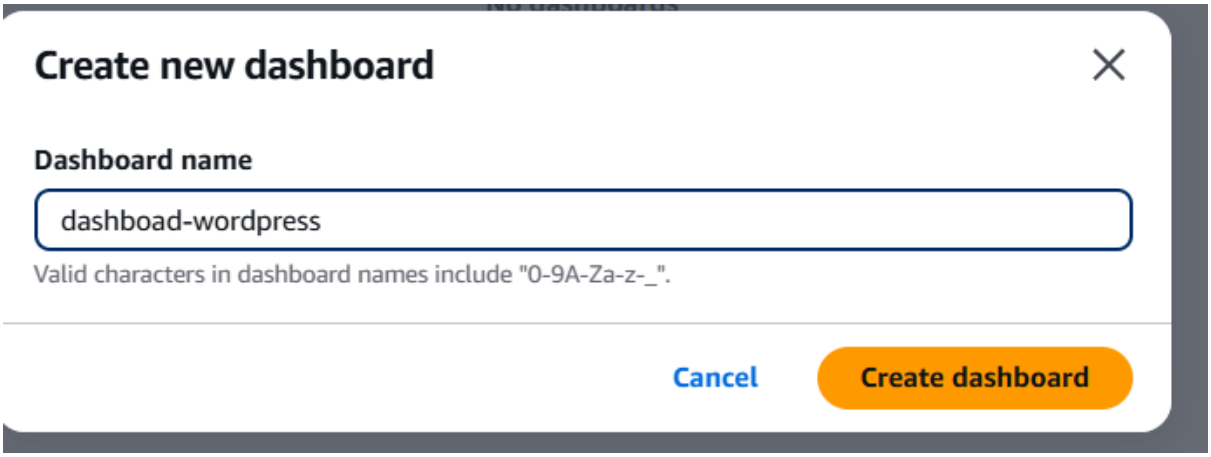
Para instancias EC2 (Auto Scaling):

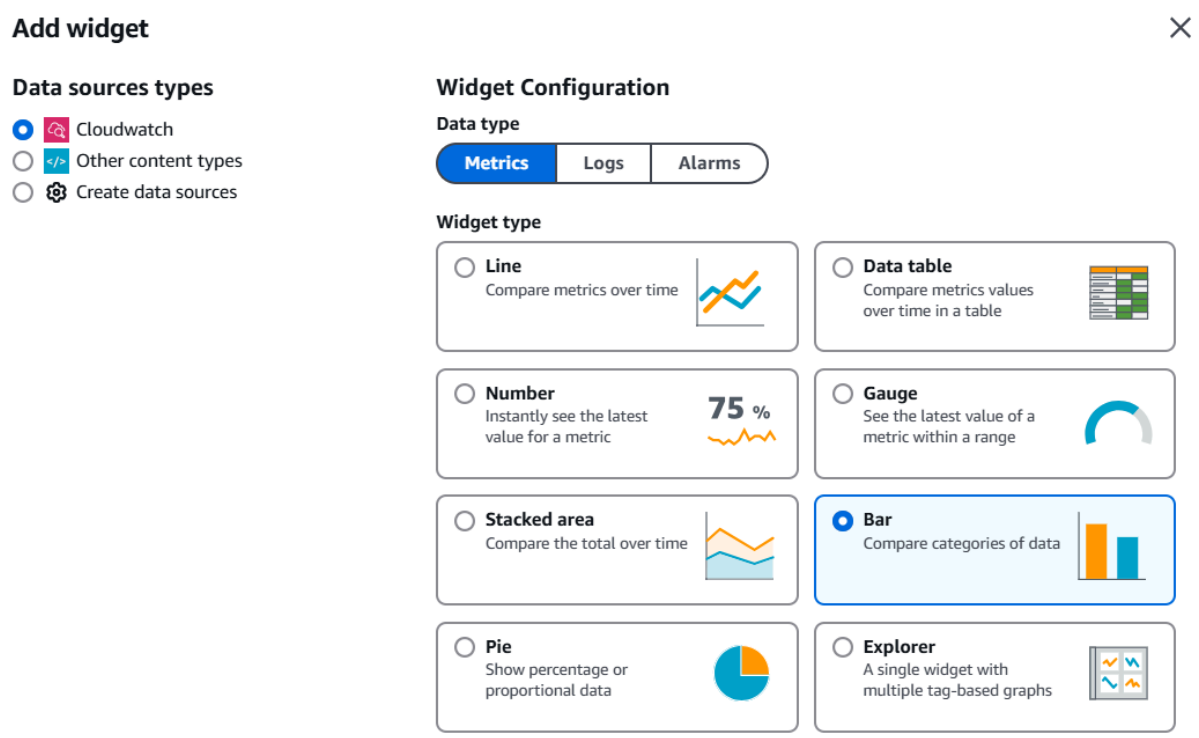
Selecciona "Line" o "Number" como tipo de widget
En "Metrics", busca "EC2" > "By Auto Scaling Group"
Selecciona las siguientes métricas para tu grupo:

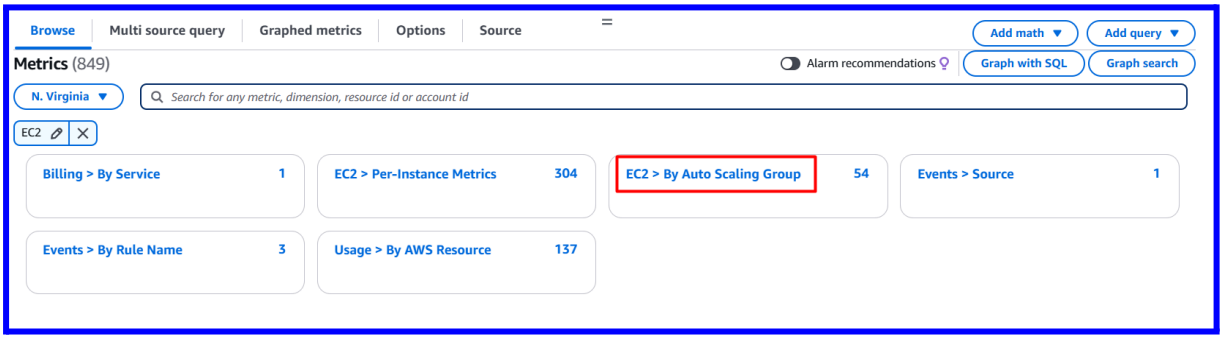
CPUUtilization
NetworkIn / NetworkOut
StatusCheckFailed (para verificar disponibilidad)

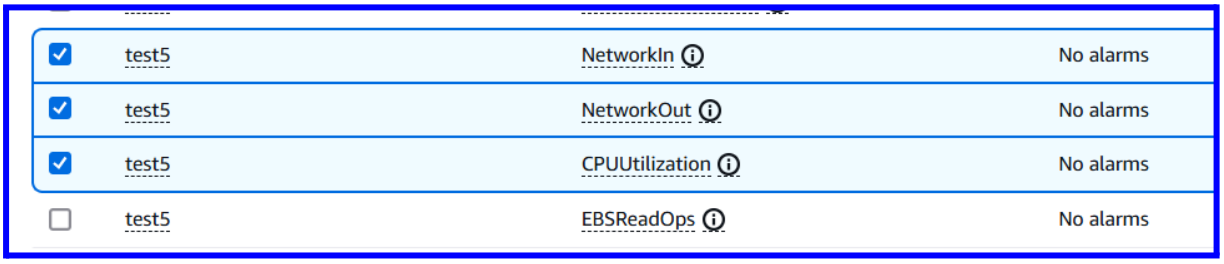
Ajusta el período a 5 minutos para mayor precisión
Haz clic en "Create widget"

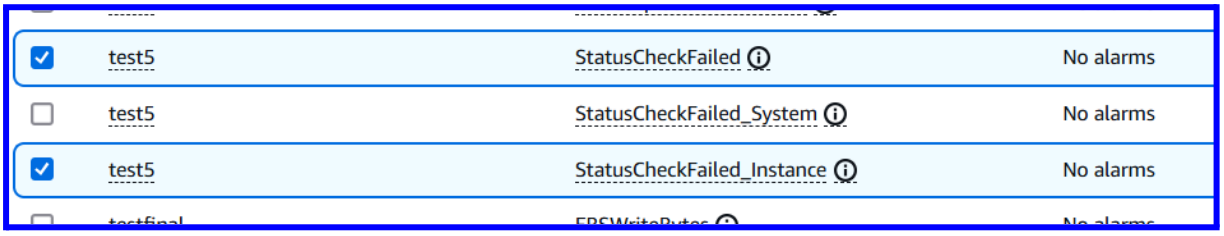




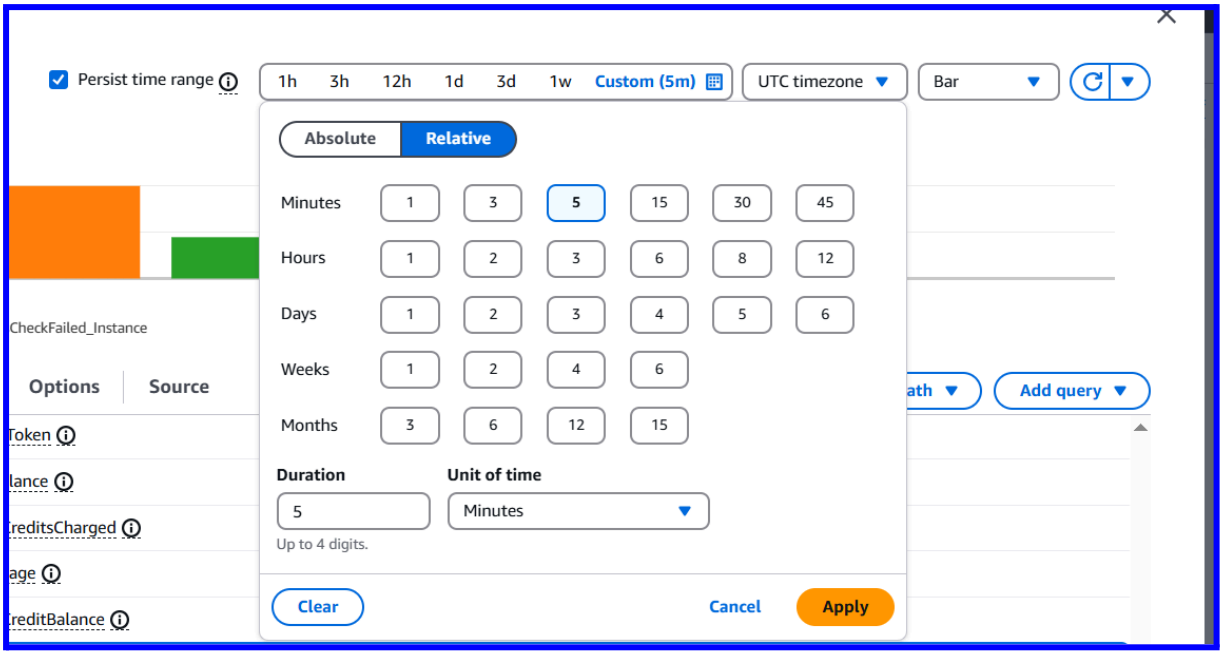

Add widget
Data sources types
Cloudwatch
Other content types
Create data sources
Widget Configuration
Data type
Metrics
Logs
Alarms
Widget type
Line
Compare metrics over time
Data table
Compare metrics values over time in a table
Number
Instantly see the latest value for a metric
75 %
Gauge
See the latest value of a metric within a range
Stacked area
Compare the total over time
Bar
Compare categories of data
Pie
Show percentage or proportional data
Explorer
A single widget with multiple tag-based graphs
Cancel
Next

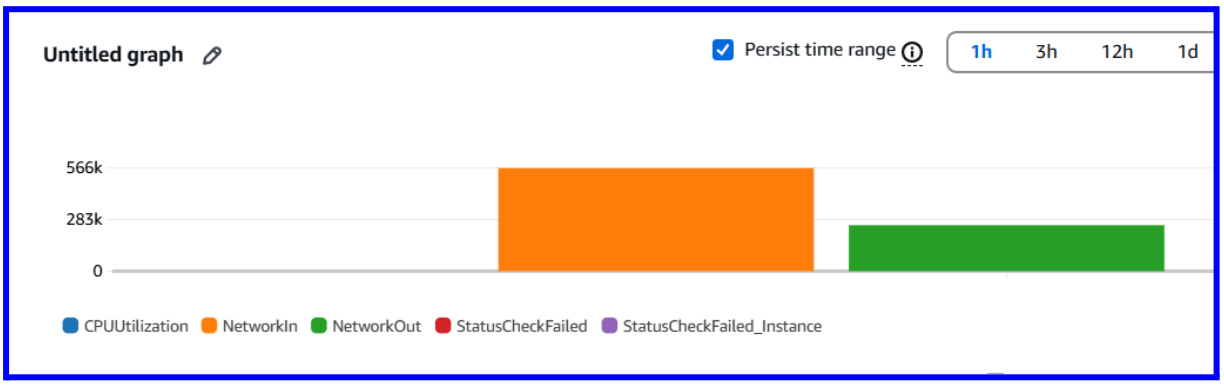

Browse
Multi source query
Graphed metrics
Options
Source
Add math
Add query
Metrics (849)
Alarm recommendations
Graph with SQL
Graph search
N. Virginia
Search for any metric, dimension, resource id or account id
EC2
Billing > By Service 1
EC2 > Per-Instance Metrics 304
EC2 > By Auto Scaling Group 54
Events > Source 1
Events > By Rule Name 3
Usage > By AWS Resource 137


test5 NetworkIn No alarms
test5 NetworkOut No alarms
test5 CPUUtilization No alarms
test5 EBSReadOps No alarms


test5 StatusCheckFailed No alarms
test5 StatusCheckFailed_System No alarms
test5 StatusCheckFailed_Instance No alarms


Persist time range
1h 3h 12h 1d 3d 1w Custom
UTC timezone
Bar


Persist time range
1h 3h 12h 1d 3d 1w Custom (5m)
UTC timezone
Bar
Absolute
Relative
Minutes 1 3 5 15 30 45
Hours 1 2 3 6 8 12
Days 1 2 3 4 5 6
Weeks 1 2 4 6
Months 3 6 12 15
Duration
5
Up to 4 digits.
Unit of time
Minutes
Clear
Cancel
Apply
Options
Source
Add query

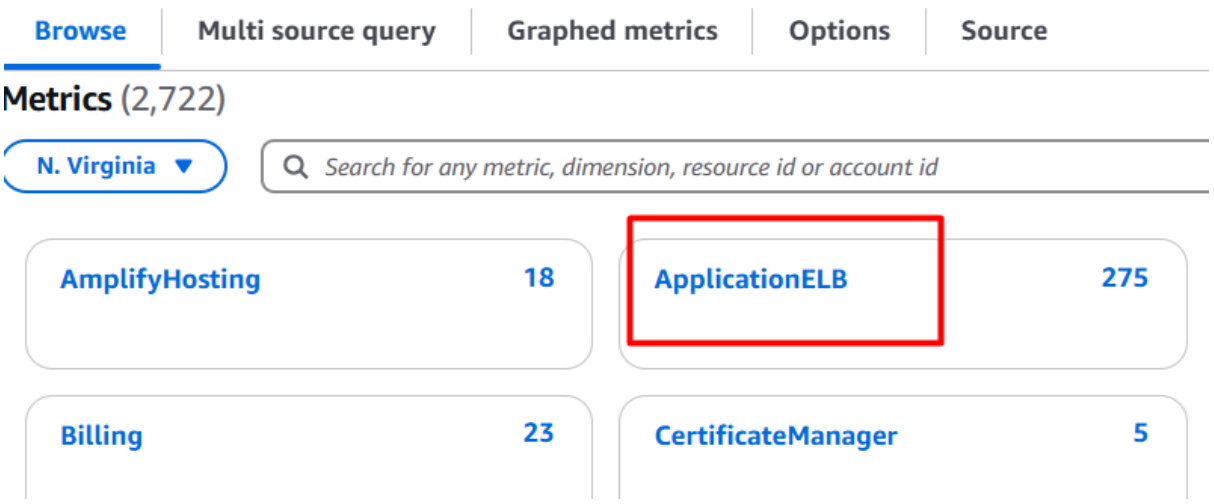

Untitled graph
Persist time range
1h 3h 12h 1d
566k
283k
0
CPUUtilization NetworkIn NetworkOut StatusCheckFailed StatusCheckFailed_Instance

Para el Load Balancer (ALB):

Añade otro widget
Busca "ApplicationELB" > "Por balanceador de carga"
Selecciona:

RequestCount (solicitudes totales)
HTTPCode_Target_2XX_Count (respuestas exitosas)
HTTPCode_Target_5XX_Count (errores del servidor)
TargetResponseTime (tiempo de respuesta)

Haz clic en "Create widget"

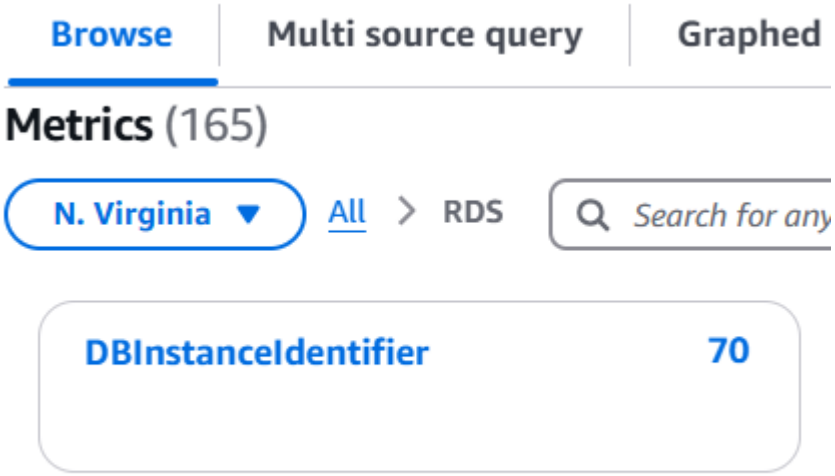


Para RDS:

1. **Añade otro widget**
2. **Busca "RDS" > "DB Instance"**
3. **Selecciona tu instancia de base de datos y monitorea:**
    - **CPUUtilization**
    - **DatabaseConnections**

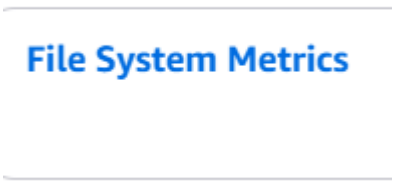
- **ReadIOPS / WriteIOPS**
- **FreeStorageSpace**

4. **Haz clic en "Create widget"**



Para EFS:

1. **Añade otro widget**
2. **Busca "EFS" > "File System Metrics"**
3. **Selecciona:**
   - **BurstCreditBalance**
   - **StorageBytes**
   - **TotalIOBytes**
4. **Haz clic en "Create widget"**

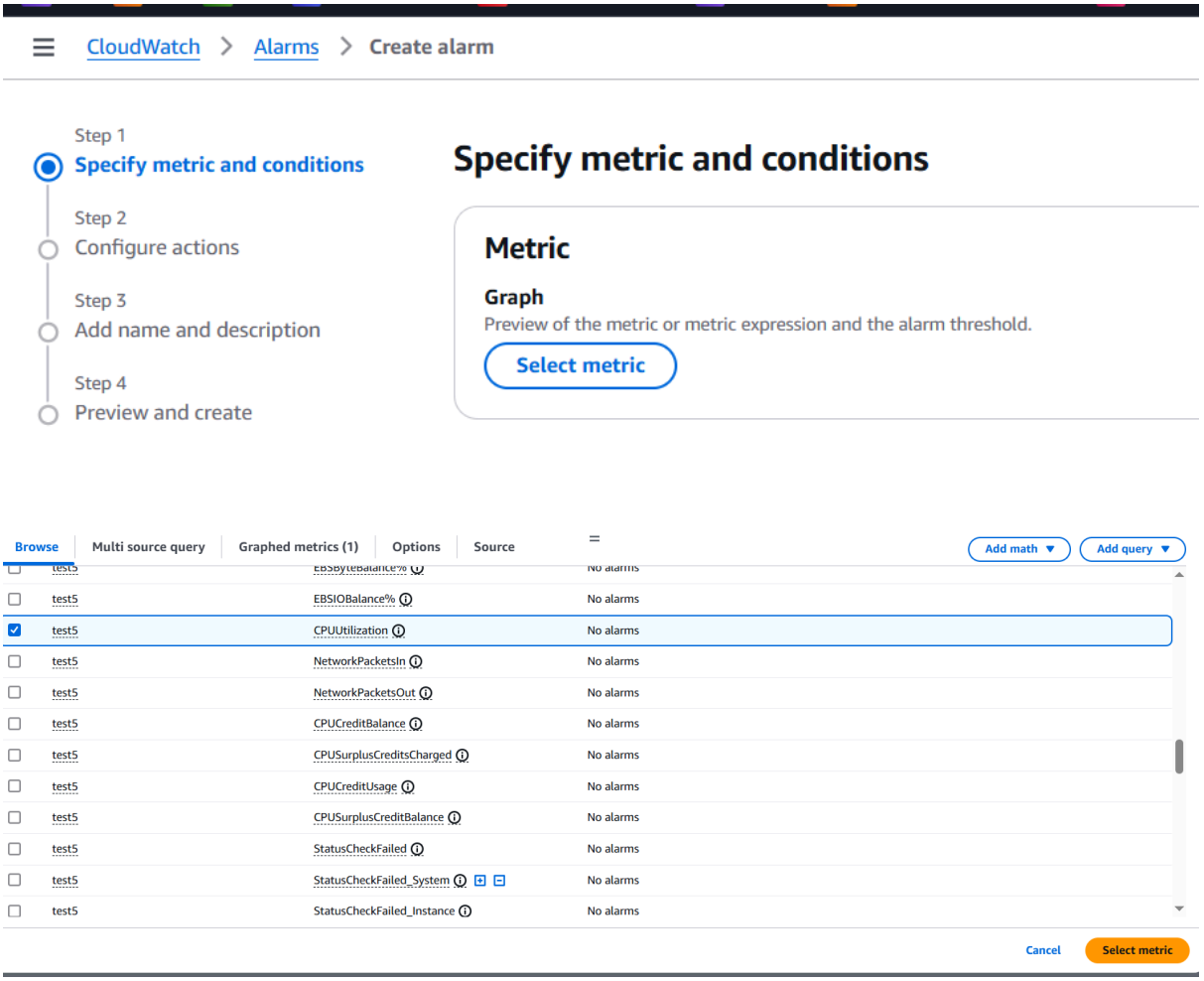


Configurar alarmas para métricas críticas

A continuación, vamos a crear algunas alarmas para recibir notificaciones cuando ocurran problemas:

Alarma para alta utilización de CPU:

1. **En el panel de navegación izquierdo, selecciona "Alarms" > "All alarms"**
2. **Haz clic en "Create alarm"**
3. **Haz clic en "Select metric"**
4. **Busca "EC2" > "By Auto Scaling Group"**
5. **Selecciona CPUUtilization para tu grupo de Auto Scaling**
6. **Haz clic en "Select metric"**
7. **Configura:**
    - **Statistic: Average**
    - **Period: 5 minutes**
    - **Threshold type: Static**
    - **Whenever CPUUtilization is: Greater/Equal than 80%**
    - **Datapoints to alarm: 3 out of 3**
8. **En "Notification", configura:**
    - **Create new topic (o usa uno existente)**
    - **Introduce tu dirección de correo electrónico**
9. **Añade un nombre para la alarma como "WordPress-High-CPU"**
10. **Haz clic en "Create alarm"**


CloudWatch
Alarms
Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Metric
Graph
Preview of the metric or metric expression and the alarm threshold.
Select metric
Browse
Multi source query
Graphed metrics (1)
Options
Source
Add math
Add query
test5 EBSIOBalance% No alarms
test5 CPUUtilization No alarms
test5 NetworkPacketsIn No alarms
test5 NetworkPacketsOut No alarms
test5 CPUCreditBalance No alarms
test5 CPUSurplusCreditsCharged No alarms
test5 CPUCreditUsage No alarms
test5 CPUSurplusCreditBalance No alarms
test5 StatusCheckFailed No alarms
test5 StatusCheckFailed_System No alarms
test5 StatusCheckFailed_Instance No alarms
Cancel
Select metric

Namespace
AWS/EC2

Metric name
CPUUtilization

AutoScalingGroupName
test5

Statistic
Average

Period
5 minutes

Conditions

Threshold type
- Static — Use a value as a threshold
- Anomaly detection — Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.
- Greater — > threshold
- Greater/Equal — >= threshold
- Lower/Equal — <= threshold
- Lower — < threshold

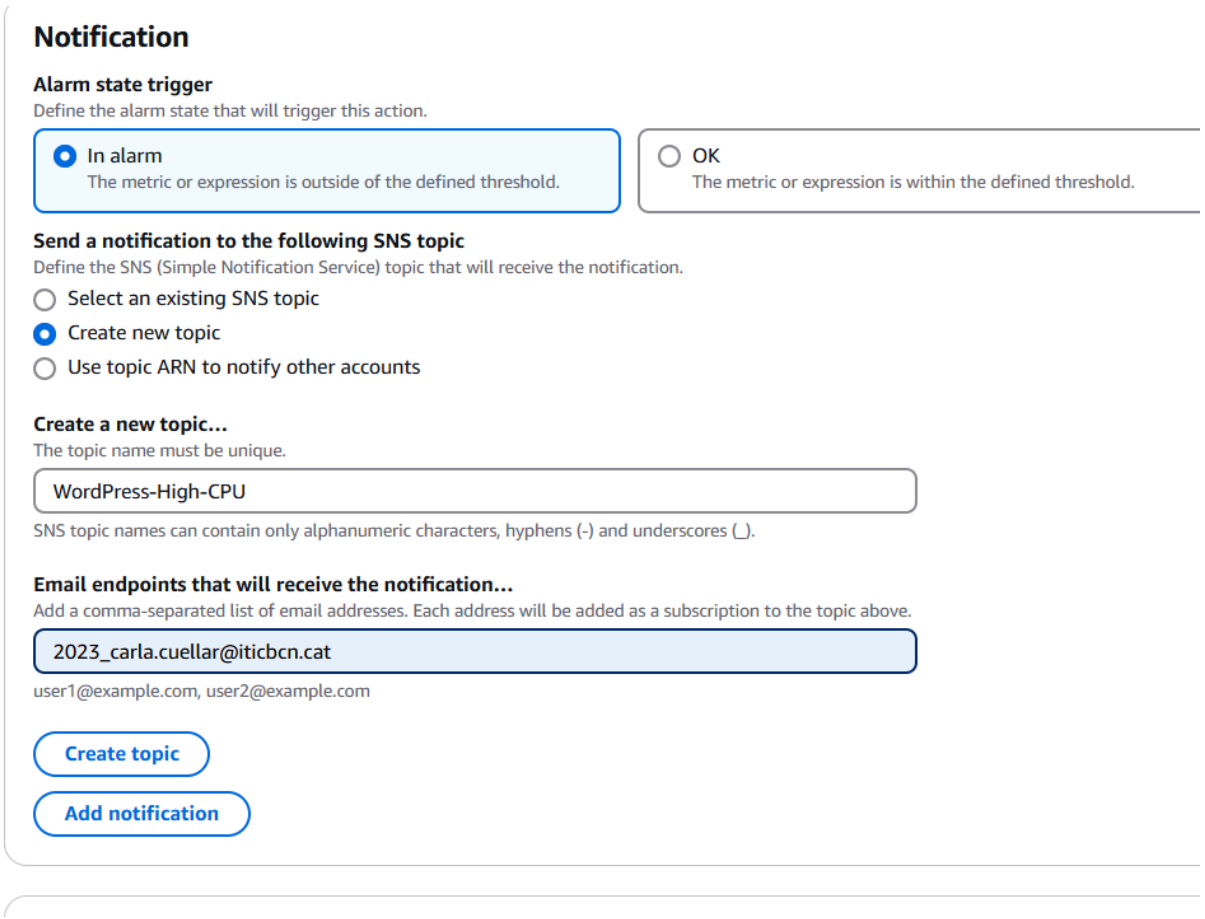
than...
Define the threshold value.
80
Must be a number

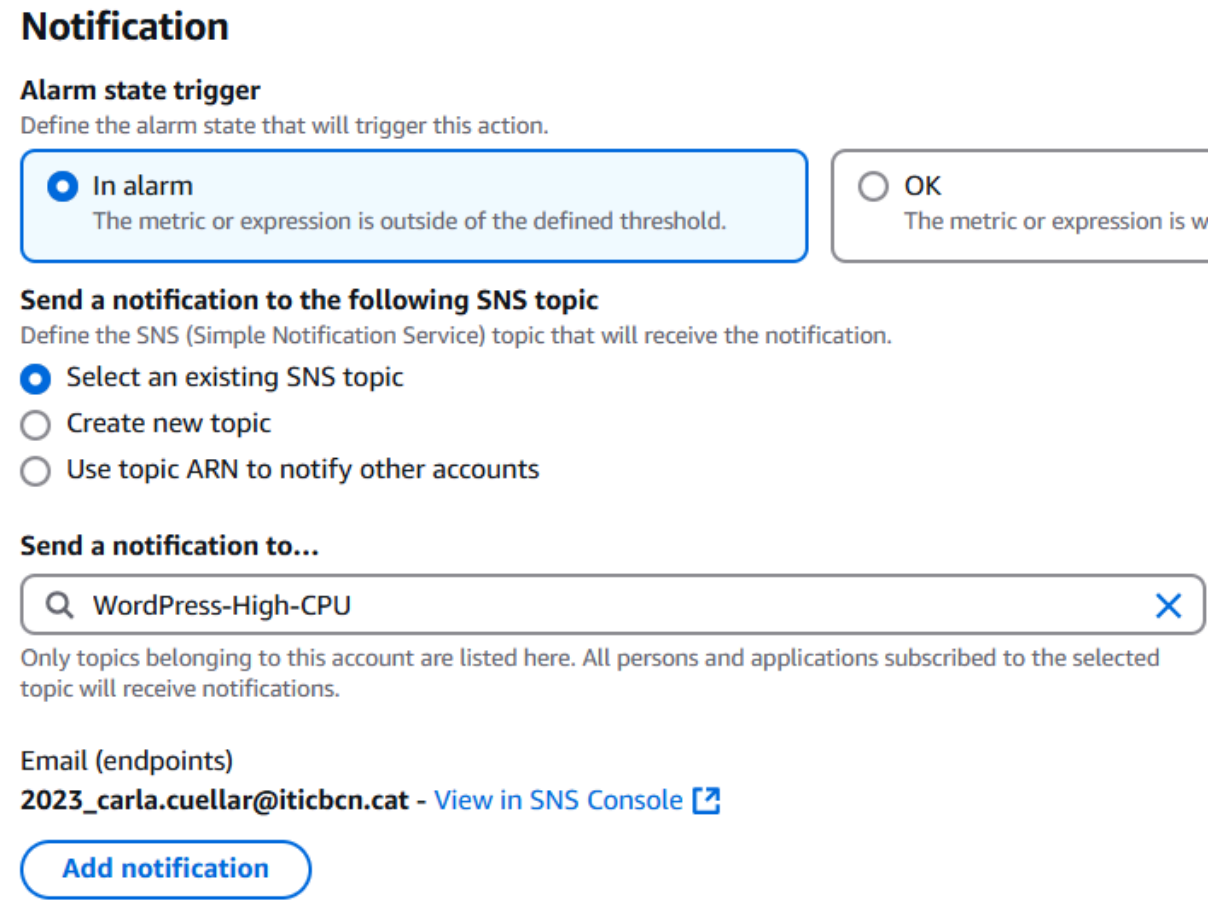
▸ Additional configuration

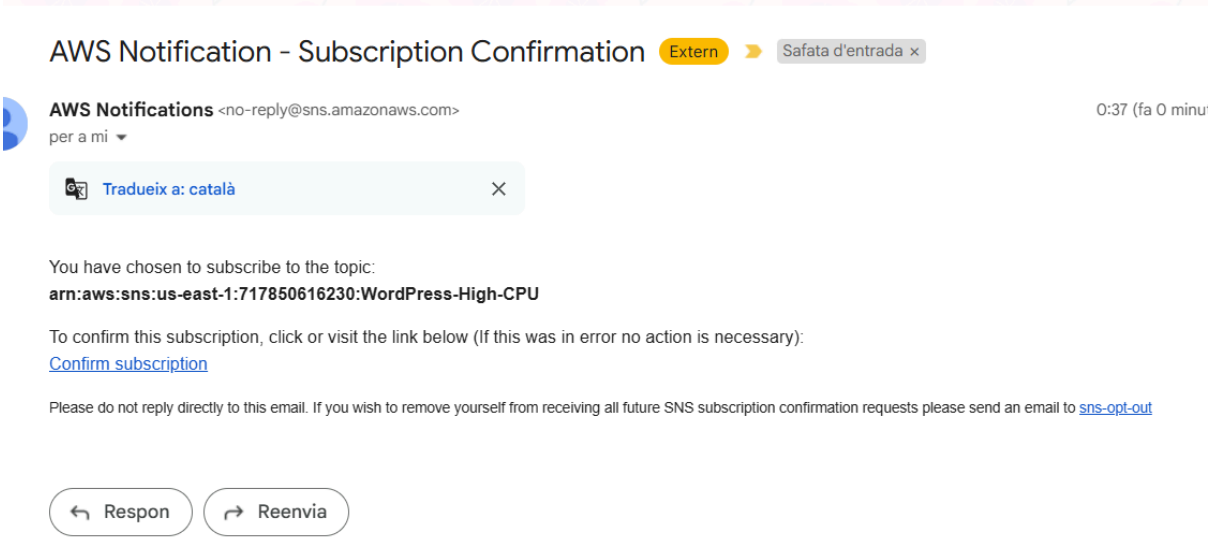
▾ **Additional configuration**

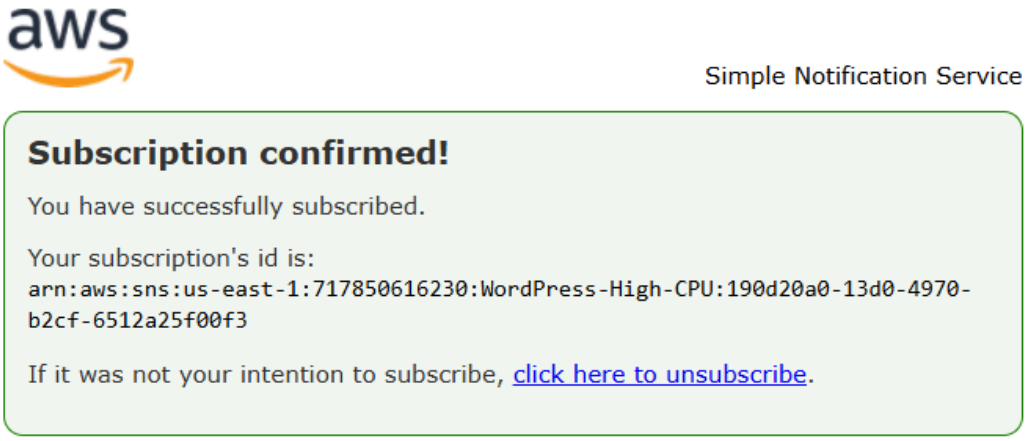
Datapoints to alarm
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.
3 out of 3

Missing data treatment
How to treat missing data when evaluating the alarm.
Treat missing data as missing


Notification
Alarm state trigger
Define the alarm state that will trigger this action.
In alarm
The metric or expression is outside of the defined threshold.
OK
The metric or expression is within the defined threshold.
Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.
Select an existing SNS topic
Create new topic
Use topic ARN to notify other accounts
Create a new topic...
The topic name must be unique.
WordPress-High-CPU
SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).
Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.
2023_carla.cuellar@iticbcn.cat
user1@example.com, user2@example.com
Create topic
Add notification


Notification
Alarm state trigger
Define the alarm state that will trigger this action.
In alarm
The metric or expression is outside of the defined threshold.
OK
The metric or expression is w
Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.
Select an existing SNS topic
Create new topic
Use topic ARN to notify other accounts
Send a notification to...
WordPress-High-CPU
Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.
Email (endpoints)
2023_carla.cuellar@iticbcn.cat - View in SNS Console
Add notification


AWS Notification - Subscription Confirmation
Extern
Safata d'entrada ×
AWS Notifications <no-reply@sns.amazonaws.com>
per a mi
0:37 (fa 0 minu
Tradueix a: català
You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:717850616230:WordPress-High-CPU
To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out
Respon
Reenvia



Alarma para errores del Load Balancer:

1. **Sigue los pasos 1-3 anteriores**
2. **Busca "ApplicationELB" > "Per AppELB" > "Per TG" > "Per AZ Metrics"**
3. **Selecciona "HTTPCode_Target_5XX_Count"**
4. **Configura:**
    - **Statistic: Sum**
    - **Period: 5 minutes**
    - **Threshold type: Static**
    - **Whenever HTTPCode_Target_5XX_Count is: Greater/Equal than 10**
    - **Datapoints to alarm: 3 out of 3**
5. **Configura la notificación como se describió anteriormente**
6. **Añade un nombre como "WordPress-Error-Rate"**
7. **Haz clic en "Create alarm"**

Alarma para latencia de la base de datos:

1. **Sigue los pasos 1-3 anteriores**
2. **Busca "RDS" > "DB Instance"**
3. **Selecciona "ReadLatency" o "WriteLatency" para tu instancia de base de datos**
4. **Configura:**
    - **Statistic: Average**
    - **Period: 5 minutes**
    - **Threshold type: Static**
    - **Whenever ReadLatency/WriteLatency is: Greater/Equal than 1 (segundo)**
    - **Datapoints to alarm: 3 out of 3**

5. **Configura la notificación como se describió anteriormente**
6. **Añade un nombre como "WordPress-DB-Latency"**
7. **Haz clic en "Create alarm"**

Stress Test en una instancia

Este método consiste en generar carga artificial en una de tus instancias EC2 para verificar que el Auto Scaling responde correctamente:

1. **Conéctate por SSH a una instancia de EC2 en tu grupo de Auto Scaling:**
   `ssh -i tuClave.pem ubuntu@ip-de-tu-instancia`

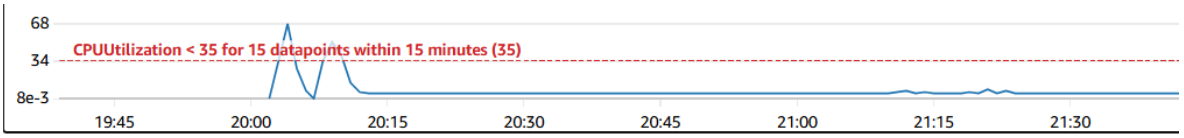
Instala la herramienta stress:

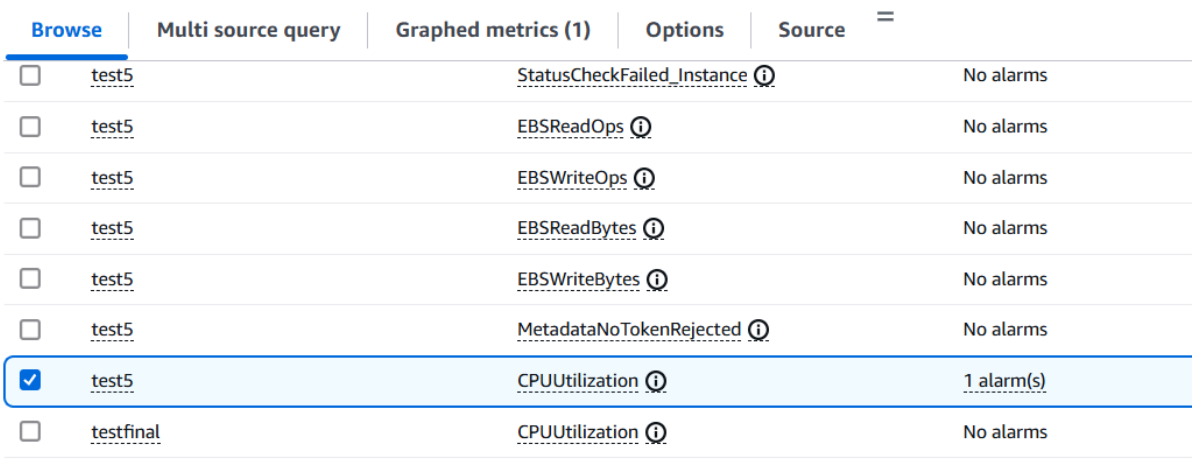
`sudo apt-get update`

2. `sudo apt-get install -y stress`

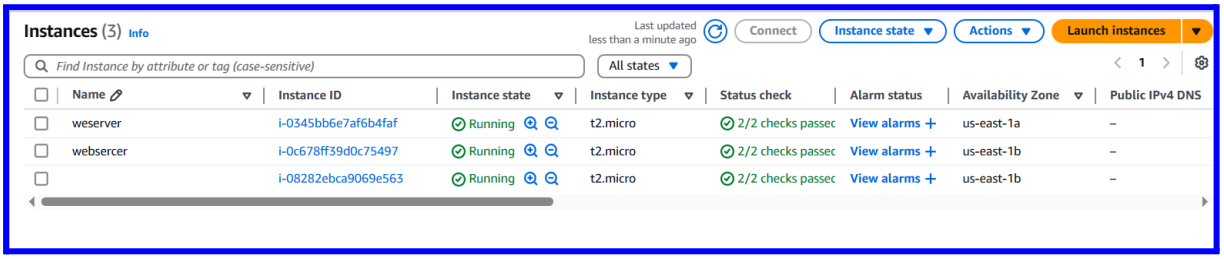
3. **Ejecuta un test de stress para aumentar la carga de CPU:**
   `sudo stress --cpu 4 --timeout 600`
   (Esto generará carga durante 10 minutos usando 4 threads de CPU)
4. **Verifica en CloudWatch mientras el test está en ejecución:**
   - **Ve a CloudWatch > Métricas > EC2 > Por Auto Scaling Group**
   - **Selecciona CPUUtilization para tu grupo**
   - **Confirma que la utilización supera el 80%**
5. **Verifica en EC2 > Auto Scaling Groups:**
   - **Selecciona tu grupo de Auto Scaling**
   - **Ve a la pestaña "Activity"**
   - **Deberías ver entradas que indiquen el lanzamiento de nuevas instancias**
   - **También ve a la pestaña "Instances" para ver las instancias nuevas**

Prueba de que funciona






```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  stress
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 18.1 kB of archives.
After this operation, 52.2 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 stress amd64 1.0.7-1 [18.1 kB]
Fetched 18.1 kB in 0s (1095 kB/s)
Selecting previously unselected package stress.
(Reading database ... 73708 files and directories currently installed.)
Preparing to unpack .../stress_1.0.7-1_amd64.deb ...
Unpacking stress (1.0.7-1) ...
Setting up stress (1.0.7-1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...

Service restarts being deferred:
 /etc/needrestart/restart.d/dbus.service
 systemctl restart networkd-dispatcher.service
 systemctl restart systemd-logind.service
 systemctl restart unattended-upgrades.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
$ sudo stress --cpu 4 --timeout 600
stress: info: [26606] dispatching hogs: 4 cpu, 0 io, 0 vm, 0 hdd
```



nstala la herramienta stress:

```
sudo apt-get install -y stress
```

Genera carga de memoria:

```
sudo stress --vm 1 --vm-bytes 1500M --timeout 600
```

Monitorea en CloudWatch la métrica mem_used_percent

Verifica que se activa la alarma y que se lanzan nuevas instancias

Conclusión