

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)

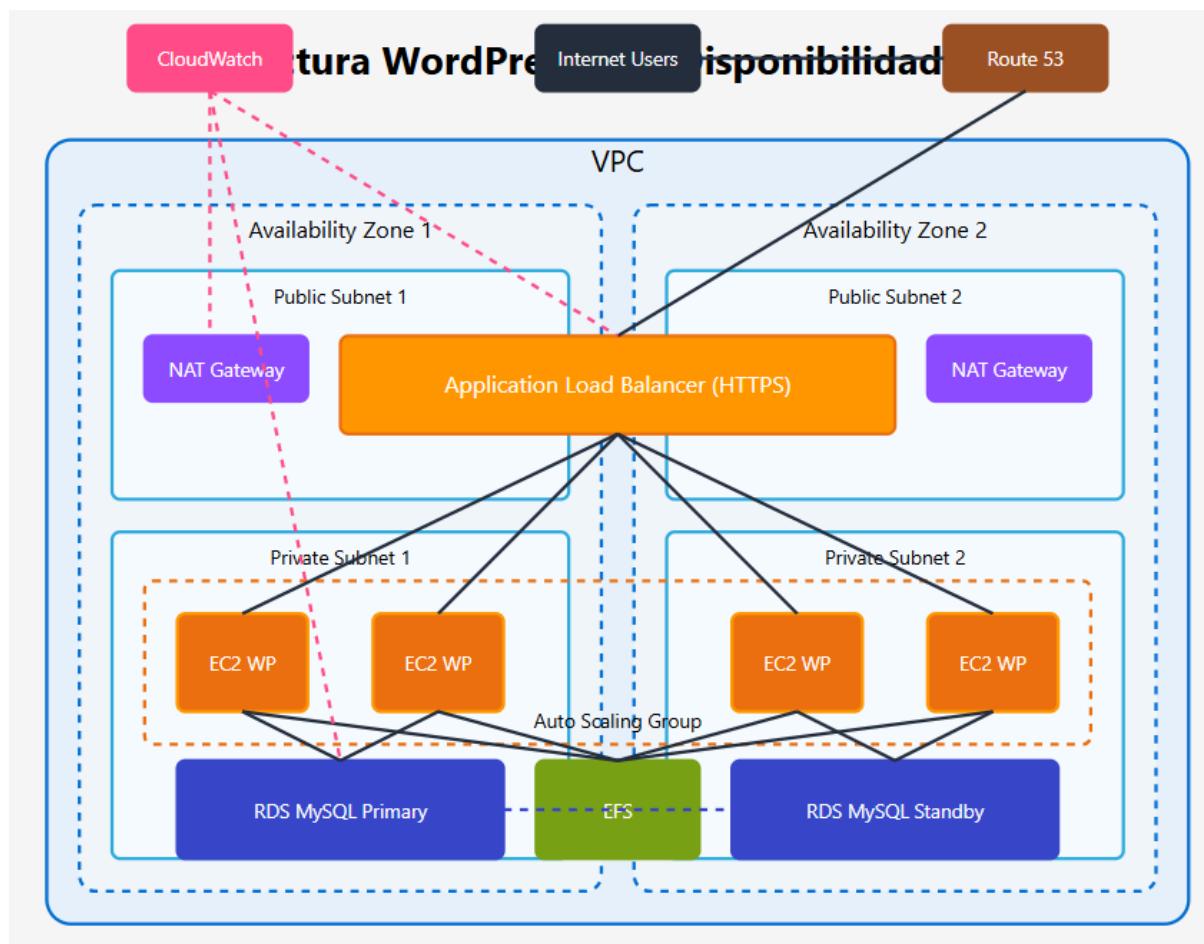
- Crear plantilla de lanzamiento con Ubuntu
- Configurar script de inicio para WordPress
- Implementar grupo de Auto Scaling

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

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as EC2 instances, Amazon RDS databases, and Amazon S3 buckets.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate
wordpress-vpc

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

10.55.0.0/16	65.536 IPs
--------------	------------

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

No IPv6 CIDR block
 Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default	▼
---------	---

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 **2** 3

► Customize AZs**Number of public subnets [Info](#)**

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 **2**

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 **2** 4

► Customize subnets CIDR blocks**NAT gateways (\$) [Info](#)**

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None **In 1 AZ** 1 per AZ

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None **S3 Gateway**

DNS options [Info](#)

- Enable DNS hostnames
- Enable DNS resolution

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

[EC2](#) > [Security Groups](#) > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
 Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description -
HTTP	TCP	80	Anywh... <input type="text" value="0.0.0.0/0"/> X	
HTTPS	TCP	443	Anywh... <input type="text" value="0.0.0.0/0"/> X	

[Add rule](#)

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

✓ Security group (sg-0083b38f9abdf04dd | alb-sg-wordpress) was created successfully X

[Details](#)

sg-0083b38f9abdf04dd - alb-sg-wordpress Actions ▾

Details		Inbound rules count		Outbound rules count	
Security group name <input type="text" value="alb-sg-wordpress"/>	Security group ID <input type="text" value="sg-0083b38f9abdf04dd"/>	Description <input type="text" value="permitir -p 80 y 443 desde internet"/>	1 Permission entries	VPC ID <input type="text" value="vpc-02c7e9d631ec5a2ab"/>	1 Permission entry
Owner <input type="text" value="717850616230"/>	Inbound rules count <input type="text" value="2"/>				

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (2)

Search		Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-04a858408e2c90db3	IPv4	HTTP	TCP	80	0.0.0.0/0	
<input type="checkbox"/>	-	sgr-0eb4ffe133d622c0a	IPv4	HTTPS	TCP	443	0.0.0.0/0	

bastianhost-sg

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info

Type Info

Protocol Info

Port range Info

Source Info



[Add rule](#)

⌚ Security group (sg-048865fcf829fb01d | bastianhost-sg) was created successfully
 ► Details

sg-048865fcf829fb01d - bastianhost-sg

[Actions](#)

Details

Security group name

Security group ID

Description

VPC ID

Owner

Inbound rules count
 1 Permission entry

Outbound rules count
 1 Permission entry

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (1)

Search		Manage tags	Edit inbound rules			
Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-06bcfbdb2122417b	IPv4	SSH	TCP	22	0.0.0.0/0

webserver-sg-wordpress

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
HTTP	TCP	80	Custom	<input type="text" value="sg-0083b38f9abdf04dd"/> X
HTTPS	TCP	443	Custom	<input type="text" value="sg-0083b38f9abdf04dd"/> X
Add rule				<input type="text"/>
Outbound rules <small>Info</small>				
Security Groups default sg-0e7cff1b851787021 alb-sg-wordpress sg-0083b38f9abdf04dd				

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Custom	sg-0083b38f9abdf04dd
HTTPS	TCP	443	Custom	sg-0083b38f9abdf04dd
SSH	TCP	22	Custom	alb-sg-wordpress sg-0083b38f9abdf04dd

[Add rule](#)

(+) Security group (sg-0765f332c0af98403 | webserver-sg-wordpress) was created successfully
[Details](#)

sg-0765f332c0af98403 - webserver-sg-wordpress

[Actions](#)

Details

Security group name sg-0765f332c0af98403	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)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-0f43794b73a448126	-	SSH	TCP	22	sg-048865fcf8
-	sgr-0b44d6f6171bdaa93	-	HTTPS	TCP	443	sg-0083b38f9a
-	sgr-05081694006f9f14c	-	HTTP	TCP	80	sg-0083b38f9a

rds-sg-wordpress

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Basic details

Security group name Info

rds-sg-wordpress

Name cannot be edited after creation.

Description Info

permitir 3306 desde webserver-sg

VPC Info

vpc-02c7e9d631ec5a2ab (wordpress-vpc-vpc)

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
MySQL/Aurora	TCP	3306	Custom	<input type="text"/> default sg-0e7cff1b851787021
Add rule				<input type="text"/> webserver-sg-wordpress sg-0765f332c0af98403

⌚ Security group (sg-0064e77c4e394574e | rds-sg-wordpress) was created successfully

► Details

sg-0064e77c4e394574e - rds-sg-wordpress

[Actions ▾](#)

Details

Security group name	<input type="text"/> rds-sg-wordpress	Security group ID	<input type="text"/> sg-0064e77c4e394574e	Description	<input type="text"/> permitir 3306 desde webserver-sg	VPC ID	<input type="text"/> vpc-02c7e9d631ec5a2ab
Owner	<input type="text"/> 717850616230	Inbound rules count	1 Permission entry	Outbound rules count	1 Permission entry		

[Inbound rules](#) [Outbound rules](#) [Sharing - new](#) [VPC associations - new](#) [Tags](#)

Inbound rules (1)

<input type="text"/> Search		Security group rule ID	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	Name	sgr-02224988dd3d5a5b2	-	MySQL/Aurora	TCP	3306	sg-0765f332c0af98403

efs-sg-wordpress

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a security group, you must provide a name, description, and VPC.

Basic details

Security group name [Info](#)

efs-sg-wordpress

Name cannot be edited after creation.

Description [Info](#)

permitir 2049 NFS desde webserver-sg

VPC [Info](#)

vpc-02c7e9d631ec5a2ab (wordpress-vpc-vpc)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
NFS	TCP	2049	Custom	<input type="text"/> Search Security Groups default sg-0e7cff1b851787021 webserver-sg-wordpress sg-0765f332c0af98403 alb-sq-wordpress sg-0083b38f9abdf04dd

Outbound rules [Info](#)

✓ Security group (sg-0cdc71d5a3b1333ab | efs-sg-wordpress) was created successfully
[Details](#)

sg-0cdc71d5a3b1333ab - efs-sg-wordpress

[Actions](#)

Details

Security group name	sg-0cdc71d5a3b1333ab efs-sg-wordpress	Security group ID	sg-0cdc71d5a3b1333ab	Description	permitir 2049 NFS desde webserver-sg	VPC ID	vpc-02c7e9d631ec5a2ab
Owner	717850616230	Inbound rules count	1 Permission entry	Outbound rules count	1 Permission entry		

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (1)

Search		Manage tags	Edit inbound rules	
Name	Type	Protocol	Port range	Source
sgr-024b54b785f349d32	NFS	TCP	2049	sg-0765f332c0af98403

1.3. Configurar EFS para almacenamiento compartido

Create file system

X

Create a file system with the recommended settings shown below by choosing Create file system. To view all settings or to customize your file system, choose Customize. [Learn more](#)

Name - optional

Name your file system.

efs-wordpress

Name can include letters, numbers, and +-=._:/ symbols, up to 256 characters.

Virtual Private Cloud (VPC)

Choose the VPC where you want EC2 instances to connect to your file system.

vpc-02c7e9d631ec5a2ab
wordpress-vpc-vpc

CUSTOMIZER

Name - optional

Name your file system.

efs-wordpress

File system type

Choose to either store data across multiple Availability Zones or within a single Availability Zone. [Learn more](#)

Regional

Offers the highest levels of availability and durability by storing file system data across multiple Availability Zones within an AWS Region.

One Zone

Provides continuous availability to data within a single Availability Zone within an AWS Region.

Automatic backups

Automatically backup your file system data with AWS Backup using recommended settings. Additional pricing applies. [Learn more](#)

Enable automatic backups

Lifecycle management

Automatically save money as access patterns change by moving files into the Infrequent Access (IA) or Archive storage class. [Learn more](#)

Transition into Infrequent Access (IA)

Transition files to IA based on the time since they were last accessed in Standard storage.

30 day(s) since last access

Transition into Archive

Transition files to Archive based on the time since they were last accessed in Standard storage.

90 day(s) since last access

Transition into Standard

Transition files back to Standard storage based on when they are first accessed in IA or Archive storage.

None

Encryption

Choose to enable encryption of your file system's data at rest. Uses the AWS KMS service key (aws/elasticfilesystem) by default. [Learn more](#)

Enable encryption of data at rest

Network access

Network

Virtual Private Cloud (VPC) [Learn more](#) Choose the VPC where you want EC2 instances to connect to your file system.

vpc-02c7e9d631ec5a2ab	wordpress-vpc-vpc
-----------------------	-------------------

Mount targets

A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone	Subnet ID	IP address	Security groups
us-east-1a	subnet-0e172d55c0ef...	Automatic	Choose security groups Remove sg-0cdc71d5a3b1333ab X efs-sg-wordpress
us-east-1b	subnet-04d41282c2e5...	Automatic	Choose security groups Remove sg-0cdc71d5a3b1333ab X efs-sg-wordpress

[Add mount target](#)

Cancel [Previous](#) [Next](#)

Mount targets

A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone	Subnet ID	IP address	Security groups
us-east-1a	subnet-0e172d55c0ef... ▲	Automatic	Choose security groups Remove sg-0cdc71d5a3b1333ab X efs-sg-wordpress
us-east-1b	subnet-0e172d55c0ef0c97f	10.55.128.0/20 ✓	Choose security groups Remove sg-0cdc71d5a3b1333ab X efs-sg-wordpress

Subnets (2/10) [Info](#)

Find subnets by attribute or tag

<input type="checkbox"/>	Name	▼	Subnet ID
<input type="checkbox"/>	wordpress-vpc-subnet-public2-us-east-1b		subnet-0fe83451953348f3e
<input type="checkbox"/>	wordpress-vpc-subnet-public1-us-east-1a		subnet-071e88e497dd3b0e0
<input checked="" type="checkbox"/>	wordpress-vpc-subnet-private2-us-east...		subnet-04d41282c2e50f188
<input checked="" type="checkbox"/>	wordpress-vpc-subnet-private1-us-east...		subnet-0e172d55c0ef0c97f

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

 **Success!**
File system (fs-04f7a4e6a26938ff9) is available.

Amazon EFS > File systems > fs-04f7a4e6a26938ff9

efs-wordpress (fs-04f7a4e6a26938ff9)

[Delete](#) [Attach](#) [Edit](#)

General	
Amazon resource name (ARN)	arn:aws:elasticfilesystem:us-east-1:717850616230:file-system/fs-04f7a4e6a26938ff9
Performance mode	General Purpose
Throughput mode	Elastic
Lifecycle management	Transition into Infrequent Access (IA): None Transition into Archive: None Transition into Standard: None
Availability zone	Regional
Automatic backups	<input checked="" type="radio"/> Disabled
Encrypted	ec1ef08f-7979-4481-aed2-39900ea78275 (aws/elasticfilesystem)
File system state	 Available
DNS name	No mount targets available
Replication overwrite protection	 Enabled

Attach

Mount your Amazon EFS file system on a Linux instance. [Learn more](#)

Mount via DNS Mount via IP

Using the EFS mount helper:

```
 sudo mount -t efs -o tls fs-04f7a4e6a26938ff9:/ efs
```

Using the NFS client:

```
 sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-04f7a4e6a26938ff9.efs.us-east-1.amazonaws.com /efs
```

See our user guide for more information. [Learn more](#)

[Close](#)

COPY dns name

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

General

Amazon resource name (ARN)

 arn:aws:elasticfilesystem:us-east-1:717850616230:file-system/fs-04f7a4e6a26938ff9

Performance mode

General Purpose

Throughput mode

Elastic

Lifecycle management

Transition into Infrequent Access (IA): 30 day(s) since last access

Transition into Archive: 90 day(s) since last access

Transition into Standard: None

Availability zone

Regional

Automatic backups

 Enabled

Encrypted

ec1ef08f-7979-4481-aed2-39900ea78275 (aws/elasticfilesystem)

File system state

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

Replication overwrite protection

 Enabled**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 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.

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

Description

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.

4 Subnets, 2 Availability Zones

Add subnets

Availability Zones

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

Subnets

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

 Subnet ID: subnet-0e172d55c0ef0c97f CIDR: 10.55.128.0/20

 Subnet ID: subnet-04d41282c2e50f188 CIDR: 10.55.144.0/20

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

i Successfully created rds-subnetgroup. [View subnet group](#)

Subnet groups (1)

<input type="checkbox"/>	Name	Description	Status	VPC
<input type="checkbox"/>	rds-subnetgroup	ponerlas en la subnet privadas	Complete	vpc-02c7e9d631ec5a2ab

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

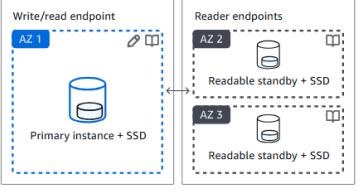
Deployment options [Info](#)

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

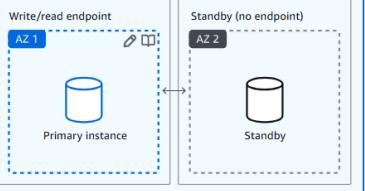
Reader endpoints
AZ 2
Readable standby + SSD

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



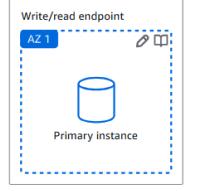
Write/read endpoint
AZ 1
Primary instance

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.

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.

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 have RDS generate one for you.

- 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 limited by the selected instance class.

DB instance class | [Info](#)

▼ Hide filters

- Show instance classes that support Amazon RDS Optimized Writes (includes db.t3 classes)
Amazon RDS Optimized Writes improves write throughput and performance for Amazon RDS for MySQL, PostgreSQL, Oracle Database, and Amazon Aurora.
- 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 so that your database can communicate with the compute resource.

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 both IPv4 and IPv6 addressing protocols.

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 can connect to the database through 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 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 traffic from the VPC.

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

Backup replication [Info](#)

Enable replication in another AWS Region
Enabling replication automatically creates backups of your DB instance in the selected Region, for disaster recovery, in addition to the current Region.

Destination Region

US West (Oregon) [▼](#)

Automated backups will be continuously replicated into another Region where they can be restored.

Replicated backup retention period [Info](#)
Choose the number of days that RDS should retain automatic backups for this instance in the destination Region.

7 days [▼](#)

AWS KMS key [Info](#)

Enter a key ARN [▼](#)

Amazon Resource Name (ARN)

[▼](#)
Example: arn:aws:kms:<region>:<accountID>:key/<key-id>

Account
None

KMS key ID
None

Encryption

Enable encryption
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

[AWS KMS](#) [▼](#)

 **Your request to create DB instance wordpress-db didn't work.**
A MonitoringRoleARN value is required if you specify a MonitoringInterval value other than 0.

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.

▼ Additional monitoring settings

Enhanced Monitoring, CloudWatch Logs and DevOps Guru

Enhanced Monitoring

Enable Enhanced monitoring

Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or th

Log exports

Select the log types to publish to Amazon CloudWatch Logs

Audit log

Error log

General log

iam-db-auth-error log

Slow query log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

 Your request to create DB instance wordpress-db didn't work.

The specified KMS key does not exist, is not enabled or you do not have permissions to access it.

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.

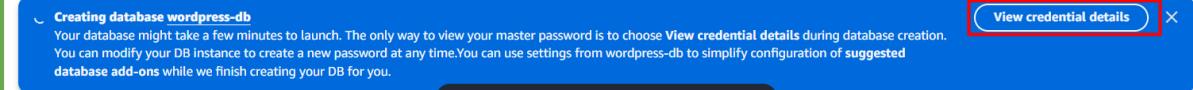
La encriptación de la base de datos es una característica adicional que aumenta la seguridad al cifrar los datos en reposo. Sin embargo, no es estrictamente necesaria para el funcionamiento básico de WordPress.

Si queremos implementar encriptación en el futuro, podremos hacerlo cuando tengamos acceso completo a IAM y KMS.

Encryption

Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list below.



Databases (1)

DB identifier	Status	Role	Engine	Region ...	Size	Recommendations	CPU
wordpress-db	Creating	Instance	MySQL Co...	us-east-1b	db.t3.micro	-	-

Connection details to your database wordpress-db

This is the only time you can view this password. Copy and save the password for your reference. If you lose the password, you must modify your database to change it. You can use a SQL client application or utility to connect to your database.

[Learn about connecting to your database](#)

Master username

 Master password copied

 [Copy password](#)

[Close](#)

Copy password

Connection details to your database wordpress-db X

This is the only time you can view this password. Copy and save the password for your reference. If you lose the password, you must modify your database to change it. You can use a SQL client application or utility to connect to your database.

[Learn about connecting to your database](#) 

Master username

 Master password copied

 [Copy password](#)

 ****

[Close](#)

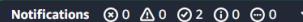
RDS PASSWORD

rtPsvolOgO7Ar8KV4oYy

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

⌚ Successfully created database [wordpress-db](#)
[View connection details](#) 

RDS has generated your database master password during the database creation and it will be displayed in the connection details. The only way to view your master password is to choose [View connection details](#) during database creation. You can modify your DB instance to create a new password at any time.
 You can use settings from [wordpress-db](#) to simplify configuration of [suggested database add-ons](#) while we finish creating your DB for you.

Notifications  0 0 2 0 0
[View connection details](#) 

wordpress-db 🕒 Modify Actions ▾

Summary				
DB identifier wordpress-db	Status  Modifying	Role Instance	Engine MySQL Community	Recommendations
CPU  0.01%	Class db.t3.micro	Current activity  0 Connections	Region & AZ us-east-1b	

- [Connectivity & security](#) ◀
- [Monitoring](#)
- [Logs & events](#)
- [Configuration](#)
- [Zero-ETL integrations](#)
- [Maintenance & backups](#)
- [Data migrations - n](#) ▶

Connectivity & security

Endpoint & port  wordpress-db.c5y99z4gvpom.us-east-1.rds.amazonaws.com	Networking Availability Zone us-east-1b VPC	Security VPC security groups rds-sg-wordpress (sg-0064e77c4e394574e)  Active
---	---	---

Copiamos el endpoint:

25 de 70

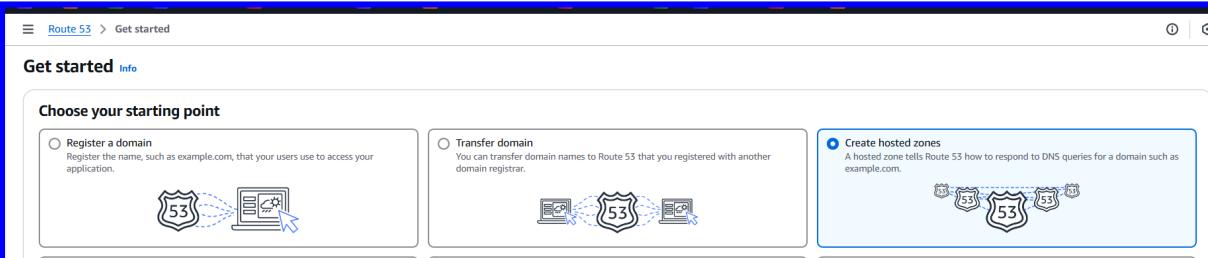
RDS ENDPOINT

wordpress-db.c5y99z4gpom.us-east-1.rds.amazonaws.com

Fase 3: Balanceador de carga

3.1. Crear certificado SSL

CREAR HOSTED ZONE en ROUTE 53



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.
 Valid characters: a-z, 0-9, ! " # \$ % & ' () * + , - / ; < = > ? @ [\] ^ _ ` { | } . ~

Description - optional Info
 This value lets you distinguish hosted zones that have the same name.

 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.

blog.karura.cat 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.

Hosted zone details

Records (2) DNSSEC signing Hosted zone tags (0)

Records (1/2) Info

The following table lists the existing records in blog.karura.cat. You can't delete the SOA record or the NS record named blog.karura.cat.

Record ...	Type	Routing p...	Differ...	Alias	Value/Route traffic to	TTL (s.)
<input checked="" type="checkbox"/> blog.karur...	NS	Simple	-	No	ns-214.awsdns-26.com. ns-997.awsdns-60.net. ns-1867.awsdns-41.co.uk. ns-1209.awsdns-23.org.	172800
<input type="checkbox"/> blog.karur...	SOA	Simple	-	No	ns-214.awsdns-26.com. awsd...	900

Record details

Copy

- ns-214.awsdns-26.com.
- ns-997.awsdns-60.net.
- ns-1867.awsdns-41.co.uk.
- ns-1209.awsdns-23.org.

Alias
No

TTL (seconds)
172800

Routing policy
Simple

Records (2) DNSSEC signing Hosted zone tags (0)

Records (1/2) Info

The following table lists the existing records in blog.karura.cat. You can't delete the SOA record or the NS record named blog.karura.cat.

Record ...	Type	Routing p...	Differ...	Alias	Value/Route traffic to	TTL (s.)
<input type="checkbox"/> blog.karur...	NS	Simple	-	No	ns-214.awsdns-26.com. ns-997.awsdns-60.net. ns-1867.awsdns-41.co.uk. ns-1209.awsdns-23.org.	172800
<input checked="" type="checkbox"/> blog.karur...	SOA	Simple	-	No	ns-214.awsdns-26.com. awsd...	900

Copy

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

Alias
No

TTL (seconds)
900

Routing policy
Simple

COPY SOA ns-214.awsdns-26.com

[ns-214.awsdns-26.com](#). awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

CLOUDFLARE

<input type="checkbox"/>	NS	blog	ns-214.awsdns-26.com	DNS only	Auto	Edit
--------------------------	----	------	----------------------	----------	------	----------------------

Comprobación:

<https://www.digui.com/>

DIG GUI

DIG Web Interface

Dig Command Manual

Record type
Tips
Restore Default

NS
 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

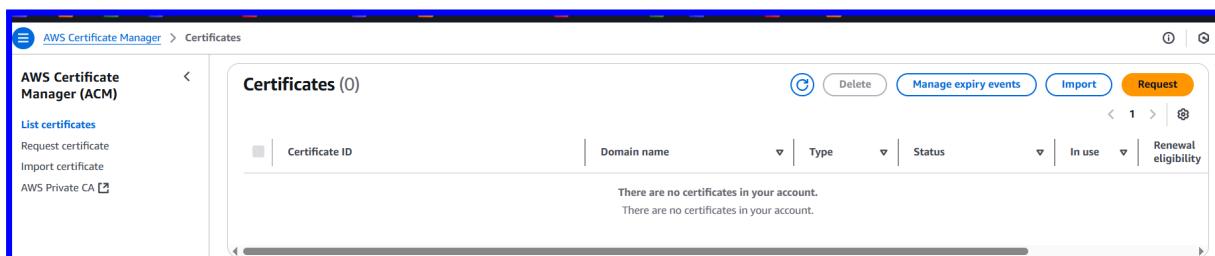
```
; <>> DiG diggui.com <>> @8.8.8.8 blog.karura.cat NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 574
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; 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



Certificate ID	Domain name	Type	Status	In use	Renewal eligibility

Request

Request certificate

Certificate type [Info](#)

ACM certificates can be used to establish secure communication.

Request a public certificate

Request a public SSL/TLS certificate from Amazon. By default, ACM certificates are issued for up to 3 years.

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

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 your domain.

Email validation

Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for your domain.

Key algorithm Info

Select an encryption algorithm. Some algorithms may not be supported by all certificate providers.

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 cb178282-e871-4402-9565-78d8bf950240
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](#)

cb178282-e871-4402-9565-78d8bf950240

[Delete](#)

Certificate status

Identifier
cb178282-e871-4402-9565-78d8bf950240

Status

ⓘ Pending validation [Info](#)

ARN

📘 arn:aws:acm:us-east-1:717850616230:certificate/cb178282-e871-4402-9565-78d8bf950240

Type

Amazon Issued

Domains (1)

[Create records in Route 53](#)
[Export to CSV](#)

< 1 >

Domain	Status	Renewal status	Type	CNAME name
blog.karura.cat	<small>ⓘ</small> Pending validation	-	CNAME	<small>📘</small> _3cc5e3dcdccceed8c086ebb1b96c053fb.blog.karura.cat.

Validar el certificado:

Domains (1)

Domain	Status	Renewal status	Type	CNAME name
blog.karura.cat	Pending validation	-	CNAME	_3cc5e3dcdceed8c086ebb1b96c053fb.blog.karura.cat.

Create records in Route 53 **Export to CSV**

Create DNS records in Amazon Route 53 (1/1)

Domain	Validation status	Is domain in Route 53?
blog.karura.cat	Pending validation	Yes

Create records

Records (3) Info

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

Record ...	Type	Routing p...	Alias	Value/Route traffic to	TTL (s.)
blog.karur...	NS	Simple	-	ns-214.awsdns-26.com. ns-997.awsdns-60.net. ns-1867.awsdns-41.co.uk. ns-1209.awsdns-23.org.	172800
blog.karur...	SOA	Simple	-	ns-214.awsdns-26.com. awsd...	900
_3cc5e3d...	CNAME	Simple	-	_21600bd35dbf427a6dcada...	300

Comprobación:

Certificate status

Identifier cb178282-e871-4402-9565-78d8bf950240	Status Issued
ARN arn:aws:acm:us-east-1:717850616230:certificate/cb178282-e871-4402-9565-78d8bf950240	
Type Amazon Issued	

Domains (1)

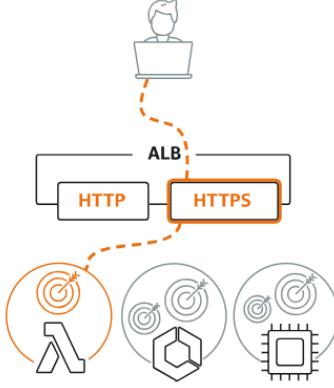
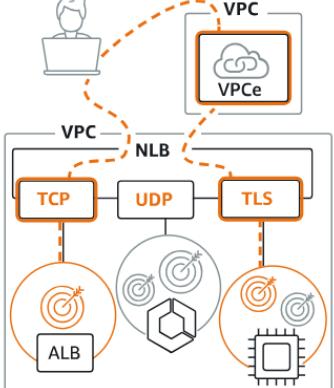
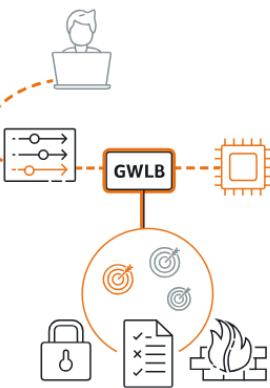
Domain	Status	Renewal status	Type
blog.karura.cat	Success	-	CNAME

3.2. Crear Application Load Balancer

EC2 > Load balancers > Compare and select load balancer type

Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types	Application Load Balancer	Network Load Balancer	Gateway Load Balancer
Application Load Balancer Info	 <p>Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.</p> <p>Create</p>	 <p>Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.</p> <p>Create</p>	 <p>Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.</p> <p>Create</p>

Basic configuration

Load balancer name

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

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

- 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 to the load balancer will be displayed below.

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-facing and VPC endpoints.

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-vpn
vpc-02c7e9d631e5a2ab
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.

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

Select up to 5 security groups

alb-sg-wordpress

sg-0083b38f9abdf04dd VPC: vpc-02c7e9d631ec5a2ab



Listeners and routing [Info](#)

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

▼ Listener HTTP:80

Protocol	Port
HTTP	: 80 1-65535

Default action | [Info](#)

Forward to	Select a target group
Create target group	



Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

[Add listener](#)

TARGET GROUP

Step 1
 Specify group details
 Step 2
 Register targets

Specify group details
 Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration
 Settings in this section can't be changed after the target group is created.

Choose a target type

Instances
 • Supports load balancing to instances within a specific VPC.
 • Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses
 • Supports load balancing to VPC and on-premises resources.

Target group name

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

Protocol : Port
 Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets an group is created. This choice cannot be changed after creation

<input type="text" value="HTTP"/>	<input type="text" value="80"/>
	1-65535

IP address type
 Only targets with the indicated IP address type can be registered to this target group.

IPv4
 Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

IPv6
 Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC

wordpress-tg

Details
[arn:aws:elasticloadbalancing:us-east-1:717850616230:targetgroup/wordpress-tg/300a57022f453b5a](#)

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-02c7e9d631ec5a2ab
IP address type IPv4	Load balancer None associated		
0 Total targets	<input checked="" type="radio"/> 0 Healthy	<input checked="" type="radio"/> 0 Unhealthy	<input type="radio"/> 0 Unused
	<input type="radio"/> 0 Anomalous	<input type="radio"/> 0 Initial	<input type="radio"/> 0 Draining

Targets **Monitoring** **Health checks** **Attributes** **Tags**

Registered targets (0) [Info](#) [Anomaly mitigation: Not applicable](#) [Deregister](#) [Register targets](#)

No registered targets
 You have not registered targets to this group yet

Seguimos con alb

Default action | [Info](#)

Forward to	Select a target group	▼
Create target group		

es so you can more easily manage them.

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer route

▼ Listener HTTP:80

Protocol	Port	Default action		Info
HTTP	: 80 1-65535	Forward to	wordpress-tg	HTTP
Create target group				

▼ Listener HTTPS:443

Protocol	Port	Default action		Info
HTTPS	: 443 1-65535	Forward to	wordpress-tg	HTTP
Create target group				

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

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	Policy name
All security policies	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

<input checked="" type="radio"/> From ACM	<input type="radio"/> From IAM	<input type="radio"/> 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
Scheme Internet-facing	Hosted zone Z35SXDOTRQ7X7K
VPC vpc-02c7e9d631ec5a2ab	Load balancer IP address type IPv4
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 arnaws:elasticloadbalancing:us-east-1:717850616230:loadbalancer/app/alb-wordpress/861e6338b23577a2	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

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched across multiple regions and accounts.

Launch template name and description

Launch template name - *required*

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '!', '@'.

Template version description

Max 255 chars

Auto Scaling guidance | [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

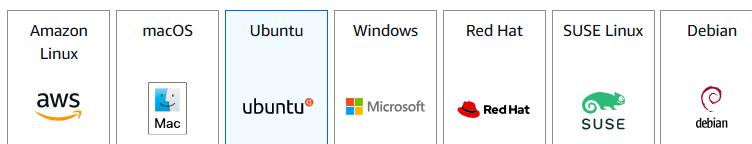
Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▼ Application and OS Images (Amazon Machine Image) - required [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Quick Start



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-084568db4383264d4 (64-bit (x86)) / ami-0c4e709339fa8521a (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture

64-bit (x86) ▾

AMI ID

ami-084568db4383264d4

Publish Date

2025-03-05

Username | [i](#)

ubuntu

Verified provider

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

vockey

 Create new key pair**▼ Network settings [Info](#)****Subnet [Info](#)**

Don't include in launch template

 Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

 Select existing security group Create security group**Security groups [Info](#)**

Select security groups

 Compare security group ruleswebserver-sg-wordpress sg-0765f332c0af98403 

VPC: vpc-02c7e9d631ec5a2ab

► Advanced network configuration**▼ Advanced details [Info](#)****IAM instance profile [Info](#)**

LabInstanceProfile

arn:aws:iam::717850616230:instance-profile/LabInstanceProfile

Detailed CloudWatch monitoring [Info](#)

Enable

Additional charges apply

```
#!/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-XXXXXXXXXXXXXX.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="rtPsvol0g07Ar8KV4oYy"
DB_HOST="wordpress-db.c5y99z4gpom.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

```

Launch Templates (1) Info						
<input type="checkbox"/>	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
<input type="checkbox"/>	lt-06066e77855337beb	wordpress-launch-template	1	1	2025-04-27T17:36:04.000Z	arn:aws:sts::717850616230:ass...

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.

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.

[Create a launch template](#)

Version

[Create a launch template version](#)

Description

a prod webserver for myapp

AMI ID

ami-084568db4383264d4

Key pair name

vockey

Launch template

[wordpress-launch-template](#)

lt-06066e77855337beb

Security groups

-

Security group IDs

[sg-0765f332c0af98403](#)

Instance type

t2.micro

Request Spot Instances

No

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 zonal 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](#) 

X

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.

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.



Desired capacity

Specify your group size.

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

Equal or less than desired capacity

Max desired capacity

Equal or greater than desired capacity

Automatic scaling - optional

Choose whether to use a target tracking policy | [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name
testpolicy

Metric type | [Info](#)
Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization

Target value
50

Instance warmup | [Info](#)
300 seconds

Disable scale in to create only a scale-out policy

Additional settings

Instance scale-in protection
If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

Enable instance scale-in protection

Monitoring | [Info](#)
 Enable group metrics collection within CloudWatch

Default instance warmup | [Info](#)
The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

Enable default instance warmup

[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

wordpress-tg Actions ▾

Details
arn:aws:elasticloadbalancing:us-east-1:717850616230:targetgroup/wordpress-tg/300a57022f453b5a

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-02c7e9d631ec5a2ab
IP address type IPv4	Load balancer alb-wordpress		
2 Total targets	2 Healthy	0 Unhealthy	0 Unused
	0 Anomalous	0 Initial	0 Draining

Distribution of targets by Availability Zone (AZ)
Select values in this table to see corresponding filters applied to the Registered targets table below.

[Targets](#) [Monitoring](#) [Health checks](#) [Attributes](#) [Tags](#)

Registered targets (2) [Info](#) Anomaly mitigation: Not applicable [Deregister](#) [Register targets](#)

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Instance ID	Name	Port	Zone	Health status	Health status details	Admini...	Overri...	Laun...
i-0b51544f52cedd443		80	us-east-1a (us...)	Healthy	-	<input type="radio"/> No override.	<input type="radio"/> No overri...	April 3
i-00e6ccb2f91e0f7a0		80	us-east-1b (us...)	Healthy	-	<input type="radio"/> No override.	<input type="radio"/> No overri...	April 3

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

Record name Info .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

Value Info

TTL (seconds) Info 1m 1h 1d Recommended values: 60 to 172800 (two days)

Routing policy Info

Add another record Add another record

Create records Create records

AWS Certificate Manager > Certificates > Request certificate > Request public certificate

Fully qualified domain name Info

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.

cac54f7e-a13d-4a3b-8481-5b7dc81df17f

[View certificate](#) [Delete](#)

Certificate status

Identifier	Status
cac54f7e-a13d-4a3b-8481-5b7dc81df17f	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](#)

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

Create DNS records in Amazon Route 53 (1/1)

[View certificate](#) [X](#)

1 match

Validation status = Pending validation Validation status = Failed Is domain in Route 53? = Yes Clear filters

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](#)

< 1 >

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

EDITAMOS

Listeners and rules (2) [Info](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

<input type="checkbox"/>	Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate
<input type="checkbox"/>	HTTPS:443	Forward to target group <ul style="list-style-type: none"> wordpress-tg [?]: 1 (100%) Target group stickiness: Off 	1 rule	ARN	ELBSecurityPolicy-TLS13-1-2...	blog.karura.cat (Certificate ID: ...)
<input type="checkbox"/>	HTTP:80	Forward to target group <ul style="list-style-type: none"> wordpress-tg [?]: 1 (100%) Target group stickiness: Off 	1 rule	ARN	Not applicable	Not applicable

Secure listener settings [Info](#)

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	Policy name
All security policies	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), or a custom provider.

Certificate source

From ACM [\[?\]](#) From IAM [\[?\]](#)

Certificate (from ACM)
The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

www.blog.karura.cat cac54f7e-a13d-4a3b-8481-5b7dc81df17f	[?] 
---	---

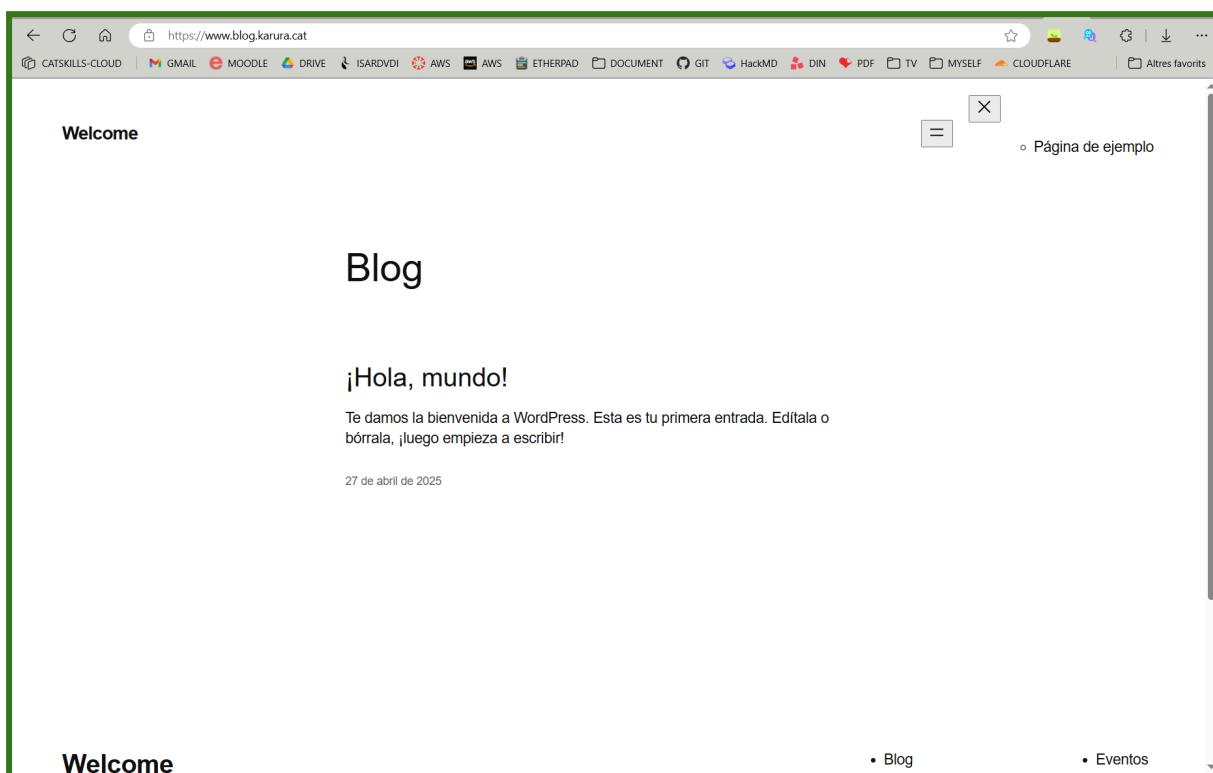
[Request new ACM certificate](#) [\[?\]](#)

www.blog.karura.cat



The screenshot shows a web browser window displaying the Apache2 Default Page from an Ubuntu system. The page includes the Ubuntu logo, a "It works!" button, and a section titled "Configuration Overview" detailing the file structure of /etc/apache2/.

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|   |-- mods-enabled
|       |-- *.Load
|       |-- *.conf
```



The screenshot shows a web browser window displaying a WordPress blog post. The post is titled "Blog" and contains the text "¡Hola, mundo!". It also includes a welcome message and a timestamp of "27 de abril de 2025".

Welcome

Blog

¡Hola, mundo!

Te damos la bienvenida a WordPress. Esta es tu primera entrada. Editala 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

New distribution 1

SSL/TLS certificate - optional

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.c5y99z4gpom.us-east-1.rds.amazonaws.com > wordpressdb.sql
```

```
rtPsvolOgO7Ar8KV4oYy  
mysql -u admin -p -h wordpress-db.c5y99z4gpom.us-east-1.rds.amazonaws.com
```

```
mysqldump -u admin -p wordpress -prtPsvolOgO7Ar8KV4oYy -h  
wordpress-db.c5y99z4gpom.us-east-1.rds.amazonaws.com > wordpressdb.sql
```

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

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

```
$ aws s3 ls  
2025-04-27 20:29:22 aws-butcket-01  
$ aws s3 cp wordpressdb.sql s3://aws-butcket-01/  
upload: ./wordpressdb.sql to s3://aws-butcket-01/wordpressdb.sql  
$ aws s3 ls s3://aws-butcket-01/  
      PRE assets/  
      PRE images/  
2025-04-27 20:39:47      17128 LICENSE.txt  
2025-04-27 20:39:47      13291 README.txt  
2025-04-27 20:39:48      18453 index.html  
2025-04-27 21:41:53      174997 wordpressdb.sql  
$
```

```
$ mysqldump -u admin -p wordpress -prtPsvolOgO7Ar8KV4oYy -h wordpress-db.c5y99z4gpom.us-east-1.rds.amazonaws.com > wordpressdb.sql  
mysqldump: [Warning] Using a password on the command line interface can be insecure.  
Warning: A partial dump from a server that has GTIDs will by default include the GTIDs of all transactions, even those that changed state to restore GTIDs, pass --set-gtid-purged=OFF. To make a complete dump, pass --all-databases --triggers --routines --events.  
Warning: A dump from a server that has GTIDs enabled will by default include the GTIDs of all transactions, even those that were executed in the dumped data. This might result in an inconsistent data dump.  
In order to ensure a consistent backup of the database, pass --single-transaction or --lock-all-tables or --master-data.  
$ ls  
snap wordpressdb.sql  
$ cat wordpressdb.sql  
-- MySQL dump 10.13 Distrib 8.0.41, for Linux (x86_64)  
--  
-- Host: wordpress-db.c5y99z4gpom.us-east-1.rds.amazonaws.com Database: wordpress
```

aws-butcket-01 [Info](#)

[Objects](#) [Metadata](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (6) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	assets/	Folder	-	-	-
<input type="checkbox"/>	images/	Folder	-	-	-
<input type="checkbox"/>	index.html	html	April 27, 2025, 22:39:48 (UTC+02:00)	18.0 KB	Standard
<input type="checkbox"/>	LICENSE.txt	txt	April 27, 2025, 22:39:47 (UTC+02:00)	16.7 KB	Standard
<input type="checkbox"/>	README.txt	txt	April 27, 2025, 22:39:47 (UTC+02:00)	13.0 KB	Standard
<input type="checkbox"/>	wordpressdb.sql	sql	April 27, 2025, 23:41:53 (UTC+02:00)	170.9 KB	Standard

```
$ aws s3 ls s3://aws-butcket-01/
                           PRE assets/
                           PRE images/
2025-04-27 20:39:47      17128 LICENSE.txt
2025-04-27 20:39:47      13291 README.txt
2025-04-27 20:39:48      18453 index.html
2025-04-27 21:41:53     174997 wordpressdb.sql
$
```

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"

☰ [CloudWatch](#) > Dashboards

[Custom dashboards](#) | [Automatic dashboards](#)

Custom Dashboards (0) [Info](#)

Filter dashboards

| Name

▼ | Sharing

| Favorite

No dashboards

You have not created any dashboards.

[Read more about Dashboards](#)

[Create dashboard](#)

Create new dashboard

X

Dashboard name

dashboard-wordpress

Valid characters in dashboard names include "0-9A-Za-z-_".

[Cancel](#)

[Create dashboard](#)

Add widget

X

Data sources types

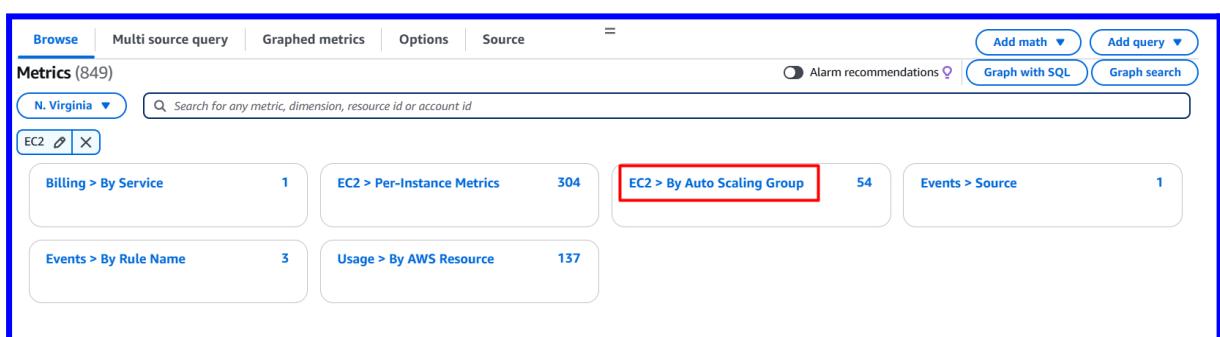
- Cloudwatch
- Other content types
- Create data sources

Widget Configuration
Data type
Metrics Logs Alarms
Widget type

- | | |
|--|--|
| <input type="radio"/> Line
Compare metrics over time  | <input type="radio"/> Data table
Compare metrics values over time in a table  |
| <input type="radio"/> Number
Instantly see the latest value for a metric  | <input type="radio"/> Gauge
See the latest value of a metric within a range  |
| <input type="radio"/> Stacked area
Compare the total over time  | <input checked="" type="radio"/> Bar
Compare categories of data  |
| <input type="radio"/> Pie
Show percentage or proportional data  | <input type="radio"/> Explorer
A single widget with multiple tag-based graphs  |

Cancel

Next



The screenshot shows the AWS CloudWatch Metrics search interface. At the top, there are tabs for 'Browse', 'Multi source query', 'Graphed metrics', 'Options', and 'Source'. Below these are buttons for 'Add math' and 'Add query'. On the right, there are buttons for 'Alarm recommendations', 'Graph with SQL', and 'Graph search'. The main area is titled 'Metrics (849)' and shows a search bar with 'N. Virginia' selected. Below the search bar, there are several metric filters: 'EC2' (selected), 'Billing > By Service' (1), 'EC2 > Per-Instance Metrics' (304), 'EC2 > By Auto Scaling Group' (54) which is highlighted with a red border, 'Events > Source' (1), 'Events > By Rule Name' (3), and 'Usage > By AWS Resource' (137).

<input checked="" type="checkbox"/>	test5	NetworkIn ⓘ	No alarms
<input checked="" type="checkbox"/>	test5	NetworkOut ⓘ	No alarms
<input checked="" type="checkbox"/>	test5	CPUUtilization ⓘ	No alarms
<input type="checkbox"/>	test5	EBSReadOps ⓘ	No alarms

<input checked="" type="checkbox"/> test5	StatusCheckFailed ⓘ	No alarms
<input type="checkbox"/> test5	StatusCheckFailed_System ⓘ	No alarms
<input checked="" type="checkbox"/> test5	StatusCheckFailed_Instance ⓘ	No alarms
<input type="checkbox"/> testfinal	FPCWriteRouter ⓘ	No alarms

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

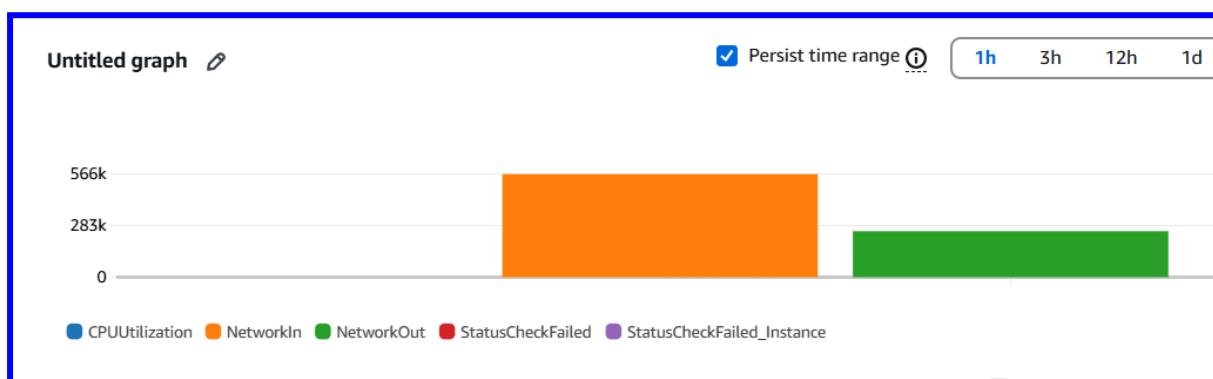
Persist time range ⓘ 1h 3h 12h 1d 3d 1w Custom (5m) UTC timezone Bar

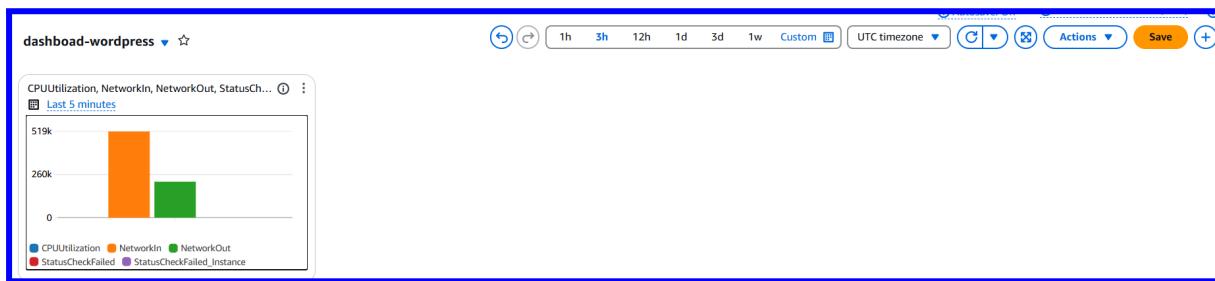
Absolute Relative

Minutes	1	3	5	15	30	45
Hours	1	2	3	6	8	12
Days	1	2	3	4	5	6
Weeks	1	2	3	4	5	6
Months	3	6	12	15		

Duration Unit of time
 Minutes
 Up to 4 digits.

Clear Cancel Apply





Para el Load Balancer (ALB):

Añade otro widget

Busca "ApplicationELB" > "Por balanceador de carga"

Selecciona:

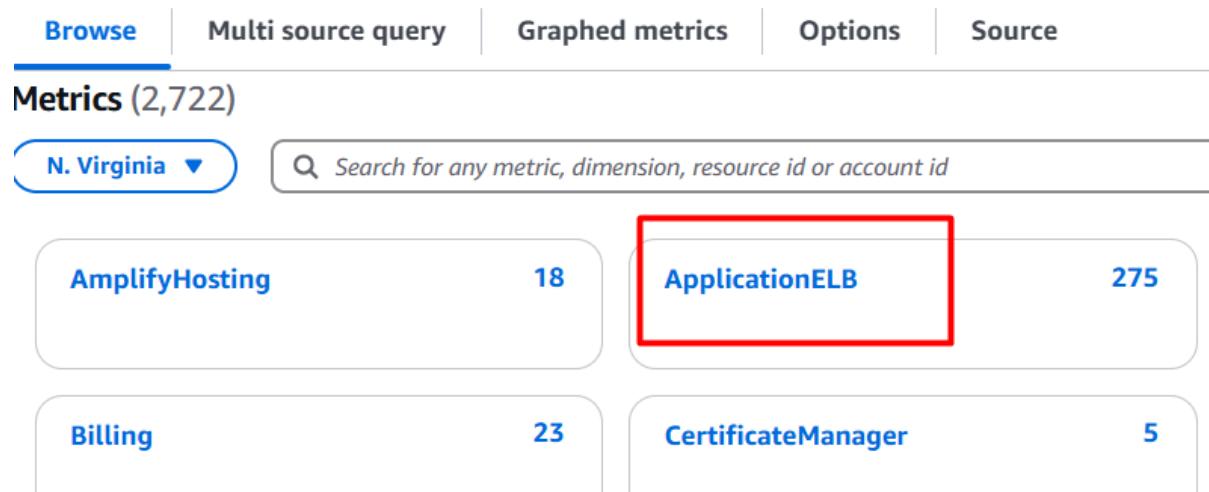
RequestCount (solicitudes totales)

HTTPCode_Target_2XX_Count (respuestas exitosas)

HTTPCode_Target_5XX_Count (errores del servidor)

TargetResponseTime (tiempo de respuesta)

Haz clic en "Create widget"



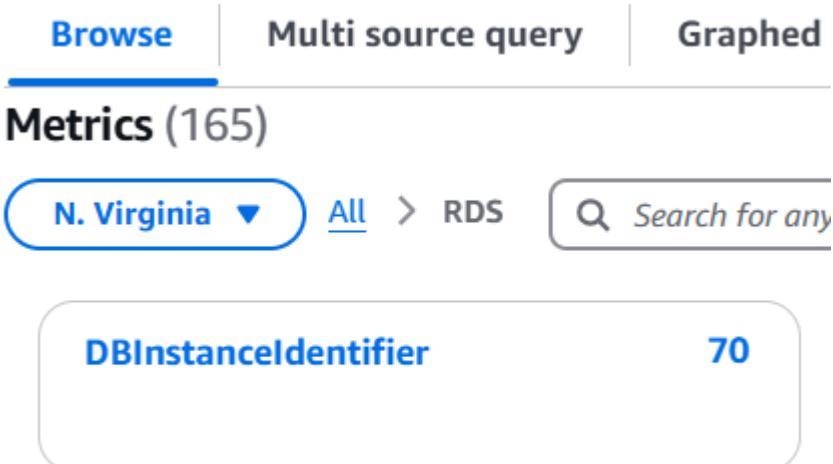
Service	Metric Count
AmplifyHosting	18
ApplicationELB	275
Billing	23
CertificateManager	5

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"

File System Metrics

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"**

- 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 ▾
<input type="checkbox"/> test5		EBSIOBalance%			No alarms		
<input type="checkbox"/> test5		EBSIOBalance%			No alarms		
<input checked="" type="checkbox"/> test5		CPUUtilization			No alarms		
<input type="checkbox"/> test5		NetworkPacketsIn			No alarms		
<input type="checkbox"/> test5		NetworkPacketsOut			No alarms		
<input type="checkbox"/> test5		CPUCreditBalance			No alarms		
<input type="checkbox"/> test5		CPUSurplusCreditsCharged			No alarms		
<input type="checkbox"/> test5		CPUCreditUsage			No alarms		
<input type="checkbox"/> test5		CPUSurplusCreditBalance			No alarms		
<input type="checkbox"/> test5		StatusCheckFailed			No alarms		
<input type="checkbox"/> test5		StatusCheckFailed_System			No alarms		
<input type="checkbox"/> test5		StatusCheckFailed_Instance			No alarms		

[Cancel](#) [Select metric](#)

Namespace

AWS/EC2

Metric name

CPUUtilization

AutoScalingGroupName

test5

Statistic Average X**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.

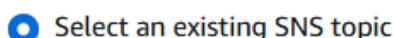


OK

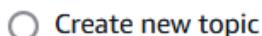
The metric or expression is w

Send a notification to the following SNS topic

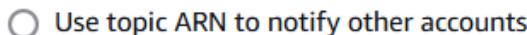
Define the SNS (Simple Notification Service) topic that will receive the notification.



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 minuts)

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



Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:us-east-1:717850616230:WordPress-High-CPU:190d20a0-13d0-4970-b2cf-6512a25f00f3

If it was not your intention to subscribe, [click here to unsubscribe](#).

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



Browse	Multi source query	Graphed metrics (1)	Options	Source
<input type="checkbox"/> test5		StatusCheckFailed_Instance ⓘ		No alarms
<input type="checkbox"/> test5		EBSReadOps ⓘ		No alarms
<input type="checkbox"/> test5		EBSWriteOps ⓘ		No alarms
<input type="checkbox"/> test5		EBSReadBytes ⓘ		No alarms
<input type="checkbox"/> test5		EBSWriteBytes ⓘ		No alarms
<input type="checkbox"/> test5		MetadataNoTokenRejected ⓘ		No alarms
<input checked="" type="checkbox"/> test5		CPUUtilization ⓘ		1 alarm(s)
<input type="checkbox"/> testfinal		CPUUtilization ⓘ		No alarms

```

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

```

Instances (3) Info							
Last updated less than a minute ago Connect Instance state Actions Launch instances							
Find Instance by attribute or tag (case-sensitive) All states							
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
weserver	i-0345bb6e7af6b4faf	Running Q Q	t2.micro	2/2 checks passed View alarms +	us-east-1a	-	-
webserver	i-0c678ff39d0c75497	Running Q Q	t2.micro	2/2 checks passed View alarms +	us-east-1b	-	-
	i-08282ebca9069e563	Running Q Q	t2.micro	2/2 checks passed View alarms +	us-east-1b	-	-

Instala 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
