

INFORME TÉCNICO – MIGRACIÓN A LA NUBE DE LA EMPRESA ABC

Portada

Título: Simulación de migración segura a la nube – Caso práctico empresa ABC

Alumno: Sergio Carretero Otero

Fecha: 19 de julio de 2025

Plataforma: Amazon Web Services (AWS) – Capa gratuita

Tecnologías utilizadas: EC2, RDS, VPC, Security Groups, PostgreSQL, SSL/TLS

Introducción

La transformación digital y la necesidad de garantizar alta disponibilidad, escalabilidad y seguridad de los servicios tecnológicos han llevado a las empresas a adoptar soluciones en la nube. Este informe documenta el proceso de simulación de migración de la empresa bancaria ficticia ABC, que actualmente opera sobre infraestructura local con dos centros de datos redundantes, hacia la nube pública de Amazon Web Services (AWS). Se cubren los criterios de selección del proveedor, la arquitectura de red propuesta, la configuración de seguridad aplicada, la conexión entre servicios y el cumplimiento normativo de las normas ISO/IEC 27017 y 27018.

1. Elección del proveedor de nube

Se ha seleccionado **Amazon Web Services (AWS)** por su liderazgo en el mercado, cumplimiento normativo, servicios avanzados y opciones gratuitas para entornos de prueba. Los principales motivos son:

- Alta disponibilidad y redundancia regional.
- Certificaciones de seguridad internacional (ISO 27001, 27017, 27018).
- Escalabilidad vertical y horizontal bajo demanda.
- Amplio ecosistema de servicios compatibles.

- Capacidad de monitoreo, cifrado y auditoría avanzada.
 - Disponibilidad de una **capa gratuita**, útil para simulaciones académicas y de laboratorio.
-

2. Mapa de red y componentes de seguridad

La arquitectura diseñada incluye:

- Una instancia EC2 (Ubuntu 22.04) actuando como cliente.
- Una instancia RDS (PostgreSQL) alojando una base de datos.
- Una VPC compartida entre ambas instancias para garantizar aislamiento.
- Grupos de seguridad configurados para permitir únicamente el tráfico necesario.
- Comunicación cifrada entre cliente y base de datos a través de SSL/TLS.

 Colocar aquí la captura **1.1.png** (Grupo de seguridad de EC2)

 Colocar aquí la captura **1.2.png** (Grupo de seguridad de RDS)

3. Simulación de funcionamiento y controles

3.1. Creación de instancia EC2

Se lanzó una máquina virtual EC2 con Ubuntu desde la consola de AWS, asignándole una IP pública para conexión remota. Se habilitó el puerto 22 (SSH)

aws

Search

[Alt+S]

Europe (Stockholm)

sercao2023

EC2 > Instances > Launch an instance

Name and tags

Info

Name

ServidorABC

Add additional tags

Application and OS Images (Amazon Machine Image)

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

Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

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-042b4708b1d05f512 (64-bit (x86)) / ami-0969826571f0530f7 (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

EC2 > Instances > Launch an instance

▼ 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 - *required*

clave-servidorABC

Create new key pair

▼ Network settings Info

Network Info

vpc-00d4cc88fa42864f4

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

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.

Create security group

Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

My IP

79.116.251.184/32

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

EC2 > Instances

EC2

Dashboard

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Instances (1/2) 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	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/> ServidorABC	i-0fd8f9491845c05b5	Running	t3.micro	Initializing	View alarms +	eu-north-1b	ec2-16-171-174-243.eu...	16.171.174.243	-
<input type="checkbox"/> servidor-web	i-0ac45d30db8ab7172	Stopped	t3.micro	-	View alarms +	eu-north-1b	-	-	-

i-0fd8f9491845c05b5 (ServidorABC)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

▼ Instance summary Info

Instance ID

i-0fd8f9491845c05b5

IPv6 address

-

Hostname type

IP name: ip-172-31-39-22.eu-north-1.compute.internal

Answer private resource DNS name

IPv4 (A)

Public IPv4 address

16.171.174.243 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-172-31-39-22.eu-north-1.compute.internal

Instance type

t3.micro

Private IPv4 addresses

172.31.39.22

Public DNS

ec2-16-171-174-243.eu-north-1.compute.amazonaws.com | open address

Elastic IP addresses

-

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

3.2. Configuración de la base de datos RDS

Se creó una instancia RDS con PostgreSQL 16, habilitando el acceso desde la instancia EC2. Se configuró un usuario de prueba `posgre` con contraseña segura.

aws

Search

[Alt+S]

Europe (Stockholm)

sercao2023

Aurora and RDS

Create database

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.

BaseABC

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

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

posgre

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 create a password that you manage.

☐ **Auto generate password**

Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

.....

Password strength [Strong](#)

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password [Info](#)

.....

Instance configuration

CloudShell

Feedback

Privacy

Terms

Cookie preferences

aws

Search

[Alt+S]

Europe (Stockholm)

sercao2023

Aurora and RDS

Create database

Instance configuration

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

DB instance class

Info

▼ Hide filters

☒ 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 2085 Mbps

▼

Storage

Storage type

Info

Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp2)

Baseline performance determined by volume size

▼

Allocated storage

Info

20

GiB

Allocated storage value must be 20 GiB to 6144 GiB

► Additional storage configuration

Connectivity

Info

CloudShell

Feedback

Privacy

Terms

Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.

aws

Search

[Alt+S]

Europe (Stockholm)

sercao2023

Aurora and RDS

Create database

Database authentication

Database authentication options

☒ Password authentication

Authenticates using database passwords.

☐ Password and IAM database authentication

Authenticates using the database password and user credentials through AWS IAM users and roles.

☐ Password and Kerberos authentication

Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Monitoring

Choose monitoring tools for this database. Database Insights provides a combined view of Performance Insights and Enhanced Monitoring for your fleet of databases. Database Insights pricing is separate from RDS monthly estimates. See Amazon CloudWatch pricing.

☐ Database Insights - Advanced

- Retains 15 months of performance history
- Fleet-level monitoring
- Integration with CloudWatch Application Signals

☒ Database Insights - Standard

- Retains 7 days of performance history, with the option to pay for the retention of up to 24 months of performance history

Performance Insights

☐ Enable Performance insights

With Performance Insights dashboard, you can visualize the database load on your Amazon RDS DB instance load and filter the load by waits, SQL statements, hosts, or users.

Additional monitoring settings

Enhanced Monitoring, CloudWatch Logs and DevOps Guru

Enhanced Monitoring

☐ Enable Enhanced monitoring

CloudShell

Feedback

Privacy

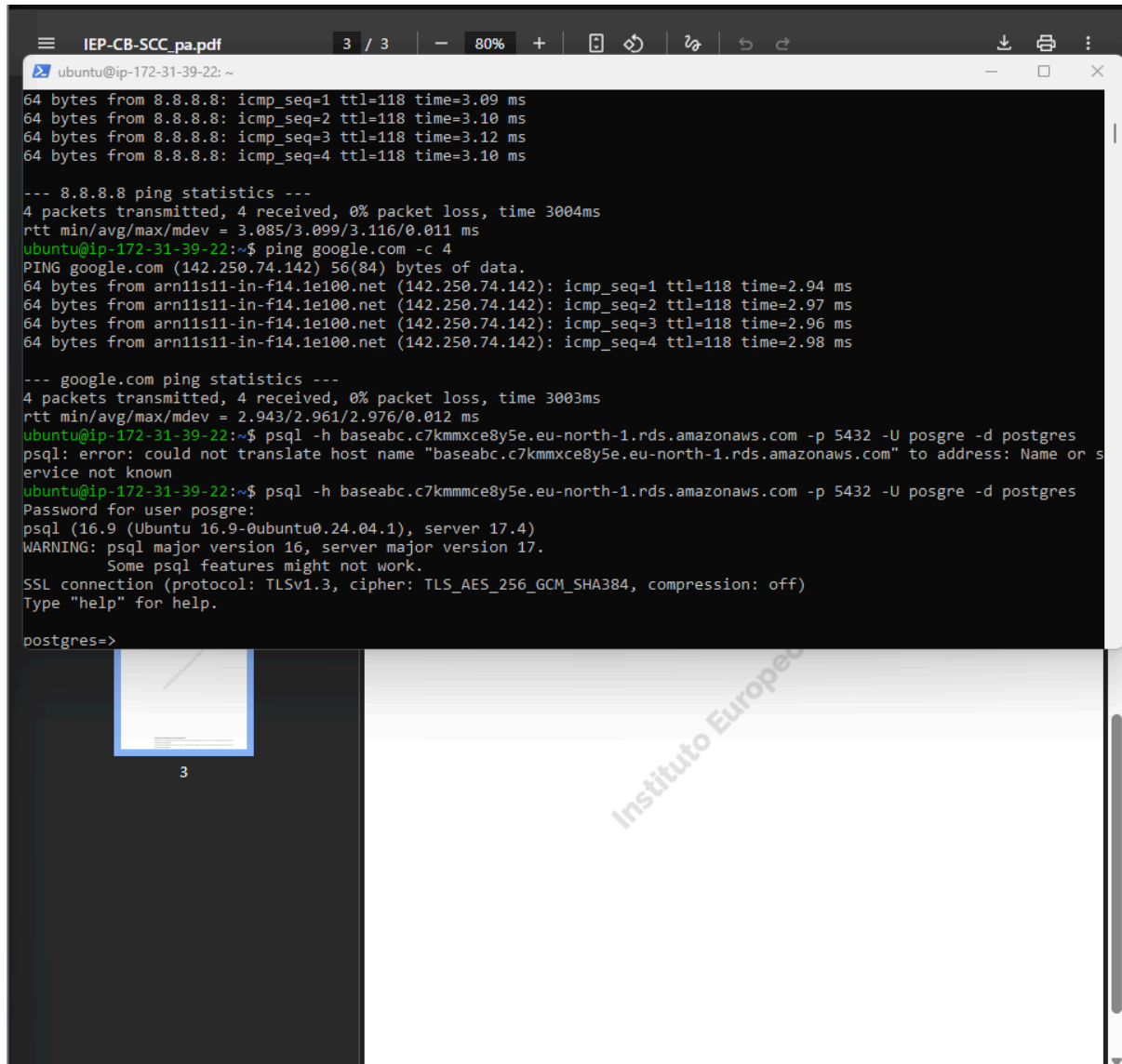
Terms

Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.

3.3. Verificación de conectividad y permisos

Se realizaron pruebas de conectividad (**ping**) desde EC2 a Internet y se probó conexión al endpoint de RDS..



```
IEP-CB-SCC_pa.pdf 3 / 3 - 80% +
ubuntu@ip-172-31-39-22: ~
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=3.09 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=3.10 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=3.12 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=3.10 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.085/3.099/3.116/0.011 ms
ubuntu@ip-172-31-39-22:~$ ping google.com -c 4
PING google.com (142.250.74.142) 56(84) bytes of data.
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=1 ttl=118 time=2.94 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=2 ttl=118 time=2.97 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=3 ttl=118 time=2.96 ms
64 bytes from arn11s11-in-f14.1e100.net (142.250.74.142): icmp_seq=4 ttl=118 time=2.98 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 2.943/2.961/2.976/0.012 ms
ubuntu@ip-172-31-39-22:~$ psql -h baseabc.c7kmmxc8y5e.eu-north-1.rds.amazonaws.com -p 5432 -U postgres -d postgres
psql: error: could not translate host name "baseabc.c7kmmxc8y5e.eu-north-1.rds.amazonaws.com" to address: Name or service not known
ubuntu@ip-172-31-39-22:~$ psql -h baseabc.c7kmmxc8y5e.eu-north-1.rds.amazonaws.com -p 5432 -U postgres -d postgres
Password for user postgres:
psql (16.9 (Ubuntu 16.9-0ubuntu0.24.04.1), server 17.4)
WARNING: psql major version 16, server major version 17.
Some psql features might not work.
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

postgres=>
```

3

Instituto Europeo

4. Seguridad de la información

Se aplicaron las siguientes medidas de seguridad para garantizar la protección de los datos en tránsito y en la nube:

Tecnología	Descripción
SSL/TLS (PostgreSQL)	Comunicación cifrada entre EC2 y RDS
Grupos de seguridad	Control del tráfico entrante y saliente (reglas de firewall)
VPC	Segmentación de red privada para aislar servicios internos
Contraseñas robustas	Usuario <code>posgre</code> con clave segura (<code>Prueba123</code>)
Configuración de cifrado (por defecto en AWS)	Protección del almacenamiento físico en RDS

5. Análisis de cumplimiento normativo – ISO 27017 y 27018

Control (ISO/IEC)	Descripción resumida	Estado en simulación
ISO 27017 – 9.1.2	Restricción de acceso a redes y servicios	✔ Aplicado mediante SG y VPC
ISO 27017 – 12.1.5	Registro y monitoreo de actividades de usuario	◆ Disponible con CloudTrail
ISO 27018 – 11.1	Protección de información personal mediante cifrado	✔ Comunicación cifrada con TLS
ISO 27018 – 11.2	Control de acceso basado en roles y autorización	◆ IAM no implementado en demo
ISO 27018 – 10.2.1	Eliminación segura de información personal	◆ No aplicable a esta simulación

Leyenda:

✔ Implementado | ◆ Disponible pero no usado | ✖ No aplicable

Conclusiones

La simulación de migración a la nube ha demostrado que es viable realizar una transición segura desde una infraestructura local hacia un entorno en AWS. Se ha logrado establecer conectividad entre servicios, aplicar controles de seguridad básicos y evaluar el cumplimiento de estándares internacionales. Aunque se trata de una demostración académica, los fundamentos aplicados son válidos para entornos reales, especialmente en sectores sensibles como el financiero.

Referencias (formato APA)

- Amazon Web Services. (2024). *Amazon RDS Documentation*.
<https://docs.aws.amazon.com/rds/>
- International Organization for Standardization. (2015). *ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.
<https://www.iso.org/standard/43757.html>
- International Organization for Standardization. (2019). *ISO/IEC 27018:2019 — Protection of personal data in cloud computing environments*.
<https://www.iso.org/standard/76559.html>