**Instalación y configuración de alta disponibilidad de sistemas de backup**

INDEX

[INFRAESTRUCTURAS DE HARWARE: 2](#_Toc165926457)

[Diagrama de funcionamiento: 4](#_Toc165926458)

[Manual de instalación y como se administran de los servidores 5](#_Toc165926459)

[Configuración para tener alta disponibilidad de sistema de backup 6](#_Toc165926460)

[INSTALACION Y CONFIGURACION BACKUPS: 9](#_Toc165926461)

[Creación y configuración del script de backup: 9](#_Toc165926462)

[Notificaciones de backup. 10](#_Toc165926463)

[Configuración del cron: 10](#_Toc165926464)

[Guardar en la nube: 11](#_Toc165926465)

# INFRAESTRUCTURAS DE HARWARE:

* Servidor principal:

HPE ProLiant DL380 Gen10.

Especificaciones – CPU Intel Xeon escalable 4210 con 10 núcleos a 2.2 HZ

Memoria RAM: 64GB DDR4 (4modulos de 16 GB)

almacenamiento: 100 TB en configuración RAID 10 (ampliable)

**portátil:**

* Marca: HP
* *Sistema operativo: Debian 12 sin interfaz grafica*

**JUSTIFICACIÓN:**

* La elección del servidor HPE ProLiant DL380 Gen 10 se basa en su velocidad y fiabilidad. Este servidor ofrece un rendimiento superior, integrando características avanzadas de gestión y seguridad. La memoria RAM de 64 GB permite el manejo eficiente de grandes conjuntos de datos y facilita la ejecución fluida de aplicaciones exigentes. Además, el almacenamiento RAID 10 de 100 TB proporciona una sólida protección de datos y garantiza una alta disponibilidad del sistema, minimizando el tiempo de inactividad.

**Servidor respaldo:**

* Servidor en la nube (aws)Amazon Elástic compute cloud (Amazon EC2)

CPU contratado 8 núcleos CPU

4 memoria RAM 64GB

Almacenamiento 100 TB.

**Instancia M5.2 large**

**Justificación:**

* Se ha elegido esta configuración debido a su alta escalabilidad y disponibilidad, lo que garantiza que el servidor de respaldo pueda crecer según las necesidades del hospital y esté siempre disponible cuando se necesite. Además, AWS ofrece una garantía de disponibilidad del 99,99%, lo que proporciona una capa adicional de confiabilidad y seguridad para los datos del hospital.

**Sistema de redundancia y replicación Configuración (activo-pasivo) mecanismo asíncrono**.

* Se ha establecido una configuración activo-pasivo, donde el servidor físico actúa como servidor principal y el servidor en la nube funciona como servidor secundario. La replicación de datos se realiza de manera asíncrona, lo que significa que la sincronización entre los servidores ocurre eventualmente, por eventos.

**Justificación:**

* Esta configuración ofrece una combinación de alta disponibilidad, tolerancia a fallos y capacidad de respuesta del sistema, lo que la hace ideal para respaldar las necesidades críticas de datos del hospital. Aunque tiene sus contras, como costos adicionales y complejidad de configuración, pero los beneficios en términos de seguridad y continuidad del servicio superan ampliamente estas consideraciones

**Configuración activo-pasivo:**

* En esta configuración, el servidor principal se encuentra en el hospital de Blanes y actúa como el nodo activo, encargado de todas las operaciones de lectura y escritura. Este nodo es el punto central de la infraestructura y maneja todas las tareas críticas para el funcionamiento del sistema.
* Por otro lado, el segundo nodo se encuentra en la nube (**cloud**) y opera como el nodo pasivo. En este caso, el servidor en la nube permanece inactivo la mayor parte del tiempo, solo activándose en caso de que el nodo principal en el hospital falle o experimente algún problema. En tal situación, el servidor en la nube asume automáticamente las funciones del servidor principal para garantizar la continuidad del servicio y minimizar cualquier impacto en las operaciones del hospital.

## Diagrama de funcionamiento:

**Diagrama

Descripción generada automáticamente**

# Manual de instalación y como se administran de los servidores

1. Instalación del Servidor Físico en el hospital:

* Determinas el hardware y sistema operativo del servidor físico. En nuestro caso es Debian12.
* Configuración de la red del servidor para que esté conectada a la misma red que los usuarios del hospital.
* Instalar Software necesario para llevar la gestión del hospital.

2. Configurar el servidor de Réplica en la Nube en Amazon

- Crear la cuenta de AWS

- Lanzar una instancia EC2

- Configuración de la seguridad. Hay que destacar que es muy importante tener unos estándares de seguridad altos ya que tratamos con datos personales de pacientes.

- Instalación del software necesario en la instancia EC2. Herramientas de monitorización, software de respaldo, etc.

- Configuración de la Replicación de Datos. Los datos al replicarse en ambos servidores tienen que estar disponibles por si uno de ellos cae.

3. Administrar ambos servidores

- Monitorizar ambos servidores

- Gestionar de usuarios y permisos

- Configuración de las copias de Seguridad

- Configurar la seguridad en ambas maquinas. Como firewalls, VPN, detección de intrusiones.

4. Técnica de balanceo

- Podemos utilizar la técnica “Route 53 Latency Based Rotuing” que proporciona AWS. Esta técnica aprovecha la red para dirigir el tráfico de los usuarios al servidor que tenga menos latencia.

## Configuración para tener alta disponibilidad de sistema de backup

* Primero creamos la máquina virtual y configuramos el postgres
* Una vez creada, la replicamos en otra MV para poder tener alta disponibilidad.

Pasos para tener alta disponibilidad:

En el fichero de postgresql.conf descomentamos las siguientes líneas:

Abrimos el fichero



Habilitar la replicación WAL: Aseguramos que el servidor principal esté escribiendo los registros WAL.

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Configuramos el método de envió. Sincrónicamente se enviarán los registros WAL.

Especificamos la IP del servidor principal. En nuestro es localhost, que es la IP 192.168.1.137.

Texto

Descripción generada automáticamente

Configuramos la identificación de la replicación proporcionando las credenciales del segundo servidor.

Imagen de la pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza baja

Habitamos los registros de replicación.



Abrimos el fichero pg\_hba.conf. Este archivo controla las conexiones a la base de datos. Añadimos la línea al final del fichero.



Aplicamos los cambios reiniciando el servicio

Texto

Descripción generada automáticamente

Entramos en la base de datos y creamos el usuario de replicación.

Texto

Descripción generada automáticamente

Ahora vamos al servidor secundario, nos tenemos que asegurar que este en la misma red que el primario y tenga postgresql.

* Seguimos los mismos pasos que el primario
* En esta máquina hay que poner la dirección del servidor principal en el fichero postgresql.conf.



Configuramos el fichero pg\_hba.conf para indicarle usuario de replica.



Creamos el usuario de replica

Texto

Descripción generada automáticamente

**Establecimiento de conexión vpn**

* Primero se configuran los parámetros de replicación en el nodo principal, incluida la habilitación del registro binario (binlog). Luego, se configura el nodo secundario para que se suscriba al binlog del nodo principal y comience a replicar los datos.

**Configurar pruebas Failover**

* Este modo operativo de respaldo, o Failover es para evitar que no haya perdida de datos, y garantizar la continuidad del servicio en caso de que el componente principal deje de estar disponible ya sea debido a una falla imprevista o a un tiempo de inactividad programada decir, si el componente principal deja de estar disponible, ya sea por falla o por tiempo de inactividad programada.

# INSTALACION Y CONFIGURACION BACKUPS:

Instalamos cron una herramienta la cual nos permite crear tareas y que se ejecuten de manera automática.

1. Sudo apt update
2. Sudo apt install cron

Para poder acceder al fichero donde se crearán las tareas:

* Crontab -e

## Creación y configuración del script de backup:

Texto

Descripción generada automáticamente

En le apartado **variables** se configuraron datos necesarios para que el script pueda acceder a la base de datos para asi buscar y crear la copia de seguridad.

La función backup logico genera copia de la base de datos especificada (DB) la cual es la principal base de datos una vez obtenida la comprime y en caso de producirse un error se crearan logs.

### Notificaciones de backup.

Texto

Descripción generada automáticamente

Para añadir el script tiene implementado unas funciones que notificaran al usuario mediante Gmail y telegram.

### Configuración del cron:

Texto

Descripción generada automáticamente

### Guardar en la nube:

Para instalar onedrive en debian se aplicaron las siguientes comandas:

sudo -- bash -c 'apt update && apt install --yes onedrive'

una vez instalado escribimos por terminal onedrive la primera vez nos mostrara un link el cual tenemos que copiar y poner en el navegador, una vez en este tendremos que iniciar sesión y darle permiso para que acceda a la información.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez terminamos de hacer lo anterior copiamos la url y la ponemos en el terminal, no retornara que la autorización ha sido un éxito.

Texto

Descripción generada automáticamente

Ahora lo sincronizamos:

Texto

Descripción generada automáticamente

Una vez terminado ahora tendremos creada una carpeta onedrive, para ver la ruta podemos hacer **onedrive --display-config,** en esa ruta se creara una carpeta para los backups.

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media

Se añadieron dos líneas mas, una para hacer una copia del comprimido y después una para sincronizar el onedrive:

Texto

Descripción generada automáticamente

Como podemos ver el fichero se subió correctamenteInterfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente