Ejercicio práctico. Creación de una nueva instancia EC2 en la subred pública donde se va a instalar el servicio NextCloud.

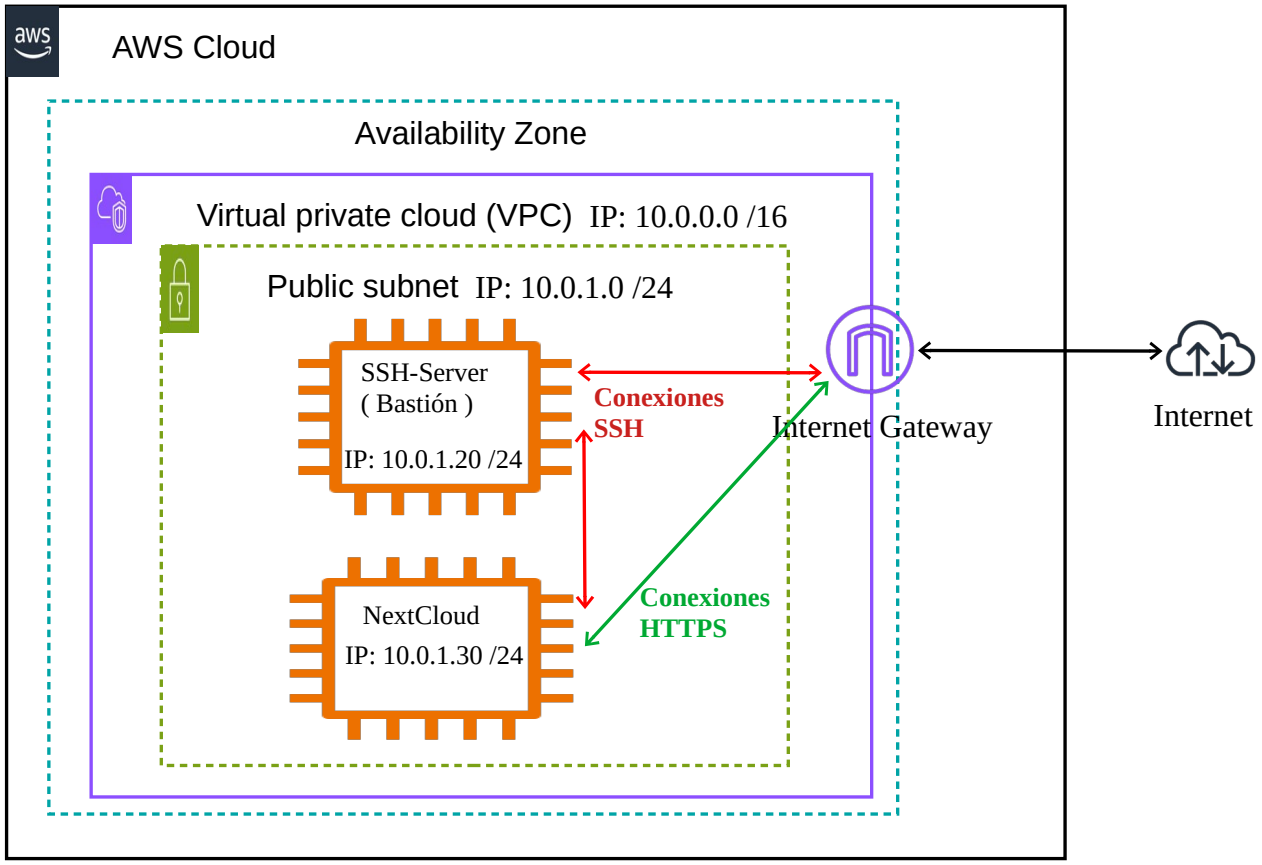
Tarea: Crear una nueva instancia EC2 donde se instala y configura el servicio NextCloud.

Objetivos de la actividad: Crear un servicio web como NextCloud, accesible **sólo** a través del puerto seguro HTTPS (443). Administrar el servidor NextCloud desde el servidor SSH creado en la sesión 3. De esta forma mejoramos la seguridad de nuestra infraestructura, puesto que desde el servidor NextCloud sólo vamos a permitir conexiones SSH que procedan del servidor Bastión (SSH-Server).

Elementos a definir en la instancia:

- ✔ Tipo de AMI.
- ✔ Tipo de instancia.
- ✔ Identificar VPC y la subred donde se ubicará la instancia.
- ✔ Direccionamiento IP.

Escenario:

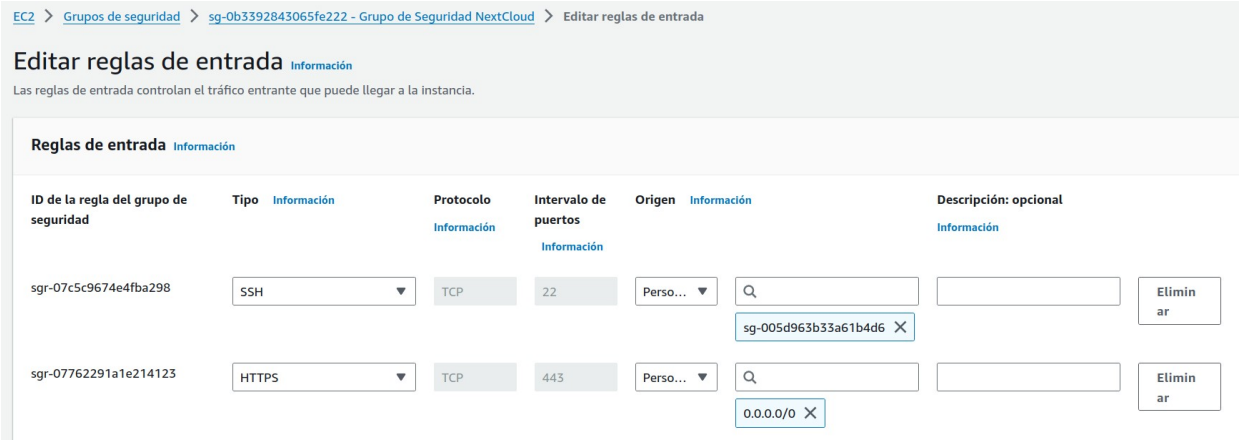


Acceso al Laboratio AWS: https://www.awsacademy.com/vforcesite/LMS_Login

Tarea 1: Lanzar la instancia EC2 NextCloud.

En primer lugar vamos a crear una nueva instancia EC2 donde se va a ejecutar el servicio NextCloud. Posteriormente nos conectaremos desde el servidor bastión por SSH a dicha instancia para poder administrarla.

1. Crea un nuevo grupo de seguridad: Grupo de seguridad NextCloud-XYZ, vinculado a nuestra VPC que permita conexiones HTTPS desde cualquier origen, y conexiones SSH sólo desde el Grupo de Seguridad XYZ-SSH-Server.



2. Creamos la nueva instancia con las siguientes características:
    - Nombre de la instancia: **XYX-NextCloud**.
    - AMI: **Ubuntu Server 22.04 LTS**. Arquitectura de 64 bits. En esta ocasión utilizaremos esta AMI en lugar de la de Debian porque tiene una mejor compatibilidad con el servicio EFS que utilizaremos más adelante.
    - Tipo de instancia: **t3.micro**.
    - Creamos un nuevo par de claves: **vockey2**. Automáticamente nos descargará la clave privada: **vockey2.pem**, que deberemos de utilizar para conectarnos al servidor NextCloud por SSH.

- Seleccionamos nuestra VPC: VPC-XYZ.
- Subred: Zona de disponibilidad: **us-east-1a**.
- Asignar automáticamente la IP pública: **Habilitar**.
- Firewall (grupos de seguridad) → Seleccionamos el grupo de seguridad creado en el punto 1.
- Asignamos la dirección IP interna del servidor NextCloud, que será: **10.0.1.30**
- Perfil de instancia de IAM: **LabinstanceProfile.**
- Tipo de nombre de anfitrión: **Nombre de recurso.**
- Crear una nueva IP elástica: **IP Elástica XYZ-NextCloud** y vincularla a la instancia NextCloud.

3. Conexión SSH al servidor NextCloud.

   En nuestro ejemplo vamos a mejorar la seguridad de los servidores desplegados en AWS, puesto que para conectarnos al servidor NextCloud por SSH, obligatoriamente deberemos primero conectarnos al servidor bastión (SSH-Server). En el siguiente enlace tenemos la información que nos permite realizar dicha conexión:

   https://repost.aws/es/knowledge-center/ec2-linux-private-subnet-bastion-host

   Siguiendo los pasos indicados para equipos Linux, ejecutaremos los siguientes comandos en nuestro PC.

   - En primer lugar comprobamos que las claves privadas tienen los permisos adecuados.

```
rbernabeu@Laptop:~/AWS_LAB/Claves$ ls -la
total 16
drwxrwxr-x 2 rbernabeu rbernabeu 4096 feb  9 11:55 .
drwxrwxr-x 6 rbernabeu rbernabeu 4096 feb  9 11:54 ..
-r-------- 1 rbernabeu rbernabeu 1674 feb  9 10:33 labsuser.pem
-r-------- 1 rbernabeu rbernabeu 1674 feb  9 11:53 vockey2.pem
rbernabeu@Laptop:~/AWS_LAB/Claves$
```

   - Ejecutamos ssh-agent en 2º plano: **eval $(ssh-agent)**
   - Cargamos en memoria la clave privada del servidor bastión (SSH-Server) : **ssh-add labsuser.pem**
   - Cargamos en memoria la clave privada del servidor NextCloud : **ssh-add vockey2.pem**
   - Podemos ver las claves privadas mediante el comando: **ssh-add -l**

```
rbernabeu@Laptop:~/AWS_LAB/Claves$ eval $(ssh-agent)
Agent pid 12407
rbernabeu@Laptop:~/AWS_LAB/Claves$ ssh-add labsuser.pem
Identity added: labsuser.pem (labsuser.pem)
rbernabeu@Laptop:~/AWS_LAB/Claves$ ssh-add vockey2.pem
Identity added: vockey2.pem (vockey2.pem)
rbernabeu@Laptop:~/AWS_LAB/Claves$ ssh-add -l
2048 SHA256:G/E9H2V5VTM+4i8mfArIHCEcw75vKcKaH6phSwe+3EA labsuser.pem (RSA)
2048 SHA256:uwdRPb4qqsNB+QgYVvXDHw+6jtvV93lJJygVS03Fmh0 vockey2.pem (RSA)
rbernabeu@Laptop:~/AWS_LAB/Claves$
```

- Nos conectamos en primer lugar al servidor bastión. Como se puede comprobar, al realizar la conexión también tenemos disponible en memoria, la clave privada del servidor NextCloud.

```
rbernabeu@Laptop:~/AWS_LAB/Claves$ ssh -A admin@34.237.158.189
Linux SSH-Server 6.1.0-17-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1 (2
23-12-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb  9 11:44:19 2024 from 89.29.212.141
admin@SSH-Server:~$ ssh-add -l
2048 SHA256:G/E9H2V5VTM+4i8mfArIHCEcw75vKcKaH6phSwe+3EA labsuser.pem (RSA)
2048 SHA256:uwdRPb4qqsNB+QgYVvXDHw+6jtvV93lJJygVS03Fmh0 vockey2.pem (RSA)
admin@SSH-Server:~$
```

- Seguidamente nos conectamos al servidor NextCloud, pero en este caso debemos de indicar su dirección IP privada: **10.0.1.30**, y el usuario **ubuntu** (en la AMI de Ubuntu el usuario con permisos de sudo no es admin, si no "ubuntu").

```
admin@RBG-SSH-Server:~$ ssh ubuntu@10.0.1.30
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Feb 29 09:29:35 UTC 2024

  System load:  0.0               Processes:             101
  Usage of /:   20.9% of 7.57GB   Users logged in:       0
  Memory usage: 22%               IPv4 address for ens5: 10.0.1.30
  Swap usage:   0%
```

- Cabe destacar que con este método si alguien consiguiera iniciar sesión en el servidor Bastión de forma ilícita, nunca podría conectarse al servidor NextCloud, puesto que el servidor Bastión no almacena la clave privada: **vockey2.pem.**
- Por otro lado, el servidor NextCloud sólo admite conexiones SSH cuyo origen sea el grupo de seguridad del servidor Bastión.
- Por último cambiamos el nombre de máquina: **XYZ-NextCloud**.

Tarea 2: Instalar en la instancia EC2 el servicio NextCloud.

Una vez ya tenemos la instancia EC2 configurada, procedemos a instalar y configurar el servicio NextCloud. En primer lugar, deberemos de instalar y configurar el servidor web: Apache2, posteriormente instalamos el sistema gestor de base de datos: MariaDB. Finalmente configuraremos el servicio Nextcloud.

Para la realización de esta tarea hemos seguido la documentación de NextCloud, pero adaptándola a las características y requisitos de nuestra infraestructura en AWS.

https://docs.nextcloud.com/server/latest/admin_manual/installation/example_ubuntu.html

1. Instalación y configuración del servidor web Apache.

   sudo apt update

   sudo apt install apache2

   Generación y configuración de certificado digital.

   sudo a2enmod ssl

   sudo systemctl restart apache2

   Para simplificar la configuración del servidor, vamos a generar un certificado digital autofirmado. Pero también se puede obtener un certificado digital gratuito de una Autoridad Certificadora, por ejemplo a través de: Let's Encrypt.

   sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache.key -out /etc/ssl/certs/apache.crt

   Indicamos los datos de nuestro certificado digital autofirmado, los datos pueden ser inventados:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Alicante
Locality Name (eg, city) []:Alicante
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nextcloud
Organizational Unit Name (eg, section) []:Dep Informatica
Common Name (e.g. server FQDN or YOUR name) []:nextcloud.com
Email Address []:admin@nextcloud.com
```

Creamos el fichero de configuración de Apache en:

```
sudo nano /etc/apache2/sites-available/nextcloud.conf
```

En este fichero redireccionamos las solicitudes HTTP (80), al puerto HTTPS (443). También indicamos la ubicación de nuestro certificado digital y su clave privada.

Es **importante** sustituir la palabra: **IP_pública_servidor**, por la **IP Elástica** de nuestro servidor **NextCloud**.

Al fichero creado le añadimos las siguientes instrucciones:

```
<VirtualHost *:80>
        ServerName IP_pública_servidor
        Redirect / https://IP_pública_servidor/
</VirtualHost>
<VirtualHost *:443>
        DocumentRoot /var/www/nextcloud/
        ServerName  IP_pública_servidor
        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/apache.crt
        SSLCertificateKeyFile /etc/ssl/private/apache.key
        <Directory /var/www/nextcloud/>
                Require all granted
                AllowOverride All
                Options FollowSymLinks MultiViews
                Satisfy Any
                <IfModule mod_dav.c>
                        Dav off
                </IfModule>
        </Directory>
</VirtualHost>
```

Activamos la configuración y cargamos los módulos necesarios:

```
sudo a2ensite nextcloud.conf
sudo a2enmod rewrite headers env dir mime
sudo systemctl reload apache2
```

Comprobamos el estado del servicio Apache:

```
sudo systemctl status apache2
```

```
root@NextCloud:/etc/ssl/certs# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-02-15 08:05:20 UTC; 31min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 417 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 510 (apache2)
      Tasks: 11 (limit: 1111)
     Memory: 287.2M
        CPU: 14.602s
```

2. Instalación de los paquetes necesarios para posteriormente instalar Nextcloud y configuración de la base de datos de MariaDB.

```
sudo apt update

sudo apt install mariadb-server libapache2-mod-php php-gd php-mysql \
php-curl php-mbstring php-intl php-gmp php-bcmath php-xml php-imagick php-zip unzip
```

3. Configuramos la base de datos. En este punto debemos de sustituir el usuario: **usuario_db** y **password** por nuestros valores. Como se puede observar la base de datos a crear será: **nextcloud**.

```
sudo mysql
CREATE USER 'usuario_bd'@'localhost' IDENTIFIED BY 'password';
CREATE DATABASE IF NOT EXISTS nextcloud CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
GRANT ALL PRIVILEGES ON nextcloud.* TO 'usuario_bd'@'localhost';
FLUSH PRIVILEGES;
quit;
```

4. Instalación del servicio NextCloud.

   Accedemos al directorio: /home/ubuntu, y descargamos el paquete de instalación y lo descomprimimos.

```
cd /home/ubuntu
wget https://download.nextcloud.com/server/releases/latest-28.zip
unzip latest-28.zip
```

   Copiamos el directorio nextcloud y todo su contenido al directorio: /var/www. Cambiamos el propietario del directorio.

```
sudo cp -r nextcloud /var/www
sudo chown -R www-data:www-data /var/www/nextcloud
```

   Comprobamos el estado del fichero de configuración de Apache:

```
sudo apache2ctl configtest
```

Recargamos el servicio apache2 y obtenemos su estado:

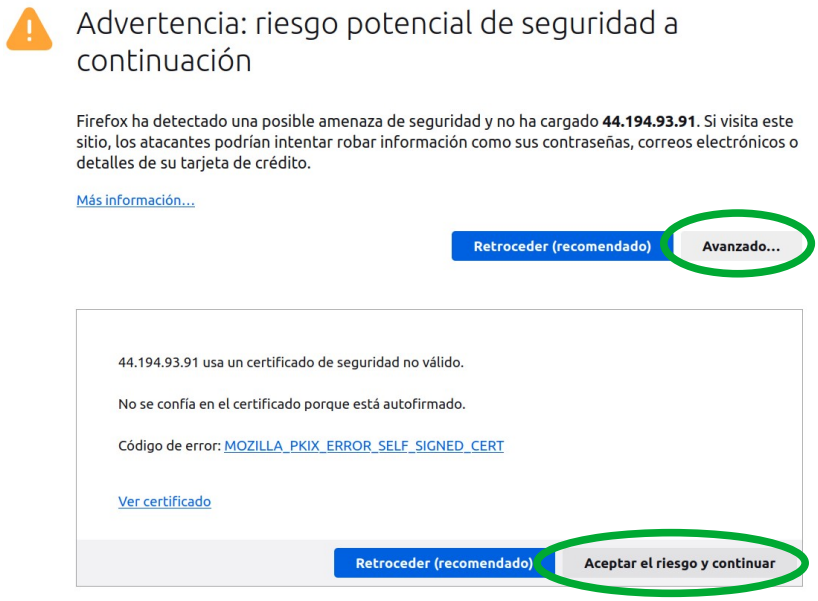
```
sudo systemctl reload apache2
sudo systemctl status apache2
```

Comprobamos el estado del servicio de la base datos:

```
sudo systemctl status mariadb
```

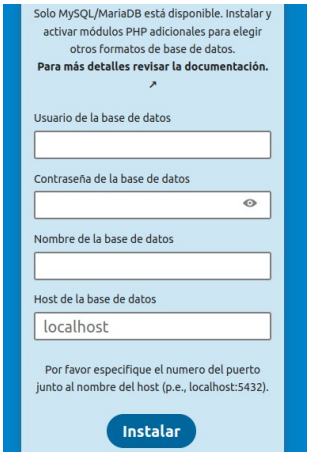
Desde nuestro ordenador, abrimos el navegador web y accedemos a la página de configuración de Nextcloud, **https://IP_pública_Servidor_NextCloud**.

Hay que tener en cuenta que al utilizar un certificado autofirmado, el navegador nos advertirá de un potencial riesgo de seguridad. Pulsamos → Avanzado → Aceptar el riesgo y continuar.



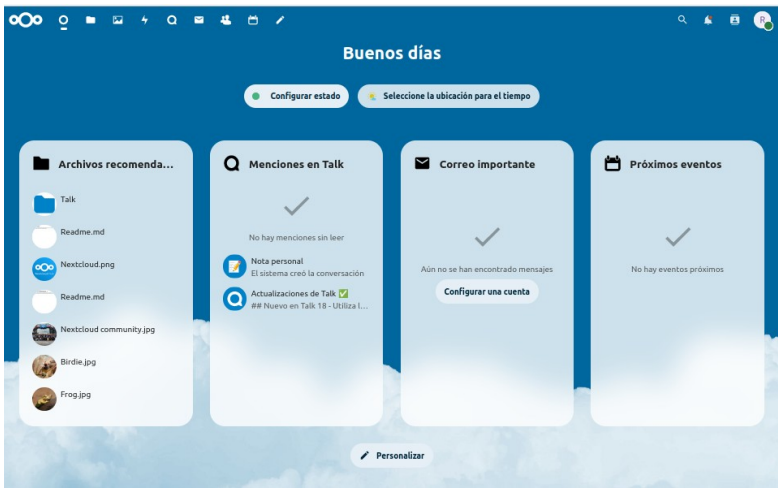
Creamos la cuenta de Administrador de NextCloud, introducimos un nombre y contraseña.

Indicamos usuario, contraseña y nombre de la base de datos, tal y como hemos definido en el punto 3, donde hemos creado la base de datos. Pulsamos instalar.



Tras la instalación, ya tendremos disponible la herramienta NextCloud.

A continuación podemos instalar las aplicaciones recomendadas.



Una vez terminada la instalación, y adicionalmente, podemos instalar la aplicación NextCloud en un disposotivo móvil y comprobar que podemos acceder al contenido de nuestro servidor NextCloud. =;-))