AWS Directory Service: Creación de un servicio de Directorio

El servicio **AWS Directory Service** es una solución integral que facilita la administración de identidades y el acceso a recursos en la nube. Ofreciendo una variedad de opciones para implementar servicios de directorio, AWS Directory Service simplifica la gestión de usuarios, grupos y recursos dentro de entornos en la nube.

En esta práctica, nos enfocaremos en desplegar un servicio de directorio basado en “Simple AD” dentro de AWS Directory Service. “Simple AD” es una opción de directorio compatible con Microsoft Active Directory (AD) que permite a los usuarios integrar aplicaciones y servicios en la nube con sus identidades locales de Active Directory.

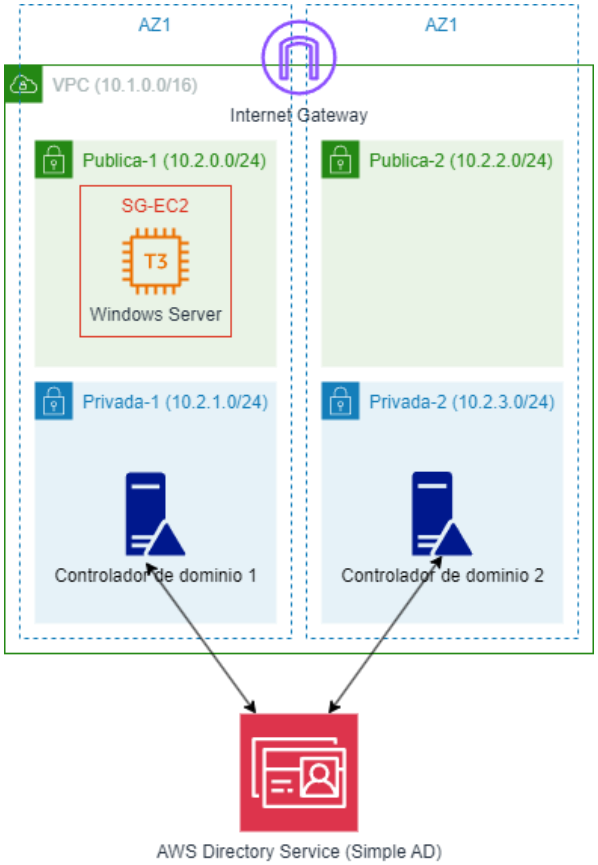
A lo largo de esta práctica, exploraremos los pasos necesarios para configurar y desplegar un servicio de directorio Simple AD en AWS. Esto incluirá la creación del directorio, así como la configuración de la conectividad.

Al finalizar esta práctica, los alumnos habrán adquirido experiencia práctica en la implementación de servicios de directorio en la nube utilizando AWS Directory Service, lo que les permitirá gestionar de manera efectiva las identidades y los recursos dentro de entornos de infraestructura en la nube.

Requerimientos:

- Disponer de acceso a los recursos de AWS a través de un *sandbox* de AWS Academy

Arquitectura propuesta:

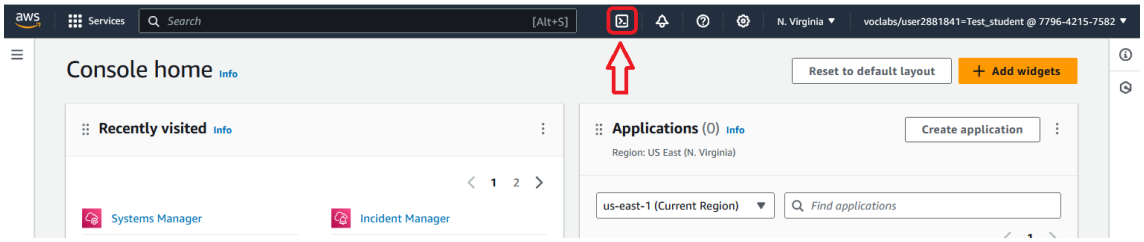


José Emilio Vera

Realización:

CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED

1) El objetivo de la presente práctica no es configurar la infraestructura de red para el despliegue del servicio de directorio, por lo que automatizaremos el despliegue de dicha infraestructura mediante el servicio de AWS CloudFormation. Para ello abrimos una sesión en AWS CloudShell, tal y como se muestra en la siguiente figura:

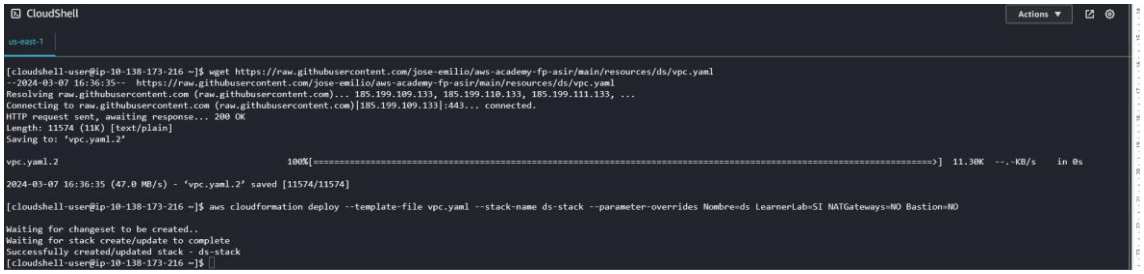


2) Una vez inicializada la sesión de AWS CloudShell, ejecutamos los siguientes comandos para descargar las plantillas de AWS CloudFormation necesarias para desplegar la infraestructura de la práctica:

```
wget https://raw.githubusercontent.com/jose-emilio/aws-academy-fp-asir/main/resources/ds/vpc.yaml
```

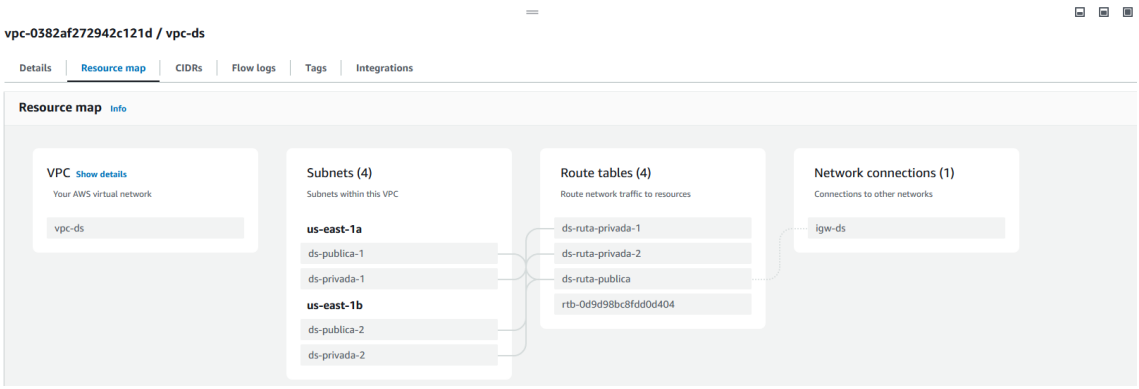
Una vez descargada la plantilla, utilizamos la AWS CLI para desplegar automáticamente la infraestructura de red:

```
aws cloudformation deploy --template-file vpc.yaml --stack-name ds-stack --parameter-overrides
Nombre=ds LearnerLab=SI NATGateways=NO Bastion=NO
```



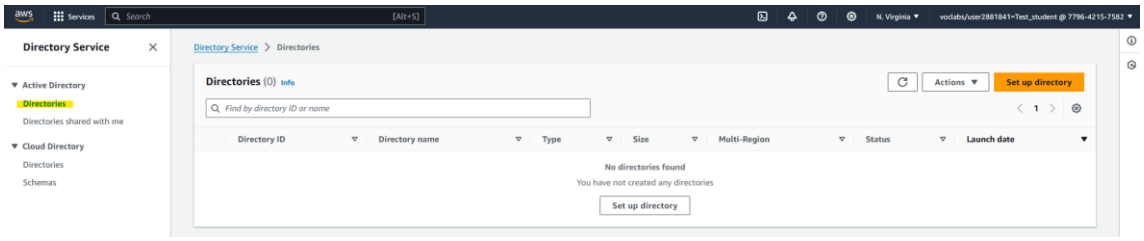
Tras la ejecución de las instrucciones anteriores será necesario esperar unos 2 minutos hasta que la infraestructura de la práctica esté completamente preparada (cuando el servicio AWS CloudFormation devuelva el control del *prompt*).

3) La infraestructura aprovisionada consta de una VPC etiquetada como *vpc-ds* con cuatro subredes, dos públicas y dos privadas, distribuidas en dos zonas de disponibilidad diferentes. Las subredes privadas se utilizarán para desplegar el servicio de directorio, de forma que los dos DC (*Domain Controller*) se encontrarán cada uno en una subred privada. Por su parte, las subredes públicas se emplearán para lanzar una instancia EC2 con Windows Server para administrar el servicio de directorio.

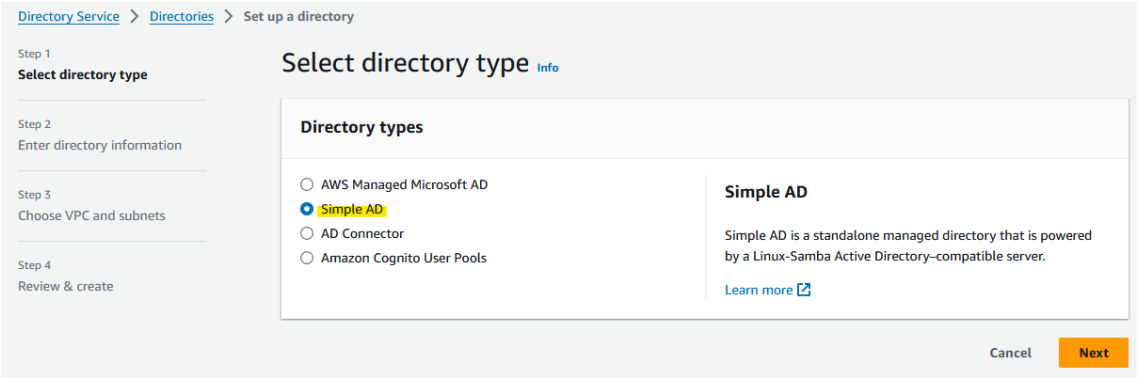


CREACIÓN DEL SERVICIO DE DIRECTORIO

4) En primer lugar, desplegaremos el servicio de directorio. Para ello accederemos a la consola de AWS Directory Service, accedemos la menú lateral **Active Directory / Directories** y presionamos el botón **Set up directory**:.

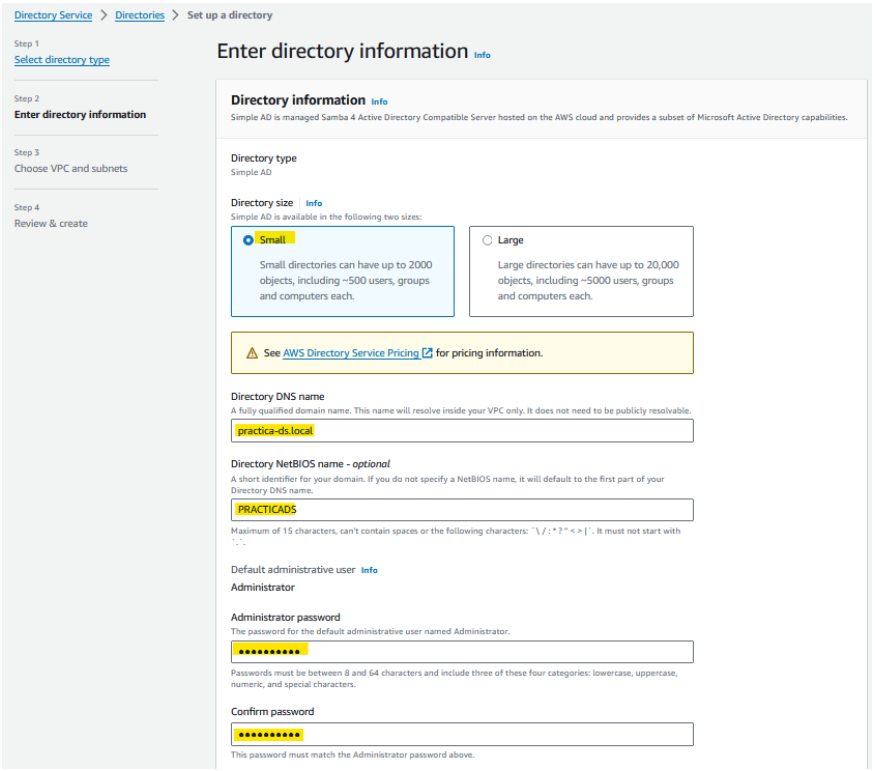


5) En el paso 1 del asistente, dentro de las opciones **Directory types** seleccionamos el valor *Simple AD* y presionamos el botón **Next**:



6) En el paso 2, introducimos la siguiente configuración:

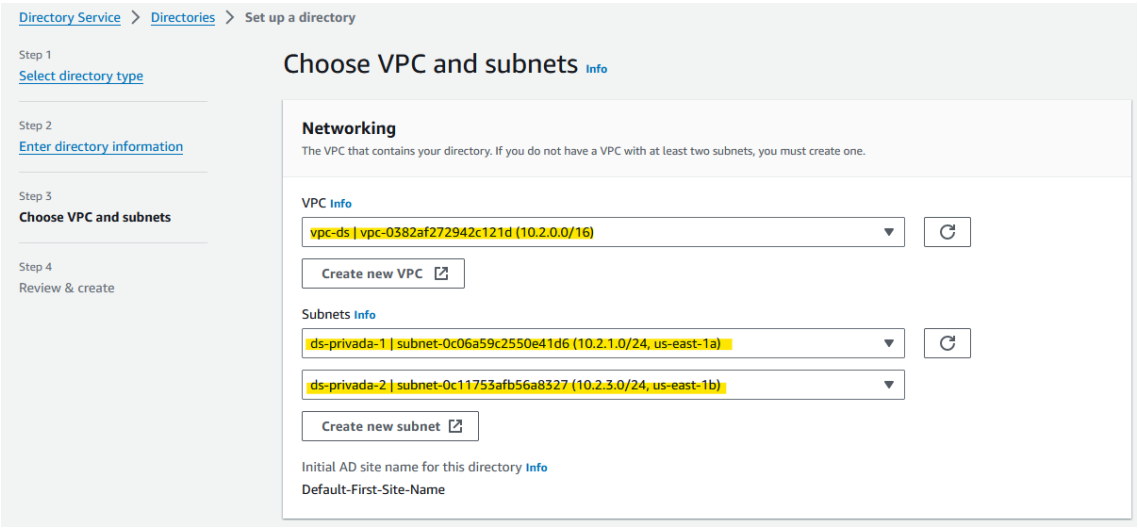
- **Directory size**: Seleccionamos el valor *Small*
- **Directory DNS name**: Indicamos el valor *practica-ds.local*
- **Directory NetBIOS name**: Indicamos el valor PRACTICADS
- **Administrator password**: Indicamos una contraseña entre 8 y 64 caracteres que incluya al menos una mayúscula, una minúscula, un número y un carácter especial
- **Confirm password**: Escribimos la misma contraseña indicada en el punto anterior



Presionamos el botón **Next**

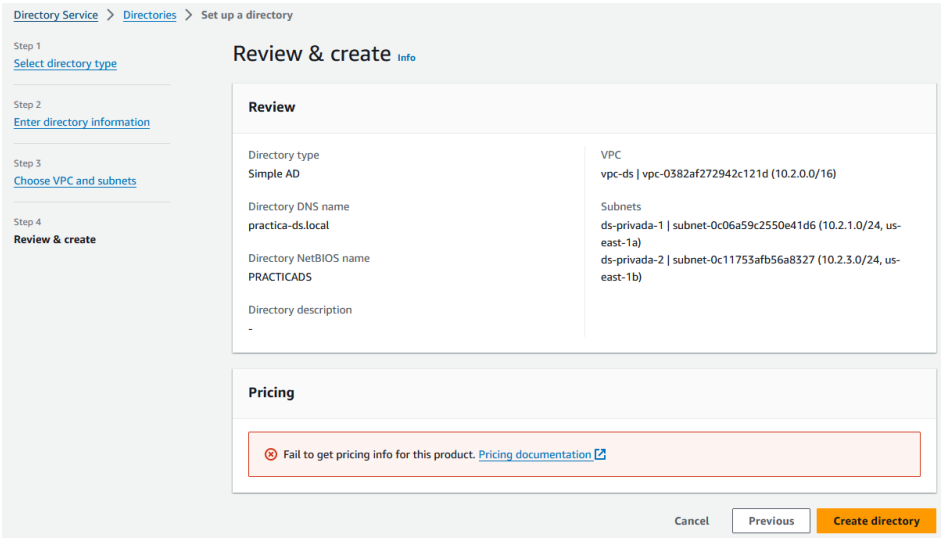
7) En el paso 3, configuramos la red donde se desplegará el servicio *Simple AD*, indicando para ello:

- **VPC**: Seleccionamos la VPC etiquetada como *vpc-ds*
- **Subnets**: Seleccionamos las subredes etiquetadas como *ds-privada-1* y *ds-privada-2*:

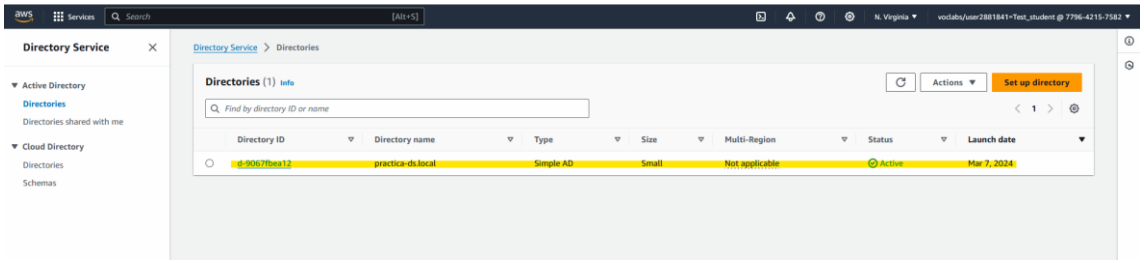


Presionamos el botón **Next.**

8) En el paso 4, presionamos el botón **Create directory**:

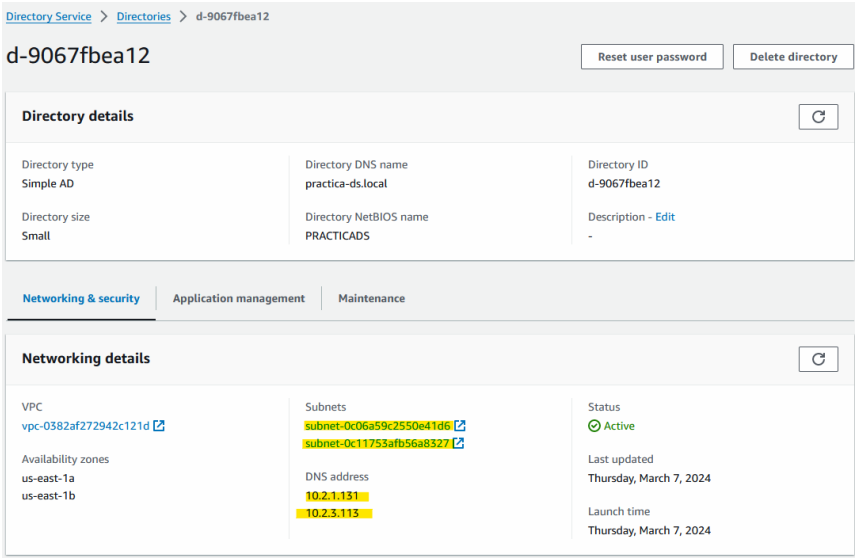


El servicio de directorio de *Simple AD* estará disponible en unos 10 minutos. Tras ello, podremos comprobar que se encuentra operativo:

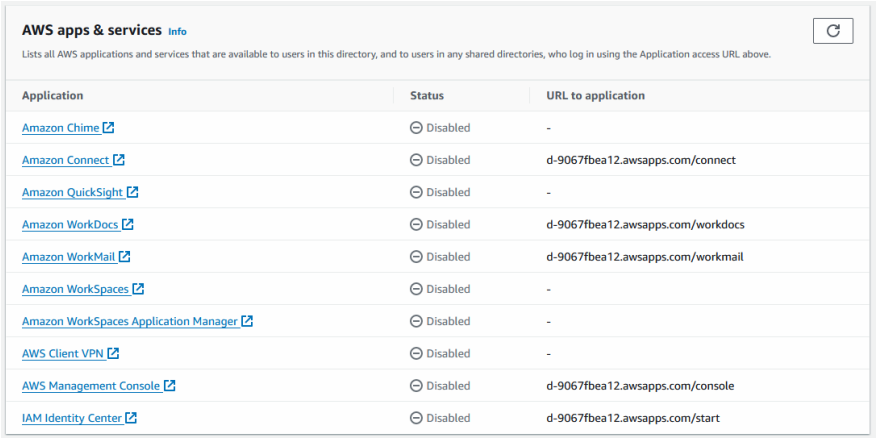


9) Si accedemos al enlace de nuestro directorio, podremos comprobar que, en la pestaña de **Networking & security**, aparece la configuración de red mostrando entre otros:

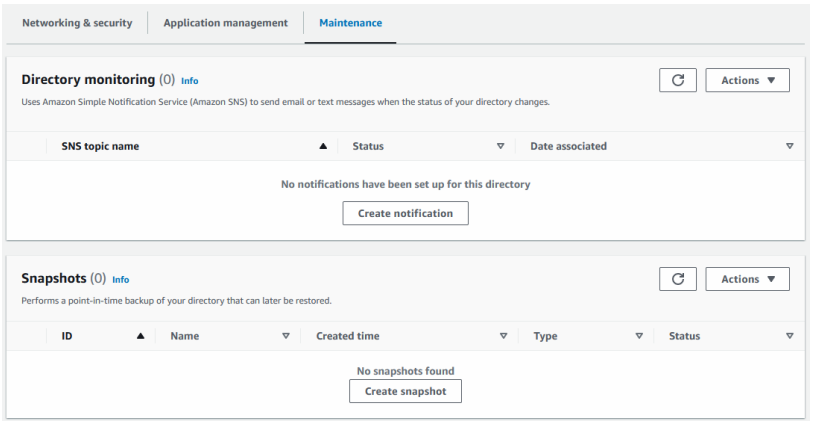
- Los dos servidores DNS (IPs) que AWS Directory Service ha creado en nuestro nombre
- Las dos subredes privadas (*ds-privada-1* y *ds-privada-2*) donde están desplegados los DCs



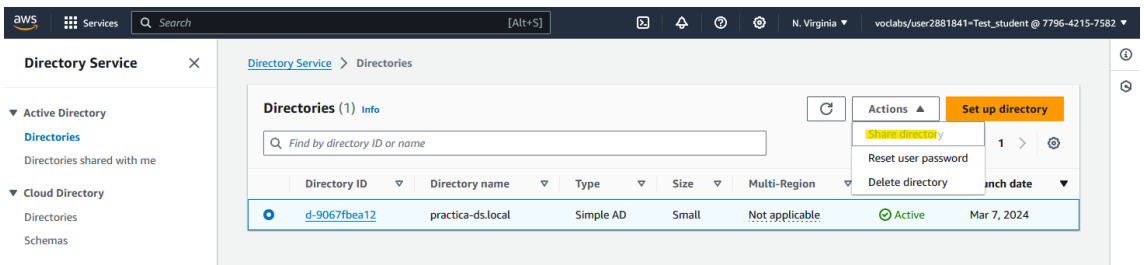
10) En la pestaña **Application management** aparecen una gran cantidad de servicios con los que se puede integrar *Simple AD*. Desgraciadamente, los AWS Academy Learner Labs están bastante limitados y sólo sería posible integrarlo con Amazon Quicksight (un servicio de inteligencia empresarial) y AWS Client VPN (para la autenticación de usuarios a una VPN administrada basada en OpenVPN)



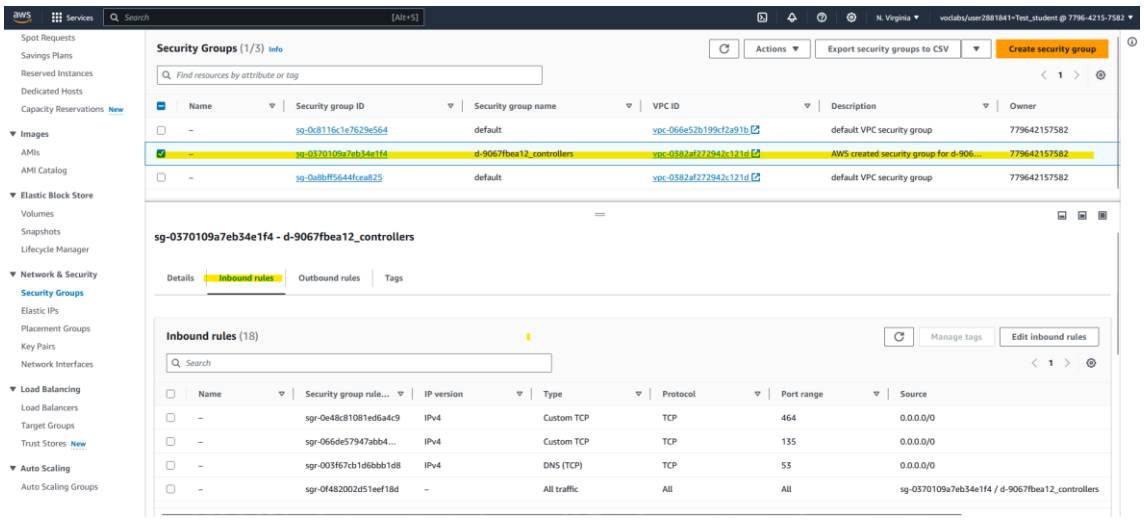
11) En la pestaña **Maintenance** podemos configurar la monitorización del directorio, para permitir que se envíen notificaciones mediante un tema de Amazon SNS cuando el directorio cambie de estado. También es posible crear una **instantánea** bajo demanda del directorio para poder ser restaurado en caso de que ocurra algún problema.



12) Otra de las características que tiene el servicio AWS Directory Service es poder compartir un servicio de directorio con otras cuentas de AWS. Sin embargo, esta funcionalidad es exclusiva de los directorios creados mediante *AWS Directory Service for Microsoft Active Directory*, por lo que no se va a contemplar en la presente práctica:

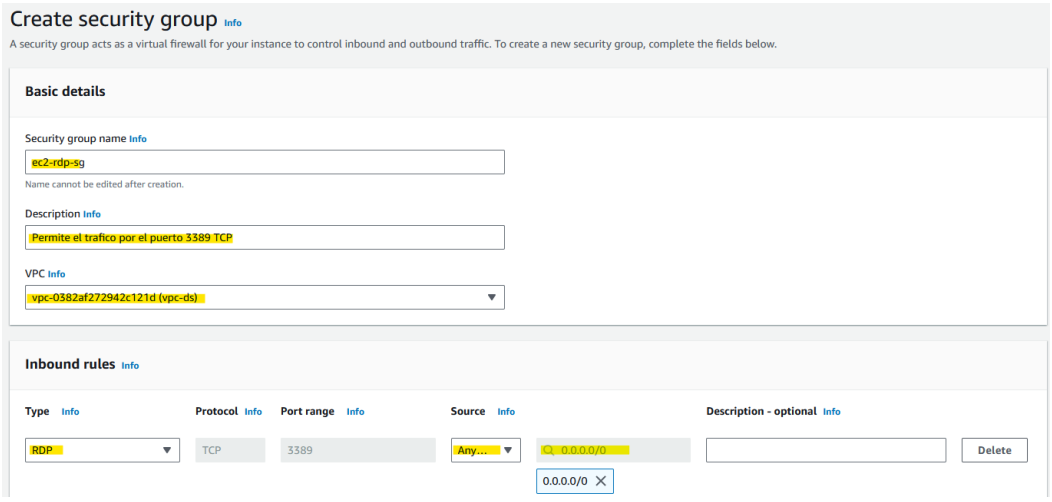


13) Accedemos a la consola de Amazon EC2 y seleccionamos la opción **Network & Security / Security Groups** donde podremos visualizar que hay un grupo de seguridad creado automáticamente por el servicio AWS Directory Service:



Este grupo de seguridad tiene 18 reglas de entrada, y se aplica a las interfaces de red elásticas (ENIs) de ambos DCs. Las reglas filtran patrones de tráfico de uso habitual en servicios de directorios, por ejemplo: 464 TCP/UDP (*Kerberos Password*), 88 TCP/UDP (*Kerberos*), 53 TCP/UDP (DNS), 636 TCP (LDAPS), 389 TCP (LDAP), …

14) A continuación, para administrar el servicio de directorio, vamos a crear una instancia EC2 con Windows Server 2022. Para ello, desde la ventana anterior creamos un grupo de seguridad que permita únicamente el tráfico mediante el protocolo RDP. Presionamos el botón **Create security group** y parametrizamos el grupo de seguridad como se muestra en la figura siguiente:



Por último, presionamos el botón **Create security group**.

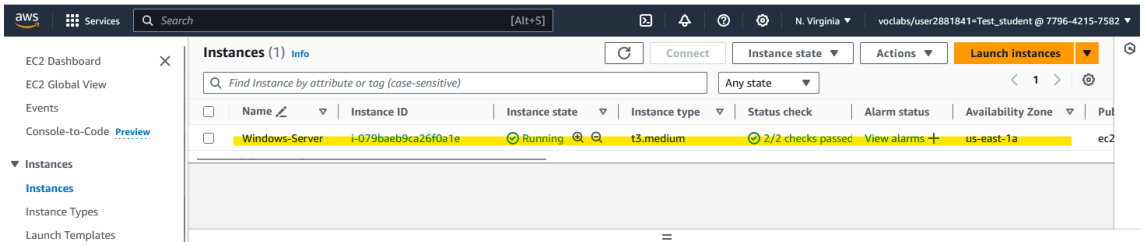
15) A continuación, creamos una instancia EC2 (véase https://github.com/jose-emilio/aws-academy-fp-ec2/blob/main/Amazon_EC2_Windows.pdf) con la siguiente configuración:

- **Name**: *Windows-Server*

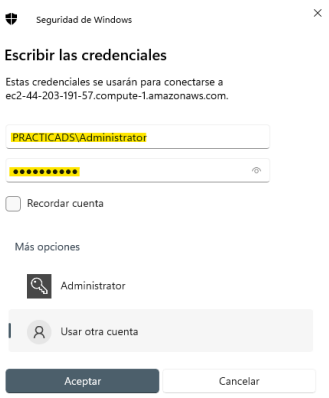
- **Application and OS Images (AMI)**: Seleccionamos una AMI de *QuickStart* con *Microsoft Windows Server 2022 Base*
- **Instance type**: *t3.medium*
- **Key pair (login)**: Seleccionamos la opción *vockey*
- **Network settings** (presionamos el botón *Edit*):
  - **VPC**: Seleccionamos la VPC etiquetada como *vpc-ds*
  - **Subnet**: Elegimos la subred etiquetada como *ds-publica-1* (en realidad podría elegirse cualquier subred pública)
  - **Firewall (security groups)**: Elegimos *Select existing security group* y seleccionamos la opción *ec2-rdp-sg* del menú desplegable siguiente
- **Configure storage**: Elegimos la opción *General Purpose (gp3)* como tipo de almacenamiento
- **Advanced details**:
  - **Domain join directory**: Elegimos la opción etiquetada como *practica-ds.local*
  - **IAM instance profile**: Elegimos la opción etiquetada como *LabInstanceProfile*
  - **User data**: Pegamos el siguiente script que instalará las herramientas de administración remota de Active Directoty.

```
<powershell>
Install-WindowsFeature RSAT-ADDS
</powershell>
```

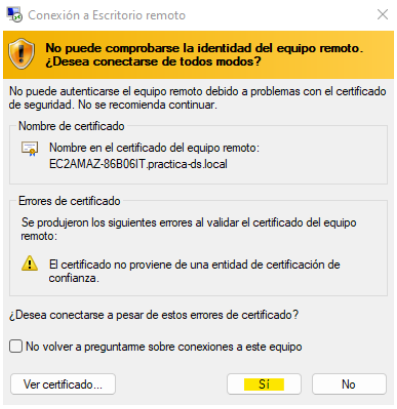
16) Tras un breve instante, podremos visualizar nuestra instancia EC2. Al tratarse de un sistema operativo Microsoft Windows Server, debemos darle unos 3-4 minutos antes de poder utilizarlo:



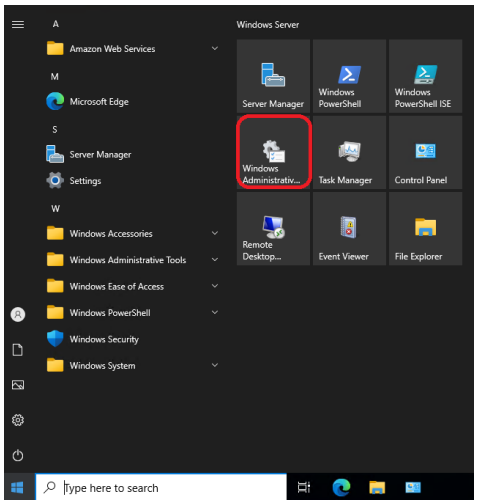
17) Realizamos una conexión vía RDP contra nuestra instancia Windows (véase procedimiento en https://github.com/jose-emilio/aws-academy-fp-ec2/blob/main/Amazon_EC2_Windows.pdf), pero en esta ocasión no utilizaremos las credenciales del usuario *Administrator* local, sino el usuario *Administrator* del directorio. Por ello, desde la ventana de autenticación seleccionamos el enlace **Mas opciones / Usar otra cuenta** e introducimos como nombre de usuario *PRACTICADS\Administrator* (se indica el nombre NetBIOS y el usuario administrador) y la contraseña que se configuró en el apartado **6)**:



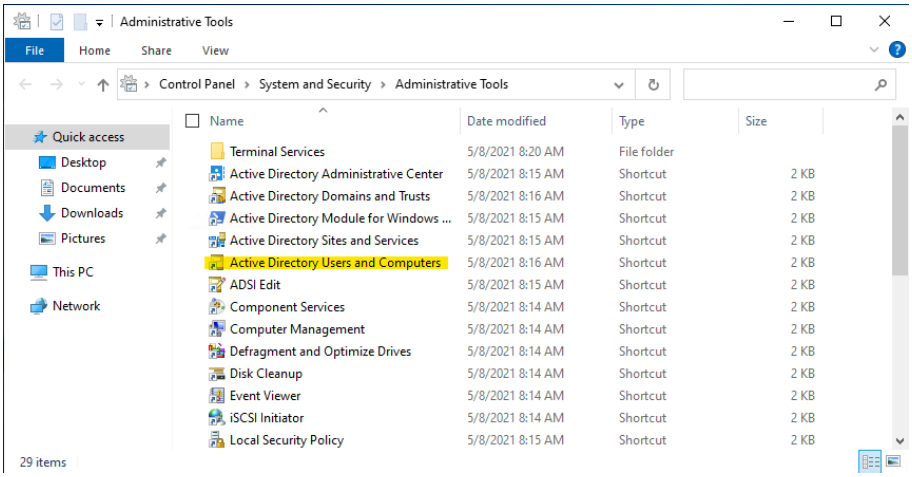
Tras presionar el botón **Aceptar**, aparecerá una nueva ventana en la que presionaremos el botón **Sí**:



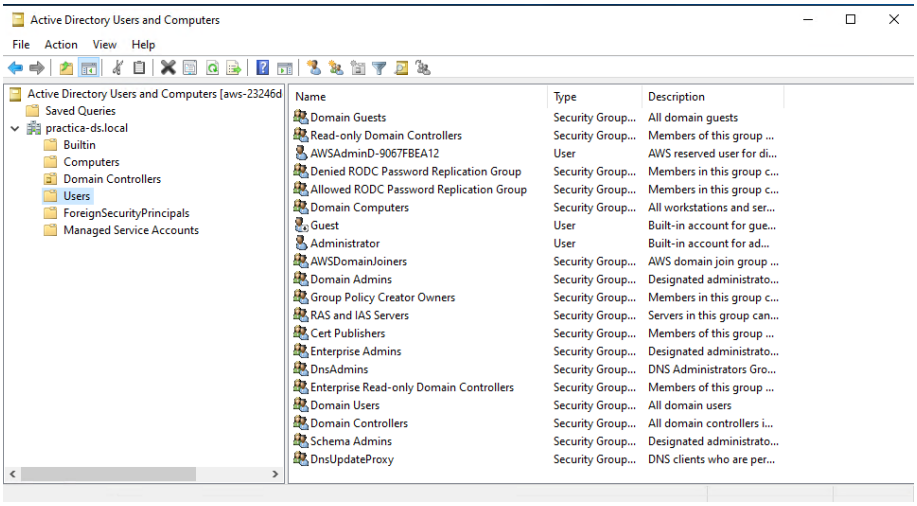
18) Una vez realizado el proceso de autenticación como administrador del dominio, se abrirá una sesión RDP. Desde esta sesión accedemos al botón de inicio y entramos en las herramientas administrativas de Windows:



19) Desde la siguiente ventana, abrimos el acceso directo a **Active Directory Users and Computers**:



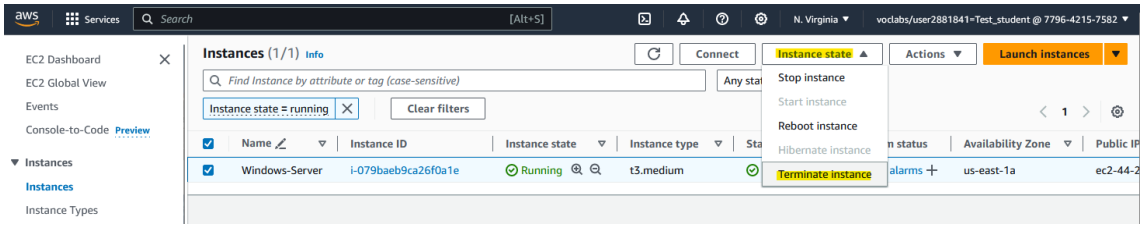
20) Desde esta herramienta podremos administrar los diferentes componentes del directorio activo vinculado a nuestro dominio *practica-ds.local*, como crear usuarios y grupos:



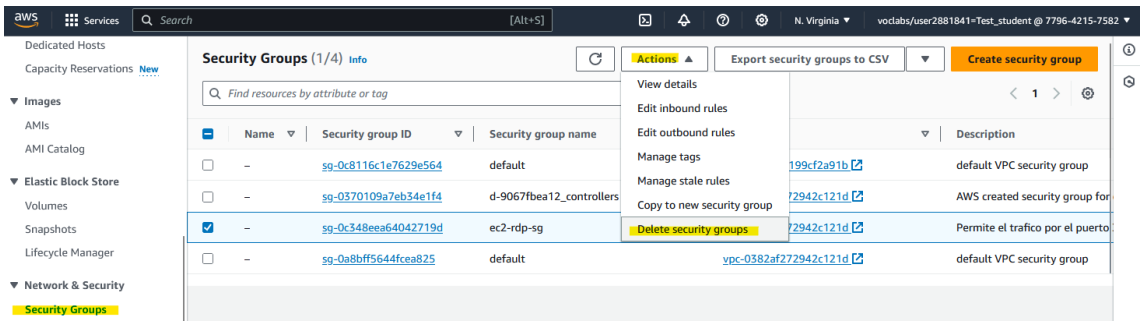
Limpieza de la Práctica:

Para terminar esta práctica y liberar los recursos creados, evitando así el consumo de créditos de AWS Academy Learner Labs, simplemente debemos dar los siguientes pasos en el orden especificado:

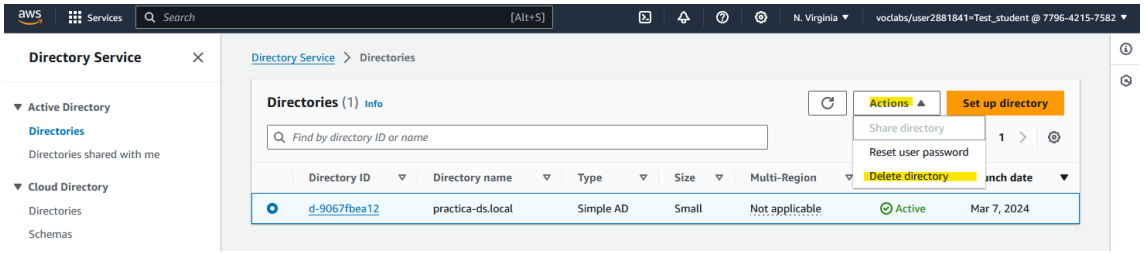
- **Eliminar la instancia EC2**. Para ello, desde la consola del servicio Amazon EC2 seleccionamos la instancia y desde presionamos el botón **Instance state / Terminate**.



- **Eliminar el grupo de seguridad asignado la instancia EC2**. Una vez nuestra instancia se encuentre en estado *Terminated* accedemos al menú lateral **Network & Security / Security Groups**, seleccionando el grupo de seguridad etiquetado como *ec2-rdp-sg* y presionar el botón **Actions / Delete security groups**.



- **Decomisionar el servicio de directorio**. Accedemos a la consola del servicio AWS Directory Service, seleccionamos nuestro directorio y presionamos el botón **Actions / Delete directory**. Este proceso podría demorar varios minutos.



- **Desaprovisionar la infraestructura de red**. Para ello utilizaremos el servicio AWS CloudFormation. Accedemos a la consola de AWS CloudShell (véase paso **1)**) y ejecutamos la siguiente orden:

```
aws cloudformation delete-stack --stack-name ds-stack
```

(NOTA: La instrucción anterior no devuelve resultado alguno, pero en cuestión de pocos minutos nuestra infraestructura de red e instancias EC2 se habrán desaprovisionado)