01/07/23

**UPNA - Pamplona**

**Calves públicas SSH en LDAP y registro de accesos Linux**

*Iban Ruiz de Galarreta Cadenas*

08

**Fall**

TABLA DE CONTENIDOS

[Ev. 1. Ut 1: CARACTERIZACIÓN DE SISTEMAS OPERATIVOS 3](#_Toc491007477)

[2. Sistema informático 3](#_Toc491007478)

[3. Clasificación de los sistemas operativos 4](#_Toc491007479)

[4. Los gestores de arranque 5](#_Toc491007480)

[5. Gestión del procesador 6](#_Toc491007481)

[Índice 6](#_Toc491007482)

# Introducción

# Despliegue de la infraestructura

En este apartado, voy a explicar cómo he preparado la infraestructura. Para todo el despliegue, he utilizado **Docker**, más concretamente **Docker Compose**. He empleado la imagen **"osixia/openldap:latest"** para el servidor LDAP y la imagen **"ubuntu:latest"** para crear una imagen personalizada llamada **"ibantxu12/uldapyssh"**. Toda la configuración de las máquinas la he programado en el archivo **"docker-compose.yaml"** y he creado dos scripts: **"./start-app.sh"** y **"./stop-app.sh"**, para facilitar la creación y eliminación de las máquinas.

A continuación, explicaré detalladamente la creación y configuración de las maquinas:

## Servidor OpenLDAP

Esta es la configuración utilizada para el servidor LDAP:

A screen shot of a computer

Description automatically generated

Imagen 1 : Docker compose LDAP

He elegido esta **imagen** poque ya disponía de el servidor openldap instalado y me permitía no tener que instalar y configurar todo el servidor.

Para el **container\_name** y el **hostname** he decidido usar el mismo nombre, para poder identificarlos bien dentro y fuera de las maquinas.

En el apartado de **volumes** he guardado la ruta donde se guardan las bases de datos de los usuarios para que se queden guardados y no haya que configurarlo cada vez que cierras las máquinas. Es posible que en este apartado en el futuro necesite añadirle nuevos volúmenes, como los certificados o los ajustes de PAM.

En el apartado **networks** he seleccionado la red donde van a estar todas las maquinas, la cual creo mas abajo y es **“openldap-n”**.

Y, por último, en el apartado **environment** he usado varias variables que ahora mismo no son muy necesarias, pero puede que en un futuro me sea útil, como toda la parte del certificado. La información que si que es importante es **“LDAP\_DOMAIN”** y **“LDAP\_BASE\_DN”** que tienen que coincidir y la información de login del admin, es decir **“LDAP\_ADMIN\_USERNAME”** y **“LDAP\_ADMIN\_PASSWORD”**.

Para crear los usuarios y grupos de ejemplo he creado dos archivos ldif que se encuentran en la carpeta “ejemplos”, estos archivos crean los usuarios: Javier, Mark, Lorea, Maite, Olatz, Mikel, Mario. Y los grupos: 1, 2 y 3. Para introducirlos en el servidor LDAP basta con acceder a la maquina **"docker exec -it openldap bash"**, introducir los archivos y ejecutarlos con el comando **"ldapadd -x -D cn=admin,dc=ibantfg,dc=com -W -f <archivo>"**. Se puede comprobar que los usuarios se han creado correctamente utilizando el comando "slapcat".

## Clientes Ubuntu

Para crear los clientes he elaborado una imagen con las herramientas necesarias de la siguiente manera:

Primero he arrancado una imagen normal de “Ubuntu:latest”, he accedido a ella **"docker exec -it ubuntu bash"** y he instalado todo lo necesario: **“sudo apt update”**, **“sudo apt install ssh”** y **“sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y”**. después del último comando se abrirá un menú para configurar el cliente LDAP. En el primer apartado he escrito la dirección de red del servidor **“ldapi:///openldap/”**, en el siguiente lo que configuré en el servidor LDAP **“dc=ibantfg,dc=com”**. Después he seleccionado la versión 3 de LDAP. Por último, el usuario y la contraseña del admin, es decir: **“cn=admin,dc=ibantfg,dc=com”** y **“LDAPapTFG”**.

Una vez instalado openldap he configurado manualmente tres archivos, uno es **“/etc/nsswitch.conf”**, en el cual he cambiado systemd por ldap en las líneas 7,8 y 9. El otro es **“/etc/pam.d/common-session”** al que he habrá que añadir al final del archivo la línea **“session optional       pam\_mkhomedir.so skel=/etc/skel umask=077”**.

Con esto la maquina ya estaba preparada y podía conectarme a un usuario del servidor LDAP. He subido esa maquina al repositorio de Docker con el nombre **“ibantxu12/uldapyssh”** para que sea accesible desde cualquier equipo. Y esta es la configuración para cada cliente:

A screen shot of a computer

Description automatically generated

Imagen 2: Docker compose Clientes

Como ya he dicho uso la imagen **“ibantxu12/uldapyssh”** que yo he creado, pongo el mismo nombre de **container\_name** y de **hostname**. Lo añado a la red **openldap\_n**. Mapeo el puerto 22 en el puerto 221 de mi maquina física, pero solo para el cliente 1, el cliente 2 mapeare el puerto 222, para el 3 el 223… Y por último añado el comando **“/usr/sbin/sshd -D”** para que el servidor ssh este funcionando y para que la maquina no se cierre automáticamente.

## Prueba de ejecución

Para comprobar el correcto funcionamiento de la red podemos conectarnos que desde cualquier usuario a cualquiera de las maquinas. Con el comando **"ssh <usuario>@localhost -p <puerto>"** donde **<usuario>** es un usuario cualquiera del servidor LDAP y **<puerto>** es el puerto de la maquina a la que conectarse ( numero entre 221 y 225). Los usuarios son javier, mark, lorea, maite, olatz, mikel y mario. Y las contraseñas **“<usuario>Pass”**. Aquí tenemos un ejemplo:

A screenshot of a computer screen

Description automatically generated

Imagen 3: Ejemplo ejecución