Proceso de instalación y pruebas OpenIAM en Docker

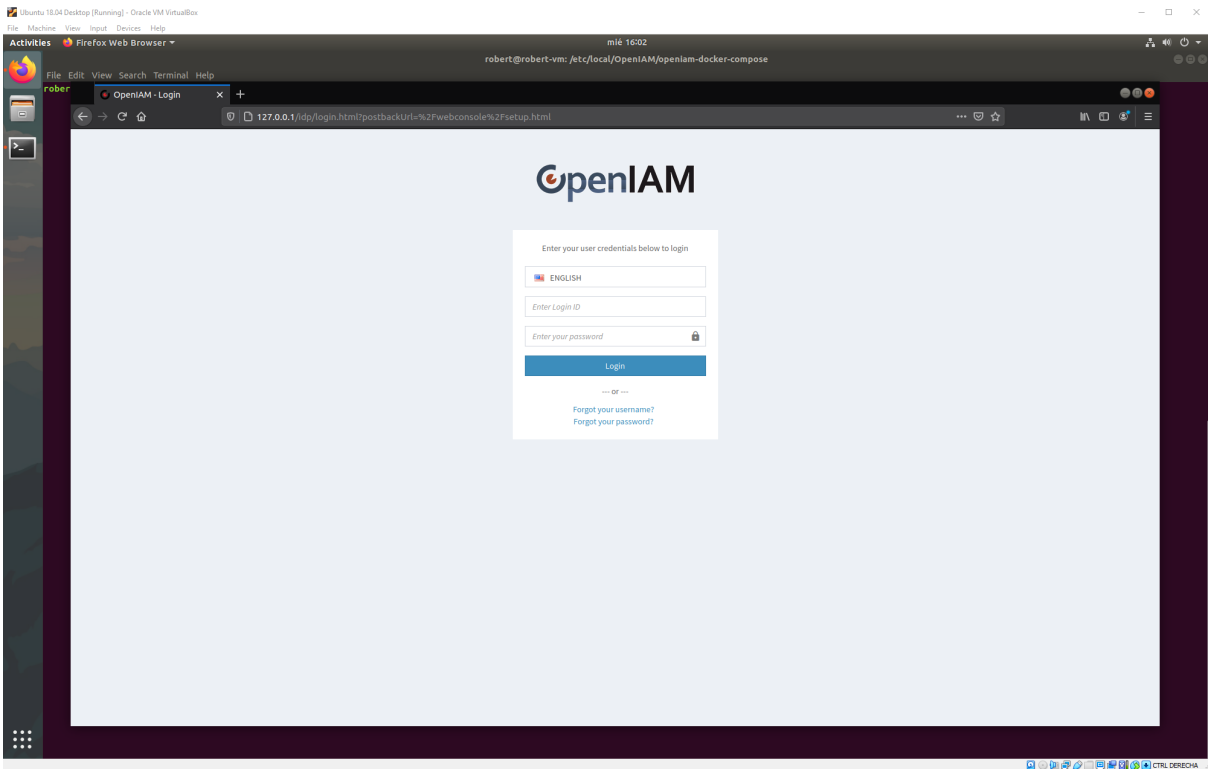
Tutorial de instalación:
https://docs.openiam.com/docs-4.1.14/html/#installation/docker410.htm%3FTocPath%3DInstallation%2520Guide%7C3.%2520Deploying%2520%2520to%2520Linux%2520with%2520Docker%2520on%2520Swarm%7C_____0#3._Deploying__to_Linux_with_Docker_on_Swarm

Máquina utilizada:

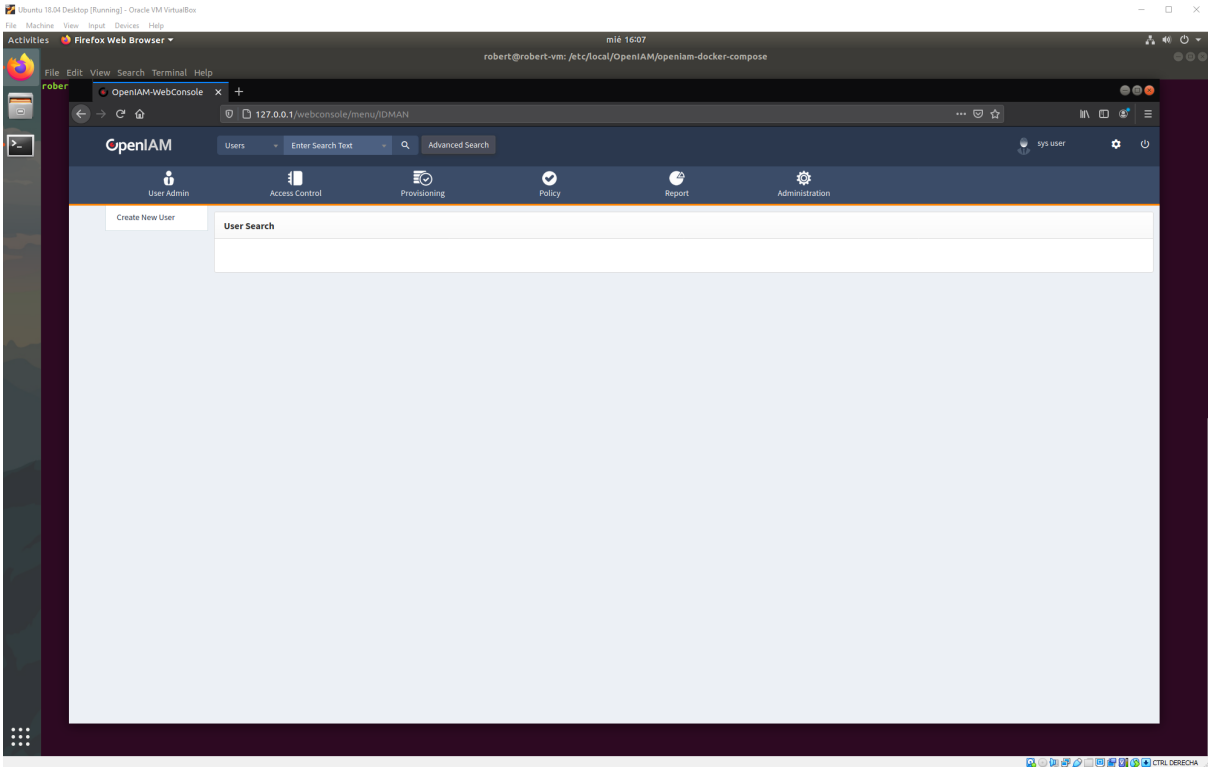
- VM Ubuntu 18.04 lts
- 8 Cores
- 8GB Ram
- 75 GB SSD

Se sigue el proceso de instalación tal cual sale en el tutorial, poner atención que al momento de bajar el repositorio se esté en la rama correspondiente a la versión del tutorial.

cred: sysadmin Operaciones1
dir: /etc/local/OpenIAM/openiam-docker-compose
cmd: ./startup.sh ./shutdown.sh ./teardown.sh



Login de OpenIAM



Vista principal de OpenIAM

Detalles encontrados

1. OpenIAM ofrece un proceso de sincronización de contraseñas con Active Directory, no obstante no nos resulta útil debido a:

    - Ocupa un middleware que se instala en Windows, por lo que si o si se necesita un Windows Server con Active Directory, no es compatible con Samba.
    - El proceso de sincronización es el que ya conocemos, se sincroniza desde AD hacia OpenIAM pero no en el sentido contrario.

2. Existe un servicio de “provisioning” en donde se menciona la capacidad de que cualquier usuario que sea creado dentro de OpenIAM sea replicado dentro de otros servicios como LDAP, AD o GSuite. Puede ser usado tanto para usuarios como grupos.

The following objects can be provisioned to target systems:

- Users
- Groups

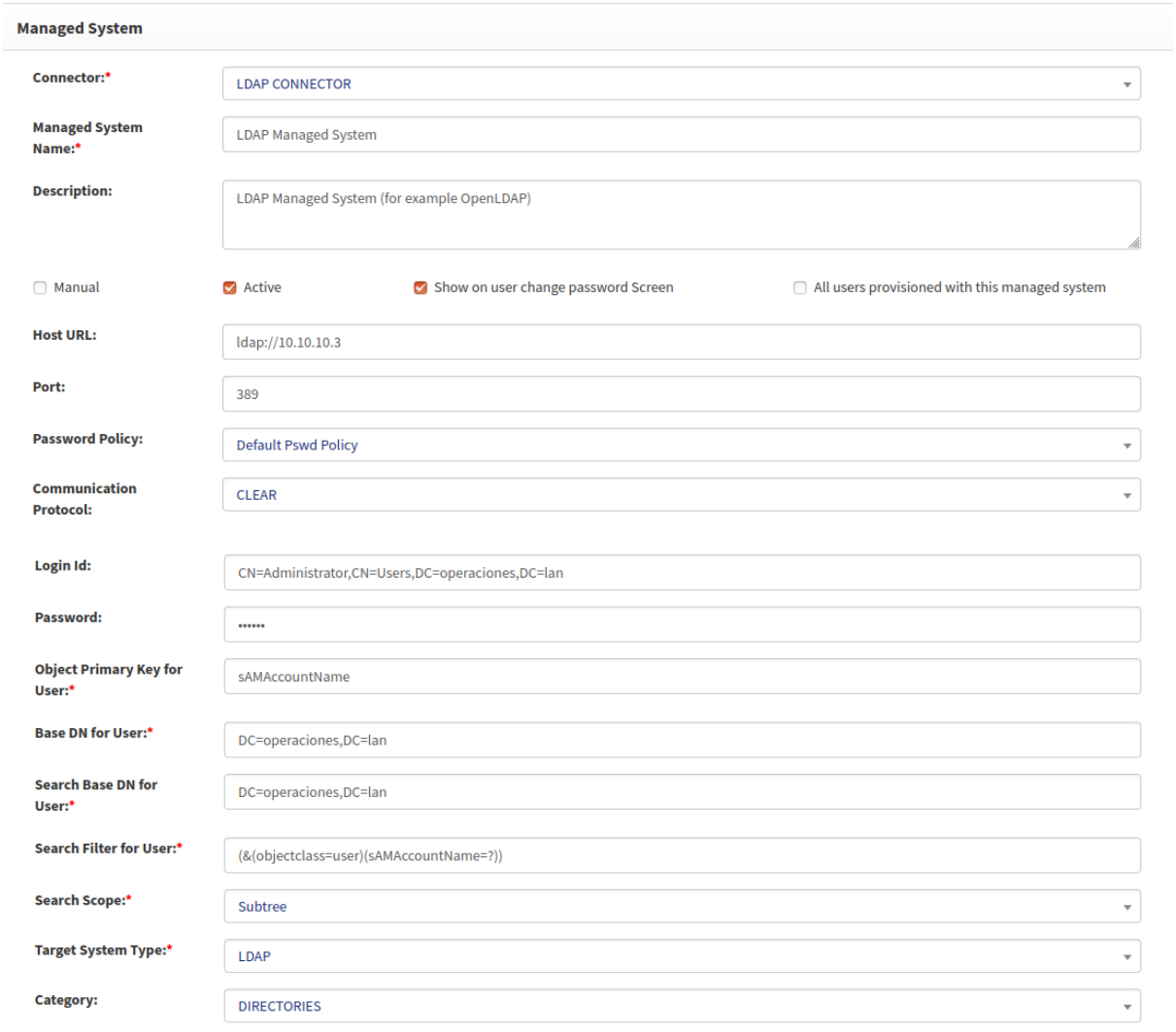
For each of these objects, a corresponding identity is created in the target system. These identities can be viewed and managed in Webconsole.

Provisioning

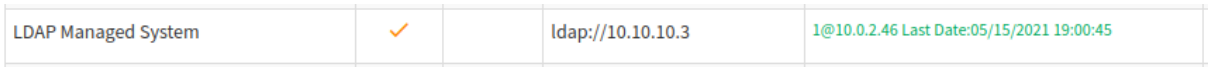
https://docs.openiam.com/docs-4.1.14/html/#administration/idm/provisioning.htm#35._Provisioning%3FTocPath%3DSystem%2520Administration%2520Guide%7CPart%2520III%253A%2520Identity%2520governance%7C35.%2520Provisioning%7C_____0

Configuración:

Entrar en la pestaña “Provisioning” y luego a “Managed System”, buscar la entrada de nombre “LDAP Managed System” e ingresar a la edición, donde se deben ingresar los siguientes valores:



Luego de un tiempo se puede ver si la configuración se aplicó correctamente:



Se configuró el siguiente mapping de atributos en la sección de “Policy Map” dentro del mismo managed system:

Object type	Attribute name	Type	Policy	Data type
PRINCIPAL	sAMAccountName	POLICY	ldap-uid	STRING

Luego de eso se creó un usuario dentro de OpenIAM para ver el asunto de la sincronización pero no se pudo encontrar el usuario en Samba AD, ya sea buscando por **RSAT Active Directory Users and Computers** o **ldapsearch**.