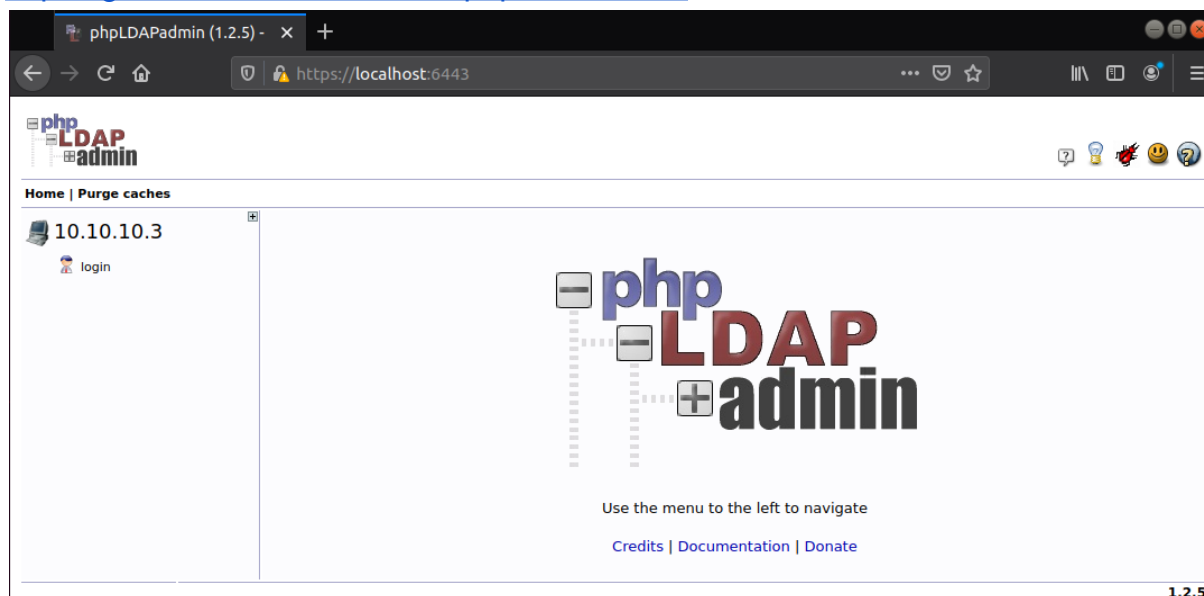


Proceso de instalación y pruebas phpLDAPAdmin en Docker

Se levanta el sistema mediante un contenedor docker:

<https://github.com/osixia/docker-phpLDAPAdmin>



Vista principal de phpLDAPAdmin

Detalles encontrados

Para poder utilizarlo, phpLDAPAdmin requiere que el servidor LDAP provea la capacidad de hacer un **anonymous bind**, opción que SAMBA trae desactivada por defecto.

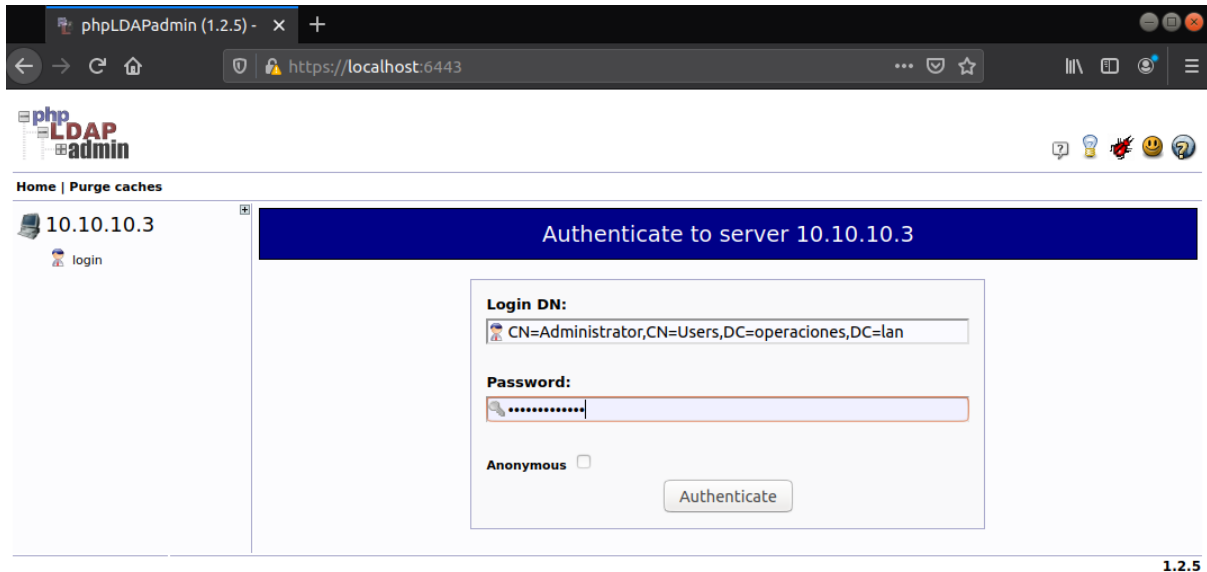
Es necesario hacer el siguiente cambio en `/etc/samba/smb.conf` en el servidor que contiene a SAMBA:

```
ldap server require strong auth = no
```

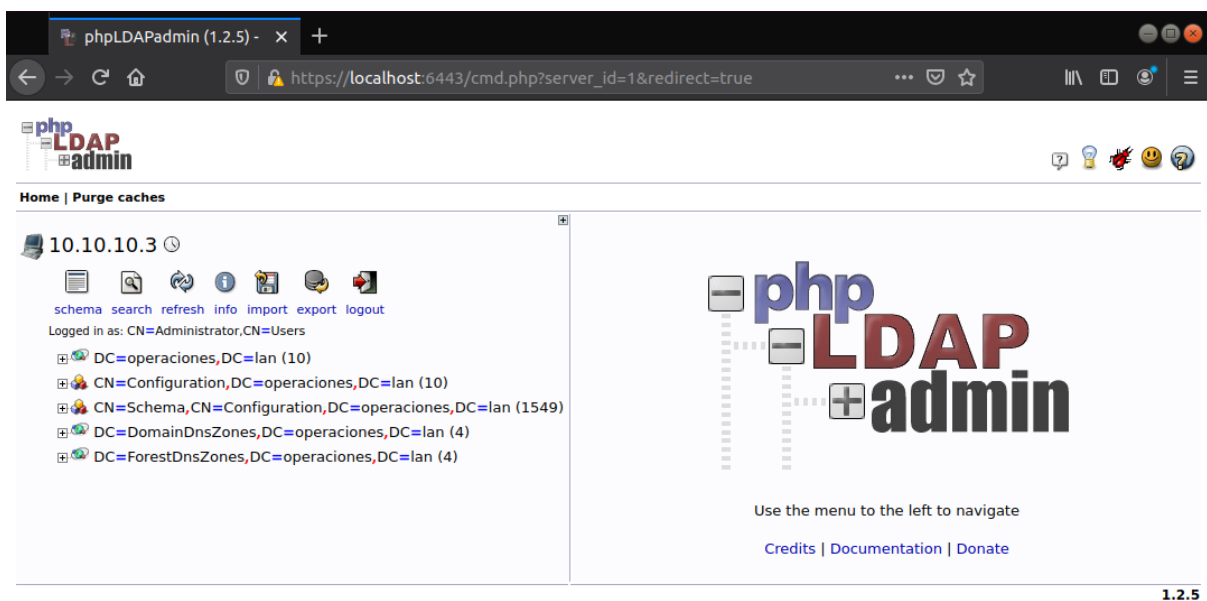
Se debe agregar el parámetro en la sección `[global]`. Una vez esto haya sido cambiado y activado (reboot) es posible entrar mediante phpLDAPAdmin.

(Side effect) este cambio hace posible las queries mediante `ldapsearch` por protocolo **ldap (389)** y no necesariamente **ldaps (636)**.

Para hacer login en phpLDAPadmin es necesario ocupar la dirección completa del **distinguished name** (DN) como Login DN, usando la password asociada a esa cuenta



Login phpLDAPadmin



Interfaz post login

Usuario para realizar pruebas: OperacionesAdmin (creado inicialmente con samba-tool)

```
# OperacionesAdmin, Users, operaciones.lan
dn: CN=OperacionesAdmin,CN=Users,DC=operaciones,DC=lan
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: OperacionesAdmin
instanceType: 4
whenCreated: 20210501195536.0Z
uSNCreated: 3771
name: OperacionesAdmin
objectGUID:: 13t7NL8BoESIDnWG8uVk6A==
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUAAAAFZelTHONeKVLueJhTwQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: OperacionesAdmin
sAMAccountType: 805306368
userPrincipalName: OperacionesAdmin@operaciones.lan
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=operaciones,DC=lan
userAccountControl: 512
memberOf: CN=Administrators,CN=Builtin,DC=operaciones,DC=lan
memberOf: CN=RSAT testgroup,CN=Users,DC=operaciones,DC=lan
memberOf: CN=Samba-tool testgroup,CN=Users,DC=operaciones,DC=lan
lastLogonTimestamp: 132643781311259680
lastLogon: 132648909389997140
pwdLastSet: 132648910110000000
whenChanged: 20210507195651.0Z
lockoutTime: 0
uSNChanged: 3793
distinguishedName: CN=OperacionesAdmin,CN=Users,DC=operaciones,DC=lan
```

Resultado de buscar el usuario "OperacionesAdmin" en Idapsearch

Todos los cambios son realizados en phpLDAPadmin y luego verificados si fueron efectivamente modificados en el servidor mediante **Idapsearch** y la herramienta **RSAT Active Directory Users and Computers**.

Se puede cambiar el **cn** (common name y name) desde phpLDAPadmin (OperacionesAdmin a OperacionesAdminPHP).

```
# OperacionesAdminPHP, Users, operaciones.lan
dn: CN=OperacionesAdminPHP,CN=Users,DC=operaciones,DC=lan
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
instanceType: 4
whenCreated: 20210501195536.0Z
uSNCreated: 3771
objectGUID:: 13t7NL8BoESIDnWG8uVk6A==
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAFAFZelTH0NeKVLueJhTwQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: OperacionesAdmin
sAMAccountType: 805306368
userPrincipalName: OperacionesAdmin@operaciones.lan
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=operaciones,DC=lan
userAccountControl: 512
memberOf: CN=Administrators,CN=Builtin,DC=operaciones,DC=lan
memberOf: CN=RSAT testgroup,CN=Users,DC=operaciones,DC=lan
memberOf: CN=Samba-tool testgroup,CN=Users,DC=operaciones,DC=lan
lastLogonTimestamp: 132643781311259680
pwdLastSet: 132648910110000000
lockoutTime: 0
lastLogon: 132648971900367020
cn: OperacionesAdminPHP
name: OperacionesAdminPHP
whenChanged: 20210507214611.0Z
uSNChanged: 3794
distinguishedName: CN=OperacionesAdminPHP,CN=Users,DC=operaciones,DC=lan
```

De igual forma, se puede cambiar el **sAMAccountName** (atributo usado por Active directory como el ID de un usuario).

sAMAccountName: OperacionesAdmin

Antes del cambio

sAMAccountName: OperacionesAdminPHP

Después del cambio

Al realizar este cambio la sesión iniciada en Windows 10 se mantuvo, incluso al cerrar sesión e intentar ingresar nuevamente con el usuario antiguo (OperacionesAdmin) es posible hacer login. No obstante, al momento de realizar un reinicio en la máquina virtual con Windows 10 se perdió esta opción y fue necesario usar la nueva credencial (OperacionesAdminPHP).

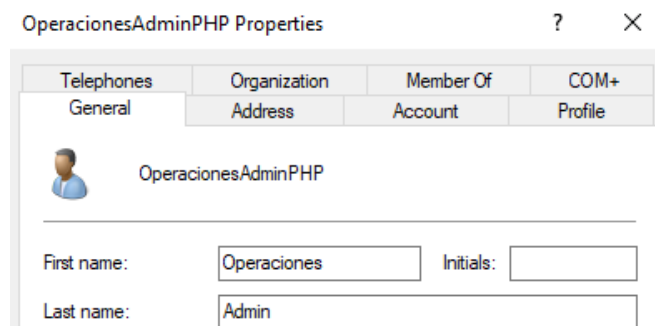
Se asume que debe ser resultado de algún aspecto de caché integrado en el sistema de Active Directory.

En cuanto a la agregación de nuevos atributos, phpLDAPadmin permite agregar atributos faltantes al usuario, no obstante, son los atributos predefinidos por el sistema.

En este caso se agregó **givenName** (primer nombre) y **sn** (surname o apellido) al usuario OperacionesAdminPHP, el cual cuando se creó en samba no se le asignó estos atributos.

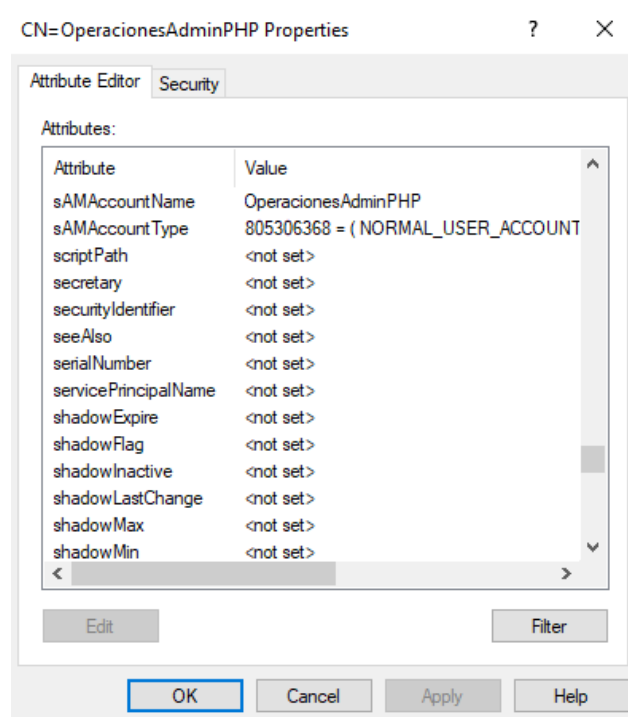
```
# OperacionesAdminPHP, Users, operaciones.lan
dn: CN=OperacionesAdminPHP,CN=Users,DC=operaciones,DC=lan
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
instanceType: 4
whenCreated: 20210501195536.0Z
uSNCreated: 3771
objectGUID:: 13t7NL8BoESIDnWG8uVk6A==
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAFAFZelTHONeKVLueJhTwQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountType: 805306368
userPrincipalName: OperacionesAdmin@operaciones.lan
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=operaciones,DC=lan
userAccountControl: 512
memberOf: CN=Administrators,CN=Builtin,DC=operaciones,DC=lan
memberOf: CN=RSAT testgroup,CN=Users,DC=operaciones,DC=lan
memberOf: CN=Samba-tool testgroup,CN=Users,DC=operaciones,DC=lan
lastLogonTimestamp: 132643781311259680
pwdLastSet: 132648910110000000
lockoutTime: 0
lastLogon: 132648971900367020
cn: OperacionesAdminPHP
name: OperacionesAdminPHP
sAMAccountName: OperacionesAdminPHP
givenName: Operaciones
sn: Admin
whenChanged: 20210507220501.0Z
uSNChanged: 3797
distinguishedName: CN=OperacionesAdminPHP,CN=Users,DC=operaciones,DC=lan
```

Resultado en ldapsearch



Resultado en RSAT Active Directory Users and Computers

En RSAT también se encuentra la herramienta **ADSI Edit**, que es una herramienta para editar usuarios, grupos y atributos del directorio pero a bajo nivel. Se pueden observar los atributos con sus nombres reales (los mismos que se obtienen desde **ldapsearch** de la siguiente forma:



Editor de atributos ADSI Edit

De todas maneras no se encuentra una forma de agregar nuevos atributos al esquema del directorio.

(Detalle encontrado más tarde) Si se activa la opción **Advanced Options** en la pestaña **View** dentro de **RSAT Active Directory Users and Computers**, es posible encontrar la misma pestaña de edición que en **ADSI Edit** al revisar las propiedades de cualquier objeto.

Se encuentra la siguiente documentación:

https://wiki.samba.org/index.php/Samba_AD_schema_extensions#Schema_Extension_in_Samba_Active_Directory

- En esta se explica el proceso de modificar el esquema del directorio, dando la capacidad de agregar nuevos atributos a utilizar.
- Se explica en la documentación que corresponde a un proceso poco seguro que puede arruinar fácilmente el sistema dejándolo inutilizable.
- Se ofrecen archivos confirmados que no generan problemas en el esquema, no obstante no se aprecia ninguno como útil.
- Personalmente, creo que es un proceso engorroso que podría trabajarse de otra forma sin la necesidad de modificar el esquema, que llevaría tiempo de pruebas, conocer y entender la sintaxis de cómo se agregan estos valores y mucho tiempo de pruebas para verificar que no ocurran problemas más tarde.