

Pruebas comparación árbol OpenLDAP y Samba

Se levanta el sistema mediante dos contenedores docker:

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

Utilizando los siguientes comandos:

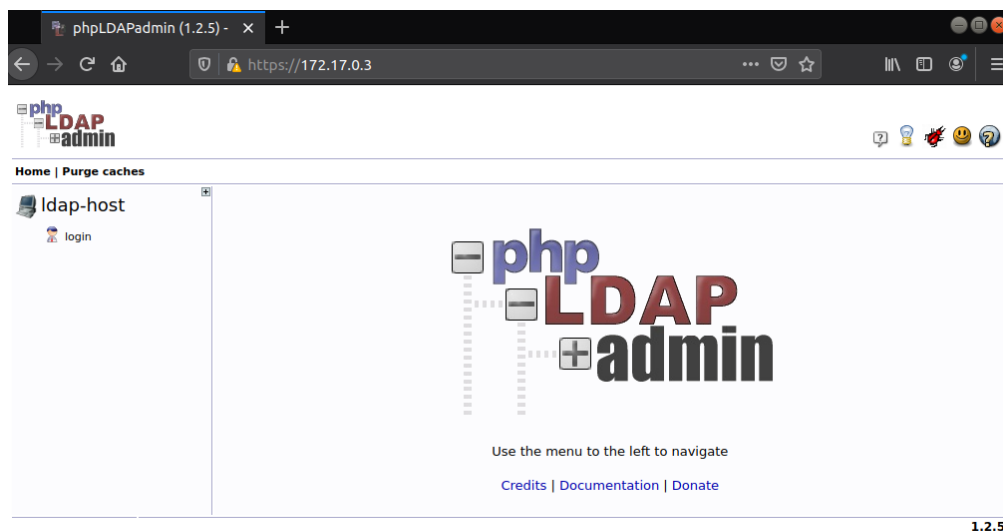
```
#!/bin/bash -e
```

```
docker run --name ldap-service --hostname ldap-service --detach osixia/openldap:1.1.8
```

```
docker run --name phpldapadmin-service --hostname phpldapadmin-service --link  
ldap-service:ldap-host --env PHPLDAPADMIN_LDAP_HOSTS=ldap-host --detach  
osixia/phpldapadmin:0.9.0
```

```
PHPLDAP_IP=$(docker inspect -f "{{ .NetworkSettings.IPAddress }}" phpldapadmin-service)
```

Con ese comando se levanta un servidor de OpenLDAP junto a un servidor de phpLDAPAdmin configurado para conectarse al contenedor de OpenLDAP.



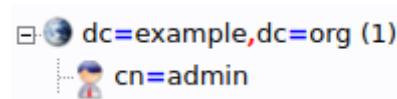
Vista principal de phpLDAPAdmin

Luego de ingresar a la dirección IP que se obtiene al final de los comandos anteriores, se inicia sesión con las siguientes credenciales:

Login DN: cn=admin,dc=example,dc=org

Password: admin

Lo único que viene creado por defecto en este servidor es el dominio “example.org” y el usuario “admin”.



Árbol inicial OpenLDAP

Diferencias

Create Object

Server: ldap-host Container: dc=example,dc=org

Select a template for the creation process

☐ Courier Mail: Account

☐ Courier Mail: Alias

☐ Generic: Address Book Entry

☐ Generic: DNS Entry

☐ Generic: LDAP Alias

☐ Generic: Organisational Role

☐ Generic: Organisational Unit

☐ Generic: Posix Group

☐ Generic: Simple Security Object

☐ Generic: User Account

☐ Kolab: User Entry

☐ Samba: Account

☐ Samba: Domain

☐ Samba: Group Mapping

☐ Samba: Machine

☒ Sendmail: Alias

☒ Sendmail: Cluster

☒ Sendmail: Domain

☒ Sendmail: Relays

☒ Sendmail: Virtual Domain

☒ Sendmail: Virtual Users

☐ Thunderbird: Address Book Entry

☐ Default

Templates OpenLDAP

Create Object

Server: 10.10.10.3 Container: DC=operaciones,DC=lan

Select a template for the creation process

☐ Courier Mail: Account

☐ Courier Mail: Alias

☐ Generic: Address Book Entry

☒ Generic: DNS Entry

☒ Generic: LDAP Alias

☐ Generic: Organisational Role

☐ Generic: Organisational Unit

☐ Generic: Posix Group

☒ Generic: Simple Security Object

☐ Generic: User Account

☐ Kolab: User Entry

☐ Samba: Account

☒ Samba: Domain

☐ Samba: Group Mapping

☐ Samba: Machine

☒ Sendmail: Alias

☒ Sendmail: Cluster

☒ Sendmail: Domain

☒ Sendmail: Relays

☒ Sendmail: Virtual Domain

☒ Sendmail: Virtual Users



☐ Thunderbird: Address Book Entry

☐ Default

Templates Samba AD

A primera vista, hay algunos templates predefinidos en phpLDAPadmin que no se encuentran disponibles en la versión de Samba AD (*Generic: DNS Entry*, *Generic: LDAP Alias*, *Generic: Simple Security Object*, y *Samba: Domain*).

Todos los objetos a ser creados en el árbol de Samba AD requieren el ingreso de los tres siguientes atributos:

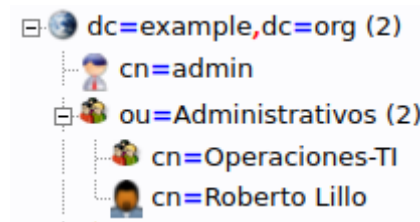
instanceType	
<input type="text"/>	*
nTSecurityDescriptor	
<input type="text"/>	*
objectCategory	
 <input type="text"/> 	*

Atributos únicos de Samba AD

Estos no son solicitados en ningún objeto creado en OpenLDAP.

Tarea: buscar cuales son esos atributos, ya que no son campos autocompletables y si no los ingreso, no puedo crear un usuario en Samba AD desde phpLDAPadmin.

En relación a las capacidades de creación de objetos para jerarquía, en OpenLDAP igualmente es posible crear Unidades Organizacionales, grupos y usuarios tal cual en Samba AD.



Árbol en OpenLDAP

Al consultar el árbol completo por `ldapsearch` se obtiene lo siguiente:

```
robert@robert-vm:~$ ldapsearch -x -H ldap://172.17.0.2 -b dc=example,dc=org -D "cn=admin,dc=example,dc=org" -w admin
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=org> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# example.org
dn: dc=example,dc=org
objectClass: top
objectClass: dcObject
objectClass: organization
o: Example Inc.
dc: example

# admin, example.org
dn: cn=admin,dc=example,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9NzNXLzI2R2pFdEk4cGx0QjN2SUo5L2ZXUEFPWnA3Zm4=

# Administrativos, example.org
dn: ou=Administrativos,dc=example,dc=org
ou: Administrativos
objectClass: organizationalUnit
objectClass: top

# Operaciones-TI, Administrativos, example.org
dn: cn=Operaciones-TI,ou=Administrativos,dc=example,dc=org
cn: Operaciones-TI
gidNumber: 500
objectClass: posixGroup
objectClass: top

# Roberto Lillo, Administrativos, example.org
dn: cn=Roberto Lillo,ou=Administrativos,dc=example,dc=org
givenName: Roberto
sn: Lillo
cn: Roberto Lillo
uid: rlillo
userPassword:: e01ENX02UF1EdURJT1JpWlpCR29hcER0RVNnPT0=
uidNumber: 1000
gidNumber: 500
homeDirectory: /home/users/rlillo
loginShell: /bin/bash
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
```

Consulta árbol completo por `ldapsearch` hacia OpenLDAP

Se puede observar que la uid creada por defecto en mi caso es “rlillo”, lo que podría explicar por qué se utiliza ese tipo de credencial de usuario en el DIINF, debe ser legado de Samba 3.

En el aspecto de agregar atributos a un objeto, OpenLDAP trae unos pocos definidos:

audio	mobile	title
businessCategory	o	userCertificate
carLicense	ou	userPKCS12
departmentNumber	pager	userSMIMECertificate
description	photo	x121Address
destinationIndicator	physicalDeliveryOfficeName	x500UniqueIdentifier
displayName	postOfficeBox	
employeeNumber	postalAddress	
employeeType	postalCode	
Fax	preferredDeliveryMethod	
gecos	preferredLanguage	
homePhone	registeredAddress	
homePostalAddress	roomNumber	
initials	secretary	
internationaliSDNNumber	seeAlso	
jpegPhoto	st	
l	street	
labeledURI	Telephone	
Email	teletexTerminalIdentifier	
manager	telexNumber	

Atributos predefinidos por OpenLDAP

En comparación Samba AD trae muchos más atributos, pero probablemente muchos fueron definidos especialmente por el tema de compatibilidad con Windows Active Directory.

Respecto a las unidades organizacionales en Unix, se encuentran la siguiente información al respecto:

- What is the difference between Organizational Unit and posixGroup in LDAP?
<https://stackoverflow.com/questions/51657903/what-is-the-difference-between-organizational-unit-and-posixgroup-in-ldap>
- OpenLDAP - Add an organizational unit (OU)
<http://www.freekb.net/Article?id=1495>
- Create Organizational units (OU) from Unix.
<https://samba.samba.narkive.com/rBIOHO0h/create-organizational-units-ou-from-unix>

Por lo que se puede apreciar en los links anteriores, el concepto de unidad organizacional es también usado en OpenLDAP y por lo tanto en Unix, no obstante, da la impresión de ser utilizado para dar orden y jerarquía al árbol solamente en vez de ser utilizado para políticas como en Active Directory.

Extra: también existe el concepto de herencia entre unidades organizacionales, lo cual no es una habilidad de los grupos, requiere un poco más de búsqueda.