



Universidad de Buenos Aires

MANUAL LDAP v1

Julio 2010

Resumen

En este documento se explica cómo dar de alta usuarios del servicio de ProxyRevistas brindado por el CCC al esquema LDAP. En la primer parte del documento se presentan los pasos a seguir por un administrador de una dependencia y en el final lo que corresponde al usuario del servicio.

Índice

1. LDAP	2
2. Administradores	2
2.1. Agregando un nuevo usuario	3
2.2. Borrando un usuario	5
3. Usuarios	6
A. Anexo	7
A.1. NetFlow	7

1. LDAP

LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red.

El protocolo accede a directorios LDAP, que siguen la siguiente estructura:

- Un directorio es un árbol de entradas de directorio.
- Una entrada consta de un conjunto de atributos.
- Un atributo tiene un nombre y uno o más valores. Los atributos son definidos en un esquema.
- Cada entrada tiene un identificador único: su Nombre distinguido (Distinguished Name, DN). Este consta de su Relative Distinguished Name (RDN) construido por algunos atributos en la entrada, seguidos del DN de la entrada del padre.

Existen diversas implementaciones de este protocolo, siendo *OpenLDAP* una de las más usadas, entre otras razones, porque es una implementación libre que soporta múltiples esquemas, pudiéndose utilizar para conectarse a cualquier otro LDAP. *OpenLDAP* es entonces la implementación elegida.

Para que la administración de usuarios sea más amigable se instaló un administrador web llamado *phpLdapAdmin*.

2. Administradores

Para comenzar, a través de cualquier navegador web debemos ingresar en **ldaps.ccc.uba.ar**. Si bien está en inglés, la interfaz es bastante amigable. Sobre la parte izquierda superior debemos hacer clic en *Login* y luego aparecerá una pantalla que nos pide usuario y contraseña. Por ejemplo, para la Facultad de Ciencias Veterinarias:

```
Login DN:          cn=admin,dc=veterinaria,dc=uba,dc=ar
Password:          123456
```

La primera vez que se ingresa es recomendable que modifiquen la contraseña que nosotros les asignamos.

Una vez logueados, podrán ver a su izquierda sólo la parte del árbol que administran, el cual sigue el esquema propuesto a nivel RedUBA. Entonces:

- Si se hace clic en el signo + se despliegan los directorios.
- Si se hace clic en el nombre del usuario, se puede ver el detalle de sus datos, modificarlos o agregar nuevos.

Para salir es recomendable, antes de cerrar la ventana, desloguearse haciendo clic en *Logout*.

2.1. Agregando un nuevo usuario

La forma más sencilla para agregar nuevos usuarios es tener una plantilla de base e importar el archivo a través de *phpLdapAdmin* en un formato *LDIF*. Por ejemplo, si se desea agregar una persona para el esquema propuesto a nivel RedUBA:

```
dn: uid=<id.unico>,ou=Personas,ou=Usuarios,dc=<dependencia>, \
    dc=uba,dc=ar
uid: <id.unico>
objectClass: top
objectClass: persona
userPassword: <password>
```

donde se debería reemplazar <id.unico>, <dependencia> y <password>.

Se recuerda que un *objectClass*, en este caso **persona**, tiene atributos obligatorios y atributos optativos. En los ejemplos sólo se especifican los obligatorios, los demás podrán agregarse posteriormente.

Aclaraciones:

- uid: todavía no hubo acuerdo sobre qué uid usar a nivel RedUBA, en algunos casos se usa DNI y en otros dirección de correo.
- userPassword: a modo de ejemplo se puso uno cualquiera en texto claro, el formato *LDIF* nos brinda la posibilidad de subir directamente el *hash md5* o cualquier otro. Para el ejemplo anterior habría que reemplazar:

```
- userPassword: 123456
+ userPassword: {MD5}+LzSTxzNcmuMstWa6HTtpA==
```

Luego, se le agrega la rama servicios a la persona creada previamente:

```
dn: cn=servicios,uid=<id.unico>,ou=Personas,ou=Usuarios,dc=<dependencia>, \
    dc=uba,dc=ar
cn: servicios
objectClass: top
objectClass: servicios
```

Y por último, se le agrega el servicio ProxyRevistas:

```
dn: cn=proxyrevistas,cn=servicios,uid=<id.unico>,ou=Personas,ou=Usuarios, \
    dc=<dependencia>,dc=uba,dc=ar
objectClass: proxyrevistas
cn: proxyrevistas
Activo: 1
mail: <usuario>@<dependencia>.uba.ar
uid: <usuario>
userPassword: 654321
```

Aclaraciones:

- mail: No es necesario que el usuario disponga de una cuenta de correo brindada por la dependencia. Este campo es el que el usuario ingresa para identificarse, y el formato propuesto sirve para delegar las autenticaciones por dependencia. Si el usuario tiene una cuenta de la dependencia, se puede aprovechar para este campo.
- usuario: el usuario del atributo mail y el usuario del atributo uid deben coincidir para que el servicio funcione.
- userPassword: es el password para acceder sólo al servicio ProxyRevistas. Dada la dificultad que le puede presentar a las personas recordar diferentes contraseñas, un buen criterio sería que utilicen una misma contraseña para todos los servicios.

Para una carga masiva de usuarios, esto podría automatizarse a través de un *script*.

La <dependencia> del mail es la misma usada como dominio de cada dependencia. En la siguiente tabla se listan todas:

Dependencia	<dependencia>
Facultad de Agronomía	agro
Facultad de Arquitectura Diseño y Urbanismo	fadu
CBC	cbc
CBC sede Avellaneda	cbc_avellaneda
CBC sede Martínez	cbc_martinez
Centro Franco-Argentino	centro_fa
Hospital de Clínicas	hospitaldeclinicas
Colegio Nacional Buenos Aires	cnba
Facultad de Derecho	derecho
Facultad de Ciencias Económicas	econ
Facultad de Ciencias Exactas y Naturales	fcen y <dpto>.fcen
Facultad de Farmacia y Bioquímica	ffyb
Facultad de Filosofía y Letras	filo y <*>.filo
INGEBI	dna
Facultad de Ingeniería	fi
Radio UBA	la_radio
Instituto Lanari	lanari
Instituto Leloir	leloir
Facultad de Medicina	fmed
Facultad de Odontología	odon
Escuela Nacional de Comercio Carlos Pellegrini	pellegrini
Facultad de Psicología	psi y <*>.psi
Rectorado	rec
Instituto Roffo	roffo
Centro Cultural Ricardo Rojas	rojas
Dirección de Salud	salud
SISBI	biblos.sisbi
Facultad de Ciencias Sociales	sociales
UBATEC	ubatec
Instituto Vaccarezza	vaccarezza
Facultad de Ciencias Veterinarias	fvet y <dpto>.fvet

2.2. Borrando un usuario

Debemos seleccionar al usuario en el directorio de la izquierda. Sobre la parte de la derecha hacemos clic en *Delete this entry* y nos pide confirmación (*Delete* o *Cancel*).

3. Usuarios

Los usuarios comunes tienen que configurar su navegador para que use Proxy Revistas:

Nombre del proxy: `proxyrevistas.uba.ar`
Puerto: 8080

Luego, en la primera página que intenten acceder se les pide usuario y contraseña. Recordar que donde dice usuario en realidad hay que poner el mail en formato *usuario@dependencia.uba.ar*.

A. Anexo

A.1. NetFlow

Aprovechamos para comentarles que se encuentra disponible para los administradores una herramienta brindada por el CCC que permite analizar el tráfico en forma detallada a través de una interfaz web, con la cual es posible hacer estadísticas, detectar tráfico anómalo, etc. Para poder realizar esto, el sistema provee datos detallados del tráfico tales como direcciones IP, protocolos de red y transporte, y los puertos que utilizan los protocolos de transporte. Los datos del tráfico son ingresados al sistema casi en tiempo real (cada 5 minutos), y se guarda un historial de aproximadamente dos semanas permitiendo realizar análisis de eventos pasados.

El acceso a la interfaz está restringido por nombre de dependencia y contraseña (autenticando contra `ldaps.ccc.uba.ar`), y es accesible sólo desde dentro de la RedUBA. Para poder ingresar deben entrar en `netflow.ccc.uba.ar`, y si es la primera vez deben completar el login con:

Usuario: `<dependencia>`

Contraseña: `123456`

Si tienen dudas con respecto al nombre asociado a su dependencia, deben ingresar a `ldaps.ccc.uba.ar` con sus claves de administradores y verificar que lo que están ingresando en NetFlow coincida con su `dc=<dependencia>,dc=uba,dc=ar`.

Recomendamos que la primera vez que accedan al sistema ingresen a la solapa *Documentación* en la cual se explica como se utiliza esta herramienta.

Para poder cambiar la contraseña tendrán que entrar en `ldaps.ccc.uba.ar`, desplegar *Aplicaciones* y modificar el contenido de `userPassword` por lo que deseen. El User Name no podrá modificarse ya que se encuentra asociado al perfil creado en NetFlow.

En la siguiente figura se resalta lo comentado anteriormente: nombre de dependencia, aplicación NetFlow y atributo `userPassword`:

phpLDAPadmin

Home Purge caches Request feature Report a bug Donate Help

phpLDAPadmin

LDAP CCC Primario

schema search refresh info import export logout

Logged in as: cn=admin,dc=derecho

- dc=uba,dc=ar (1)
- dc=derecho (3)
- cn=admin
- ou=Aplicaciones (1)
 - cn=netflow
- ou=Usuarios (2)

LDAP CCC Primario

Server: LDAP CCC Primario Distinguished Name: cn=netflow,ou=Aplicaciones,dc=derecho,dc=uba,dc=ar Template: No Template

Refresh Copy or move this entry Delete this entry Compare with another entry Add new attribute

Export Show internal attributes Rename Create a child entry

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

cn required, rdn

netflow (rename) *

objectClass required

top *

netflow (structural) (add value)

User Name alias, required

derecho (add value) *

userPassword required

***** (add value) *

Check password...

Save Changes