Servei SAMBA (part3)
Samba-Ldap

Curs 2016-2017

Descripció dels aprenentatges:

1. Configurar un servidor ldap autònom en un docker amb el DIT complet de edt.org.
2. Configurar un docker amb el servei samba amb shares amb permisos a nivell d'usuaris.
3. Configurar el servidor samba per usar de backend ldapsam.
4. Instal·lar i configurar smbldap-tools per poder-les usar contra el ldap.
5. Fer el populate del DIT del ldap per afegir-hi les entitats i els usuaris/grups/recursos de samba necessaris per poder usar ldap.
6. Configurar el servidor samba perquè la resolució d'usuaris unix es faci via ldap. Configurar nslcd.
7. Provar la creació/modificació/bloqueig/desbloqueig/eliminar usuaris samba. Llistar-los via pdbedit i via ldapsearch.

Consulteu:

github edtasixm06/samba:18ldapsam
dockerhub edtasixm06/samba:18ldapsam

github: edtasixm06/ldapserver:18samba
dockerhub edtasixm06/ldapserver:18samba

github: edtasixm06/hostpam:18homesamba
dockerhub edtasixm06/hostpam:18homesamba

Documentació

Samba wiki: LDAP

- **Chapter11: Account information database. The official samba 3.5 Howto ans reference guide**
  https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html#id2592519
- samba & ldap
  https://wiki.samba.org/index.php/Samba_%26_LDAP
- The official samba 4 howto
  https://www.samba.org/samba/docs/man/Samba4-HOWTO/
- User documentation
  https://wiki.samba.org/index.php/User_Documentation

- **The Linux samba openldap howto (2007)**
  http://download.gna.org/smbldap-tools/docs/samba-ldap-howto/

Ubuntu Samba amb ldap:

- **Ubuntu Samba amb ldap:**
  Samba & Ldap the official ubuntu documentation

O'reilly 2007 using samba

- **Oreilly 2007 using samba….**
  chapter 5 Accounts….

Samba PDC

- Stting up samba as an active domain controller
  https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller

edoceo

- samba tdbsam to ldap migration
  https://edoceo.com/howto/samba-ldap-migration

Samba amb Ldap: Stand Alone Server

Dockers:

- edtasixm06/ldap:ldapSmbServer
- edtasixm06/samba:smbldap

Procediment d'instal·lació:

- Instal·lar samba i smbldap-tools

Servidor slapd:

- slapd.conf modificar per incloure el schema de samba.
- ?? posar al salpd.conf els índex pertinents per a objectes samba

Servidor samba:

- configurar samba amb el backend *ldapsam:ldap://172.17.0.2/*
- configurar els fitxers de *smbldap-tools /etc/smbldap-tools/smbldap.conf* i *smbldap_bind.conf*. establint els noms del DIT i els passwords apropiats.
- posar el passwd de samba admin dn: ***smbpasswd -x secret***
- *smbldap-populate* afegeix a la base de dades ldap l'estructura de samba necessària. Podem generar un ldif intermig amb tot allò que generarà. Genera tot de users i grups.

```
[root@samba docker]# smbpasswd -w secret
Setting stored password for "cn=Manager,dc=edt,dc=org" in secrets.tdb
```

Generar el servidor samba (unix users locals)

```
[root@samba01 /]# smbldap-populate
Populating LDAP directory for domain SAMBA
(S-1-5-21-955855521-2459260878-1327528046)
(using builtin directory structure)

entry dc=edt,dc=org already exist.
entry ou=usuaris,dc=edt,dc=org already exist.
entry ou=grups,dc=edt,dc=org already exist.
entry ou=hosts,dc=edt,dc=org already exist.
entry ou=domains,dc=edt,dc=org already exist.
adding new entry: sambaDomainName=SAMBA,dc=edt,dc=org
adding new entry: sambaDomainName=sambaDomain,dc=edt,dc=org
adding new entry: uid=root,ou=usuaris,dc=edt,dc=org
adding new entry: uid=nobody,ou=usuaris,dc=edt,dc=org
adding new entry: cn=Domain Admins,ou=grups,dc=edt,dc=org
adding new entry: cn=Domain Users,ou=grups,dc=edt,dc=org
adding new entry: cn=Domain Guests,ou=grups,dc=edt,dc=org
adding new entry: cn=Domain Computers,ou=grups,dc=edt,dc=org
adding new entry: cn=Administrators,ou=grups,dc=edt,dc=org
adding new entry: cn=Account Operators,ou=grups,dc=edt,dc=org
adding new entry: cn=Print Operators,ou=grups,dc=edt,dc=org
adding new entry: cn=Backup Operators,ou=grups,dc=edt,dc=org
adding new entry: cn=Replicators,ou=grups,dc=edt,dc=org

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
```

Llistat de dn elements afegits

```
dn: sambaDomainName=SAMBA01,dc=edt,dc=org
dn: sambaDomainName=SAMBA,dc=edt,dc=org
dn: sambaDomainName=sambaDomain,dc=edt,dc=org
dn: uid=root,ou=usuaris,dc=edt,dc=org
dn: uid=nobody,ou=usuaris,dc=edt,dc=org
dn: cn=Domain Admins,ou=grups,dc=edt,dc=org
dn: cn=Domain Users,ou=grups,dc=edt,dc=org
dn: cn=Domain Guests,ou=grups,dc=edt,dc=org
dn: cn=Domain Computers,ou=grups,dc=edt,dc=org
dn: cn=Administrators,ou=grups,dc=edt,dc=org
dn: cn=Account Operators,ou=grups,dc=edt,dc=org
dn: cn=Print Operators,ou=grups,dc=edt,dc=org
dn: cn=Backup Operators,ou=grups,dc=edt,dc=org
dn: cn=Replicators,ou=grups,dc=edt,dc=org
```

Utilitats smbldap:

```
[root@samba docker]# smbldap-
smbldap-config     smbldap-grouplist        smbldap-passwd           smbldap-useradd          smbldap-userlist
smbldap-groupadd         smbldap-groupmod         smbldap-populate         smbldap-userdel
smbldap-usermod
smbldap-groupdel         smbldap-groupshow        smbldap-upgrade-0.9.6.pl  smbldap-userinfo
smbldap-usershow
```

Trick: enganyar amb usuaris unix locals

El servidor ldap conté els usuaris unix i està configurat amb el populate per rebre les dades de samba.

El servidor samba amb *smbldap-populate* posa al DIT els elements estructurals necessaris per al samba com objectes de descripció del domini, comptes de root, admin, etc. Crea root i nobody (entre altres) perquè són els usuaris que hi ha al /etc/password del samba.

?? Potser populate posaria al servidor samba més usuaris del /etc/passwd si els tingues? o no per evitar conflicte amb el DIT

En fer pdbedit -Lv es veu que com a usuaris ara únicament hi ha root i nobody.
No es pot crear usuaris samba nous perquè no existeixen com a unix localment.
El samba busca els usuaris a unix, el unix pot estar configurat a /etc/passwd o a ldap.
Si encara no està configurat a ldap el samba no pot crear usuaris samba com “Pau Pou” que està al ldap perquè no el troba.

Truc:
enganyem el sistema creant localment al /etc/passwd un Pau Pou amb idem uid i gid que el del ldap i fem el smbpasswd. Veurem que si el dona d’alta i el podem llistar amb pdbedit i també omple els camps samba del ldap del Pau Pou.
És a dir, hem enganyat al samba que ha trobat el pau pou de únic /etc/passwd i ha desat les dades al pau pou de ldap.

Arreglar-ho
Cal que si volem usar ldap el servidor samba implementi els usuaris de unix també via ldap. Caldrà configurar nscd i nslcd.

Generar el servidor samba: unix users ldap

Configurar el servidor samba perquè els usuaris unix els localitzi via ldap, que es pugui fer getent i trobi usuaris i grups ldap.. Cal usar nscd i nslcd.

- paquets nss-pam-ldapd
- (your host will need to be able to see (enumerate) those users via NSS; install and configure either libnss-ldapd or libnss-ldap):
- libnss-ldapd or libnss-ldap

Configurar /etc/nsswitch.conf

```
passwd:     ldap files sss
shadow:     ldap files sss
group:      ldap files sss
```

Configurar /etc/nscd.conf

```
<no cal modificar res>
```

Configurar /etc/nslcd.conf

```
[root@samba01 docker]# grep -v "^#" /etc/nslcd.conf  | grep -v "^ *$"
uid nslcd
gid ldap
uri ldap://172.17.0.2
base dc=edt,dc=org
```

Engegar el servei nslcd

```
[root@samba01 docker]# /usr/sbin/nslcd && echo "ok"
ok
```

Comprovació amb getent: passwd

```


[root@samba01 docker]# getent passwd
pau:*:5000:100:Pau Pou:/tmp/home/pau:
pere:*:5001:100:Pere Pou:/tmp/home/pere:
anna:*:5002:600:Anna Pou:/tmp/home/anna:
marta:*:5003:600:Marta Mas:/tmp/home/marta:
jordi:*:5004:100:Jordi Mas:/tmp/home/jordi:
admin:*:10:10:Administrador Sistema:/tmp/home/admin:
user01:*:7001:610:user01:/tmp/home/1asix/user01:
user02:*:7002:610:user02:/tmp/home/1asix/user02:
user02:*:7003:610:user03:/tmp/home/1asix/user03:
user04:*:7004:610:user04:/tmp/home/1asix/user04:
user05:*:7005:610:user05:/tmp/home/1asix/user05:
user06:*:7006:611:user06:/tmp/home/2asix/user06:
user07:*:7007:611:user07:/tmp/home/2asix/user07:
user08:*:7008:611:user08:/tmp/home/2asix/user08:
user09:*:7009:611:user09:/tmp/home/2asix/user09:
user10:*:7010:611:user10:/tmp/home/2asix/user10:
mao:*:11001:650:mao tse tung:/tmp/home/1wiaw/mao:
ho:*:11002:650:ho chi minh:/tmp/home/1wiaw/ho:
hiro:*:11003:650:hirohito:/tmp/home/1wiaw/hiro:
nelson:*:11004:650:nelson mandela:/tmp/home/1wiaw/nelson:
robert:*:11005:650:robert mugabe:/tmp/home/1wiaw/robert:
ali:*:11006:650:ali bey:/tmp/home/1wiaw/ali:
konrad:*:11007:651:konrad adenauer:/tmp/home/2wiaw/konrad:
humphrey:*:11008:651:humpprey appleby:/tmp/home/2wiaw/humphrey:
carles:*:11009:651:carles puigdemon:/tmp/home/2wiaw/carles:
francisco:*:11010:651:francisco franco bahamonde:/tmp/home/2wiaw/fracisco:
vladimir:*:11011:651:vladimir putin:/tmp/home/2wiaw/vladimir:
jorge:*:11012:651:jorge mario bergoglio:/tmp/home/2wiaw/jorge:
```

```
root:x:0:0:Netbios Domain Administrator:/home/root:/bin/false
nobody:x:999:514:nobody:/nonexistent:/bin/false
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-timesync:x:999:998:systemd Time Synchronization:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
nslcd:x:65:55:LDAP Client User:/:/sbin/nologin
```

Comprovació amb getent group

```
[root@samba01 docker]# getent group
cup:*:0:
admin:*:10:
system:*:10:
alumnes:*:600:
profes:*:100:
1wiaw:*:650:
2wiaw:*:651:
1asix:*:611:
2asix:*:651:
Domain Admins:*:512:root
Domain Users:*:513:
Domain Guests:*:514:
Domain Computers:*:515:
Administrators:*:544:
Account Operators:*:548:
Print Operators:*:550:
Backup Operators:*:551:
Replicators:*:552:
root:x:0:
bin:x:1:
```

```
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
input:x:999:
systemd-journal:x:190:
systemd-timesync:x:998:
systemd-network:x:192:
systemd-resolve:x:193:
dbus:x:81:
nscd:x:28:
ldap:x:55:
```

Crear un usuari samba

Crear al ldap sobre un usuari unix ja existent un usuari samba (li afegeix els camps samba).

```
[root@samba01 docker]# smbpasswd -a pau
New SMB password:
Retype new SMB password:
Added user pau.
```

```
[root@samba01 docker]# pdbedit -L
pau:5000:Pau Pou
```

```
root:0:root
nobody:999:nobody

[root@samba01 docker]# pdbedit -Lv pau
Unix username:         pau
NT username:           pau
Account Flags:         [U          ]
User SID:              S-1-5-21-955855521-2459260878-1327528046-1002
Primary Group SID:     S-1-5-21-955855521-2459260878-1327528046-513
Full Name:             Pau Pou
Home Directory:        \\samba01\pau
HomeDir Drive:
Logon Script:
Profile Path:          \\samba01\pau\profile
Domain:                SAMBA01
Account desc:          Watch out for this guy
Workstations:
Munged dial:
Logon time:            0
Logoff time:           never
Kickoff time:          never
Password last set:     Mon, 19 Dec 2016 16:26:35 UTC
Password can change:  Mon, 19 Dec 2016 16:26:35 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```
[root@ldapserver docker]# ldapsearch -xLLL -b 'dc=edt,dc=org' "cn=Pau Pou"
dn: cn=Pau Pou,ou=usuaris,dc=edt,dc=org
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
cn: Pau Pou
cn: Pauet Pou
sn: Pou
homePhone: 555-222-2220
mail: pau@edt.org
description: Watch out for this guy
ou: Profes
uid: pau
uidNumber: 5000
gidNumber: 100
homeDirectory: /tmp/home/pau
sambaSID: S-1-5-21-955855521-2459260878-1327528046-1002
```

```
displayName: Pau Pou
userPassword:: e1NTSEF9MlNxaFUvR05pQzZ0NitnWlZrVDBFQmh6VzBybGx2a3U=
sambaNTPassword: 06A7F4852E85B2256DD2C18845D22112
sambaPasswordHistory:
00000000000000000000000000000000000000000000000000000000
 00000000
sambaPwdLastSet: 1482164795
sambaAcctFlags: [U          ]
```

Sinchronizing passwords

Apèndix

Ordres utilitats

```
net getlocalsid
net getdomainsid
net usersidlist
pdbedit -Lv
```

```
[root@samba docker]# smbpasswd -w secret
Setting stored password for "cn=Manager,dc=edt,dc=org" in secrets.tdb
```

```
[root@samba01 docker]# net getlocalsid
SID for domain SAMBA01 is: S-1-5-21-955855521-2459260878-1327528046
[root@samba01 docker]# net getdomainsid
SID for local machine SAMBA01 is: S-1-5-21-955855521-2459260878-1327528046
```

```
[root@samba01 docker]# pdbedit -L
root:0:root
nobody:99:Nobody
[root@samba01 docker]# pdbedit -Lv
---------------
Unix username:        root
NT username:          root
Account Flags:        [U          ]
User SID:             S-1-5-21-955855521-2459260878-1327528046-500
Primary Group SID:    S-1-5-21-955855521-2459260878-1327528046-513
Full Name:            root
Home Directory:       \\PDC-SRV\root
HomeDir Drive:        H:
Logon Script:
Profile Path:         \\PDC-SRV\profiles\root
Domain:               SAMBA01
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Tue, 19 Jan 2038 03:14:07 UTC
Kickoff time:         Tue, 19 Jan 2038 03:14:07 UTC
Password last set:    Sun, 18 Dec 2016 19:27:28 UTC
Password can change:  Sun, 18 Dec 2016 19:27:28 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
---------------
Unix username:        nobody
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-955855521-2459260878-1327528046-501
Primary Group SID:    S-1-5-21-955855521-2459260878-1327528046-513
Full Name:            Nobody
Home Directory:
HomeDir Drive:        (null)
Logon Script:
Profile Path:
Domain:               SAMBA01
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          never
Kickoff time:         never
Password last set:    0
Password can change:  0
Password must change: 0
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Llistat de DIT:

```
dn: sambaDomainName=SAMBA01,dc=edt,dc=org
sambaDomainName: SAMBA01
sambaSID: S-1-5-21-955855521-2459260878-1327528046
sambaAlgorithmicRidBase: 1000
objectClass: sambaDomain
sambaNextUserRid: 1000
sambaMinPwdLength: 5
sambaPwdHistoryLength: 0
sambaLogonToChgPwd: 0
sambaMaxPwdAge: -1
sambaMinPwdAge: 0
sambaLockoutDuration: 30
```

```
sambaLockoutObservationWindow: 30
sambaLockoutThreshold: 0
sambaForceLogoff: -1
sambaRefuseMachinePwdChange: 0

dn: sambaDomainName=SAMBA,dc=edt,dc=org
objectClass: sambaDomain
sambaDomainName: SAMBA
sambaSID: S-1-5-21-955855521-2459260878-1327528046
sambaNextRid: 1000

dn: sambaDomainName=sambaDomain,dc=edt,dc=org
objectClass: sambaDomain
objectClass: sambaUnixIdPool
sambaDomainName: sambaDomain
sambaSID: S-1-5-21-955855521-2459260878-1327528046
uidNumber: 1000
gidNumber: 1000

dn: uid=root,ou=usuaris,dc=edt,dc=org
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: posixAccount
objectClass: shadowAccount
uid: root
cn: root
sn: root
gidNumber: 0
uidNumber: 0
homeDirectory: /home/root
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaHomePath: \\PDC-SRV\root
sambaHomeDrive: H:
sambaProfilePath: \\PDC-SRV\profiles\root
sambaPrimaryGroupSID: S-1-5-21-955855521-2459260878-1327528046-512
sambaSID: S-1-5-21-955855521-2459260878-1327528046-500
loginShell: /bin/false
gecos: Netbios Domain Administrator
sambaPwdMustChange: 1485977248
sambaPwdLastSet: 1482089248
sambaLMPassword: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
sambaAcctFlags: [U]
sambaNTPassword: 55F79BF273802801CFC79712AAC292F3
userPassword:: e1NTSEF9SnlyWDYzZXlkblJGdEdjVnYxbXZmdGlRWjRwRU1qSnY=
shadowLastChange: 17153
shadowMax: 45

dn: uid=nobody,ou=usuaris,dc=edt,dc=org
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: posixAccount
objectClass: shadowAccount
cn: nobody
sn: nobody
gidNumber: 514
uid: nobody
uidNumber: 999
homeDirectory: /nonexistent
sambaPwdLastSet: 0
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
sambaHomePath: \\PDC-SRV\nobody
sambaHomeDrive: H:
sambaProfilePath: \\PDC-SRV\profiles\nobody
sambaPrimaryGroupSID: S-1-5-21-955855521-2459260878-1327528046-514
sambaLMPassword: NO PASSWORDXXXXXXXXXXXXXXXXXXXXX
sambaNTPassword: NO PASSWORDXXXXXXXXXXXXXXXXXXXXX
sambaAcctFlags: [NUD        ]
sambaSID: S-1-5-21-955855521-2459260878-1327528046-501
loginShell: /bin/false

dn: cn=Domain Admins,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Domain Admins
gidNumber: 512
memberUid: root
description: Netbios Domain Administrators
sambaSID: S-1-5-21-955855521-2459260878-1327528046-512
sambaGroupType: 2
displayName: Domain Admins
```

```
dn: cn=Domain Users,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Domain Users
gidNumber: 513
description: Netbios Domain Users
sambaSID: S-1-5-21-955855521-2459260878-1327528046-513
sambaGroupType: 2
displayName: Domain Users

dn: cn=Domain Guests,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Domain Guests
gidNumber: 514
description: Netbios Domain Guests Users
sambaSID: S-1-5-21-955855521-2459260878-1327528046-514
sambaGroupType: 2
displayName: Domain Guests

dn: cn=Domain Computers,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Domain Computers
gidNumber: 515
description: Netbios Domain Computers accounts
sambaSID: S-1-5-21-955855521-2459260878-1327528046-515
sambaGroupType: 2
displayName: Domain Computers

dn: cn=Administrators,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Administrators
gidNumber: 544
description: Netbios Domain Members can fully administer the computer/sambaDom
 ainName
sambaSID: S-1-5-32-544
sambaGroupType: 4
displayName: Administrators

dn: cn=Account Operators,ou=grups,dc=edt,dc=org
```

```
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Account Operators
gidNumber: 548
description: Netbios Domain Users to manipulate users accounts
sambaSID: S-1-5-32-548
sambaGroupType: 4
displayName: Account Operators

dn: cn=Print Operators,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Print Operators
gidNumber: 550
description: Netbios Domain Print Operators
sambaSID: S-1-5-32-550
sambaGroupType: 4
displayName: Print Operators

dn: cn=Backup Operators,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Backup Operators
gidNumber: 551
description: Netbios Domain Members can bypass file security to back up files
sambaSID: S-1-5-32-551
sambaGroupType: 4
displayName: Backup Operators

dn: cn=Replicators,ou=grups,dc=edt,dc=org
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: Replicators
gidNumber: 552
description: Netbios Domain Supports file replication in a sambaDomainName
sambaSID: S-1-5-32-552
sambaGroupType: 4
displayName: Replicators
```

Configuracions: smb / smbldap / smbldap_bind

```
[root@samba01 docker]# grep -v "^#" /etc/smbldap-tools/smbldap.conf  | grep -v "^ *$"
slaveLDAP="ldap://172.17.0.2/"
masterLDAP="ldap://172.17.0.2/"
ldapTLS="0"
verify="require"
cafile="/etc/pki/tls/certs/ldapserverca.pem"
clientcert="/etc/pki/tls/certs/ldapclient.pem"
clientkey="/etc/pki/tls/certs/ldapclientkey.pem"
suffix="dc=edt,dc=org"
usersdn="ou=usuaris,${suffix}"
computersdn="ou=hosts,${suffix}"
groupsdn="ou=grups,${suffix}"
idmapdn="ou=domains,${suffix}"
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
scope="sub"
password_hash="SSHA"
password_crypt_salt_format="%s"
userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
shadowAccount="1"
defaultMaxPasswordAge="45"
userSmbHome="\\PDC-SRV\%U"
userProfile="\\PDC-SRV\profiles\%U"
userHomeDrive="H:"
userScript="logon.bat"
mailDomain="example.com"
lanmanPassword="0"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

```
[root@samba01 docker]# grep -v "^#" /etc/smbldap-tools/smbldap_bind.conf
slaveDN="cn=Manager,dc=edt,dc=org"
slavePw="secret"
masterDN="cn=Manager,dc=edt,dc=org"
masterPw="secret"
```

```
[root@samba01 docker]# grep -v "^#" /etc/samba/smb.conf
[global]
   workgroup = SAMBA
   server string = Standalone Samba %v %h @edt
   log file = /var/log/samba/log.%m
   max log size = 50
   security = user
   passdb backend = ldapsam:ldap://172.17.0.2
         ldap suffix = dc=edt,dc=org
         ldap user suffix = ou=usuaris
         ldap group suffix = ou=grups
         ldap machine suffix = ou=hosts
         ldap idmap suffix = ou=domains
         ldap admin dn = cn=Manager,dc=edt,dc=org
         ldap ssl = no
         ldap passwd sync = yes
   load printers = yes
   cups options = raw
```

Trick: enganyar samba amb usuaris locals unix falsos

```
[root@samba01 docker]# tail -1 /etc/passwd
pau:x:5000:100:Pau Pou local:/tmp/home/pau:/sbin/nologin
```

```
root@ldapserver docker]# ldapsearch -xLLL -b 'dc=edt,dc=org' "cn=Pau Pou"
dn: cn=Pau Pou,ou=usuaris,dc=edt,dc=org
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
cn: Pau Pou
cn: Pauet Pou
sn: Pou
homePhone: 555-222-2220
mail: pau@edt.org
description: Watch out for this guy
ou: Profes
uid: pau
uidNumber: 5000
gidNumber: 100
homeDirectory: /tmp/home/pau
```

```
root@samba01 docker]# smbpasswd -a pau
New SMB password:
```

```
Retype new SMB password:
Added user pau.
[root@samba01 docker]# pdbedit -L
pau:5000:Pau Pou local
root:0:root
nobody:99:Nobody


[root@samba01 docker]# pdbedit -Lv
---------------
Unix username:        pau
NT username:          pau
Account Flags:        [U          ]
User SID:             S-1-5-21-955855521-2459260878-1327528046-1001
Primary Group SID:    S-1-5-21-955855521-2459260878-1327528046-513
Full Name:            Pau Pou local
Home Directory:       \\samba01\pau
HomeDir Drive:
Logon Script:
Profile Path:         \\samba01\pau\profile
Domain:               SAMBA01
Account desc:         Watch out for this guy
Workstations:
Munged dial:
Logon time:           0
Logoff time:          never
Kickoff time:         never
Password last set:    Mon, 19 Dec 2016 15:34:50 UTC
Password can change:  Mon, 19 Dec 2016 15:34:50 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```
[root@ldapserver docker]# ldapsearch -xLLL -b 'dc=edt,dc=org' "cn=Pau Pou"
dn: cn=Pau Pou,ou=usuaris,dc=edt,dc=org
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
cn: Pau Pou
cn: Pauet Pou
sn: Pou
homePhone: 555-222-2220
mail: pau@edt.org
description: Watch out for this guy
ou: Profes
```

```
uid: pau
uidNumber: 5000
gidNumber: 100
homeDirectory: /tmp/home/pau
sambaSID: S-1-5-21-955855521-2459260878-1327528046-1001
displayName: Pau Pou local
userPassword:: e1NTSEF9dHFpd05jL2dLVGw2dVBxbFlGekU5ZVpRdzlZWElCeWg=
sambaNTPassword: 06A7F4852E85B2256DD2C18845D22112
sambaPasswordHistory:
00000000000000000000000000000000000000000000000000000000
 00000000
sambaPwdLastSet: 1482161690
sambaAcctFlags: [U          ]
```

smbpasswd

Disable Account

```
[root@samba01 docker]# smbpasswd -d pau
Disabled user pau.

[root@samba01 docker]# pdbedit -Lv pau
Unix username:        pau
NT username:          pau
Account Flags:        [DU     ]
User SID:             S-1-5-21-955855521-2459260878-1327528046-1001
Primary Group SID:    S-1-5-21-955855521-2459260878-1327528046-513
Full Name:            Pau Pou local
Home Directory:       \\samba01\pau
HomeDir Drive:
Logon Script:
Profile Path:         \\samba01\pau\profile
Domain:               SAMBA01
Account desc:         Watch out for this guy
Workstations:
Munged dial:
Logon time:           0
Logoff time:          never
Kickoff time:         never
Password last set:    Mon, 19 Dec 2016 15:34:50 UTC
Password can change:  Mon, 19 Dec 2016 15:34:50 UTC
Password must change: never
Last bad password   : 0
```

```
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```
[root@ldapserver docker]# ldapsearch -xLLL -b 'dc=edt,dc=org' "cn=Pau Pou"
dn: cn=Pau Pou,ou=usuaris,dc=edt,dc=org
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
cn: Pau Pou
cn: Pauet Pou
sn: Pou
homePhone: 555-222-2220
mail: pau@edt.org
description: Watch out for this guy
ou: Profes
uid: pau
uidNumber: 5000
gidNumber: 100
homeDirectory: /tmp/home/pau
sambaSID: S-1-5-21-955855521-2459260878-1327528046-1001
displayName: Pau Pou local
userPassword:: e1NTSEF9dHFpd05jL2dLVGw2dVBxbFIGekU5ZVpRdzlZWElCeWg=
sambaNTPassword: 06A7F4852E85B2256DD2C18845D22112
sambaPasswordHistory:
00000000000000000000000000000000000000000000000000000000
 00000000
sambaPwdLastSet: 1482161690
sambaAcctFlags: [DU          ]
```

Enable Account

```
[root@samba01 docker]# smbpasswd -e pau
Enabled user pau.

[root@samba01 docker]# pdbedit -Lv pau
Unix username:        pau
NT username:          pau
Account Flags:        [U          ]
User SID:             S-1-5-21-955855521-2459260878-1327528046-1001
Primary Group SID:    S-1-5-21-955855521-2459260878-1327528046-513
Full Name:            Pau Pou local
Home Directory:       \\samba01\pau
HomeDir Drive:
```

```
Logon Script:
Profile Path:          \\samba01\pau\profile
Domain:                SAMBA01
Account desc:          Watch out for this guy
Workstations:
Munged dial:
Logon time:            0
Logoff time:           never
Kickoff time:          never
Password last set:     Mon, 19 Dec 2016 15:34:50 UTC
Password can change:  Mon, 19 Dec 2016 15:34:50 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours            : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Delete Account

S’esborra dels usuaris samba però no de unix. Si es mira el DIT de ldap l’usuari unix encara existeix

```
[root@samba01 docker]# smbpasswd -x pau
Deleted user pau.

[root@samba01 docker]# pdbedit -Lv pau
Username not found!
```

```
[root@ldapserver docker]# ldapsearch -xLLL -b 'dc=edt,dc=org' "cn=Pau Pou"
dn: cn=Pau Pou,ou=usuaris,dc=edt,dc=org
objectClass: posixAccount
objectClass: inetOrgPerson
cn: Pau Pou
cn: Pauet Pou
sn: Pou
homePhone: 555-222-2220
mail: pau@edt.org
description: Watch out for this guy
ou: Profes
uid: pau
uidNumber: 5000
gidNumber: 100
homeDirectory: /tmp/home/pau
userPassword:: e1NTSEF9dHFpd05jL2dLVGw2dVBxbFlGekU5ZVpRdzlZWElCeWg=
```

Ordres net

```
[root@samba01 docker]# net
Invalid command: net
Usage:
net rpc         Run functions using RPC transport
net rap         Run functions using RAP transport
net ads         Run functions using ADS transport
net file        Functions on remote opened files
net share       Functions on shares
net session     Manage sessions
net server      List servers in workgroup
net domain              List domains/workgroups on network
net printq      Modify printer queue
net user        Manage users
net group       Manage groups
net groupmap            Manage group mappings
net sam         Functions on the SAM database
net validate    Validate username and password
net groupmember         Modify group memberships
net admin       Execute remote command on a remote OS/2 server
net service     List/modify running services
net password            Change user password on target server
net changetrustpw   Change the trust password
net changesecretpw  Change the secret password
net setauthuser         Set the winbind auth user
net getauthuser         Get the winbind auth user settings
net time        Show/set time
net lookup      Look up host names/IP addresses
net g_lock      Manipulate the global lock table
net join        Join a domain/AD
net dom         Join/unjoin (remote) machines to/from a domain/AD
net cache       Operate on the cache tdb file
net getlocalsid         Get the SID for the local domain
net setlocalsid         Set the SID for the local domain
net setdomainsid        Set domain SID on member servers
net getdomainsid        Get domain SID on member servers
net maxrid      Display the maximum RID currently used
net idmap       IDmap functions
net status      Display server status
net usershare           Manage user-modifiable shares
net usersidlist Display list of all users with SID
net conf        Manage Samba registry based configuration
```

net registry	Manage the Samba registry
net eventlog	Process Win32 *.evt eventlog files
net printing	Process tdb printer files
net serverid	Manage the serverid tdb
net notify	notifyd client code
net help	Print usage information