Open-E external LDAP HOWTO

1. Connecting two Open-e systems to each other:

- use the same software version on both systems,
- use the same workgroup on both systems,
- the source system should be configured with Internal LDAP, while the destination system uses External LDAP to connect to the source system. All advanced settings should be left at default values.

---

2. Open-E system as client + LDAP server without Samba (here called SRVA):

- build the basic LDAP structure on SRVA:

dn: dc=server,dc=nas
dn: cn=admin,dc=server,dc=nas
dn: ou=People,dc=server,dc=nas
dn: ou=Computers,dc=server,dc=nas
dn: ou=Groups,dc=server,dc=nas
dn: cn=users,ou=Groups,dc=server,dc=nas

- and :

dn: sambaDomainName=workgroup_name,dc=server,dc=nas

- for example, if SRVA contains the entry:

sambaDomainName=WORKGROUP,dc=server,dc=nas

set the workgroup name on the Open-E system also to WORKGROUP,

- there must be compatibility in sambaSID between the sambaDomainName entry and the entries for users and groups. If you need to rewrite sambaSID values for your users and groups, see the sections 4. and 5. below.

---

3. Open-E system as client + External LDAP server with Samba (here called SRVB)

SRVA configuration:
- make sure the following line is present in the Samba config file (smb.conf):

domain logons = yes

- create the basic LDAP structure (as detailed in point 2 above) **without** a sambaDomainName entry (this entry will be automatically generated by Samba),

- use the same workgroup name on both the server and the client.

---

4. How to check SambaSIDs and why are they important?

First of all, you need to check the existing sambaSID for your sambaDomainName entry. Under Linux, you can do this using ldapsearch:

ldapsearch -x -h 192.168.243.4 -b dc=server,dc=nas -D cn=admin,dc=server,dc=nas -w secret

where:
192.168.243.4 - ldap server
dc=server,dc=nas - basedn
cn=admin,dc=server,dc=nas - rootdn
secret - password

Below you can find example output from the ldapsearch command. This record was generated in LDAP for a server using Samba with domain logons set to *no* (therefore, it is based on netBIOS name of the connecting server). In this example the netBIOS name is DSS:

 # DSS, server.nas
dn: sambaDomainName=DSS,dc=server,dc=nas
sambaDomainName: DSS
sambaSID: S-1-5-21-2896602268-470177729-4123194723
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

In contrast, this is a record generated for a server using Samba with domain logons set to *yes* (therefore, it is based on the workgroup name). In this case the workgroup name is WORKGROUP (this record will be automatically added after connecting the storage server to the LDAP server)

 # WORKGROUP, server.nas
dn: sambaDomainName=WORKGROUP,dc=server,dc=nas
sambaDomainName: WORKGROUP
sambaSID: S-1-5-21-677905249-1957579923-4221919332
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

As you can see the sambaSIDs for these two entries are different. This situation may occur when you connect Samba servers with different domain logons values to the same LDAP server. Since users can have only one sambaSID, the result of this would be that only one of these two servers would have Samba access (because the LDAP users' sambaSIDs can only be compatible with one sambaDomainName sambaSID).

The solution is to use the same sambaSID for both the sambaDomainName entries. Following the previous example, we can rewrite the sambaSID value from our old record 'dn: sambaDomainName=DSS,dc=server,dc=nas' to record 'dn: sambaDomainName=WORKGROUP,dc=server,dc=nas'

How to do this in Linux?

Create a file called 'modify' with the following content:

dn: sambaDomainName=WORKGROUP,dc=server,dc=nas
replace: sambaSID
sambaSID: S-1-5-21-2896602268-470177729-4123194723

where:
a) WORKGROUP is the workgroup name that you indicated in your DSS,
b) S-1-5-21-2896602268-470177729-4123194723 - correct sambaSID value (you can get this from the record 'dn:sambaDomainName=DSS,dc=server,dc=nas')

next type:

ldapmodify -h 127.0.0.1 -D cn=admin,dc=server,dc=nas -w secret -r -x -f modify

where:
127.0.0.1 - IP of LDAP server
cn=admin,dc=server,dc=nas - rootdn (you can get this from /etc/ldap/slapd.conf)
secret - password
modify - your file

After these modifications you must restart Samba (please restart your DSS or click again APPLY in the Authentication Method box which will cause Samba to be restarted).

---

5. Setting up user sambaSIDs

When creating users for the external LDAP, you need to pay special attention to their sambaSIDs.

Correct Samba entries for a user look like the following example:

uidNumber: 1001

sambaSID: S-1-5-21-2896602268-470177729-4123194723-3002
gidNumber: 1000

sambaPrimaryGroupSID: S-1-5-21-2896602268-470177729-4123194723-3001

As you can see, there is a 4-digit number appended to the regular sambaSID (which is taken from the WORKGROUP example above). This is generated in the following manner:

sambaSID: uidNumber * 2 + 1000
sambaPrimaryGroupSID: gidNumber * 2 + 1001

These entries must always match and conform to the schema above – otherwise the user will not be able to connect via SMB.

Please also note the user password must always be encrypted using CRYPT. A proper entry looks like this:

userPassword: {CRYPT}emaDqnIPfsR7A

---

6. An example LDAP dump

This is an example LDAP dump with 2 users and a single group.

dn: dc=server,dc=nas

objectClass: top

objectClass: dcObject

objectClass: organization

o: server

dc: server

dn: cn=admin,dc=server,dc=nas

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

```
description: LDAP administrator

userPassword: secret


dn: ou=employees,dc=server,dc=nas

objectClass: top

objectClass: organizationalUnit

ou: employees


dn: cn=James Bond,ou=employees,dc=server,dc=nas

objectClass: inetOrgPerson

objectClass: sambaSamAccount

objectClass: posixAccount

objectClass: top

givenName: James

sn: Bond

cn: James Bond

uid: jbond

mail: james.bond@company.com

uidNumber: 1000

sambaSID: S-1-5-21-2896602268-470177729-4123194723-3000

sambaPwdLastSet: 1228941481

userPassword: {CRYPT}LOUqYm05xCb2E

sambaLMPassword: E52CAC67419A9A224A3B108F3FA6CB6D

sambaNTPassword: 8846F7EAEE8FB117AD06BDD830B7586C
```

gidNumber: 1000

sambaPrimaryGroupSID: S-1-5-21-2896602268-470177729-4123194723-3001

homeDirectory: /home/users/SambaGroup/nd

sambaAcctFlags: [U]

dn: cn=Jason Bourne,ou=employees,dc=server,dc=nas

objectClass: inetOrgPerson

objectClass: sambaSamAccount

objectClass: posixAccount

objectClass: top

givenName: Jason

sn: Bourne

cn: Jason Bourne

uid: jbourne

mail: jason.bourne@company.com

uidNumber: 1001

sambaSID: S-1-5-21-2896602268-470177729-4123194723-3002

sambaPwdLastSet: 1228941481

userPassword: {CRYPT}emaDqnIPfsR7A

sambaLMPassword: E52CAC67419A9A224A3B108F3FA6CB6D

sambaNTPassword: 8846F7EAEE8FB117AD06BDD830B7586C

gidNumber: 1000

sambaPrimaryGroupSID: S-1-5-21-2896602268-470177729-4123194723-3001

homeDirectory: /home/users/SambaGroup/urne

sambaAcctFlags: [U]

```
dn: ou=groups,dc=server,dc=nas

objectClass: top

objectClass: organizationalUnit

ou: groups


dn: cn=SambaGroup,ou=groups,dc=server,dc=nas

objectClass: posixGroup

objectClass: sambaGroupMapping

objectClass: top

cn: SambaGroup

displayName: SambaGroup

gidNumber: 1000

sambaSID: S-1-5-21-2896602268-470177729-4123194723-3001

sambaGroupType: 2


dn: sambaDomainName=3511,dc=server,dc=nas

sambaDomainName: 3511

sambaSID: S-1-5-21-2896602268-470177729-4123194723

sambaAlgorithmicRidBase: 1000

objectClass: sambaDomain

sambaNextUserRid: 1000
```

VERSION HISTORY

Version number	Date	Author	Notes
1.00	19/10/2009	Szymon Duda	Initial version