

Création OpenLdap

Install package openldap, on utilise yum pour éviter les problèmes de dépendances

```
yum -y install openldap* migrationtools
```

```
[root@redhat ~]# yum -y install openldap* migrationtools
```

Une fois installé, crée le Password admin du ldap

slappaswd

```
[root@redhat ~]# slapasswd  
New password:  
Re-enter new password:  
{SSHA}nLrrt
```

Copier le SHA pour l'intégrer plus tard dans le fichier de configuration

Accéder au dossier config du ldap et modifier le fichier olcDatabase={2}hdb.ldif

```
[root@redhat ~]# cd /etc/openldap/slapd.d/cn=config
[root@redhat cn=config]# vi olcDatabase={2}hdb.ldif
```

Modifier les paramètres "olcSuffix" et "olcRootDN" selon votre domaine et ajouter "olcRootPW"

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 9f295b19
dn: olcDatabase={2}hdb
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=[REDACTED],dc=fr
olcRootDN: cn=Manager,dc=[REDACTED],dc=fr
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
olcRootPW: [REDACTED]
structuralObjectClass: olcHdbConfig
entryUUID: 02d0ac38-2d37-103e-822b-fb904797972b
creatorsName: cn=config
createTimestamp: 20231212123752Z
"olcDatabase={2}hdb.ldif" 19L, 657C
```

Ajout des droits de monitor au compte en modifiant le fichier olcDatabase={1}monitor.ldif :

```
[root@[REDACTED] cn=config]# vi olcDatabase={1}monitor.ldif
```

Modifier les paramètres "olcAccess" de votre domaine et ajouter

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 bd9e375b
dn: olcDatabase={1}monitor
objectClass: olcDatabaseConfig
olcDatabase: {1}monitor
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,[REDACTED],dc=fr" read by * none
structuralObjectClass: olcDatabaseConfig
entryUUID: 02d0a8b4-2d37-103e-822a-fb904797972b
creatorsName: cn=config
createTimestamp: 20231212123752Z
entryCSN: 20231212123752.474096Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20231212123752Z
~
~
"olcDatabase={1}monitor.ldif" 14L, 561C
```

Vérifier la configuration avec la commande suivante

```
slaptest -u
```

```
[root@[REDACTED] cn=config]# slaptest -u
65785521 ldif_read_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif"
65785521 ldif_read_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif"
config file testing succeeded
```

Nous pouvons ignorer les erreurs checksum

Démarrer le service, l'ajouter au démarrage automatique et vérifier le démarrage

```
[root@██████████ cn=config]# systemctl start slapd
[root@██████████ cn=config]# systemctl enable slapd
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to /usr/lib/systemd/system/slapd.service.
[root@██████████ cn=config]# netstat -lt | grep ldap
bash: netstat: command not found...
[root@██████████ cn=config]# netstat -lt | grep ldap
tcp        0      0 0.0.0.0:ldap 0.0.0.0:*      LISTEN
tcp6       0      0 :::ldap     :::*           LISTEN
```

Copier le sample de la base et attribuer les droits :

```
[root@██████████ cn=config]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
[root@██████████ cn=config]# chown -R ldap:ldap /var/lib/ldap
```

Crée les schéma pour le ldap :

```
[root@██████████ cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
[root@██████████ cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
[root@██████████ cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

Un annuaire d'un site applicatif : pour répondre sur le ldap

```
4 <!-- Annuaire OpenLDAP -->
5 <add key="Ldap_ServerName" value="OpenLDAP interne ██████████" />
6 <add key="Ldap_Type" value="Open" />
7 <add key="Ldap_Serveur" value="██████████17.105:389" />
8 <add key="Ldap_OrganisationUtilisateurs" value="ou=██████████" />
9 <add key="Ldap_Partition" value="dc=██████████,dc=██████████" />
10 <add key="Ldap_Code" value="uid" />
11 <add key="Ldap_Email" value="mail" />
12 <add key="Ldap_Nom" value="sn" />
13 <add key="Ldap_Prenom" value="givenName" />
14 <add key="Ldap_ServeurSsl" value="" />
15 <add key="Ldap_Utilisateur" value="██████████" />
16 <add key="Ldap_MotDePasse" value="██████████" />
17 <add key="AuthenticationCreationUtilisateur" value="False" />
18 <!-- Libellé du profil à associer par défaut aux utilisateurs créés automatiquement (clé : Client-Environnement) -->
19 <add key="AuthenticationProfilDefaut,██████████Prod" value="" />
20
21 <add key="Ldap_EnablePasswordChange" value="True" />
22 <add key="Ldap_EnableLdapUserUpdate" value="True" />
23 <add key="Ldap_EnableLdapUserCreate" value="True" />
24 <add key="Ldap_EnableLdapUserDelete" value="True" />
25 <add key="Ldap_SecurityErrorMessage" value="Votre compte sera désactivé pendant 5 minutes après 3 échecs d'authentification." />
26 <add key="Ldap_Member" value="" />
27 <add key="Ldap_SecurityGroupDnToCheck" value="" />
28
29 <!-- Blocage accès Back -->
30 <add key="LoginPage_DisableLdap" value="True" />
31
32
33 </appSettings>
```

Revision #3

Created 31 October 2024 17:47:53 by Cavallone

Updated 19 November 2024 16:36:08 by Cavallone