LDAP

- Anonymous Bind deaktivieren
- Fedora Directory Server
- LDAP Datensicherung mit slapcat
- LDAP-Server abfragen mit ldapsearch

Anonymous Bind deaktivieren

Standardmäßig darf jeder priviligierte Systemuser per ldapsearch die LDAP-DB abfragen. Mit folgendem Snippet muss man sich per Bind (also einen LDAP-User mit entsprechenden Rechten besitzen), um die DB abfragen zu dürfen.

disable_anon_backend.ldif

```
dn: olcDatabase={1}hdb,cn=config
add: olcRequires
olcRequires: authc
```

disable_anon_frontend.ldif

```
dn: olcDatabase={-1}frontend,cn=config
add: olcRequires
olcRequires: authc
```

```
ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f disable_anony_backend.ldif
ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f disable_anony_frontend.ldif
```

Fedora Directory Server

Namenskonventionen

- server: der LDAP-Server
- server.domaene.de: FQDN des Servers

Console starten

- Console mit SSL-Unterstützung

```
./startconsole -u admin -a https://server:45000/
```

- Console ohne SSL-Unterstützung

```
./startconsole -u admin -a http://server:45000/
```

SSL-Verschlüsselung für den Directory-Server aktivieren

- Zertifikatsdatenbank erzeugen und füllen:

```
cd /opt/fedora-ds
# Zertifikatsdatenbank erstellen
shared/bin/certutil -N -P slapd-server- -d /opt/fedora-ds/alias
# vorhandene Zertifikate ins PKCS#12-Format umwandeln (Key und Zertifikat getrennt) (sofern nich
openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12 -name "Server-Cert"
# Zertifikat in die Datenbank importieren
shared/bin/pk12util -i server.p12 -d alias -P slapd-server-
# Berechtigungen korrigieren
chown nobody.nobody alias/slapd-server-*
```

- PIN-File zum passwortlosen Start anlegen:

```
echo "internal:secret" > /opt/fedora-ds/alias/slapd-server-pin.txt
```

- Datei /opt/fedora-ds/admin-serv/config/nss.conf editieren:

```
#   Pass Phrase Dialog:
#   Configure the pass phrase gathering process.
#   The filtering dialog program (`builtin' is a internal
#   terminal dialog) has to provide the pass phrase on stdout.
#NSSPassPhraseDialog  builtin
NSSPassPhraseDialog file:/opt/fedora-ds/alias/admin-serv-server-pin.txt
```

- Nun sollte der passwortlose Start der LDAP-Servers möglich sein

```
cd /opt/fedora-ds/slapd-server
./start-slapd
```

> Dies gilt für den Fedora Directory Server 1.0.4 (in 1.1 hat sich einiges geändert)

SSL-Verschlüsselung für den Admin-Server aktivieren

- Zertifikatsdatenbank erzeugen und füllen:

```
cd /opt/fedora-ds
# Zertifikatsdatenbank erstellen
shared/bin/certutil -N -P admin-serv-server- -d /opt/fedora-ds/alias
# vorhandene Zertifikate ins PKCS#12-Format umwandeln (Key und Zertifikat getrennt) (sofern nich
openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12 -name "Server-Cert"
# Zertifikat in die Datenbank importieren
shared/bin/pk12util -i server.p12 -d alias -P admin-serv-server-
# Berechtigungen korrigieren
chown nobody.nobody alias/admin-serv-server-*
```

- PIN-File zum passwortlosen Start anlegen:

```
echo "internal:secret" > /opt/fedora-ds/alias/admin-serv-server-pin.txt
```

- Datei /opt/fedora-ds/admin-serv/config/nss.conf editieren:

```
#   Pass Phrase Dialog:
#   Configure the pass phrase gathering process.
#   The filtering dialog program (`builtin' is a internal
#   terminal dialog) has to provide the pass phrase on stdout.
#NSSPassPhraseDialog  builtin
NSSPassPhraseDialog file:/opt/fedora-ds/alias/admin-serv-server-pin.txt
```

- Nun sollte der passwortlose Start der Admin-Servers möglich sein

```
cd /opt/fedora-ds
./start-admin
```

Zertifikate via Kommandozeile erneuern

zuerst in das Verzeichnis mit der Directory-Datenbank wechseln:

```
cd /opt/fedora-ds/alias
```

- Zertifikat-Datenbank anzeigen

```
../shared/bin/certutil -L -d . -P slapd-<hostname>-
```

- einen Zertifikatsrequest erzeugen:

```
TODO (ich habs über die grafische Konsole gemacht)
```

- Zertifikat aus der Datenbank löschen:

```
../shared/bin/certutil -D -n server-cert -d . -P slapd-<hostname>-
```

- neues Zertifikat der Datenbank hinzufügen:

```
../shared/bin/certutil -A -t u,u,u -n Server-Cert -d . -P slapd-<hostname>- -i /tmp/newcert.pem
```

LDAP Datensicherung mit slapcat

Mit folgendem Script wird ein Backup der LDAP-Directory im laufenden Betrieb erzeugt (der find sorgt dafür, dass Backups älter als 60 Tage gelöscht werden):

```
#!/bin/bash
# dump the ldap database

OUTFILE=/srv/backup/ldapdb-`/bin/date +%d-%m-%y_%H-%M`.ldif

echo "Starting slapcat..."
/usr/sbin/slapcat -n0 > $OUTFILE && /usr/sbin/slapcat -n1 >> $OUTFILE && echo "Backup created, n
#find `dirname $OUTFILE` -name "*.ldif" -mtime +60 -exec rm -f {} \;
STATE=$?
exit $STATE
```

- Listenpunkt„ `slapcat -n0` “ - sicher Konfiguration und Schemata
- „ `slapcat -n1` “ - sichert die Userdaten

LDAP-Server abfragen mit ldapsearch

Eine normale Abfrage des Users „test“ mit der neueren URI-Syntax:

```
ldapsearch -H ldap://server.ldap.net -b "dc=ldap,dc=net" -D "cn=Manager,dc=ldap,dc=net" "uid=tes
```

eine Abfrage des Users „test“ mit TLS-Verschlüsselung (Transport Layer Security) über den normalen LDAP-Port 389:

```
ldapsearch -H ldap://server.ldap.net -b "dc=ldap,dc=net" -D "cn=Manager,dc=ldap,dc=net" "uid=tes
```

eine Abfrage des Users „test“ mit SSL-Verschlüsselung über den SSL-LDAP-Port 636:

```
ldapsearch -H ldaps://server.ldap.net -b "dc=ldap,dc=net" -D "cn=Manager,dc=ldap,dc=net" "uid=te
```