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
```

Revision #1
Created 2021-04-30 11:41:11 UTC by magenbrot
Updated 2021-04-30 11:42:04 UTC by magenbrot