Správa identit s OpenLDAP a FusionDirectory v malé firmě

Ondřej Kolín

sysadmin @Benocs.com

Velká část dostupná na mojefedora.cz formou článků

Cíle

Centrální správa uživatelů

- Přiřazení poštovních účtů
- Skupiny
- Správa hesel
- Samba, ...

OpenLDAP

Projekt (nejen) svobodného adresáře nad protokolem LDAP

Široce konfigurovatelný

Dostupné v každé dobré distribuci

OpenLDAP struktura

`/var/lib/ldap`

`/etc/ldap/openldap`

Schémata, overlays

Co chceme nakonfigurovat

1. Základní přístupy
2. Replikaci mezi instancemi
3. Fusion Directory

Volitelně

memberOf overlay

TLS certifikáty

Ansible řízené

Po instalaci

systemctl start/enable/status openldap

firewall-cmd ...

příkazy slap*

Základní přístup

ldapi, ldap(s)

```
ldapmodify -Y EXTERNAL -H ldapi:///
ldapadd -x -W -D "cn=admin,dc=mojefedora,dc=cz"
```

Základní konfigurace

`/usr/share/slapd/slapd.init.ldif`

`sed -i -e "s|@BACKEND@|${backend}|g" ${initldif}`

`configPass.ldif`

`domain.ldif`

`memberOfConfig.ldif`

`memberOfLoad.ldif`

Instalace synchronizačního overlay

`syncoverlay.ldif.j2`

Instalace Fusion directory

1. gpg key
2. Přidat repozitář
3. Instalace

Konfigurace FD

Připojení databáze

Doinstalování potřebných schémat

Pluginy do Fusion Directory

Exploration time!

Co víc?

TLS certifikát

Připojení Fedora Workstation

Připojení generického linuxového serveru

Alternativy

Active Directory (obsahuje LDAP server)

FreeIPA (obsahuje LDAP server)

DS 389 (je ldap alternativní server)

Díky za pozornost

Otázky?