LDAP jako centralna baza użytkowników dla wielu usług

Marek Marczykowski
marmarek@staszic.waw.pl

14 stycznia 2008

Wpisy w LDAP

- struktura drzewa

Wpisy w LDAP

- struktura drzewa
- specjalny atrybut objectClass - klasa/y elementu

Wpisy w LDAP

- struktura drzewa
- specjalny atrybut objectClass - klasa/y elementu
- atrybuty systemowe

Wpisy w LDAP

- struktura drzewa
- specjalny atrybut objectClass - klasa/y elementu
- atrybuty systemowe

Filtry

- (attr=value)
- (&(attr1=value)(attr2=val2))

LDIF

```
uid=cypisek,ou=People,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: cypisek
givenName: cypisek
uid: cypisek
loginShell: /bin/bash
gidNumber: 101
userPassword: {CRYPT}$1$uKGFs$R8BpNBuvRPVFm/vttKK0//
```

SASL

slapd.conf

```
sasl-host       sasl.example.com
sasl-realm      EXAMPLE.COM
sasl-regexp
    uid=(.+),cn=(.+),cn=.+,cn=auth
    ldap:///dc=example,dc=com??sub?(|(uid=$1)(cn=$1@$2))
sasl-regexp
    gidNumber=0\\\+uidNumber=0,cn=peercred,cn=external,cn=
    "uid=ldapmaster,ou=System,dc=example,dc=com"
```

SASL

slapd.conf

```
sasl-host       sasl.example.com
sasl-realm      EXAMPLE.COM
sasl-regexp
    uid=(.+),cn=(.+),cn=.+,cn=auth
    ldap:///dc=example,dc=com??sub?(|(uid=$1)(cn=$1@$2))
sasl-regexp
    gidNumber=0\\\+uidNumber=0,cn=peercred,cn=external,cn=
    "uid=ldapmaster,ou=System,dc=example,dc=com"
```

Działanie

```
# ldapwhoami -Y EXTERNAL
SASL username: gidNumber=0+uidNumber=0,cn=peer...
dn:uid=ldapmaster,ou=system,dc=example,dc=com
```

Po co to

- centralne zarządzanie

Po co to

- centralne zarządzanie
- duża elastyczność

Po co to

- centralne zarządzanie
- duża elastyczność
  - klasy

Po co to

- centralne zarządzanie
- duża elastyczność
  - klasy
  - filtry

Po co to

- centralne zarządzanie
- duża elastyczność
  - klasy
  - filtry
- wsparcie w dużej ilości oprogramowania

Po co to

- centralne zarządzanie
- duża elastyczność
  - klasy
  - filtry
- wsparcie w dużej ilości oprogramowania
- niezawodność (replikacja)

nss_ldap, PAM

/etc/ldap.conf

```
base dc=example,dc=com
uri ldap://ldap.example.com
nss_base_passwd ou=People,dc=example,dc=com
nss_base_group ou=Group,dc=example,dc=com

pam_filter objectclass=posixAccount
pam_login_attribute uid
pam_member_attribute memberUid
```

PAM

Przydatne opcje

- pam_check_host_attr
- pam_check_service_attr
- pam_password exop
- pam_groupdn cn=PAM,ou=Groups,dc=example,dc=com

OpenSSH

OpenSSH-LPK

Projekt dodający obsługę LDAP do OpenSSH

sshd_config

LpkUserDN ou=People,dc=example,dc=com
LpkGroupDN ou=Groups,dc=example,dc=com

użytkownik

objectClass: ldapPublicKey
sshPublicKey: ssh-rsa AAAAB3NzaC1AAAABIwAAAGEAvpJn...

Postfix

Co można z LDAP

- bazy aliasów

Postfix

Co można z LDAP

- bazy aliasów
- mapy użytkownik-adres (smtpd_sender_login_maps)

Postfix

Co można z LDAP

- bazy aliasów
- mapy użytkownik-adres (smtpd_sender_login_maps)
- restrykcje (np odrzucanie dla zablokowanych kont)

Postfix

Co można z LDAP

- bazy aliasów
- mapy użytkownik-adres (smtpd_sender_login_maps)
- restrykcje (np odrzucanie dla zablokowanych kont)
- bazy wirtualnych domen

Postfix

Co można z LDAP

- bazy aliasów
- mapy użytkownik-adres (smtpd_sender_login_maps)
- restrykcje (np odrzucanie dla zablokowanych kont)
- bazy wirtualnych domen
- właściwie dowolne mapy

Postfix

Co można z LDAP

- bazy aliasów
- mapy użytkownik-adres (smtpd_sender_login_maps)
- restrykcje (np odrzucanie dla zablokowanych kont)
- bazy wirtualnych domen
- właściwie dowolne mapy
- używając Dovecot SASL, również autoryzacja z LDAP

Postfix

main.cf

alias_maps = ldap:/etc/postfix/aliases-ldap.cf

aliases-ldap.cf

```
search_base = ou=People,dc=example,dc=com
query_filter = (|(mail=%s)(mail=%s@example.com))
result_attribute = uid
```

Postfix

main.cf

alias_maps = ldap:/etc/postfix/aliases-ldap.cf

aliases-ldap.cf

```
search_base = ou=People,dc=example,dc=com
query_filter = (|(mail=%s)(mail=%s@example.com))
result_attribute = uid
```

group-aliases-ldap.cf

```
search_base = ou=Group,dc=example,dc=com
query_filter = (cn=%s)
special_result_attribute = memberdn
leaf_result_attribute = uid
```

Dovecot

Autoryzacja

Można na co najmniej dwa sposoby:

- standardowo - próba podłączenia się do bazy
- hasła w plaintext (wtedy dostępne są CRAM-MD5 i DIGEST-MD5)

Informacje o skrzynce

- katalog
- uid, gid
- quota
- nice

Amavis

Możliwe opcje do nadpisania

- amavisVirusLover

Amavis

Możliwe opcje do nadpisania

- amavisVirusLover
- amavisSpamTagLevel

Amavis

Możliwe opcje do nadpisania

- amavisVirusLover
- amavisSpamTagLevel
- amavisSpamQuarantineTo

Amavis

Możliwe opcje do nadpisania

- amavisVirusLover
- amavisSpamTagLevel
- amavisSpamQuarantineTo
- amavisSpamAdmin

Amavis

Możliwe opcje do nadpisania

- amavisVirusLover
- amavisSpamTagLevel
- amavisSpamQuarantineTo
- amavisSpamAdmin
- amavisSpamSubjectTag

Amavis

Możliwe opcje do nadpisania

- amavisVirusLover
- amavisSpamTagLevel
- amavisSpamQuarantineTo
- amavisSpamAdmin
- amavisSpamSubjectTag
- amavisBlacklistSender

Amavis

Możliwe opcje do nadpisania

- amavisVirusLover
- amavisSpamTagLevel
- amavisSpamQuarantineTo
- amavisSpamAdmin
- amavisSpamSubjectTag
- amavisBlacklistSender
- i wiele innych...

Samba

Możliwości

- większość danych w LDAP

Samba

Możliwości

- większość danych w LDAP
  - SID

Samba

Możliwości

- większość danych w LDAP
  - SID
  - hashe haseł

Samba

Możliwości

- większość danych w LDAP
  - SID
  - hashe haseł
  - ścieżka do profilu

Samba

Możliwości

- większość danych w LDAP
  - SID
  - hashe haseł
  - ścieżka do profilu
  - flagi konta

Samba

Możliwości

- większość danych w LDAP
  - SID
  - hashe haseł
  - ścieżka do profilu
  - flagi konta
  - konta maszyn

Samba

Możliwości

- większość danych w LDAP
  - SID
  - hashe haseł
  - ścieżka do profilu
  - flagi konta
  - konta maszyn
- mimo to potrzebuje użytkowników w systemie (nss_ldap) również kont maszyn

Samba

Możliwości

- większość danych w LDAP
  - SID
  - hashe haseł
  - ścieżka do profilu
  - flagi konta
  - konta maszyn
- mimo to potrzebuje użytkowników w systemie (nss_ldap) również kont maszyn
  (teoretycznie wystarczy ldapsam:trusted i ldapsam:editposix, ale nie działa dobrze)

Samba

Możliwości

- większość danych w LDAP
  - SID
  - hashe haseł
  - ścieżka do profilu
  - flagi konta
  - konta maszyn
- mimo to potrzebuje użytkowników w systemie (nss_ldap) również kont maszyn
  (teoretycznie wystarczy ldapsam:trusted i ldapsam:editposix, ale nie działa dobrze)
- obsługa dodawania, usuwania użytkowników

Samba

Jak to zrobić

- passdb backend = ldapsam:"ldapi://"
- ldap suffix = dc=example,dc=com
- ldap . . . suffix
- skrypty do zarządzania kontami (pakiet smb-ldap-tools)
- ldap passwd sync = only

Konfiguracja, uruchomienie

/etc/krb5.conf

```
database = {
  realm = EXAMPLE.COM
  dbname = ldap:ou=Kerberos,dc=example,dc=com
}
```

Konfiguracja, uruchomienie

/etc/krb5.conf

```
database = {
  realm = EXAMPLE.COM
  dbname = ldap:ou=Kerberos,dc=example,dc=com
}
```

kadmin -l

```
init EXAMPLE.COM
```

Konfiguracja, uruchomienie

/etc/krb5.conf

```
database = {
  realm = EXAMPLE.COM
  dbname = ldap:ou=Kerberos,dc=example,dc=com
}
```

kadmin -l

```
init EXAMPLE.COM
```

/etc/krb5.conf

Teraz można zmienić dbname na ldap:dc=example,dc=com

ACL

Prawa potrzebne heimdal-owi

- uid, krb5*
- poddrzewo ou=Kerberos

Utrzymanie porządku

```
rwm-rewriteContext  addDN
rwm-rewriteRule
  "^krb5PrincipalName=([^/]*)/([^,]*),dc=example..."
  "krb5PrincipalName=$1/$2,ou=Kerberos,dc=example..."
  ":"
```

smbk5pwd

Synchronizacja hashy haseł różnych systemów

Używając operacji PASSMOD (LDAPv3) można na raz zmienić hasło w:

- userPassword
- sambaNTPassword, sambaLMPassword
- krb5Key

Aby to działało wszystko musi używać operacji PASSMOD do zmiany hasła, zapisy do userPassword nie są blokowane.

ppolicy

Polityka haseł

- wymuszanie zmiany nie rzadziej/nie częściej niż
- podpięcie crackliba
- historia haseł (ileśtam wstecz musi być różnych)
- blokowanie po nieudanych próbach zalogowania
- wymuszenie zmiany hasła
- każdy może mieć przypisaną inną politykę

ppolicy

Przykład

```
cn=defaultpwcheck,ou=System,dc=example,dc=com
cn: defaultpwcheck
pwdCheckModule: check_password.so
objectClass: applicationProcess
objectClass: pwdPolicy
objectClass: pwdPolicyChecker
pwdAllowUserChange: TRUE
pwdAttribute: userPassword
pwdMinLength: 8
pwdCheckQuality: 1
pwdInHistory: 5
```

syncprov

Replikacja bazy

Istnieje kilka trybów replikacji, ale obecnie preferowany jest ten.
Podstawowe cechy:

- to slave się stara utrzymać swoją kopię aktualną
- po dowolnej awarii/zmianie automatycznie slave się synchronizują do mastera
- bez overlay accesslog początkowa synchronizacja może być obciążająca

syncprov

Przykład

```
syncrepl rid=123
  provider=ldap://master.example.com/
  starttls=critical
  tls_cacert=/etc/ssl/certs/cert.pem
  type=refreshAndPersist
  interval=00:00:15:00
  retry="10 12 60 10 300 +"
  searchbase="dc=example,dc=com"
  schemachecking=off
  bindmethod=simple
  binddn="uid=syncuser,ou=System,dc=example,dc=com"
  credentials=xxxx
```

Co dalej

- radius
- apache, asterisk, bind, jabberd2
- książka adresowa w LDAP
- moodle, squirrelmail
- LAM (LDAP Accout Manager)
- sudo

Przydatne linki i projekty

- OpenLDAP, smbldap-tools, LDAP-HOWTO, ldapvi
- `http://www.openinput.com/auth-howto/`
- `http://www.boobah.info/howto/samba-ldap.html`
- `http://www.padl.com/`
- Trochę patchy m. in. poprawiające obsługę LDAP: `http://marmarek.w.staszic.waw.pl/patches/`
- Overlay do gentoo zawierający powyższe poprawki (i wiele innych): `https://boss.staszic.waw.pl/svn/marmarek-portage/`
- Paczka konfiguracji z działającego systemu: `http://marmarek.w.staszic.waw.pl/ldap-krb-conf.tar.gz`

Dziękuję za uwagę

Pytania?