Samba 3.x + LDAP

Filip Piękniewski 2004

1. Wstęp

Serwer samby zdobywa sobie dzisiaj sporą popularność, podobnie jak usługi katalogowe typu LDAP. Jeśli nasz system oparty jest jedynie o Windows, możemy wykorzystać mechanizm domenowy udostępniony w produktach Microsoft z serii serwer. Jeśli jednak nasz system w pewnej części oparty jest o maszyny unixowe, a w pewnej o maszyny windowsowe, stajemy przed problemem. Jeśli zdecydowaliśmy się trzymać hasła w ldapie, mamy dużą łatwość w udostępnianiu i autoryzacji użytkowników na całej gamie maszyn unixowych, ale co z Windows? System ten nie potrafi współpracować z serwerami ldap. Jednak można wykorzystać dodatkowe narzędzie jakim jest samba. Ustawienie sterownika domeny opartego o sambę nie jest dzisiaj zadaniem trudnym (i nie jest przedmiotem tego dokumentu). Tematem tego dokumentu jest skonfigurowanie samby tak aby potrafiła autoryzować użytkowników w istniejącej juz w naszym systemie bazie ldapowej.

2. Instalacja

W tym dokumencie zakładamy że mamy zainstalowanego i skonfigurowanego ldapa. Wystarczy wspomnieć że na systemach opartych o Fedorę instalacja serwera ldap sprowadza się do polecenia

yum install ldap-servers

Warto zajrzeć na stronę http://www.openldap.org/ oraz http://www.padl.com/ .

Instalacja samby jest dobrze opisana na stronach tego projektu. W tym dokumencie przedstawie zaledwie szkic tego procesu. W systemach Linuxowych opartych o Fedora Core najszybszym sposobem instalacji binarnej wersji samby jest wykonanie polecenia

yum install samba

Kompilacja ze źródeł wymaga nieco więcej zachodu. Po wejściu na stronę www.samba.org możemy ściągnąć jedną z dostępnych dystrybucji pakietu. Najnowsze (ale nie koniecznie najbardziej stabilne) wersje można pobrać z CVS, co jednak nie będzie przedmiotem tego dokumentu. Wybieramy wersje stabilną np. 3.0.7. Ściągamy poleceniem

wget http://us1.samba.org/samba/ftp/samba-3.0.7.tar.gz

Rozpakowujemy poleceniem

tar -zxvf samba-3.0.7.tar.gz

W rozpakowanym drzewie odnajdujemy katalog source i wykonujemy komendę

./configure –help

Dostajemy listę dostępnych opcji kompilacji samby. W naszym przypadku istotne jest aby aktywna była opcja –with-ldap. Opcja –with-ldapsam umożliwi nam parsowanie konfiguracji samba+ldap w wersji 2.2. Domyślnie ta opcja jest wyłączona i nie będziemy z niej korzystać. W razie potrzeby możemy dodać także inne opcje. Przed kompilacją warto się upewnić, że posiadamy odpowiednie nagłówki do ldapa. Istotne też jest też ustawienie opcji –prefix= i ustawić katalog w którym ma być zainstalowana samba. Po skonfigurowaniu wykonujemy

make

I jeśli nie pojawiły się błędy (pewne warningi z linkowania modułów są do pewnego stopnia dopuszczalne), wykonujemy

make install

Jeśli wszystko się udało, możemy przystąpić do konfiguracji.

3. Konfiguracja LDAPa

Cały proces zaczynamy od skopiowania schematu ldapowego samby w miejsce w którym trzymamy nasze schematy. Domyślnie jest to /etc/openldap/schema .

cp samba-3.0.7/examples/LDAP/samba.schema /etc/opeldap/schema/

Następnie trzeba zainkludować ten schemat w pliku slapd.conf. Powinno to wyglądać mniej więcej tak (w miejscu pliku slapd.conf gdzie występują podobne linijki):

(...)
include /etc/openldap/schema/samba.schema
(...)

Można jeszcze dodać użytkownika, z którego będzie korzystać samba do modyfikowania bazy

ldapowej oraz ustawić odpowiednie ACL'e. W tym dokumencie dla uproszczenia założymy że tym użytkownikiem będzie rootdn zdefiniowany już w pliku slapd.conf. Samba będzie wymagała sporych praw (modyfikacji bazy) zatem użycie rootdn nie jest pozbawione sensu.

Po zrestartowaniu slapd możemy przyjąć że ldap jest gotowy.

4. Konfiguracja samby

Konfiguracja samby wymaga nieco więcej czasu. Na początku warto sprawdzić czy nasza samba w ogóle działa, żeby później nie spotkała nas przykra niespodzianka. W tym celu można wykorzystać domyślną konfigurację, dodać użytkownika do bazy smbpasswd za pomocą polecenia

smbpasswd -a user

(Przy czym “user” musi istnieć w systemie), oraz sprawdzić za pomocą smbclient czy widzimy jakiekolwiek zasoby (przykładowo możemy uzyskać wynik podobny do poniższego):

```
[user1@host user1]$ smbclient -L 127.0.0.1  --username="user1"
Password:
Domain=[HOSTNAME] OS=[Unix] Server=[Samba 3.0.7-2.FC2]

        Sharename       Type      Comment
        ---------       ----      -------
        tmp             Disk      Temporary file space
        IPC$             IPC       IPC Service (myserver)
        ADMIN$          IPC       IPC Service (myserver)
        lj4200          Printer   lj4200
        user1           Disk      Home Directories
Domain=[HOSTNAME] OS=[Unix] Server=[Samba 3.0.7-2.FC2]
```

Jeśli dostępne są jakieś zasoby sieciowe, warto któryś z nich spróbować zamontować np. komendą (jako root):

smbmount \\\\hostname\\homes /mnt/smb/ -o username=user1

Gdy ponad wszelką wątpliwość stwierdzimy poprawne działanie samby, możemy przystąpić do konfigurowania autoryzacji w ldapie. W pliku smb.conf w sekcji global należy dodać następujące opcje:

```
ldap admin dn = "cn=rootdn,dc=example,dc=com"
passdb backend = ldapsam:ldap://nasz_ldap:389
```

ldap ssl = start tls
ldap suffix = "dc=suff, dc=example, dc=com"

Oczywiście musimy tu ustawić poprawny suffix naszego ldapa, jego adres oraz admin dn. Opcja ldap ssl może przyjmować wartość off jeśli nie mamy skonfigurowanego ssl'a, jednak takiej konfiguracji należy unikać. Opcja start tls może sprawiać kłopoty jeśli mamy nie do końca dobrze zrobione certyfikaty, w szczególności jeśli nazwa hosta zapisana w certyfikacie różni się od nazwy rzeczywistej.

Następnie musimy zapisać hasło rootdn z ldapa. Samba zapisuje to hasło w pliku secrets.tdb. Domyślnie znajduje się on w katalogu /etc/samba, lub w podkatalogu private katalogu samby. Hasło zapisujemy poleceniem:

smbpasswd -w hasło

UWAGA, hasło przetrzymywane w pliku secrets.tdb jest niezaszyfrowane. Należy zadbać aby prawa do odczytu tego pliku były odpowiednio ograniczone. Jako root możemy odzyskać to hasło poleceniem

tdbdump secrets.tdb

Po restarcie samby możemy przystąpić do testowania.

5. Testowanie

Poprawne działanie autoryzacji samby w ldapie wymaga dodania odpowiednich pól w bazie. Przykładowy wpis użytkownika mogłby wyglądać mniej więcej tak:

```
[user@host user]$ ldapsearch -x -W -D "cn=rootdn,dc=example,dc=com" uid=user1
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <> with scope sub
# filter: uid=user1
# requesting: ALL
#

# user1, People, example.com
dn: uid=user1,ou=People,dc=testy,dc=com
uid: user1
```

objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
objectClass: sambaSamAccount
userPassword:: ahHUYEb ahyeHgJAIIUsdjhbdfhuisdfjJUskauLDueUDjsybBDysjwYtwbReq=
shadowLastChange: 12659
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 218
gidNumber: 10
homeDirectory: /home/user1
cn: user1
sambaSID: S-1-5-21-652118892-417317042-705933398-1436
sambaPrimaryGroupSID: S-1-5-21-652118892-417317042-705933398-1021
sambaLMPassword: BDT53JSIS84JDYSIF8HDU38CBWKSAI9E
sambaAcctFlags: [U]
sambaNTPassword: DKJIFIJ38S62JXBDHDS92KLAPD9FH7E0
sambaPwdCanChange: 1097575852
sambaPwdMustChange: 2147483647
sambaPasswordHistory: 0000000000000000000000000000000000000000000000000000000000000000
00000000
sambaPwdLastSet: 1097575852

 # search result
search: 2
result: 0 Success

 # numResponses: 2
 # numEntries: 1

Oczywiście wszystkie hasze zostały zmienione. Warto zwrócić uwagę na atrybuty:

objectClass: sambaSamAccount
sambaSID: S-1-5-21-652118892-417317042-705933398-1436
sambaPrimaryGroupSID: S-1-5-21-652118892-417317042-705933398-1021
sambaLMPassword: BDT53JSIS84JDYSIF8HDU38CBWKSAI9E
sambaAcctFlags: [U]
sambaNTPassword: DKJIFIJ38S62JXBDHDS92KLAPD9FH7E0

sambaSID jest numerem identyfikującym użytkownika w domenie (zakładamy że nasza samba jest

kontrolerem domeny). Ostatnia liczba powstaje z unixowego UID*2+1000, w przypadku sambaPrimaryGroupSID jest to unixowy GID*2+1001. Pola sambaLMPassword oraz sambaNTPassword są funkcjami skrótu haseł w formacie znanym z windows NT oraz nowszym (LANMAN) znanym z windows 2000. Zauważmy że pola te nie mają nic wspólnego z polem przechowującym hasło unixowe.

Aby utworzyć odpowiednie struktury w LDAPie można wykorzystać polecenie

smbpasswd -a user

Które wykonane z roota (o ile user istnieje w systemie) ustawi sambowe hasło oraz wszystkie inne potrzebne pola automatycznie. Póki takie polecenie nie będzie wykonane, user nie będzie miał możliwości korzystania z dobrodziejstw samby. Synchronizacja haseł z unixowymi jest zadaniem nieco trudniejszym. Samba potrafi synchronizować hasła z ldapem jeśli do autoryzacji wykorzystujemy pam_ldap. W takim przypadku ustawienie w smb.conf opcji:

ldap passwd sync=yes

spowoduje, że w tak skonfigurowanym systemie gdy użytkownik wykona komendę

smbpasswd

Zmieniając swoje hasło sambowe zmieni także hasło unixowe (nie na odwrót!!!)

6. Narzędzia smb-ldap

Wraz z dystrybucją samby dostajemy ciekawy zestaw narzędzi migracyjnych pod nazwą smbldap-tools (dostępne w katalogu zrodla-samba-3.0.7/examples/LDAP/smbldap-tools lub na systemach redhatowych w katalogu /usr/share/doc/samba-ver/LDAP/smbldap-tools). Do poprawnego działania potrzebują zestawu perlowych modułów (Net:LDAP) które możemy zainstalować z CPAN (jeśli ich jeszcze nie posiadamy) za pomocą polecenia:

perl -MCPAN -e shell

Wykonanym z roota. Po dostaniu odpowiedniego shella wpisujemy

install Net::LDAP

aby system automatycznie ściągnął i skompilował odpowiednie narzędzia. Gdy już nam się to uda możemy przystąpić do konfigurowania narzędzi. Po wykonaniu ls w katalogu powinniśmy uzyskać

widok podobny do poniższego:

```
[root@host smbldap-tools]# ls
cgi          INFRASTRUCTURE  smbldap_conf.pm       smbldap-migrate-accounts.pl  smbldap-tools.spec   TODO
ChangeLog    INSTALL         smbldap-groupadd.pl   smbldap-migrate-groups.pl    smbldap-useradd.pl
CONTRIBUTORS Makefile        smbldap-groupdel.pl   smbldap-passwd.pl            smbldap-userdel.pl
COPYING      mkntpwd         smbldap-groupmod.pl   smbldap-populate.pl          smbldap-usermod.pl
FILES        README          smbldap-groupshow.pl  smbldap_tools.pm             smbldap-usershow.pl
```

W pliku smbldap_conf.pm wpisujemy odpowiednie dane:

```
(...)
# LDAP Suffix
# Ex: $suffix = "dc=IDEALX,dc=ORG";
$suffix = "dc=suffix,dc=examples,dc=com";
(...)
# Bind DN passwd used
# Ex: $bindpasswd = 'secret'; for 'secret'
$bindpasswd = "tajnehasloldapa";
(...)
```

Oraz odpowiednie ścieżki do narzędzi ldapa i narzędza mkntpwd (zawyczaj dostępnego w podkatalogu mkntpwd katalogu z narzędziami – trzema je koniecznie skompilować poleceniem make).

Po wykonaniu konfiguracji i zadbaniu aby plik smbldap_conf.pm miał odpowiednie prawa, możemy rozpocząć korzystanie z narzędzi. Pomoc na temat każdego z nich możemy uzyskać poleceniem:

perldoc nazwa_narzędzia

Funkcjonalność narzędzia uzyskujemy wykonując polecenie:

perl nazwa_narzędzia

Narzędzia te pozwalają migrować konta windowsowe z plików pwdump, a także edytować wpisy w bazie ldapowej.

7. Podsumowanie

Ldap w połączeniu z sambą może okazać się najlepszym sposobem zintegrowania dużego systemu komputerowego działającego zarówno w środowisku Windows jak i Unix. Staranne skonfigurowanie tych narzędzi pozwala uzyskać stan w którym użytkownik posiadający konto w

systemie unixowym może się logować z tym samym hasłem na komputery windowsowe, a co więcej może uzyskać dostęp do swojego katalogu domowego (eksportowanego przez smb).

8. Literatura

[1] http://us1.samba.org/samba/docs/man/Samba-HOWTO-Collection/
[2] http://www.ofb.net/~jheiss/samba/ldap.shtml
[3] http://www.unav.es/cti/ldap-smb-howto.html
[4] http://ldap.uni.torun.pl/raporty/ftp/uci/samba-ldap.html