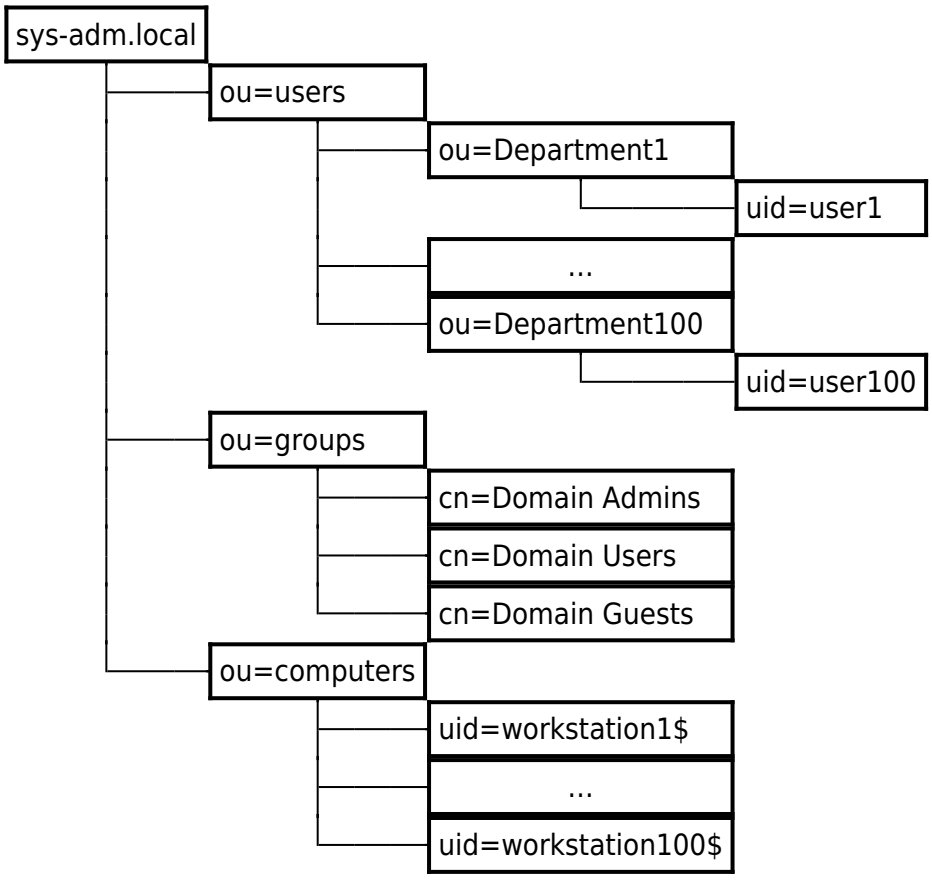
Доменный файл сервер с аудитом доступа к данным

Введение

Думаю в каждой организации возникает необходимость в использовании корпоративного файл сервера. Но в отличие от Гостевого файл сервера на данном сервере нам необходимо строгое и четкое разделение уровня доступа пользователей к информации.

Данная статья подразумевает что у вас уже настроен и работает контроллер домена на базе samba + OpenLDAP, так как все учетные данные мы будем брать именно с контроллера домена. В случае если у вас роль КД выполняет windows server, то данная статья не подойдет вам, хотя для использование в среде windows AD необходимо будет сделать не так уж и много изменений, но это уже совсем отдельная тема. Для решения поставленной задачи мы будем использовать samba.

Подразумевается что наш LDAP каталог имеет следующую структуру, а контроллер домена у вас поднят на samba



Настройка nsswitch на работу с LDAP каталогом

Итак, в нашем распоряжении имеется следующая система:

```
# cat /etc/redhat-release
CentOS release 6.2 (Final)

# uname -r
2.6.32-220.17.1.el6.x86_64
```

Устанавливаем необходимые пакеты

```
# yum install samba samba-client samba-common samba-winbind nss-pam-ldapd
openldap-clients
```

Редактируем файл **/etc/hosts** и настраиваем корректное имя нашего хоста

```
# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain
192.168.127.10 fs1 fs1.sys-adm.local
```

Настраиваем демон ntp для синхронизации времени

Редактируем файл **/etc/nsswitch.conf** и настраиваем поиск пользователей в LDAP каталоге. Так же поиск компьютеров будет производиться с помощью wins сервера.

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap

hosts:      files dns wins
```

Все остальные строки оставляем без изменений. Таким образом при поиске пользователей, групп и их паролей система так же будет обращаться в LDAP каталог. Для того, чтобы система знала к какому именно LDAP каталогу обращаться и где искать необходимую информацию нам необходимо настроить nslcd демон.

Редактируем файл **/etc/nslcd.conf**. Настройки производим в соответствии с нашей структурой (см схему выше).

```
# Пользователь и группа от имени которого работает демон
uid nslcd
gid ldap

# Указываем адрес нашего LDAP каталога, в нашем случае LDAP сервер располагается на
том же сервере где и samba
uri ldap://pdc.sys-adm.local/

# Версия LDAP протокола
```

```
ldap_version 3

# База для поиска в LDAP каталоге
base dc=sys-adm,dc=local

# Указываем область поиска. В данном случае sub (subtree) поиск будет производится и в подкаталогах тоже
scope sub

# Указываем фильтры для поиска пользователей, групп и паролей
base group  ou=groups,dc=sys-adm,dc=local
base passwd ou=users,dc=sys-adm,dc=local
base shadow ou=users,dc=sys-adm,dc=local
base passwd ou=computers,dc=sys-adm,dc=local
```

Запускаем демон и проверяем его работу.

```
# service nslcd start
Starting nslcd:                                            [  OK  ]

# id adomoradov
uid=1111(adomoradov) gid=512(Domain Admins) groups=512(Domain
Admins),513(Domain Users)

# getent passwd adomoradov
adomoradov:x:1111:512:System User:/home/adomoradov:/bin/false

# getent group "Domain Admins"
Domain Admins:*:512:adomoradov,root
```

Как мы видим система видит пользователя с LDAP каталога, чего собственно мы и добивались. Так же вы можете проверить корректность работы nsswitch с помощью getent passwd и getent group. В результате выполнения этих команд должны возвращаться все пользователи и группы с LDAP каталога.

При большом количестве записей в LDAP каталоге и большом количестве файлов, а так же при интенсивной работе файл сервера, можно запустить кеширующий сервер nscd, который будет кешировать все запросы nsswitch. Редактируем файл **/etc/nscd.conf** и запускаем демон.

```
        logfile                 /var/log/nscd.log
        server-user             nscd
        debug-level             0
        paranoia                no

        enable-cache            passwd          yes
        positive-time-to-live   passwd          600
        negative-time-to-live   passwd          20
        suggested-size          passwd          211
        check-files             passwd          yes
        persistent              passwd          yes
        shared                  passwd          yes
```

```
        max-db-size             passwd          33554432
        auto-propagate          passwd          yes

        enable-cache            group           yes
        positive-time-to-live   group           3600
        negative-time-to-live   group           60
        suggested-size          group           211
        check-files             group           yes
        persistent              group           yes
        shared                  group           yes
        max-db-size             group           33554432
        auto-propagate          group           yes
```

```
# service nscd start
Starting nscd:                                             [  OK  ]
```

Его работу очень легко проверить. Для этого мы делаем просмотр любого доменного пользователя, чтобы его информация закешировалась. После этого мы останавливаем демон nslcd, т.е. система уже не сможет получать информацию из LDAP каталога, но при этом информацию, которая осталась в кеше мы всегда сможем получить, во время жизни самого кеша, который в нашем случае составляет 10 минут.

```
# id adomoradov
uid=1111(adomoradov) gid=512(Domain Admins) groups=512(Domain
Admins),513(Domain Users)

# service nslcd stop
Stopping nslcd:                                            [  OK  ]

# id adomoradov
uid=1111(adomoradov) gid=512(Domain Admins) groups=512(Domain
Admins),513(Domain Users)

# id sysadmin
id: sysadmin: No such user
```

Снова запускаем nslcd демон и проверяем работу

```
# service nscd start
Starting nscd:                                             [  OK  ]

# id adomoradov
uid=1111(adomoradov) gid=512(Domain Admins) groups=512(Domain
Admins),513(Domain Users)

# id sysadmin
uid=1200(sysadmin) gid=513(Domain Users) groups=513(Domain Users)
```

Если у вас все работает верно, то можно приступать непосредственно к настройке samba.

Установка и настройка samba

Редактируем основной конфигурационный файл самбы **/etc/samba/smb.conf**

```
[global]

  # Общие настройки сервера
    workgroup = SYSADM
    server string = File server
    netbios name = FS1
    security = domain

  # Отключаем все, что связанно с печатью
    load printers = no
    show add printer wizard = no
    printcap name = /dev/null
    disable spoolss = yes

  # Путь log файла и его максимальный размер в килобайтах
    log file = /var/log/samba/samba.log
    max log size = 50000

  # Включаем использование шифрованных паролей
    encrypt passwords = yes
  # Вызов wbinfo -u и wbinfo -g будет возвращать список доменных пользователей и групп соответственно
    winbind enum groups = yes
    winbind enum users = yes

  # Настраиваем idmap бекенд для хранение соответствий sid uid/gid
    idmap backend = ldap:"ldap://pdc.sys-adm.local/"
    ldap idmap suffix = ou=idmap

    idmap uid = 1000-500000
    idmap gid = 1000-500000

    idmap config SYSADM : backend  = nss
    idmap config SYSADM : range = 1000-500000

    ldapsam:trusted = yes
    ldapsam:editposix = yes

  # Указываем, где LDAP хранит информацию о пользователях, группах и компьютерах
    ldap suffix = dc=sys-adm,dc=local
    ldap user suffix = ou=users
    ldap group suffix = ou=groups
    ldap machine suffix = ou=computers
    # DN (Distinguished Name) используемой самбой при доступе к LDAP каталогу
    ldap admin dn = "uid=ldap_reader,ou=users,dc=sys-adm,dc=local"
```

```
    enable privileges = yes
  # Наш файл сервер не будет участвовать в выборе master browser, а так же не будет
выполнять роль доменного мастера
    os level = 3
    local master = no
    domain master = no
    preferred master = no
    domain logons = no

  # Указываем wins сервер
    wins server = 192.168.127.2
  # Так как наш файл сервер не является wins сервером, отключаем данный функционал
    dns proxy = no

  # Используем NTLMv2
    client ntlmv2 auth = yes
  # Запрещаем отправлять пароль в чистом виде, если сервер не поддерживает шифрование
    client plaintext auth = no

  # Отключаем использование старых методов аутентификации
    lanman auth = no
    lm announce = no

  # Время неактивности в минутах, после чего соединение считается мертвым и
закрывается.
    deadtime = 15

  # Задаем кодировки
    display charset = utf8
    unix charset = utf8
    dos charset = cp866

  # Уровень информативности в log файлах
    log level  = 3
    host msdfs  = no

[Department1]
    comment = Department1
    path = /samba/department1/
    public=yes
  # Запрещаем доступ гостям
    guest ok = no
  # Список пользователей, которым разрешено производить запись
    write list = adomoradov, @"SYSADM\department1"
  # Список пользователей, которым разрешено подключаться к ресурсу
    valid users = @"SYSADM\department1"
    browseable = yes
  # Настраиваем маски для вновь создаваемых файлов и папок. С данными масками
  # объекты смогут редактировать только владельцы и члены группы department1
    force create mode = 0770
    create mode = 0770
```

```
    force directory mode = 0770
    directory mode = 0770
  # Включаем ауйдит следующих действий: создание, удаление, изменение и
переименование
    vfs objects = full_audit
    full_audit:prefix = [Department1]:%u|%I
    full_audit:success = write rmdir rename mkdir unlink open read pread
write pwrite
    full_audit:failure = none
    full_audit:facility = LOCAL1
    full_audit:priority = ALERT
```

Задаем пароль для доменного пользователя, которого мы указали в ldap admin dn

```
# smbpasswd -w 1234567
Setting stored password for "uid=ldap_reader,ou=users,dc=sys-adm,dc=local"
in secrets.tdb
```

Так как пароль сохраняется в файле secrets.tdb, то после смены пользователя, указанного в ldap admin dn, необходимо будет ввести новый пароль с помощью этой же команды.

На PDC создаем учетную запись для сервера

```
# smbldap-useradd -W -g 515 FS1
# smbldap-usershow FS1
dn: uid=FS1$,ou=computers,dc=sys-adm,dc=local
cn: FS1$
uid: FS1$
uidNumber: 1962
gidNumber: 515
homeDirectory: /nonexistent
loginShell: /bin/false
description: Computer
gecos: Computer
objectClass: posixAccount,account,sambaSamAccount
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
sambaPwdLastSet: 1337355106
sambaAcctFlags: [W          ]
sambaSID: S-1-5-21-206255134-223837211-2022137911-4924
sambaPrimaryGroupSID: S-1-5-21-206255134-223837211-2022137911-515
displayName: FS1$
sambaDomainName: SYSADM
```

Вводим наш файл сервер в домен. В принципе в параметре -U можно указать любого пользователя, у которого есть право на добавление компьютеров в домен.

```
# net rpc join -U adomoradov MEMBER
```

```
Enter adomoradov's password:
Joined domain SYSADM.
```

Сохраняем доменный SID и проверяем информацию о домене

```
# net getdomainsid
SID for local machine FS1 is: S-1-5-21-483159814-3832461950-2058659463
SID for domain SYSADM is: S-1-5-21-206255134-223837211-2022137911

# net rpc info -U adomoradov
Enter adomoradov's password:
Domain Name: SYSADM
Domain SID: S-1-5-21-206255134-223837211-2022137911
Sequence number: 1337889347
Num users: 18
Num domain groups: 17
Num local groups: 0
```

Запускаем демон winbind и производим базовые проверки

```
# service winbind start
Starting Winbind services:                                 [  OK  ]

# wbinfo -p
Ping to winbindd succeeded

# wbinfo -t
checking the trust secret for domain SYSADM via RPC calls succeeded

# wbinfo -u | grep ldap_reader
SYSADM\ldap_reader

# wbinfo -g | grep "domain"
SYSADM\domain admins
SYSADM\domain users
SYSADM\domain guests
SYSADM\domain computers
```

Проверяем аутентификацию через демон winbind

```
# wbinfo -a SYSADM\\ldap_reader%1234567
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

Проверяем преобразование SID → uid и uid → SID

```
# wbinfo -i SYSADM\\adomoradov
SYSADM\adomoradov:*:1111:512:Aleksey Domoradov:/home/adomoradov:/bin/bash

# wbinfo --name-to-sid=SYSADM\\adomoradov
```

```
S-1-5-21-206255134-223837211-2022137911-1111 SID_USER (1)

# wbinfo --sid-to-uid=S-1-5-21-206255134-223837211-2022137911-1111
1111
```

Запускаем самбу

```
# service smb start
Starting SMB services:                                     [  OK  ]
```

```
# service nmb start
Starting NMB services:                                     [  OK  ]
```

Добавляем запуск самбы при старте системы

```
# chkconfig --level 35 nmb on
# chkconfig --level 35 smb on
# chkconfig --level 35 winbind on
```

Настройка аудита и тестирование

Так как мы хотим знать, кто и что делал с определенным файлом, то мы настроим логирование аудита в файл. Для этого необходимо добавить следующую строку в файл **/etc/rsyslog.conf**

```
local1.*   /var/log/samba/audit.log
```

Создаем соответствующий файл и перезапускаем демон

```
# touch /var/log/samba/audit.log
# chmod 640 /var/log/samba/audit.log
# service rsyslog restart
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
```

Создадим несколько файлов и папок, переименуем их и удалим, в результате чего в log файле аудита появятся подобные записи

```
# tail -f /var/log/samba/audit.log
May 18 20:09:15 fs1 smbd[4282]:
[Department1]:adomoradov|192.168.127.50|mkdir|ok|test
May 18 20:09:25 fs1 smbd[4282]:
[Department1]:adomoradov|192.168.127.50|rename|ok|./test|./test1
May 18 20:09:30 fs1 smbd[4282]:
[Department1]:adomoradov|192.168.127.50|rename|ok|./test1|./test2
May 18 20:09:34 fs1 smbd[4282]:
[Department1]:adomoradov|192.168.127.50|rename|ok|./test2|./test3
May 18 20:10:17 fs1 smbd[4282]:
[Department1]:adomoradov|192.168.127.50|rename|ok|test3/debian-
```

```
handbook.pdf|test3/debian.pdf
May 18 20:10:28 fs1 smbd[4282]:
[Department1]:adomoradov|192.168.127.50|unlink|ok|test3/debian.pdf
May 18 20:10:33 fs1 smbd[4282]:
[Department1]:adomoradov|192.168.127.50|rmdir|ok|test3
```

На этом настройку можно считать завершенной.