SAMBA - внедряемся в офисную сеть

Опубликовано muff в Чт, 2009-09-03 16:30

Вот, в очередной раз необходимо предоставить виндовым админам доступ к файлам на сервере под управлением FreeBSD. Поскольку сервер находтся в одной локальной сети с остальными компьютерами, доступ решено организовать по протоколу SMB. Что не может не радовать, так это то, что по утверждениям ITLabs, в условиях многопользовательского доступа, скорость работы Samba в качестве файлового и принт-сервера более чем в два раза выше по сравнению с Windows Server 2003 с теми же ролями.

В нашем случае нужна почти минимальная конфигурация: поддержка виндовых шар и разграничение прав доступа...

Итак, начнем установку samba-сервера из портов (за актуальностью которых не забываем следить):

```
# cd /usr/ports/net/samba3/
# make install clean
```

Рассмотрим доступные опции:

```
Options for samba 3.0.36,1


[ ] LDAP         With LDAP support[ ] ADS          With Active Directory support[ ]
CUPS         With CUPS printing support[ ] WINBIND      With WinBIND support[X] ACL_
SUPPORT  With ACL support[ ] AIO_SUPPORT  With Asyncronous IO support[X] FAM_SUPPORT
  With File Alteration Monitor[X] SYSLOG       With Syslog support[X] QUOTAS       W
ith Disk quota support[ ] UTMP         With UTMP accounting support[ ] PAM_SMBPASS
With PAM authentication vs passdb backends[ ] CLUSTER      With experimental cluster
 support[ ] DNSUPDATE    With dynamic DNS update(require ADS)[ ] EXP_MODULES  With e
xperimental modules[X] POPT         With system-wide POPT library[X] PCH          Wi
th precompiled headers optimization[ ] MAX_DEBUG    With maximum debugging[ ] SMBTOR
TURE   With smbtorture
```

LDAP - поддержка LDAP [1]. Не использую. Отключаем.

ADS -поддержка Active Directory [2]. Отключаем.

CUPS - поддержка сервера печати CUPS. Не интересно. Отключаем.

WINBIND - обьединение пользвателей Windows/Unix. Почитать можно здесь [3]. Отключаем.

ACL_SUPPORT - поддержка Access Control List [4]. Очень даже нужная фича. Включаем.

AIO_SUPPORT - поддержка возможности асинхронного ввода-вывода. По дефолту оключено... И я включать не буду ;)

FAM_SUPPORT - API для мониторинга за состоянием файла или группы файлов/директорий.

Возможно пригодится. Включаем.

SYSLOG - поддержка логирования syslog. Однозначно пригодится :). Включаем.

QUOTAS - поддержка квотирования. Поскольку диски не резиновые, а пользователи жадные до дискового пространства - включаем.

UTMP - включаем поддержку уникального идентификатора для каждого вновь подключенного пользователя. Поскольку понижает производительность - выключаем.

PAM_SMBPASS - поддержка синхронизации системных пользователей и пользователей samba. В нашем случае неактуально, поэтому оставляем выключеным.

DNSUPDATE - поддержка динамического обновления DNS. Поскольку данный вариант работает с поддержкой Active Directory, что нам не нужно, то оставляем отключенным.

EXP_MODULES - поддержка експериментальных модулей. А нам нужна стабильность в работе. Соответственно не включаем ;)

POPT - поддержка системной библиотеки анализа коммандной строки. Авось пригодится ;). Включаем.

PCH - предкомпиляционная оптимизация заголовков. Звучит заманчиво. Включаем.

MAX_DEBUG - включение режима максимальной отладки. На всякий случай включим.

SMBTORTURE - утилита для стресс-тестирования серверов. У нас и так стрессовых ситуаций достаточно, можно обойтись ;). Отключено.

С опциями разобрались... Дождемся завершения установки и перечитаем пути.

```
# rehash
```

Лезем "копаться" в конфиге. В результате нехитрых манипуляций конфигурационный файл приобретает следующий вид:

```
# cat /usr/local/etc/smb.conf

#======================== Global Settings
=====================================
# В разделе global задаются все основные настройки (голбальные для сервера Samba)

[global]

# Название рабочей групы. Должно совпадать с названием рабочей групы

# на клиентских машинах.
workgroup = LOCALNET

# Строка описания сервера. Высвечивается в сетевом окружении.
server string = FreeBSD Samba Server
# Тип входа. user - авторизация пользователей по логину и паролю. Те, кто

# хочет создать файлообменник,  могут воспользоваться опцией share.

security = user

# Список сетей, которым разрешено коннектиться к серверу.
```

```
hosts allow = 192.168.0. 127.

# Куда будут писаться логи, и в каком формате.
log file = /var/log/samba/log.%m

# Задаем максимальный размер лог-файла (в килобайтах). 10 мегабайт - для среднего
сервера

# достаточно

max log size = 10240

# Если несколько сетевых интерфейсов, указываем, на каких "слушать" запросы
пользователей.

# Даже если интерфес только один, по привычке указываю. А вдруг что-то поменяется ;)
interfaces = 192.168.0.155/24

# Если уж есть samba-сервер, то сделаем его мастер-браузером для нашей сети.
local master = yes

# "Крутость" операционной системы. Учитывается при выборах мастер-браузера.
os level = 255

#Дает дополнительный приоритет во время "голосования" и выборов мастер-браузера.

preferred master = yes

#============================= Share Definitions
==============================
# Здесь начинается описание расшареных ресурсов

# comment - комментарий к ресурсу

# path - путь к каталогу, который необходимо "расшарить"

# browseable - будет ли каталог виден в "сетевом окружении", или будет скрытым

# writable - возможно ли записывать данные в этот сетевой ресурс

# valid users - список пользователей, которым разрешен доступ к данной шаре

# hosts allow - перечень IP, которым разрешен доступ к данной шаре

# guest ok - разрешаем гостевой доступ

[winadmin]
   comment = Share for admins
   path = /var/samba/admin
   browseable = yes
   writable = yes
   valid users = winadmin
   hosts allow = 192.168.0.2


[share]
   comment = Share for all users
   path = /var/samba/share
   browseable = yes
```

```
writable = yes
guest ok = yes
```

Как видим, сам файл конфигурации пока минимален. Но мы потом это исправим в случае необходимости.

Добавим поддержку загрузки стартового скрипта samba в /etc/rc.conf:

```
# echo '### Samba-server' >> /etc/rc.conf
# echo 'samba_enable="YES"' >> /etc/rc.conf
```

Далее добавим пользователя winadmin. samba имеет свою базу логинов и паролей. Работать с этой базой можно с помощью утилиты smbpasswd. Однако не стоит забывать про то, что для корректной работы в системе должен присутствовать точно такой же пользователь. Что ж, если должен, значит сделаем. Добавим системного пользователя winadmin, правда доступ к консоли ему давать не будем ;)

```
# adduser
Username: winadmin
 Full name: Local administrators
 Uid (Leave empty for default):
Login group [admin]: nobody
 Login group is nobody. Invite admin into other groups? []:
Login class [default]: rusian
 Shell (sh csh tcsh nologin) [sh]: nologin
Home directory [/home/admin]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]: no
Lock out the account after creation? [no]:
Username   : winadmin
Password   : <disabled>
Full Name  : Local administrators
Uid        : 1003
Class      : rusian
Groups     : nobody
Home       : /home/admin
Home Mode  :
Shell      : /usr/sbin/nologin
Locked     : no
OK? (yes/no): yes
adduser: INFO: Successfully added (admin) to the user database.
Add another user? (yes/no): no
Goodbye!
```

Теперь воспользуемся утилитой smbpasswd, чтобы добавить пользователя samba:

```
# smbpasswd -a winadmin
New SMB password:
Retype new SMB password:
startsmbfilepwent_internal: file /usr/local/etc/samba/smbpasswd did not exist. File successfully created.
Added user winadmin.
```

Опция **-a** указывает на то, что пользователь в базе пользователей samba еще не существует, то есть указывает, что мы добавляем нового пользователя. В случае, если вам необходимо просто сменить пароль для пользователя, этот ключ опускаем.

Как вы уже догадались, пароли samba и пароли системных пользователей хранятся в рахных хранилищах, соответственно могут отличатся (и я рекомендую использовать разные пароли).

Из вывода видно, что пароли samba хранятся в файле /usr/local/etc/samba/smbpasswd.

У меня еще не созданы папки шар. Нужно создать :). Кстати, samba бережно относится к правам доступа файлов. Доступ будет осуществлятся от имени авторизовавшегося пользователя. Соответственно выставляем необходимые права доступа:

```
# mkdir -p /var/samba/winadmin
 # mkdir /var/samba/share
 # chown winadmin:nobody /var/samba/winadmin/
 # chmod 777 /var/samba/share
```

Пробуем запустить samba.

```
# sh /usr/local/etc/rc.d/samba start
 Removing stale Samba tdb files:  done
Starting nmbd.
Starting smbd.
# ps -ax | grep smb
 97289  ??  Ss     0:00,01 /usr/local/sbin/nmbd -D -s /usr/local/etc/smb.conf
97293  ??  Is     0:00,01 /usr/local/sbin/smbd -D -s /usr/local/etc/smb.conf
97294  ??  I      0:00,00 /usr/local/sbin/smbd -D -s /usr/local/etc/smb.conf
```

Кажется все заработало... На всякий случай посмотрим, что делается в логах:

```
# tail - f /var/log/messages

Sep  4 10:48:42 mail nmbd[97421]: [2009/09/04 10:48:42, 0]
nmbd/nmbd_become_lmb.c:become_local_master_stage2(396)
Sep  4 10:48:42 mail nmbd[97421]:   *****
Sep  4 10:48:42 mail nmbd[97421]:
Sep  4 10:48:42 mail nmbd[97421]:   Samba name server MAIL is now a local master browser for
workgroup LOCALNET on subnet 192.168.0.155
Sep  4 10:48:42 mail nmbd[97421]:
Sep  4 10:48:42 mail nmbd[97421]:   *****
```

Отлично. Samba даже стала мастер-браузером для рабочей группы LOCALNET в подсети 192.168.0.0/24. После набора в командной строке адреса сервера (\\192.168.0.155), появилось окно запроса логина и пароля доступа к сетевому ресурсу. После ввода логина winadmin и заданого пароля, доступ был разрешен. Это уже неплохо :)

Чтобы ознакомиться с полными возможностями samba, воспользуемся интерфейсом управления.

Немного общей информации... SWAT (Samba Web Administration Tool) - программа, которая позволяет сконфигурировать сервер Samba через web-интерфейс изменяя таким образом конфигурационный файл smb.conf. SWAT является частью набора Samba, поэтому развивается параллельно и не использует устаревшие опции в smb.conf.

SWAT запускается через суперсервер inetd. Чтобы разрешить запуск SWAT, необходимо в конфигурационном файле /etc/inetd.conf раскомментировать такую строку:

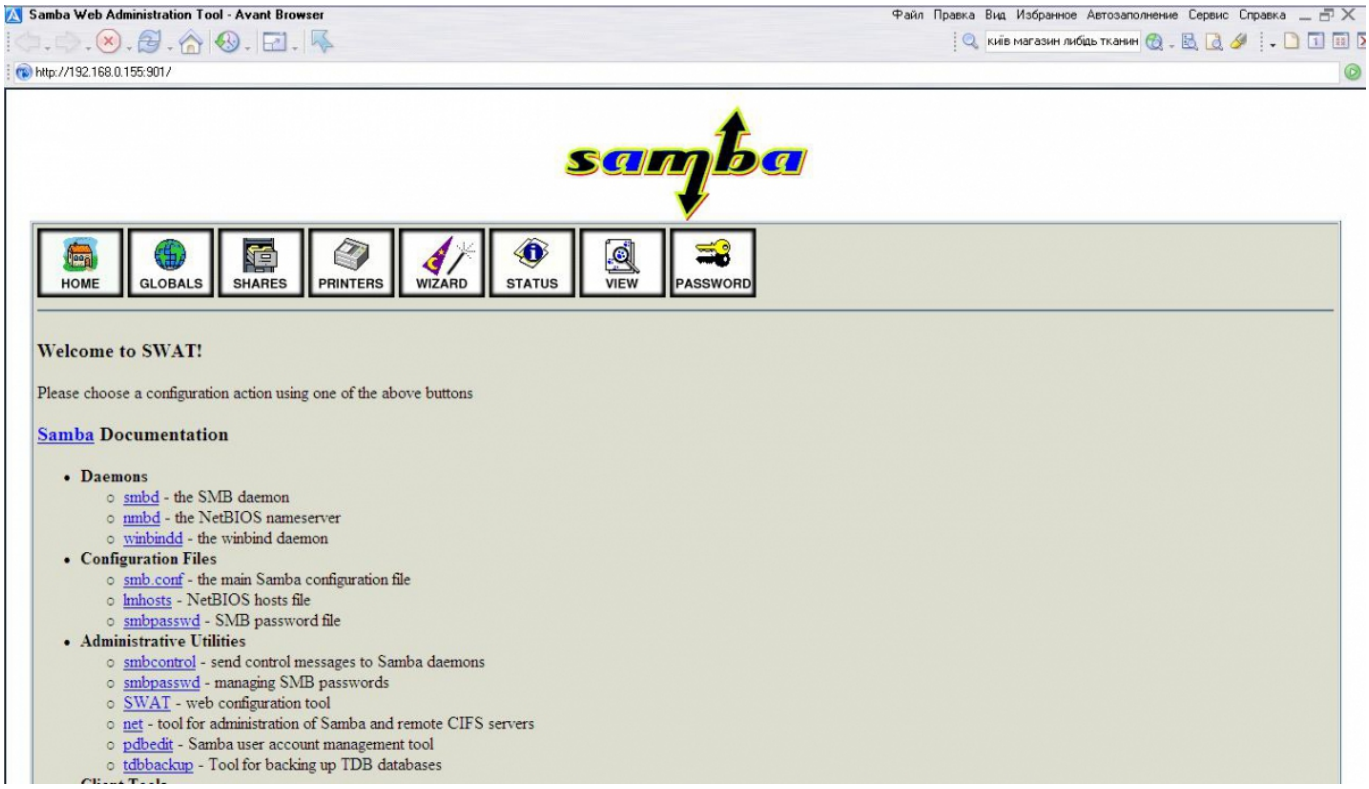
```
swat    stream  tcp     nowait/400      root    /usr/local/sbin/swat    swat
```

Добавляем в rc.conf поддержку inetd и запускаем службу:

```
# echo 'inetd_enable="YES"' >> /etc/rc.conf
# sh /etc/rc.d/inetd start
 Starting inetd.
```

Открываем любимый браузер и в строке адреса набиваем: http://ip_interface_samba-servera:901 [5]. В моем случае это http://192.168.0.155:901 [6]. В окне запроса логина и пароля вбиваем рутовый логин и пароль.

Вуаля... Открывается сие чудо:



Выставляем необходимые параметры, применяем. Потом в образовательных целях просматриваем конфигурационный файл, чтобы посмотреть на то, как изменения записываются в конфиг.

Поле деятельности довольно широкое... Но дальше проблем возникать не должно. Более обширную информацию о samba можно получить, например, здесь [7].

На что еще стоит обратить пристальное внимание, так это на безопасность. Наведу несколько опций контроля доступа, которые могут пригодится:

- **encrypt passwords** - глобальная опция; принимает значение no или yes. Отвечает за возможность включения или отключения шифрования паролей при пересылке по сети.
- **smb passwd file** - глобальная опция; указывает пуль к файлу, в котором хранится список пользователей и паролей Samba (по умолчанию имеет значение /usr/local/etc/samba/smbpasswd).
- **unix password sync** - глобальная опция; указывает на необходимость синхронизации паролей Samba с системными паролями; принимает значение yes или no.
- **null passwords** - глобальная опция; разрешает вход пользователей с пустым паролем.
- **update encrypted** - глобальная опция; при установке значения в yes, указывает изменять файл с шифрованными паролями, в случае, когда пользователь входит в систему, указывая пароль в явном виде.
- **invalid users** - список пользователей, которым будет отказано в доступе к ресурсу
- **path** - опция, используемая при описании ресурсов; позваоляет задать системную директорию.

- **comment** - комментарий к общедоступному ресурсу.
- **writable** - определяет, доступен ли ресурс на запись.
- **admin users** - список пользователей, которые будут иметь доступ как пользователь root.
- **valid users** - список пользователей, имеющих доступ к ресурсу.
- **read list** - список пользователей, имеющих доступ только на чтение к ресурсу с правами на запись.
- **write list** - список пользователей, имеющих право чтения и записи в ресурсе, доступном только на чтение.
- **browsable** - определяет видимость ресурса для пользователей.
- **guest ok** - определяет, разрешен ли доступ гостевых пользователей.
- **guest only** - если установлено значение в yes, то доступ к ресурсу смогут получить только гостевые пользователи.
- **username map** - позволяет указать файл, в котором хранится список сопоставлений имен груп и пользователей системы FreeBSD с именами и группами Windows (пароли должны совпадать). Пример записи из файла: "root = Admin Administrator"

Ссылки:
[1] http://ru.wikipedia.org/wiki/LDAP
[2] http://ru.wikipedia.org/wiki/Active_Directory
[3] http://admin.dn.ua/index.php/*nix/Ispolzovanie-uchetnyh-zapisey-Domena.html
[4] http://ru.wikipedia.org/wiki/ACL
[5] http://ip_interface_samba-servera:901
[6] http://192.168.0.155:901
[7] http://www.linux.org.ru/books/using-samba/ch01_01.html