Установка и конфигурирование Samba

Здесь описан мой опыт в установке и конфигурировании Samba. Я постарался описать

все процедуры для получения работающих конфигураций. Конечно это не user manual

- скорее информация к размышлению. Дополнительное описание настроек можно найти

в документации, прилагаемой к исходным текстам.

Не претендуя на абсолютную истину, с нетерпением жду замечаний и описания

ошибок, допущенных мной. Буду рад обмениваться опытом по конфигурации Samba.

Почему мне понадобилась Samba

Первый звонок

Примерно 2 года назад я установил машину под Linux для обеспечения

корпоративного выхода в Internet. Сразу встала проблема резервного копирования.

Дело в том, что файл-сервер с установленным стримером работал под управлением

Windows NT. Нужно было выбирать: искать клиент NFS для Windows NT или пытаться

найти другой способ. Тогда же я услышал название Samba.

Пресловутая совместимость продуктов Microsoft

В июне 1998 наша компания купила сетевой принтер HP4000N. Сервером печати был

выбран PDC под WindowsNT3.51sp5. Windows 95 прекрасно работал с этим

принт-сервером, но в сети, как на грех, были две Windows NT 4.0 Workstation.

Может быть по незнанию (не думаю, что все так плохо на самом деле), но в течение

месяца, я безуспешно пытался настроить печать из под Windows NT Workstation

4.0sp3. Система упорно требовала наличия драйверов на принт-сервере. Насильная

установка сетевого принтера вызывала зависание системы. Устав от бесполезной

траты нервов, я настроил принт-сервер (используя Linux Slakware 3.5 и Samba

1.9p18-10). Уже несколько месяцев весь офис (примерно 30 компьютеров) прекрасно

печатает независимо от операционной системы на компьютере пользователя.

SysAdmin едет в отпуск (или мечты, которые БУДУТ реальностью)

Так или иначе, но даже компьютерщик должен иногда отдыхать или просто поболеть.

Прекрасно, если он обладает супер-квалификацией и достаточно суров, чтобы

выдрессировать пользователей. Тогда один раз настроив систему, он может

увольняться.

Но я к таким не отношусь; и хотел бы иметь возможность время от времени

проверять работоспособность системы, находясь вне пределов офиса, и если надо,

вносить исправления. Как это сделать, если на сервере стоит WindowsNT (и не

использовать Remote Access, не удобно звонить на модем из другого города или

страны наример - ведь есть Internet)?

Можно использовать BackOrifice ;-) или воспользоваться Microsoft Unix AddOn

Pack.

Это прекрасное решение наталкивается на финансовые трудности. Очень трудно

убедить начальство потратить ~900$ на upgrade Windows NT3.51 до Windows NT4.0 и

ещеё чуть-чуть на AddOn Pack (не узнавал точно, но думаю не мало), чтобы

АДМИНИСТРАТОР КОМЬЮТЕРНОЙ СЕТИ ПОЕХАЛ В ОТПУСК. При этом нужно учитывать, что в

этот комплект входит демон телнета, пароли по сети передаются plain-text. При

наличии у злоумышленника заинтересованности и snifer все ваши ухищрения по

безопасности будут сведены к нулю.

Стоит ли городить огород, если возможность удаленного управления давно заложена

во все UNIX-подобные системы, а развитие средств криптографии позволяет свободно

распространяемым продуктам (я имею в виду SSH) обеспечить гарантию длительных

затрат времени и машинных ресурсов для расшифровки сетевого трафика? Можно было

использовать Samba, но нельзя преуменьшать удобство Windows NT DOMAIN system

(особенно если рабочие станции в сети сплошной Wintel). И вот появилась Samba

2.0, с ещё не полной, но достаточно мощной поддержкой WINDOWS NT DOMAIN. Всё

идёт к тому, что все серверы в нашей компании постепенно будут переведены на

UNIX-подобные системы. Прошу прощения за столь долгое предисловие.

Что такое Samba

Samba - свободно распространяемое програмное обеспечение (GPL), позволяющее:

а) создавать файл- и принт-серверов (для клиентов поддерживающих одну из

реализаций протокола SMB) на базе открытых систем (OpenVMS, Digital Unix, AIX,

IRIX, HPUX, Solaris, FreeBSD, NetBSD, Linux, и т.д.);

б) поддерживать (не полностью) доменную структуру NT DOMAIN;

1) функции первичного контроллера NT DOMAIN (с некоторыми ограничениями, более

подробно - "NT DOMAIN support" на сайте Samba Team;

2) функции участника NT DOMAIN; (с некоторыми ограничениями, более подробно -

"NT DOMAIN support" на сайте Samba Team;

в) обеспечивать сервисы WINS (клиент и сервер), TIME-server и т.д. ;

Рассматривались две конфигурации:

а) Linux-Samba - Primary DOMAIN Controller с клиентами Windows 9x, Windows NT

4.0;

б) Linux-Samba - участник NT DOMAIN с Primary DOMAIN Controller под Windows NT

Server 3.51 sp5.

Также были рассмотрены случаи применения encrypted и plain-text passwords и

опробована конфигурация с поддержкой квотирования дисков. На данный момент

опробованные конфигурации используются в работе (файл- и принт-серверы).

Мой опыт в установке и настройке пакета ограничен системами на базе Linux

Slakware. Самостоятельно были установлены последние стабильные версии версии

automake, autoconf, make, binutils, egcs. Использовались libc5 стандартной

поставки Linux Slakware. Пакет shadow был пересобран с поддержкой md5crypt.

Системы строились с использованием ядер версий 2.0.35 и 2.2.x. В качестве

системы печати использовался пакет LPRng. Последнюю версию samba- latest.tar.gz

можно получить на сайте Samba Team.

Установка

Можно скопировать с ftp-сервера бинарные файлы, скомпилированные под Вашу

систему или исходные тексты.

При использовании исходных текстов

Конфигурирование и сборка с поддержкой syslog:

hostname:/usr/src# tar -xvzf samba-2.0.4b.tar.gz

hostname:/usr/src# cd samba-2.0.4b/source

hostname:/usr/src/samba-2.0.4b/source# ./configure --prefix=/usr/local/samba

--with-syslog

hostname:/usr/src/samba-2.0.4b/source# make

hostname:/usr/src/samba-2.0.4b/source# make install

Конфигурирование и сборка с поддержкой syslog и quota:

(должен быть установлен пакет quota из раздела ap1)

hostname:/usr/src# tar -xvzf samba-2.0.4b.targz

hostname:/usr/src# cd samba-2.0.4b/source

hostname:/usr/src/samba-2.0.4b/source# ./configure --prefix=/usr/local/samba

--with-syslog --with-quota

host:/usr/src/samba-2.0.4b/source# make

host:/usr/src/samba-2.0.4b/source# make install

Опция

--prefix=/usr/local/samba

задаёт путь установки. Для получения полного списка опций:

host:/usr/src/samba-2.0.4b/source#./configure --help more

После этого копируется файл smb.conf c установками по умолчанию:

host:/usr/src/samba-2.0.4b/source#cp ../examples/smb.conf.default

/usr/local/samba/lib/smb.conf

Далее конфигурируется SWAT (Samba Web-based Administrative Tool):

- в файл /etc/inetd.conf добавляеться строка:

#

swat stream tcp nowait.400 root /usr/local/samba/bin/swat swat

#

- в файл /etc/services добавляеться строка:

#

swat 901/tcp # Samba web-based administrative tool

#

Затем перезапускаетя daemon inetd. При обращении к http://host:901 при помощи

браузера, после введения login & password (root), Вы получаете web-интерфейс

конфигурирования Samba (насколько я знаю - возможна работа с SSL).

Конфигурации

Primary DOMAIN controller.

Сценарий установки создаёт следующую структуру:

host:/usr/local/samba#ls -la

total 6

drwxr-xr-x 8 root root 1024 Jun 16 10:34 .

drwxr-xr-x 26 root root 1024 Jun 8 17:06 ..

drwxr-xr-x 2 root root 1024 Jun 10 09:31 bin

drwxr-xr-x 3 root root 1024 May 10 17:24 lib

drwxr-xr-x 6 root root 1024 May 7 13:26 man

drwxr-xr-x 5 root root 1024 May 12 21:16 swat

drwxr-xr-x 3 root root 1024 May 7 14:27 var

host:/usr/local/samba#cd lib

host:/usr/local/samba/lib#ls -la

total 3

drwxr-xr-x 3 root root 1024 May 10 17:24 .

drwxr-xr-x 8 root root 1024 Jun 16 10:34 ..

drwxr-xr-x 2 root root 1024 May 7 13:26 codepages

-rw-r--r-- 1 root root 971 Jun 8 17:06 smb.conf

Дополнительные дирректории

Нужно создать несколько дирректорий (даны пути по умолчанию, выбор остаётся за

Вами - всё можно описать в smb.conf:

host:/usr/local/samba/lib# mkdir netlogon

host:/usr/local/samba/lib# chown root:root netlogon ; chmod 751 netlogon

host:/usr/local/samba/lib# cd ../ ; mkdir profiles

host:/usr/local/samba# chown root:root profiles ; chmod 751 profiles

host:/usr/local/samba#

При использовании в качестве клиентов Windows NT Workstation или Windows 98,

имеет смысл создавать [profiles] на квотированном разделе диска. Windows 95 (без

дополнительных правок в Registry) сохраняет в [profiles] только user.dat

Также следует обратить внимание, что logon-scripts надо создавать с

использованием Dos- или Windows- редактора текста.

Plaintext Password

Следует определиться с типом security. Хост, сконфигурированный как PDC, несёт

функцию авторизации. Значения ключа [security] могут принимать значения [share],

[user], [server], [domain]. Для каждой из ниже приведённых конфигураций можно

указать различный тип [security].

Ключ [encrypt password] определяет какой механизм авторизации будет включен.

Если ключу [encrypt password] присвоено значение "No", то авторизация

пользователей производится исходя из учётных записей в passwd и shadow. В этом

случае, пароли прередаются по сети PlainText. Windows 95OSR2, Windows 98,

Windows NT требуют изменений в registry:

(не рекомендуется для Windows NT)

Windows 95 OSR2

[HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]

"EnablePlainTextPassword"=dword:00000001

Windows 98

[HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]

"EnablePlainTextPassword"=dword:00000001

Windows NT

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]

"EnablePlainTextPassword"=dword:00000001

Encripted Password

Все дальнейшие конфигурации рассматриваються для значения ключа [encrypted

password] = Yes.

При значении ключа [encript passwords] = Yes , авторизация проходит с

использованием файла smbpasswd. Месторасположение по умолчанию:

/usr/local/samba/private/smbpasswd

По умолчанию инсталяционный скрипт не создаёт private/smbpasswd. Для внесения

учётной записи пользователя в файл smbpasswd, нужно:

1. создать smbpasswd

host:/usr/local/samba#ls -la

total 6

drwxr-xr-x 8 root root 1024 Jun 16 10:34 .

drwxr-xr-x 26 root root 1024 Jun 8 17:06 ..

drwxr-xr-x 2 root root 1024 Jun 10 09:31 bin

drwxr-xr-x 3 root root 1024 May 10 17:24 lib

drwxr-xr-x 6 root root 1024 May 7 13:26 man

drwxr-xr-x 5 root root 1024 May 12 21:16 swat

drwxr-xr-x 3 root root 1024 May 7 14:27 var

host:/usr/local/samba#mkdir private

host:/usr/local/samba#echo > /private/smbpasswd ; cd private

host:/usr/local/samba/private# chown root:root smbpasswd ; chmod 600 smbpasswd ;

cd ../

host:/usr/local/samba/# chown root:root private ; chmod 500 private

2. должна существовать учётная запись Unix:

Нужно отметить, что файлы passwd и shadow должны содержать учётные записи

пользователей. При значении ключа [encrypt password] = Yes , учётные записи

могут иметь вид:

passwd:

...

username:x:1016:100:MYGROUP User,,,:/home/user\_name:/dev/null

...

shadow:

...

username:\*:10666:0:99999:7:::

...

3. использовать smbpasswd для создания учётной записи в

/usr/local/samba/private/smbpasswd

host:~#/usr/local/samba/bin/smbpasswd -a user\_name

Added interface ip=x.x.x.x broadcast=x.x.x.255 netmask=255.255.255.0

New SMB password:

Retype New SMB password:

Addedd user user\_name

Password changed for user user\_name

host:~#

4. активировать учётную запись (по умолчанию выставляется ключ [account

disabled]):

host:~#/usr/local/samba/bin/smbpasswd -e user\_name

Added interface ip=x.x.x.x broadcast=x.x.x.255 netmask=255.255.255.0

User user\_name enabled

host:~#

При начальной установке можно использовать скрипт mksmbpasswd.sh, входящий в

комплект поставки.

host:~#chmod +x /usr/src/samba-2.0.4b/source/script/mksmbpasswd.sh

host:~#cat /etc/passwd /usr/src/samba-2.0.4b/source/script/mksmbpasswd.sh > \

/usr/local/samba/private/smbpasswd

host:~#

Пример рабочей конфигурации Primary Domain Controller (клиенты Windows 9x):

используется тип security = user

# Samba config file created using SWAT

# Global parameters

workgroup = MYGROUP

netbios name = ASERVER

server string = DOMAIN Controller

security = user

encrypt passwords = Yes

passwd program = /usr/bin/passwd

log file = /usr/local/samba/var/log.%U

max log size = 50

nt acl support = Yes

time server = Yes

socket options = SO\_KEEPALIVE SO\_BROADCAST TCP\_NODELAY SO\_RCVBUF=4096

SO\_SNDBUF=4096

load printers = No

character set = KOI8-R

client code page = 866

logon script = %U.bat

logon path = \\%N\Profiles\%U

domain logons = Yes

os level = 33

preferred master = Yes

domain master = Yes

dns proxy = Yes

wins proxy = Yes

wins support = Yes

hosts allow = x.x.x.

[homes]

comment = Home Directories

read only = No

create mask = 0600

browseable = No

[netlogon]

comment = Network Logon Service

path = /usr/local/samba/lib/netlogon

guest ok = No

public = No

locking = No

share modes = No

browseable = Yes

[Profiles]

comment = Users' Profiles

path = /usr/local/samba/profiles

read only = No

browseable = No

[Public]

comment = Public

path = /usr/pub

read only = No

create mask = 0650

Всё! Можно запускать:

host:~#/usr/local/samba/bin/smbd -D -d2

host:~#/usr/local/samba/bin/nmbd -D -d2

host:~#

Проведя соответствующие настройки в Network Neighbrohood (такие как enable NT

Domain logon и т.д), можно попробовать зайти в сеть. Для сохранения настроек

user.dat(для Windows 95) или полного User Profile (для Windows 98) нужно

сделать:

host:~#cd /usr/local/samba/profils

host:/usr/local/samba/profiles#mkdir user\_name

host:/usr/local/samba/profiles#chown -R user\_name:root user\_name ; chmod -R 751

user\_name

host:/usr/local/samba/profiles#

Добавление участников Samba PDC

Если в сети есть клиенты Windows NT, необходимо произвести некоторые изменения в

конфигурации Samba. Также станция с Windows NT, должна быть включена в Samba

DOMAIN, то есть в smbpasswd должна быть внесена учётная запись mashine account.

Прежде всего создаём Unix-учётную запись (вносим пользователя с user\_name =

[netbios\_name включаемой в NT DOMAIN рабочей станции]+[$], что-то типа

nt\_ws\_1$):

host:~#adduser

Login name for new user (8 characters or less) []: netbios\_name$

User id fot netbios\_name [defaults to next available]:

Initial groups for netbios\_name [users]: nobody

netbios\_name$'s home directory [/home/netbios\_name]: /dev/null

netbios\_name$'s shell [/bin/bash]:

netbios\_name$'s account expiry date [MM/DD/YY]:

Ok, I'm about to make a new account. Here's what you entered so far:

New login name: netbios\_name$

New UID: [Next available]

Initial group: nobody

Additional groups: [none]

Home directory: /dev/null

Shell: /bin/false

Expiry date: [no expiratron]

This is it... if you want to bail it out, hit Control-C. Otherwise, press

ENTER to go ahead and make the account.

Making new account...

Changing the user information for netbios\_name

Enter the new value, or press return for the default

Full Name []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Changing password for netbios\_name

Enter the new password (minimum of 8, maximum of 127 characters)

Please use a combination of upper and lower case letters and numbers.

New password: some\_password\_will\_be\_changed\_to-"\*-in\_shadow\_files

Re-enter new password: some\_password\_will\_be\_changed\_to-"\*-in\_shadow\_files

Done...

host:~#

После этого я правил shadow, меняя зашифрованный пароль на "\*".

Следуюший шаг - внесение учётной записи машины в smbpasswd:

host:~# /usr/local/samba/bin/smbpasswd -a -m netbios\_name

Added interface ip=x.x.x.x broadcast=x.x.x.255 netmask=255.255.255.0

Addedd netbios\_name$

Password changed for user netbios\_\_name$

host:~#

Обратите внимание, что имея Unix-учётную запись netbios\_name$, при внесении в

smbpasswd используем netbios\_name.

Пример рабочей конфигурации Primary Domain Controller (клиенты Windows 9x /

Windows NT):

используется тип security = user

# Samba config file created using SWAT

# Global parameters

workgroup = MYGROUP

netbios name = ASERVER

server string = DOMAIN Controller

security = user

encrypt passwords = Yes

passwd program = /usr/bin/passwd

log file = /usr/local/samba/var/log.%U

max log size = 50

nt acl support = Yes

time server = Yes

socket options = SO\_KEEPALIVE SO\_BROADCAST TCP\_NODELAY SO\_RCVBUF=4096

SO\_SNDBUF=4096

load printers = No

character set = KOI8-R

client code page = 866

logon script = %U.bat

logon path = \\%N\Profiles\%U

domain logons = Yes

os level = 33

preferred master = Yes

domain master = Yes

dns proxy = Yes

wins proxy = Yes

wins support = Yes

hosts allow = x.x.x.

[homes]

comment = Home Directories

read only = No

create mask = 0600

browseable = No

[netlogon]

comment = Network Logon Service

path = /usr/local/samba/lib/netlogon

guest ok = No

public = No

share modes = No

locking = No

browseable = Yes

[Profiles]

comment = Users' Profiles

path = /usr/local/samba/profiles

read only = No

browseable = No

[Public]

comment = Public

path = /usr/pub

read only = No

create mask = 0650

Всё! Можно запускать:

host:~#/usr/local/samba/bin/smbd -D -d2

host:~#/usr/local/samba/bin/nmbd -D -d2

host:~#

После этого следует стандартная процедура подключения Windows NT Workstation к

PDC. Перегружаем Windows NT - можно попробовать зайти!

NT DOMAIN members

Сначала модифицируeтся файл smb.conf. Ниже приведены рабочие конфигурации файл-

и принт-сервера (участников NT DOMAIN).

Файл-сервер (пароли шифрованы и проверяются на указанном сервере, выполняющем

роль Primary DOMAIN controller):

используется тип security = domain.

# Samba config file created using SWAT

# Global parameters

workgroup = MYGROUP

netbios name = FSERVER1

server string = File-server 1

security = DOMAIN

encrypt passwords = Yes

password server = ASERVER

username map = /usr/local/samba/lib/username.map

log level = 2

log file = /usr/local/samba/var/log.%U

nt acl support = Yes

name resolve order = host wins bcast lmhosts

keepalive = 30

lpq cache time = 30

socket options = SO\_KEEPALIVE SO\_BROADCAST TCP\_NODELAY SO\_RCVBUF=4096

SO\_SNDBUF=4096

load printers = No

character set = KOI8-R

client code page = 866

os level = 30

lm interval = 10

dns proxy = No

wins server = x.x.x.x

hosts allow = x.x.x.

wide links = No

[Public]

comment = Varios files

path =/pub/

read only = No

create mask = 0744

Print-сервер (пароли шифрованы, и проверяются на указанном сервер, выполняющем

роль Primary DOMAIN controller):

используется тип security = domain

# Samba config file created using SWAT

# Global parameters

[global]

workgroup = MYGROUP

netbios name = PSERVER1

server string = Print server

security = DOMAIN

encrypt passwords = Yes

password server = ASERVER

username map = /usr/local/samba/lib/username.map

log level = 2

syslog = 2

log file = /usr/local/samba/var/log.%U

name resolve order = host wins bcast lmhosts

keepalive = 60

lpq cache time = 5

socket options = SO\_KEEPALIVE SO\_BROADCAST TCP\_NODELAY IPTOS\_THROUGHPUT

SO\_RCVBUF=4096 SO\_SNDBUF=4096

load printers = No

os level = 30

wins server = x.x.x.x

hosts allow = x.x.x.

printing = lprng

wide links = No

[hp6p]

print command = /usr/local/bin/lpr -h -r -P%p %s; rm %s

lpq command = /usr/local/bin/lpq -P%p

lprm command = /usr/local/bin/lprm -P%p %j

comment = hp6p Laser Jet

path = /usr/local/samba/spool/hp6p

print ok = Yes

printer name = hp6p

[hp4000n]

print command = /usr/local/bin/lpr -h -r -P%p %s; rm %s

lpq command = /usr/local/bin/lpq -P%p

lprm command = /usr/local/bin/lprm -P%p %j

comment = hp4000n Laser Jet

path = /usr/local/samba/spool/hp4000n

print ok = Yes

printer name = hp4000n

[tek350e]

print command = /usr/local/bin/lpr -h -r -P%p %s; rm %s

lpq command = /usr/local/bin/lpq-P%p

lprm command = /usr/local/bin/lprm -P%p %j

comment = Tektronix 350 ext

path = /usr/local/samba/spool/tek350e

print ok = Yes

printer name = tek350e

Должна существовать Unix-учётная запись в passwd и shadow.

Нужно отметить, что файлы passwd и shadow должны содержать учётные записи

пользователей NT Domain (можно использовать username.map).

passwd:

...

username:x:1016:300:MYGROUP User,,,:/dev/null:/dev/null

...

shadow:

...

username:\*:10666:0:99999:7:::

...

Добавление Samba-box в DOMAIN

После окончания конфигурации (при незапущенных демонах smbd и nmbd)

производиться добавление Samba-box в NT DOMAIN (используя Server Manager for

DOMAIN, если PDC - Windows NT Server или рассмотренную выше процедуру). Сначала

на PDC добавляем Samba-box. Далее используем smbpasswd:

host:~#/usr/local/samba/bin/smbpasswd -j MYGROUP -r PDC\_netbios\_name

Added interface ip=x.x.x.x broadcast=x.x.x.255 netmask=255.255.255.0

YYYY/MM/DD hh:mm:ss : change\_trust\_account\_password:

Changed password for domain MYGROUP.

Joined domain MYGROUP.

host:~#

Можно запускать!

host:~#/usr/local/samba/bin/smbd -D -d2

host:~#/usr/local/samba/bin/nmbd -D -d2

host:~#