Организация работата на Samba server

written by superflay123(Андон Николов)
благодарности на www.dhstudio.eu

С Ъ Д Ъ Р Ж А Н И Е

и неговите начини за настройка.

2.1 разглеждане на основни параметри и примери за конфигуриране на Самба

2.2 Поддръжка на класическите средства за печат

2.2.1 Примерна конфигурация на Samba за печата и разяснение на настройките

2.2.2 Поддръжка на печат с CUPS

2.2.2.1 Конфигурация за базова поддръжка на CUPS

2.3 Разглеждане изискванията и настройките на Самба като контролер на домейн

2.4 SWAT (Samba Web Administration Tools) – инструмент за администриране на Самба през WEB interface.

2.4.1 Възможности и предимства

2.4.2 Тхенични насоки

2.4.3 Активиране на SWAT за употреба

2.4.4 Обобщение и бърз преглед

2.5 Минимална или средна защита на Самба

2.5.1 Защита на базата на хостове

2.5.2 Защита на базата на потребители

2.5.3 Защита на базата на мрежови интерфейси

2.5.4 Употреба на огнена стена (firewall)

2.5.5 Забрани за споделения ресурс IPC$

Глава 3 - Организация работата на Самба сървър под операционна система GNU/Linux Fedora 8 (примерна конфигурация на Самба сървър като домейн контролер)

Увод

Андрю Триджел разработил първата версия на Samba Unix през 1992 в Австралийския национален университет, правейки мрежови анализи на протоколите използвани от DEC PATHWORKS сървърният софтуер. “nbserver 1.5” бил пуснат през Декември 1993. По-късно Триджел открил, че протокола бил много идентичен с тези използвани от други мрежови сървърни системи, включително и Microsoft’s LAN Manager софтуера. Той решил да се съсредоточи над съвместимостта с Microsoft мрежовия софтуер. Първоначално Самба била наричана smbserver. Името било сменено, заради предупреждението относно търговската марка от компанията “Syntax”, която също продала продукт наречен TotalNet Advanced Server, и също притежавала търговска марка за “SMBserver” Името “Самба” било измислено като се използвала Unix командата “grep” в системния речник, търсейки думи, които съдържат буквите С, М и Б в този ред.

Самба представлява изпълнение на десетки услуги и протоколи, включително и NetBIOS чрез TCP/IP (NBT), SMB, CIFS, DCE/RPC или още по-точно MSRPC, Network Neighborhood протоколите, WINS сървъра още известен като NetBIOS Name Server (NBNS), NT Domain групата протоколи, които включват NT Domain Logons,базата данни Secure Accounts Manager (SAM), услугата Local Security Authority (LSA), NT-style принтиращата услуга (SPOOLSS), NTLM и още по-скорошната услуга Active Directory Logon, която включва модифицирана версия на Kerberos и LDAP. Всички тези услуги и протоколи, често пъти грешно се свързват само със NetBIOS и/или SMB. Освен това, Самба може да вижда и споделя

принтерите. Създадената от самба мрежа, може да бъде споделена от определени Linux/Unix директории(включително и всички съдържани в тях поддиректории) Те се появяват за Microsoft Windows потребителите, като нормални Windows папки, достъпни чрез мрежата. Linux/Unix потребителите могат както да нагласят споделените директории като част от тяхната файлова структура, така и да използват удобството smbclient (libsmb) инсталирано заедно със Самба, за да виждат споделените файлове със интерфейс подобен на стандартната command line FTP програма. Всяка директория може да има различен слой със нивото й на достъп, намиращ се в горната част на нормалния Unix file protections. Например: home директориите биха имали read/write достъп за всички известни потребители, давайки на всеки от тях достъп до техните собствени файлове, но те все пак не биха имали достъп до чуждите файлове, освен ако нямат позволение за това. Трябва да се отбележи, че netlogon share, която по принцип е предлагана като read only share от /etc/samba/netlogon, е logon директория за потребителските logon скриптове. Конфигурацията е постижима след като се редактира един единствен файл (който по принцип е инсталиран като /etc/smb.conf или /etc/samba/smb.conf). Самба може също така да осигури потребителски logon скриптове и осъществяване на group policy, чрез poledit.

ГЛАВА 1. Разучаване състава на Samba. Стартиране и Инсталиране на Samba

1.1 Разучаване състава на Samba

Самба се състой от два или три демона. Демон (daemon) е Linux/Unix приложение което се изпълнява във фонов режим и предоставя различни услуги. Пример за услуга е уеб сървърът Apache чиито демон се нарича httpd. При самба има три демона два от които са задължителни.

Самба сървър се състои от следните демони:

nmbd – Този демон обработва всички заявки за регистриране и преобразуване на имена. Той е основното средство , което се използва за образуване на мрежата. Обработва всички UDP протоколи. Демонът nmbd би трябвало да е първата команда, стартирана при зареждането на Самба.

smbd – Този демон предоставя TCP/IP връзките, свързани с всички услуги за споделяне на файлове и принтери. Освен това извършва локално удостоверяване. Би трябвало да бъде стартиран директно след демона nmbd.

winbindd – Този демон трябва да се стартира ако Самба е член на Windows Domain или ADS domain. Нужен е и когато Самба има доверени взаимоотношения с друг домейн. Домейнът winbindd проверява в smb.conf за наличието на параметрите “idmap uid” и “idmap gid” ако не ги открие winbindd няма да се

стартира.

Когато Samba е пакетирана като част от операционната система, процесът на стартиране обикновено е предоставен по различен начин, за да е интегриран по-добре с операционната система .

Други основни приложения в Samba са:

smbclient – клиент за SMB за UNIX™ машини

smbprint – скрипт за печатане на принтер на SMB машина

smbstatus – показва информация за осъществените SMB връзки

smbmount и ***smbumount*** – монтира и демонтира отдалечените SMB ресурси на локалната файлова система

smb.conf – конфигурационния файл на Samba сървъра

1.2 Стартиране на Samba

При повечето Gnu/Linux дистрибуции стартирането на Samba става по следния начин описан в **примерите 1.1** и **1.1.1,**

Пример: 1.1

```
]# /etc/init.d/smb restart   #рестартира сървъра
]# /etc/init.d/smb stop      #спира сървъра
]# /etc/init.d/smb start     #стартира сървъра
```

Или изпълнението на следната команда

Пример: 1.1.1

]# service smb restart # за рестартиране
]# service smb start # за стартиране на сървъра
]# service smb stop # за спиране на сървъра

а командата от **пример 1.2** дава информация дали Samba server е стартиран и с какъв номер на процеса е стартиран.

Пример: 1.2

]# service smb status
smbd (pid 10007 10005) is running...
]# /etc/init.d/smb status
smbd (pid 10007 10005) is running...

Преди да се пусне Samba трябва да се провери дали редове от **пример: 1.3** съществуват във файла /etc/services и ако не съществуват да се добавят:

Пример: 1.3

netbios-ns 137/tcp nbns
netbios-ns 137/udp nbns
netbios-dgm 138/tcp nbdgm
netbios-dgm 138/udp nbdgm
netbios-ssn 139/tcp nbssn

1.3 Инсталиране на Samba

Повечето дистрибуции на Linux пристигат с вграден Samba софтуер, но при инсталирането на самата ОС може да не е указано да бъде инсталиран. Съществуват много начини за инсталация на Samba и при различните дистрибуции те са различни.

За да се провери дали Samba е инсталирана на даден компютър е нужно да се изпълни следната команда изобразена в **пример: 1.4**

Пример: 1.4

```
]# whereis smbd
smbd: /usr/sbin/smbd /usr/man/man8/smbd.8.gz /usr/share/man/man8/smbd.8.gz
```

Ако изхода е подобен на показания, то Samba пакета е инсталиран. В противен случай ще трябва да се инсталира. Това може да стане както от предоставяните от дистрибуцията пакети, така и от изходен код. В момента на писане на дипломната работа последната версия на Samba е 3.0.28 и може да бъде изтеглена от http://us1.samba.org/samba/ftp/samba-latest.tar.gz

1.3.1 Инсталиране на Samba при дистрибуцията Debian

пример: 1.5 показва примерна инсталация на приложението Samba за дистрибуцията Debian чрез използване на **apt-get (**Apt-**Advanced packaging tool** е мощен инструмент, който се грижи за "благосъстоянието" и правилното инсталиране/деинсталиране и надграждане на всеки софтуерен пакет.) инсталаторът които автоматично изтегля от така наречените хранилища(**repositories -** отдалечен сървър, хранилище на софтуерни пакети на дадена дистрибуция) , добавя зависимости(dependencies) и инсталира даденото приложение за тази GNU/Linux дистрибуция.

пример: 1.5

]# apt-get install samba samba-common samba-doc libcupsys2-gnutls10 libkrb53 winbind smbclient

1.3.2 Инсталиране на Samba при дистрибуцията Fedora

пример: 1.6 е аналогичен на пример: 1.5, но при Fedora инсталаторът се казва **yum (**инструмент за инсталиране/деинсталиране ъпдейт на пакети ъпдейт на операционната система за RPM базирани дистрибуции.)

пример: 1.6

]# yum -y install samba
]# yum -y install samba-client
]# yum -y install system-config-samba

1.3.3 Инсталиране на Samba от Source Code чрез създаване на RPM пакет

За инсталирането на Samba от Source пакет е необходимо първо да се изтегли такъв. Последната версия на Samba може да се намери на официалната страница на производителя където също така се намира и официалната документация на това приложение. http://us1.samba.org

Пример: 1.7 показва инсталацията на Samba чрез създаване на RPM пакет от Source code

#cd /tmp #Влизаме в директорията където ще се тегли Source Code

#wget -c "http://us1.samba.org/samba/ftp/samba-latest.tar.gz" #изтегля пакетът от официалната страница

#tar -zxvf samba-3.0.28.tar.gz #разархивира пакета

 # chown -R root:root samba-3.0.28 # задава root права на директорията
 # cd samba-3.0.28/packaging/RHEL # влиза в директорията от която ще се създава пакетът за инсталиране за съответната дистрибуция в случая е RHEL.След неговото разархивиране се създава папка "samba-3.0.28" в която се намира сървърното приложение и неговите модули. В тази папка се намира Source Code а в под папка packaging се намират модулите за създаване на инсталационни пакети. Инсталационни пакети могат да се създадат за повечето известни GNU/Linux

дистрибуции като Debian, RHEL (Red Hat Enterprise Linux), Mandrake и SuSE.

 # sh makerpms.sh #стартиране на скрипта които създава инсталационните пакети

След безпроблемното изпълнение на скрипта се създават следните пакети:

/usr/src/redhat/RPMS/i386/samba-3.0.28-19990228.i386.rpm

/usr/src/redhat/SRPMS/samba-3.0.28-19990228.src.rpm

 # rpm -Uvh /usr/src/redhat/RPMS/i386/samba-3.0.28*.i386.rpm # инсталиране на пакетите

1.3.4 Инсталиране на Samba от Source code(изходен код) чрез компилиране.

Инсталирането на това приложение от Изходен код, при всички дистрибуции на Linux или при Unix подобните операционни системи става по следния начин описан в пример: 1.8

Пример: 1.8

```
# tar -zxvf sourcefile
# cd tosourcedir.
# cd /docs/textdocs
# vi UNIX_INSTALL.txt
# ./configure
# make
# make install
```

Където командата tar -zxvf sourcefile (sourcefile се замества с пълното наименование на пакета пример: tar -zxvf samba-3.0.28.tar.gz)разархивира пакетът, командата cd tosourcedir влиза в директорията която е създадена след разархивирането на пакета (преди да се започне с изпълнението на компилацията на Самба е желателно да се прочете документацията за инсталиране от

директорията docs/textdocs), а командите ./configure make make install са тези които конфигурират създават и инсталират Самба от изходния код специално конфигуриран за дадената машина.

Глава 2 Конфигуриране на Samba. Разучаване на smb.conf и неговите начини за настройка

2.1 Разглеждане на основни параметри и примери за конфигуриране на Самба

Настройките на Samba в Linux (или други UNIX-системи) се контролира единствено от файла**, smb.conf** който се намира в **/etc** или **/etc/samba**.

Пример**: /etc/smb.conf**, **/etc/samba/smb.conf**

Този файл определя към какви системни ресурси ще се даде достъп за външния свят и какви ограничения ще се определят при използването на тези ресурси.

Всеки раздел на файла започва със заглавие на раздела, такива като **[global], [homes], [printers],** и т.н..

Секцията **[global]** определя някой променливи, които Samba ще използва за определяне на достъпа до всички ресурси.

Раздела **[homes]** позволява на отдалечените потребители да имат достъп до своите (и само до тях) домашни директории на локалната Linux-машина. Така че, ако потребителите на Windows се пробват да се включат към този раздел от своите

Windows-машини, то те ще бъдат включени към своите персонални домашни директории, но за да могат да направят това те трябва да са регистрирани на Linux-машината.

Простия файл smb.conf, който е посочен в пример: 2.1, позволява на отдалечените потребители да имат достъп към техните домашни директории на локалната машина и да пишат във временна директория. За да могат потребителите с Windows да видят тези ресурси машината с Linux трябва да бъде в локалната мрежа. След това потребителите просто включват мрежовите дискове с помоща на Windows File Manager или Windows Explorer.

Пример: 2.1

```
[global]
   ; guest account = nobody #може да се разкометира този ред ако е нужно да се даде достъп на потребителя "гост"
    log file = /var/log/samba-log.%m
    lock directory = /var/lock/samba
    share modes = yes
[homes]
    comment = Home Directories
    browseable = no
    read only = no
    create mode = 0750
[tmp]
    comment = Temporary file space
    path = /tmp
    read only = no
    public = yes
```

Секцията **[global]** съдържа шест реда, първият от които е коментиран. Вторият указва къде ще се пази журналния файла на Samba сървъра, а третия - файла, който заключва Samba от повторно стартиране. Четвъртия ред задава групата в която ще работи сървъра и петия – неговото име. Последният ред задава кратко обяснение на сървъра.

Секцията [global] може да съдържа и още параметри по-важните от които са:

interfaces – задава на кой мрежови интерфейс ще работи Samba сървъра.

пример: 2.2

interfaces = 192.168.0.1/24 127.0.0.1/24

bind interfaces only – ако стойността на този параметър е yes, то заявките идващи от броадкаст адреси различни от тези на интерфейсите описани в interfaces, ще бъдат отказвани. Това, в комбинация с параметъра interfaces повишава сигурността на сървъра.

time server – ако стойността е yes, то nmbd се идентифицира като time сървър на Windows машините.

encrypt passwords – ако стойността е no, се деактивира криптирането на паролите. Трябва да се има в предвид, че Windows 98/NT и по-нови версии на Windows използват криптирани пароли.

socket option – задава специални параметри към сокета на който работи Samba сървъра. Чрез тях се контролира мрежовото ниво от ISO/OSI модела. Параметъра се използва за ускоряване работата на сървъра. Препоръчителни опции са TCP_NODELAY и SO_SNDBUF=8192.

preferred master – ако стойността на параметъра е yes, то Samba сървъра ще стане

master browser - за дадената работна група (workgroup). Това означава, че останалите компютри в групата ще се свързват към него, за да получат информация за другите компютри в групата.

security – задава как клентите да отвръщат на Samba сървъра и е един от най-важните параметри. Възможните стойности са:

user – използва се ако потребителите, които ще се свързват към сървъра имат същите потребителски имена под Windows, както тези под Линукс. Ако някое име не съвпадне, то достъпа му се отказва. Това е стойността по подразбиране.

share – сървъра не изисква валидно потребителско име и парола, за да позволи на клиента да осъществи връзка.

domain – тази стойност на параметъра security трябва да се използва само ако машината е добавена в Windows NT Domain (чрез програмата net идваща с пакета Samba). Освен това тя изисква параметъра encrypt passwords да има стойност yes.

За да може Линукс да свърже потребителя е необходимо той да присъства като валиден потребител и в Линукс машината.

server – в този режим Samba ще се опита да валидира потребителското име и паролата от друг SMB сървър, например NT машина. Ако това пропадне, Samba превключва на security = USER. Изисква се encrypt passwords да има стойност yes, с изключение в случаите когато другата машина не поддържа криптирани пароли.

ADS – в този режим Samba ще работи като член на домейн в ADS (Active Directory Service)област . Този режим изисква инсталиран и конфигуриран Kerberos. Освен това Линукс машината трябва да се добави към ADS областта чрез помощната програма net (man net).

В секцията **[homes]** се описват параметрите на достъп до домашните директории на потребителите. Първият ред указва коментара, който се появява срещу директорията. Вторият ред задава дали дадения споделен ресурс ще се вижда в списъка с достъпни споделени ресурси. Третия ред задава режим на достъп до ресурса, а последния ред – позволенията с които ще се създават файловете.

В секцията **[tmp]** параметъра public показва, че за достъп до този ресурс не се изисква парола, а параметъра path, задава пътя до директорията, която се споделя.

След промяна на файла е добре той да се провери за валидност. Това става с командата testparm. Ако тя не върне грешка, конфигурацията е валидна. За да влезе новата конфигурация в сила трябва да се рестартира сървъра.

Пример: 2.3

```
[Music]
    comment = Music folder
    path = /mnt/storage/Music
    guest only = Yes
    guest ok = Yes
```

В пример: 2.3 параметъра guest ok е синоним на public. Параметъра guest only задава достъпа до споделения ресурс, като в случая никой освен guest потребителите нямат достъп до ресурса. Това е най-основната конфигурация за осигуряване достъп на Windows машини до Линукс чрез SMB протокола.

Освен файлове, чрез Samba може да се споделят и принтери.

Пример: 2.4 примерна конфигурация за споделяне на принтер от Линукс:

```
[global]
    printing = bsd
    load printers = yes
    printcap name = /etc/printcap
    max print jobs = 100
[printers]
    comment = All printers
    printable = yes
    path = /var/spool/samba
    browseable = no
    guest ok = yes
    public = yes
    read only = yes
    writable = no
```

Значението на отделните параметри е следното:

[global]

printing = bsd – казва на Samba да използва BSD стил на принтиране.

В новите дистрибуции се предпочита използването на CUPS.

load printers = yes – при използването на този параметър се избягва

дефинирането на секция за всеки отделен принтер. Споделят се всички принтери описани в /etc/printcap.

max print jobs = 100 – задава максималния брой едновременни задачи.

printcap name = /etc/printcap – задава пътя на файла където са описани достъпните принтери. Ако се използва CUPS този файла трябва да има права за писане.

[printers]

printable = yes – ако този параметър не е със стойност yes, smbd ще откаже да се стартира.

path = /var/spool/samba – трябва да сочи към директория където Samba да съхранява пристигащите файлове. Тази директория трябва да е различна от тази зададена на системата за принтиране на Линукс.

browseable = no

Ако дистрибуцията използва CUPS (Common UNIX Print System), то параметрите printing и printcap name трябва да са със стойности cups. За да може да се използва CUPS, то Samba трябва да е компилирана с такава поддръжка.

За случая на принтиране от Линукс машина на споделен принтер работещ под Windows. Linux платформата трябва да отговаряте на следните условия:

Трябва да има правилни записи във файла /etc/printcap (те трябва да съответстват на локалната структура на директориите за буферна директория и т.н.)

Трябва да има скрипт /usr/bin/smbprint. Той се доставя заедно с изходните кодове на Samba, но не със всички двоични дистрибутиви на Samba (например в пакета на Slackware, smbprint не присъства). В по-новите дистрибутиви на Samba е заменен със smbspool.

2.2 Поддръжка на класическите средства за печат в Samba

Печатът е услуга, която обикновено е жизнено важна за потребителите. Samba може лесно и надеждно да осигури тази услуга за клиентска мрежа, която се състои от работни станции под Windows.

Услугата печат може да се извършва от самостоятелен сървър, от такъв, който е член на домейн и едновременно функционира като файлов сървър, или от специално предназначен сървър за печат. Този сървър може да бъде по-силно или по-слабо защитен в зависимост от изискванията. Конфигурациите могат да бъдат прости или сложни. Съществуващите методи за удостоверяване на потребителите не се различават съществено от тези при предоставяне на услугата файлов сървър. Като цяло, поддръжката на печата в Samba вече може изцяло да замени сървър за печат с Windows 200x, като осигури и редица допълнителни предимства. Клиентите могат да свалят и инсталират драйвери и принтери посредством познатия им механизъм „Point'n'Print". С помощта на logon ckpunmo-ве инсталацията на принтер се извършва много лесно. Администраторите могат да качат драйвери, предназначени за ползване от клиентите чрез познатия съветник “Add Printer Wizard”. Като допълнително улеснение, управлението на драйвери и принтери може да се осъществява от командния ред или чрез скриптове; по този начин се повишава производителността при работа с много принтери, Обновената подсистема за печат, използвана и от Samba (Common UNIX Printing System - CUPS), поддържа специална функция за централно регистриране на заданията на всеки принтер

(регистриране на всяка отделна страница и предоставяне на основни данни за различни видове статистически справки).

За поддръжка на печата Samba винаги използва подсистемата за печат на съответната операционна система тип Linux/UNIX, върху която работи. Samba е „посредник". Тя изтегля предназначените за печат файлове от клиенти с Windows (или с други SMB клиенти) и ги предава на съюинската система за печат за по-нататъшна обработка. Така, че тя трябва да установи връзка с двете страни: клиента с Windows, направил заявката за печат, и програмата за печат под UNIX. Ето защо трябва да направим разграничение между различните клиентски операционни системи, всяка от koumo работи по различен начин, както и между различните подсистеми за печат под UNIX, които имат своите особености, включително и по отношение на достъпа.

Много администратори-новаци си мислят, че Samba извършва някакъв вид обработка при печат. Samba не извършва каквато и да било обработка. Тя по никакъв начин не филтрира данните за печат. Samba получава от своите клиенти поток от данни (задание за печат), които тя спулира в своята локална опашка. Когато Samba получи цялото задание за печат, тя се обръща към съответната команда от локалната UNIX/Linux система и й предава съхранения в опашката файл. Локалните подсистеми за печат имат за задача да обработят правилно заданието за печат и да го предадат на принтера.

Успешното изпълнение на функцията печат от клиент с Windows посредством Samba сървър на принтер под Linux включва 6 (или 7) последователни стъпки:

Windows установява връзка със споделения принтер. Samba удостоверява потребителя. По мрежата Windows изпраща в опашката на Samba копие от файла за печат. Windows прекъсва връзката. Samba поръчва на командата за печат да предаде файла в опашката на локалната подсистема за печат на Linux.

Подсистемата за печат на Linux обработва заданието за печат.

Може да съществува изрично изискване файлът за печат да бъде изтрит от опашката на Samba. Наличието на подобно изискване зависи от това как е конфигурирана опашката на даден принтер.

2.2.1 Примерна конфигурация на Samba за печата и разяснение на настройките

Пример: 2.5 Разширена конфигурация на системата за печат на BSD

```
[global]
    printing = bsd
    load printers = yes
    show add printer wizard = yes
    print cap name = /etc/printcap
    printer admin = ©ntadmin, root
    max print jobs = 100
    Ipq cache time = 20
    use client driver = no
[printers]
    comment = All Printers
    printable = yes
    path = /var/spool/samba
    browseable = no
    guest ok = yes
    public = yes
    read only = yes
    writable = no
[my_printer_name]
    comment = Printer with Restricted Access
    path = /var/spool/samba_my_printer
    printer admin = kurt
    browseable = yes
    printable = yes
    writable = no
    hosts allow = 0.0.0.0
    hosts deny = turbo_xp, 10.160.50.23, 10.160.51.60
    guest ok = no
```

Подробно обяснение на настройките

Раздел [global]

Раздел **[global]** един от четирите специални раздела (заедно с **[homes], [printers]** и **[print$]**...). Разделът **[global]** съдържа всички параметри, които се прилагат за сървъра като цяло. Тук се намират параметрите, които имат единствено глобално значение. Може да има и параметри на ниво услуги, които в конкретния случаи задават настройки по подразбиране за всички останали раздели и споделени ресурси. По този начин можете да се опрости конфигурирането и да се спести постоянното задаване на една и съща стойност. (Обаче има възможност да се отмени глобално зададените настройки и да се посочат други стойности за всеки отделен раздел или споделено устройство).

printing = bsd - Кара Samba да използва подразбиращите се команди, приложими за системата за печат на BSD (позната още kamo RFC 1179 или LPR/LPD). Изобщо, параметърът printing информира Samba относно подсистемата за печат, която тя трябва да очаква. SAMBA поддържа CUPS, LPD, LPRNG, SYSV, HPUX, AIX, QNX и PLP. Всяка от тези системи по подразбиране използва различна команда за печат (и други специфични команди, контролиращи опашката).

Параметърът printing обичайно е параметър на ниво услуги. Тъй като тук е включен в раздел [global], той ще бъде приложим за всички споделени принтери, за които няма никакви други настройки. Samba-3 вече не поддържа SOFTQ-системата за печат.

load printers = yes - Казва на Samba автоматично да сподели всички налични настроени за споделяне принтери. Наличните споделени принтери се откриват чрез търсене във файла printcap. всички споделени принтери стават достъпни в мрежата. Ако се използва този параметър, не се налага поотделно да се посочва всеки споделен принтер. Всеки автоматично споделен принтер дословно ще заимства опциите за конфигурация от раздел [printers].

show add printer wizard = yes - Обичайно възмжността за настройка на параметрите е предоставена по подразбиране (дори и параметърът да не е посочен в smb.conf). По този начин иконата **Add Printer Wizard** ще се появи в папка **Printers** на списъка със споделени устройства на хоста (както се показва в **Network Neighborhood** или от командата **net view**). За да се отмени този конфигурационен параметър, трябва изрично да се зададе стойност **"no"** (не е достатъчно само да се коментира параметъра).

max print jobs = 100 - Задава горна граница от 100 задания за печат, които Samba може да изпълнява по едно и също време. Ако заявката на даден клиент излиза извън това ограничение, Samba ще даде на клиента следното съобщение за грешка: *„no more space available on server",* Стойност нула (която е зададена по подразбиране) означава, че *не* съществуват никакви ограничения.

printcap name =/etc/printcap - Казва на Samba къде да търси списъка с наличните имена на принтери. Ако се използва CUPS,трябва да се провери дали съществува файл printcap. Това се контролира от директивата Print-cap във файла cupsd.conf.

printer admin = @ntadmin - Членовете на групата ntadmin трябва да могат да добавят драйвери и да задават свойства на принтерите **(ntadmin** е само примерно име); Винаги root е по подразбиране администратор на печата. Знакът **@** се поставя

пред имена на групи в **/etc/group**. Администраторът на печата може да прави всичко с принтерите посредством отдалечените администраторски интерфейси, предлагани от MS-RPC. При по-големи инсталации, параметърът printer admin обикновено се задава за всеви отделен споделен ресурс. Това позволява различни групи да администрират всеки отделен споделен принтер.

Ipq client driver = no - Контролира времето за кеширане на резултатите от командата Ipq. По този начин се избягва прекалено честото и използване и се намалява натоварването на интензивно използваните сървъри за печат.

use client driver = no - Ако бъде посочено *yes,* този параметър ще бъде приложим само за клиенти с Windows NT/200x/XP (но не е за Win 95/98/ME). Стойността му по подразбиране е “No” (или False). Нетрябва да бъде прилаган за споделени принтери (със стойност yes или true), които имат валидни драйвери, инсталирани на Samba-сървъра.

Раздел [printers]

Това е вторият специален раздел. Ако раздел с това име се появи в smb.conf, потребителите имат възможност да се свържат към всеки принтер, посочен в printcap файла на Samba-хоста, защото при стартирането си Samba създава споделен ресурс за всяко име на принтер, което открие във файла printcap. Може да се гледа на този раздел като удобна препратка, посредством която може да се споделят всички принтери с минимална конфигурация. Освен това секцията съдържа настройки, които би трябвало да се прилагат по подразбиране за всички принтери. Настройките в рамките на тази секция трябва да бъдат на ниво споделени устройства.

comment = All printers - Коментарът се показва непосредствено до споделения ресурс в случай, че даден клиент поиска от сървъра, чрез Network Neighborhood или чрез командата net view, да покаже списък с наличните споделени ресурси.

printable = yes - Услугата [printers] трябва да бъде посочена като разрешена за печат. Ако се посочи обратното, smbd няма да се зареди при стартиране. Този параметър позволява свързаните клиенти да отварят, пишат и изпращат файлове от опашката (spool files) в предназначената за тази услуга директория, указана с параметъра path. Използвасе от Samba за различаване на споделени принтери от споделени файлове.

path = /var/spool/smba - Трябва да сочи към директория, в която Samba подрежда файловете за печат в опашката. Тази директория трябва да бъде различна от директория със същото предназначение в дадена UNIX/Linux подсистема за печат. Path обикновено сочи към директория със зададен „лепкав" бит, която е достъпна за писане от всички.

browsable = no - Винаги се задава **“no”**, ако printable = yes. Това прави споделения ресурс **[printer]** невидим в списъка с налични споделени ресурси, изведен от командата net view или от Explorer. (Естествено, ще се видят индивидуалните принтери).

guest ok = yes - Ако за този параметър е зададено “yes”, няма да се изисква парола за достъп до услугата печат. Достъпът ще бъде предоставян с правата на акаунт на гост. При повечето системи акаунтът на гост съответства на потребителя „nobody". Този потребител обикновено може да бъде открит във файла passwd на UNIX/linux с празна парола, но без право за влизане в система. (В някои системи акаунтът на гост може да няма право да печата).

public = yes - Синоним на guest ok = yes. Тъй като съществува guest ok = yes в действителност тук няма нужда от него. (ако случайно има две противоположни настройки на един и същи споделен ресурс побеждава онази настройка, на която Samba попадне последно.)

read only = yes - По правило (при други типове споделени ресурси) не позволява на потребителите да създават или променят файлове в директорията на съотбетната услуга. Когато обаче тази услуга е **„printable”,** Винаги е разрешено да се записва в

директорията (ako правата на потребителя позволяват свързване), но само чрез използване на опашката за печат. Нормалните операции за запис не са разрешени. **writable = no** - Синоним на **read only = yes.**

2.2.2 Поддръжка на печат с CUPS

Системата за печат Common UNIX Print System (CUPS) е вече твърде популярна. В по-големите Linux дистрибуции CUPS е подразбиращата се система за печат.

CUPS притежава значителен брой уникални и съществени възможности. Макар, че основните им функции се усвояват твърде лесно, те все пак са нови.

CUPS е повече от система за буфериране на данните за печат. Това е цялостна система за управление на принтер, съвместима с Internet Printing Protocol (IPP). IPP е индустриален и IETF (Internet Engineering Task Force) стандарт за мрежов печат. Много от неговите функции могат да бъдат управлявани дистанционно (или локално) през уеб-браузър (предоставящ платформено независим достъп до CUPS сървъра за печат). Наред с това, CUPS притежава възможност за работа и от традиционния команден ред, както и няколко по-модерни ГПИ-интерфеиси (ГПИ интерфейси, разработени от независими страни, както например изумителния KDE Print на KDE).

CUPS позволява създаването на *„сурови"* принтери (т.е. Такива , за които не се извършва преобразуване на формата на файла за печат) и *„умни"* принтери (т.е., CUPS променя формата на файловете според изискванията за съответния принтер). По този начин възможностите на CUPS се доближават до възможностите на системата за наблюдение на печата на MS Windows.

2.2.2.1 Конфигурация за базова поддръжка на CUPS

За да се печата с CUPS, за най-простата настройка на Samba-3 (или Версия 2.2.x) са необходими само две опции: printing = cups и printcap = cups. CUPS се нуждае от файл printcap. В конфигурационния файл cupsd.conf, обаче, има две свързани директиви, които контролират автоматичното създаване на този файл и неговата поддръжка от CUPS за безпроблемна работа на приложения от независими страни (пример: **Printcap /etc/printcap** и **PrintcapFomat BSD)**. Наследените програми често изискват да съществува файл printcap, съдържащ имена на принтери; в противен случай те отказват да печатат, CUPS задължително трябва да е настроена да генерира и поддържа файла printcap.

Samba има особена връзка с CUPS. Тя може да бъде компилирана с поддръжка на библиотеките на CUPS. По-новите инсталации позволяват това. По подразбиране, свързването с CUPS е компилирано в smbd и в други двоични файлове на Samba. Но, може да се използва CUPS, дори и Samba да не е свързана **с libcups.so -** но има някои различия в поддържаната или изискваната конфигурация.

Когато Samba е компилирана с поддръжката на libcups, printcap = cups използва CUPS API, за да регистрира принтерите, да предаде заданията, за подаване на задания за печат в опашката на сървъра и т.н. В противен случай този параметър се асоциира с командите от System V с допълнителна опция за печат-oraw. Под Linux може да се използва командата ldd, за да се открият подробности (ldd може да липсва в другите OS платформи или пък нейните функции да се изпълняват от друга команда):

Редът libcups.so.2 => /usr/lib/libcups.so.2 (0x00260000) изпълнен от командата **ldd '/usr/sbin/smbd'** (пълната реализация на командата може да се види в приложение 1)

показва, че тази версия на Samba е компилирана с поддръжка на CUPS. Ако случаят е такъв и е зададено printing = cups, тогава всяка ръчно зададена команда за печат в smb.conf се игнорира.

В случай, че по някакъв повод се наложи да се зададът собствени команди за печат, може да се направи това с опцията printing = sysv. При задаването на тази опция ще се лишим от всички преимущества на тясната интеграция между CUPS и Samba. В този случай трябва ръчно да се конфигурират командите от системата за печат (най-важна е командата print; други команди са: lppause, lpre-sume, lpq, lprm, queuepause и queue resume).

Пример: 2.6 Най-проста конфигурация на smb.conf, свързана с печата

```
[global]
    load printers = yes
    printing = cups
    print cap name = cups
[printers]
    comment = All Printers
    path = /var/spool/samba
    browseable = no public = yes
    guest ok = yes
    writable = no
    printable = yes
    printer admin = root, @ntadmins
```

Пример: 2.6 представлява най-проста конфигурация за печат на smb.conf, която позволява базова поддръжка на CUPS.

Базова настройка на CUPS е описана и в пример: 2.7 . Чрез нея могат да бъдат печатани всички графични, текстови, PDF и PostScript файлове, подавани от Windows клиентите. Повечето потребители с Windows не са наясно как да изпратят тези файлове за печат, без да отварят GUI (Graphic User Interface)

приложение. Повечето от клиентите с Windows имат инсталирани локални драйвери за принтери, бутоните за печат на GUI приложението стартират драйвер за принтер, освен това потребителите рядко изпращат файлове от командния ред. За разлика от клиентите с Linux, тези потребители почти не изпращат графични, текстови или PDF файлове директно към опашката.

Пример: 2.7 Предефиниране на глобалните настройки на CUPS за даден принтер.

```
[global]
    printing = cups
    printcap name=cups
    load printers = yes
[printers]
    comment = All Printers
    path = /var/spool/samba
    public = yes
    guest ok = yes
    writable = no
    printable = yes
    printer admin = root, @ntadmins
[special_printer]
    comment = A special printer with his own settings
    path = /var/spool/samba-special
    printing = sysv
    printcap = Ipstat
    print command = echo "NEW: 'date':printfile %f" \ » /tmp/smbprn.log; \
echo " 'date':p-%p s-%s f-%f"» /tmp/smbprn.log; \ echo " 'date': j-%j J-%Jz-%z
c-%c"» /tmp/smbprn.log; rm %f
    public = no
    guest ok = no
    writable = no
    printable = yes
    printer admin = kurt
    hosts deny = 0.0.0.0
    hosts allow = turbo_xp, 10.160.50.23, 10.160.51.
```

2.3 Разглеждане изискванията и настройките на Самба като контролер на домейн

Контролер на домеин е SMB/CIFS сървър, които:

- Се регистрира и се представя като контролер на домеин (чрез NetBIOS бродкаст и чрез някакъв вид регистриране на имена -Mailslot Broadcasts през UDP бродкаст, WINS сървър през UDP уникаст или DNS и Active Directory).

- Предоставя услугата NETLOGON. (Това всъщност са няколко услуги, които работят с няколко протокола. Това са услугата LanMan Logon, услугата Netlogon, услугата Local Security Account и техни вариации).

- Предоставя споделен ресурс, наречен NETLOGON.

Конфигурирането на Samba за постигането на горното не е никак трудно. Всеки контролер на домеин със Samba трябва да предоставя услуга NETLOGON, наричана от Samba „domain logons" (като името на параметър в smb.conf). Освен това, един от сървърите в домеин със Samba-3 трябва да се представя като мастър браузър на домеин (Domain Master Browser). Като резултат, глабният контролер на домейна ще му определи NetBIOS име, което го идентифицира като мастър браузър за съответния домейн или работна група. След това локалните мастър браузъри в същия домейн или работна група в подмрежи, които са изолирани за бродкастите си, изискват пълно копие на списъка за браузване на цялата глобална мрежа. Клиентите се сбързват с локалния си мастър браузър и получават списъка за целия домейн, вместо само за тяхната подмрежа.

Първата стъпка при създаването на работещ Samba PDC контролер е да се разберат необходимите параметри във файла smb.conf. Примерен smb.conf за роля на PDC е описан в пример: 2.8.

Пример: 2.8

```
[global]
    netbios name = BELERIAND
    workgroup = MIDEARTH
    passdb backend = tdbsam
    os level = 33
    preferred master = yes
    domain master = yes
    local master = yes
    security = user
    domain logons = yes
    logon path = 11%N\piofiles\%U
    logon drive = H:
    logon home = \\homeserver\%U\winprofile
    logon script = logon, cmd
[netlogon]
    path = /var/lib/samba/netlogon
    read only = yes
    write list = ntadmin
[profiles]
    path = /var/lib/samba/profiles
    read only = no
    create mask = 0600
    directory mask =0700
```

passdb backend Съдържа цялата информация за всички акаунти на потребители и групите им. Правелните параметри за този ред са smbpasswd, tdbsam и Idupsam.

С ,guest" се създава подразбиращ се акаунт, но той е включен по подразбиране, не е необходимо да се посочва допълнително

Ако е необходимо използването на резервни контролери на домейни (BDC), единственият логичен избор е да се използва **LDAP,** така че бекенда **passdb** да може

да бъде разпространен, файловете **tdbsam** и **smbpasswd** не могат да бъдат разпространявани и следователно не трябва да бъдат използвани.

Domain Control Parameters Параметрите **os level, preferred master, domain master, security, encrypt passwords** и **domain logons** играят централна роля при осигуряването на поддръжка на контролиране на домейн и влизане в мрежа.Параметърът os level трябва да бъде по-голям или равен на 32. Всеки контролер на домейн трябва да бъде мастър браузъра на домейна, трябва да бъде в режим на сигурност на ниво потребител, трябва да поддържа криптирани пароли в стил Microsoft и трябва да предоставя услугата за влизане в системата (domain logons). Криптираните пароли трябва да бъдат разрешени.

Environment Parameters Параметрите logon path, logon home, logon drive и logon script са настройки за поддръжката на среда, които спомагат за улесняване на операциите по влизане на клиентите и за предоставяне на автоматизирани контролни устройства за дейностите за поддръжка на мрежата.

NETLOGON Share Споделеният ресурс NETLOGON играе централна роля при влизането в домейн и членството в домейн. Този споделен ресурс съществува на всички контролери на домейни на Microsoft. Използва се за предоставяне на logon скрипове, за съхраняване на файлове и за групови политики (NTConfig.POL), както и за търсенето на други често използвани инструменти, които са необходими при влизане в домейна. Това е изключително важен споделен ресурс на всеки контролер на домейн.

PROFILE Share Този споделен ресурс се използва за съхраняване на настолни профили на потребителите. Всеки потребител трябва да има директория на кореново ниво в този споделен ресурс. Директорията трябва да бъде разрешена за запис за потребителя и да може да се чете от всички. Samba-3 разполага с VFS модул, **fake_permissions,** които може да бъде инсталиран в този споделен ресурс. Това ще позволи на администратора на Samba да направи директорията с

възможност за четене от всички. Разбира се, тази възможност е полезна само ако профила е бил правилно създаден.

Горните параметри са пълния набор за дефиниране на режима на работа на сървъра. Минимално необходимите са описани в пример: 2.9

Пример: 2.9

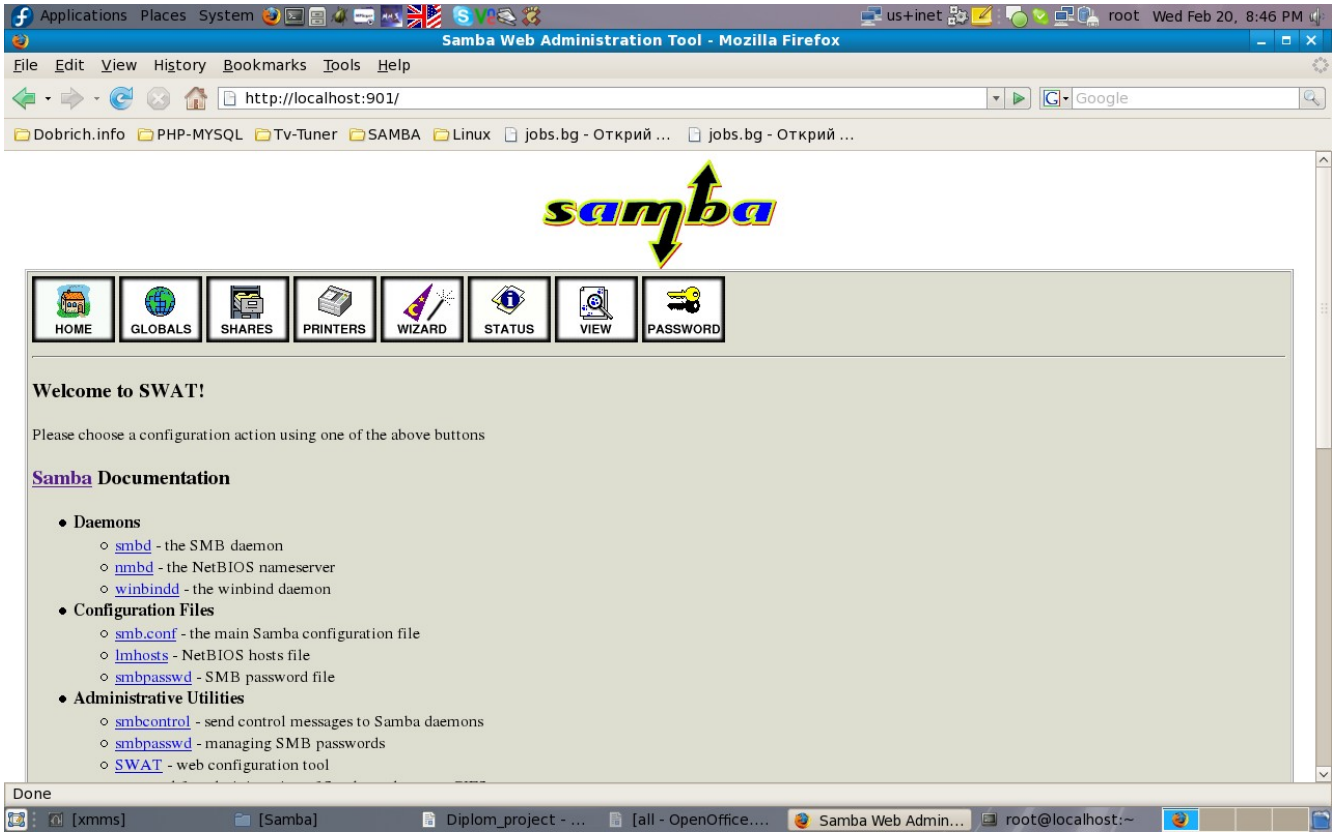
```
netbios name = BELERIAND
  workgroup = M1DEARTH
  domain logons = Yes
  domain master = Yes
  security = User
```

2.4 SWAT (Samba Web Administration Tools) – инструмент за администриране на Самба през WEB interface.

За бързо, по-лесно конфигуриране и администриране на Samba Server съществуват много приложения като например SWAT.

Swat е иснтрумент, даващ възможност за конфигуриране на Samba през WEB интерфейс. Той съдържа съветник (wizard), който може да е от полза за бързо конфигуриране на Samba, предлага индивидуална помощна информация за всеки параметър от smb.conf, представая наблиюдение на текущото състояние на връзките.

Фиг. 2.1



2.4.1 Възможности и предимства

SWAT е инструмент от комплекта SAMBA. Основната част от него е командата swat която се изпълнява от inetd или xinetd. SWAT използва вътрешни компоненти на Samba, за да намери поддържаните от дадена версия на Samba параметри. За Разлика от инструментите, които са външни за Samba, SWAT е винаги актуален. SWAT предоставя отделна помощна информация за всеки конфигурационен параметър директно от man страницата.

Някои мрежови администратори считат, че е добре да се пише системна документация в самите конфигурационни файлове и за тях SWAT винаги ще бъде неприятен инструмент.SWAT не пази конфигурационния файл в никаква междинна форма, а вместо това съхранява само настройките на параметрите. Така когато SWAT запише файла smb.conf на диска, той ще запише само параметрите, които се различават от подразбиращите се настройки. В резултат на това всички коментари, както и всички вече неподдържани параметри ще бъдат загубени от файла smb.conf. Освен това параметрите ще бъдат записани във вътрешна подредба.

2.4.2 Технически насоки

Проверка на инсталацията на SWAT. Някои Linux дистрибуции по подразбиране при инсталирането на Samba не включват SWAT въпреки, че съдържат двойчен пакет с този инструмент.

За да се уверим, че SWAT е инсталиран, е необходимо да проверим дали инсталацията на Samba съдържа изпълнимия файл swat, както и помощните текстови и уеб файлове. Изпълнимите файлове на SWAT могат да се намерят в някои от следните директории

/usr/local/samba/bin - подразбиращото се местоположение на Samba

/usr/sbin - подразбиращото се местоположение при повечето Linux системи

Съществуват редица методи, които могат да се използват за намирането на изпълнимия файл **swat.** Следните методи вероятно са едни от най-ефективните:

Ако **swat** се намира в текущия път за търсене на операционната система, ще бъде много лесно да се намери през испълнението на командата от пример: 2.10.

Пример: 2.10

```
    # whereis swat
swat: /usr/sbin/swat /usr/share/man/man8/swat.8.gz
```

Друг начин за намирането на SWAT е изпълнението на команда “find” показана в пример: 2.11

Пример: 2.11

```
# find / -name swat -print
/etc/xinetd.d/swat
/usr/sbin/swat
/usr/share/samba/swat
```

тази разпечатка показва, че има контролен файл xinetd, инсталиран на този сървър. Местоположението на изпълнимия файл на SWAT е /usr/sbin/swat, а поддържащите файлове за него се намират в директорията /usr/share/samba/swat.

2.4.3 Активиране на SWAT за употреба

SWAT трябва да работи през демона **inetd**. В зависимост от това каква е Linux системата, той ще е **inetd** или **xinetd.**

Естеството и местоположението на inetd са различни за различните реализации на операционната система GNU/Linux. Контролният файл (или файлове) могат да се представят от файла /etc/inetd.conf или да се намират в директорията **/etc/[x]inet[d].d.**

Контролният запис във файла в стария формат ще е подобен на показания в пример: 2.12.

Пример: 2.12

```
#  swat е уеб инструмент за администриране на Samba
swat stream tcp nowait.400 root /usr/sbin/swat swat
```

Контролният файл за новия вид xinetd би изглеждал като показания в пример: 2.13

Пример: 2.13

```
#По подразбиране: изключен
#описание: SWAT е уеб инструмент за администриране на Samba.
#Използвайте го за конфигуриране на Вашия Samba сървър. За \
#целта се свържете към порт 901 с любимия си уеб браузър.

service swat
{
port    = 901
        socket_type      = stream
        wait    = no
        only_from = localhost
        user    = root
        server  = /usr/sbin/swat
        log_on_failure  += USERID
```

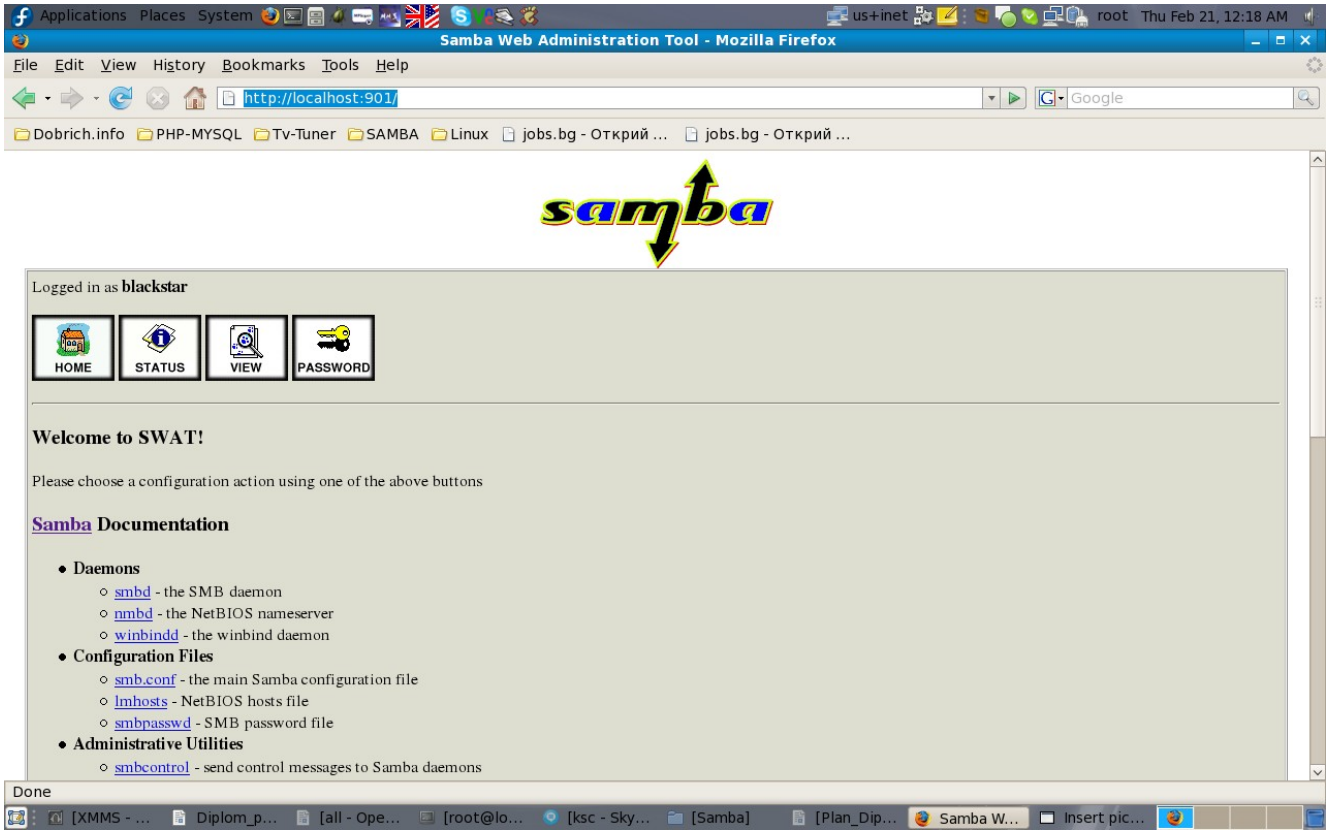
disable = no

В горния пример, подразбиращата се настройка за **“disable”** е **“yes”**. Това означава, че SWAT не е активен. За да се разреши използването на SWAT, трябва да се зададе стойност “no” на този параметър, както е показано.

И двата примера по-горе предполагат, че изпълнимия файл swat се намира в директорията **/usr/sbin**. В допълнение на това, SWAT използва директория, от която зарежда своите помощни файлове, както и друга контролна информация. Подразбиращото й се местоположение при повечето системи с Linux е директорията **/usr/share/samba/swat**. Местоположението при подразбиращите се настройки на Samba е **/usr/local/samba/swat**.

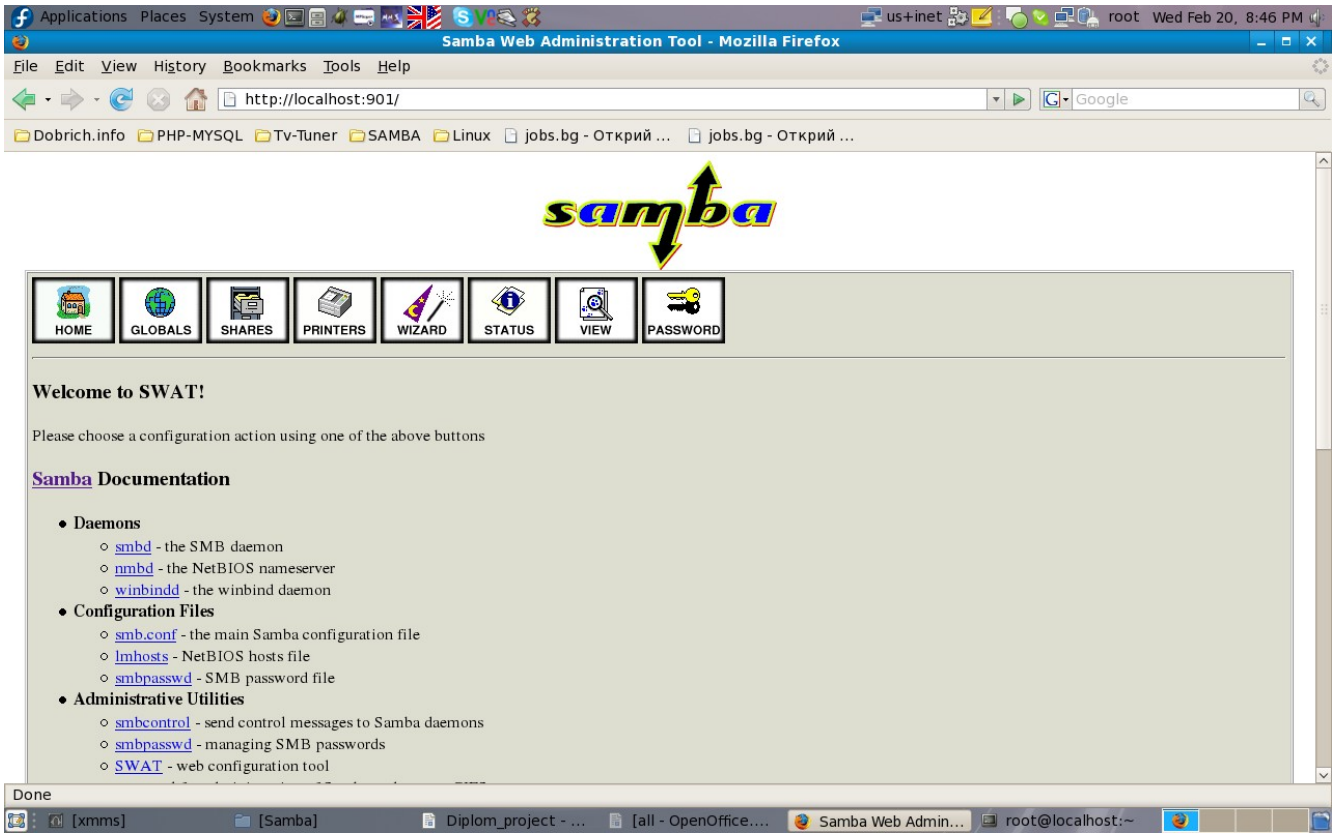
Достъпът до SWAT преминава през процедура за удостоверяване с потребителско име и парола. Ако се влезе в SWAT като какъвто и да е потребител, различен от root, единственото, което ще има възможност да се види, ще са определени части от конфигурацията и инструмента за промяна на паролата. Бутоните, видими за не-root потребителя са**: HOME, STATUS, VIEW, PASSWORD**. В този случай, единствената страница, даваща възможност за някаква промяна е PASSWORD фиг. 2.2.

фиг. 2.2


Applications Places System
us+inet root Thu Feb 21, 12:18 AM
Samba Web Administration Tool - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:901/
Google
Dobrich.info PHP-MYSQL Tv-Tuner SAMBA Linux jobs.bg - Открий ... jobs.bg - Открий ...
samba
Logged in as blackstar
HOME
STATUS
VIEW
PASSWORD
Welcome to SWAT!
Please choose a configuration action using one of the above buttons
Samba Documentation
Daemons
smbd - the SMB daemon
nmbd - the NetBIOS nameserver
winbindd - the winbind daemon
Configuration Files
smb.conf - the main Samba configuration file
lmhosts - NetBIOS hosts file
smbpasswd - SMB password file
Administrative Utilities
smbcontrol - send control messages to Samba daemons
Done
[XMMS - ... Diplom_p... [all - Ope... [root@lo... [ksc - Sky... [Samba] [Plan_Dip... Samba W... Insert pic...

Ако обаче влизането се осъществи като **root,** ще получим пълни права за извършване на промени и запис. В този случай, Видимите бутони ще бъдат; **HOME, GLOBALS, SHARES, PRINTERS, WIZARD, STATUS, VIEW, PASSWORD.** Фиг.2.3

фиг. 2.3



2.4.4 Обобщение и бърз преглед

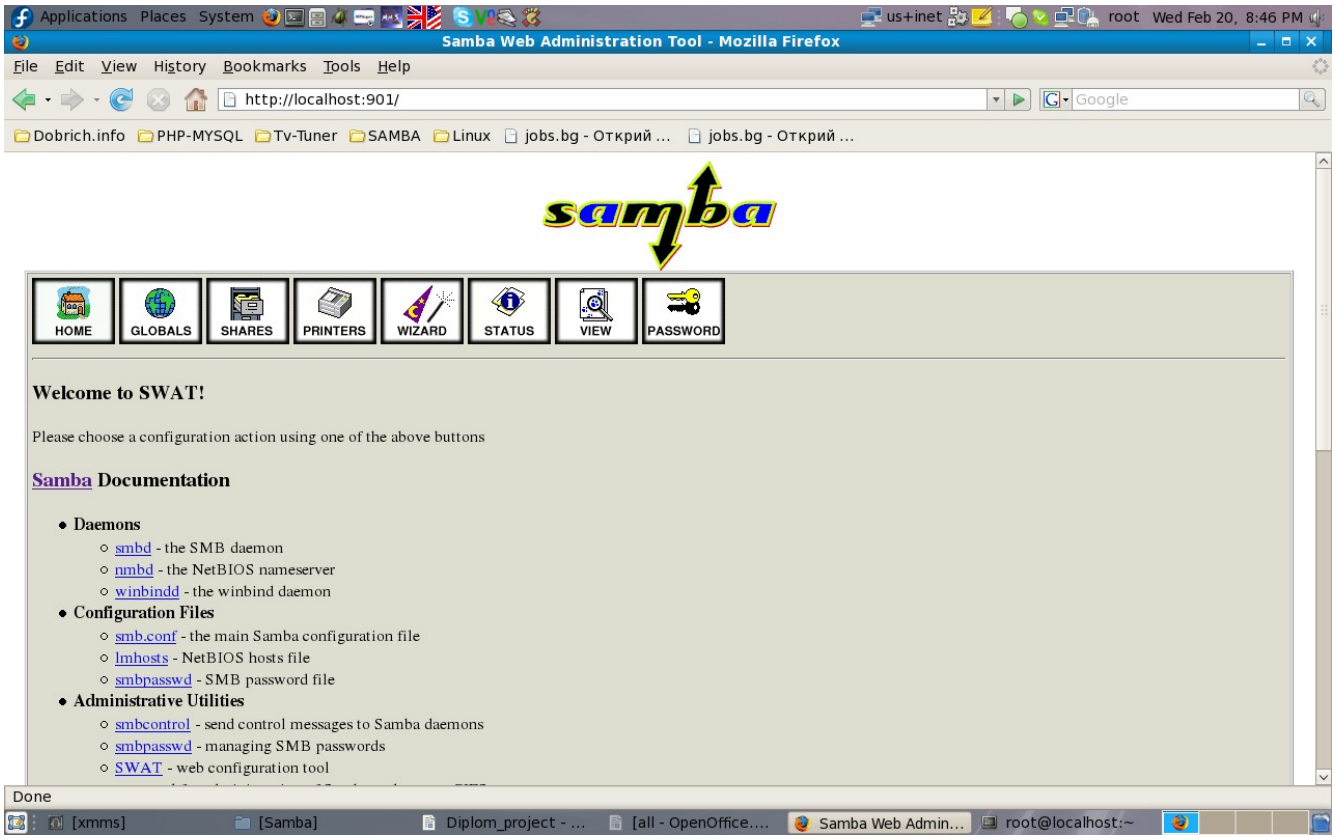
SWAT е инструмент, които може да се използва за конфигуриране на Samba, или просто за научаване на полезни връзки към важни материали за справка.

Началната страница на SWAT (HOME)

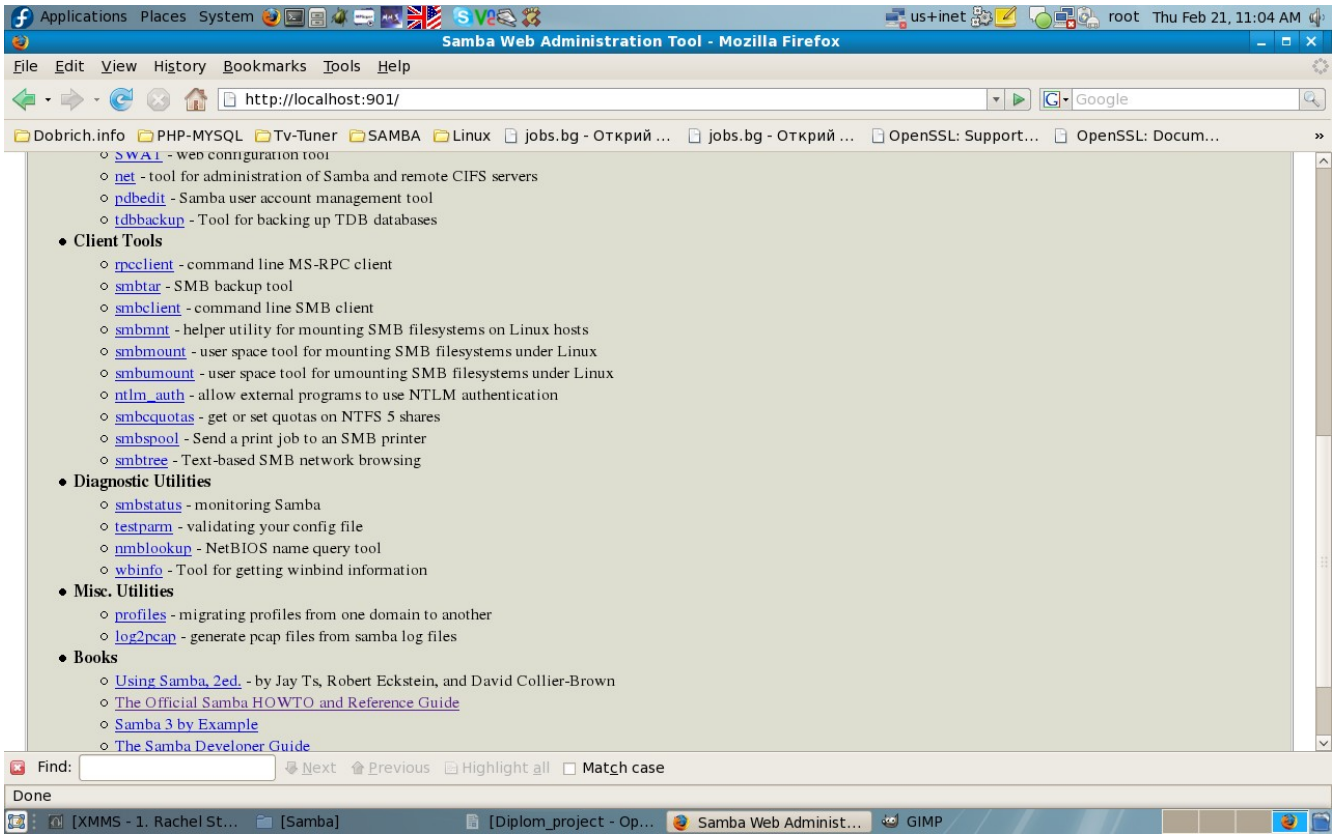
Заглавната страница на SWAT предоставя достъп до най-новата документация на Samba. От нея може да се отвори man (linux manual pages) страница за всеки компонент на Samba, както и колекцията Samba HOWTO и книгата на **O'Reilly „Using Samba"** от секцията **[book]** в края на началната страница

Администраторите, които искат да проверят конфигурацията на своята Samba, могат да научат полезна информация от man страниците на диагностичните инструмент. Тези документи са на разположение и от домашната страница на SWAT. фиг. 2.4 и фиг. 2.5

фиг. 2.4


Applications Places System
us+inet root Wed Feb 20, 8:46 PM
Samba Web Administration Tool - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:901/
Google
Dobrich.info PHP-MYSQL Tv-Tuner SAMBA Linux jobs.bg - Открий ... jobs.bg - Открий ...
samba
HOME
GLOBALS
SHARES
PRINTERS
WIZARD
STATUS
VIEW
PASSWORD
Welcome to SWAT!
Please choose a configuration action using one of the above buttons
Samba Documentation
Daemons
smbd - the SMB daemon
nmbd - the NetBIOS nameserver
winbindd - the winbind daemon
Configuration Files
smb.conf - the main Samba configuration file
lmhosts - NetBIOS hosts file
smbpasswd - SMB password file
Administrative Utilities
smbcontrol - send control messages to Samba daemons
smbpasswd - managing SMB passwords
SWAT - web configuration tool
Done
[xmms] [Samba] Diplom_project - ... [all - OpenOffice.... Samba Web Admin... root@localhost:~

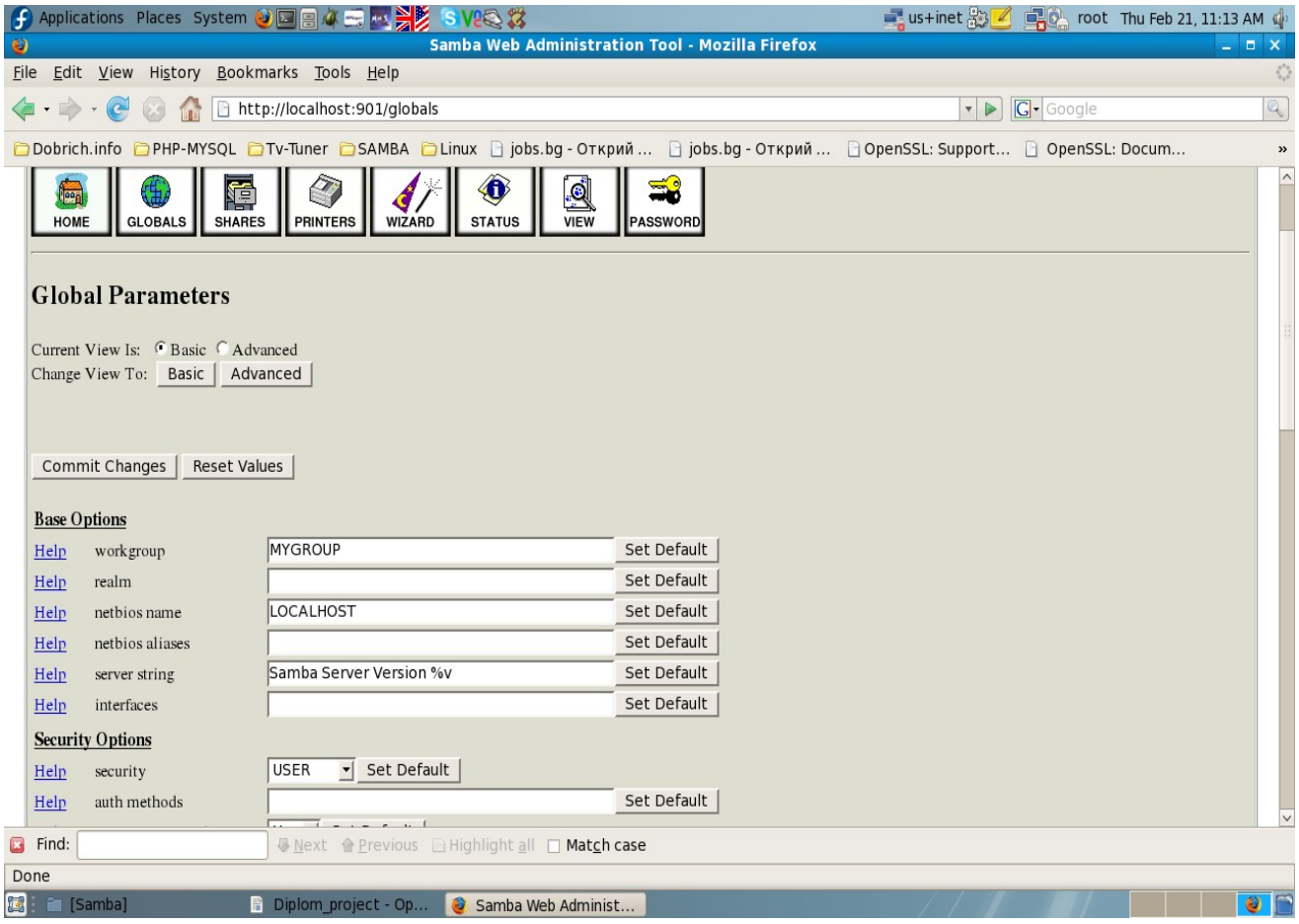
фиг. 2.5


Applications Places System
us+inet root Thu Feb 21, 11:04 AM
Samba Web Administration Tool - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:901/
Google
Dobrich.info PHP-MYSQL Tv-Tuner SAMBA Linux jobs.bg - Открий ... jobs.bg - Открий ... OpenSSL: Support... OpenSSL: Docum...
SWAT - web configuration tool
net - tool for administration of Samba and remote CIFS servers
pdbedit - Samba user account management tool
tdbbackup - Tool for backing up TDB databases
Client Tools
rpcclient - command line MS-RPC client
smbtar - SMB backup tool
smbclient - command line SMB client
smbmnt - helper utility for mounting SMB filesystems on Linux hosts
smbmount - user space tool for mounting SMB filesystems under Linux
smbumount - user space tool for umounting SMB filesystems under Linux
ntlm_auth - allow external programs to use NTLM authentication
smbcquotas - get or set quotas on NTFS 5 shares
smbspool - Send a print job to an SMB printer
smbtree - Text-based SMB network browsing
Diagnostic Utilities
smbstatus - monitoring Samba
testparm - validating your config file
nmblookup - NetBIOS name query tool
wbinfo - Tool for getting winbind information
Misc. Utilities
profiles - migrating profiles from one domain to another
log2pcap - generate pcap files from samba log files
Books
Using Samba, 2ed. - by Jay Ts, Robert Eckstein, and David Collier-Brown
The Official Samba HOWTO and Reference Guide
Samba 3 by Example
The Samba Developer Guide
Find: Next Previous Highlight all Match case
Done
[XMMS - 1. Rachel St... [Samba] [Diplom_project - Op... Samba Web Administ... GIMP

Глобални настройки (GLOBALS)

Бутонът GLOBALS показва страница, даваща възможност за конфигуриране на глобалните параметри в smb.conf. Фиг. 2.6

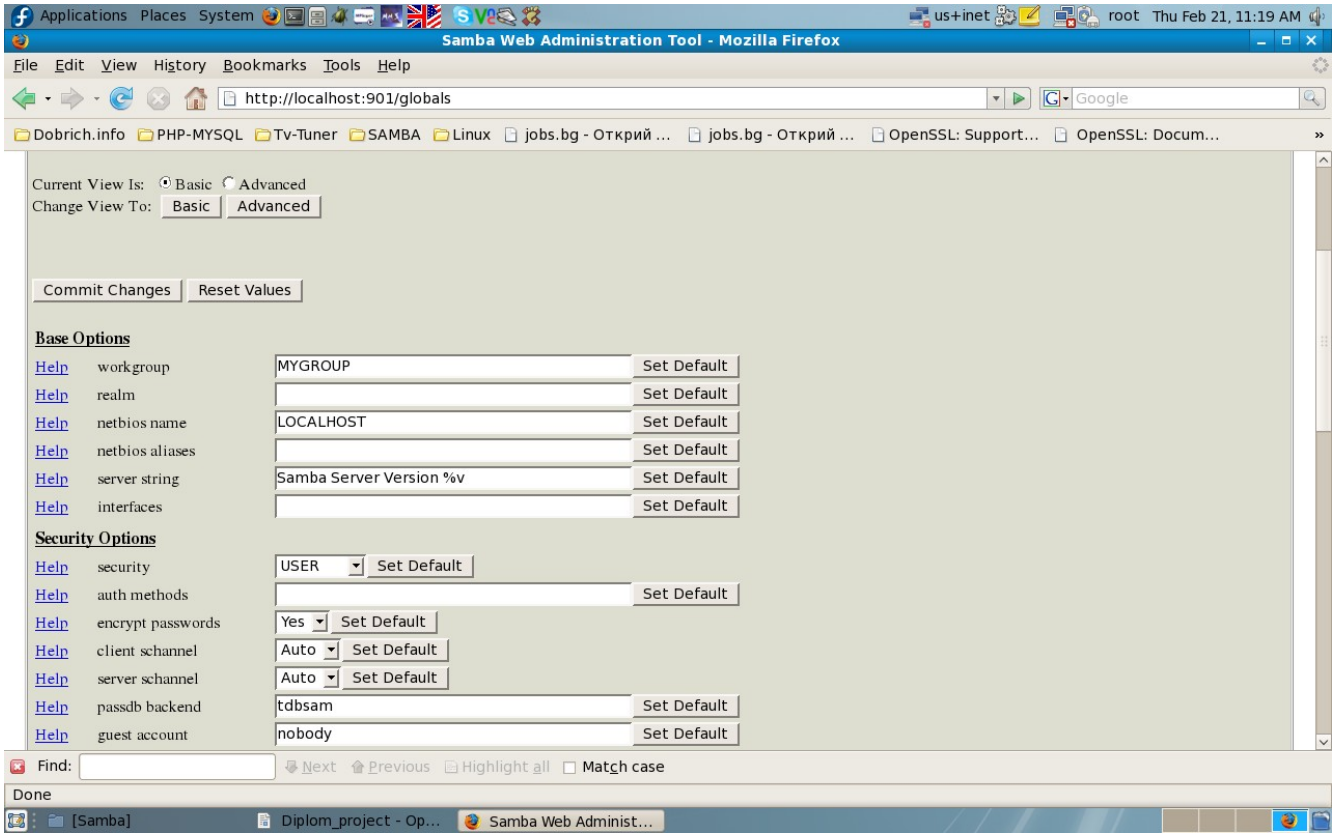
фиг. 2.6



Предлагат се две нива на разкриване на параметрите:

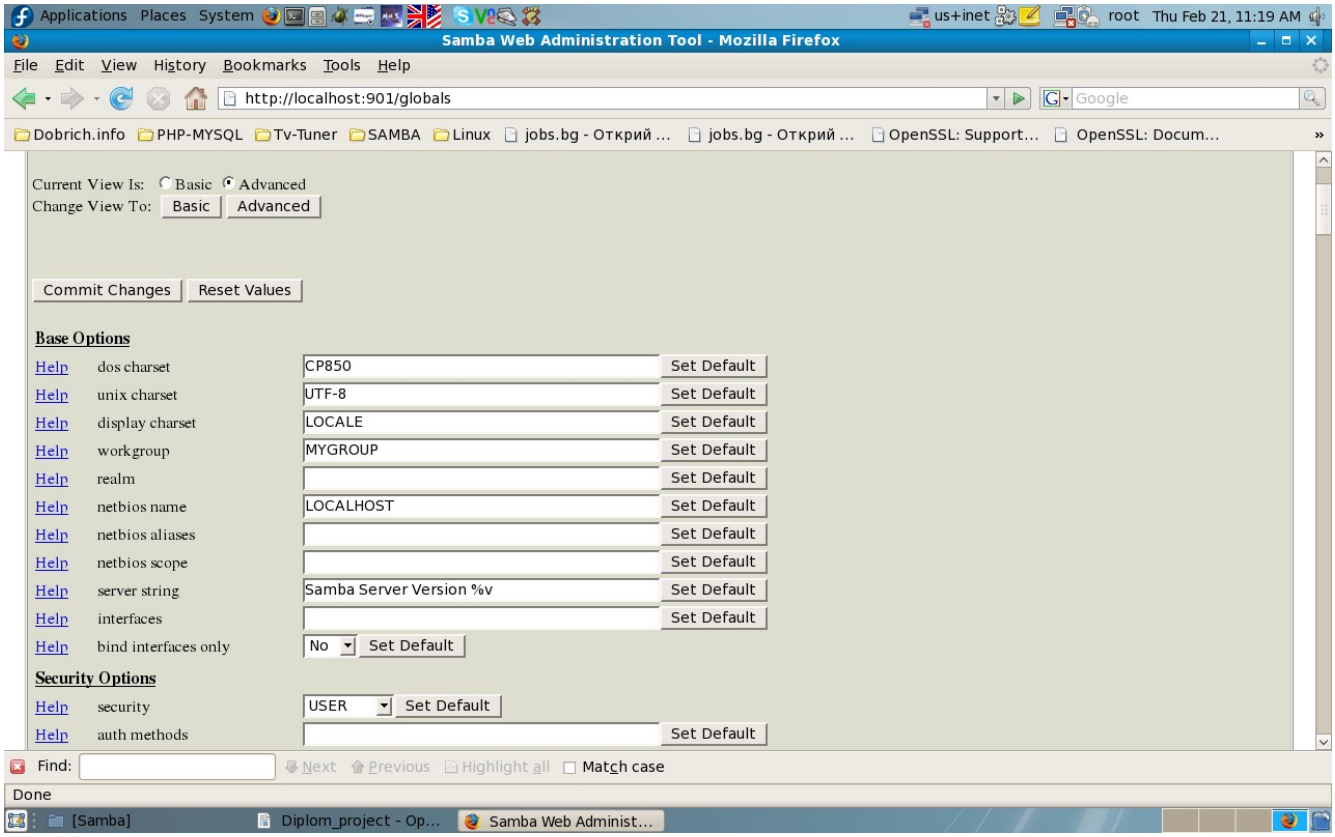
Basic - показват се често използвани конфигурационни опции. фиг. 2.7

фиг. 2.7



Advanced - показват се конфигурационни опции, необходими в по-сложни среди. фиг. 28

фиг. 2.8



За да се превключи в друг режим от **Basic,** трябва да се натисне върху бутона Advanced. Това може да се направи и като се натисне върху радио бутона и след това да се натисне бутона **Commit Changes.**

След като са направени промените по конфигурационните параметри не трябва да се забравя да натиснете бутона **Commit Changes** преди да преминете към друга област**,** за да се запазят. В противен случай направените промени ще бъдат изгубени.SWAT предлага контекстна помощна информация за всеки параметър от бутона Help, който се намира в ляво от съответния конфигурационен параметър.

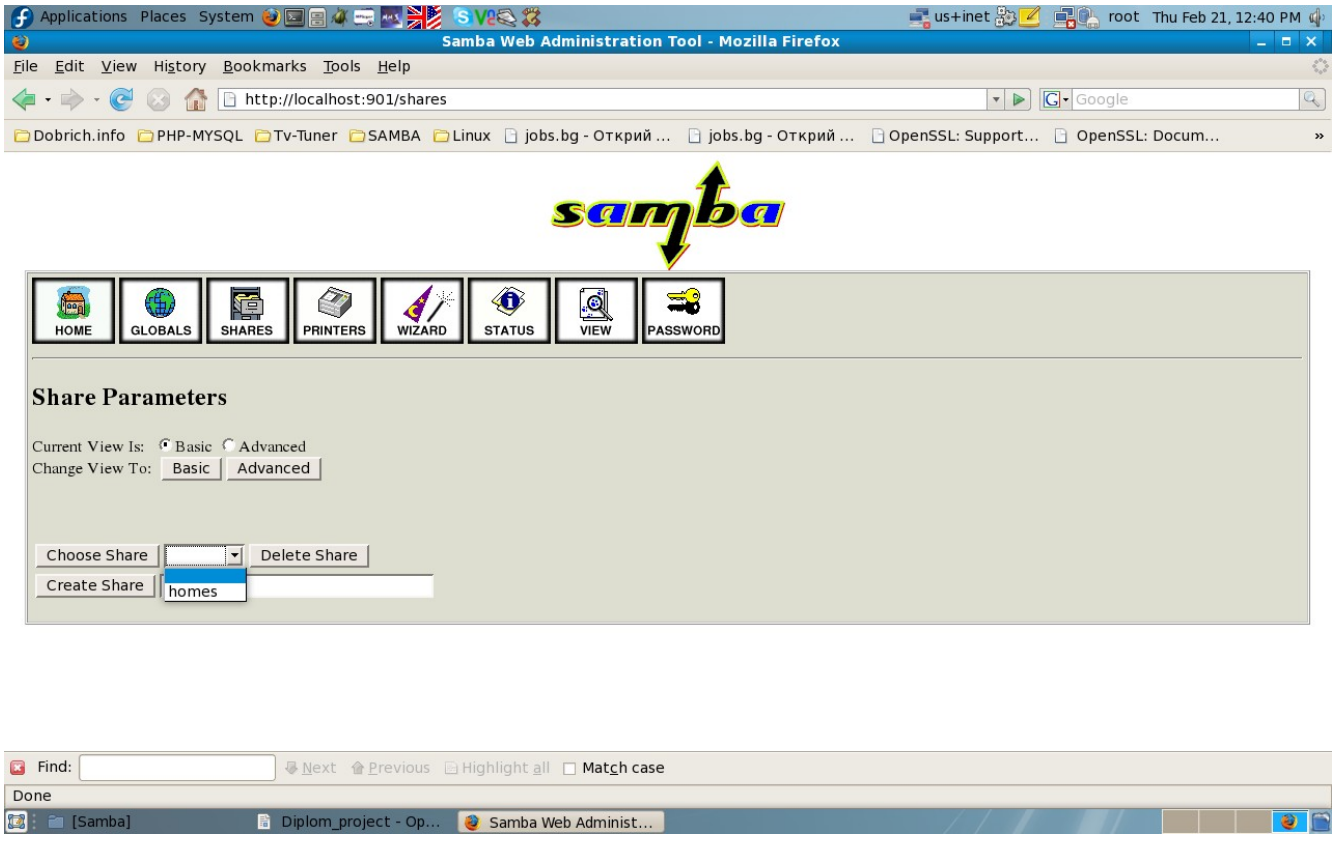
Настройки на споделени ресурси (SHARES)

За да се покажете вече конфигуриран споделен ресурс, просто трябва да се щракне върху падащото меню между бутоните **[Choose Share] u [Delete Share],** да се избере желания ресурс и ako се налагат редакции на настройките му, да се натисне бутона **[Choose Share].** За да изтриване на споделения ресурс, се натиска бутона **Delete Share.**

За създаването на нов споделен ресурс, трябва да се въведе име в текстовото поле, намиращо се до бутона [Create Share], и след това да се натисне самия бутон.

Фиг. 10 показва изглед на секцията (SHARES)

фиг. 2.9

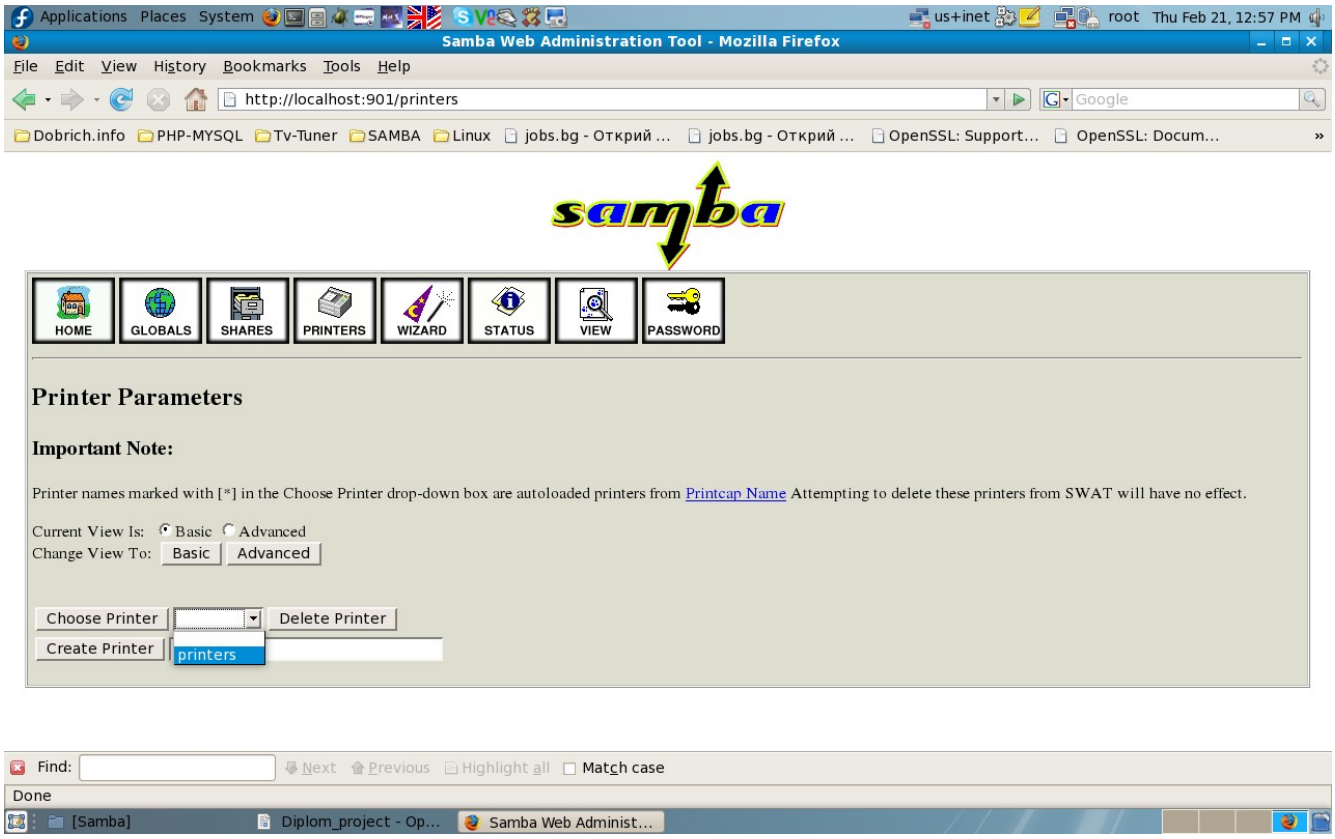


Настройки на принтерите (PRINTERS)

За въвеждане на вече конфигуриран принтер, е необходимо да се щракне върху падащото меню между бутоните [**Choose Printer] и [Delete Printer],** да се избере принтер и ako се налага редakmиране на настройките му,да се натисне бутона [**Choose Printer].** За да се изтрие принтера, трябва да се натисне бутона **[Delete Printer]**.

За да се създаде нов принтер,трябва да се въведе име в текстовото поле, намиращо се до бутона [**Create Printer],** и след това да се натиснете самия бутон. Фиг. 11

фиг. 2.10

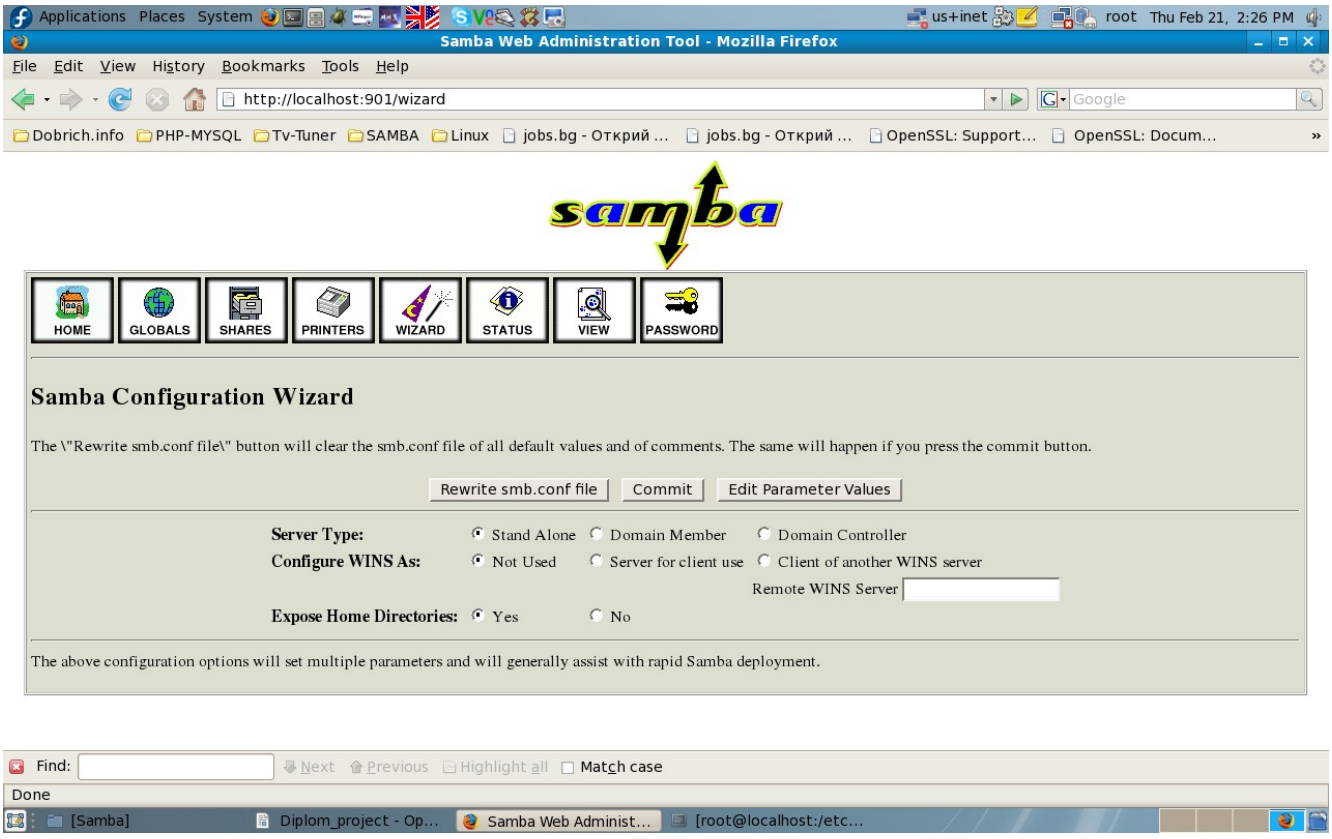


Съветникът на SWAT (WIZARD)

Целта на SWAT Wizard е да помогне на мрежовите администратори с познания по Microsoft мрежи да конфигурират Samba с минимални усилия.

Страницата Wizard предоставя инструмент за пренаписване на файла smb.conf в напълно оптимизиран формат. Същото ще се случи и ако се натисне бутона [**Commit].** Двете възможности се различават по това, че бутонът [**Rewrite]** игнорира всякакви направени промени, докато [**Commit]** ги взима предвид. Фиг. 2.11 показва изгледа на съветника на SWAT.

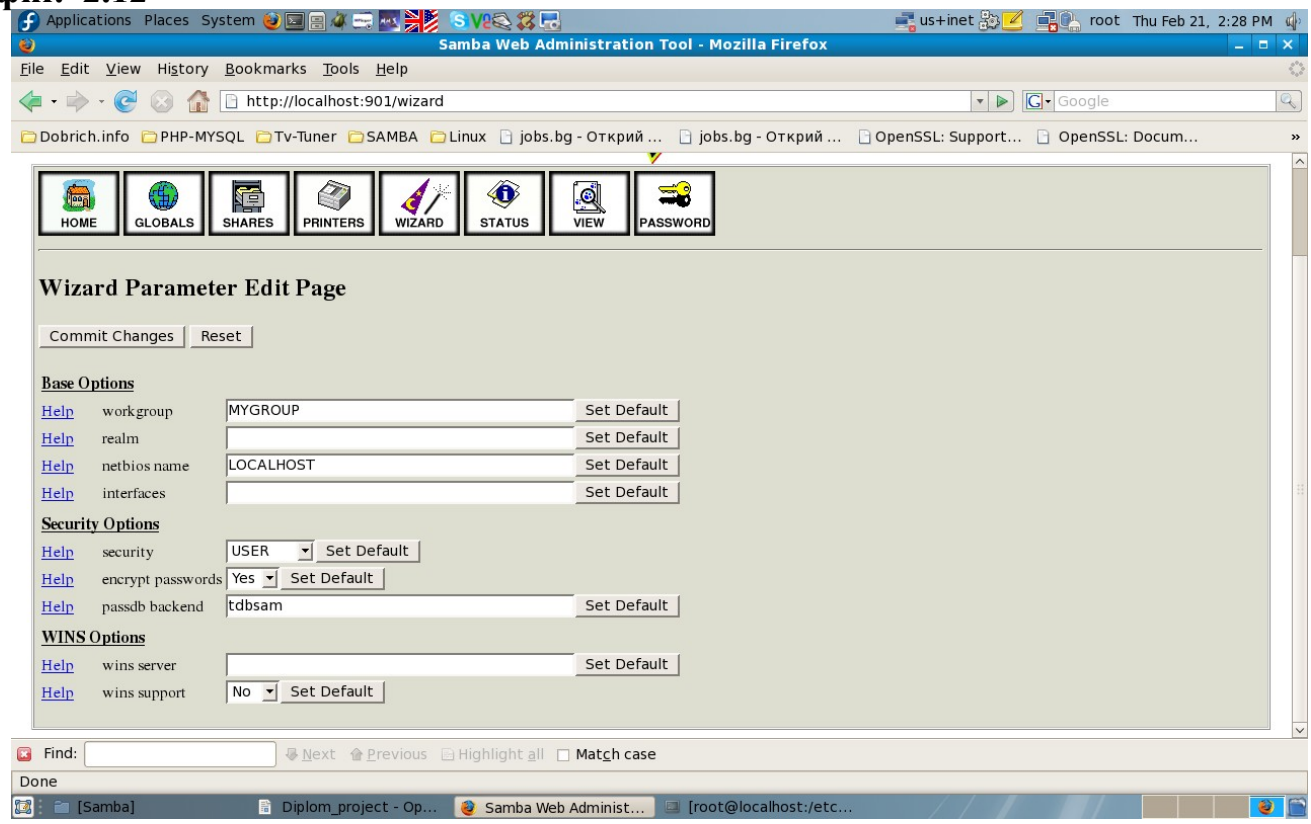
фиг. 2.11



Бутонът **Edit** разрешава редактирането (задаването) на минималния набор от настройки, който са необходими за създаването на работещ Samba сървър.

Фиг. 2.12 показва секцията за реализация на промени от съветника на SWAT.

фиг. 2.12



Накрая, има ограничен набор от опции, определящи какъв вид сървър ще е Samba - дали ще е WINS сървър, дали ще участва като WINS клиент или дали ще работи без поддръжка на WINS. С натискането на един бутон има възможност да се избер дали домашните директории на потребителите да са видими или не.

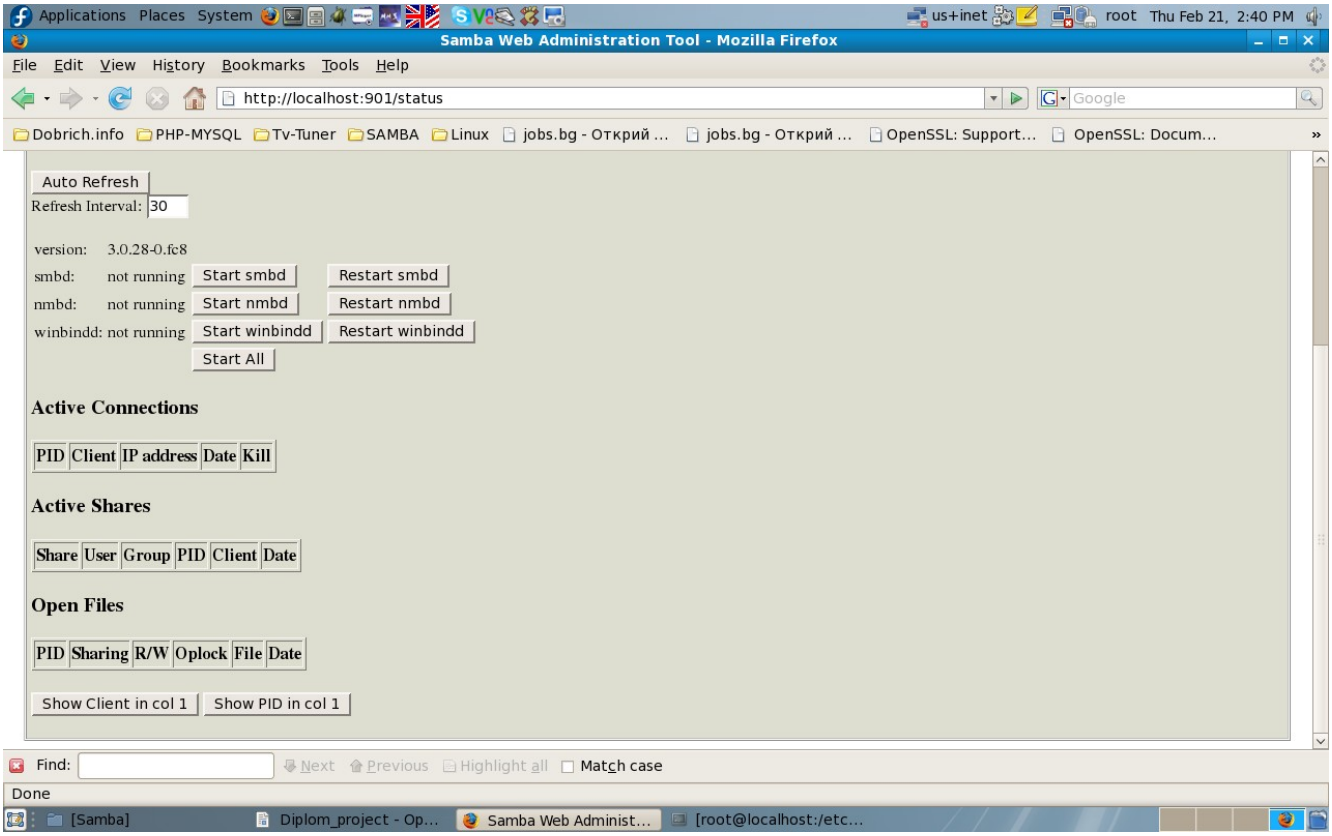
Страницата за състоянието (STATUS)

Страницата за състоянието има ограничена функция. Първо, тя дава възможност за контрол на Samba демоните. Ключовите демони, създаващи средата на Samba сървъра, са: smbd, nmbd, winbindd.

Демоните могат да бъдат контролирани по отделно или като група. Освен това, има възможност да се задава и интервал за автоматично опресняване на екрана. При взаимодействието на клиенти с MS Windows със Samba, ще се получават нови smbd процеси. Инструментът за автоматично опресняване дава Възможност за следене на променящите се условия при минимално усилие.

Накрая, страницата за състоянието може да се използва и за прекъсване на връзките на smbd с даден клиент, за да се освободят файловете, които той евентуално е заключил. Фиг. 2.13 показва екрана на страницата от (STATUS) от SWAT.

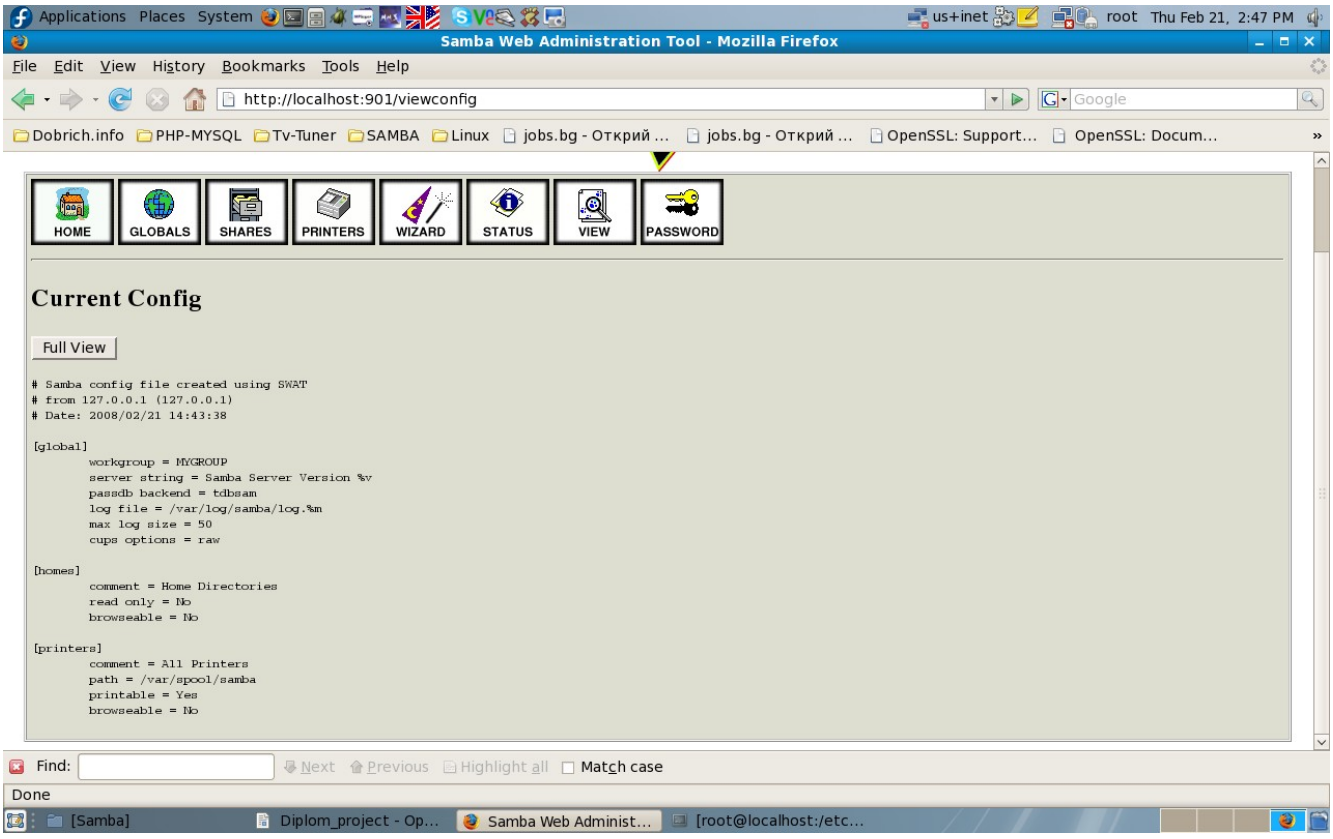
фиг. 2.13


Applications Places System
us+inet root Thu Feb 21, 2:40 PM
Samba Web Administration Tool - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:901/status
Google
Dobrich.info PHP-MYSQL Tv-Tuner SAMBA Linux jobs.bg - Открий ... jobs.bg - Открий ... OpenSSL: Support... OpenSSL: Docum...
Auto Refresh
Refresh Interval: 30
version: 3.0.28-0.fc8
smbd: not running Start smbd Restart smbd
nmbd: not running Start nmbd Restart nmbd
winbindd: not running Start winbindd Restart winbindd
Start All
Active Connections
PID Client IP address Date Kill
Active Shares
Share User Group PID Client Date
Open Files
PID Sharing R/W Oplock File Date
Show Client in col 1 Show PID in col 1
Find: Next Previous Highlight all Match case
Done
[Samba] Diplom_project - Op... Samba Web Administ... [root@localhost:/etc...

Страница (View)

Тази страница дава възможност на администратора да види оптимизирания файл smb.conf и ако е особено мазохистично настроен - да Види всички възможни глобални конфигурационни параметри и техните настройки. На фиг. 2.14 може да се види изгледа на страницата (VIEW)

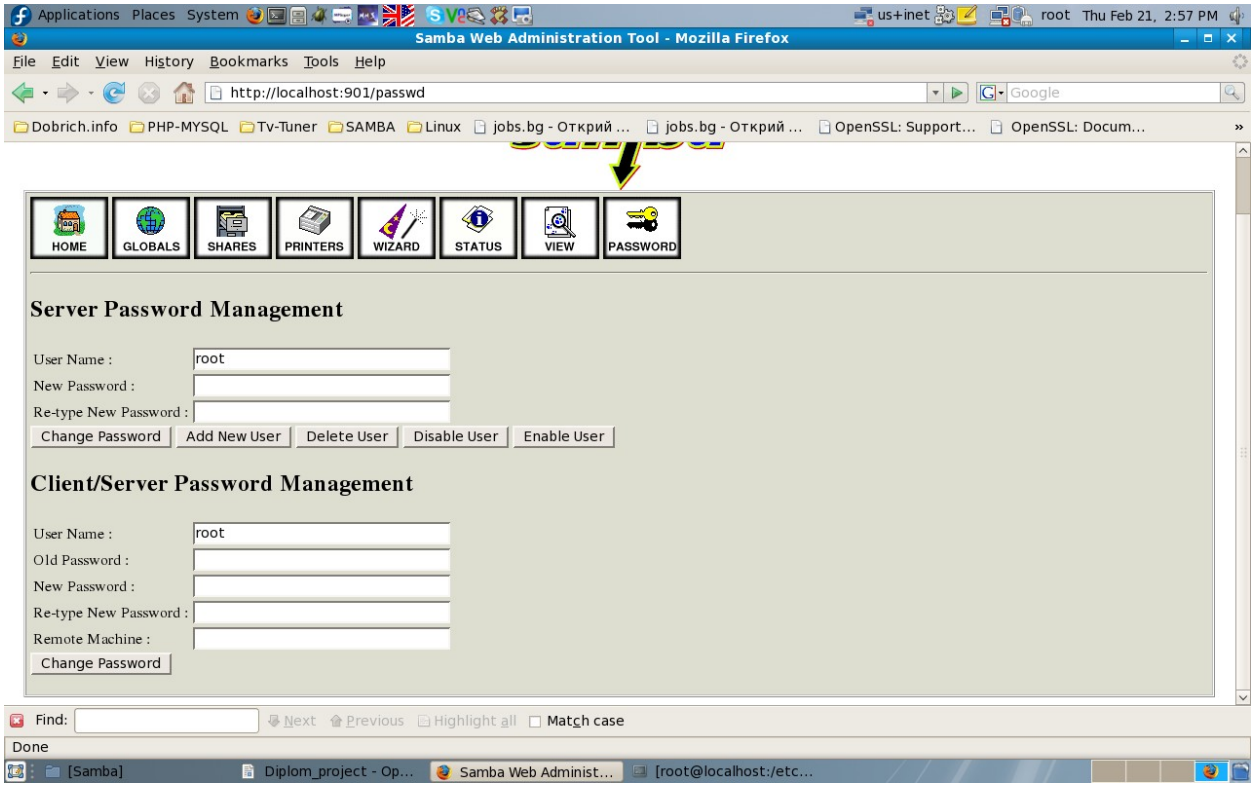
фиг. 2.14



Промяна на паролата (PASSWORD)

Страницата Password Change е популярен инструмент за създаване, изтриване, деактивиране и повторно активиране на акаунтите на потребители на MS Windows мрежи на локалната машина. Освен това, този инструмент може да се използва за промяна на локалната парола на потребителските акаунти. Изгледът на страницата (PASSWORD) може да се вид на фиг. 2.15

фиг. 2.15



2.5 Минимална или средна защита на SAMBA

Основното предизвикателство пред сигурността е фактът, че мерките за защита стигат единствено за затваряне на вратите пред познати експлойти и техники за проникване. Никога не трябва да се допуска, че след като е бил конфигуриран даден сървър вече е непревземаема крепост! Ако се има предвид историята на информационните системи, въпрос само на време е някой да намери поредната уязвимост.

Трябва да се разгледат внимателно три нива принципи, за да се постигне поне средна сигурност. Те са огнената стена(firewall) в периметъра, конфигурацията на хост сървъра на Samba и конфигурацията на самата Samba.

Samba предоставя възможно най-гъвкав подход към мрежовата сигурност. До колкото е възможно, екипът й реализира последните протоколи, за да предостави възможно най-сигурни операции с файлове и принтери на MS Windows.

За да бъде защитена Samba от връзки, постъпващи от външни за локалната мрежа ресурси се постига или **със защита на базата на хостове**, чрез реализираната в Samba технология **„tcpwrappers" ,** или чрез изключения **на базата на интерфейси,** позволявайки на smbd да се обвързва само с конкретно разрешени интерфейси. Възможно е да се заложат и някои изключения за конкретни споделени ресурси, например за автоматично споделен ресурс **[IPC$]**. Той се използва за целите на браузването, както и за изграждане на TCP/IP връзки.

Друг начин за защита на Samba е създаването на записи за контрол на достъпа (Access Control Entries - ACE) в списъците за контрол на достъпа (ACL) за Всички споделени ресурси.

2.5.1 Защита на базата на хостове

В много приложения на Samba най-голямата заплаха идва от източници, които се явяват външни за самата мрежа. По подразбиране Samba приема връзки от всеки хосm, което означава, че ако Samba е с незащитена версия на хост, който е свързан директно с Интернет, сървърът е особено уязвими.

Едно от най-простите решения в този случай е да се използват опциите hosts allow и hosts deny в конфигурационния файл на Samba - smb.conf. Чрез тях може да се разреши достъп до сървъра само на определен набор от хостове. Пример: 2.13 показва как биха изглеждали редовете във конфигурационния файл на SAMBA.

Пример: 2.13

hosts allow = 127.0.0.1 192.168.2.0/24 192.168.3.0/24
hosts deny = 0.0.0.0/0

Горните редове разрешават SMB връзка само от localhost (самият сървър) и от две частни мрежи - 192.168.2 и 192.168.3. Всички останали връзки ще бъдат отхвърлени още при изпращането на първия пакет от клиента. Отказът ще се маркира като грешка „not listening on called name".

2.5.2 Защита на базата на потребители

Ако трябва да се осигури достъп до сървъра само на някой потребители може да се използва методът от пример: 2.14.

Пример: 2.14 В секцията [GLOBAL] да се постави редът:

valid users = @smbusers, jacko

Този ред позволява достъпа до сървъра само на потребители с **име jacko** и членовете на група **smbusers**.

2.5.3 Защита на базата на мрежови интерфейси

По подразбиране Samba приема връзки от всеки мрежов интерфейс на системата. Това означава, че ако сървърът има външна връзка към интернет (пример:ADSL ISDN CableMODEM и др.) Samba ще приема връзки от тях. А това не винаги е желателно.

Поведението на Samba може да бъде променено по начинът описан в пример: 2.15

Пример: 2.15 (промените се извършват в секцията [GLOBAL] на smb.conf)

interfaces = eth* lo
bind interfaces only = yes

Тези редове указват на Samba да слуша само за връзки от интерфейси, чиито имена

започват с eth, например eth0, ethl, както и от loopback интерфейса lo. Името, което трябва да се използва, зависи от това през кой интерфейс минава вътрешната мрежа. В горния пример е използвано общото име за Ethernet адаптери в Linux.

Ако при наличието на горната опция някои ако се опита да изгради SMB връзка към хоста от PPP интерфейса ppp0 (или ако опцията е с “eth1 да се опита да изгрази SMB връзка от ppp0, eth0), ще получи отказ за TCP връзка. В този случай не се изпълнява никакъв код от Samba, тъй като на самата система е посочено да не пропуска връзки от този интерфейс към процесите на Samba.

2.5.4 Употреба на огнена стена (firewall)

Много администратори използват огнена стена (firewall) за ограничаване на достъпа до услуги, които не трябва да бъдат видими извън мрежата. Това не е лош метод, въпреки, че е препоръчително да се използва заедно с горните методи. Така Samba сървърът ще бъде защитен, дори и ако огнената стена не е активна поради някаква причина или бъде преудоляна.

Ако се настройва firewall, трябва да се знаят TCP u UDP портовете, които са желани да се блокират или разрешът. Samba използва следните:

UDP/137 - използва се от nmbd
UDP/138 - използва се от nmbd
TCP/139 - използва се от smbd
TCP/445 - използва се от smbd

Примерен firewall е описан в приложение 2

2.5.5 Забрани за споделения ресурс IPC$

Ако никой от горните методи не е подходящ, може да се наложи да се добави по-конкретна забрана за споделения ресурс IPC$, който се използва в една наскоро открита дупка в сигурността. Забраната позволява да се предоставя достъп до други споделени ресурси, забранявайки в същото време достъпа до IPC$ от потенциално недоверени хостове. За целта може да се използва начинът описан в пример: 2.16

Пример: 2.16

[IPC$]
hosts allow = 192.168.115.0/24 127.0.0.1
hosts deny = 0.0.0.0/0

Тези редове казват на Samba, че връзките към IPC$ са забранени от всички места, с изключение на двата посочени мрежови адреса (localhost и подмрежата 192.168.115). Връзките към други споделени ресурси остават разрешени. Тъй като споделеният ресурс IPC$ е единствения, до който винаги има достъп чрез анонимни връзки, горните редове предоставят определено ниво на защита срещу хакери, които не знаят валидно потребителско име и парола за определения хост.

Ако се използва този метод, клиентите ще получават отговор „достъпът забранен", винаги когато се опитват да се свържат със споделения ресурс IPC$. Тези клиенти няма да могат да браузват за споделени ресурси, освен това има известна възможност да нямат достъп до някои други ресурси. Затова този метод за защита не е препоръчителен, освен ако няма възможност да се използва някой от по-горе изброените.

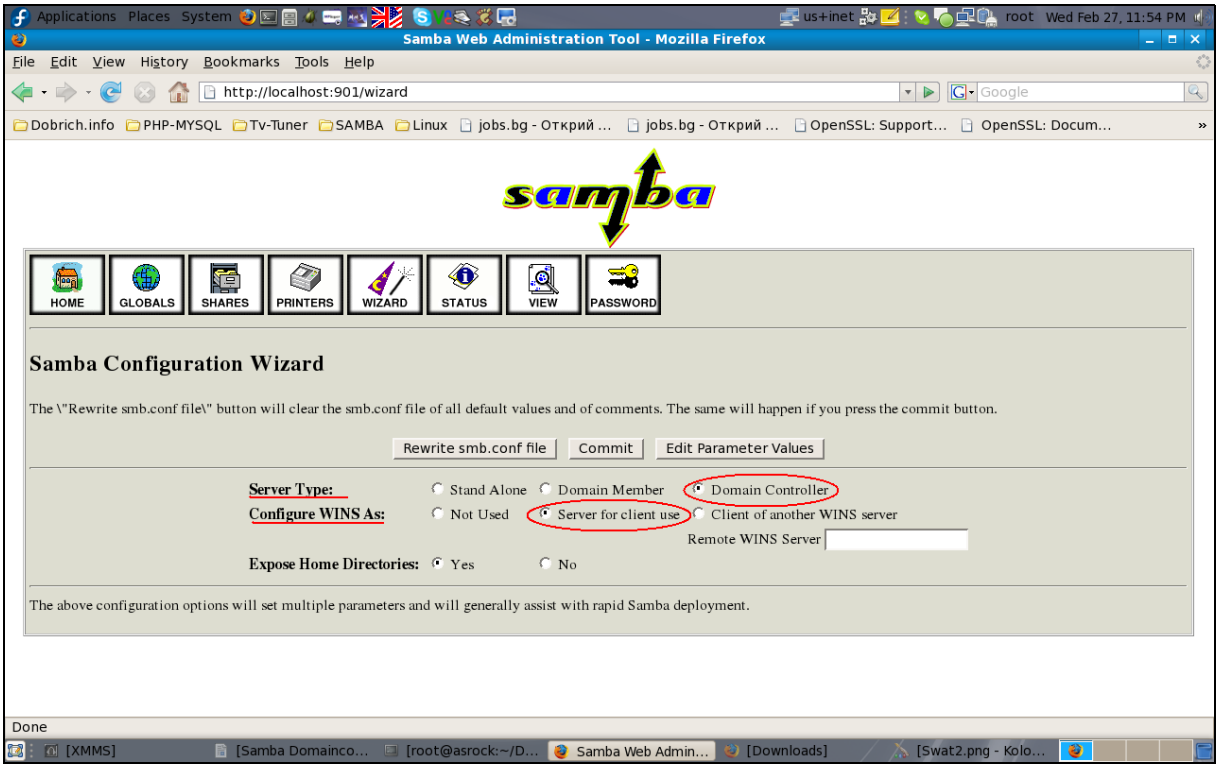
Глава 3 - Организация работата на Самба сървър под операционна система GNU/Linux Fedora 8 (примерна конфигурация на Самба сървър като домейн контролер)

Когато е необходимо централизирано управление на група от компютри трябва да се създаде Primary Domain Controller (PDC). Конфигурацията на Samba server като PDC се осъществява изключително лесно и бързо през приложението SWAT (Samba Web Administration Tool). Организация работата на Samba server под GNU/Linux дистрибуция Fedora 8, се изпълнява в няколко стъпки, които описват подробно реализирането на промените и последователността в която се осъществават.

В първата стъпка след като е установена връзка със SWAT през Web Browser е необходимо да се направят промени в настройките в секцията Wizard. Като в тази секция актуалните опции са:

Server Type = Domain Controller
Configure WINS As = Server for client use

Фиг. 3.1 (изобразява страницата Wizard на SWAT и текущите настройки)

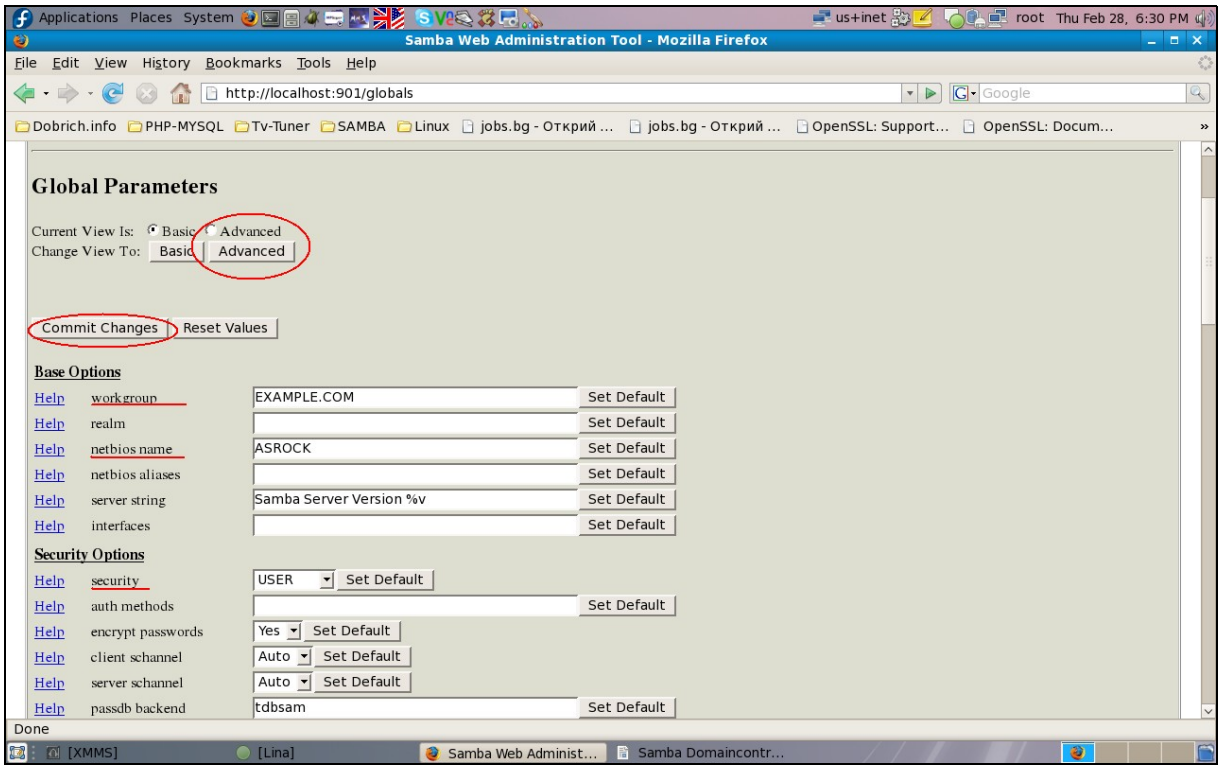


След въвеждането на тези промени те трябва да се запазят с бутона **[Commit]**

Във втората стъпка промените се осъществяват в секцията "Global". Необходимо е да се попълнят следните параграфи с параметрите показани в пример: 3.1

Пример: 3.1
workgroup = EXAMPLE.COM
netbios name = ASROCK
username map = /etc/samba/smbusers
preferred master = yes
printcap name = CUPS
logon drive = H:
logon script = scripts/logon.bat
logon path = \\server1\profiles\%U (If there is no DNS available in your network you have to replace server1 with the IP that belongs to the Samba server)
logon home = \\server1\%U (If there is no DNS available in your network you have to replace server1 with the IP that belongs to the Samba server)
add user script = /usr/sbin/useradd -m '%u' -g users -G users
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usernod -G %g %u
add machine script = /usr/sbin/useradd -s /bin/false/ -d /var/lib/nobody %u
idmap uid = 15000-20000
idmap gid = 15000-20000
template shell = /bin/bash
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\sUNIX\spassword:* %n\n
***Retype\snew\sUNIX\spassword:* %n\n *password\supdated\ssuccessfully* .**
passwd chat debug = yes
unix password sync = yes
log level = 3
os level = 200
profile acls = yes

Фиг. 3.2 (направените промени се запазват с бутона "Commit Changes")



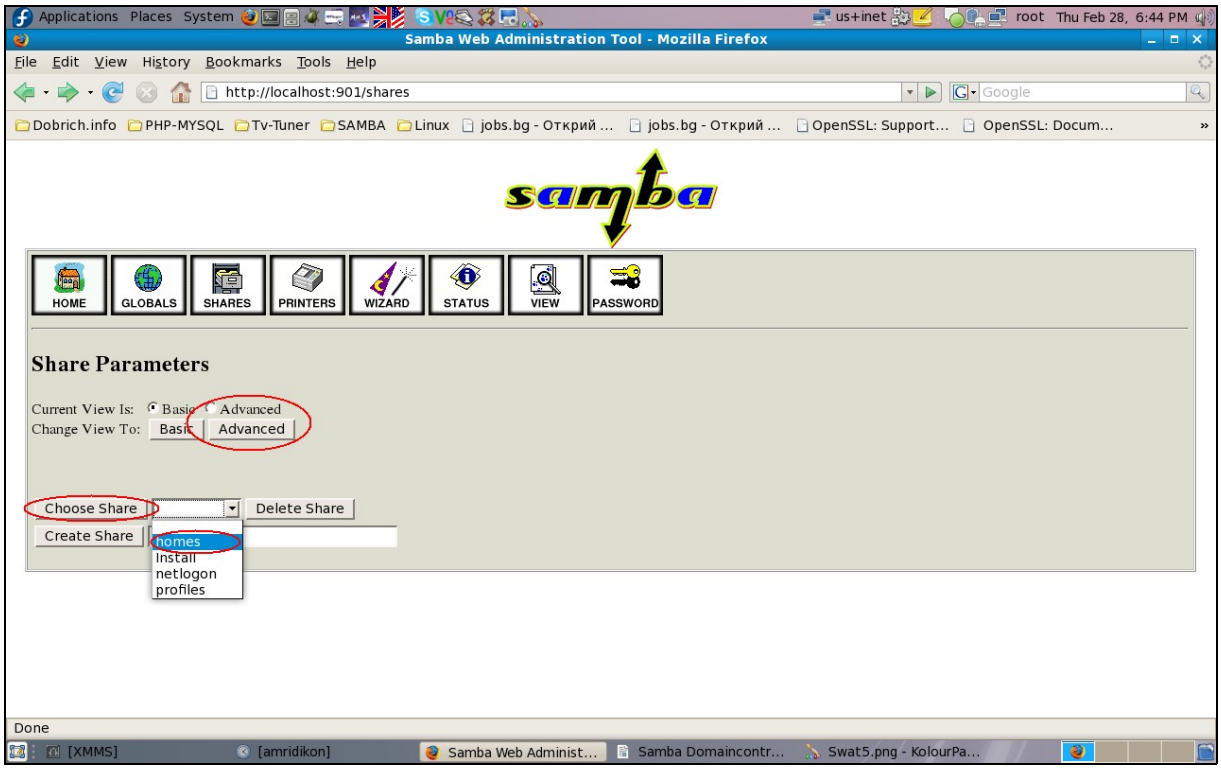
В стъпка три се разглежда и описва как се създават и споделят директориите за потрбителите членове на домейна, а именно пример: 3.3 и фиг. 3.3 показват самите действия които трябва да се извършат.

Пример: 3.3 (Създаване на директории през команден ред и техните превилегии)

```
# mkdir -p /home/samba/netlogon
# mkdir /home/samba/profiles
# chmod 777 /var/spool/samba/
# chown -R root:users /home/samba/
# chmod 777 /home/samba/
# chmod 755 /home/samba/netlogon/
# chmod 770 /home/samba/profiles/
```

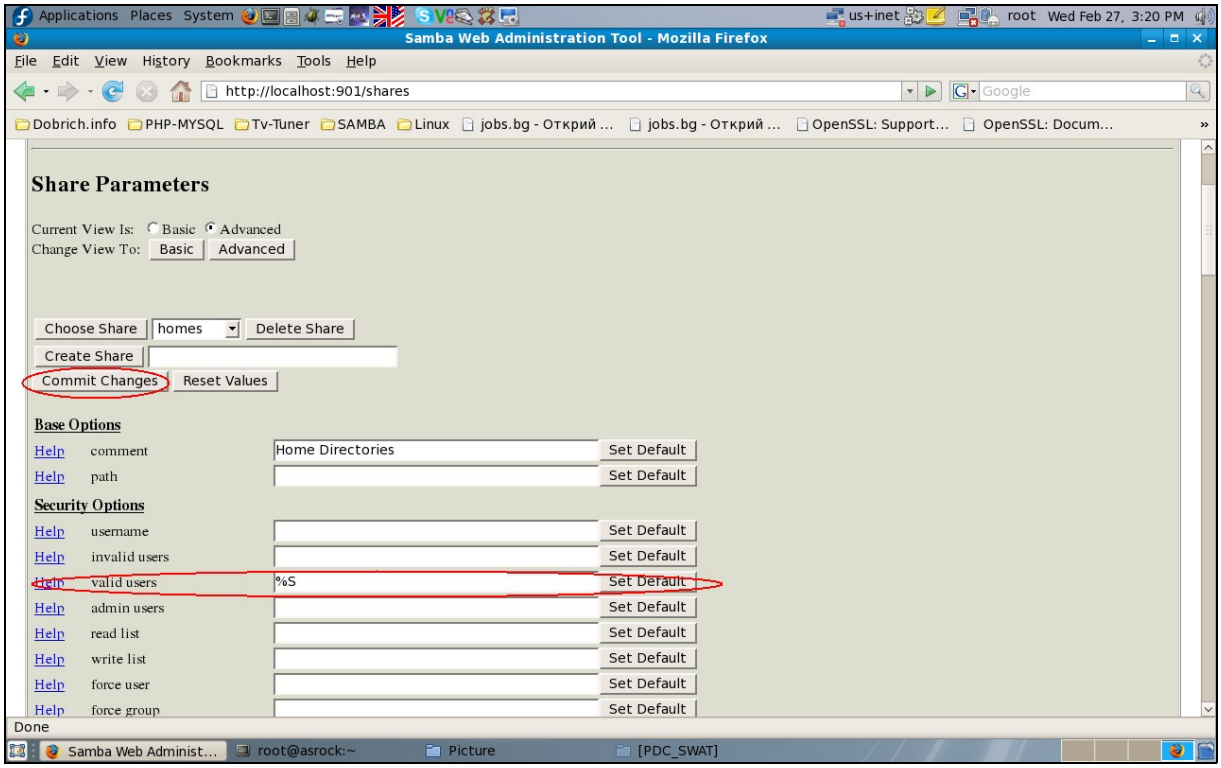
споделянето на директории става през SWAT от секцията "Shares" за целта след като е избрана опцията "Shares" се преминава в разширените настройки от бутона advanced view. Фиг. 3.3

Фиг. 3.3



Първите настройки които ще се осъществяват са на директорията "homes" която може да се избере от падащото меню между бутоните [Choose Share] и [Delete Share]. Ако не съществува такава директория тя може да бъде създадена от бутона [Create share] чрез въвеждане на името в кутиката до него. Валидните опции които трябва да се въведат за тази директория са: valid users = %S. Пример: фиг. 3.4

Фиг. 3.4



В четвърта стъпка се описва как се създават като споделен ресурс

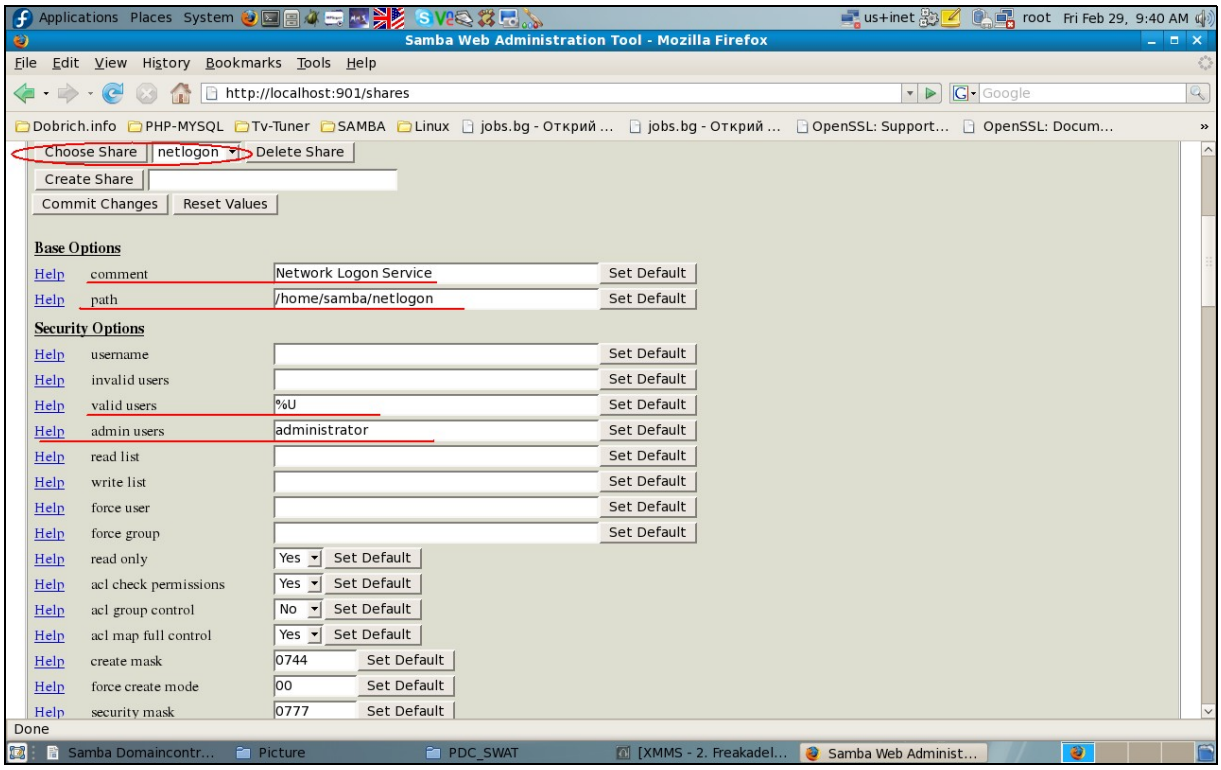
директориите "netlogon" и "profiles" и съответно техните параметри на споделяне пример: 29 и пример: 30 обхващат техните параметри.

Пример:създаване на "netlogon" като споделен ресурс (създаването на " netlogon " е аналагочно на създаването на „homes” но с други параметри) пример: 3.4 и фиг. 3.5

Пример: 3.4

```
[netlogon]
    comment = Network Logon Service
    path = /home/samba/netlogon
    admin users = administrator
    valid users = %U
    read only = yes
    guest ok = yes
    share modes = no
    browseable = no
    available = yes
```

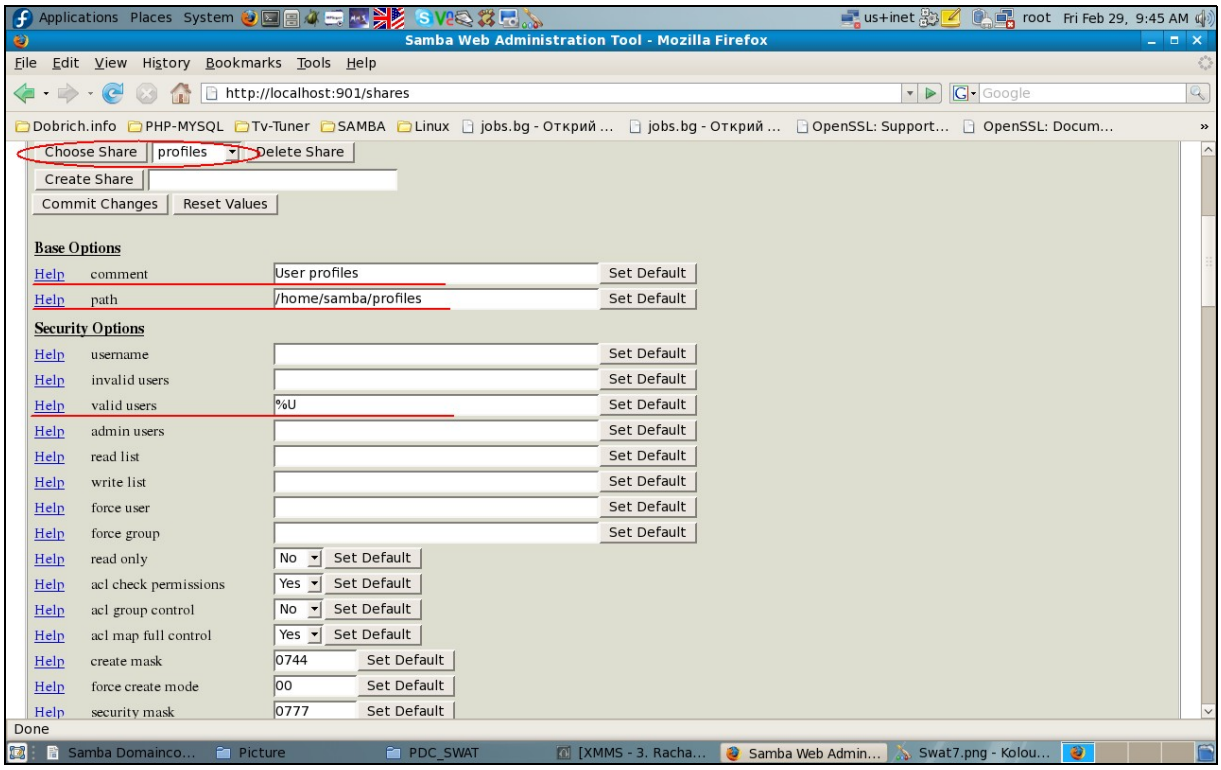
фиг. 3.5



Пример: 3.5 създаване на "profiles" като споделен ресурс

```
[profiles]
    comment = User profiles
    path = /home/samba/profiles
    valid users = %U
    create mask = 0600
    security mask = 0600
    directory mask = 0770
    directory security mask = 0770
    read only = no
    browseable = no
    available = yes
```

фиг. 3.6 (реализиране на промените на profiles)



Пета стъпка: съществуват и промени които трябва да се направят във файла nsswitch.conf които се намира в /etc/nsswitch.conf, а те са следните. (след като се отвори файлът с текстов редактор се правят следните промени посочени в пример: 3.6)

Пример: 3.6
mcedit /etc/nsswitch.conf

#hosts: files dns //този ред се заменя с

hosts: files wins dns

След което трябва да се въведе root потребителят в базата с данни на Самба (SAMBA password database) което става по следният начин:

smbpasswd -a root

Всъщност този потребител ще бъде и администраторски акаунт на домейнът които беше създаден

Домейнът може да се изпробва чрез следната команда

smbclient -L localhost -U%

Която трябва да върне отговор подобен на този посочен в пример: 3.7

пример: 3.7

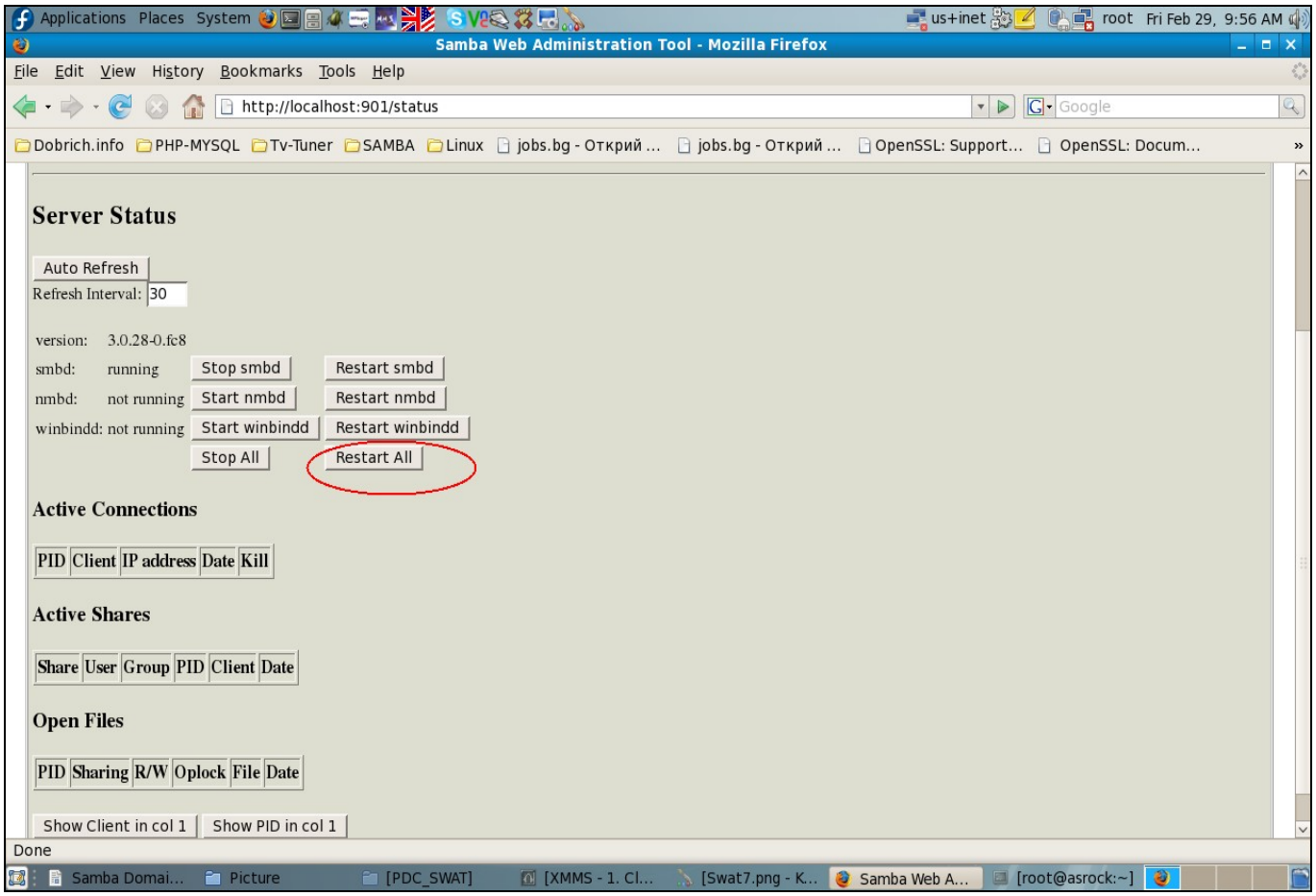
```
[root@asrock ~]# smbclient -L localhost -U%
Domain=[EXAMPLE.COM] OS=[Unix] Server=[Samba 3.0.28-0.fc8]
Sharename       Type      Comment
---------       ----      -------
 IPC$        IPC       IPC Service (Samba Server Version 3.0.28-0.fc8)
Domain=[EXAMPLE.COM] OS=[Unix] Server=[Samba 3.0.28-0.fc8]
Server               Comment
---------            -------
ASROCK               Samba Server Version 3.0.28-0.fc8
Workgroup            Master
---------            -------
EXAMPLE.COM          ASROCK
[root@asrock ~]#
```

В шеста стъпка е описано как се добавят групи за SAMBA domain които вече е създаден.

net groupmap add ntgroup="Domain Admins" unixgroup="root" type=domain -U root
net groupmap add ntgroup="Domain Users" unixgroup="users" type=domain -U root
net groupmap add ntgroup="Domain Guests" unixgroup="nobody" type=domain -U root

след като са създадени групите сървърът трябва да се рестартира което става по следният начин: в страницата на SWAT се преминава в секцията "STATUS" от където се рестартират всички приложения. Фиг. 3.7

Фиг. 3.7 (рестартиране на Samba от страницата Status на SWAT)



Или с изпълнението на посочените команди то пример: 3.8

Пример: 3.8

service smb restart
/etc/init.d/smb restart

След като са добавени групите трябва да се добавят и акаунтите със следните команди които се изпълняват за всеки потребител по отделно: пример: 3.9

net rpc user add %username% -U root
net rpc user password %username% "%userpassword%" -U root
smbpasswd -e %username%

Пример: 3.9
net rpc user add james -U root
net rpc user password james "secret" -U root
smbpasswd -e james

В тази стъпка е описано как се създава споделена директория достъпна за всички потребители.

Пример: 3.10 (създаване на директорията allusers)
mkdir -p /home/shares/allusers/
chown -R root:users /home/shares/allusers/
chmod -R 775 /home/shares/allusers/

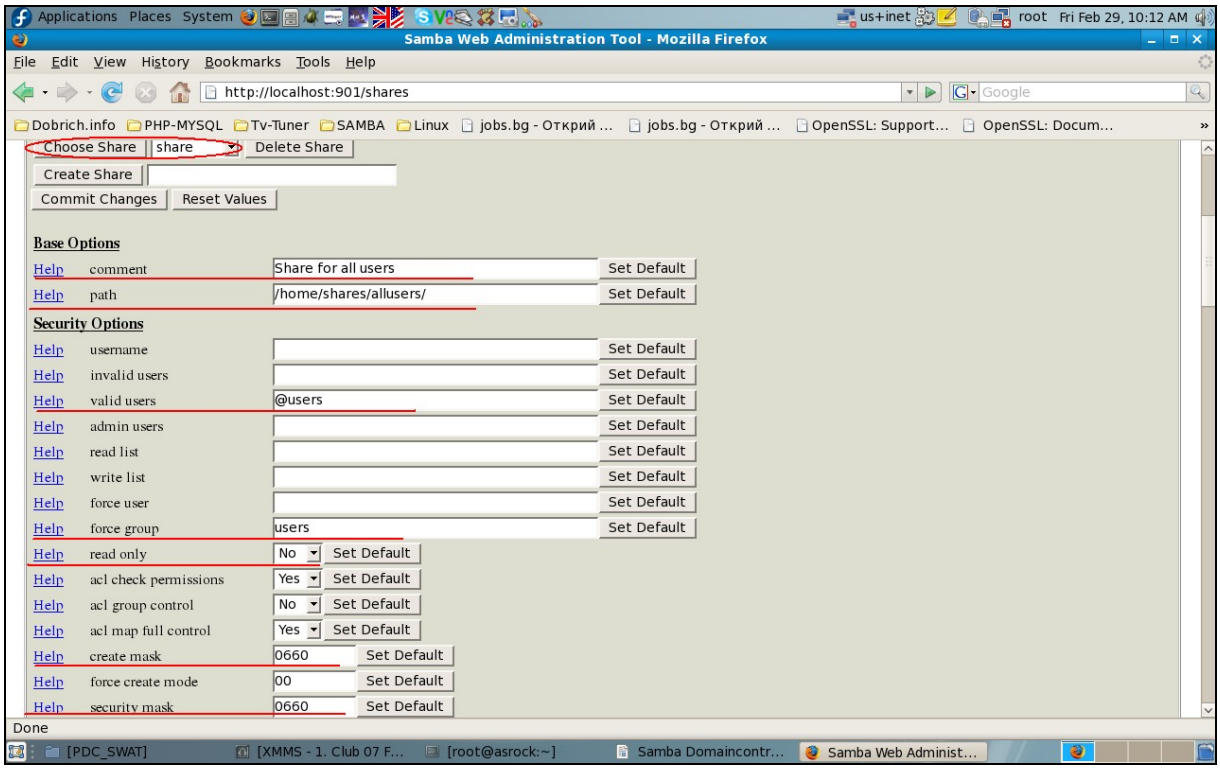
Конфигурирането се осъществяват чрез следните промени. В секцията "SHARES" от менюто на SWAT приложението се въвежда името на директорията която трябва да се сподели след което се създава с бутона **"Create Share"**.

След което трябва да се смени в **Advanced view** мод за да се въведът следните условия на дадената директория. Пример: 3.11 и фиг. 3.8

Пример: 3.11

comment = Share for all users (или нещо друго)
path = /home/shares/allusers/ (пътят до директорията от пример:)
valid users = @users
force group = users
read only = No
create mask = 0660
security mask = 0660
directory mask = 0771
directory security mask = 0771
available = Yes

фиг. 3.8



промените се запазват със бутона "Commit Changes" в по-горното меню.

В последната стъпка се правят промени в конфигурационният файл /etc/hosts. В него трябва да се добавят всички IP адреси на комютрите от **workgroup EXAMPLE.COM**. Конфигурацията на файла е описана в пример: 3.12

Пример: 3.12

mcedit /etc/hosts

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
 127.0.0.1       localhost.localdomain   localhost
 192.168.0.100   server1.example.com     server1
 192.168.0.110   workstation1
 192.168.0.111   workstation2
 192.168.0.112   workstation3
 ::1     localhost6.localdomain6 localhost6
```

(пълният набор на промените по конфигурационният файл smb.conf са описани накрая)

Пълен конфигурационен файл на Samba за PDC

```
# Samba config file superflay123 using SWAT
```

```
# from 127.0.0.1 (127.0.0.1)
# Date: 2008/02/29 10:16:33

[global]
        workgroup = EXAMPLE.COM
        server string = Samba Server Version %v
        passdb backend = tdbsam
        passwd program = /usr/bin/passwd %u
        passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:*
%n\n *password\supdated\ssuccessfully*
        passwd chat debug = Yes
        username map = /etc/samba/smbusers
        unix password sync = Yes
        log level = 3
        log file = /var/log/samba/log.%m
        max log size = 50
        printcap name = CUPS
        add user script = /usr/sbin/useradd -m '%u' -g users -G users
        delete user script = /usr/sbin/userdel -r %u
        add group script = /usr/sbin/groupadd %g
        delete group script = /usr/sbin/groupdel %g
        add user to group script = /usr/sbin/usernod -G %g %u
        add machine script = /usr/sbin/useradd -s /bin/false/ -d /var/lib/nobody %u
        logon script = scripts/logon.bat
        logon path = \\10.10.10.1\profiles\%U
        logon drive = H:
        logon home = \\10.10.10.1\%U
        domain logons = Yes
        os level = 200
        preferred master = Yes
        wins support = Yes
        ldap ssl = no
        idmap uid = 15000-20000
        idmap gid = 15000-20000
        template shell = /bin/bash
        profile acls = Yes
        printing = cups
        cups options = raw
        print command =
        lpq command = %p
        lprm command =

[homes]
        comment = Home Directories
        valid users = %S
        read only = No
        browseable = No

[printers]
```

```
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[printer_prob]
        comment = Home Directories
        path = /var/spool/samba
        printable = Yes
        browseable = No

[Install]
        comment = Install programs and etc.
        path = /Windows/Samba/Install
        valid users = %S
        available = No

[netlogon]
        comment = Network Logon Service
        path = /home/samba/netlogon
        valid users = %U
        admin users = administrator
        browseable = No

[profiles]
        comment = User profiles
        path = /home/samba/profiles
        valid users = %U
        read only = No
        browseable = No

[share]
        comment = Share for all users
        path = /home/shares/allusers/
        valid users = @users
        force group = users
        read only = No
        create mask = 0660
        security mask = 0660
        directory mask = 0771
        directory security mask = 0771
```

Конфигурационният файл smb.conf след неговото конфигуриране за PDC чрез инструментът SWAT.