

# Приложение

## Использование UNIX как контроллера домена

Задача данного приложения — дать слушателю практическое понимание специфики реализации домена средствами UNIX (Linux/FreeBSD).

### *Настройка стенда*

Выведите WinXP из домена corpX.un и перезагрузите виртуальную машину. На контроллере домена (Windows 2003) в оснастке Active Directory Users and Computers удалите gate из списка компьютеров.

В FreeBSD/Linux выполните:

```
gate# cat /etc/nsswitch.conf
...
passwd:    files
group:     files
shadow:    files # только в Linux
...
```

Остановите контроллер домена (Windows 2003).

Во FreeBSD выполните следующее:

```
gate# cd /etc/namedb
gate# ee named.conf
...
zone "corpX.un" {
    type master;

    file "/etc/namedb/master/corpX.un";

    allow-update { 127.0.0.1; };

};
```

```
gate# /etc/rc.d/named restart
```

Новым контроллером домена будет server

```
server# pkg_add -r samba3
server# cd /usr/local/etc/

server# cat smb.conf
[global]
    workgroup = CORPX
    os level = 128
    domain master = yes
    security = user
    domain logons = yes
    logon path = \\%L\profiles\%U
[netlogon]
    path = /home/samba
[profiles]
    path = /home/
    read only = no
```

```
server# testparm
server# mkdir /home/samba
```

```
server# pw groupadd users
server# net groupmap add ntgroup="Domain Admins" unixgroup=wheel rid=512 type=d
server# net groupmap add ntgroup="Domain Users" unixgroup=users rid=513 type=d
server# net groupmap add ntgroup="Domain Guests" unixgroup=nobody rid=514 type=d
server# net groupmap list
```

```
server# more /etc/rc.conf
```

```
...
nmbd_enable="YES"
smbd_enable="YES"
winbindd_enable="NO"
...
```

```
server# /usr/local/etc/rc.d/samba start
```

```
server# smbpasswd -a root
Smb password: password
```

```
server# smbpasswd -e root
Enabled user root.
```

```
server# pw usermod root -G users
server# pw useradd winxp$ -d /tmp -s /usr/sbin/nologin
```

В Ubuntu выполните следующие шаги:

```
root@server:~# apt-get install samba
root@server:~# cd /etc/samba/
```

```
root@server:~# cat smb.conf
[global]
    workgroup = CORPX
    os level = 128
    domain master = yes
    security = user
    domain logons = yes
    logon path = \\%L\profiles\%U
[netlogon]
    path = /home/samba
[profiles]
    path = /home/
    read only = no
```

```
root@server:~# testparm
root@server:~# mkdir /home/samba
root@server:~# net groupmap add ntgroup="Domain Admins" unixgroup=root rid=512 type=d
root@server:~# net groupmap add ntgroup="Domain Users" unixgroup=users rid=513 type=d
root@server:~# net groupmap add ntgroup="Domain Guests" unixgroup=nogroup rid=514 type=d
root@server:~# net groupmap list
root@server:~# restart smbd
root@server:~# restart nmbd
root@server:~# smbpasswd -a root
Smb password: password
```

```
root@server:~# smbpasswd -e root
Enabled user root.
```

```
root@server:~# usermod -G users root
```

```
root@server:~# adduser --force-badname --home /tmp --shell /bin/false winxp$
...
Enter new UNIX password: Pa$$w0rd
```

## Проверка работоспособности PDC

Введите WinXP в домен corpX.un.

На контроллере домена (server) добавьте пользователя user1, а затем включите его в группу локальных администраторов WinXP.

## Включение gate в домен (server)

Во FreeBSD выполните следующие шаги:

```
server# pw useradd gate$ -d /tmp -s /usr/sbin/nologin
server# smbpasswd -a gate$
```

```
...
Added user gate$.
```

```
server# smbpasswd -e gate$
Enabled user gate$.
```

Дальнейшие шаги выполняются на gate

```
gate# /usr/local/etc/rc.d/samba stop
```

```
gate# pkg_delete -x samba3
```

```
gate# pkg_add -r samba3
```

```
gate# cat /etc/rc.conf
```

```
...
nmbd_enable="NO"
smbd_enable="NO"
winbindd_enable="YES"
...
```

```
gate# cd /usr/local/etc/
```

```
gate# cat smb.conf
```

```
[global]
    workgroup = CORPX
    security = DOMAIN
    winbind use default domain = Yes
    winbind enum users = yes
    winbind enum groups = yes
    winbind cache time = 36
    idmap uid = 20000-40000
    idmap gid = 20000-40000
    template homedir = /home/%U
    template shell = /bin/sh
```

```
gate# /usr/local/etc/rc.d/samba restart
```

```
gate# cat /etc/nsswitch.conf
```

```
...
passwd:          files winbind
group:           files winbind
...
```

```
gate# net rpc join -U root
```

```
Enter root's password:
```

```
Joined domain CORPX.
```

В Ubuntu выполните следующие шаги:

```
root@server:~# adduser --force-badname --home /tmp --shell /bin/false gate$
```

```
...
```

```
...Password: Pa$$w0rd
```

```
root@server:~# smbpasswd -a gate$
```

```
...
```

```
Added user gate$.
```

```
root@server:~# smbpasswd -e gate$
```

```
Enabled user gate$.
```

Дальнейшие шаги выполняются на gate

```
root@gate:~# stop nmbd
```

```
root@gate:~# stop smbd
```

```
root@gate:~# apt-get purge samba winbind
```

```
root@gate:~# rm -rf /var/cache/samba /var/lib/samba
```

```
root@gate:~# apt-get install winbind
```

```
root@gate:~# cd /etc/samba
```

```
root@gate:~# cat smb.conf
```

```
[global]
```

```
workgroup = CORPX
security = DOMAIN
winbind use default domain = Yes
winbind enum users = yes
winbind enum groups = yes
winbind cache time = 36
idmap uid = 20000-40000
idmap gid = 20000-40000
template homedir = /home/%U
template shell = /bin/bash
```

```
root@gate:~# /etc/init.d/winbind restart
```

```
root@gate:~# cat /etc/nsswitch.conf
```

```
...
```

```
passwd:      files winbind
```

```
group:       files winbind
```

```
shadow:      files winbind
```

```
...
```

```
root@gate:~# net rpc join -U root
```

```
Enter root's password:
```

```
Joined domain CORPX.
```

## ***Проверка аутентификации на gate***

В FreeBSD/Ubuntu выполните следующее:

```
gate# ntlm_auth --username=user1
```

```
password:
```

```
NT_STATUS_OK: Success (0x0)
```

```
gate# wbinfo -u
```

```
...
```

```
gate# wbinfo -g
```

```
...
```

```
gate# id user1
```

## ***Управление доступом к файлам***

В FreeBSD/Ubuntu внесите в конец файла smb.conf следующие строки:

```
[user_write]
```

```
path = /tmp
```

```
valid users = CORPX\root
```

```
    read only = no
[group_write]
    path = /tmp
    valid users = "@CORPX\domain users"
    read only = no
    force user = nobody
```

Перезапустите samba на server и проверьте доступ к шарам под разными учетными записями: доменного пользователя и администратора домена.