

Единая прозрачная авторизация пользователей домена Active Directory на сервере Squid

Александр Соколов

Многие администраторы применяют прокси-серверы для распределения доступа в Интернет. Это не только позволяет экономить трафик, но и вести статистику о том, кто куда и когда заходил. Существуют схемы, когда для выхода в Интернет не требуется регистрация, используется анонимный доступ, но как в таком случае управлять доступом, если на всех один пароль? Можно предложить разделение доступа по IP-адресам компьютеров, но и здесь за одним компьютером могут работать несколько человек. Как же в таком случае поступить?

Все очень просто: каждый пользователь идентифицируется и получает доступ к прокси-серверу только при наличии действующей регистрационной записи в домене Windows. Дополнительным плюсом такой системы будет незаметная для пользователя авторизация.

Итак, существует успешная корпорация. Все организационные подраз-

деления этой корпорации входят в единый домен, а локальная сеть корпорации подключена к Интернету. Хотелось бы схему единой аутентификации пользователей, предлагаемую контроллером домена, применить и к доступу в Интернет.

Назовем домен корпорации `corporation.local`, сам контроллер домена – `dc.corporation.local` (192.168.120.2),

шлюз в Интернет – `gate.corporation.local` (с «внутренним» – 192.168.120.12 и «внешним» 192.168.100.12 адресами). Пользователям домена `sanya`, `daria` и `maria` необходим доступ к Интернету.

Домен управляется контроллером домена Active Directory (здесь нам понадобится Windows Server 2003 R2, включающий сервисы аутентифика-

ции UNIX). Доступ в Интернет контролируется прокси-сервером Squid2.6, установленным на платформе OpenSolaris.

Подготовка Active Directory

Установка Windows Server 2003 производится в штатном режиме. Повышение роли сервера до контроллера домена выполняется с помощью мастера Active Directory Installation Wizard («Administration → Server Management»), при этом используется типовая настройка. При установке DNS-сервера необходимо создать новый домен в новом лесу, зону обратного просмотра и настроить пересылку запросов на DNS-сервер провайдера. Настраивая DHCP-сервер, следует указать адрес сервера DNS (192.168.120.2) и адрес маршрутизатора (192.168.120.12) для раздачи клиентским компьютерам.

Для расширения схемы LDAP и поддержки UNIX-атрибутов пользователей надо добавить компонент Active Directory Services: Identity Management for UNIX, включая Server for NIS и Subsystem for UNIX-based applications. В результате появится вкладка «UNIX Attributes» на странице свойств пользователей и групп. Также следует скачать из Интернета и установить Windows Support Tools, которые включают утилиту ktpass для генерации Kerberos-ключей.

Подготовка пользователей домена

Для начала создадим группу unixusers. В ее свойствах на вкладке «UNIX Attributes» укажем имя NIS домена (оно совпадает с NetBIOS-именем домена (по умолчанию corporation)). Теперь каждого пользователя, которому необходима аутентификация на прокси-сервере, следует включить в эту группу. Уберем галочку «Требовать смену пароля при следующем входе в систему», иначе мы не сможем зарегистрироваться в UNIX.

Для аутентификации с использованием схемы LDAP необходим объект-посредник. В группе «Domain Guests» создается непривилегированная учетная запись ldapuser с именем Agent (см. рис. 1) и паролем «n0123pasaram!».

Для аутентификации самого объекта-посредника создается Kerberos-ключ:

```
C:\Program Files\Support Tools>ktpass -out gate.keytab -pass n0123pasaram! -princ host/gate.corporation.local@CORPORATION.LOCAL -mapuser ldapuser@CORPORATION.LOCAL -crypto DES-CBC-MD5 +DesOnly -ptype KRB5_NT_PRINCIPAL
```

Установка OpenSolaris

В OpenSolaris устанавливается только поддержка ядра (Core System Support), графическая оболочка нам ни к чему. Нажатием <F4> предлагается выбрать устанавливаемые приложения, добавляем Squid Web Proxy Cache.

Настройка маршрутизации

Мы не будем заниматься фильтрацией трафика, просто разрешим все входящие и исходящие соединения. Правим файл /etc/ipf/ipnat.conf:

```
pass in log quick all
pass out log quick all
```

Для настройки NAT создадим файл /etc/ipf/ipnat.conf:

```
map pcn0 192.168.120.0/24 -> 192.168.100.12 portmap tcp/udp 40000:59999
map pcn0 192.168.120.0/24 -> 192.168.100.12
```

Включим перенаправление пакетов:

```
#routeadm -e ipv4-forwarding
#routeadm -u
```

и фильтрацию трафика:

```
# svcadm enable ipfilter
# ipnat -Cf /etc/ipf/ipnat.conf
```

Теперь поправим файл /etc/hosts, изменив строчку с поставлением имени на:

```
192.168.120.12 gate.corporation.local gate loghost
```

Лицензионное ПО — это высокое качество, надежность и репутация!

- ❖ ВЫСОКОКВАЛИФИЦИРОВАННЫЙ КОНСАЛТИНГ
- ❖ ПОДБОР ПО ДЛЯ БИЗНЕСА
- ❖ АНАЛИЗ И АУДИТ
- ❖ КОРПОРАТИВНОЕ ЛИЦЕНЗИРОВАНИЕ
- ❖ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Softway.ru — авторизованный партнер крупнейших производителей программного обеспечения:

- ❖ Microsoft Gold Certified Partner,
- ❖ Oracle, Autodesk, IBM, Adobe, Corel, 1C, Symantec, Kerio, Лаборатория Касперского, Eset, ABBYY, Acronis и других.

Москва, ул. Б. Грузинская, д. 36А, стр. 5
(495) 987 10 50

Новосибирск, ул. Восход 20, офис 305
(383) 254 03 05



Softway.ru

лицензионное
программное
обеспечение

www.softway.ru

Рисунок 1. Создание учетной записи объекта-посредника

Настроим разрешение имен (/etc/resolv.conf):

```
domainname corporation.local
nameserver 192.168.120.2
search corporation.local
```

В /etc/nsswitch.conf должна присутствовать запись:

```
hosts dns files
```

Запустим DNS-клиент:

```
# svcadm enable svc:/network/dns/client:default
```

Проверку верности настроек можно осуществить утилитой ping:

```
# ping dc
```

Настройка Kerberos-клиента

Первым делом надо поправить файл /etc/krb5/krb5.conf:

```
[libdefaults]
    default_realm = CORPORATION.LOCAL
    verify_ap_req_nofail=false
    clockskew=300

[realms]
    CORPORATION.LOCAL={
        kdc=dc.corporation.local:88
        admin_server=dc.corporation.local:749
        kpasswd_protocol=SET_CHANGE
    }
    [domain_realm]
        .corporation.local=CORPORATION.LOCAL
    [logging]
        default=FILE:/var/krb5/krb.log
        kdc=FILE:/var/krb5/krb.log
        kdc_rotate={
            period=1d
            version=10
        }
    [appdefaults]
        kinit={
            renewable=true
            forwardable=true
        }
```

Проверяем настройку:

```
#kinit -p maria
```

```
Password for maria@CORPORATION.LOCAL:
```

```
#klist
```

```
Default principal: maria@CORPORATION.LOCAL
Valid starting    Expires          Service principal
05/27/08 13:30:32 05/27/08 23:30:45  krbtgt/CORPORATION.LOCAL@CORPORATION.LOCAL
Renew until 06/03/08 13:30:32
```

Настройка сменных модулей аутентификации (PAM)

Здесь все просто: в цепочку модулей аутентификации надо вставить модули аутентификации, отвечающие за проверку Kerberos и LDAP.

Для поддержки прозрачной Squid-аутентификации достаточно внести следующие изменения в файле /etc/pam.conf:

```
other auth requisite pam_authtok_get.so.1
other auth required pam_dhkeys.so.1
other auth sufficient pam_unix_cred.so.1

other auth sufficient pam_ldap.so.1 use_first_pass debug
other auth required pam_krb5.so.1 try_first_pass debug

other auth sufficient pam_unix_auth.so.1
```

Настройка поддержки LDAP

Теперь добавим наш шлюз в домен.

Выполним команду:

```
ldapclient manual
-a credentialLevel=proxy
-a authenticationMethod=simple
-a proxyDN=cn=Agent,cn=Users,dc=example,dc=com
-a proxyPassword=n0123pasaram!
-a defaultSearchBase=dc=corporation,dc=local
-a domainName= corporation.local
-a "defaultServerList=192.168.120.2"
-a attributeMap=group:userpassword=userPassword
-a attributeMap=group:memberuid=memberUid
-a attributeMap=group:gidnumber=gidNumber
-a attributeMap=passwd:gecos=cn
-a attributeMap=passwd:gidnumber=gidNumber
-a attributeMap=passwd:uidnumber=uidNumber
-a attributeMap=passwd:homedirectory=unixHomeDirectory
-a attributeMap=passwd:loginshell=loginShell
-a attributeMap=shadow:shadowflag=shadowFlag
-a attributeMap=shadow:userpassword=userPassword
-a objectClassMap=group:posixGroup=group
-a objectClassMap=passwd:posixAccount=user
-a objectClassMap=shadow:shadowAccount=user
-a serviceSearchDescriptor=passwd:dc= corporation,dc=local?sub
-a serviceSearchDescriptor=group:dc= corporation,dc=local?sub
```

Для чтения паролей аппликантов используется объект-посредник (cn=Agent,cn=Users,dc=example,dc=com).

После перезапуска LDAP-клиента:

```
# svcadm restart svc:/network/dap/client:default
```

gate.corporation.local становится членом домена:

```
# domainname
corporation.local
```

Проверим доступность каталога LDAP.

При запросе:

```
# ldaplist passwd sanya
```


мы должны получить имя объекта:

```
dn: gecos=Alexander Sokolov,OU=developers,DC=corporation,DC=local
```

Затем необходимо снова поправить файл /etc/nsswitch.conf:

```
hosts dns files
```

Теперь пришло время ключа Kerberos gate.keytab: копируем его в /etc/krb5/krb5.keytab. Проверим его работоспособность:

```
# kinit -t /etc/krb5/krb5.keytab \
-k host/lda.corporation.local
```

Если ошибок не возникает, можем заняться непосредственно прозрачной авторизацией.

Настройка прокси-сервера

Для аутентификации пользователей применяется помощник /usr/squid/squid_ldap_auth, для работы которого нужен еще один объект-посредник – squidreader (cn=Reader, cn=Users, dc=corporation, dc=local). Его пароль записываем в файл /etc/squid/adpwd. Конфигурация прокси-сервера в файле /etc/squid/squid.conf:

```
http_port 3128
visible_hostname localhost
cache_effective_user webserverd
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath regex cgi-bin \?
no_cache deny QUERY
cache_mem 64 MB
cache_swap_low 90
cache_swap_high 95
maximum_object_size 8192 KB
minimum_object_size 0 KB
maximum_object_size_in_memory 256 KB
ipcache_size 2048
ipcache_low 90
ipcache_high 95
fqdn_cache_size 4096
cache_replacement_policy lru
memory_replacement_policy lru
cache_dir ufs /var/squid/cache 5000 16 256
```

```
logformat squid %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm \
%ru %un %Sh/%<A %mt
access_log /var/squid/logs/access.log squid
cache_log /dev/null
cache_store_log none
auth_param basic program \
/usr/squid/libexec/squid_ldap_auth \
-R -b "dc=corporation,dc=local" \
-D "cn=Reader,cn=Users,dc=corporation,dc=local" \
-W "/etc/squid/adpwd" -f sAMAccountName=%s \
-h 192.168.120.2
auth_param basic children 5
auth_param basic realm CORPORATION.LOCAL
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
acl users proxy_auth ALL
acl allowed_users proxy_auth "/etc/squid/allowed_users"
acl banners url_regex "/etc/squid/banners"
http_access deny banners
http_access allow allowed_users
http_access deny all
coredump_dir /var/squid/cache
```

В файле allowed_users записаны учетные записи пользователей, которым разрешен доступ:

```
sanya
daria
maria
```

С помощью паттернов в файле banners осуществляется борьба с баннерами:

```
^http://bs\.yandex\.ru
^http://images\.rambler\.ru
^http://top100-images\.rambler\.ru
^http://ban\.aport\.ru
^http://[^\]*top\.list\.ru/counter
^http://[^\]*spylog\.com/cnt
```

Более тонкая настройка прокси-сервера позволяет справедливо разделить канал, ограничить доступ пользователей в Интернет по времени, оптимизировать кэширование объектов. Файл /var/squid/logs/access.log содержит журнал доступа пользователей в Интернет: время обращения (в миллисекундах с 1 января 1970 года), IP-адрес и учетную запись клиента, сайт, к которому была совершена попытка обращения, и другие параметры. Таким образом, зная формат файла журнала, можно контролировать доступ пользователей к Интернету.

Запуск сервера:

```
# /usr/squid/sbin/squid -z
# svcadm enable squid
```

Итог

Пользователям домена достаточно прописать в браузере адрес прокси-сервера (192.168.120.12) и порт (3128), после чего при попытке открыть сайт будут запрошены их аутентификационные данные (см. рис. 2). Пользователи sanya, maria, daria получают доступ к Интернету, используя доменные учетные данные. Для ограничения доступа пользователя достаточно закоментировать строку, содержащую его имя, в файле allowed_users.

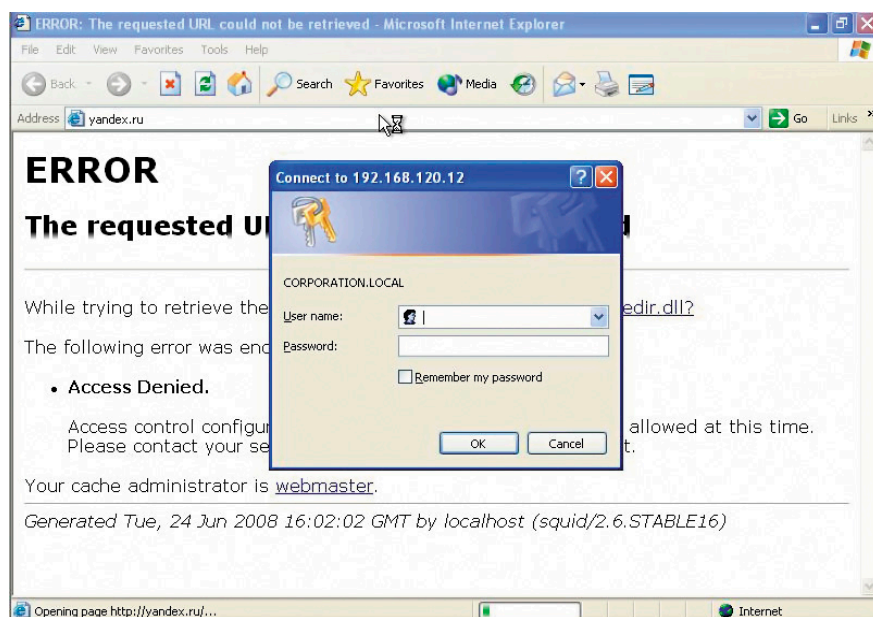


Рисунок 2. Запрос аутентификации