

??:

?? win proxy server ????, ??????????????????, ????? Linux ????, ??????????, ??????????.

??:

OS= Redhat Enterprise Linux AS 4(????)

Kernel= 2.6.9-22.0.1.ELsmp

Squid= squid-2.5.STABLE6-3 (rpm -qa | grep squid)

Samba= Version 3.0.10-1.4E (smbd -V)

??????????????, ???????.

????:

Step 1) ?? Samba

?? Samba ??????

#!/usr/sbin/smbd -b

--with Options:

WITH\_ADS

WITH\_AUTOMOUNT

WITH\_PAM

WITH\_QUOTAS

WITH\_SENDFILE

WITH\_SMBMOUNT

WITH\_SYSLOG

WITH\_UTMP

WITH\_WINBIND <<

?????? winbind, ????, ?????????, ?????, ??????.

???? samba rpm:

?????????????? source rpm = samba-3.0.10-1.4E.src.rpm

<ftp://ftp.redhat.com>

#rpm -i samba-3.0.10-1.4E.src.rpm

#cd /usr/src/redhat/SPECS

#vi samba.spec

?????

CFLAGS=-D\_GNU\_SOURCE %configure

--with-acl-support

--with-automount

.....

--with-swatdir=%{\_datadir}/swat

????????

```
--with-winbind
--with-winbind-auth-challenge
```

```
????
```

```
#rpmbuild -bb samba.spec
```

```
????????????, ?????????? /usr/src/redhat/RPMS/i386,
????????? rpm ??????????, ?????????????????,
??????, ????(force)????.
```

```
#service smb stop
#cd /usr/src/redhat/RPMS/i386
#rpm -ivh --force samba-3.0.10-1.4E.i386.rpm
#rpm -ivh --force samba-client-3.0.10-1.4E.i386.rpm
#rpm -ivh --force samba-common-3.0.10-1.4E.i386.rpm
#rpm -ivh --force samba-debuginfo-3.0.10-1.4E.i386.rpm
#rpm -ivh --force samba-swat-3.0.10-1.4E.i386.rpm
```

```
?? smb.conf ? krb5.conf
```

```
#vi /etc/samba/smb.conf
[global]
workgroup = NTDOMAIN
realm = NTDOMAIN.COM
security = ADS #AD????
password server = MyDC #??Domain Controller
encrypt passwords = yes
wins server = MYWINS #??WINS server
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template shell = /bin/bash #???
template homedir = /home/%D/%U
winbind use default domain = yes
```

```
#vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = NTDOMAIN.COM
dns_lookup_realm = false
dns_lookup_kdc = false
```

```
[realms]
GTTW.COM.TW = { ##????
kdc = MyDC
default_domain = NTDOMAIN.COM
```

```
admin_server = MyDC
}
```

```
[domain_realm]
.gttw.com.tw = NTDOMAIN.COM
gttw.com.tw = NTDOMAIN.COM
```

? Linux ?? AD ??

```
#net ads join -U Administrator%mypass
```

```
?????"KDC has no support for encryption type"
```

```
??? AD Administrator ???,???????
```

[http://gentoo-wiki.com/HOWTO\\_Adding\\_...ting\\_AD\\_Domain](http://gentoo-wiki.com/HOWTO_Adding_...ting_AD_Domain)

```
??/var/lib/samba/winbindd_privileged?????750, ??squid, ?squid????winbind?socket.
```

```
???DC???????
```

```
# wbinfo --set-auth-user=user%password (?????????????)
```

```
??(??) Samba & winbind
```

```
#service smb restart
```

```
#service winbind restart
```

Step 2) ?? Squid

```
?? Squid ????????
```

```
#squid -v
```

```
?????????
```

```
--enable-auth=ntlm,basic
```

```
--enable-basic-auth-helpers=winbind
```

```
--enable-ntlm-auth-helpers=winbind
```

```
--enable-external-acl-helpers="winbind_group,wbinfo_group"
```

```
?????, ?????????, ???, ??????.
```

```
???? Squid rpm:
```

```
????????????? source rpm = squid-2.5.STABLE6-3.src.rpm
```

<ftp://ftp.redhat.com>

```
#rpm -i squid-2.5.STABLE6-3.src.rpm
```

```
#cd /usr/src/redhat/SPECS
```

```
#vi squid.spec
```

??????????????????.

#rpmbuild -bb squid.spec

?? RPM ?????? Samba ???.

?? squid.conf

# NT challenge Authentication for IE

auth\_param ntlm program /usr/bin/ntlm\_auth --helper-protocol=squid-2.5-ntlmssp

auth\_param ntlm children 5

auth\_param ntlm max\_challenge\_reuses 0

auth\_param ntlm max\_challenge\_lifetime 20 minutes

# Plain Text Authentication for others

auth\_param basic program /usr/bin/ntlm\_auth --helper-protocol=squid-2.5-basic

auth\_param basic children 5

auth\_param basic realm Squid proxy-caching web server

auth\_param basic credentialsttl 2 hours

###Authorization program,????????????(????????????????????)

external\_acl\_type NT\_global\_group ttl=300 %LOGIN /usr/lib/squid/wbinfo\_group.pl

###Access Control list, ??external\_acl\_type, ?????????????????????????????? acl UserGroup proxy\_auth REQUIRED

??

acl UserGroup external NT\_global\_group "/etc/squid/usergroup"

# ????????

http\_access allow UserGroup

????????????????,??Samba3.0.2(wbinfo -r????????)?????/usr/lib/squid/wbinfo\_group.pl

#!/usr/bin/perl -w

#

# external\_acl helper to Squid to verify NT Domain group

# membership using wbinfo

#

# This program is put in the public domain by Jerry Murdock

# <jmurdock@itraktech.com>. It is distributed in the hope that it will

# be useful, but WITHOUT ANY WARRANTY; without even the implied warranty

# of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

#

# Author:

# Jerry Murdock <jmurdock@itraktech.com>

#

# Version history:

# 2002-07-05 Jerry Murdock <jmurdock@itraktech.com>

# Initial release

```

#
# 2003-12-16 Jim Barber
# Added mutiple Group check in Group file

# external_acl uses shell style lines in it's protocol
require 'shellwords.pl';

# Disable output buffering
$|=1;

sub debug {
# Uncomment this to enable debugging
# print STDERR "@_n";
}

#
# Check if a user belongs to a group
#
sub check {
local($user, @group) = @_ ;
local($group);
foreach $group (@group)
{
$groupSID = `wbinfo -n "$group"`;
chop $groupSID;
$groupGID = `wbinfo -Y "$groupSID"`;
chop $groupGID;
&debug( "User: -$user-nGroup: -$group-nSID: -$groupSID-nGID: -$groupGID-");
return 'OK' if(`wbinfo -r Q$userE` =~ /^$groupGID$/m);
}
return 'ERR';
}

#
# Main loop
#
while (<STDIN>) {
chop;
&debug ("Got $_ from squid");
($user, @group) = &shellwords;
$ans = &check($user, @group);
&debug ("Sending $ans to squid");
print "$ansn";
}

**????????

??/etc/squid/usergroup?, ??????squid?AD??, ???

```

Domain Admins  
Internet User

????, ?? Squid ,????????.

#service squid start

### FAQ:

1. ???????, ?????????? AD ??????, ?? Squid ?????, ?????????? SELinux service ???.
2. squid ?????, squid -v ?????, ??? SELinux ? Squid ?, Desktop-->Applications->security level-->SELinux--SELinux Service Protection-->Disable SELinux Protection for squid daemon

3. ??? Linux ? AD ????????????

?? Join win2K AD ????????????

wbinfo -g //??AD ?????

wbinfo -u //??AD ?????

wbinfo -a myid%mypass //??????

wbinfo -t //? AD ?????

wbinfo -n "somegroup" //Convert group name to sid

4. ??? AD ?????, ??? wbinfo -n ?? sid ??? "Could not lookup name"???

????????, ?????, ????????? 3.0.21 ,?????????????

??,????????? sid, ??????????, ??? wbinfo\_group.pl ?, ???????.

??? /usr/lib/squid/wbinfo\_group.pl

?????

```
sub check {
```

```
local($user, $group) = @_;
```

```
$groupSID = `wbinfo -n "$group"`;
```

```
chop $groupSID;
```

```
$groupGID = `wbinfo -Y "$groupSID"`;
```

```
chop $groupGID;
```

????

```
sub check {
```

```
local($user, $group) = @_;
```

```
$groupSID = `wbinfo -n "$group" | cut -d" " -f1`;
```

```
chop $groupSID;
```

```
$groupGID = `wbinfo -Y "$groupSID"`;
```

```
chop $groupGID;
```

5. ??????? 15 ??, ?????????, ?????????????????, ?????????????.

A:??? cache.log ???????

=====

WARNING: All ntlmauthenticator processes are busy.

2006/04/14 09:17:01|

WARNING: up to 14 pending requests queued

2006/04/14 09:17:01|

Consider increasing the number of ntlmauthenticator processes to at least 19 in your config file.

=====

?????????-->20

auth\_param ntlm children 20

auth\_param basic children 20

6. How to avoid JVM authentication dialog box.

A:Add the following

acl java\_jvm browser Java

Then,before your http\_access for the authenticated users, use:

http\_access allow java\_jvm

????:

- [Configure two node Squid \(Proxy Server\) Clustering using Pacemaker on CentOS 7 / RHEL 7](#)