Winbind NTLM Authentication configuration for squid and apache

July 2, 2010 / Gavin Jackson

apache ntlm samba squid sysadmin winbind windows

Introduction We want squid and apache (running on SLES 11) to use Microsoft Active Directory NTLM authentication. This means that users who have logged into our windows domain will not have to enter their user credentials to use these services. Package installation

Install the following packages:

```
samba
samba-winbind
apache2-mod_auth_ntlm_winbind (for apache)
```

Samba Configuration Samba configuration (/etc/samba/smb.conf):

```
[global]
workgroup = LESMILLS
passdb backend = tdbsam
security = ADS
realm = lesmills.net.au
password server = fs.lesmills.net.au
encrypt passwords = yes
winbind separator = \\
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
template shell = /bin/false
template homedir = /home/winnt/%U
allow trusted domains = no
```

Next, you need to bind the Linux host to the windows domain:

```
root# net ads join -U Administrator%password
```

Modify /etc/nsswitch add the following line:

```
passwd: files winbind
```

Restart winbind and samba and you should be able to run getent passwd (you should see the AD users come back). Before modifying squid and/or apache you can test that ntlm_auth is working by typing:

```
/usr/bin/ntlm_auth --username gavinj --domain=lesmills.net.au

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

This is a good sign that the system can talk to your AD server. Squid Add the following lines to your /etc/squid/squid.conf:

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp --
domain=lesmills.net.au
auth_param ntlm children 5
auth_param ntlm keep_alive on
```

Apache

```
zypper install pam_smb
setfacl -m u:wwwrun:rx /var/lib/samba/winbindd_privileged
a2enmod auth_ntlm_winbind
rcapache2 restart
```

Add the following directives to your Directory entry:

```
AuthName "NTLM Authentication thingy"
NTLMAuth on
NTLMAuthHelper "/usr/bin/ntlm_auth --domain=lesmills.net.au --helper-protocol=squid-2.5-ntlmssp"
NTLMBasicAuthoritative on
AuthType NTLM
require valid-user
```

Note, to check that a user belongs to a specific AD group, you can use the following entry (it took me an hour to figure out the correct DOMAIN\\GROUP syntax).

```
AuthName "NTLM Authentication thingy"
NTLMAuth on
NTLMAuthHelper "/usr/bin/ntlm_auth --domain=lesmills.net.au --require-membership-of=LESMILLS\\\IT --
helper-protocol=squid-2.5-ntlmssp"
NTLMBasicAuthoritative on
AuthType NTLM
require valid-user
```

Browser Testing This technique works over http under IE8 and Firefox 3.6.3 on Windows 2008 (Terminal Server). This technique does not work over https under IE 8 (get a 500 server error). It does however seem to work fine in Firefox 3.6.3.

To white list ntlm servers in recent versions of Firefox (so that it doesn't ask for a username and password), you need to use about:config and edit the network.automatic-ntlm-auth.trusted-uris option (enter your webserver name). References

- http://en.wikipedia.org/wiki/NTLM
- http://blog.netnerds.net/2009/10/enable-windows-ntlm-pass-through-authentication-in-linux-based-apache/
- http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/domain-member.html#ads-member

Downloaded from https://www.gavinj.net/post/winbind-ntlm-authentication
Generated July 9, 2026. Copyright Gavin Jackson. All rights reserved.