Xinet TechNote 218: Directory Services (Active Directory) Authentication with FullPress and WebNative – Red Hat Enterprise Linux Version 5 32bit & 64bit

By: Keigo Kiyohara, Hitesh Chhatrala, Yi Zhang

Last modified: 3/10/08

Note: these instructions were written for FP 15.03 / WNV 8.03. If you are running an older version, you may want to upgrade.

Overview

1) Bind your Red Hat Enterprise Linux Version 5 32bit and 64bit (RHEL5) Server to Active Directory.

2) Configure FullPress 15.03 and WebNative 8.03

1. Binding RHEL5 32bit Server to a Windows Server 2003 Active Directory

These directions are a rough guideline on how to bind a RHEL5 32bit / 64bit Server to Active Directory. Our test setup is a RHEL5 32bit / 64bit server (with the latest patches applied as of 12/10/07) and Windows Server 2003 Standard Edition Service Pack 1.

We expect that patches released after 12/10/07 will work correctly, but there is always the possibility that problems will arise in future updates.

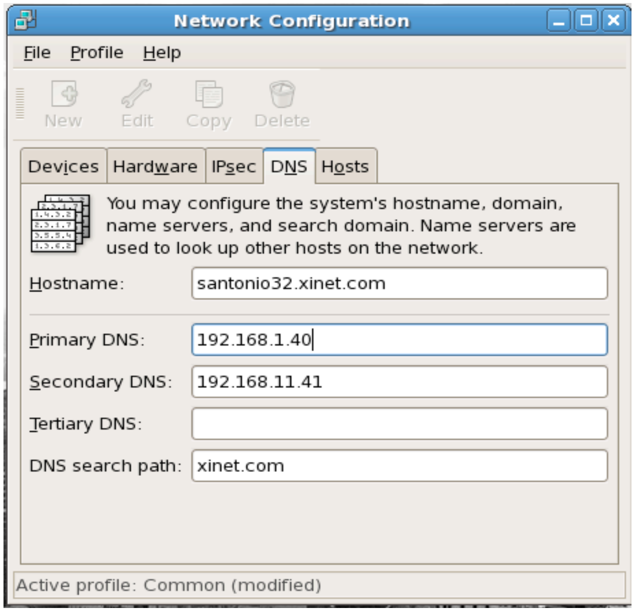
Preparation notes:

- The method we use here requires the RHEL 5 server's NetBIOS name be no longer than 15 characters. You can change the NetBIOS name in the GUI tool System | Administration | Network. Click on the DNS tab to edit the hostname. Save the change and restart the server after the name change.

- Login to the console as root or enable ssh and login as root remotely. Keep this window open during the whole configuration procedure. That way, in case a mistake is made and you are locked out of your system, you can move the backup files back into place.

- Back up the following files:
  /etc/nsswitch.conf
  /etc/pam.d/system-auth
  /etc/samba/smb.conf

- Make sure DNS is configured properly on the RHEL5 server. The first DNS server entry should be the IP address of your AD server. In the screenshot below, the IP address of the AD server is 192.168.1.40.



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname: santonio32.xinet.com

Primary DNS: 192.168.1.40

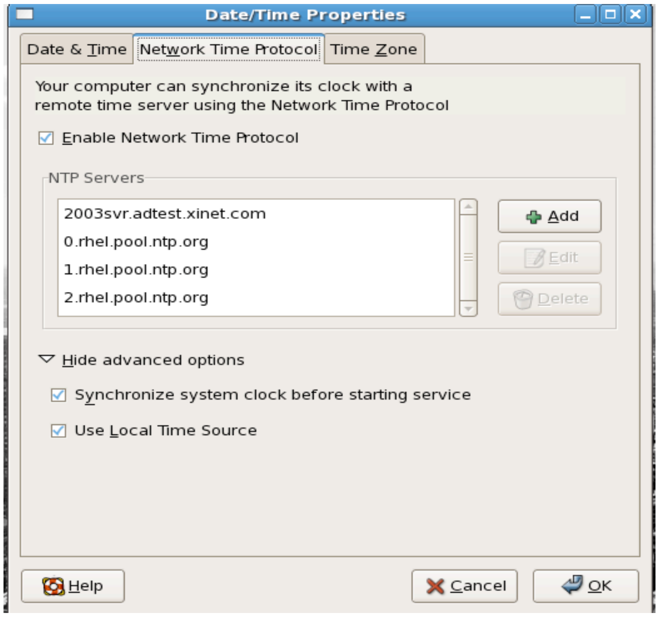
Secondary DNS: 192.168.11.41

Tertiary DNS:

DNS search path: xinet.com

Active profile: Common (modified)

- Make sure the date / time on your RHEL5 server is synced to the AD server. In order to do this, set your AD server as your ntp server in the Date/Time panel, and check the option to synchronize system clock before starting service. In the screenshot below, the AD server is 2003svr.adtest.xinet.com.



Your computer can synchronize its clock with a remote time server using the Network Time Protocol

☑ Enable Network Time Protocol

NTP Servers

2003svr.adtest.xinet.com
0.rhel.pool.ntp.org
1.rhel.pool.ntp.org
2.rhel.pool.ntp.org

Hide advanced options

☑ Synchronize system clock before starting service

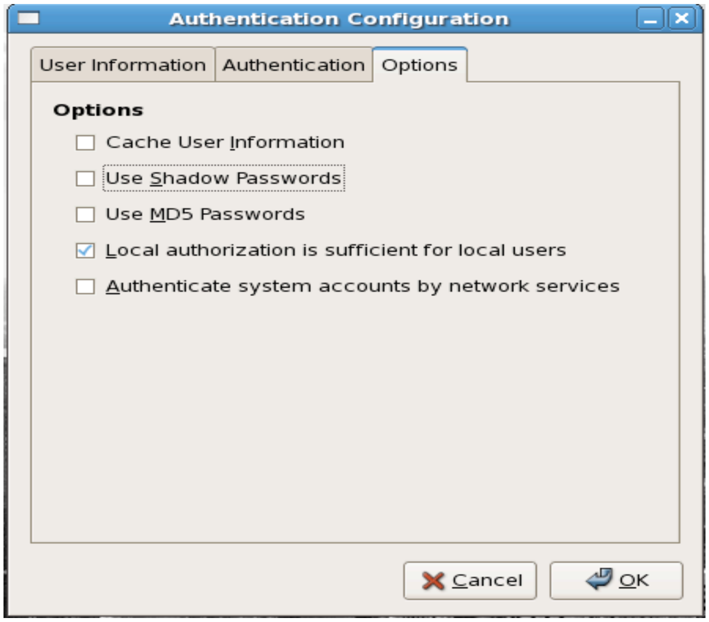
☑ Use Local Time Source

Once the preparation steps are complete, you are ready to bind your server to Active Directory.

Binding to Active Directory

Run the Authentication GUI tool on the RHEL5 server, in System | Administration | Authentication. You will see a screen similar to the one below. Set the options as shown below and move on to the next screen when finished:

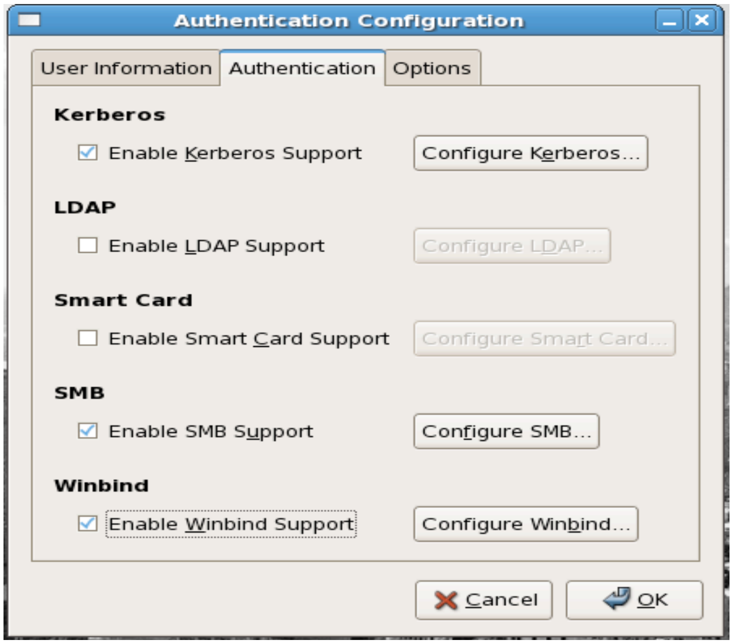
In the 'Options' tab, check the option "Local authorization is sufficient for local users."



Options

- ☐ Cache User Information
- ☐ Use Shadow Passwords
- ☐ Use MD5 Passwords
- ☑ Local authorization is sufficient for local users
- ☐ Authenticate system accounts by network services

In the 'Authentication' tab, enable Kerberos, SMB and Winbind.



Kerberos

- ☑ Enable Kerberos Support

LDAP

- ☐ Enable LDAP Support

Smart Card

- ☐ Enable Smart Card Support

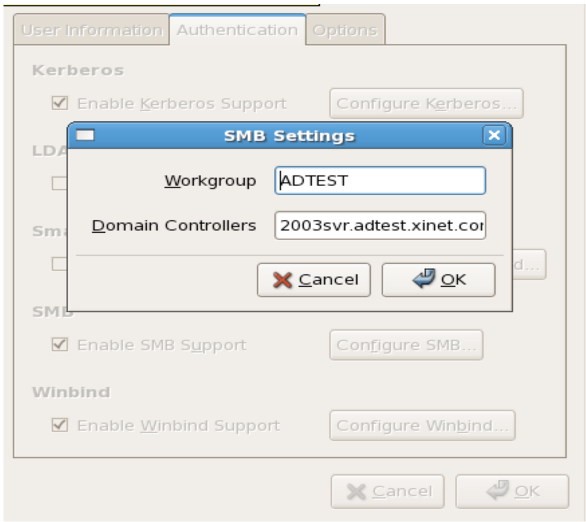
SMB

- ☑ Enable SMB Support

Winbind

- ☑ Enable Winbind Support

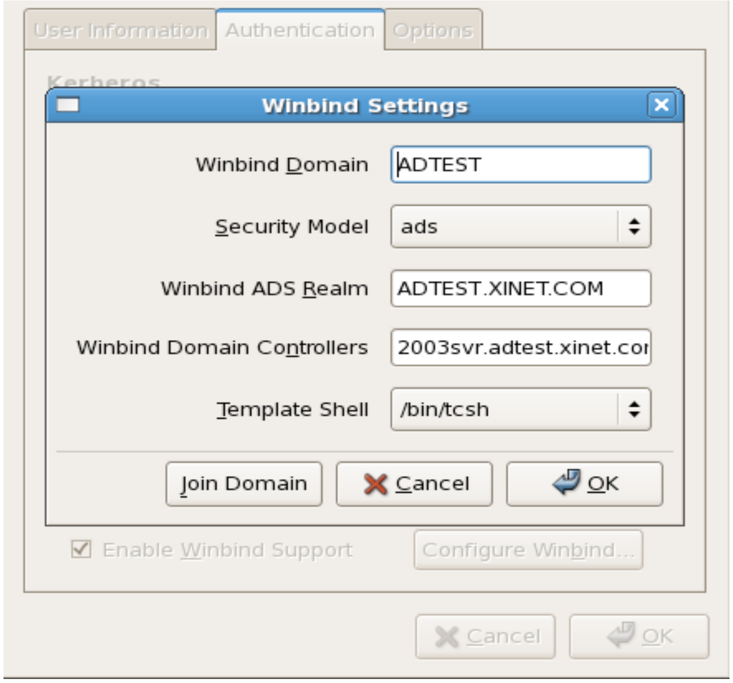
Click the ‘Configure Samba’ button. Fill in the workgroup and domain controllers. In our example, the workgroup is ‘ADTEST’ and the domain controller is ‘2003svr.adtest.xinet.com’. Click OK when finished.



Workgroup ADTEST

Domain Controllers 2003svr.adtest.xinet.coı

Click the ‘Configure Winbind’ button. In the ‘Winbind Domain’ field, enter the NetBIOS name for the domain. In the ‘Security Model’ pulldown, select ‘ads’. In the ‘Winbind ADS Realm’, type in the FQDN (fully qualified domain name) of the domain. In ‘Winbind Domain Controllers’ type in the FQDN of the domain controller, and set a template shell. Click OK when finished to close the window. Note: do not click ‘Join Domain’ at this time, because if it fails, you won’t see debug information. Later we will join the domain via the command line.



Winbind Domain ADTEST

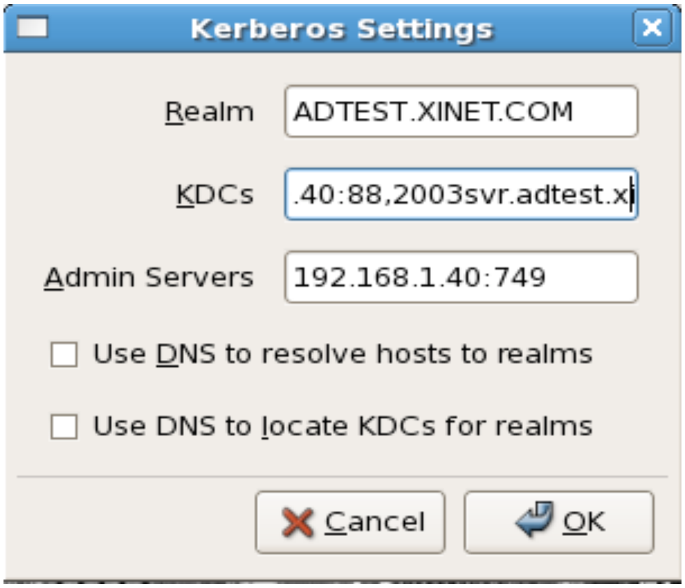
Security Model ads

Winbind ADS Realm ADTEST.XINET.COM

Winbind Domain Controllers 2003svr.adtest.xinet.coı

Template Shell /bin/tcsh

Click the ‘Configure Kerberos’ button. In ‘Realm’ type in the FQDN of the domain. In KDCs (Key Distribution Center) type in the IP address of the domain controller with port 88, then the FQDN of the domain controller separated by a comma. In our example, it is ‘192.168.1.40:88,2003svr.adtest.xinet.com’. In ‘Admin Servers’ type in the IP address of the domain controller with port 749. Click OK when finished to close the window.



Realm: ADTEST.XINET.COM

KDCs: .40:88,2003svr.adtest.x

Admin Servers: 192.168.1.40:749

□ Use DNS to resolve hosts to realms

□ Use DNS to locate KDCs for realms

You should be returned to the ‘Authentication Configuration’ window. Click ‘OK’ to save the settings. We need to do more configurations before we restart winbind and samba for the above configurations to take effect.

Edit /etc/samba/smb.conf file from command line.
Find the line “winbind use default domain = false’ and add these two lines after it:

```
        winbind enum users = yes
        winbind enum groups = yes
```

Save and close the smb.conf file.

Edit /etc/nsswitch.conf file from command line.
Find these 3 lines:

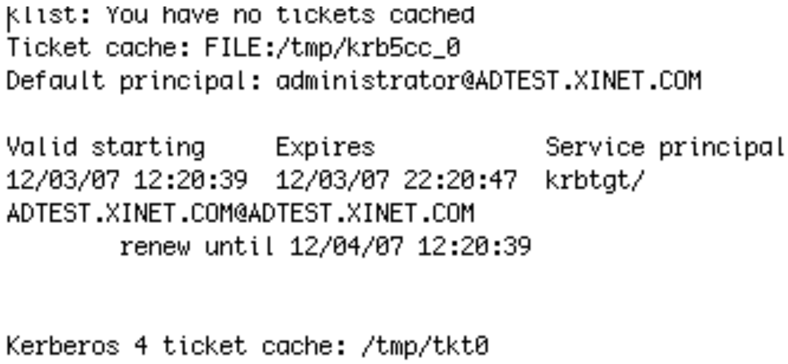
```
       passwd:  files
       shadow:   files
       group:  files
```

and change them into:

```
      passwd: files winbind
      shadow:  files winbind
      group:  files winbind
```

Save and close the nsswitch.conf file.

From the command line, run ‘klist’ to verify there are no Kerberos tickets. (If there are tickets, run ‘kdestroy’ to remove them). Create new Kerberos tickets by typing ‘kinit administrator@FQDN’ (replace FQDN with the FQDN of your domain). In our example, the command is ‘kinit administrator@ADTEST.XINET.COM’. After running this command, the output of ‘klist’ look similar to the following:



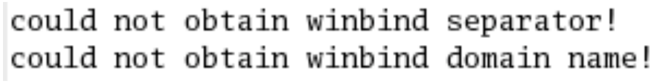
```
klist: You have no tickets cached
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@ADTEST.XINET.COM

Valid starting     Expires            Service principal
12/03/07 12:20:39  12/03/07 22:20:47  krbtgt/
ADTEST.XINET.COM@ADTEST.XINET.COM
        renew until 12/04/07 12:20:39


Kerberos 4 ticket cache: /tmp/tkt0
```

Note: you may get an error that says the clock skew is too great between the FullPress server and the AD master. In order to correct this, restart ntpd dameon by issuing the command ‘service ntp restart’. If any step returns the output of ‘FAIL’ re-run the command.

From command line set the username and password used by Winbind, then verify it by running the following commands:

‘wbinfo --set-auth-user administrator’
‘wbinfo --get-auth-user’ to verify the account used is administrator.

There may be errors like the following during the set-auth-user command:



```
could not obtain winbind separator!
could not obtain winbind domain name!
```

These error messages don’t seem to affect the binding process.

Join the domain by running the net command. You should see output similar to the following:

```
[RHEL5_server/]$ net ads join –U administrator
administrator’s password:
Using short domain name -- ADTEST
Joined 'RHEL5_server' to realm 'ADTEST.XINET.COM'
```

From the command line, restart Samba and Winbind services and make sure they are successfully started by issuing the following command:

```
‘service smb restart’
‘service winbind restart’
```

Now your RHEL5 server should be bound to Active Directory.

To test it, make sure ssh is enabled on the RHEL5 server. Then, from a separate unix workstation, you should be able to login to the RHEL5 server via ssh using an AD account.

You can also try running the following commands:

```
[RHEL5_server/]$ wbinfo –u
…
[RHEL5_server/]$ getent passwd
…
[RHEL5_server/]$ getent group
```

After each command, you should see a listing of AD users and groups, respectively.

If these tests fail, you may need to restart Winbind again.

Note: you may get a series of errors about a home directory not being present when logging in via ssh using an Active Directory account. This can be resolved by making changes to certain files in /etc/pam.d.   However, this does not affect functionality with Xinet products, so details on how to do this are outside the scope of this technote.

2. Configuring FullPress and WebNative

Part I: FullPress

If you plan to install Xinet products on a version of Red Hat 5, you must install other versions of Red Hat libraries before the Xinet software will work. We suggest you install the libraries before installing Xinet software. If you have a support contract with Red Hat, you can easily download the libraries from the Red Hat web site. You need to install the following. Newer versions might be available:

- compat-libstdc++-33-3.2.3-61.i386.rpm
- libXp-1.0.0-8.i386.rpm
- openmotif22-2.2.3-18.i386.rpm
- openssl097a-0.9.7a-9.i386.rpm

On 64bit RHEL 5, you have 2 options to make FullPress authenticate through Samba:

Option 1: Use the 32bit version Samba suite, which includes the packages samba, samba-common, and samba-client. (If the operating system already has the 64bit Samba suite installed, you may have to uninstall them first then install the 32bit version.)

Option 2: Use the 64bit version Samba suite, then install those additional 32bit libraries of the same version as the running samba version on the RHEL5 server.
/lib/security/pam_winbind.so
/lib/libnss_winbind.so.2
/lib/libnss_wins.so.2

you can run ‘smbd –V’ to find out the running samba’s version. The needed 32bit libraries usually can be found in that version of ‘samba-common’ 32bit RPM. For example, in our tests ‘smbd –V’ gave ‘Version 3.0.25b-1el5_1.4’, so we found the 32bit samba-common-3.0.25b-1el5_1.4.i386 RPM from Redhat network, then used the command ‘rpm –I --replacefiles samba-common-3.0.25b-1el5_1.4.i386.rpm’ to install those libraries. This method also proved to work with the 3.0.23c-2 version. However, there is a chance that other versions of Samba will not work exactly this way.

Once the libraries are there, install and license FullPress.

Since FullPress relies on /etc/pam.d/other, (as opposed to /etc/pam.d/login), you will need to make sure the contents of ‘other’ matches ‘login’.

First, back up ‘other’:

```
[RHEL5_server/]$  cp /etc/pam.d/other /etc/pam.d/other.backup
```

Then, overwrite other with the contents of login:

```
[RHEL5_server/]$  cp /etc/pam.d/login /etc/pam.d/other
```

Once this is done, you should be able to mount FullPress volumes using Active Directory accounts. Once you have defined volumes in the FullPress Admin GUI, you can attempt to mount volumes from a Mac workstation using an Active Directory account username and password.

Notes:

- If you only have one domain, you can set the default domain option in smb.conf to ‘yes’   To do this, add this line to the “Share Definitions” section of the file:

  ```
  winbind use default domain = yes
  ```

  This way, users (including FullPress users) will not have to type in the domain name. For example, instead of typing this:

  ADTEST\cchelios

  …they could type this:

  cchelios

Part II: WebNative

Only do this after installing and configuring FullPress.

1. Install WebNative and make sure it is licensed.

2. Confirm that you are running Apache 2.2.x. You can do this by running the following command. Your output should look similar to the following (we happen to be using 2.0.52):

```
[RHEL5_server/]$ /usr/sbin/httpd -v
Server version: Apache/2.2.3
Server built:   Nov 29 2006 11:45:10
```

Versions below 2.2 have not been tested on RHEL5 and may not work.

3. Download Xinet Apache module, called ‘mod_auth_xinet2.so’. Select the one for the Linux RHEL5 32bit platform or the one for RHEL5 64bit.   Modules for all platforms are available on the TechNote 218 web page.

Copy ‘mod_auth_xinet2.so’ to ‘modules’ folder for Apache. By default the modules folder is located at /etc/httpd/modules.

Confirm that permissions for ‘mod_auth_xinet2.so’ are similar to other modules in that folder. If not, please make the necessary changes.

4. Make a backup of /etc/httpd/conf/httpd.conf.

5. Edit /etc/httpd/conf/httpd.conf file to load the Xinet Apache module.

To do so, comment out any authentication related modules in httpd.conf. For example:

```
#LoadModule auth_basic_module modules/mod_auth_basic.so
#LoadModule auth_digest_module modules/mod_auth_digest.so
#LoadModule authn_file_module modules/mod_authn_file.so
#LoadModule authn_alias_module modules/mod_authn_alias.so
#LoadModule authn_dbm_module modules/mod_authn_dbm.so
#LoadModule authn_default_module modules/mod_authn_default.so
…
#LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
#LoadModule authz_dbm_module modules/mod_authz_dbm.so
#LoadModule authz_default_module modules/mod_authz_default.so
#LoadModule ldap_module modules/mod_ldap.so
#LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
```

Then, continue to the end of the LoadModule section. Add this line, so it is loaded last:

```
LoadModule auth_xinet_module modules/mod_auth_xinet2.so
```

6. Next, you will make changes to Xinet-related entries further down in the document.

Search for this line:

```
    AuthUserFile /var/adm/webnative/apache.userfile
```

Change it to:

```
    XinetAuthUserFile /var/adm/webnative/apache.userfile
```

The line appears three times in total. Change all three instances of it.

7. Restart Apache by running:

```
[RHEL5_server/]$ /usr/sbin/apachectl restart
```

While Apache is loading module auth_xinet2.so it may complain that it can’t find library ‘libldap.so.2’. Usually that library is in /usr/lib directory. If the library is not there, make a symbolic link of it to the latest libldap version. In our example, the latest ldap library is libldap-2.3.so.0.2.15, so we did ‘ln –s libldap-2.3.so.0.2.15 libldap.so.2’. After that, restart apache again.

8. Create a system.userlist file

In order for WebNative to pull the user information from Active Directory, you will need to create a blank file named system.userlist by running this command in the terminal:

```
[RHEL5_server/]$  touch /usr/etc/webnative/system.userlist
```

Note that once you do this, any local WebNative accounts will no longer appear in WebNative Administration.   Only accounts from Active Directory will appear. Also, the “New Users” and “Delete Users” tabs will no longer be accessible under the “Users” tab. This is because all administration of users should be done on Active Directory.

At this point you should see all your AD users when you login to Nativeadmin.

Note: In the past, creating a file called system.grouplist was an option to help speed up the time it took to display users. However, that functionality has been incorporated into system.userlist. If you are upgrading from past versions to 8.03, we recommend you to log in WebNative as nativeadmin and visit the ‘Groups’ tab; any editing, such as a simple save, will prompt the system to incorporate groups information into system.userlist file.

As of 15.03, in some cases FullPress will also consult system.userlist file to filter out groups that are not in it. If you don’t want this behavior, you can modify the Xinet services file and add this option ‘-groupfile no’ as the first option to ksd.