

# Unite your Linux and Active Directory Authentication

By Eric Andersen

Authentication is easily one of the most critical services provided by your network infrastructure. It is the gatekeeper for every resource on your network. Workstations, applications, printers, and files would all be open to the world without a system of ensuring that only those people who need any given resource can gain access to it. Once you have accepted the fact that you need authentication, you must decide whether to stay with one network operating system in the interest of a completely homogenous network, or accept a "best of breed" system that will better fulfill your needs, even though it will complicate your environment. If you choose the second option, often times you are left with a management nightmare, where you have two, three, or even more authentication engines to maintain across your network operating systems.

One way of simplifying your authentication environment is to use a single authentication source for all of your nodes -- Windows, Linux, or Unix. You can authenticate them all against a directory service such as Active Directory or eDirectory. In this article, we'll describe how to unify your Linux and Active Directory environments. With minor changes, this same procedure can be used to authenticate your Linux hosts against eDirectory or any other LDAP compliant directory service.

For the purposes of this article, we have used Fedora Core 1 as a Linux operating system, Windows Server 2003 (in native mode) as the Active Directory Controller, and Microsoft's Services for Unix 3.5 to simplify the extension of the schema. Your Windows 2003 server should be installed as an Active Directory Controller, and your Fedora device can be just a basic installation with the OpenLDAP client tools and libraries. You'll also need updated NSS\_LDAP software; the NSS\_LDAP software included in the release has a bug that disables schema mapping.

## Preliminary Windows procedures

In this section, we are going to perform the procedures on the Windows device that are a prerequisite to the use of AD to authenticate Linux against Active Directory. These tasks include the installation of Services for Unix, which will perform a schema extension for us.

1. Authenticate to the domain controller as a user that has schema admin rights.
2. Take note of the structure of your directory service. Specifically, we are looking to note the location of your user and group objects. These objects are often located in a container similar to the following:

```
CN=UserContainer,DC=NetBIOSDomain,DC=DNSDomain,DC=DNSSuffix Or  
CN=UserContainer,DC=DNSDomain,DC=DNSSuffix For example:  
CN=Users,DC=LanRx,DC=com Or CN=Users,DC=LanRxDomain,DC=LanRx,DC=com
```

3. Extract the files from Microsoft's Services for Unix 3.5 to a location such as c:\temp\sfu
4. Run c:\temp\sfu\setup.exe to install the Services for Unix software -Accept the standard installation -Where prompted for "security settings", leave both boxes blank -Where prompted for "username mapping" select "Local Username Mapping Server" and subsequently "Network Information Services" -Select the Windows Domain Name -Reboot server when complete

# Unite your Linux and Active Directory Authentication

By Eric Andersen

5. Create basic user for LDAP bind. We recommend that you set the password to not expire, and that the user not be allowed to change the password. This account should be used only for binding the Linux device to the Active Directory.

## Linux integration

Next, we configure the Linux workstation to perform a pure LDAP authentication against the Active Directory controller. We first install the software to permit us to perform schema mapping, then authenticate as superuser. Next, we run `rpm -Uvh nss_ldap-207-6.i386.rpm` to install the new NSS\_LDAP package (or upgrade if it was already installed). Now we configure the LDAP client on the Linux device to map the POSIX information to point to the domain controller to collect the appropriate attributes within Active Directory:

1. Run `mv /etc/ldap.conf /etc/ldap.orig` to backup your existing `/etc/ldap.conf` file.
2. Run `vi /etc/ldap.conf` to create your `ldap.conf` file.
3. Ensure that the following lines exist in the `ldap.conf` file. These lines will provide the mapping for the PAM/NSS objects to pull the appropriate Unix POSIX attributes out of Active Directory in a manner that can be used by the PAM modules.

```
host 192.168.100.18
base cn=Users,dc=lanrx,dc=com
binddn cn=dirsearch,cn=Users, dc=lanrx,dc=com
bindpw Directory
scope sub
ssl no
nss_base_passwd cn=Users,dc=lanrx,dc=com?sub
nss_base_shadow cn=Users,dc=lanrx,dc=com?sub
nss_base_group cn=Users,dc=lanrx,dc=com?sub
nss_map_objectclass posixAccount user
nss_map_objectclass shadowAccount user
nss_map_attribute uid sAMAccountName
nss_map_attribute uidNumber msSFU30UidNumber
nss_map_attribute gidNumber msSFU30GidNumber
nss_map_attribute loginShell msSFU30LoginShell
nss_map_attribute gecos name
nss_map_attribute userPassword msSFU30Password
nss_map_attribute homeDirectory msSFU30HomeDirectory
nss_map_objectclass posixGroup Group
nss_map_attribute uniqueMember msSFU30PosixMember
nss_map_attribute cn cn
pam_login_attribute sAMAccountName
pam_filter objectclass=user
pam_member_attribute msSFU30PosixMember
pam_groupdn cn=unixusergroup,dc=lanrx,dc=com
pam_password ad
```

Above, notice the line for `pam_groupdn`. It specifies that any user to gain access to this server needs to be a `posixMember` of this particular user group. Upon successful authentication, the

# Unite your Linux and Active Directory Authentication

By Eric Andersen

system will verify that the authenticated user is a member of the appropriate group. If the user is a member, authentication will occur. If the user is not a member, the system will notify the user that he needs to be a member of the specified group to authenticate entirely.

4. Run `vi /etc/nsswitch.conf` to edit the nsswitch configuration file. Ensure that the following lines are configured as follows:

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

5. Run `authconfig` to perform the configuration of "Pluggable Authentication."

**Note: To the best of my knowledge, `authconfig` is specific to Red Hat Linux distributions. For a sample system-auth configuration file, please see the example configuration file package associated with the article.**

- a.) Select LDAP to provide NSS information
- b.) Select "Use LDAP"
- c.) In the "Server" field, confirm that the IP address of the domain controller appears.

**Note:** Do NOT select TLS. TLS is not supported with Active Directory until Certificate Services is installed. It is possible to leverage TLS within this infrastructure, but outside the scope of this document.

- d.) In the "BaseDN:" field, add the location of your user accounts to have access to this device i.e. "cn=Users,dc=ad,dc=lanrx,dc=com"
  - e.) Click Next
  - f.) Select LDAP to provide authentication
  - g.) Select "Use Shadow Passwords"
  - h.) Select "Use MD5 Passwords"
  - i.) Select "Use LDAP Authentication"
  - j.) DO NOT SELECT "Use TLS"
  - k.) Server should be prepopulated with the domain controller
  - l.) BaseDN should also be prepopulated with the user location
  - m.) Select OK
6. This process writes the `/etc/pam.d/system-auth` file. Once this process has been completed, you will want to prepend the following lines into the system-auth file prior to the account components.

**Note: This line provides us with the ability to authenticate locally as superuser in the event of a network failure.**

```
account sufficient /lib/security/pam_localuser.so
```

# Unite your Linux and Active Directory Authentication

By Eric Andersen

## Active Directory object management

As is the case with any other authentication mechanism, we need to configure the user objects for the users that are to use the system. However, if you are implementing this solution, more than likely your users already have Windows accounts. In that case, all we need to do is to modify the objects to be POSIX compliant.

1. Open the Active Directory Users and Groups management tool.
  - a.) Modify a group object to function as a POSIX group.
  - b.) Right-click on the user group for assignment of a GID.
  - c.) Click on the Unix Attributes tab.
  - d.) Populate the NIS Domain dropdown and the GID number as appropriate.
2. Modify a user object to function as a POSIX user.
  - a.) Locate and activate the tab that says Unix Settings.
  - b.) Under Unix Settings, set the UID and GID for the user, as well as the home directory location (on the Linux filesystem /home/). Note: You will need to ensure that the directory exists with the appropriate user object having access to the directory.
  - c.) Reset the user's password. This causes the AD password and the Unix password attributes to synchronize.
3. Add the user as a Unix member of the group.
  - a.) After you have added the user as a Unix user, you will also need to come back to the group properties and add the user as a member on the Unix Attributes tab. Otherwise, the user will not be populated in the msSFU30PosixMember attribute.
4. This user should now be able to authenticate onto the Linux machine via any desired mechanism, including an SSH session. One thing that can sometimes cause problems authenticating is to have the POSIX home directory be unavailable or not exist. Either you can create the directory manually, or you can run a script to collect the home directories and ensure that the directory exists.

## Mission: Accomplished

At this point, you should have been able to provide authentication for your user objects against an Active Directory. If you would like example configuration files, you can reach them online with this article. Our intention was to help you find your way in Active Directory authentication. This by no means is a solution for everybody. For instance, many organizations will want to perform all LDAP communication over SSL/TLS, which adds a touch of complexity to your implementation due to some limitations on different software packages. If you experience issues pertaining to your implementation, you are welcome to visit our forums with questions.