

Using Server for NIS, IdMU and Kerberos for Unix/Linux directory and authentication services

Tech Note #2 in the "Identity Management" series

By Doug Miller (Interop Systems)

Scenario

The scenario for this tech note is as follows. You have Active Directory installed on Windows Server 2003 R2 and use Active Directory to provide directory and authentication services to Windows-based clients. You also have Linux and UNIX installed in the same datacenter and you wish to use Active Directory as your central system for providing consistent directory and authentication services to these systems as well. In the past you have used NIS for centralized directory services on UNIX. Ultimately you want to have one centralized account entry and password for each user and group in Active Directory and have users and systems able to leverage the account information and credentials from Windows, UNIX and Linux client systems.

Solution Overview

This solution uses NIS (Network Information Service) technology for user and group information look-ups. NIS has been used on UNIX systems for many years and is a standard part of virtually every Linux and UNIX system. NIS support is also built into Windows Server 2003 R2 and Microsoft Windows Services for UNIX. Kerberos is used for authentication and password validation in this solution. Kerberos is the default system for authentication for modern Windows domains and is also widely used and included in most UNIX and Linux systems. The final solution will allow users to log into UNIX and Linux systems using their Windows account name and password via Active Directory. In addition, UNIX specific information such as the user's shell is also stored in Active Directory and used during the login session. This solution can also lay the groundwork for enabling true single sign-on capabilities through the use of Kerberos-enabled utilities on UNIX.

Solution Implementation Details

To implement this solution we used Microsoft Windows Server 2003 R2 Standard Edition with Service Pack 2 as the server environment. This server was configured with the following capabilities installed and enabled:

- Active Directory Domain Controller
- DNS Server
- DHCP Server
- Active Directory Services: Identity Management for UNIX (which includes Server for NIS)
- Other Network File and Print Services: Microsoft Services for NFS (which includes the User Name Mapping service)

On the client side, we installed Fedora Core Linux 6. The key packages that were leveraged for this solution include:

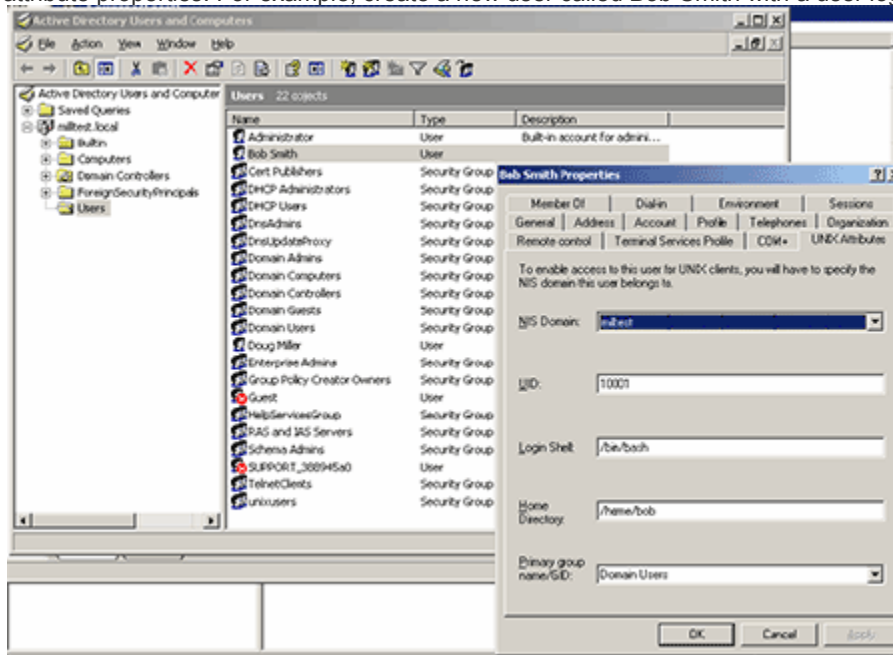
- krb5-libs
- pam_krb5
- krb5-workstation

The required NIS client components are installed by default on Fedora Core. For other systems, you may need to install NIS client software separately. This tech note assumes that you are familiar with the basic administration concepts for both Windows Server and Fedora Core Linux.

Setting up Windows Server 2003 R2

We begin by setting up the environment on the Windows Server system. Complete the following steps on your Windows Server system:

1. Install Windows Server 2003 R2 and accept the standard options during the install.
2. Using the “Manage Your Server” wizards, set up the server as a first server which means installing and configuring the system as an Active Directory Domain Controller, DNS Server and DHCP Server. For this implementation, we called our domain “milltest”.
3. Using the “Add or Remove Programs” tool in the Control Panel, add the following components:
 - Active Directory Services: Identity Management for UNIX. Be sure that “Server for NIS” and “Administration Components” are installed as part of this package.
 - Other Network File and Print Services: Microsoft Services for NFS. It is recommended that you install all the components of this package although technically you do not need all the NFS components.
4. Run the program: All Programs à Identity Management for UNIX à Microsoft Identity Management for UNIX. This MMC plugin is the key interface for configuring the Server for NIS service. Enable the “Server for NIS” service by right clicking on “Server for NIS” and selecting “Start Service”.
5. Run the program: All Programs à Administrative Tools à Active Directory User and Computers. For this example implementation, create a Security Group called “unixusers” and open the properties for this group. Click on the UNIX Attributes tab for “unixusers” and select the default domain name for your NIS Domain (which should be the same as your Active Directory domain) and enter a GID such as 10000. Click OK to save your changes to this new group. You could also enable an existing group such as “Domain Users” however some UNIX systems are not able to handle group names beyond a certain length or ones that have spaces in the name.
6. For each Active Directory user that you want to enable for UNIX logins, you will need to configure their UNIX attribute properties. For example, create a new user called Bob Smith with a user logon name of “bob”.



Give “bob” a password and uncheck the “User must change password at next logon” option. Open the properties for user “Bob Smith” and select the UNIX Attributes tab. For the NIS Domain field, select the default domain name. The rest of the attributes should be automatically filled in; however you can change these to suit your needs. For example, you could change the Login Shell to “/bin/bash”. The primary group name should be set to

“unixusers” or another group that is UNIX enabled. In our example, we set the primary group to “Domain Users” since Fedora Core Linux support long group names and group names with spaces.

7. Run the program: All Programs à Administrative Tools à Microsoft Services for Network File System. This MMC plug-in is the key interface for configuring the NFS and User Name Mapping services. Enable the “User Name Mapping” service by right clicking on “User Name Mapping” and selecting “Start Service”. Now, right click on “User Name Mapping” and select Properties. Under the “UNIX User Source” tab, ensure “Use Network Information Service (NIS)” is enabled. Now, select the “Simple Mapping” tab and make sure “Use simple maps” is checked and your domain name is selected as the Windows domain. Click on “Add...” at the bottom of this dialog box to add a new NIS mapping. The defaults that are provided should be fine which will have your Windows domain name in lower case listed as the NIS domain name, the NIS server should be the name of the Windows server you are working on and the Windows domain name should be the domain name in all upper case. Hit Apply and then go back to the “UNIX User Source” tab and select “Synchronize Now”.
8. Right click on “User Maps” and make sure that “Show simple maps” is selected and do the same for “Group Maps”. You should see the enabled users and groups in the right panel. It is also possible to set up more complex maps between Windows user names and UNIX user names. See the Microsoft nfmgmt help system for more information if you need to do this.
9. There are no special steps required to enable Kerberos services for UNIX clients.

Your Windows Server system is now ready to provide NIS directory services and Kerberos authentication services to UNIX and Linux clients.

Setting up Fedora Core Linux

The next step is to set up a Linux system as a client for Active Directory services. In this case, the Linux client can be either a Linux desktop or server. The term client refers to how the Linux system is configured to use Active Directory client services from a Windows server system. Complete the following steps on your Fedora Core Linux system:

1. Install a standard version of Fedora Core Linux. We used most of the defaults for our install. Make sure that the Kerberos (krb) packages are installed on your system.
2. Use DHCP to get an IP address from Windows Server by providing the IP address for the Windows Server system when prompted for the DHCP server. Alternatively, you can hard code an IP address in the same network as the Windows domain.
3. Make sure the DNS client is set up to use the Windows Server domain controller (normally automatic if DHCP is used). Check the /etc/resolv.conf file once you have installed Linux to be sure that DNS is configured correctly.
4. Configure your Linux system to use the Network Time Protocol and set it to use the Windows Server IP address as the first NTP Server. This is done on Fedora by running System >> Administration >> Date & Time. It is essential to have the Linux system clock synchronized with the Windows Server clock, otherwise Kerberos authentication will not work correctly.
5. Run the program: System >> Administration >> Authentication. This tool assists with configuring the appropriate directory and authentication services for your Fedora system.
 - Click on the “User Information” tab, check “Enable NIS Support” and uncheck any other options.
 - Configure NIS with the Windows domain name and IP address for the Windows Active Directory controller.
 - Click on the “Authentication” tab and check “Enable Kerberos support” and uncheck any other options.
 - Click on “Configure Kerberos ...” and fill in Kerberos fields with:

- Realm = Windows domain name in upper case
 - KDCs = the fully qualified domain name of the Windows domain controller appended with :88.
 - Admin Servers = fully qualified domain name of the Windows domain controller appended with :749.
 - Check the two DNS options, “Use DNS to resolve hosts to realms” and “Use DNS to locate KDCs for realms”.
 - Click on the “Options” tab and check “Cache User Information” and “Local authentication is sufficient for local users”
 - Click on OK to save all changes.
6. Once the changes have been made using the Authentication tool, check the various `/etc/krb*` files to ensure that there are no example realm entries in the files. These should just contain information relevant to connecting to the Windows Server system.
 7. It is useful to add an extra entry to the file `/etc/pam.d/system-auth` to enable the creation of home directories on first login to the Linux system by a user. In the session section of this file towards the end, add the line:

```
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

Your Fedora Linux system should now be configured to use the NIS services on Windows Server for user and group information directory services and Kerberos authentication using the KDC on Windows Server. In order to test the setup, use “`getent passwd`” command to confirm that you can see both local users that exist in `/etc/passwd` and Windows domain users from Active Directory. You will only be able to see Active Directory users if the Active Directory user has been enabled as a UNIX user in the “Active Directory Users and Computers” MMC on Windows Server.

You should now test whether the setup is working correctly by logging in to the Linux system using a UNIX-enabled Active Directory account name and password. If the user has no home directory on the system, it should be automatically created for them. If the login fails, double check that the clocks are synchronized to the same time on both Windows and Linux and that all services mentioned above are enabled. If the clocks are off by even a few minutes, then Kerberos will not work correctly.

Summary

By implementing this solution, you will substantially reduce the management overhead for account and authentication management for heterogeneous Windows and Linux environments. Users now have one account name and password to remember for logging into both Windows and Linux. Administrators can setup new user accounts for both Windows and Linux by simply adding a single new account entry into Active Directory. Administrators can also deny access to all systems for any user by simply disabling their Active Directory account. Policy settings such as password complexity and length requirements are now enforced for users on both Windows and Linux. Deploying new Linux systems is simplified since administrators no longer need to set up individual user accounts for every new Linux machine.

There are two other methods for solving the Windows/UNIX/Linux Active Directory integration challenge that are presented in this series. If you wish to use Samba instead of NIS for storing user information then you should read the tech note titled: “Using Samba client technology and Kerberos for Active Directory-based identity management”. If you wish to use LDAP for storing user information then you should read the tech note titled: “Using native LDAP, native Kerberos and Windows Server 2003 R2 Active Directory services and schema for cross-platform identity management”.

If you have comments on these tech notes or wish to provide enhancements or corrections, please free to post a question in the [Interop Community](#) forums.