Notes from the Cross Platform / Network Authentication & SAMBA BOF

These are notes taken from a rough draft by Del during the BOF session. The BOF was moderated by Del, Andrew Tridgell, and Jeremy Allison.

A Linux Only Solution

OpenLDAP

A Linux Only solution for networked authentication would use the following components:

- OpenLDAP, latest release from http://www.openldap.org/
- nss_ldap and pam_ldap from http://www.padl.com/
- PAM and NSS configured appropriately to use a central authentication and NSS store in OpenLDAP. This works quite nicely.

SAMBA

Current Status

2.2.3a of SAMBA has just been released. For more information see the web site: http://www.samba.org/ or your closest mirror.

This release includes bug fixes and some updated schema documentation. There is also some new documentation.

LDAP

This release of SAMBA can have an LDAP back end.

There are extensions to this version of SAMBA which allow such things as the SMP passwords (or the MD4 hashes thereof) to be stored in an LDAP directory. The release notes make some mention of this and indicate where to find the appropriate documentation.

WINBIND

WINBIND is an NSS solution which can use a SAMBA or NT PDC back end as an NSS server for Linux machines.

This uses the NT domain model, and not LDAP, as its repository.

WINBIND ships with SAMBA.

A demonstration of WINBIND was made during the BOF session, and a diagram of how WINBIND works was made, which is not included here.

NDS

NDS LDAP server	Since NDS version 8.0 (NetWare version 5 and later, also available for Windows NT, 2000, Linux, and Solaris), NDS has been a standards compliant LDAP server.
Client end	Linux clients of NDS work fine with the nss_ldap and pam_ldap modules available from http://www.padl.com/ An NT and Windows client is available. Using NDS as an authentication only system "eDirectory" costs $US2 per user.
NDS / Account Management / Corporate Edition	The product formerly known as anything from NDS, to NDS corporate edition, is now known as eDirectory Account Management. This gives more advanced features and includes an nss_nds and pam_nds module which also comes in a single-sign on version. This costs $US26 per user.

Microsoft Active Directory (MAD)

Credit

I "borrowed" the acronym "MAD" from a Novell salesperson. I don't believe that it's the official Microsoft approved acronym.

Server

Active Directory of course only runs on Windows 2000 or XP servers.

Client

There are active directory clients for Windows 2000 and XP. Microsoft originally planned to introduce an active directory client for NT but later scrapped the idea.

Note that older workstations running NT, 98, or 95 can join a non-native-only mode Active Directory network as if it were an NT domain network, because Active Directory also works in "downlevel" mode to support these clients.

SAMBA

It is possible to set up SAMBA version 3.0 as an active directory client -- essentially getting a SAMBA 3.0 server to join an active directory network as a server.

WINBIND from SAMBA 3.0 also supports NSS functions using an Active Directory back end, however this is also possible with nss_ldap.

Linux

Linux can use the nss_ldap and pam_ldap to become an Active Directory client in the same way as it becomes an OpenLDAP client. The Microsoft schema breaks several IETF schema conventions, and so a very recent version of nss_ldap is required, with some modifications to the ldap.conf file to support schema mapping.

Anyone interested in doing this should go here:

http://www.css-solutions.ca/ad4unix/

Replacing Active Directory with OpenLDAP

New Project

A new project was started today to add some schema extensions and additional code to a (probably forked) release of OpenLDAP that would make OpenLDAP appear to be an Active Directory server for the purposes of Windows and SAMBA clients joining the tree.

A lot of work needs to be done on this. Don't hold your breath.