Implementation Panel:  
Active Directory, OpenLDAP, Sun, and Novell

Notes from CAMP Directory Workshop  
February 3-6, 2004 Tempe Arizona

Moderated by: Michael Gettes  
Panel members: Mark Adamson, Robert Banz, Victor Bolet, Allan Huisman  
Scribe: Nate Klingenstein

OpenLDAP

Pros:

It's free.

The word "Open" means the product is open-source. If there's missing functionality and sufficient in-house development resources, it's generally possible to implement that functionality as needed. There is a large community doing this and contributing the code back into the base, leading to an ever-evolving set of functionality.

Cons:

There is still a lot of core functionality other directory products have that OpenLDAP lacks. Notably, the ability for OpenLDAP to put access control into the directory seems to be very weak.

iPlanet

Pros:

The server scalability and performance, especially in higher-load and object environments, is extraordinary. A panelist reported that it "performed just as well with 300,000 entries as with a few test entries." It was impossible to even load that many into OpenLDAP at the time of testing. It should be noted that this is with iPlanet 4.1, a product that is no longer supported or maintained, and not the newer versions.

Cons:

The API interface has been occasionally buggy, causing strange memory leaks when even very simple plug-ins are used. This can cause strange and damaging symptoms such as corruptions in unrelated parts of the directory.

The management tools are very clumsy and difficult to use, and incomplete at the same time. Certain functions, such as maintenance of certificates, can only be done through
the GUI, and sometimes the console stops working entirely. Sun is aware of this and constantly striving to improve the console.

**Novell**

Pros:

Novell on a campus is ubiquitous and very stable. It's also very big, with a large number of features and suite of functionality. This makes it a complete solution with little building and customization needed.

Cons:

A large amount of staff is needed to bring up a Novell environment with eDir/NDS. It would be difficult for campuses with minimal support staff to handle this deployment.

**Active Directory**

Pros:

Active Directory bundles excellent tools with the newest version, which is part of Windows Server 2003. These can accomplish a lot in an environment.

Directly out of the box, AD offers a quick solution with little pain and fairly extensive functionality.

Cons:

Very heavy per user object, Active Directory has scaling problems. While these have been remedied somewhat in 2003, campuses needing a very large number of objects may run into difficulties that cannot be easily addressed. The panelists were careful to remind campuses to keep in mind future potential scaling needs because it's painful to migrate from one directory solution to another once committed.

As with many Microsoft products, it is extremely difficult to extricate the Windows from Active Directory. While this is not an issue in a Windows-only shop, it can cause obvious problems with other operating systems.

**Oracle**

Pros:

Oracle can perform a wide variety of cool referential integrity and data management that most LDAP servers can't provide. It can also apply logic and automatically populate values based on other values, and a host of other useful functionality.

Cons:
LDAP servers are exceptionally fast when it comes to read operations, and have been highly optimized for the directory environment. Even the very quick Oracle databases will have severe issues handling the standard load placed on a campus directory service.

Special Considerations:

A deployment approach that's gaining popularity is to backend an LDAP environment with an Oracle database. The Oracle database is responsible for maintaining identity, attributes, etc., with all the attendant functionality it provides. That information is then fed into an LDAP directory and replicated into the live environment where the production LDAP server can handle the constant load. This approach offers the best of both worlds in many ways. However, it's not advisable to use an Oracle database as a live back-end for an LDAP server; as services beat on the LDAP directory, Oracle will have to handle every query as well and it'll blow up anyway.