Spring, 2007

LTER

01001100 01010100 01000101 01010010

LTER DataBits

Information Management Newsletter of The Long Term Ecological Research Network

01001100 01010100 01000101 01010010

Information Infrastructure: Transitioning Directory Services

- Karen Baker, Jerry Wanetick, Nate Huffnagle, and Mason Kortz (CCE & PAL)

1. Introduction

What is 'Directory Services' and how can we benefit from this technology? Directory Services (DS) addresses 'scaling' up in terms of resources and users, an issue that arises, for example, when an organization grows from a small, dedicated project or laboratory data management group to a larger more complex and interconnected environment. By incorporating Directory Services into the network, we address the need to use and/or to manage an increasing number of users, servers and application services. DS enables the federation of user and application authentication and authorization information over a distributed network of desktop computers and servers. Individuals carrying out research or providing system support for cross-project and cross-program activities often find the type of information system infrastructure provided by DS simplifies the work arena.

Directory Services have been around for a number of years as part of the ISO X.500 series of networking standards. The most popular and ubiquitous of these has been Sun's Network Information Service (NIS). Electronic directory services include Directory Access Protocol (DAP) and Lightweight Directory Access Protocol (LDAP). The LDAP standard is highly customizable. However, this flexibility introduces inconsistencies when manufacturers modify standard configurations to accommodate specialized product functionality, thus building in cross-platform incompatibilities.

The PAL and CCE sites work within the Ocean Informatics (OI) environment. OI is transitioning from NIS to LDAP as part of an ongoing effort to improve the information infrastructure, in this case with a more contemporary Directory Services approach. Based on consideration of the state of industry standards, the transition is centered on the use of Apple's implementation of Directory Services, known as Open Directory (OD) [http://www.apple.com/server/macosx/opendirectory.html]. This approach was selected because it is based entirely on Open Source projects. This contrasts with other approaches such as Microsoft's Active Directory and Sun's Java System Directory.

Open Directory brings together OpenLDAP [http://www.openldap.org], MIT Kerberos [http://web.mit.edu/kerberos], and Simple Authentication and Security Layer (SASL) developed at Carnegie Mellon University [http://tools.ietf.org/html/rfc4422; http://asg.web.cmu.edu/sasl] into a coherent and secure Directory Services framework. Here Kerberos, along with the SASL-based password server, provides a secure authentication method so passwords are never sent across the network. OpenLDAP provides authorization information, enabling central administration for provisioning infrastructure assets. The OD provides these authentication and authorization services across a heterogeneous network of computer architectures, such as: Sun Solaris, Redhat Linux, Microsoft Windows XP (and now, Vista) and Apple MacOSX operating systems.

Packaging services in a more modular, streamlined fashion allows for certain economies of scale. For instance, when a user is authenticated by the Open Directory authentication services, the user is handed a Kerberos ticket (i.e., certificate or credential) that is then used to allow access to the assets that the user is authorized to use. From the user perspective, what was previously a set of machine specific user accounts with separate passwords and account information has been replaced by a "single-sign-on" environment. From a systems administration perspective, asset management is made easier by providing a central means of handling user account and application information. In addition, the collection of services, as well as who has access to these services, are available in the newly centralized schema. Also, by centralizing user authentication and authorization information, the stage is set to implement tokenized or one-time password technologies to allow secure remote access to local infrastructure.

2. Our Local Experience

In a homogenous environment, implementation of native directory services is fairly simple. If the groups associated with Ocean Informatics were completely Mac-based, bringing all of the computers and services under an OD managed environment would be straightforward. However, this is not the case. The PAL/CCE/IOD infrastructure is comprised of Sun Solaris, Redhat Linux, Microsoft Windows XP (and now, Vista) and Apple MacOSX operating systems. The greatest challenge in implementing OD in this environment has been integrating these disparate operating systems into the OD infrastructure. Each platform - Apple, Microsoft, Sun and Redhat - uses a slightly different approach to directory services, though all start from the same standard and are loosely based on similar technologies. By modifying the default Open Directory schema in MacOSX, we are able to bridge the differences between these platforms and to increase interoperability across diverse, heterogeneous networks.

Incorporating these new technologies into a heterogeneous network environment has taken time, that is, it has not been an effortless process. As a bridge between pre-existing or legacy directory services and the new OD framework, we have adopted a long-term approach with a strategy of phased-in implementation to minimize the impact of change on our user base, and to allow for testing as new elements are enacted. The first step, after populating the directory server with user and server information, was to integrate core services such as email, file sharing and user authentication. Subsequently the division's mail server, file sharing/home directory servers, storage servers were integrated into the OD domain. The next step is to integrate client workstations and new servers into the OD domain. For example: when called upon to repair or install new clients or servers, such as when the IOD business office purchased a new server in Fall 2005, these machines are integrated into the OD domain. In upcoming months, the department ftp, web and collaboration servers, and the other independent servers will be integrated into the Open Directory Services. As of January 2007, 80% of legacy servers, 100% of new servers, 40% of existing clients and 40% of new clients have been migrated.

Services currently supported by OD in our local Ocean Informatics environment include email, file sharing (via AFP, SMB, and NFS protocols), print, website authentication (via Apache, mod_auth_apple, and mod_auth_ldap), and user login services. Directory Services minimizes the need for users to track multiple accounts, and also minimizes user account management overhead, thus allowing users to move from machine to machine without the need for an administrator to create a local account and transfer file and settings on each machine.

The pace of change can be measured in phases over a period of years:

Phase 1 (2004) Started planning in summer; mapping NIS schema to LDAP schema
Phase 2 (2004) Synchronize UID/GID space across standalone servers
Phase 3 (2005) Set up an OD server for testing and pick test clients
Phase 4 (2006) Migrate NIS to OD on a production server
Phase 5 (2006-2007) bring servers and clients under LDAP umbrella

3. Conclusion

Implementing Directory Services is part of Ocean Informatics' ongoing quest for balancing of resource access expansion and sustainable practices. With Open Directory in place, system administrators are able to spend more time attending to the needs of a growing user base and implementing new tools, and less time involved in simple but time-consuming user management tasks, and users only have to track a single account rather than multiple accounts on numerous computational resources. In addition to central user management, OD allows for more refined and centralized control over system resources. One central server can now control disk shares, server connectivity and access to workstations.

Apple's Open Directory fits well with the Ocean Informatics open architecture approach with an emphasis on Open Source Software. Implementing Directory Services in a homogeneous environment is fairly straightforward. The continuing challenge for PAL and CCE within the Ocean Informatics approach, is to implement services in a heterogeneous computational arena with a variety (Mac, Microsoft, Unix, and Linux) of new and legacy systems. The challenge has been to make the interoperability between various platforms as seamless and coherent as possible. Our goal is to increase the availability of information that is platform independent. By using a scalable, network standard for directory services, we can connect multiple machine architectures and technologies in a unifying manner that increases availability and accessibility of digital resources.