Automated and Centralised UNIX Authentication, Account Provisioning and Account Administration

Anton Koren

Computer Associates

<anton.koren@ca.com>

Luke Howard

PADL Software Pty Ltd

<lukeh@padl.com>

ABSTRACT

As enterprises grow from tens to hundreds to thousands of UNIX systems from various vendors, the administration overhead of account provisioning, de-provisioning and password resets becomes labour-intensive and cost-prohibitive. This paper discusses an open standards-based approach to UNIX authentication, account provisioning and account administration using LDAP/X.500 directory services, pam_ldap and NIS. The technologies being discussed are UNIX-vendor-independent. They are developed in Melbourne and used throughout the world. The benefit to businesses is substantial savings in support and labour costs. The benefit to UNIX administrators is more time to work on interesting and challenging aspects of UNIX administration. And finally, this paper describes how to implement technologies which are available today.

UNIX systems have historically used NIS (Network Information System) and NIS+ for centralised user management and centralised authentication. Most vendors are phasing out NIS and NIS+ and migrating to pam_ldap. We will now discuss the current technologies available for user management and user authentication on UNIX systems.

1. NIS

Sun introduced Network Information Service NIS in 1985 (formerly Sun Yellow Pages [yp]). As such, there are many Solaris and UNIX installations from other vendors which rely on NIS. The Domain Name System (DNS) serves to access hosts by name rather than numerical IP address, and NIS provides centralised control over a more than just machine names and addresses. NIS stores information about machine names and addresses, users, the network itself, and network services. This is known as the 'NIS namespace'. The namespace information is stored in NIS maps. NIS maps were designed to replace UNIX /etc files, as well as other configuration files, so they store much more than names and addresses.

A network using a NIS relies on it completely for normal operation so maintaining its integrity is vital. Most NIS systems in use today have very little protection against active attackers: they depend on the IP address of the server being widely known and assume that nobody has taken over its address. This is obviously insecure in a world where TCP connections can be hijacked at a distance, so system designers are turning to cryptography to provide assurance that good data is being used.

2. NIS+

The *Network Information Service Plus* (NIS+) is similar to NIS but as the + suggests, it has many more features. NIS+ is a totally separate application to NIS. Unlike NIS, the NIS+ namespace is hierarchical and can be configured to match the logical hierarchy of an organisation. NIS+ stores information about machine addresses, security information, mail information, Ethernet interfaces, and network services on central servers which can be accessed by all machines on a LAN. This configuration of network information is referred to as the NIS+ *namespace*.

3. Directories, X.500 and LDAP

Most of us are familiar with printed directories such as the white pages telephone directories. Electronic directories serve a similar purpose, that is: to provide names, locations and other information about people and organizations. In a LAN or WAN, a directory service is used for instantaneous access to information such as e-mail address lookups,

user authentication and network access. Directories are also able to provide information about physical devices (e.g., servers, printers, and other network hardware). Electronic directories provide this information to applications and also to users in human-readable form.

3.1 X.500

In the 1980's and early 1990's, electronic directories evolved with each vendor producing their own proprietary repository which served specific applications. The ITU-T X.500 standard emerged from a requirement to manage e-mail addresses in conjunction with the X.400 messaging applications. This later evolved to encompass shared information between applications, using common models for user information, administration, distribution, security and replication.

Many directories support the X.500 information model, which is essentially a way of organising information about real world entities in an organised manner. The properties of this model are as follows:

- Information about entities is organised in a hierarchical structure, called the directory information tree (*DIT*).
- The tree contains *entries* which represent an entity in the real world (a user, a group, for example)
- Each entry contains a collection of *attributes* for each property of the entity (for example, a user's name, their e-mail address)

  Each attribute contains one or more *values*

The information model provides for constraints that limit each of the above; for example, schema enforces which attributes can belong to an entry. It is well suited to storing identity information, and indeed that is one of its main uses.

3.2 LDAP

The Lightweight Directory Access Protocol (LDAP) originated from the University of Michigan in the mid-1990s. The LDAP standard was originally intended to access X.500 directory services. X.500's Directory Access Protocol (DAP) never achieved significant presence amongst directory vendors because LDAP became the defacto standard.

Although LDAP started as a simplified component of the X.500 Directory, it is evolving into an almost complete directory service which is far more complex than it was originally intended. Many directory experts agree that LDAP servers are no longer as lightweight and efficient as originally intended.

Some vendors, including Computer Associates, support LDAP access into an X.500 directory backbone.

4. RFC 2307

(An Approach for Using LDAP as a Network Information Service)

UNIX systems require naming services to resolve lookups for various types of information, for example: hosts, passwords, groups, networks, services and printers. RFC2307 written back in March 1998 proposes schema for holding this information within directory entries. Directory software such as eTrust Directory ships this schema (included as nisschema), containing the following classes: posixAccount, shadowAccount, posixGroup, ipService, ipProtocol, oncRpc, ipHost, ipNetwork, nisNetgroup, nisMap, nisObject, ieee802Device, bootableDevices as defined by the RFC.

RFC 2307 evolved out of the author's experience porting NetInfo, NeXT's directory service, to UNIX in late 1996. Like LDAP, NetInfo was a hierarchical and distributed directory service, and we were using it for UNIX authentication and account administration. However, not really being an open standard NetInfo never gained much market traction outside NeXT's client base.

At that time, LDAP was relatively new and no one seemed particularly interested in using it as a replacement for NIS. Experience with NetInfo seemed to suggest that it was a natural fit, and so the work to develop RFC 2307 begun. The RFC was finally published in 1998, after which I had developed three implementations - LDAPAgent for Apple's then-nascent Mac OS X, the NIS/LDAP Gateway and nss_ldap. The latter two are still core parts of PADL's software portfolio. In the coming years, despite some initial reluctance, and through some fairly persistent lobbying, UNIX vendors agreed to adopt the schema.

5. NSS

Sun introduced the Name Service Switch (NSS) mechanism, allowing applications to perform lookup through a common API without knowledge of which naming is being used. Initially this supported lookup to NIS or NIS+ (offered by a NIS server in the network) with failover to local files if that should become unavailable. This mechanism has evolved to

include LDAP as a naming service for the switch.

With their investment in iPlanet, Sun are integrating their Solaris operating system with the Sun Directory Server, more commonly known as iPlanet. For example, Solaris 9 can be configured to lookup this information from a central Solaris system running iPlanet V5.1. They are directory-enabling the operating system giving all the benefits of managing hosts, users, groups, printers and services centrally. The Name Service Switch is configured by editing the file /etc/nsswitch.conf. Template files are provided for NIS, NIS+, DNS and LDAP.

5.1 PAM

In Unix, the Pluggable Authentication Module (PAM) architecture provides an extensible framework for application authentication to multiple back-end repositories without the need for recompilation.

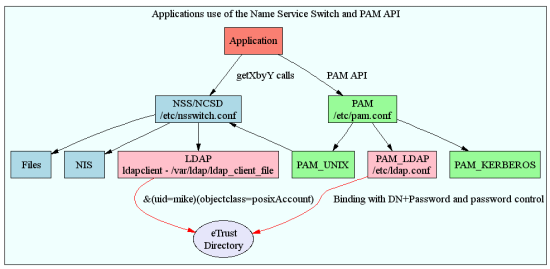
The Pluggable Authentication Module (PAM) framework enables new authentication technologies (e.g. LDAP, Kerberos) to be "plugged-in" without the need to change commands such as login, ftp and telnet. Each module can support up to 4 mechanisms: authentication, account, session and password management:

- Authentication - This module provides authentication for the users and enables credentials to be set, refreshed or destroyed.
- Account Management - This module checks for password aging, account expiration, and access hour restrictions.
- Session Management - This module is used to log activity or clean up after the session is over.
- Password Management - This module enables changes to the password and the password-related attributes.

PAM is configured by editing the file /etc/pam.conf.

6. pam_ldap

One such PAM module is pam_ldap. pam_ldap provides a mechanism to authenticate to a centralised LDAP directory, such as CA's eTrust Directory. The beauty of this approach is that all accounts, passwords and userids can be centrally managed in the Directory instead of having to be 'pushed' out to every machine as is the case with localised authentication.



6.1 pam_ldap security model

pam_ldap is designed to avoid a privileged or "proxy" account. In this way, the check of the name and password is always performed using credentials of the user that is attempting the login.

7. Migrating from NIS

NIS/LDAP Gateway (ypldapd) is commercial software supplied by PADL Software. The ypldapd server replaces the NIS server and its database of maps with the flexibility and scalability of LDAP Directory services. eTrust Directory provides the fastest, most reliable and most scalable LDAP-enabled Directory service for NIS/LDAP and pam_ldap implementations.

In large scale Unix environments, it is difficult and costly to manage user accounts either locally or through NIS domains. A solution is to use pam_ldap to centralise the management of accounts, passwords and authentication to an Enterprise Directory.

Whilst eTrust Directory currently supports pam_ldap in such environments, it is desirable to also enforce rich password policy, such as account expiry warnings, forcing password changes, account locking and password quality.

8. Password policies

Security audits require organisations to enforce password policies. Most employees who use Windows will have experienced such policies. The general types of password policies that get enforced can be summarised into five main areas:

- **Account locking** – to lock the account after a configurable number of password failures
- **Account disable** – the ability for an administrator to temporarily disable an account., for example, when an employee goes on leave.
- **Password expiry warnings** – at login being warned when a password is about to expire
- **Force change password** – after login being forced to immediately supply a new password. This is case when either an

administrator has reset an account or a password has expired.

- **Password quality** – when a password is changed, being forced to supply a non-trivial password. For example, enforcing a minimum length, that the password contains non-alphabetic characters and ensuring that it is different from passwords recently used.

In order to support rich password policy, the directory server and pam_ldap client need to extended to support LDAPv3 password controls on the BIND. In this case you will need:

- eTrust Directory 8.0 or later
- PADL pam_ldap client V169 or later

An LDAP control for password status was introduced in eTrust Directory 8.0. This control follows the definition in the Behera Password Policy Draft and conveys password status information to a client (Refer to 'Draft Standard on Password Policy' later in this document)

- PADL's pam_ldap module 169 and above now support eTrust Directory's Password Policy LDAP Control. Thus password management functions within eTrust Directory now work in synergy with the PAM API.
- Placing users in a central directory gives them access to all or none of the machines in the network. PADL's pam_ldap module checks a host attribute in the user's directory entry and only allows access if the host exists in that list.

For details on configuring eTrust Directory with pam_ldap, contact Computer Associates at http://supportconnect.ca.com.

8.1 Password policies and controls

The pam_ldap security model (above) requires that LDAP controls be passed on a Bind to communicate account status.

Unfortunately, there are only draft LDAP standards for password policies and password controls.

8.2 Draft Standard on Password Policy

The internet draft: Password Policy for LDAP Directories describes a common password policy model for LDAP directories. Note that this draft expires in August 2004. http://www.ietf.org/internet-drafts/draft-behera-ldap-password-policy-07.txt

The draft basically defines:

- A number of password policy attributes in each entry.
- A client request control on a bind with controlType 1.3.6.1.4.1.42.2.27.8.5.1 with a criticality of FALSE and no control value.
- A response control with the above controlType and a control value that can convey status or errors.

9. Access Controls (ACLs)

Directory services include access controls (ACLs) that govern access to the data. Most importantly, write access to the userPassword attribute should only be allowed for the UNIX user, in this case where we are storing passwords in an attribute, albeit in a crypted form.

Refer to the directory vendor's recommendations for implementing access controls for pam_ldap. More detailed information on eTrust Directory's access controls for pam_ldap are available from http://supportconnect.ca.com.

10. Security considerations

- It is advisable to use SSL on all connections to avoid 'man-in-the-middle' interception of passwords.
- It is not advisable to put an entry for the root account in the LDAP Directory on the grounds that if one system is compromised then they all are.
- Choose a hashing algorithm that is not vulnerable to dictionary attacks For example. When using pam_ldap it is opaque to the directory client how the passwords are being stored, and indeed there are lots of good reasons NOT to use UNIX crypt(3) for this (eg. easy to crack, 8 character password limits, etc). MD5 is a better choice.

11. Replication

Another advantage of a directory service is the ability to have replicas for failover and load sharing. High availability of the directory system, enables pam_ldap queries be directed to the server that is closest, thus reducing response time. In choosing your directory software, the replication mechanism is critical in guaranteeing data integrity and currency for failover and load sharing. eTrust Directory from Computer Associates includes a zero-latency, multi-master replication scheme designed for servicing large replication groups.

For high availability, the directory should be replicated across at least three different machines for resilience and recovery. The pam_ladp client can be given a list of Directory Servers to use in the case of support fail-over.

12. Identity Management

In recent years the cost of delivering IT to business has come under increasing scrutiny. The huge IT budgets of pre-Y2K and the Dot Com boom have given way to lean, efficient ROI-based IT expenditure. The cost of IT operations such as creation of new accounts and password resetting has given rise to a more efficient way of managing user accounts across multiple systems. We call this Identity Management.

13. Provisioning UNIX Accounts

UNIX vendors knew of the importance of Identity and Access Management (IAM) many years before the term gained popularity. NIS, NIS+ and PAM are all methods of managing identities. Many organisations are happily managing UNIX users with NIS, NIS+ or pam_ldap, so what more is there to Identity Management?

Continuous evolution of IT systems management is required for the survival and success of your business. Increased incidence of identity fraud, hacking attempts and the awareness of security vulnerabilities requires increased vigilance from IT managers and systems administrators.

13.1 Automated provisioning

Automated provisioning is achieved when Identity Management systems (e.g. eTrust Admin, eTrust Identity and Access Management suite) are integrated with authoritative identity sources, such as HR systems. Advanced IAM systems also incorporate workflow and role-based access control (RBA). Thus, when a new employee, programmer joins the development team of a financial corporation, the HR system should generate a workflow item, which in turn generates a create account(s) action based on that role.

13.2 Role Based Access

If the new employee's role includes UNIX access, the provisioning engine should then send a job to the systems administration team to create a new account with access according to their job function. This is commonly known as Role Based Access. During this process a new user is created in the Directory which includes UNIX account attributes. Once generated, the new employees will have access to all necessary UNIX systems using that one account (which is authenticated via pam_ldap).

13.3 Self-service, Password Reset

Advanced Identity Management systems should also incorporate self-service administration and automated password resetting. Systems like eTrust Admin free up help desk operators and systems administrators by allowing users to change their passwords and have the ability to automatically reset forgotten passwords (following sufficient validation).

14. Conclusion

By implementing an Automated and Centralised UNIX Authentication, Account Provisioning and Account Administration systems based on pam_ldap and eTrust Directory, UNIX administrators will free them from mundane tasks and have more time to spend on solving the more challenging and complex UNIX activities.

Business owners will quickly see the ROI from these automated Identity and Access Management systems and their users, staff and IT systems will become more efficient and more profitable.

References

[1] PADL Software (pam_ldap, NIS/LDAP Gatreway), http://www.padl.com

[2] PADL Software's Documentation and list of related links, http://www.padl.com/Contents/Documentation.html

[3] PADL's migration tools, http://www.padl.com/OSS/MigrationTools.html

[4] eTrust Identity and Access Management, Computer Associates, http://www3.ca.com/Solutions/SubSolution.asp?ID=4348

[5] eTrust Identity and Access Management White Papers, Computer Associates, http://www3.ca.com/Solutions/CollateralList.asp?CCT=19505&ID=4348

[6] eTrust Directory 8.0 Administrator Guide, Computer Associates, http://supportconnectw.ca.com/public/etrust/etrust_dir/etrustdir_supp.asp

[7] eTrust Admin 8.0 Administrator Guide, Computer Associates, http://supportconnectw.ca.com/public/etrust/etrustadmin-dmo/etrustadmin-dmo_supp.asp

[8] Unix Authentication, Mike Smith, Computer Associates, 2004, On request from CA Support, http://supportconnect.ca.com

[9] Naming and Directory Services (0803 or later), Sun System Administration Guide: http://docs-pdf.sun.com/817-0962/817-0962.pdf

[10] LDAP in the Solaris Operating Environment, Michael Haines, Tom Bialaski. Prentice Hall, 2003, ISBN: 0131456938

[11] Sun's PAM Documentation, http://wwws.sun.com/software/solaris/pam/

[12] System Authentication using LDAP, Brad Marshall, http://staff.pisoftware.com/bmarshal/publications/system_auth/sage-au/system_auth.html

[13] Integrating PAM_LDAP/NSS_LDAP for centralized Unix authentication, Alexis Tremblay, http://www.giac.org/practical/Alexis_Tremblay_GSEC.html

Standards

[14] Recommendation X.500, ITU-T, http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.500

[15] RFC 2251 - Lightweight Directory Access Protocol (v3), http://www.ietf.org/rfc/rfc2251.txt

[16] RFC 2307 - An approach for using LDAP as a Network Information Service, http://www.ietf.org/rfc/rfc2307.txt?number=2307

[17] Draft Password Policy for LDAP Directories, http://www.ietf.org/internet-drafts/draft-behera-ldap-password-policy-07.txt