Taking Unix Identity and Access Management to the Next Level

Now that you’ve taken care of local users and groups—what’s next?

Written by Quest Software, Inc.
## Contents

Abstract ................................................................................................................................. 3

The Problem with Unix ......................................................................................................... 4

Quest Identity Manager for Unix and Quest Authentication Services ............................. 5
   Local User and Group Management .................................................................................. 5
   Authentication and Single Sign-on .................................................................................... 5
   Group Policy ..................................................................................................................... 5
   NIS Migration ................................................................................................................... 6
   Strong Authentication ....................................................................................................... 6
   Audit, Alerting, and Change Tracking ............................................................................... 6

Conclusion ............................................................................................................................ 8
Abstract

One of the biggest challenges facing administrators of Unix and Linux systems is the management of local users and groups. Typically these accounts must be managed individually, on a box-by-box basis, or by using cumbersome and limited tools. Quest Identity Manager for Unix overcomes these deficiencies by providing a web-based console that enables administrators to remotely manage all Unix/Linux users and groups from a single, centralized interface.

The benefits of centralized management are obvious, but Identity Manager for Unix extends these benefits to truly simplify identity and access management for Unix systems. This technical brief explains how you can not only move to centralized management of local Unix users and groups, but to full identity and access management without adding infrastructure, relying on obsolete and non-compliant technologies (such as NIS), or deploying cumbersome and limited synchronization solutions. Identity Manager for Unix provides the path to:

- Full Kerberos authentication and single sign-on for Unix, Linux, and Mac systems
- Group Policy-based management of Unix, Linux, and Mac
- Complete migration from NIS
- Centralization and consolidation of identities
- Strong authentication
- Reporting on Unix-related identity and access information
- Auditing, alerting, and change tracking
- Streamlining of identity administration tasks around a single identity and a single administrator action
- Security and compliance for Unix, Linux, and Mac systems
The Problem with Unix

None of us can survive without our Unix and Linux systems. They host critical data and applications, and the diversity they bring insulates our businesses from being held hostage by any one platform vendor.

Unfortunately, Unix systems pose significant challenges when it comes to correlating a single physical user’s access with the dozens, hundreds, or even thousands of individual Unix systems that he must access.

Typically in an organization with 100 Unix servers, each user could have 100 local accounts (one on each box) and be a member of hundreds of locally-managed groups. This means there could be 100 passwords to be managed, 100 separate provisioning actions, and 100 trips to servers to manually audit the rights and specifics of each user’s 100 accounts.

Who does all this work? You do. But is that really where you should be spending your time? Or even where you want to be spending your time?
Technical Brief: Taking Unix Identity and Access Management to the Next Level

Quest Identity Manager for Unix and Quest Authentication Services

Local User and Group Management

Quest Identity Manager for Unix overcomes many of these challenges by providing a centralized, web-based console that makes the management of local Unix users and groups intuitive, convenient, and more cost-effective. But Identity Manager for Unix doesn't stop at the local user and group level. While you were using the tool, you may have noticed its capacity to assess Unix systems for Active Directory bridge readiness. But what does that mean?

Active Directory (AD) bridge solutions, such as Quest Authentication Services, enable Unix systems to take advantage of the Kerberos authentication, Group Policy, and centralized identity management capabilities of Microsoft Active Directory. When Unix systems become “full citizens” in Active Directory through Authentication Services, many, if not all, of the most pressing Unix identity and access management challenges disappear.

Recall our example above of the user who has 100 Unix identities, one on each box. Using Authentication Services, these 100 Unix identities can be retired—the user’s single Active Directory account can provide the necessary access, authentication, and authorization services to all Unix systems. Imagine the relief that this will provide to your Unix administrators, not to mention your Unix users! No longer will a user have 100 passwords that need 100 individual resets from the Unix administration team. When a new user comes on board, Unix administrators no longer need to physically go to 100 Unix boxes and provision 100 user accounts and grant membership to all necessary groups. And even more important, when a user leaves the organization, a single AD-based deprovisioning action terminates access across all 100 Unix systems—eliminating the security holes and compliance violations that typically accompany these events.

In addition to providing these local user and group management capabilities, Identity Manager for Unix acts as the management console that unlocks the full Authentication Services functionality that truly simplifies identity and access management. The most important of those capabilities are discussed below.

Authentication and Single Sign-on

Quest Authentication Services provides the necessary integration to enable Unix, Linux, and Mac systems to act as “full citizens” in Active Directory. The heart of this functionality is centralized authentication and single sign-on for Unix systems. The solution provides the integration between Unix’s native PAM and NSS components with the Kerberos and LDAP provided by AD.

From within Identity Manager for Unix, the Join Unix System to AD command moves authentication from native Unix protocols to the more secure, efficient, and compliant Kerberos capabilities of Active Directory. This “join” functionality extends from simple mapping of a Unix account to a corresponding AD account for authentication and password policy, to full migration from Unix identity to an entirely AD-based, consolidated identity scenario.

For more information, visit us on the web for a deeper discussion of single sign-on through Authentication Services.

Group Policy

One of the biggest benefits of making Unix systems “full citizens” in Active Directory is streamlining management through Group Policy principles leveraging the Active Directory Group Policy framework. Quest Authentication Services provides the industry’s most powerful extension of Windows Group Policy to Unix, Linux, and Mac, including:
- Pre-built policies for critical operations (such as configuring and administering elevated privilege delegation)
- A full management interface for Group Policy management of the complete set of Mac preferences and settings
- Management of strong authentication
- All the flexibility to leverage Group Policy for virtually any task that may be required

All of the full-featured power of Group Policy is launched, controlled, monitored, and audited through Identity Manager for Unix on Authentication Services-enabled Unix, Linux, and Mac systems.

To learn more about the powerful Group Policy capabilities of Authentication Services, read the technical brief “Enterprise Group Policy.”

**NIS Migration**

Quest Authentication Services provides all the tools to migrate Unix identity and access management from Network Information Service (NIS) into the more secure and compliant Active Directory infrastructure. The process of migrating from NIS to unified, AD-based IAM requires significant planning, careful system and identity assessment, and reconciliation of NIS data with the newly-unified AD identity namespace.

Identity Manager for Unix provides intuitive access and powerful control over the entire process of NIS migration, as well as access to all of the Authentication Services capabilities needed to execute the migration in a controlled, transparent, and safe manner. These capabilities include:

- Mapping and editing existing NIS maps for AD-based IAM
- Alignment of Unix ownerships
- Reconciliation of disparate identity information
- Reporting on identity, access, and migration progress, including “what if” pre-assessment of planned migration activities
- Roll-back to previous states

For a complete discussion of Authentication Services’s tools and capabilities for NIS migration, read the technical brief “Quest Authentication Services: A Comprehensive Solution for NIS Migration.”

**Strong Authentication**

Every installation of Authentication Services 4.0 includes strong authentication through Quest Defender (25 user licenses and 25 one-time password tokens). This empowers organizations to add a deeper level of security to Unix authentication. You can use Identity Manager for Unix to configure and manage the two-factor solution for Authentication Services-enabled Unix systems, and control it through Group Policy.

To learn more about Quest Defender and its strong authentication capabilities, visit [http://www.quest.com/defender/](http://www.quest.com/defender/).

**Audit, Alerting, and Change Tracking**

In addition to the local Unix user and group reporting and AD-bridge readiness assessments available in Identity Manager for Unix, Authentication Services provides full auditing, alerting, and change tracking for Unix systems that participate as “full citizens” in Active Directory. This expanded audit functionality is available through Quest ChangeAuditor, which is included with each Authentication Services 4.0 installation.

Available information includes:

- NIS object settings and changes
- Personality object settings and changes
- Computer object and attribute settings and changes
- GPO settings and changes
- The state of Unix GECOS, User, Group, Name, Directory, Login, ID, Shell, etc., as well as changes to all of these

To learn more about Quest Change Auditor, visit [http://www.quest.com/changeauditor-for-active-directory](http://www.quest.com/changeauditor-for-active-directory).
Conclusion

Integrating Unix, Linux, and Mac systems with AD has quickly become mainstream since Quest introduced the first AD bridge solution with Authentication Services in 2004. In fact, more than 2,000 companies have adopted Active Directory-bridge technologies, according to a 2009 Burton Group report.

But today’s Unix organization demands more than simple AD-based authentication. With Identity Manager for Unix, Quest brings the path to AD bridge to the masses. This freeware web console provides powerful, centralized management of local Unix users and groups and readiness assessments for moving to AD bridge through Authentication Services. Identity Manager for Unix also provides a simple path to a full AD bridge by launching the full range of Authentication Services capabilities to Authentication Services-enabled systems.

To try Authentication Services for yourself, download a free trial, watch a recorded demo, or take the solution for a QuestDrive.
About Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

PHONE  800.306.9329 (United States and Canada)
        If you are located outside North America, you can find your local office information on our Web site.

E-MAIL  sales@quest.com

MAIL   Quest Software, Inc.
       World Headquarters
       5 Polaris Way
       Aliso Viejo, CA 92656
       USA

WEB SITE  www.quest.com

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.


SupportLink gives users of Quest Software products the ability to:

- Search Quest’s online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.