QUEST SOFTWARE
Smart Systems Management

Extending Native Active Directory Capabilities to Unix and Linux

Quest Authentication Services is the Foundation for an Enterprise-wide, Active Directory-based, Identity Management Strategy

Written by
David Eyes
Product Manager
Identity Management
Quest Software, Inc.

TECHNICAL BRIEF

© 2009 Quest Software, Inc.
ALL RIGHTS RESERVED.

This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Quest Software, Inc. ("Quest").

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: **legal@quest.com**

Refer to our Web site for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BridgeAccess, BridgeAutoEscalate, BridgeSearch, BridgeTrak, BusinessInsight, ChangeAuditor, ChangeManager, Defender, DeployDirector, Desktop Authority, DirectoryAnalyzer, DirectoryTroubleshooter, DS Analyzer, DS Expert, Foglight, GPOADmin, Help Desk Authority, Imceda, IntelliProfile, InTrust, Invirtus, iToken, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogADmin, MessageStats, Monosphere, MultSess, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Point,Click,Done!, PowerGUI, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportADmin, RestoreADmin, ScriptLogic, Security Lifecycle Map, SelfServiceADmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer, vRanger, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, WebDefender, Webthority, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Updated—November 2009

Contents

Introduction

As enterprises become more complex, involving multiple operating systems and the challenges of identity management also become greater.

What is identity management? At the core, it is about control of authentication, authorization and access. All other areas of identity management—provisioning, single sign-on, password management, audit, federation, etc.—grow from the fundamental challenge: to ensure that the right users are given the right access to the right resources.

This basic definition of identity management indicates that it will come into play in any consideration of regulatory compliance requirements, as well as operational efficiency goals. Gaining control of and visibility into individual authentication, authorization and access activities provides a clear path to enhanced compliance, as well as an opportunity to streamline operations, reduce the total cost of ownership of systems and increase the return on investment of IT expenditures.

Typically organizations confront multiple, disparate identity stores and multiple (often conflicting) identities for users. Management tasks that appear so simple on a single platform, (such as for Windows systems through Active Directory (AD)) become increasingly difficult when they involve several, dozens, or even thousands of disparate Unix or Linux systems.

Imagine the benefits if Unix and Linux systems and applications could take advantage of the same identity management infrastructure already in place for Windows resources. Suddenly, single sign-on, enhanced regulatory compliance and simplified identity management can become a reality. If multiple Unix and Linux identity stores and authentication mechanisms can be eliminated in favor of a single store for the entire enterprise, then the time-consuming, expensive, cumbersome tasks of Unix provisioning, audit, password management, and others can be achieved through a single infrastructure and strategy—for all systems.

Quest Software provides Quest One Identity Solution, a set of enabling technologies to simplify identity and access management, to deliver such a capability. Using Quest Authentication Services' patented technology, Unix and Linux systems and applications can join the AD domain for centralized management and single sign-on.

Quest One provides a superior integration point for AD-based identity management, using a standards-based approach. This standards-based strategy provides tight, often seamless integration with other identity management offerings within the Quest One technologies, as well as other vendors (including meta-directory providers).

Business Problem: User Authentication in Heterogeneous Environments

Today, many organizations require IT support for a variety of mission-critical software solutions. IT management has become more complex with the need to address mixed-platform environments, which include Windows, Unix, Linux and Java platforms. Incompatibilities between these disparate platforms can complicate management tasks that would otherwise be straightforward in a single-platform environment.

System administrators are forced to use separate tools and processes for each platform, to accomplish tasks that are essentially the same. Many Unix and Linux platforms provide proprietary tools, but often administrators must resort to third-party tools or write scripts to accomplish routine tasks. The ongoing overhead associated with maintaining multiple tools, to accomplish the same task, is significant in both cost and inefficiency.

While heterogeneity is a fact of life, most IT organizations have standardized their business infrastructure on Microsoft products, specifically Windows 2000/2003 (including AD), Windows XP, and the various applications associated with them (such as Microsoft Office). Having based the bulk of their infrastructure on these technologies, it is only natural that a new, centralized, cross-platform authentication and management system leverage Microsoft AD.

An authentication and management scheme built around AD works very well at providing key identity management capabilities for Windows systems. For Windows, AD offers authentication services, single sign-on, access management and even federation. But what happens when Unix and Linux enter the mix? In Windows, when a user logs in using a username and password (or smart card and PIN), AD issues an encrypted credential (or ticket) based on the secure Kerberos standard. This credential fundamentally follows the user around, providing authentication and authorization, which results in access. In Windows, AD delivers true single sign-on.

Unfortunately, Unix and Linux systems do not authenticate users in the same way that Windows systems do. This disparity requires that system administrators support and maintain two or more distinct authentication schemes—a practice that is both problematic and expensive. Keeping track of multiple per-system passwords is error prone and in some cases can lead to security vulnerabilities or compliance shortcomings. Some system administrators resort to home-brewed password synchronization scripts, but quite often, what they end up with is an unnecessary point of failure and a labyrinth of multi-platform scripts that must be maintained and supported. Such “limited” solutions lack commercial maintenance and support, as well as important functionality and flexibility.

A typical, non-integrated identity management strategy offers a number of challenges, which are only exacerbated as the enterprise becomes more heterogeneous.

- **Password Management Nightmare:** According to a 2003 IT survey conducted by the Meta Group, on average, a single user will have access as many as 27 accounts in a large organization. As a result, IT administrators must create, manage, maintain and delete all the various user identities for a single user. Compounding this problem is the management and maintenance of multiple user accounts, across multiple platform environments, including Windows, Unix and Linux systems.
- **Remembering Multiple Passwords:** Remembering multiple user names and passwords present several challenges, not only for the user, but also for those who are responsible for supporting that user.
- **Help Desk Support Costs:** Users often call the help desk to obtain access to systems when they forget or lose their user name and/or password. According to the Meta Group, approximately 45 percent of all help desk calls are for access-related requests, due to a user forgetting his or her password. The cost associated with a password-reset request, according to Meta, is an estimated $38.00 per call. A leading provider of consulting services for enterprise organizations, PriceWaterhouseCoopers, estimates that 70 percent of users call the help desk at least once a month for access-related requests.

- **Provisioning/De-provisioning:** Administrators also face the challenge of granting user rights and establishing identity for a large mix of identity stores. This process—often called provisioning—becomes even more cumbersome when multiple systems require their own unique treatment of user identity information. A single, simple assignment in AD can provide provisioning for all Windows resources. But the task becomes much more complex, costly and error-prone, as administrators manually add users and identities to Unix, Linux and Java systems.

  While, cross-platform provisioning is inconvenient and inefficient, de-provisioning (or revoking rights and removing identities), in complex heterogeneous environments, presents a major security challenge. Meta reports that only 70 percent of users are deleted from accessing systems upon termination. Allowing a former employee, particularly a disgruntled employee, to continue to access systems and mission-critical data poses the risk of data loss and disruption to business, not to mention its compliance implications.

- **Increased Operational Cost and Complexity:** IT managers are continually challenged to minimize operational expenses. The complexity of managing mixed operating environments has forced many enterprise organizations to use separate tools and processes to accomplish tasks that are functionally the same, regardless of the platform, while operationally different. The ongoing overhead associated with maintaining multiple tools and processes to accomplish the same task is an inefficient and costly use of resources.

What about Regulatory Compliance?

Since the management of identities determines how sensitive enterprise data will be accessed, it is increasingly subject to regulatory requirements, calling for application of best practices. While some requirements can be implemented with manual policies and procedures, the overhead involved typically demands an automated solution.

The most well known regulatory legislation, affecting identity management and access rights, is the Sarbanes-Oxley Act of 2002 (SOX). Depending on industry and national jurisdiction, these could include:

- The Gramm-Leach Bliley Act (GLB)
- Healthcare Insurance Portability and Accountability Act (HIPAA)
- Statement on Auditing Standards No. 70 (SAS 70)
- Title 21 Code of Federal Regulations (21 CFR Part 11 FDA)
- European Union Data Protection Directive (EUDPD)

Conventional Approaches to Addressing Heterogeneous Identity Management

The problems associated with identity and access management for heterogeneous enterprises are nothing new. Over the years, a number of options have arisen in an attempt to alleviate the pain.

Inefficient Solutions Developed In-house

In an effort to overcome these challenges, some enterprise organizations have developed their own "in-house" processes for addressing identity management. Most of these processes require the use of scripts to address the problems presented by Unix-based systems. However, there are several limitations and security risks associated with implementing a script-based or "home-grown" identity management process. Those limitations and risks include:

- **Undocumented Processes:** Administrators will often create a custom process, without completely documenting how the process was designed or tested, and how it should be implemented in specific environments.
- **On-Going Support and Maintenance:** Change is constant within any organization. IT administrators may change positions, responsibilities and jobs. The intellectual knowledge used to develop an in-house or "home-grown" process usually disappears when the administrator leaves or changes positions.
- **Lack of Standards and Security:** Developing an in-house method may only address a portion of the problem, without completely meeting the objectives and requirements for controlling access and protecting systems. For example, a home-grown solution for authentication and authorization in a Unix environment may pass clear text passwords over the network, thus allowing someone to easily capture the information.

Large Security Frameworks and Meta-directories

Some organizations seek to address the challenge of heterogeneity through implementing complex identity solutions, typically implemented with meta-directories and other agents and levels of infrastructure. While these solutions can provide significant value in a number of identity management scenarios (such as centralized authentication for legacy systems and applications), they are often very expensive, require additional management overhead, and do not address the fundamental problem of multiple identity stores, multiple identities and multiple authentication mechanisms. These solutions impose their own infrastructure, an additional directory, and another authentication layer that functionally "synchronizes" the still-in-existence mix of disparate identity stores for Unix, Linux and Windows.

Even in organizations, in the processes of deploying meta-directories, any approach that actually consolidates identities (that is reduces the number of identity stores, centralizing on a single authentication mechanism), will dramatically improve the efficiency, ease of implementation and management and cost-effectiveness of the solution.

Regardless of the "traditional" approach" an organization may choose, the underlying problem still exists—multiple systems with multiple identity stores and multiple authentication mechanisms. Ideally, an organization would "get to one". ONE identity, ONE authentication mechanism and ONE identity store. If an organization can consolidate disparate identities in a single infrastructure, preferably one that is already in place for a large portion of the enterprise, the corresponding benefits of single sign-on, streamlined identity administration, compliance and security can be achieved.

The Integrated Identity Management Solution

The challenge of managing identity and access across multiple platforms is well documented. As discussed above, conventional solutions have major disadvantages. But there is an alternative. What if:

- You could provide a single point of authentication and authorization for the entire range of systems (Windows, Unix and Linux)?
- That capability was based on an infrastructure you already have, that's already compliant, and has proven scalability in the largest companies?
- You could eliminate the myriad of identity stores, redundant user logins and identities, and authentication mechanisms in favor of a single store and single mechanism that provides single sign-on?
- You could use that solution to enable compliance and provide a platform for advanced identity administration capabilities?
- You could streamline cross-platform identity management through an infrastructure that has already proven itself on a single mission-critical platform in your enterprise?
- Users only had to remember one password?
- IT only had to provision and manage one identity per user?
- Your provisioning, password management, audit, and change and configuration management tools could extend beyond Windows to also include your Unix, Linux and Java systems?

In short: what if you could extend what AD does for Windows systems to the range of Unix and Linux systems that present the biggest challenges for identity and access management?

If you could do that, then all of the issues discussed above become manageable or disappear entirely. Today, a solution exists that does just that. This solution is Quest Authentication Services, which innovated this integrated approach to identity management. No other Unix-to-AD integration solution offers the proven track record, standards-based approach or identity management flexibility offered by Quest Authentication Services.

What makes this Possible now?

As independent platforms from competing vendors emerged, no one vendor possessed the foresight or motivation to build authentication integration with its competitors. Consequently, each platform performs authentication in its own unique way. The various Unix vendors based their solutions on standards (PAM and NSS), yet each implementation was unique and proprietary to the platform it was designed to protect.

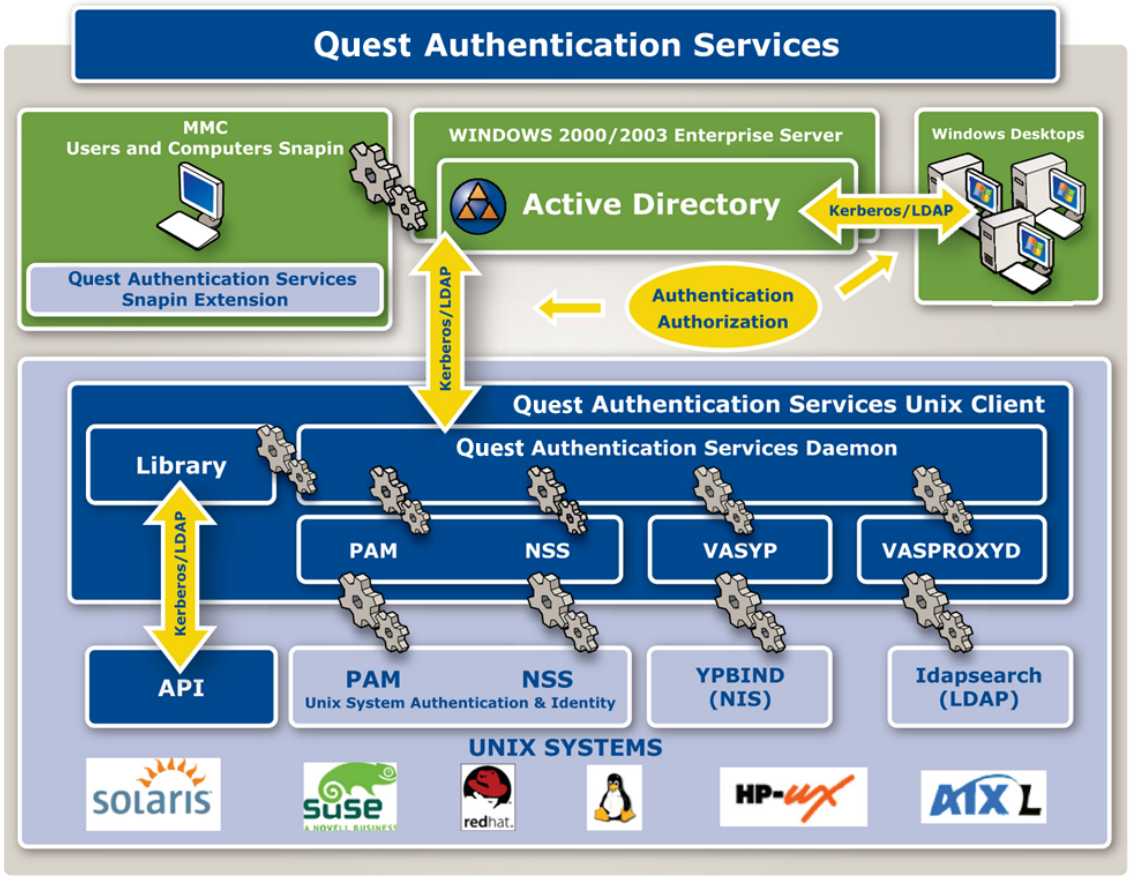
In parallel, Microsoft developed its own directory service—AD—that leveraged newer and more secure standards (namely Kerberos and LDAP). AD is designed to provide compliant authentication, authorization and single sign-on for Windows systems, but not for Unix, Linux or Java.

Without coordination between the platform vendors, no common implementation of standards, and no openness across providers, each platform's authentication infrastructure and mechanism developed independent of the others. Consequently, as organizations organically grow to include systems crossing a number of platforms, they must adopt the authentication process and tools specific to each OS. Today's organization could have a large and robust AD installation, several NIS (Network Information Service) domains for Unix systems, and a variety of identity stores based on the etc/passwd file in Unix and Linux systems.

The industry needed an independent third-party to build the unique integration required for each Unix and Linux platform to enjoy the benefits of AD-based authentication. Quest One, through its Quest Authentication Services technology, was the first to address this need and today is the leader in AD integration for Unix and Linux systems.

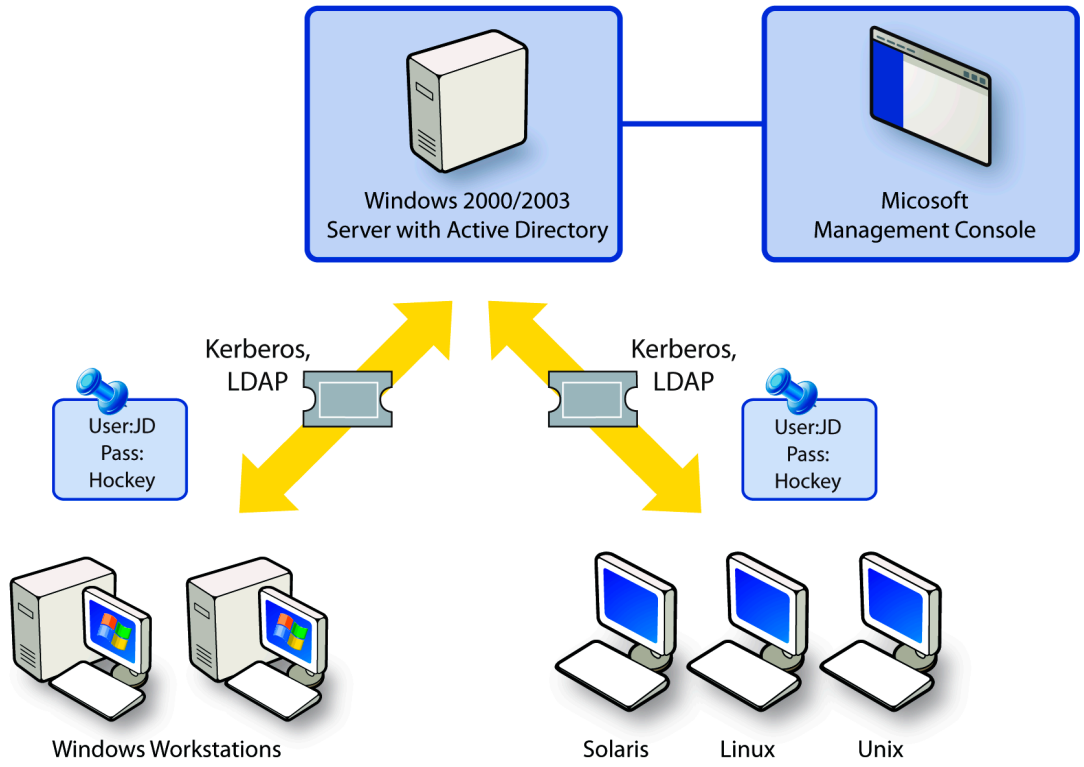
Quest Authentication Services

Quest Authentication Services extends AD's reach, allowing Unix and Linux system administrators to centralize their access, authentication and authorization needs around AD. Quest Authentication Services allows system administrators to provide a secure environment where users have the same user name and password for Windows, Unix and Linux logins, without the need to maintain password synchronizers or perform user-administration tasks on multiple systems.



With Quest Authentication Services, users only need to remember the user name and password for their account in AD. Since the product integrates seamlessly with Unix and Linux Pluggable Authentication Modules (PAM) and Name Service Switch (NSS) systems, authentication through Quest Authentication Services automatically provides authentication to any PAM/NSS-enabled service that has joined the AD domain through the integration that the product provides. Issuing "session keys" permits one login or authentication to remain active for all enabled services until the user logs out, signaling the end of the session—the same as AD does for Windows.

Using the Microsoft Management Console from a central location, the system administrator can manage user and computer accounts in AD. In addition, administration for Unix and Linux can be performed using command line tools. Quest Authentication Services gives organizations the best of both worlds—the security, compliance and scalability of AD for Unix and Linux, while maintaining the flexibility and "Unix-ness" of those non-Windows systems.



The Advantage of Standards

Quest Authentication Services utilizes a number of Internet Engineering Task Force (IETF) interoperability standards. These standards provide the "glue" that allows AD to serve authentication information to Unix and Linux.

These interoperability standards include:

- LDAP v3 (RFC 2251)
- Kerberos v5 (RFC 1510)
- Simple Authentication and Security Layer (SASL)
- Generic Security Services API (GSSAPI)
- Pluggable Authentication Modules (PAM)
- Name Service Switch (NSS)
- LDAP as a Network Information Service (RFC 2307)

Through these standard mechanisms, Quest Authentication Services integrates transparently with Windows, Unix and Linux environments, without the use of proprietary protocols or additional infrastructure. Other solutions that attempt to address similar customer issues aren't as rigorously standards-based, and consequently they require proprietary consoles, proprietary treatment of Unix attributes in AD, and non-standard interactions with AD. On the other hand, Quest Authentication Services is entirely standards-based. This in turn protects an organization's investment in the solution, its identity asset by storing it in standards-based directory structures, and enables a much wider range of interoperability options than non-standard alternatives.

The RFC 2307 standard is of particular note. With the R2 release of Windows Server 2003, which includes AD, Microsoft adopted this Unix standard for the schema—providing new attribute fields in the base AD schema for storing the Unix attribute information required to define a user in the Unix environment. Microsoft's adoption of the RFC 2307 standard in the schema is direct evidence of support on the part of Microsoft to enable standards-based solutions, such as the Quest Authentication Services solution for integration with AD. Other solutions may claim to work with R2, however they do not natively use the schema in the way Microsoft intends.

This rigorous adherence to standards also enables Quest Authentication Services to provide value beyond its core capability of allowing Unix and Linux systems to join the AD domain. Since Unix and Linux attributes are stored in the AD schema transparently (and in precisely the way AD intends), integration with third-party provisioning, password management, auditing, and reporting tools (including Quest One tools) is seamless and easy. For example, Quest Authentication Services integrates natively with Microsoft Identity Integration Server (MIIS), with no modification or additional modules required. Other solutions must build custom integration to serve Unix attribute information to MIIS—more complexity, more expense and more software requiring support.

Benefits of Quest Authentication Services

- **Secure:** One defining feature of Quest Authentication Services is its ability to establish secure client/server communication without the usual aggravations associated with other secure transports such as SSL or TLS.

  For example, the traditional technologies used to secure LDAP are SSL and TLS, both of which require the distribution and maintenance of X.509 security certificates. Instead of using SSL or TLS with LDAP, Quest Authentication Services employs SASL authentication and "GSSAPI wrapping" using Kerberos session keys. This allows the product to encrypt the entire LDAP session. Consequently, LDAP information is never transmitted as any kind in clear text.

  A natural byproduct of this security, coupled with that already offered by AD, enhances compliance for Unix and Linux systems. This includes an alternative to non-compliant NIS systems and a migration path from NIS to an entirely AD-based authentication service.

- **Unobtrusive:** Quest Authentication Services is designed to integrate into existing networks with minimal disruption of users and system administrators. Unix and Linux authentication and account abstractions (collectively referred to as PAM/NSS) are utilized, making the product immediately compatible with a wide range of commercial and open-source software. After product installation, Unix and Linux systems continue to behave exactly as they did before–except for the added benefit of a central authentication and account management system, specifically that offered by AD.

- **Scalable:** In a Kerberos/LDAP-based authentication system, the scalability bottleneck is always the LDAP server. Quest Authentication Services is designed to minimize the demands made on the LDAP server and the Kerberos key distribution center (KDC) that are located on the Windows 2000/2003 server. The product's design includes the following considerations:
    - Caching of user and group account information
    - Fail-over to cache when LDAP service busy or unavailable
    - One LDAP connection per client machine (as opposed to one connection per NSS-linked process)
    - Tunable performance parameters, allowing system administrators to minimize LDAP bottlenecks according to specialized usage patterns

These considerations significantly reduce the load on the AD back-end.

- **Robust:** Quest Authentication Services is designed to operate in environments that are weakly connected, continuing operation even if AD goes down or if network components fail. This makes it suitable to use with systems such as Unix and Linux laptops. Even if completely disconnected from the network these systems will continue to operate normally, allowing system logins as if still connected.
- **Flexible:** Quest Authentication Services was designed and developed by a company that understands the "toolkit" heritage associated with Unix and Linux—which were both originally designed as collections of flexible building blocks that can be assembled to solve specialized problems. True to this tradition, Quest Authentication Services is designed to expose functionality by means of a robust, versatile set of command line tools. This permits Unix and Linux system administrators to assemble specialized tools to fit their unique needs.

Key Capabilities and Features

Quest Authentication Services functionally extends the native identity management capabilities of AD to Unix and Linux systems. Generally, any capability of AD can be extended to non-Windows platforms through Quest Authentication Services.

Single Sign-on

One of AD's key capabilities is single sign-on for Windows systems. As a user logs on to Windows, AD verifies the users identity (authentication) and grants a Kerberos credential (authorization) that provides access to the applications and services defined by the individual's role and rights as contained in AD. Quest Authentication Services extends that capability to Unix and Linux systems.

Quest Authentication fully supports the most comprehensive list of non-Windows platforms in the industry.

For a complete list of supported platforms please see
www.quest.com/Quest_Authentication_Services/Supported_Platforms.aspx

In addition, any Unix/Linux-based application that relies on OS-level authentication will also benefit from AD-based single sign-on through Quest Authentication Services. The product also includes specific integration to provide single sign-on for SAP applications on Unix through the SAPgui interface. Single sign-on is also possible for DB2 and Oracle databases. Due to the standards-based architecture of Quest Authentication Services, each of these single sign-on offerings is included as a native capability of the product with no additional modules or infrastructure required.

Detailed guidance for SAP single sign-on and DB2 single sign-on is available upon request from your Quest representative or through the Web.

Other Unix/Linux based-application can also be easily integrated with Quest Authentication Services for AD-based single sign-on through a powerful API included with the product. This API allows organizations to quickly and easily integrate any GSSAPI- or LDAP-based application on Unix or Linux hosts with AD. That means by Quest Authentication Services-enabling these applications, the number of resources that can achieve true single sign-on can increase dramatically.

Enabling Single Sign-on in common open source applications

Since Quest Authentication Services integrates the Unix and Linux systems joined to the AD domain into the same Kerberos realm as the Windows systems in AD, it provides the foundation for true Single Sign-on. Some applications (i.e. SAP R/3 or Oracle with Advanced Security Option) have support for the Kerberos GSS-API interface "built in" so that SSO can be easily enabled with the proper guidance documents. Other common tools from the open source community, such as openssh, PuTTY, Apache, and Samba either need to be "Kerberized" or else built with the correct library interfaces to integrate with Quest Authentication Services environment.

Resource Central is the Quest Web site (http://rc.quest.com) that serves as distribution point for the above-mentioned open source tools as modified by Quest to support Quest Authentication Services. Now users can authenticate securely, without login, using ssh, Apache (from both Internet Explorer and Firefox), Samba, and ftp and telnet clients. These open source tools are provided in pre-built and source code versions on the Resource Central Web site. Quest fully supports the integration of these tools with the Quest Authentication Services environment. Resource Central is also host to a number of helpful guidance documents and other software projects of interest to the Quest Authentication Services user.

NIS Migration and UID Consolidation

One of the major issues facing organization seeking to bring non-Windows systems into AD is how to deal with the wide range of disparate (and possibly conflicting) User IDs that may exist across a variety of Unix and Linux systems and users. These issues become more critical as the enterprise grows and becomes more complex. Ideally, organizations will arrive at an end-state where each user is associated with only one UID, and that identity exists in AD and provides authentication to Windows as well as the full range of integrated Unix and Linux systems and application. Unfortunately reaching this end-state is much easier said than done.

Quest Authentication Services includes a powerful feature called Unix Personality Management that allows organizations to take advantage of AD-based authentication for Unix and Linux systems and applications even while conflicting UIDs exist. Unix Personality Management is designed as a tool to help organizations achieve the ideal end state of ONE identity, ONE UID, and ONE directory for all users in a logical, controlled and calculated manner.

With Unix Personality Management, administrators can assign “personalities” based on organizational units (OUs) that maintain the existing Unix/Linux UID while authenticating with the overriding AD identity, which is mapped to the assigned personality. This approach allows the immediate benefit of Quest Authentication Services to be realized, even if an organization cannot (or will not) reconcile the conflicting UIDs that exist across the range of Unix and Linux systems. It also allows an existing OU structure to remain intact as those systems join the AD domain.

Other approaches to the same issue propose mapping “contained” Unix UIDs as the ideal end-state and architect their solutions with no path to the ideal situation of consolidated and resolved UIDs for all systems. Consequently, to achieve the UID mapping, these solutions store the Unix attributes in the AD schema in a non-standard, proprietary way, which functionally locks the mapping and prevents the organizations from achieving the ideal objective down the road.

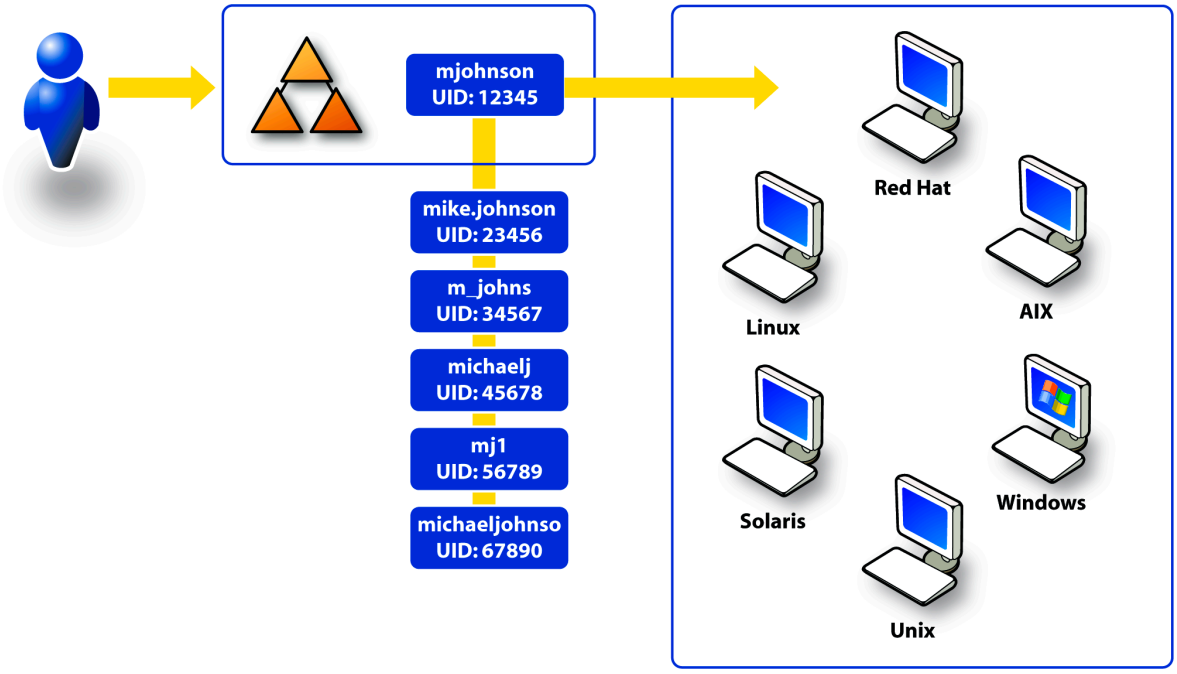
Unix Personality Management is particularly useful in NIS migration projects within legacy enterprises with multiple NIS domains. Typically NIS causes compliance or management concerns but a wholesale switch from NIS prior to implementing the Quest Authentication Services solution may be counter-productive. To address these concerns, the Unix Personality Management feature allows each NIS domain to be associated with a “Personality OU” within AD. A user’s AD Windows account provides the actual identity and the authentication and Kerberos credential. This account is mapped to all associated “personalities” residing in AD and representing the user attributes from the former NIS domains. Thus, multiple conflicting UIDs can still exist in Unix and Linux systems, while achieving the benefit of AD-based authentication and single sign-on.

Since Quest Authentication Services stores Unix and Linux attributes in the manner indicated and preferred by Microsoft, (using the RFC2307 schema attributes as included in R2) it provides an open and logical path to future identity consolidation projects.

AD as the Authorative Source for Unix Info

Unix Personality Menegement (UPM):

- All UID conflicts are migrated into AD
- Eliminate the etc/passwd file
- Unix account remains infact



The Unix Personality Management feature is a major component of Quest One's overall strategy to provide the tools, capabilities and guidance to equip customers of Quest Authentication Services with a path to the ideal state of consolidated identities within AD. Future product releases will include additional functionality aimed specifically at helping organizations achieve this objective.

Personality Service Switch

However, one of the design strengths of the Quest Authentication Services solution is that it provides a high degree of flexibility. Other solutions have a "one size fits all" approach to problems such as migration and user attribute conflict management. Quest Authentication Services also provides another mechanism, the Personality Service Switch, that provides an alternative approach to migration and attribute management.

In this approach, for the first stage of migration to the unified identity store, the attribute information—the "personality" associated with an identity—remains in the existing NIS or file-based identity store. This personality is bound to the Windows account identity by storing the user principal name—the account@domain.com value—associated in AD with the user. When Quest Authentication Services detects this value using the Name Service Switch, the user will be required to authenticate using the AD credentials. The same AD password policies will be applied as with normal Quest Authentication Services usage, and the Kerberos ticket will be issued to the user as normally with Quest Authentication Services. But the attribute information—the User ID, default group, and so on—will be derived from the existing NIS or file database.

With the Personality Service Switch, associating Unix users with their AD Windows accounts is almost completely transparent and unobtrusive and can provide the shortest route to achieving immediate term compliance goals. Of course, over time, User ID's can be reconciled at leisure and the attributes moved either to AD personalities or to the Windows account object itself, entirely at leisure.

Enterprise Group Policy

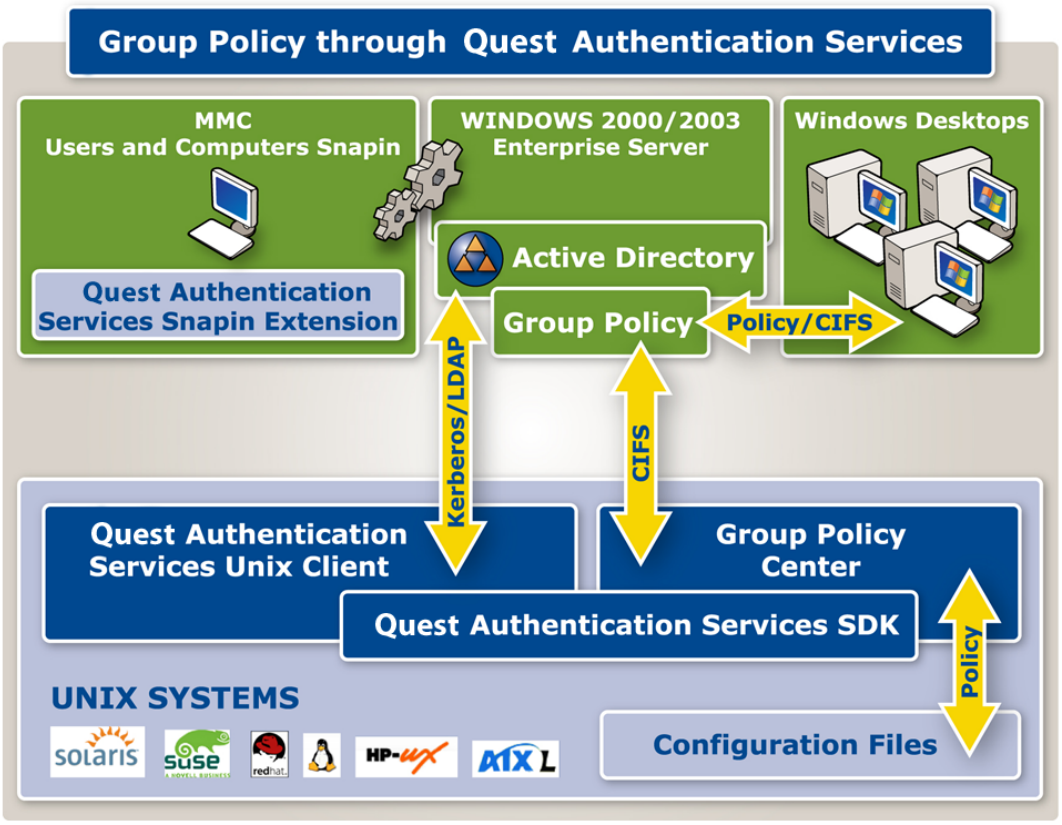
One of the major benefits AD delivers to Windows enterprises is Group Policy. Windows Group Policy is a powerful, and extremely flexible, tool for change and configuration management. To date, nothing similar has been available for Unix and Linux systems. A task that may be automated for hundreds of servers and thousands of users through a single Group Policy Object (GPO) in Windows would require hundreds or thousands of individual command-line transactions in the Unix and Linux world. Simply allowing Unix and Linux systems to join the AD domain opens a world of policy-based management to a key piece of the enterprise that previously had no such capability.

Quest Authentication Services provides a framework for Group Policy for those Unix and Linux systems—it truly delivers Enterprise Group Policy. Again, other solutions exist that claim Group Policy capability and may even offer many pre-packaged policies for Unix, but those solutions lack the depth of integration or robust Group Policy capabilities offered by Quest Authentication Services.

Such solutions provide policies based on the ADM template concept. This confines the policies to only the limited functionality offered by that interface and prevents use of complex policies. Also this approach makes management of policies much more cumbersome. In addition the ADM approach offers a difficult-to-use user interface and requires frequent Group Policy refreshes, which can tax network bandwidth and CPU usage while requiring the ADM on every GPO—a laborious manual process.

Quest Authentication Services, on the other hand, leverages native and powerful server-side extensions on the Unix and Linux systems to provide an infinitely scalable, extremely flexible and powerful Group Policy capability. This approach delivers a rich native interface that provides policy creation and distribution beyond the simple extension of Group Policy to custom applications offered by ADM templates.

With Quest Authentication Services' Group Policy module policy creation and use is only limited by the creativity, expertise and needs of the organization implementing the solution. The server-side extension approach allows user of Quest Authentication Services to create and manage even the most complex and mission-critical policies. This approach allows organization to base policies on scripts and files—functionally allowing an organization to anything they want with Enterprise Group Policy. The ADM approach cannot offer a fraction of the flexibility, power or control of the Quest One approach. In addition due to Quest's standards-based approach to integration, Group Policy management tools, such as Quest Group Policy Manager, can seamlessly enhance the value of Group Policy for Unix and Linux as well as Windows.



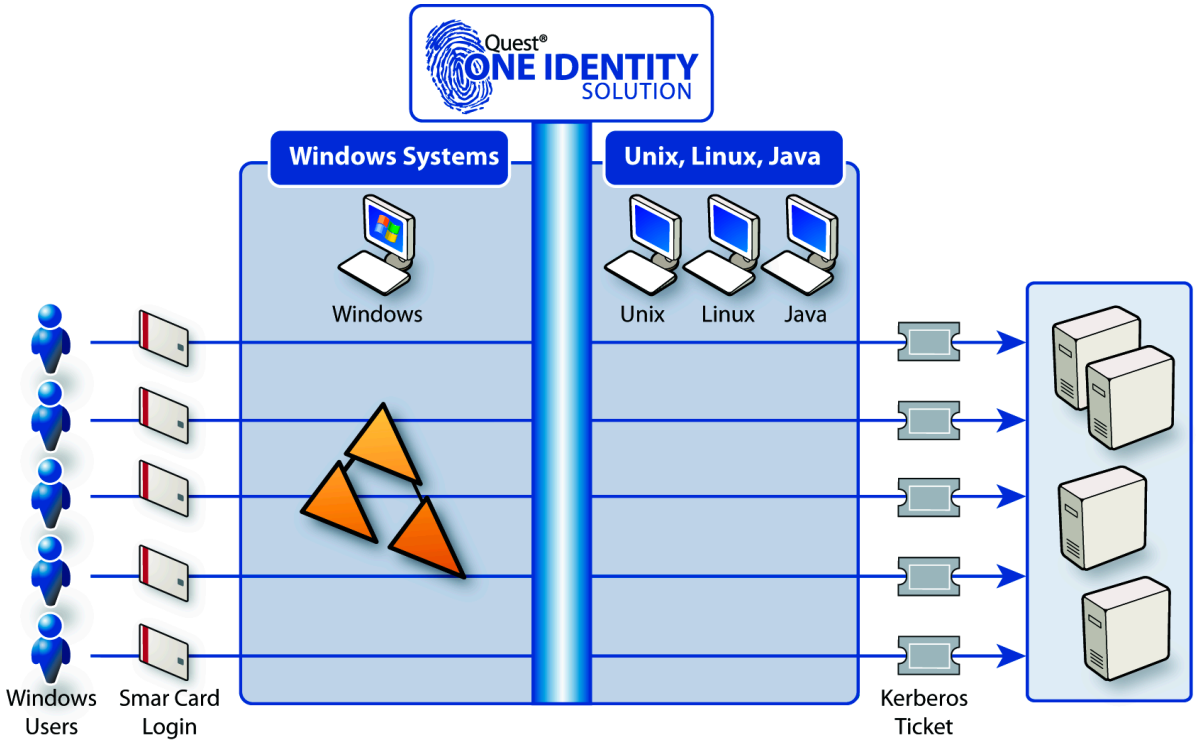
Quest Authentication Services ships with a core set of valuable Group Policies for Unix and Linux. These include:

- **Cron Policy:** The product includes a template and translator to customize cron.allow, cron.deny and crontabs for any user on the client system.
- **Sudo Policy:** Allows administrators to control sudoers file entries through Group Policy, as well as delegate client permissions, command rights and be able to report on whether a password is required to run sudo or not.
- **File Policy:** Allows any file to be pushed from AD to the Unix host.
- **Other Policies:** Quest Authentication Services includes a number of policies including policies for symbolic link, login prompt, message-of-the-day and service access control.

Smart Card/Multi-factor Authentication

In an effort to address the increasing security demands and to satisfy regulatory compliance, many organizations are adding multi-factor authentication to their identity management strategies. Once again Microsoft has lead the way with smart card integration as a core capability of AD and the Windows operating system. Similarly, Quest Authentication Services can extend Windows-based smart card authentication to Unix and Linux systems. The capability is also available to Java/J2EE applications through the Quest Single Sign-on for Java product.

The seamless integration of Quest Authentication Services with Unix and Linux platforms and AD makes this Unix authentication through a Windows smart card as robust, scalable, and secure as the traditional extended username/password authentication offered by the product.



For a more detailed discussion of smart card authentication for Unix and Linux systems from AD, refer to the white paper, Working Towards an Enterprise without Passwords.

Quest Authentication Services and Quest Reporter

One of the important elements of compliance auditing is the ability to produce reports on account and access information. Quest Authentication Services now includes Quest Reporter, a powerful reporting tool for AD. Reporter features include:

- **Data Analysis and Presentation:** Reporter provides more than 300 predefined, editable reports, including reports customized for the Quest Authentication Services Unix Personality Management capabilities. The reports can be output in multiple formats including CSV, RTF and HTML.
- **Live and Scheduled Data Collection:** Allowing to optionally collect the most current data available, or otherwise to take advantage of scheduling capabilities in order to minimize the use of network resources.
- **Action-Enabled Reports:** Reporter allows you to automate changes to objects in reports based on report results. Reporter eliminates previously manual processes and saves you valuable time.
- **Change-tracking Report:** Reporter provides a history of all changes related to a specified directory object or group of directory objects. This powerful reporting feature gives you more in-depth insight for historical analysis.
- **Customized Reports:** Reporter empowers you to create customized reports using any attribute that it collects. This helps to ensure that the report reflects the unique informational needs of your organization and supports informed decision-making.
- **Scheduled Report Generation:** Decreasing the administrative effort required to run reports, Reporter enables you to automatically run reports at configurable times. Delivering an added level of flexibility, Reporter ensures that you have the information you need at the moment you need it.

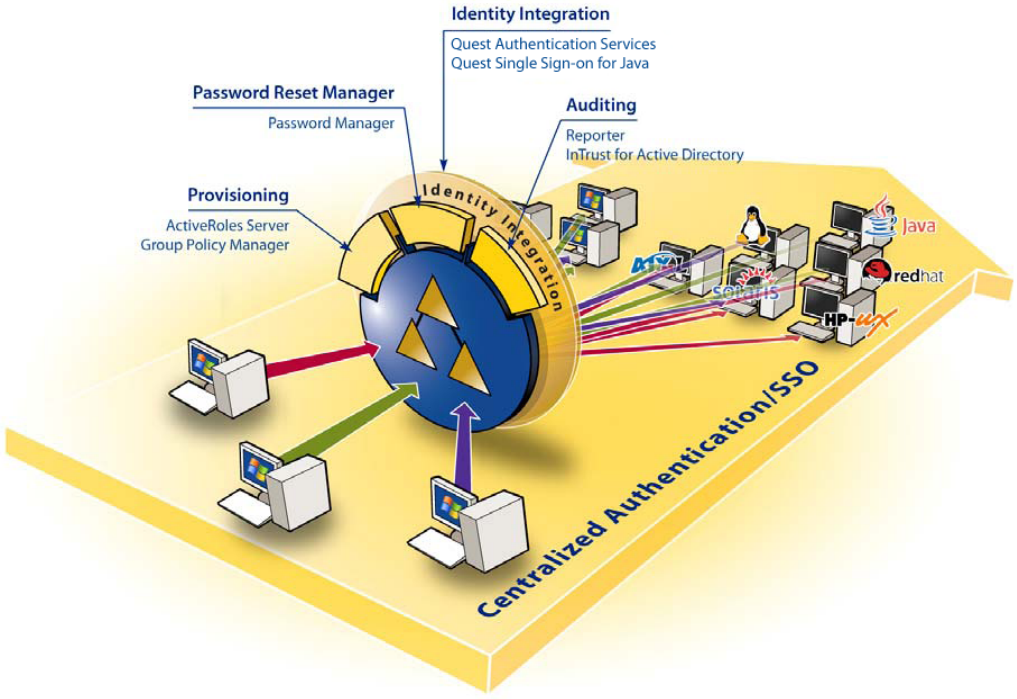
Integration with Identity Management Tools

Quest Authentication Services is designed to extend the native identity management capabilities of AD—namely authentication, access management, and single sign-on—to Unix and Linux systems and applications that traditionally do not enjoy the robust, secure and compliant capabilities that AD offers for Windows systems. However, to most organizations, identity management encompasses capabilities beyond what AD offers natively. Many organizations seek third-party tools for advanced identity administration tasks such as provisioning, password management, role management, and audit and compliance.

Many of the tools designed to round out AD-based identity management of Windows users and systems are based on the same standards that both AD and Quest Authentication Services use. As these tools treat identity information in a standard way within the AD schema, they consequently make those attributes available for use (or extension) by other standards-based solutions. Through this same strategy, Quest Authentication Services integrates seamlessly with such tools.

Other solutions—those that do not address identity information according to the standards established by Microsoft in AD, including RFC 2307—cannot offer the simple and direct integration with such tools. In order for a non-standard solution to integrate with a provisioning solution, custom integration must be built to facilitate the accessing, interpretation, and use of attributes stored in the schema in a non-standard way. This same short coming also influences these solutions' ability to natively integrate with identity management framework solutions, such as MIIS. To integrate with MIIS, such a solution requires a separate, custom module which locks the user into a non-standard approach for the life of AD and the integration solution.

Quest Authentication Services, on the other hand, uses the Microsoft supported schema attributes expressed as RFC 2307. Consequently any solution (such as MIIS, the Quest ActiveRoles Server provisioning solution, Quest Password Manager, Quest InTrust for Active Directory, Quest Reporter, or a myriad of other standards-based solutions from other identity management vendors), that also leverages RFC 2307 in a standard way will seamlessly integrate with Quest Authentication Services for powerful cross-platform identity administration based on AD.



Due to this approach, a combination of AD and Quest Authentication Services can form the foundation for an efficient and powerful identity management solution. As additional advanced identity administration capabilities, (such as provisioning, role management, password management, and audit and compliance) are added, their value extends beyond Windows to also include those Unix and Linux systems and applications that joined the AD domain. Compliance and identity management objectives can be achieved through a significantly simplified, streamlined and cost-effective strategy based on existing infrastructure—AD.

In addition, this approach also empowers meta-directory and framework solutions to become more efficient and effective participants in identity management. Simply by eliminating the need for a meta-directory to synchronize the myriad of Unix and Linux identity stores and authentication mechanisms that previously required so much management and created so much inefficiency presents significant opportunity for enhanced ROI. A meta-directory will still provide significant benefit, particularly for legacy systems or other portions of the enterprise that cannot participate in AD- and standards-based authentication. Ultimately, reducing the number of moving parts, enhancing those systems with AD-based advanced identity administration capabilities, and leveraging an exiting investment in AD to its fullest will present the greatest benefit to complex heterogeneous organizations seeking to simplify identity management. Quest Authentication Services is the prime mover of such an initiative.

For more information on Quest One solutions for simplifying identity management, please refer to the technical brief, Simplifying Identity Management.

Extending Active Directory-native Capabilities to Unix and Linux

A number of powerful enterprise features of AD are automatically extended to Unix and Linux systems and applications simply due to the fact that those systems can now participate as “full citizens” in AD. For example, AD password policies naturally apply to Unix and Linux systems through Quest Authentication Services. The amount of similar AD capabilities that can benefit Unix and Linux systems are too many to mention here. Those evaluating other solutions that claim to do what Quest Authentication Services does, should carefully consider which claimed features are actually the result of innovation, and which are simply a natural byproduct of more systems joining the AD domain. Quest One only claims those features that are enhanced or created through its technology.

Other Features

Quest Authentication Services includes a number of other innovative and powerful features designed to further enhance the Unix and Linux-to-AD integration story. These features include:

- **Active Directory Microsoft Management Console Integration:**
  Quest Authentication Services provides a standard Microsoft Management Console (MMC) snapin extension for the AD Users and Computers snapin. This allows administrators to manage Unix account information for users and groups using the same tools already in place. The product’s MMC tools include Unix Personality Management information, configurable user account defaults and advanced filtering support to enforce rules regarding Unix account values.
- **Active Directory Multiple Domain Support:** Quest Authentication Services automatically detects the AD Forest structures, and allows users to login to Unix and Linux machines joined to different domains. Cross Forest authentication is also supported.
- **Active Directory Strong Encryption Support:** Quest Authentication Services uses the strong encryption types that AD supports. It supports 128-bit keys, which provide greater security than the standard 56-bit DES keys commonly used for Kerberos.
- **Automatic Support for Time Synchronization:** Kerberos requires that Unix and Linux machines have their system clocks closely synchronized with their Domain Controllers. Quest Authentication Services can automatically synchronize Unix systems’ clocks with AD.

- **Centralized Access Control:** Quest Authentication Services allows you to configure access rules to determine what users can access on the Unix and Linux machines and the individual services running on those systems. These rules can be centrally managed through AD. Access control may also be affected using the Unix Personality Management feature.
- **Active Directory Site Aware:** Unix and Linux systems joined to AD using Quest Authentication Services automatically detect which AD site they belong to. The product will communicate with the domain controllers that it is closest to, allowing administrators to efficiently add Unix and Linux to their AD sites topology without manual configuration.
- **Active Directory Nested Group Support:** Administrators can use AD nested groups for Unix file permissions and access control to simplify user and group management. Quest Authentication Services efficiently processes this information for the flat Unix group namespace using the PAC information in Kerberos tickets obtained from AD.
- **Disconnected Support:** Quest Authentication Services uses an intelligent caching architecture to enable Unix and Linux systems to continue to operate efficiently when Domain Controllers are unavailable.
- **Native Packaging Support:** The product's client software is packaged with native support for Linux, HP-UX, Solaris and AIX platforms, to simplify deployments and updates.
- **Secure LDAP without SSL:** All LDAP communication with AD is secured using Kerberos, which eliminates the need for configuring AD to support SSL and distributing SSL certificates to Unix and Linux systems.
- **Legacy NIS Compatibility:** Quest Authentication Services allows administrators to migrate NIS information to AD (including managing NIS Maps in AD), while providing backward-compatibility for existing NIS client applications without compromising security.
- **Schema Compatibility:** Quest Authentication Services supports the RFC 2307 schema adopted for the R2 release of AD. The product also allows for custom schema configuration.
- **Third-party Kerberos Compatibility:** Quest Authentication Services allows administrators to quickly point their Kerberized applications at the AD configuration used by the product.
- **User/Group Migration Utilities:** Quest Authentication Services provides a scriptable utility that can create Unix-enabled users and groups in AD, migrate existing Unix account information to existing AD users and groups and create customized migration scripts. It also allows for quick creation of alternative Unix personality objects when migrating conflicting account domains.

Quest Authentication Services in the Real World

Currently Quest Authentication Services solution has been adopted by more than 300 enterprise companies worldwide. These customers represent an installed base of more than one million “seats” (users and servers) of the product. In addition nearly 50 percent of the Fortune 500 are either current users of the solution or are deeply involved in serious evaluation. No other Unix and Linux-to-AD integration solution can claim the installed base, market success, or large-scale implementations than Quest Authentication Services.

Identity Consolidation—Southern Company “Gets to One”

Southern Company, one of the largest electricity providers in the United States experienced significant ROI as it migrated from Windows NT to Windows XP and AD. The identity management benefits of a single UID in AD, for 20,000 Windows users saved the company millions of dollars annually in streamlined administration and enhanced security and compliance. Unfortunately, Southern Company did not enjoy the same benefits for its 350 Unix servers.

An internal audit revealed weaknesses in the way the company provisioned and de-provisioned Unix users. In addition, due to the fragmented nature of identity management in Unix, highly compensated Tier 3 Unix IT staff were tasked with the menial tasks of password rests and de-provisioning on Unix resources. This approach was not cost-effective and produced negative implications on the rest of the Unix environment as core support personnel were diverted from their primary responsibilities to address Unix issues that in the Windows world could be handled by the help desk.

The company pursued internal projects to integrate its variety of Unix systems with AD but found the available do-it-yourself solutions didn’t scale to the desired level, would be difficult to support, and required a higher level of internal expertise that Southern Company possessed. The project lead found Quest Authentication Services through a Google search on “Unix to AD integration”.

Southern Company adopted Quest Authentication Services and went through the process of reconciling all Unix UIDs with AD. This best-practices approach allowed the company to extend the benefits of single sign-on and one source of authentication to Unix systems. Consequently Southern Company was able to achieve its compliance goals while dramatically improving operational efficiency. Unix de-provisioning tasks that previously required up to 350 separate visits to Unix servers, could now be performed through a one-time transaction in AD. In addition, Unix password resets were no longer the responsibility of Tier 3 support personnel but could be managed by the Windows help desk and could be managed much more efficiently since only the single AD password is required for access to all systems.

For a more detailed discussion of Southern Company’s implementation of Quest Authentication Services, see the case study: Quest Helps Southern Company “Make it One” with Quest Authentication Services.

NIS Migration—Large Technology Company

One of the world’s largest technology companies included a very large and widely distributed Unix environment. Due to growth by acquisition, the company ended up with literally hundreds of sites worldwide and each site represented at least one NIS domain. Realizing the compliance liability of NIS the company looked to Quest for a solution that would provide immediate benefit of eliminating NIS and bringing all Unix identities and authentication into AD. At the same time, the company wanted a solution that would provide the future path to consolidation of Unix identities into a single AD identity for tens-of-thousands of users.

A very thorough evaluation of available solutions convinced the company to adopt Quest Authentication Services. Key differentiators were the Quest One legacy in the Unix-to-AD integration space, the solution’s strict adherence to standards, and the long-term viability and flexibility that approach brings to a transition from hundreds of NIS domains and tens-of-thousands of conflicting identities to a truly consolidated authentication infrastructure based on one identity in AD.

Long-term ROI—Large Financial Institution

One of the United States' largest banks—and one of the ten largest AD installations in the world—found that the task of password management for a very diverse and widespread enterprise was costing $1 million a month. The typical user at this bank had 18 separate identities, and consequently 18 separate usernames and passwords. In an effort to overcome this obviously inefficient and possibly non-compliant practice, the bank spent several million dollars on various password synchronization solutions. Unfortunately these solutions did not address the underlying problem—too many UIDs and passwords—and the monthly password management expense did not decrease.

The bank adopted Quest Authentication Services and immediately was able to consolidate identities from 18 down to 2 by bringing all Unix and Linux systems into AD. With a gradual roll-out of the solution, the bank was able to realize an immediate 35 percent decrease in password resets alone with the ROI increasing as the rollout continues. Currently Quest Authentication Services and AD are responsible for more than two million Internet-based customer authentications a day.

As it expanded its deployment of Quest Authentication Services, the company found it could easily implement a single sign-on solution for its Unix based applications at its retail banking branches, allowing thousands of teller applications to be accessed directly using the Kerberos credential acquired when the user logs on to their Windows desktop with AD.

Conclusion

The challenge of identity management in heterogeneous environments is primarily caused by the multitude of identity stores and authentication mechanisms that traditionally accompany Unix and Linux systems. Windows, on the other hand, provides a much more compliant, scalable and manageable identity management infrastructure, through the powerful standards-based capabilities of AD. AD offers true single sign-on, and a platform for powerful identity management and compliance of Windows resources—but only Windows resources. Many organizations are looking for ways to extend the benefits of AD to Unix, Linux and Java—those systems that pose the biggest challenge in cross-platform identity management.

Quest Authentication Services provides a standards-based extension of AD's authentication, single sign-on, and access management capabilities to Unix and Linux systems. It provides a more secure alternative to non-compliant Unix directories such as NIS, and allows for a single point of authentication, management, and administration of Unix and Linux from within the infrastructure already in place for Windows systems. In addition, Quest Authentication Services provides a foundation for simplified identity management as AD becomes the platform for advanced identity administration capabilities for Windows, Unix and Linux systems. The standards-based architecture of Quest Authentication Services, allows provisioning, password management, audit and meta-directory solutions from the Quest One, Microsoft, and others to seamlessly integrate.

Key capabilities of Quest Authentication Services include:

- Single sign-on for Unix and Linux systems and applications
- NIS migration and UID consolidation
- Enterprise Group Policy
- Smart card/multi-factor authentication
- Integration with identity management tools
- Extending AD-native capabilities to Unix and Linux systems and applications

Among the benefits of an integrated approach to identity management, some of the most prominent include:

- Enhanced security
- A path to regulatory compliance
- Increased ROI
- Operational efficiency
- Requires no change to existing infrastructure
- Scalability
- Flexibility

Through Quest Authentication Services Unix and Linux systems and applications can actually join the AD domain for centralized management and single sign-on.

Quest One Identity Solution provides a superior integration point for AD-based identity management due to their strict adherence to and use of industry standards. This same standards-based strategy provides tight, often seamless integration with other identity management offerings that Quest One has to offer, as well as other vendors, including meta-directory providers.

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.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service. Visit SupportLink at **https://support.quest.com**.

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.

QUEST SOFTWARE
Smart Systems Management

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.

© 2009 Quest Software, Inc.
ALL RIGHTS RESERVED.

Quest Software is a registered trademark of Quest Software, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.
TBW-ExtendingNativeADCapabilities-US-AG-20091206