

Integrating Unix and Linux Systems with Active Directory

Technical Brief



*written by
Jackson Shaw
Senior Director,
Product Management - Active Directory
Infrastructure Management
Quest Software, Inc.*

© Copyright Quest® Software, Inc. 2005. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Updated—October, 21 2005

ABSTRACT

Integrating Unix, Linux, and Java Systems with Microsoft Active Directory

One of the biggest challenges facing heterogeneous enterprises is providing secure access, authentication, and authorization of users to all systems, regardless of platform. Microsoft Active Directory (AD) has proven ideal in meeting this objective for Windows resources. Unfortunately, by itself AD can't provide the same level of security, compliance, and scalability to Unix, Linux, and Java systems. Quest Software can bridge that gap by natively integrating the same standards that make AD so powerful for Windows systems on non-Windows systems. The result is a single, proven, and powerful access, authentication, and authorization mechanism for all systems and platforms based on the already ubiquitous AD infrastructure.

CONTENTS

- ABSTRACT I**
- ABOUT QUEST INFRASTRUCTURE MANAGEMENT..... 3**
- ABOUT QUEST SOFTWARE, INC. 3**
 - CONTACTING QUEST SOFTWARE..... 3
 - CONTACTING CUSTOMER SUPPORT..... 4
- BUSINESS PROBLEM: USER AUTHENTICATION IN HETEROGENEOUS ENVIRONMENTS..... 5**
- ADDRESSING INTEGRATED ACCESS, AUTHENTICATION AND AUTHORIZATION FOR THE ENTERPRISE 7**
- THE SOLUTION: IDENTITY INTEGRATION THROUGH VINTELA AUTHENTICATION SERVICES 11**
- THE BENEFITS OF IDENTITY INTEGRATION 12**
- CONCLUSION 15**
- ABOUT THE AUTHOR 16**

ABOUT QUEST INFRASTRUCTURE MANAGEMENT

Quest Software, Microsoft's 2004 Global Independent Software Vendor Partner of the Year, provides solutions that simplify, automate, and secure Active Directory, Exchange, and Windows, as well as integrate Linux and Unix into the managed environment. Quest's Infrastructure Management products deliver comprehensive capabilities for secure management, migration, and integration of the heterogeneous enterprise.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Customer Support

Quest Software's world-class support team is dedicated to ensuring successful product installation and use for all Quest Software solutions.

SupportLink www.quest.com/support
Email at support@quest.com.

You can use SupportLink to do the following:

- Create, update, or view support requests
- Search the knowledge base
- Access FAQs
- Download patches

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 handle mixed-platform environments that 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. Some platforms have 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.

Most IT organizations have standardized their business infrastructure on Microsoft products, specifically Windows 2000/2003, 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 employ Microsoft AD.

An authentication and management scheme built around AD works very well for Windows systems, but what happens when Unix and Linux enter the mix?

Windows systems do not authenticate users the same way that Unix and Linux systems authenticate users. 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. 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 labyrinthine multi-platform scripts that must be maintained and supported. Such “limited” solutions lack commercial maintenance and support as well as important functionality and flexibility.

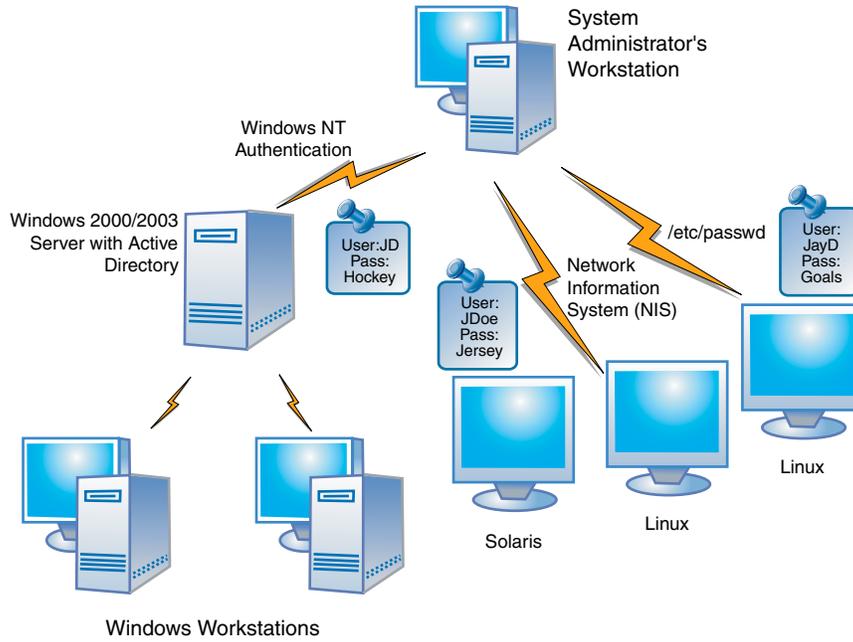


Figure 1.1: Example of multiple authentication schemes

ADDRESSING INTEGRATED ACCESS, AUTHENTICATION AND AUTHORIZATION FOR THE ENTERPRISE

The rapid growth of technology and the expansion of business boundaries beyond the enterprise have led to a growing problem for system and IT administrators. The need to provide secure and authorized access for employees, suppliers, partners, and customers to networks, systems, applications, and data across multiple operating system environments has been difficult for organizations to manage. Solutions and methods are available to address the problems associated with providing users with authorized access to systems, applications, and data, but most of these solutions:

- Lack a single, centralized point of control across multiple platforms
- Are expensive and difficult to implement
- Are inefficient in mitigating the risk of unauthorized access

To provide users with secure access to systems, applications, and data, an IT administrator must create, manage, and maintain each user's unique identity. This unique identity provides authentication and authorization for the user to access specific systems and information. Authentication is the process that verifies who the user is and how the user proves who he or she is. Authorization gives a user access to specific network resources and applications based on policies established by the administrator. A user's identity is traditionally established by creating a user name and password. This user name and password is unique for each user.

Implementing Integrated Identity Management for Mixed Environments

The complexity and cost associated with managing and maintaining a user's identity has grown due to several factors affecting enterprise organizations throughout the world. First, it is common for medium- to large-enterprise organizations to employ multiple operating system environments, such as Windows, Unix, or Linux to address their critical business needs. Second, the boundaries of business have grown beyond the traditional brick and mortar confines of a company and its infrastructure. No longer are business boundaries limited to internal employees accessing data on company networks. Today's global business model enables not only employees to access network resources, systems, and applications, but partners, suppliers, and customers may also have access to these mission-critical systems. Often, this access is achieved through Web services and applications based on the Java and J2EE architecture.

Compliance with Industry Regulations and Standards

In addition to the changing landscape of business and the deployment of multiple operating systems, regulatory requirements have also emerged as a factor influencing the need to control, monitor, and manage the secure access of systems and applications by users of all types. Several regulations have been established to control and safeguard the access of network resources and applications. Examples of these industry regulations and standards include:

- The Gramm-Leach Bliley Act (GLB)
- Healthcare Information Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act of 2002 (SOX)
- 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)

Enabling secure and authorized access to multiple users has become a necessity for IT managers. The challenge of protecting systems and data has grown, as more and more users require 24 x 7 access to systems and applications. The dilemma for IT managers is how to effectively enable various users to access systems and application, while ensuring safeguards and controls are in place to not only control access, but also protect the organization's "crown jewels"—its mission-critical systems and data.

Password Management Nightmare

According to a 2003 IT survey conducted by the Meta Group, users have access rights to multiple systems and applications. The survey indicated that, on average, a single user will have access to 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, such as Windows, Unix and Linux systems.

Typically, user accounts that provide access to a Windows infrastructure are established and managed by the Windows IT administrator. Likewise, user accounts for a Unix environment are created and maintained by the Unix administrator. As a result, a user with access to multiple systems and applications must remember their specific user name and password for each system or network that they are authorized to access.

Remembering Multiple Passwords

Remembering multiple user names and passwords provides several challenges, not only for the user, but also for those who are responsible for supporting that user. Research has found that users with multiple user names and passwords often write their user identities down on a piece of paper, such as a post-it note, for easy recall. Writing a user name and password down creates a potential security risk for the organization. A genuine threat exists for disruption and loss of data if someone other than the designated user were to gain access to network resources, systems or mission-critical data.

Help Desk Support Costs

In addition to problems and risks associated with unauthorized access, 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 estimated to be \$38 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.

Supporting, managing, and maintaining user access to systems and information can be complex and costly for enterprise organizations with multiple platform environments. Potentially more costly to an organization is unauthorized access to systems and mission-critical data by an employee or by an outside threat.

Disabling Access for Terminated Employees

Managing and maintaining user access for existing users represents only part of the challenge for IT administrators. Another challenge is removing a user with multiple identities or access to multiple systems and applications once that user has been terminated. According to Meta, most organizations do not have an effective process for removing terminated users. In fact, 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 a potential risk of data loss and disruption to business.

Many companies have begun addressing the problems associated with identity management, and the management of multiple user names and passwords. However, IT managers are finding it difficult to effectively address identity management across multi-platform environments, due to the fact that independent solutions are based on proprietary technologies which are not centralized or integrated for multiple platforms.

Increased Operational Cost and Complexity

In addition to the dilemma of enabling access to multiple users while mitigating risks and ensuring protection of mission-critical systems and applications, IT managers are increasingly charged with minimizing operating expenses. Likewise, service providers are looking for solutions and methods to increase their margins and reduce time-to-closure rates for service level agreements.

The complexity of managing mixed operating environments has forced many enterprise organizations to use separate tools and processes to accomplish tasks that are essentially the same regardless of the platform. Some operating systems offer proprietary tools to address this problem, but many administrators simply resort to third-party tools or develop custom scripts to accomplish routine tasks. The ongoing overhead associated with maintaining multiple tools and processes to accomplish the same task is an inefficient and costly use of resources.

Inefficient Solutions Developed In-House

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 a Unix-based implementation to solve the problem. However, there are typically several limitations and potential 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, tested, and how it should be implemented in specific environments. Undocumented processes for identity and access management represent a significant risk to the organization.
- **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. On-going support and maintenance of a process is often diluted when changes occur in personnel responsible for these processes. Additionally, when an administrator does leave, an IT department may have a duplication of efforts as a new administrator responsible for identity management creates a new process based on scripts and methods he or she prefers using.
- **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. Using proprietary or non-standards based tools can lead to compromises and breakdowns in security. 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.

THE SOLUTION: IDENTITY INTEGRATION THROUGH VINTELA AUTHENTICATION SERVICES

Many organizations are attempting to address the growing problem of implementing identity and access management. However, because of the complexity caused by disparate platforms, IT managers and service providers are looking for solutions that provide interoperability and integration across platforms while simplifying implementation and reducing costs.

Vintela Authentication Services from Quest Software, Inc. extends AD's reach, allowing Unix and Linux system administrators to centralize their access, authentication, and authorization needs around AD. Vintela 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 Vintela 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 Vintela 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.

Using the Microsoft Management Console from a central location, the system administrator can manage user and computer accounts in AD. Administration for Unix and Linux can be performed using command line tools.

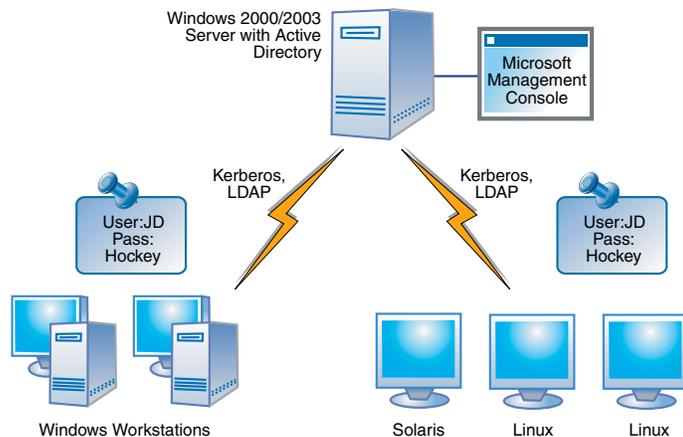


Figure 2.1: Centralized authentication using Active Directory and Vintela Authentication Services

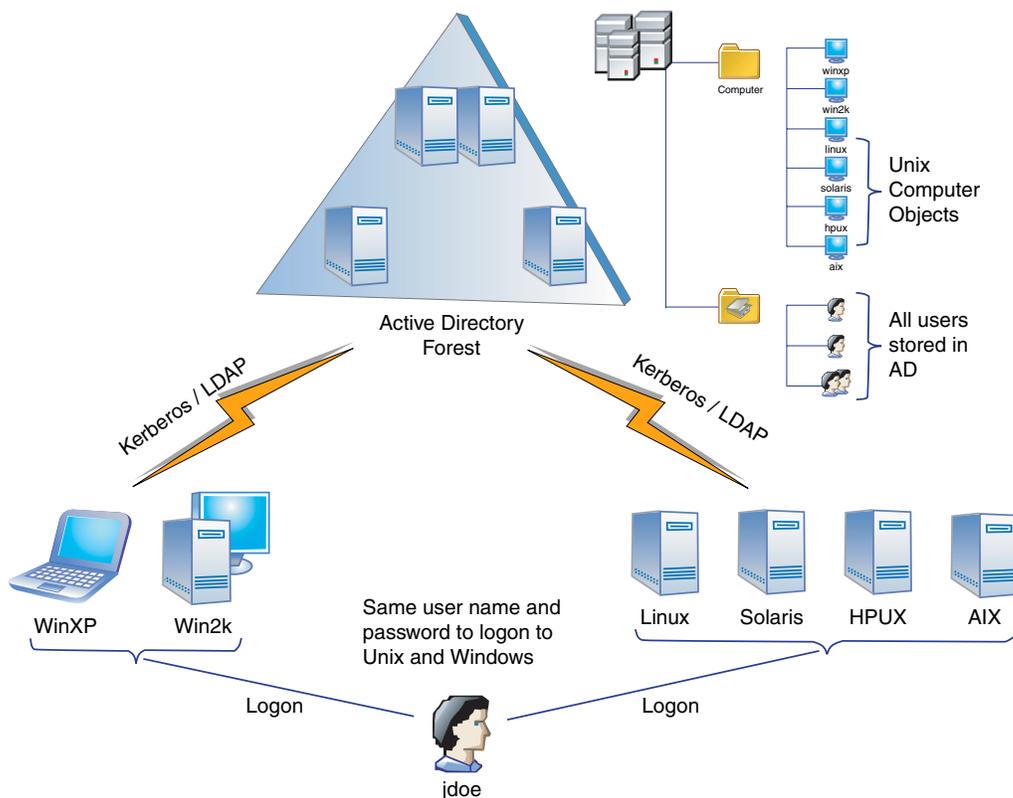
THE BENEFITS OF IDENTITY INTEGRATION

Vintela 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)

Utilizing these standards enables Vintela Authentication Services to integrate transparently with Windows, Unix, and Linux environments without the use of proprietary protocols, methodologies, or additional infrastructure.



Secure

One defining feature of Vintela 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, Vintela 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.

Unobtrusive

Vintela 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 AD.

Scalable

In a Kerberos/LDAP-based authentication system, the scalability bottleneck is always the LDAP server. Vintela 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
- LDAP_BUSY fail-over to cache
- 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

Vintela 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

Vintela 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, Vintela 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.

CONCLUSION

The current deployment standard in IT organizations belongs to Microsoft. There is ample reason to believe this standard will continue in the foreseeable future. However, not all IT organizations have the luxury of a single-vendor infrastructure, so it is not uncommon for system administrators to have more than just Windows machines providing their business infrastructure.

Over the past few years, Unix and Linux have been gaining considerable momentum. The migration of servers and workstations from one operating system to another, or even the introduction of a new operating system into the existing infrastructure, has been problematic, mostly due to incompatibilities between the new technologies and those that already exist. This is as true for bringing Unix or Linux into a Windows network as it is for bringing Windows into a Unix or Linux network.

To date there has been a considerable amount of “gray area” between the Unix and Linux and Windows worlds, making deployment and integration of divergent operating systems difficult for system administrators. It is within this gray area that Quest has focused Vintela Authentication Services. By providing an intermediary between AD and industry-standard authentication technologies used by Unix and Linux, Vintela Authentication Services eases the pain of deployment, migration, and integration of Windows, Unix, and Linux. It also provides a centralized, secure, and robust solution for all of your access, authentication, and authorization needs based on an already deployed, proven, and preferred AD infrastructure.

For more information about Vintela Authentication Services, please visit the Vintela Web site at www.vintela.com/products/vas.

ABOUT THE AUTHOR

Jackson Shaw joined Quest Software, Inc. with its recent acquisition of Vintela. Shaw oversees product direction, strategy, and go-to-market activities for all Active Directory and multi-platform integration products. With more than 15 years of experience, Shaw was a key member of the Identity and Access Management marketing team for the Windows Server Marketing group at Microsoft Corp. He was responsible for product planning and marketing for Microsoft's identity and access management products, including Active Directory and Microsoft Identity Integration Server (MIIS) 2003.

Before joining Microsoft in 1999, Shaw served as vice president of sales for Toronto-based ZOOMIT Corp., a pioneer in the development of meta-directory products. He was also a member of the management team that successfully oversaw the company's acquisition by Microsoft in 1999. Before joining ZOOMIT, Shaw held IT management roles at the International Development Research Centre, a Canadian corporation created to help developing countries find long-term solutions to social, economic, and environmental problems. Shaw has been involved in directory, meta-directory, and security initiatives since 1988. He studied computer science and management information systems at the University of Ottawa. He is a member of the Association for Computing Machinery.