

An introduction to Active Directory integration for Unix and Linux systems

Tech Note #1 in the "Identity Management" series

By Doug Miller (Interop Systems)

Many IT shops in both large and small organizations use more than one operating system to solve their computing needs. While Windows is the market leader for both server and desktop computing, Linux is being used more and more – especially for server workloads. UNIX has a long history as a server operating system and is widely used for many business workloads. In fact, in a recent Gartner report 92% of IT organizations that responded to a recent survey stated that their company uses Windows and Linux or UNIX for server computing (as well as other operating systems such as mainframes in some cases).

While having the freedom to select the right operating system for your particular workloads is appealing, it is sometimes not so appealing trying to solve common integration challenges. One of the most requested integration needs is the ability to use a single identity management infrastructure across all operating systems in an organization. Identity management in this case is the ability to create a single user account within a directory services system and be able to leverage the account information and authentication credentials across multiple systems.

This series of tech notes will focus on several ways to solve this integration need for bridging the identity management requirements for an environment with both Windows and UNIX or Linux systems. For each of the solutions, we will use Microsoft's Active Directory as the central repository for user account information and passwords. The challenge that is addressed in these notes is how to enable Linux and UNIX systems to use Active Directory-based user account information and passwords as the centralized directory system for authorizing and authenticating users who log in to the system. Why use Active Directory for centralized account information storage? Microsoft's Active Directory has been deployed in virtually every organization that uses Windows. Given that Windows desktop systems, including XP and Vista, are enabled to use Active Directory servers for validating credentials when a user logs in, it makes sense to also use Active Directory as the directory solution for non-Windows systems. Using a single directory system for Windows, Linux and UNIX has numerous advantages, including:

- Users have one login name and one password that can be used across Windows, Linux and UNIX
- If the user changes his or her password on one of the systems, the new password is automatically applicable to the other systems
- Help desk calls are reduced as users have fewer account names and passwords to remember
- Sys admin costs are reduced as you are no longer required to create user accounts on every system that is deployed – instead you now create the account once in Active Directory and each enabled Windows, Linux or UNIX system can now use that account information for validating users
- Consistent policies such as password length and complexity can now be enforced across Windows, Linux and UNIX

It should be noted that there are at least two popular commercial products that provide solutions to these challenges. [Centrify's DirectControl](#) product line and [Quest's Vintela Authentication Services](#) both provide off-the-shelf solutions to allow Linux and UNIX systems to join an Active Directory domain and use Active Directory as the centralized authority for authentication, authorization, directory information and policy management. However, many users need only basic identity management capabilities and wish to solve this need using "free" software.

To address these basic requirements, this series of tech notes will cover the steps required to enable various levels of Active Directory integration using three popular solution sets. While there may be other methods or products that can be used to address these requirements, we have chosen three common methods that leverage "free" software and use widely available software and tools. The three methods are:

1. Using Microsoft's Server for NIS, Identity Management for UNIX and Kerberos for Directory and Authentication Services

By using the UNIX NIS server capabilities in Windows Server 2008 or Windows Server 2003 R2 for directory services and the built-in Kerberos system in Windows Server for authentication, Linux and UNIX systems can use Active Directory for user account information and password services. This solution uses native Kerberos on Windows, Linux and UNIX instead of password synchronization for validating users at log in, and the Active Directory NIS server for storing and retrieving user information instead of using the /etc/passwd file on Linux and UNIX.

2. Using Samba client technology and Kerberos for Active Directory-based identity management

This solution also uses Kerberos for authentication but uses Samba for user account information storage. Many customers use Samba file sharing technology on UNIX and Linux and wish to use Samba client technology to enable centralized integrated directory and identity management services with an Active Directory Windows Server. This tech note outlines how to accomplish this with the standard Samba technology that ships in popular Linux distributions and commercial UNIX systems.

3. Using native LDAP, native Kerberos and Windows Server Active Directory services and schema for cross-platform identity management

This final tech note addresses the fact that many customers are moving away from NIS and are standardizing on LDAP for directory services across all platforms. Active Directory is an LDAP directory. Windows Server 2008 and Windows Server 2003 R2 even include a standards-based LDAP schema for typical UNIX user and group attributes. This tech note describes how to leverage these Microsoft technologies on the server side and use Open Source technologies on the UNIX or Linux client side to build an integrated Active Directory-based identity management solution for Windows, UNIX and Linux.

SOLUTION	PROS	CONS
Microsoft's Server for NIS, Identity Management for UNIX and Kerberos for Directory and Authentication Services	<ul style="list-style-type: none"> • Uses standard components that ship with Windows and Linux • Easy to setup on Linux, requires configuration on Windows Server • Uses standards-based technology for all components (NIS, Kerberos) • Centralized UID, GUI mapping 	<ul style="list-style-type: none"> • Uses NIS for directory services rather than LDAP • Does not allow for joining the Active Directory domain. Only provides centralized directory and authentication services. • Self-supported solution
Samba client technology and Kerberos for Active Directory-based identity management	<ul style="list-style-type: none"> • Requires no special configuration on the Windows Server side • Easy to setup on the Linux side • Mature technology that is widely used • Allows Linux system to join Active Directory domain 	<ul style="list-style-type: none"> • Stores some user information on each Linux system instead of centrally, requiring manual synchronization in some cases • Proprietary solution (Samba) vs. standards-based solution (LDAP) • Self-supported solution
Native LDAP, native Kerberos and Windows Server Active Directory services and schema for cross-platform identity management	<ul style="list-style-type: none"> • Uses LDAP instead of NIS for directory services • Standards-based solution (LDAP, Kerberos) • Detailed setup instructions in Microsoft Solution Accelerator 	<ul style="list-style-type: none"> • More complex to setup • Does not allow for joining the Active Directory domain • Self-supported solution
Commercial solutions such as Centrify's DirectControl or Quest's Vintela Authentication Services	<ul style="list-style-type: none"> • Very easy to set up • Provides virtually all AD client services to Linux and UNIX • Allows Linux system to join Active Directory domain • Fully supported commercial solution 	<ul style="list-style-type: none"> • Proprietary software installed on both server and client • Requires per system license to be purchased

For each of the tech notes in this series, we have used Windows Server 2003 R2 Standard Edition on the server side and Fedora Core 6 Linux on the client side. However, most of the steps or similar steps can be used to implement these solutions on other Linux or UNIX systems and on Windows Server 2008. For more detailed information on addressing the need for integrating Active Directory security and directory services into a Linux or UNIX environment it is also worth reading the Microsoft Solution Accelerator titled:

“Windows Security and Directory Services for UNIX Guide v1.0” and found on:

<http://www.microsoft.com/technet/solutionaccelerators/cits/interopmigration/unix/usecdirw/00wsdsu.mspix>

If you have comments on these tech notes or wish to provide enhancements or corrections, please feel free to post a question in the [Interop Community](#) forums.