Cross-Platform Authentication and Identity Management Using Microsoft Active Directory

By Matt Peterson

THE world of enterprise management is at a crossroads, with several forces pulling at the support and management staff of organizations of all sizes.

On one hand, the modern enterprise is a complex mix of Windows, UNIX (often several different flavors of UNIX), Linux, Java, and even Mac systems, each requiring unique and specialized management attention. On the other hand, organizations are constantly charged with streamlining operations, reducing costs, and gaining firmer control of the total cost-of-ownership (TCO) of computing resources. Add to the mix the glut of federal regulations—such as Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley—that require greater security, and a higher level of corporate accountability for data. Suddenly the mission of centralizing IT support and management in a more cost-effective infrastructure seems impossible.

THE NATURE OF TODAY'S ENTERPRISE

Today's enterprise organization requires IT support for a variety of mission-critical software solutions running on several different platforms. Typically, Windows resides on a vast majority of an enterprise's desktops. An organization also generally has a high number of Windows servers and a significant investment in Microsoft infrastructure and management technologies such as Active Directory and Systems Management Server. Often, these Windows-centric organizations have centralized Windows resources into a single Active Directory domain—or "trusted zone"—streamlining authentication and identity management to a single sign-on function.

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 are unique for each user.

In the Windows world the infrastructure and tools are in place, laying a foundation for single sign-on and regulatory compliance, management task consolidation, and reduced TCO for Windows resources. But what about UNIX, Linux, Java, and Mac resources?

A typical enterprise supplements its Windows environment with a variety of specialized systems and application running on UNIX boxes. The same organization might have a small, but mission-critical segment of Macs supporting a creative team. Linux is quickly finding root in enterprises of all sizes. And any organization with Web services, eCommerce, or rich applications will use Java.

Unfortunately this highly diverse (some might say fragmented) mix of operating systems brings an entirely new level of complexity to enterprise management. Incompatibilities between these disparate platforms 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 offer proprietary tools, but often administrators must resort to third-party tools or manual, "home-grown" processes to accomplish routine tasks. For example, let's look at a simple process of de-provisioning an employee. In Windows, a single transaction in Active Directory will eliminate access for the entire Windows domain. But the same employee also has access to UNIX, Linux, Mac, and Java systems. De-provisioning on each of these systems requires individual actions with each OS. There is no centralized point of management that touches all systems. A task that takes mere seconds in Windows quickly grows to many minutes, or even hours, when other platforms enter the mix. In the worst case, the de-provisioning occurs where it is easy to do (for example, on Windows and select high-volume UNIX systems) but doesn't happen for other more obscure systems. Security is compromised, and

valuable management personnel are diverted to unproductive password management tasks.

ADDRESSING INTEGRATED IDENTITY MANAGEMENT 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 exist that 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, and are expensive and difficult to implement. And are inefficient at addressing critical requirements to sufficiently mitigate the risk of unauthorized access.

Several key challenges face managers of multi-platform networks:

- ***The Password Management Nightmare*—**According to a 2003 IT survey conducted by the Meta Group, 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, including 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 his or her specific user name and password for each system or network he or she is authorized to access.
- ***Remembering Multiple Passwords*—**Remembering multiple user names and passwords provides several challenges, not only for users, but also for support personnel. 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. This practice creates a security risk for the organization. Operations can be disrupted and data lost if someone other than the designated user were to gain access to network resources, systems, or mission-critical data.
- ***Help Desk Support Costs*—**Beyond the risk associated with unauthorized access, users generally call the help desk 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 an employee—particularly a disgruntled employee—to continue to access systems and mission-critical data presents a genuine risk of data loss and disruption to business.

  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*—**It's a tough balancing act to enable access for multiple users on multiple systems while mitigating risks and ensuring protection of mission-critical systems and applications. But the charge from corporate administration increasingly demands that IT managers minimize operating expenses.

  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 Unix-based scripts to solve the problem. However, these solutions present several limitations and security risks, including:
  - 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 a constant within any organization. IT administrators may change positions, responsibilities, and jobs. The knowledge used to develop an in-house or "home-grown" process usually goes with the administrator when he or she 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.

ACTIVE DIRECTORY—A SCALABLE IMPLEMENTATION OF STANDARDS

In the Windows world, each of these challenges is very effectively addressed by Active Directory. Most IT organizations have standardized the bulk of 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 centralized authentication and management system employ Microsoft Active Directory.

Active Directory uses an industry standard called Kerberos to provide secure single sign-on for all users and resources in an Active Directory domain. Through Kerberos, credentials are secured in an infinitely scalable way that allows organizations of any size to authenticate and manage user identity for all Windows resources from a single, centralized interface—Active Directory. An authentication and management scheme built around Active Directory works very well for Windows systems, but what happens when UNIX and Linux are brought into the fold?

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. As discussed earlier, some system administrators resort to home-grown password synchronization scripts, but quite often what they end up with is an unnecessary point-of-failure and a labyrinthine 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.

On the other hand, commercial synchronization solutions or meta-directories require complex infrastructure and are difficult to manage while still not addressing some of the core concerns that are driving the move to single sign-on in the first place. In addition, these solutions often require redundant infrastructure that can be extremely complex and add still another layer of management.

IT managers must find a way 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.

THE SOLUTION—BRINGING UNIFORMITY THROUGH STANDARDS

With an Active Directory infrastructure already in place and providing efficient, secure identity and authentication management, the logical result is to extend the reach of Active Directory to non-Windows resources—much easier said than done.

The very standards that make Active Directory so valuable in Windows (namely Kerberos and LDAP) can be equally valuable for UNIX and Linux systems if only they could be applied natively and consistently across all Platforms. Unfortunately, the highly diverse world of UNIX and Linux has prevented all but the most ambitious organizations from making the attempt. And even those organizations generally abandon the effort due to its complexity. Basically a SuSE Linux box requires a unique implementation of Kerberos just like a Sun box and an AIX box require their own unique implementations. And different versions of the OS also require unique and specialized implementations.

An example of the commercial application of these principles is a solution from Vintela called Vintela Authentication Services (VAS). Developers created that uniformity by applying Kerberos natively to the wide range of Unix (AIX, HP-UX, and Solaris) and Linux (SuSE and Red Hat) platforms in such a way that each can act as a full citizen in Active Directory. With Kerberos implemented natively, UNIX and Linux systems appear in Active Directory just like Windows machines. Now the efficiencies, security, and control available in Windows through Active Directory have been extended to the rest of the enterprise.

The solution utilizes a number of Internet Engineering Task Force (IETF) interoperability standards. These standards provide the "glue" that allows Active Directory 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)

Let's go back to our de-provisioning example. Because our large variety of UNIX systems have now become part of the Active Directory "trusted zone", a single task in Active Directory inactivates the user's account across all systems. No longer does an IT manager or help desk technician need to manually roam from system to system—using unique tools on each platform, with separate processes for each system—simply to de-activate a user account. Similarly, the end user has a single user name and password to remember. Valuable support personnel are free to focus on critical support issues, not trivial password management tasks. And, the security holes have been slammed shut.

Password synchronization is unnecessary because all systems belong to Active Directory. Meta-directory solutions can be eliminated, removing a complex, costly, and cumbersome layer of infrastructure. A tool that most organizations are already using and using successfully—Active Directory—can now extend its value to the rest of the enterprise.

Total cost of ownership drops. Compliance increases. And complexity diminishes.

By integrating seamlessly with UNIX and Linux *Pluggable Authentication Modules* (PAM) and *Name Service Switch* (NSS) systems, these commercial solutions automatically provide authentication to any PAM/NSS-enabled service. Issuing "session keys" permits one

login/authentication to remain active for all 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 Active Directory. Administration for UNIX and Linux can be performed using command line tools.

The beauty of this native application of standards to each individual Unix/Linux operating system lies in its ability to leverage the advantages of Windows security and efficiency through Active Directory while preserving the unique aspects, characteristics, and experience of the Unix/Linux system.

THE BENEFITS OF CROSS-PLATFORM AUTHENTICATION AND IDENTITY MANAGEMENT

Approaching identity management and authentication in this way provides some distinct benefits over password synchronization, meta-directories, or home-grown scripting. These benefits include:

- ***Security***—One defining feature of this approach 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, VAS employs SASL authentication and "GSSAPI wrapping" using Kerberos session keys. This allows for encryption of the entire LDAP session—no LDAP information of any kind is ever sent in clear text.
- ***Unobtrusiveness***—This approach is designed to integrate into existing networks with minimal disruption of users and system administrators. It uses Unix and Linux authentication and account abstractions (collectively referred to as PAM/NSS) to make the solution compatible with a wide range of commercial and open-source software. Consequently, 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 through Active Directory.
- ***Scalability***—In a Kerberos/LDAP-based authentication system, the scalability bottleneck is always the LDAP server. VAS minimizes the demands made on the LDAP server and the Kerberos key distribution center (KDC) that are located on the Windows 2000/2003 server, significantly reducing the load on the Active Directory back-end.
- ***Robustness***—Authentication and identity management in this form is ideal for weakly connected environments. It is suitable for use with systems such as UNIX and Linux laptops because it can continue operation even if Active Directory goes down or if network components fail, allowing system logins as if still connected.
- ***Flexibility***—This solution was built with an understanding of 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, it exposes 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, very few IT organizations have the luxury of a single-vendor infrastructure. 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 and existing technologies. 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/Linux and Windows worlds, making deployment and integration of divergent operating systems difficult for system administrators. It is within this gray area that a native, consistent, and sound implementation of standards can bring uniformity to these disparate systems to create a single sign-on "trusted zone." By providing an intermediary between Active Directory and industry-standard authentication technologies used by Unix and Linux, organizations can ease the pain of deployment, migration, and integration of Windows, Unix, and Linux, and provide a centralized, secure, robust solution for all of their authentication needs.

NaSPA member Matt Peterson is Chief Technology Officer for Vintela, an innovative company dedicated to making Windows and non-Windows resources truly interoperable.