Planning for Single Sign-On: Part 1 — An Overview

Single sign-on (SSO) and enterprise network management (ENM) software can improve the security and management efficiency of an enterprise network infrastructure. Because different vendors offer very different approaches to providing SSO and ENM services, the immediate challenge is to identify products that offer a "here-and-now" solution and best suit your short- and long-term needs.

BY GUY C. YOST

NEW products are being introduced to help alleviate overall inefficiencies in managing large multi-platform networks. Specific types of software that would improve the security and management efficiency of an enterprise network infrastructure fall in the "platform independent" single sign-on (SSO) and enterprise network management (ENM) categories. Because different vendors offer very different approaches to providing SSO and ENM services, the immediate challenge is to identify products that offer a "here-and-now" solution, as opposed to those based on emerging standards, and to ascertain which products would best suit your short- and long-term needs from a cost/benefit perspective. It is also important to identify common technology between SSO and ENM solutions, so if possible, a foundation for both types of services can be shared.

This article presents an overview of SSO and password synchronization technology, their functional characteristics, and how they can help improve network security as well as simplify network administration. Part II will offer a project-planning guide for evaluating and implementing an SSO solution, and the concluding article will offer specific implementation details based on a real-life case study.

MULTI-PLATFORM SECURITY AND ADMINISTRATION HEADACHES

Today's legacy and client/server systems comprise a variety of hardware and operating system platforms that host an even more diverse set of applications, many requiring their own (stand-alone) user security management. The challenge of managing dissimilar computing environments is not unique to any large enterprise network and is considered "the norm" for most medium to large organizations.

In fact, most large networks will have at least one point of administration per multi-user platform type (OS), each likely to have its own set of guiding principles and policies. In addition, culturally distinct management procedures naturally result from distributed IT management. Inevitable differences in policy and practice will eventually cause confusion and frustration between departments within the enterprise, ultimately affecting a wide customer base.

For example, an average enterprise network user may have up to eight user accounts and corresponding passwords that he must use daily to access the Novell LAN, MVS applications, Oracle database, remote access, PeopleSoft applications, and NT and Citrix servers. Not only does the user need to keep track of all user ID/password sets, but several different customer support groups ultimately manage support for the accounts as well.

Even if users can request and maintain the same user ID on each platform, the task of keeping the passwords in sync is nearly impossible due to differences in password change policies between platforms. For example, password parameters such as minimum length, uniqueness, alphanumeric content, and forced periodic changes are very difficult to align across disparate systems that are managed by separate departments. Consequently, users end up choosing "easy" passwords so that they won't have trouble accessing their productive environments. If IT management enforces tighter security to disallow easy passwords, then all too often passwords and user IDs end up on Post-IT notes stuck to the monitor. In both cases, network security is greatly compromised.

Even if users can request and maintain the same user ID on each platform, the task of keeping the passwords in sync is nearly impossible due to differences in password change policies between platforms.

To ease the burden of forcing several simultaneous password changes on users, many IT administrators feel compelled to allow users longer password expiration periods on less-used secondary systems (like stand-alone database applications), while they maintain stricter password requirements to access the enterprise network. This will assuredly lead to increased user support and password maintenance because passwords are literally forced out of sync.

In general, ongoing efforts associated with supporting the multiple sign-on ordeal adversely affect end users, network administrators, and security personnel. Although support and customer service groups have risen to the challenge, the effort to maintain customer satisfaction has become expensive. The overall financial impact is notable when the cost of all support efforts and lost user productivity are combined.

According to estimates by the Securities Industries Association, a company with 1,000 employees using a true SSO solution would save $832,500 per year in user productivity alone, not including the savings from reduced calls to help-desk staff, who would no longer spend a significant percent of their time resetting forgotten passwords. As bold as that statement may sound, even if it is only 10 percent accurate, the potential return on investment justifies a formal evaluation of SSO technology.

Beyond password and login management, controlling application and data access for a typical network user currently requires several points of administration. For example, separate management efforts are required to assign rights to applications and resources that reside on MVS, NetWare, PeopleSoft, Oracle, UNIX, and NT platforms. Organizations also stand to gain on investments that will help tie together and streamline management efforts across these multi-user platforms.

LEVERAGING DIRECTORY SERVICES

One of the industry's earliest commercially supported Directory Services available for PC-based LANs, Novell's NDS, was introduced in 1991. The uniqueness of its design combined many of today's SSO and ENM product objectives from its conception.

More than 400 products now leverage the network management and security infrastructure provided by NDS, the world's most popular directory service with more than 40 million users. With broadening OEM and third-party vendor support, NetWare shops will likely continue to benefit from NDS technology. However, the challenge that NDS (or other Directory Service) customers currently face is being able to obtain true SSO and multi-platform ENM objectives within a pure NDS environment. The industry direction suggests that independent standards will be used to allow disparate networks to share authentication services and resource security control.

Specifically, IBM, Novell, Microsoft and other major OS vendors have strong commitment to support the LDAP protocol and X.509 digital certificates. The common vision being that a central directory can maintain enterprise resource and user access information for all OS platform types and their applications. Specific aspects of distributed management on each independent platform, therefore, could be replaced by managing a central directory. While that sounds ideal, larger organizations will still need the ability to distribute directory management among appropriate support groups, though perhaps merely to avoid unpleasant politics associated with dethroning existing departmental managing entities. The directory, therefore, needs to be hierarchical and partitionable to allow independent management of organizations within the tree. Using a central directory would require that the highest management policies could be consistently implemented down through the directory structure — regulating access to mainframes, mid-range computers, LANs, and even to the desktop.

As part of an ongoing strategy, IT management will need to determine the importance of achieving SSO and ENM objectives, understand how available and emerging technology can be tied into the existing enterprise infrastructure, and evaluate the cost/benefit of doing so. The advent of Directory Enabled Applications (DEAs) and Directory Enabled Network (DEN) initiatives will also influence the role of Directory Services in the Enterprise. Finally, while the industry's commitment to making Directory Services more extensible and platform-independent strengthens, rapid developments in "platform independent" single sign-on technology have many

organizations opting to implement problem-specific solutions now, rather than waiting for standards-based products to become available. Whether to implement these "here and now" solutions is yet another issue for IT management to consider.

PASSWORD SYNCHRONIZATION AND SSO TECHNOLOGY

With various vendors offering SSO solutions, it is important to distinguish between product categories and to understand how they can benefit your existing infrastructure.

- **Single sign-on:** SSO programs are used to allow a user to authenticate once, and from then on be able to access additional network resources without providing additional passwords or login challenges. Examples: Passgo, ASG Technologies, Belcore's OnePass, Dynasoft's BoKs Desktop, CA's Unicenter, Memco's Proxima, HP Praesidium/Single Sign-On Desktop Client.

- **Password synchronization:** software used to ensure that each of a user's multiple passwords is set to the same value so that users need not remember multiple passwords for multiple systems. Examples: MPS Palace Guard Software, Passgo, Proginet.

When evaluating SSO and password synchronization solutions, it is important to keep in mind the basic pros and cons of each solution. Single sign-on systems generally have the following characteristics:

- **Convenience:** Using single sign-on, users only have to type their password when they first log in. Users can access additional systems without entering their ID and password again.

- **Centralized administration:** Most single sign-on systems are built around a centralized "authentication" server design. This allows a single administrator to add and delete accounts across the entire network from one user interface.

- **Better Auditing:** Users' activities of accessing resources on disparate systems can be centrally tracked and recorded when using an SSO system.

- **Intrusive Technology:** For today's proprietary SSO packages to function, authentication modules must be loaded on each participating OS server platform, which directs login requests to a central authentication server (AS). Client login software must be modified to send login requests to the AS, and customized API hooks for all stand-alone applications such as PeopleSoft, Oracle, and other database programs are required. Frequent upgrades to API hooks and authentication scripts are necessary as new releases of network clients, applications, and desktop OS versions become available.

> With various vendors offering SSO solutions, it is important to distinguish between product categories and to understand how they can benefit your existing infrastructure.

Password synchronization is characterized by the following characteristics:

- **Improved security over SSO:** A user must still enter his password to access each system. If a workstation is left unattended, only the systems currently logged into are vulnerable to access by someone who can reach the workstation.

- **Less intrusive than SSO:** Password synchronization does not require any new servers on the network and can be implemented without installing any new software on existing servers.

- **Lower cost:** Password synchronization can be implemented for about one-tenth the cost of single sign-on technology, but does not typically offer auditing or general centralized user management functions as does SSO.

Note: *For both technologies the "Better and Worse" Security paradox exists: An intruder knowing a valid user ID and password combination for any user would have "the master keys" to that person's network environment. However, this is thought to be offset by the fact that users are able to use stronger passwords because they have only one to remember. Security policies can therefore enforce use of more secure passwords using parameter rules.*

Although several organizations have proprietary SSO and password synchronization solutions in place, the overwhelming consensus has been that implementation is lengthy and complex. For example, we met with local IT representatives from a large insurance company who have been working with Passgo's SSO package (formerly known as Mynet from CKS) for more than two years now and have yet to achieve their SSO goals across a subset of platforms found in most large network environments. The company admits that they believe in the technology and that Passgo (considered a significant player in the SSO and password synchronization industry) has been very supportive in their efforts to achieve their goals. However, as of our recent meeting, an SSO demonstration within their MVS and NT environment was not ready to be shown due to technical problems they were currently attempting to resolve. This event is consistent with other written accounts from organizations working with SSO products, Passgo and otherwise.

It therefore seems that even with a strong commitment from a leading vendor, companies should expect implementing a proprietary SSO solution to require significant time, tribulations and internal resources. The other problem with proprietary SSO technology is that most are not based on emerging standards (LDAP or X.509 certificates), which might mean throwing out the solution (and investment) in a couple of years. As a readily available solution, however, they are in high demand, which could explain the high price tag associated with today's leading SSO software.

Advances are being made in the non-proprietary category, as well. Standards put forward by the Open Group (X/Open Single Sign On - Pluggable Authentication Modules, or XSSO-PAM) are advertised to provide an open interface between applications and sign-on systems so that whatever the underlying technology of the application's authentication technology, they will plug-and-play with a "coordinating primary"

single sign-on system. Host systems continue to maintain their own account databases, yet PAM allows applications to use a more strategic distributed security service by supporting a migration path from multiple uncoordinated security systems to a coherent security architecture for all applications.

Although that solution may sound ideal, the troubling questions that always surround "open" solutions are how well will the technology work with existing products, how well will it be supported, and by whom?

STAY TUNED

In order for your organization to objectively determine which type of products will help to achieve your streamlined network management goals, a formal project study is needed. Parts II and III of this series will suggest a "generic" project plan to achieve this end and will also investigate the types of SSO and ENM products that seem to be "real" and best suited for your network environment. ts

NaSPA member Guy C. Yost is the owner of Redstone Consulting, an IT management consulting firm in New York. He has authored several books on networking for Que Publishing, including Learning NetWare 4.1*, and* NetWare 4.1 SmartStart*, and contributes to* Technical Support *magazine as an author, columnist and technical editor. Guy also develops and conducts seminars on networking with Windows NT, UNIX, NetWare and Internet/intranet technologies across the United States and Canada. He can be reached at (518) 674-5606 or gyost@logical.net.*