

Novell Access Manager 3.0: The Shape of Things to Come

Date: November, 2006

Author: Jon Oltsik, Security Analyst

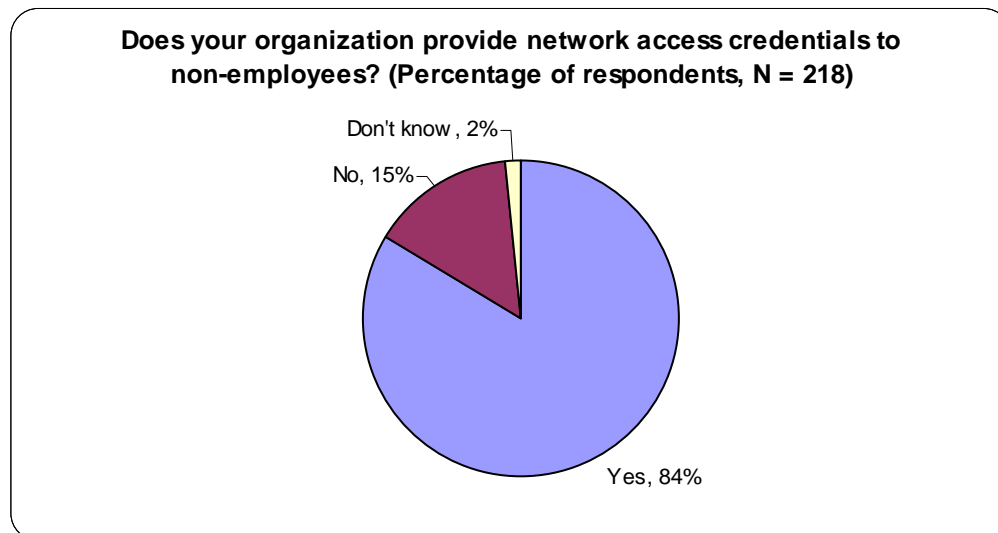
Abstract: The need to support remote user access to web, Java and legacy applications is an increasingly difficult challenge for IT but business pressures demand a good solution pronto. To scale remote access, IT can no longer depend upon a bevy of tactical point tools -- it needs integrated enterprise solutions. This is where Novell's new Access Manager 3.0 comes in.

Remote access used to be pretty simple. Provide dial-up access to a small cadre of traveling executives and remote field workers. A few dial-up clients here, a modem bank there and mission accomplished.

Times have certainly changed. External connectivity is no longer a productivity-enhancing luxury. It has become mission critical for business operations. Why? Globally distributed skills and ever-increasing bandwidth are driving a sharp increase in mobile workers. In 2006, roughly 20% of the U.S. working population (between 25 and 30 million people) works at home at least once per month. A study by the International Telework Association & Council (ITAC) forecasts that this number will grow to over 40 million by 2010.

Aside from employees, external constituencies such as business partners, customers, outsourcers and suppliers are increasingly provided with access to internal resources in order to bolster productivity, profitability and revenue. This trend was illustrated in a 2006 ESG Research study - 84% of North American-based security professionals from organizations with over 1,000 employees said that they provide network access credentials to non-employees (see Figure One).

Figure One: Most organizations provide network access to non-employees



Today's Access Control Technologies are no Match for Business Requirements

Clearly, business requirements for user access control are growing more pressing and sophisticated. Unfortunately, many organizations address this demand with a series of individual tactical point products. Firms implement a potpourri of web access controls for HTTP and Java applications, SSL VPNs for legacy system connectivity and identity integration glue for federated identity. As witnessed with other IT services, a stovepiped approach like this leads to:

- **Operational overhead.** Managing multiple point tools means provisioning users again and again, creating multiple new name repositories and dealing with a list of redundant tasks. Given that the need for remote connectivity continues to increase, these burdens will only get worse.
- **Security vulnerabilities.** With security, more products always lead to more security problems related to configuration errors, software vulnerabilities and attack vectors. When a rogue employee is escorted out the door by security guards, IT is on the hook to delete all of this person's user accounts immediately. With multiple products to administer, a de-provisioning oversight on a web SSO or SSL VPN can lead to a major security breach or IP theft.
- **User inconvenience.** Numerous access control technologies can create an environment where users have to memorize multiple passwords, master different GUIs and commands and log onto one system after another. This tedious set up is sure to increase help desk calls and reinforce the business managers' notion that IT "doesn't get it."

All of this is bad enough but the real issue here is the impact on the business. External applications promising increased productivity will face the red tape associated with provisioning users, managing profiles and writing identity-based business rules on an application-by-application basis. When this happens, identity and access management will become a bottleneck, standing in the way of progress.

Novell Access Manager 3.0 Offers an IT and Business Solution

Savvy IT managers realize that user access control has morphed from a technology to a business issue and are looking for new aggregated approaches. As they do their research, they will find a lot of promises, hype and future plans but few solutions. Fortunately, there may be an answer to this paradox. In October, Novell announced the release of a new product, Access Manager 3.0, bringing multiple aspects of access controls and identity manager functionality together on a common platform.

Access Manager 3.0 is the next generation - and new nomenclature - for Novell's successful iChain. The obvious IT benefit of Access Manager 3.0 is a single integrated platform for web access, SSL VPN, federated identity bridging and identity management. This alone should help IT managers lower costs, improve security and ease the integration burden associated with remote access controls for internal resources. These advantages should make Novell's sales phones ring, but ESG believes that Access Manager 3.0 also offers some hidden gems such as the facts that it:

- **Ties into the existing infrastructure.** Novell Access Manager 3.0 is not an extension of the legacy NetWare environment. Rather, it is built to drop into Novell and non-Novell shops. For example, Novell Access Manager 3.0 supports both SUSE Linux Enterprise Server (SLES) and Windows servers, interoperates with eDirectory, Active Directory and SunOne identity stores and supports LDAP, x.509 certificates and two-factor authentication tokens (via RADIUS) for authentication. Novell's design proves that it recognizes that enterprise organizations need product flexibility out of the box.
- **Streamlines the complexity of federated identity.** One issue around federated identity is the multitude of standards and implementation choices. When your major supplier wants to talk SAML, how will he communicate with your internal infrastructure based upon WS-Federation? No problem for Novell. Access Manager 3.0 provides an extensive menu with support for the Liberty Alliance v2.0 with web services

framework and SAML 1.1/2.0. In addition to basic standards coverage, Novell added tools that ease the configuration of this federated alphabet soup. Creating trust and federated identity relationships can actually be accomplished through a pull-down menu in the management tool that performs a middleware-like role of mapping one standard to another.

- **Eases identity-driven business rule creation.** Access Manager 3.0 includes a policy manager that takes advantage of the Web Services framework to normalize identity and thus add customized business logic. For example, the role defined as “manager” may have the ability to approve purchase orders below \$10k but needs VP sign-off for higher amounts. And Access Manager 3.0’s data abstraction layer enables administrators to write a simple policy statement to enforce this type of rule. Other products either demand separate statements for each data source or simply leave business rule creation to application developers. In other words, Access Manager 3.0 provides tools for the rapid creation of customized business rules, accelerated ROI and fewer development headaches.
- **Centralizes policy and reporting.** Since Access Manager consolidates access controls, user roles and policies are carried across web, legacy and Java application domains. Novell also flexed some of its Java development muscle in this release by providing fine-grained access controls for J2EE applications. Finally, Access Manager 3.0 provides centralized logging and reporting for regulatory compliance, forensics and user behavior analysis.

Novell Access Manager 3.0 integrates with its other identity management products for user provisioning, SSO and management. The company’s roadmap outlines a direction where future releases will tie identity and access management with resource management (i.e., asset management, configuration management, device provisioning), security management (i.e., event correlation, behavior analysis, anomaly detection) and storage management (i.e., disk quota management, file access control, data management policy). The overall goal? Consolidate identity/access management functions for IT while providing specific identity-centric information for IT, business managers and auditors.

The Bottom Line

Back in the 1990s, the tech industry used to talk about how business was moving in “Internet time.” Yes, this was self-serving hype, but it is certainly true that product cycles continue to accelerate. Two years ago, SSL VPNs were new technology. Now we need an integrated platform that combines SSL VPNs with other access technologies.

Finding vendors who can aggregate functions is hard enough, let alone those that can do so AND deliver business - not just IT -- benefits. Novell Access Manager 3.0 is somewhat unique in that it actually does address these IT, business and enterprise requirements. As such, business and IT executives would be well served by adding Novell to its short list of identity and access management vendors.