How Dell Streamlined Authentication and Identity Management Using Quest's Vintela Authentication Services

BY DAVE WILSON AND ROMMEL MERCADO

IMPLEMENTATION STUDY

CHALLENGE

Integrate authentication and identity management for Microsoft Windows, UNIX, and Linux platforms into Microsoft Active Directory across the entire Dell infrastructure

SOLUTION

Vintela Authentication Services from Quest Software deployed with the help of Quest Professional Services

BENEFITS

- Streamlined Active Directory–based system helps simplify authentication and identity management and frees IT staff to focus on other projects, helping increase operational efficiency
- Consistent cross-platform approach helps eliminate common compliance problems and reduce audit costs without requiring additional infrastructure
- Advanced features enable directory consolidation and identity migration at the pace—and according to the needs—of each organization's unique circumstances
- Automated provisioning and de-provisioning can help increase security in the future
- Implementing the solution in-house allows Dell to confidently recommend the solution to its own customers facing the same challenges

Related Categories:

Authentication, Linux, Microsoft Active Directory, Quest Software, Security

Visit www.dell.com/powersolutions for the complete category index.

When security, management, and compliance demands required Dell authentication and identity management systems to be consolidated into a single common directory, the Dell IT group turned to Quest Software's Vintela® Authentication Services, which enabled the integration of Microsoft® Windows®, UNIX®, and Linux® platforms with the Microsoft Active Directory® directory service.

Compliance concerns can drive enterprises to reexamine the way they handle identity and authentication. At the core of many regulations—including the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Graham-Leach-Bliley Act—is the mandate to securely authenticate users, grant appropriate access to data and resources, and track the activities surrounding that authentication and access. As enterprises become increasingly complex and diverse, the challenges presented by authentication and access are mounting. Compliance requires effective solutions to the challenges of identity across multiple, disparate operating systems. Dell is no exception: the Dell IT group faced such challenges when consolidating its heterogeneous authentication and identity management systems.

Managing a diverse environment

"Along with Microsoft Windows as our core platform, we also have a wide mix of systems running UNIX and Linux," says David Taylor, principal Linux engineer at Dell. "We have a significant installed base of servers running three different versions of Linux from two different vendors, plus a very small subset of systems using different versions of AIX and Solaris. All in all, we have about 2,200 combined UNIX- and Linux-based systems. Primarily, these platforms act as database servers for systems like our core Oracle business systems, but they do fill other functions as well."

But why not just base everything on a single platform—like Windows—and eliminate the problems heterogeneous systems present? For many organizations, the answers lie in the financial advantages of a multi-vendor approach and the fact that many mission-critical applications require specific platforms. In addition, organic growth can often introduce diverse systems. Although those answers are valid for Dell as well, the company has another compelling reason.

"We need to stand on our corporate principles," says Taylor. "And that means proving that Dell works on Dell. In accordance with this strategy, we have been migrating our UNIX-based systems to Linux for a number of years. Today, our standard Oracle database server runs Linux, but we still have a handful of legacy AIX- and Solaris-based systems running as well."

Providing centralized authentication and granting secure access in this diverse mix of operating systems would be a challenge for any organization. Dell's traditional approach to

> “In fairly short order, we have eliminated our security, compliance, and management concerns with cross-platform identities. And I think we are not even using Vintela Authentication Services to its fullest yet.”
>
> —David Taylor
> Principal Linux engineer at Dell
> February 2007

authentication across heterogeneous systems was to build a single domain and authenticate through the Server Message Block (SMB) protocol. Unfortunately, this approach requires distributed accounts across all systems. “Passwords were held in the domain, but for that technology to work, you still must have a local account on every computer,” says Taylor.

This approach was adequate for the short term because Dell had relatively low personnel turnover, but it still presented management and security concerns. “With our old approach, any kind of turnover meant you had to touch all of the systems to modify the user lists,” says Taylor. “No one is going to be perfect in this area—or at least we were not perfect about it—so we would end up leaving user accounts out there for people that have moved on to other jobs when we should have been terminating their access immediately. We were creating a security problem as well as a management problem. We built some scripts to de-provision from a centralized location, but it still is not a very effective way to manage user accounts.”

Consolidating authentication and identity management systems

Dell realized that security, management, and compliance demands would require centralizing authentication and bringing all user accounts into a single common directory for the entire enterprise. So the company launched a project called Multi-Platform Management Integration (MPMI). Its goal was to make the Microsoft Active Directory directory service the authoritative authentication system and master source for all user accounts across all systems within Dell—those running Microsoft Windows, IBM® AIX, Sun Solaris, and the various Linux operating systems.

“We could have created another directory and either passed authentication through it or run some sort of synchronization,” says Taylor. “But that would not be as simple and elegant as going directly into Active Directory.”

Adds Tony The, the MPMI project manager, “Active Directory is already the company standard directory, and every user already has an Active Directory account. Active Directory supports our current needs, and from a management perspective, our people already know and understand it.”

With the decision made to expand the influence of Active Directory to include UNIX- and Linux-based systems, the next challenge Taylor and The faced was how to execute the project. Active Directory authentication is based on the Kerberos encryption standard and the Lightweight Directory Access Protocol (LDAP). Because Active Directory is based on industry standards, several open source technologies are available for integrating UNIX and Linux with Active Directory.

“A couple of years ago I looked at integrating our UNIX- and Linux-based systems with Active Directory using open source technologies based on Kerberos and LDAP,” says Taylor. “But with the size of our Active Directory structure, it really was not a workable solution. It would have required LDAP to constantly query the directory for group membership, creating a significant burden on the network. Without a local caching mechanism, open source solutions really are not a viable option for an organization of our size. We also considered using Winbind, but that would not work either, because it requires a mapping database on every server.”

After ruling out open source alternatives, Taylor began a search for a third-party solution that provided the functionality the MPMI project demanded as well as the support and stability of a commercial product. One of the project architects began doing Internet research looking for vendors that offered the type of solution Dell required. One solution quickly rose to the top.

Finding the solution: Vintela Authentication Services from Quest

“Our research led us to Quest Software and a product called Vintela Authentication Services,” says Taylor. “It offered the features we needed and allowed our UNIX- and Linux-based systems to join Active Directory. With a very tight time frame—we needed to implement a solution as quickly as possible—we gave Vintela Authentication Services a two-day proof-of-concept test in our lab, purchased the solution, and began a rollout plan.”

The Vintela Authentication Services software is installed on UNIX- and Linux-based systems and integrates the native identity and authentication mechanisms of each OS with the Kerberos and LDAP components of Active Directory. Fundamentally, Vintela Authentication Services allows the AIX, Solaris, and various Linux platforms to act as full citizens in Active Directory. It helps eliminate the need for local accounts on each non-Windows system, leverages the secure authentication already present in Active Directory for UNIX and Linux, and allows other advanced Active Directory functionality, such as Group Policy, password policies, Windows security policies, and single sign-on. Vintela Authentication Services extends to many popular and widely deployed UNIX and Linux platforms.

“Quest Professional Services guided us through the design of the solution,” says Taylor. “With so many differences across platforms and all that we wanted to accomplish, it was a more involved process than it originally appeared. Quest helped us design the Group Policy Objects we used in our rollout. The deployment began in July 2006. Today, the Vintela Authentication Services client is installed on all of our UNIX- and Linux-based servers, and they are authenticating

> "Quest Software delivered a comprehensive authentication solution that did not require any additional infrastructure. It mirrors Windows authentication as closely as we could have hoped."
>
> —Tony The
> Multi-Platform Management Integration project manager at Dell
> February 2007

against Active Directory. We also are now preinstalling the client on every new Linux-based system provisioned within Dell."

Planning for the future

With the UNIX and Linux platforms joined to the Active Directory domain, the next step in the Dell MPMI project is to migrate the local user accounts from each non-Windows system into Active Directory. Vintela Authentication Services offers several advanced features to enable directory consolidation and identity migration at the pace—and according to the needs—of each organization's unique circumstances. These options range from simply leveraging Active Directory for passwords and authentication while maintaining existing UNIX and Linux structures, to moving existing UNIX and Linux structures into Active Directory as a subset of the Active Directory user account, to fully migrating from multiple, disparate identities to a single Active Directory–based identity for all systems. "In the future, we expect to migrate all of the accounts into Active Directory," says The.

Adds Taylor, "We plan to set up our own import file. Our accounts are pretty straightforward; they are either local or already use Active Directory. Next, we plan to use the Vintela Authentication Services Ownership Alignment Tool to resolve conflicting file ownerships as we move from multiple UNIX and Linux accounts to a single Active Directory account.

"When MPMI is complete, we should no longer need local user accounts on our UNIX- or Linux-based systems—just required system accounts such as root and bin," says Taylor. "All the systems that are provisioned these days have no local user accounts on them, and that is the way they stay. Everything going forward is based on Active Directory, so systems start out clean. In fairly short order, we have eliminated our security, compliance, and management concerns with cross-platform identities. And I think we are not even using Vintela Authentication Services to its fullest yet. I would estimate that just streamlining operations through directory consolidation and centralizing authentication is freeing up one or two people each year. We can put those people on more important and interesting projects than managing authentication and user accounts."

"Beyond the obvious operational expense savings this solution has brought us, an even more important benefit is cost avoidance," says The. "We are going to be growing our Linux environment quite a bit going forward, and Vintela Authentication Services can help us avoid a lot of cost simply by eliminating one of the areas that may cause problems in our compliance audits. The benefit to Dell is a combination of cost avoidance and operational efficiency."

In the future, Dell plans to gain additional benefits from its integrated identity environment by leveraging Active Directory Group Policy to control security-related parameters in the UNIX and Linux environments. In addition, future projects may involve automating provisioning and de-provisioning for all systems based on Active Directory and extending the benefits of Vintela Authentication Services to additional UNIX applications.

"My focus is security, and from that perspective, Vintela Authentication Services did exactly what we needed it to do," says The. "Quest Software delivered a comprehensive authentication solution that did not require any additional infrastructure. It mirrors Windows authentication as closely as we could have hoped."

Building a relationship

According to Mark Witucki, the account manager at Quest Software who managed the relationship with Dell, "The fact that this project was extremely successful has really catapulted the relationship to the next level. We have felt how important this was to the Dell field."

"Quest and Dell have a relationship that extends well beyond the simple vendor-customer relationship that our MPMI project introduced," says Taylor. "Many Dell customers are running into the same challenges we encountered—compliance, security, and managing identity in a heterogeneous environment. People are always asking how we manage our own systems. It is nice to be able to say that we have implemented a centralized solution for the same problem these Dell customers face. The fact that it works in-house at Dell, and works so well, allows our sales force to confidently offer a similar solution to Dell customers.

"Vintela Authentication Services is the best product we have found on the market," concludes Taylor. "It satisfies our needs and can help us expand where we need to in the future."

Dave Wilson *is the vice president of identity management and interoperability at Quest Software.*

Rommel Mercado *is the senior manager of the IT Core Platform Engineering team at Dell.*

more Online
www.dell.com/**powersolutions**

QUICK LINK

Quest identity management solutions:
www.quest.com/IdM_Dell