Increase the Security, Privacy and Compliance of Your SAP Data

QUEST® VINTELA AUTHENTICATION SERVICES ENABLES UNIQUE SECURITY CAPABILITIES FOR SAP

Single Sign-on for SAP through Vintela Authentication Services:

- Provides true AD-based single sign-on for SAP running on Unix or Linux
- Eliminates the transmission of users' passwords over the network
- Securely encrypts SAP data, while it is transported over the network
- Simplifies deployment without the need for PKI or certificate infrastructure
- Provides an audit trail for SAP authentication activities with AD

Vintela™

is now part of

QUEST SOFTWARE®

Mission-critical Data Demands Mission-critical Security

For many organizations, SAP applications and services are mission-critical. Compliance, security and economics demand control over user access, authentication to resources, and the protection of data as it moves across the network.

Some of the biggest challenges facing organizations, that rely on SAP, include:

- Ensuring that only the right people have access to data
- Guaranteeing that those people can access SAP when they need to
- Ensuring that mission critical information is secure as it moves across the network

SAP applications must meet the strict standards demanded by regulatory compliance, internal controls defined by governance policies and corporate best practices. But how can an organization make that happen in today's increasingly heterogeneous, multi-platform, complex service-oriented architecture (SOA) environment? Achieving unified authentication, data protection and single sign-on for SAP has been virtually impossible—until now.

For many organizations the answer lies in leveraging the secure, compliant and scalable infrastructure offered by Microsoft's Active Directory (AD). If SAP is running on Windows servers, the SAPGUI interface can deliver secure AD-based authentication for SAP applications and services. However, single sign-on has not been available for users accessing SAP hosted on Unix platforms. Wouldn't it be great if that same, powerful Windows-based authentication could apply to those systems?

Single Sign-on for SAP

AD provides a true single sign-on environment for Windows resources. Through its use of the industry standards Kerberos and LDAP, AD provides a compliant, secure and scalable infrastructure for authentication, authorization and access. For users of SAP on Unix systems, Quest® Vintela Authentication Services provides the same capability. It allows Unix and Linux systems to "join" the AD domain, which extends the compliant and secure AD-based authentication, for SAP to SAP on Unix servers.

Consequently, the workload required of the SAP BASIS team can be dramatically reduced, as they no longer need to focus on provisioning and password issues. This integration also results in a superior user experience and increases the security of a mixed Unix, Linux and Windows SAP environment, including protection of SAP data in transit through the latest encryption technologies.

The efficiency, end user satisfaction and control provided by single sign-on for SAP (on any platform), through AD and Vintela Authentication Services, yields significant ROI. This solution helps to reduce the help desk burden caused by multiple identities and multiple logins, as it reduces the total cost-of-ownership and leverages the existing investment in AD and SAP for maximum benefits.

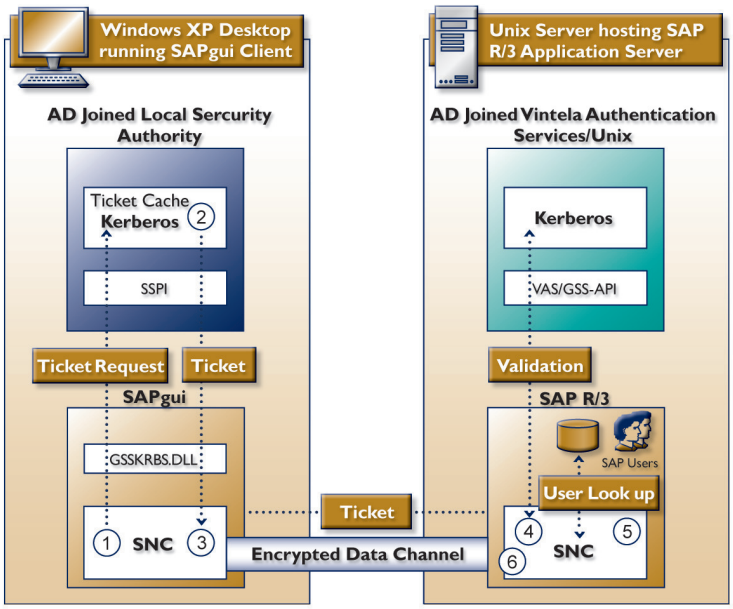
Increase the Security, Privacy and Compliance of Your SAP Data

QUEST® VINTELA AUTHENTICATION SERVICES ENABLES UNIQUE SECURITY CAPABILITIES FOR SAP

Implementing Vintela Authentication Services for SAP:

- Provides true AD-based single sign-on for SAP running on Unix or Linux
- Eliminates the transmission of users' passwords over the network
- Securely encrypts SAP data, while it is transported over the network
- Simplifies deployment without the need for PKI or certificate infrastructure
- Provides an audit trail for SAP authentication activities with AD

Vintela Authentication Services integrates Unix and Linux hosts, running SAP with Windows-based clients through robust, standards-based security. The SAP SNC interface provides SAP clients and servers a platform-independent security and authentication infrastructure, which fully leverages native Windows and Unix security mechanisms. Windows-based SAP clients can exchange secure authentication tokens, using Kerberos tickets with Unix-hosted SAP R/3 servers.



1. SAPGUI requests a Kerberos Ticket via SAP's SNC gsskrb5. dll, which translates GSS API requests to SSPI.
2. A Windows KDC generated ticket is returned.
3. SAPGUI client connects to the SAP R/3 Application Server, passing the returned ticket.
4. SAP R/3 Application Server validates the ticket via the Vintela Authentication Services Unix GSS API libraries.
5. The Kerberos tickets UPN is mapped to SAP R/3 account.
6. An encrypted data channel is established using information provided in the Kerberos ticket.

Moving Single Sign-on "Up the Stack"

Vintela Authentication Services natively implements Kerberos and LDAP on Unix and Linux systems in the same way those standards are used in Windows. It enables a single "trusted realm" that includes Unix, as well as Windows, allowing them to use the same Kerberos tickets used for Windows authentication. This creates true single sign-on between Windows desktops and Unix systems. Vintela Authentication Services also enables single sign-on for GSS-API aware applications, such as SAP, DB2, Apache and ssh.

Quest's Vintela Resource Central Web site provides customized implementations of tools, such as openssh, PuTTY and Apache. These solutions are configured to provide single sign-on and to allow users to leverage this security and single sign-on infrastructure at a more integrated level than they could with a certificate/PKI-based product. The site also includes guidance documents describing other application integration procedures.

Vintela

is now part of

QUEST SOFTWARE

More about Vintela Authentication Services

Vintela Authentication Services provides a cost-effective, enterprise-proven and standards-based alternative to cumbersome and complex synchronization or meta-directory solutions. With Vintela Authentication Services, the same infrastructure, processes and personnel that are already in place to manage Windows resources can now be extended to support and manage a full range of Unix and Linux systems, as well as a growing number of applications including SAP. The result is enhanced security and a clear path to enterprise-wide regulatory compliance.

Benefits of this cross-platform integration of non-Windows platforms and applications with AD include:

Single Sign-on for Heterogeneous Systems: Vintela Authentication Services natively implements Kerberos and LDAP on Unix and Linux systems in the same way those standards are used in Windows. It allows AD to create a single, "trusted realm" that includes Unix, Linux and Windows. This creates true single sign-on between Windows desktops and Unix and Linux systems, and for GSS-API aware applications, such as SAP, Apache and ssh.

Enterprise-wide Identity Management Based on Existing Infrastructure: Vintela Authentication Services provides the seamless capability to extend the already deployed and highly robust AD infrastructure to the rest of the enterprise. Rather than purchasing, deploying and supporting additional infrastructure, tools and technologies for non-Windows systems, this product allows organizations to consolidate all identity and authentication management in AD—the preferred platform that's already in place.

Simplified Identity Management: By integrating Unix and Windows accounts into a single identity store (namely AD), Identity Management complexity is greatly reduced. Provisioning and de-provisioning of Unix accounts can be performed with the same tools and at the same time as Windows. Additionally, other advanced identity administration capabilities, such as password management, audit and role management, can be centralized on an AD-based infrastructure.

Advanced Data Protection: Vintela Authentication Services supports both DES and RC4 encryption. This provides the users of Vintela Authentication Services with the choice of cryptographic algorithms to protect the privacy of data while it is "in flight".

is now part of

www.quest.com/microsoft
e-mail: info@quest.com
Please refer to our Web site for
international office information.

WMG_VASSAP_DS_UX_06142006