QUEST SOFTWARE
Smart Systems Management

DATASHEET

Quest® Privilege Manager for Unix

Quest® Authentication Services

Powerful, Cost-Effective Authentication and Authorization in Unix Environments

Leverage the Combined Value of Two Unparalleled Quest Solutions

Authentication and authorization are two key aspects of identity and access management. Neither is complete without the other, and organizations are concerned about both. For Unix and Linux systems, Quest offers the best solutions for both authorization and authentication:

- Privilege Manager provides an advanced level of authorization control beyond that available natively in Unix and Linux. It enables organizations to delegate the Unix root privilege at an extremely granular level, based on policy, with all activities thoroughly audited.
- Quest Authentication Services' (formerly Vintela Authentication Services) patented technology provides the best available authentication solution by extending Active Directory, Kerberos-based authentication to non-Windows platforms. It enables users to access Unix and Linux systems through an Active Directory log in and account.

Authentication Services and Privilege Manager—Better Together

While both Authentication Services and Privilege Manager deliver significant value on their own, using the two solutions provides enhanced value. Specifically, Authentication Services uses Active Directory group membership to control which Unix systems each Active Directory user is allowed to access; Privilege Manager extends this capability by using the same Active Directory group membership to control the elevated privileges authorized for each user after being authenticated.

By using the products together, Active Directory group membership controls access to specific Unix systems (authentication) as well as any user rights and elevated privileges (authorization).

Benefits of the Combined Solution

Some of the key benefits of using both Authentication Services and Privilege Manager are:

- **Automated Policy File Distribution:** The Group Policy component of Authentication Services can distribute Privilege Manager policy and configuration files from a central Active Directory-based location to the appropriate Unix and Linux hosts. This integration provides value by allowing Active Directory to remain the primary source for authentication while also providing a central point for the configuration of Privilege Manager.
- **Enhanced Security:** Authentication Services extends Active Directory's Kerberos infrastructure to non-Windows platforms. With Privilege Manager running on the same system, Active Directory's encryption capabilities can also benefit Privilege Manager operations by enabling highly secure connections and eliminating the need for dedicated keys within Privilege Manager. It is easy to enable Kerberos support for Privilege Manager by using an Active Directory Group Policy setting provided by Authentication Services.
- **Easy Management of Authorization Policies:** The core capability of Privilege Manager is to control the decisions (policy) related to executing commands that require an elevated privilege (typically root on Unix and Linux systems). These policies and their associated actions can be based on a number of external factors: date, time, hostname, command, parameters, IP address, group membership, and others.

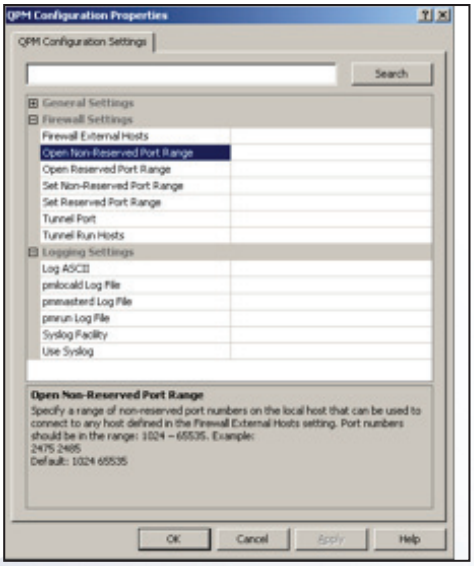

Figure 1. The Authentication Services Group Policy console includes control for Privilege Manager policy.

Authentication Services enables Privilege Manager to request group membership information for a Unix-enabled Authentication Services user so Privilege Manager can make policy-related decisions based on a user's Active Directory group membership. This integration makes Active Directory central to the decision-making and control process, and eliminates the need to manage authorization policy in two places: in Active Directory for Windows administrators and in Privilege Manager for Unix administrators.

- Enhanced Compliance with Powerful Audit and Reporting Capabilities: Just as it is important to control user activity on Unix and Linux systems, it is equally important to audit their activities and report on the results. Privilege Manager provides the industry's most powerful auditing tool for Unix activities, including keystroke logging and playback.

  The combination of Privilege Manager and Authentication Services enables powerful reporting for those who control and administer Unix and Linux systems. Detailed maps show who is and who is not permitted to execute commands on Unix and Linux hosts; this is invaluable for compliance efforts. Reports highlight behavior that varies from an accepted baseline, enabling Unix and Linux administrators to pinpoint areas of activity that require further scrutiny.

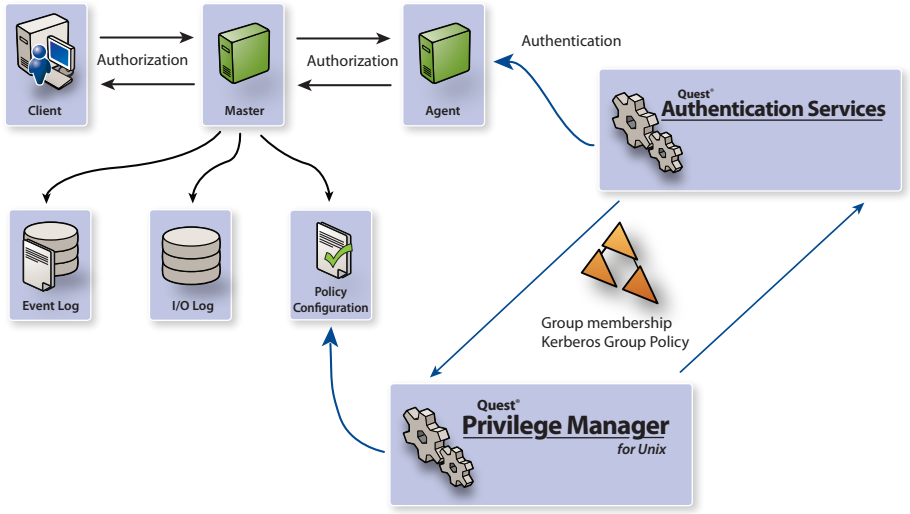

Figure 2. Authentication Services and Privilege Manager for Unix combine to deliver automated policy file distribution, enhanced security, easy management of authorization policies, and enhanced compliance.

Two Solutions, One Powerful Result

Whether an organization is seeking to simplify infrastructure by consolidating Unix and Linux identities in Active Directory or control access to the most privileged Unix and Linux account (root), Quest provides the best solution in Authentication Services and Privilege Manager for Unix. Combining these two powerful solutions yields additional benefits: automated policy file distribution, enhanced security, easy management of authorization policies and powerful reporting and auditing capabilities.

Authentication Services and Privilege Manager for Unix – better together.

About Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit **www.quest.com** for more information.

QUEST SOFTWARE
Smart Systems Management

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.

DSW-AuthServ_PrivMgr-US-AG-20091205