

# Quest InTrust Solaris Knowledge Pack

## Benefits

- Saves time and improves efficiency by automating the collection of Solaris based syslogs and BMS logs
- Ensures tighter information security by collecting and reporting on logons, as well as file and object access
- Enables organizations to address regulatory compliance requirements by reporting on access to information

Understanding user activity at every level and in every application is imperative to the security of all organizations. Whether supporting an internal security requirement or external regulatory compliance initiative, collecting, storing and reporting on this data must be a priority for any IT organization.

Most organizations have enabled auditing at the local file level, but soon realize that the amount of data generated is much too large to manage, and oftentimes they end up turning it off. The amount of data generated can quickly become overwhelming and costly due to their storage requirements.

Solaris based log files have become much more critical to organizations as many business critical applications are housed on these servers. Failure to collect these logs can lead to non-compliance to external regulations.

Complicating matters, if logs are collected they can be modified and deleted by users with sufficient enough rights. This can lead to theft, fraud and a failure to meet compliance requirements.

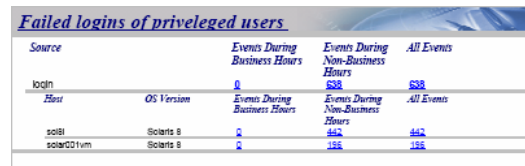
The challenge is set: In order to meet external compliance objectives or internal security mandates, a company must securely audit access and changes in permissions to files and objects deemed critical to the organization such as:

- Solaris file access
- Logon times
- Logon failures
- Security log correlation

The Quest InTrust® Solaris Knowledge Pack can help. It automates the process of collecting, storing and reporting on Solaris events, helping to further strengthen a company's information security while addressing compliance requirements. Through agent-side caching, InTrust assures the logs are in their native state and that no logs have been lost due to deletion or roll-over.

Having all this information available, and ensuring the integrity of the data, means an executive is able to determine what user permissions have changed and what users are accessing business critical files and objects. For instance, if a change was made and turns out to be invalid, permissions can be reversed. If the change was made by unauthorized personnel, their rights can be revoked and appropriate action can be taken against that employee.

Reports can be generated on a daily, weekly or quarterly basis depending on a company's needs. The figure below represents a detailed view into failed logons of privileged users.



Source	OS Version	Events During Business Hours	Events During Non-Business Hours	All Events
login		0	538	538
solB	Solaris 8	0	462	462
solar001um	Solaris 8	0	158	158

Figure 1: Solaris Knowledge Pack Report Sample

Having this functionality means that companies can provide auditors and investigators with a complete view into file/object access, local logons and logon failures.

For more information on how InTrust can help your organization address internal security mandates and external compliance requirements, regardless of your environment, visit <http://wm.quest.com/products/intrust/>.