

Quest® InTrust® AIX 5L Knowledge Pack

Benefits

- **Saves time and improves efficiency by automating the collection AIX based audit logs**
- **Ensures tighter information security by collecting and reporting on logons as user sessions and administrative activity**
- **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 the IT organization. Most organizations have enabled auditing at the server level but soon realize that the amount of data being generated is much too large to manage and end up turning it off. This can lead to non-compliance in many external regulations which affect most companies in one form or another. AIX is a widely used server platform for applications therefore these audit logs are extremely critical to organizations.

Audit logs are open to modification and deletion by users with enough rights. This can lead to theft, fraud and a failure to meet compliance requirements. Non-compliance can result due to a failure to collect all logs and the inability to assure the integrity of the logs collected.

In order to meet external compliance objectives or internal security mandates, a company must audit local user activity and other information such as:

- Detailed information about user sessions
- Multiple failed logon attempts
- Successful logins

The amount of data being generated can quickly become overwhelming and costly due to the storage requirements. In order to meet these requirements and recognize an ROI,

companies must implement a scalable solution with cost effective long term storage.

The new InTrust AIX Knowledge Pack can help. It automates the process of collecting, storing and reporting helping to further strengthen a company's information security while assisting in 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 now able to determine what user permissions are changed and what users are accessing business critical files and objects. In the case the change made was invalid permission can be reversed, and if the change was made by unauthorized personnel their rights can be revoked and appropriate action 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 view into all events generated on an AIX server.



The screenshot shows a report titled "AIX 5L successful logins". It includes a filter section for "Date/time from" (1/1/1990 12:00:01 AM) and "Date/time to" (2/1/2007 4:22:28 PM). Below this, it specifies the host as "spb9487". The main data is presented in a table with columns for Time, Event, Source, and For User.

Time	Event	Source	For User
1/11/2007 1:32:24 PM	session opened	sshd	fred
1/11/2007 1:32:25 PM	session opened	sshd	fred
1/11/2007 1:32:26 PM	session opened	sshd	fred
1/11/2007 1:32:27 PM	session opened	sshd	fred
1/11/2007 1:32:28 PM	session opened	sshd	fred

Figure 1: AIX Knowledge Pack Report Sample

Having this functionality means that companies can provide auditors and investigators a complete view into the AIX server environment and correlate activity with the rest of the enterprise.

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