

Quest® InTrust® Linux Redhat/SUSE Knowledge Pack

Benefits

- Saves time and improves efficiency by automating the collection of Linux Redhat/SUSE-based audit logs
- Ensures tighter information security by collecting and reporting on logons, 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.

Although most organizations have enabled auditing at the server level they soon realized 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 to many external regulations which affect most companies in one form or another.

Linux Redhat/SUSE has been accepted on a much broader level and therefore these audit logs have become much more critical to organizations. Many business critical applications are housed on Linux servers. But these logs are open to modification and deletion 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 audit local user activity and other information such as:

- Detailed information about user sessions
- Failed logon attempts
- New user accounts created/modified

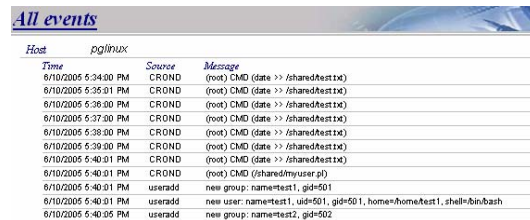
In order to meet these requirements and recognize a return on investment, companies

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

The InTrust® Linux Redhat/SUSE Knowledge Pack can help. It automates the process of collecting, storing and reporting on Linux Redhat/SUSE events, helping to further strengthen a company's information security posture while assisting in addressing compliance requirements.

Having this information available, and ensuring the integrity of the data, means an executive is able to determine how user permissions have changed and what users are accessing business critical files and objects. In the case a change was invalid, permission can be reversed. 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 a Linux Redhat/SUSE server.



Host	pglinux	Time	Source	Message
		6/10/2005 6:34:00 PM	CROND	(root) CMD (date >> /shared/test1)
		6/10/2005 6:35:01 PM	CROND	(root) CMD (date >> /shared/test1)
		6/10/2005 6:36:00 PM	CROND	(root) CMD (date >> /shared/test1)
		6/10/2005 6:37:00 PM	CROND	(root) CMD (date >> /shared/test1)
		6/10/2005 6:38:00 PM	CROND	(root) CMD (date >> /shared/test1)
		6/10/2005 6:39:00 PM	CROND	(root) CMD (date >> /shared/test1)
		6/10/2005 6:40:01 PM	CROND	(root) CMD (date >> /shared/test1)
		6/10/2005 6:40:01 PM	CROND	(root) CMD (/shared/myuser.pl)
		6/10/2005 6:40:01 PM	usersdd	new group: name=test1, gid=501
		6/10/2005 6:40:01 PM	usersdd	new user: name=test1, uid=501, gid=501, home=/home/test1, shell=/bin/bash
		6/10/2005 6:40:05 PM	usersdd	new group: name=test2, gid=502

Figure 1: Linux Redhat/SUSE Knowledge Pack Report Sample

Having this functionality means that companies can provide auditors and investigators a complete view into administrative activity, failed logon attempts and user sessions.

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