

Quest InTrust® EMC® Content Addressed Storage (CAS) Module

Benefits

- **Guarantees the authenticity of audit data once stored on the server**
- **Provides online accessibility through uniquely assigned content addresses**
- **Scales automatically for long term audit log storage**

Today, companies are faced with the need to adhere to a multitude of regulatory requirements, which requires them to provide reasonable assurance that stored and presented audit log data is authentic and tamper-free. Reasonable assurance is a standard that applies both in a court of law or with an external auditor. Clearly, the authenticity of this data is critical to any organization in order to determine the exact cause of user actions.

Audit data, if stored on a normal file server without NTFS security applied, is open to modification and deletion by users with sufficient enough rights. Failure to collect all logs and the inability to assure the integrity of the collected logs 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 enterprise activities, securely store this data for an extended period of time and provide reasonable assurance that the stored data is tamper free.

Regardless of how important the data is, the amount of collected audit log data can quickly become overwhelming and costly to manage due to storage requirements. 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 new Quest InTrust® EMC® Content Addressed Storage (CAS) Module can help. This product automates the process of collecting, storing and consolidating critical audit information, while retaining the authenticity of it from source to repository.

Through agent-side caching, InTrust assures that the logs are in their native state and that no logs have been lost due to deletion or roll-over at the source server. The logs are then encrypted over the network line and then assigned a unique identifier once stored on the EMC Centera server, which prevents the data from being manipulated in any way.

Having all this information available online, and ensuring the integrity of the data, means an IT or business manager is now able to validate user activity and system configuration changes in a heterogeneous environment with confidence. This helps enhance a company's information security and operational efficiency, while assisting in addressing compliance requirements.

An easy-to-use wizard guides the InTrust administrator through the creation of a repository on a Centera server, where collected audit data can be stored. The figure below demonstrates the easy-to-use wizard.

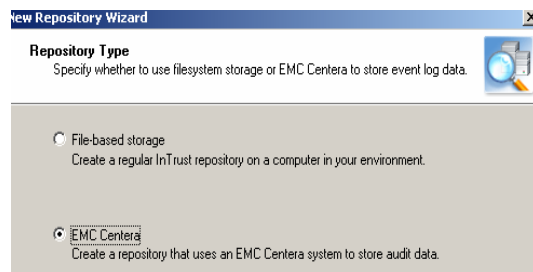


Figure 1: CAS Module Configuration Wizard

This functionality enables any organization to provide reasonable assurance that the collected and stored audit data has retained its authenticity. This can be critical if the organization is involved in any forensic investigation.

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/>.