

Quest InTrust Microsoft Internet Information Server Knowledge Pack

Benefits

- Saves time and improves efficiency by automating the collection of Windows based Internet Information Server (IIS) logs
- Provides valuable information about the IIS environment ensuring that the security and use of servers are in accordance with company policies
- Correlates IIS information with client and internal user activity

- Failed access attempts to HTTP and FTP sites
- Traffic information
- Directories requested
- Files accessed

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.

The new Quest InTrust[®] Internet Information Server Knowledge Pack can help. This product automates the process of collecting, storing and reporting on IIS events, helping to further strengthen a company's information security. InTrust assures that logs are in their native state so you can be assured of their unimpeachability.

However, sometimes addressing these mandates really means understanding client activity as well. For corporations who have externally facing Websites, these logs are of utmost importance. Corporations must be aware of client activity to ensure that the clients are not gaining access into the internal network and that they are acting in an appropriate manner.

Having all this information available, and ensuring the integrity of the data, means an administrator and the organization are now able to determine how their IIS environment is used and how users and clients are behaving. Organizations can be proactive in their security posture. Reports can be generated on a daily, weekly or quarterly basis depending on a company's needs. The figure below represents a report of successful logons after several failures to an FTP server.

Indeed, most organizations have scanned through their IIS .txt log information, but have struggled to understand or trend the information. The amount of data generated can quickly become overwhelming and costly due to the storage requirements. Companies must implement a scalable solution with cost effective long term storage. Not understanding this critical information can lead to an unsecured infrastructure and its assets. The ability to understand and use this information can also help lead to discovering misuse by internal employees.

Successful logon to FTP server after several failures

Displays successful logons to an FTP server that occurred after series of failures.

Filter for	Operation	Values
Number of Attempts:	Parameter expression	10
Time Interval:	Parameter expression	2
Measurement Units:	Parameter expression	minute

Client IP [10.30.44.144](#)

Logon DateTime	Server	Site	User Name	From	To	Attempts
10/13/2005 3:18:40 PM	ACCORDEON	Default FTP Site	anonymous	10/13/2005 3:17:38 PM	10/13/2005 3:18:03 PM	16
10/13/2005 3:23:35 PM	ACCORDEON	Default FTP Site	TestDomain\ids\lida	10/13/2005 3:22:36 PM	10/13/2005 3:23:17 PM	22

Figure 1: IIS Knowledge Pack Report Sample

The challenge is set: In order to secure the network and provide a better IIS environment, a company must audit, collect and report on IIS log information such as:

Having this functionality means that companies can provide a complete view into the IIS infrastructure, thus providing a more secure network.

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/>.