Quest® InTrust 11.4.2

Audit Database Structure

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

i **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Audit Database Structure
Updated - September 2020
Version - 11.4.2

Contents

Computers

Name	Type	Description
ComputerName	nvarchar (255)	Name of the computer from which the log was gathered.
Domain	nvarchar (255)	Name of the domain to which the computer belongs.
Type	int	Computer type, e.g. server or workstation. For Windows computers, this field has a bitmask value. For other computers, the value is 0. For more information about bitmask values, see the description of the **SERVER_INFO_101** network management structure in the MSDN library. The **sv101_type** member defines the possible values.
PlatformID	int	The computer's platform (operating system) ID. The following platform IDs are used: • 500 (Windows) • 610 (Solaris) • 620 (HPUX) • 630 (LINUX) • 640 (AIX)
VersionMajor	int	Major version number of the computer's operating system. For example, the major version of Windows 8 is 6.
VersionMinor	int	Minor version number of the computer's operating system. For example, the minor version of Windows 8 is 2.

Events

Name	Type	Description
ID	int	ID of the event in the InTrust gathering session.
SessionID	int	ID of the gathering session.
GatheringComputer	nvarchar (255)	Computer from which the event was retrieved.
PlatformID	int	Platform (operating system) ID of the computer from which the event was retrieved.
VersionMajor	int	Major version number of the audited software on the computer where the data was collected. InTrust data sources define the major version values as specified below. When event caching is not used during gathering: • **Microsoft Windows Events**, **Microsoft DHCP Server Events**, **Solaris Audit Log Events**, **HP-UX Audit Log Events**—Major version of the operating system. For example, the major version of Windows 8 is 6. • **Custom Text Log Events**, **Database Events**—Major version of the operating system, unless specified otherwise. • **Microsoft IIS Events**—The MajorVersion dword value in the HKLM\SOFTWARE\Microsoft\InetStp registry key. • **Microsoft ISA Server Events**—The major version number in the string representation of the ISAS version. This string is retrieved from the ProductVersion(BSTR*) property of the IFPCServer interface. • **Microsoft Proxy Server Events**—The major version is 2. • **Microsoft Exchange Events**—Major version of Microsoft Exchange Server. When event caching is used during gathering: • **Microsoft Windows Events**, **AIX Audit Log Events**—Major version of the operating system. • **Syslog**, **Account Monitoring Events**, **Text File Monitoring Events**—Major version of the operating system, unless specified otherwise.

Name	Type	Description
		- **Microsoft IIS Events**—The MajorVersion dword value in the **HKLM\SOFTWARE\Microsoft\InetStp** registry key.
VersionMinor	int	Minor version number of the audited software on the computer where the data was collected. InTrust data sources define the minor version values as specified below. When event caching is not used during gathering: - **Microsoft Windows Events**, **Microsoft DHCP Server Events**, **Solaris Audit Log Events**, **HP-UX Audit Log Events**—Minor version of the operating system. For example, the minor version of Windows 8 is 2. - **Custom Text Log Events**, **Database Events**—Minor version of the operating system, unless specified otherwise. - **Microsoft IIS Events**—The MinorVersion dword value in the HKLM\SOFTWARE\Microsoft\InetStp registry key. - **Microsoft ISA Server Events**—The minor version number in the string representation of the ISAS version. This string is retrieved from the ProductVersion(BSTR*) property of the IFPCServer interface. - **Microsoft Proxy Server Events**—The minor version is 0. - **Microsoft Exchange Events**—Minor version of Microsoft Exchange Server. When event caching is used during gathering: - **Microsoft Windows Events**, **AIX Audit Log Events**—Minor version of the operating system. - **Syslog**, **Account Monitoring Events**, **Text File Monitoring Events**—Minor version of the operating system, unless specified otherwise. - **Microsoft IIS Events**—The MajorVersion dword value in the **HKLM\SOFTWARE\Microsoft\InetStp** registry key.
EventLog	nvarchar (255)	Name of the log from which the event was retrieved.
RecordNumber	int	The event's number, used for storing the position of the last gathered event.
Computer	nvarchar (255)	Computer on which the event occurred.
UserName	nvarchar (255)	Name of the user who produced the event.
UserDomain	nvarchar (255)	Domain of the user who produced the event.
EventType	int	Event type.
Source	nvarchar (255)	Name of the event's source.

Name	Type	Description
EventID	int	ID of the event.
Category	nvarchar (255)	Category of the event.
GMT	datetime	Event generation time in GMT format.
LocalTime	datetime	Event record time; this time is local to the computer from which the event was retrieved.

EventsData

Name	Type	Description
EventID	int	ID of the event in the InTrust gathering session. This field corresponds to the ID field in the Events table.
SessionID	int	ID of the gathering session. This field corresponds to the SessionID field in the Events table.
EventData	image	Binary data of the event.

EventsDescriptions

Name	Type	Description
EventID	int	ID of the event in the InTrust gathering session. This field corresponds to the ID field in the Events table.
SessionID	int	ID of the gathering session. This field corresponds to the SessionID field in the Events table.
Description	ntext	Description of the event.

EventsStrings

Name	Type	Description
EventID	int	ID of the event in the InTrust gathering session. This field corresponds to the ID field in the Events table.
SessionID	int	ID of the gathering session. This field corresponds to the SessionID field in the Events table.
StringIndex	int	Index of the event's insertion string.
StringValue	nvarchar (4000)	Value of the event's insertion string.

GatheredEvents

Name	Type	Description
Computer	nvarchar (150)	Computer on which the event occurred.
PlatformID	int	Platform (operating system) ID of the computer on which the event occurred.
VersionMajor	int	Major operating system version number of the computer on which the event occurred. For example, the major version of Windows 8 is 6.
VersionMinor	int	Minor operating system version number of the computer on which the event occurred. For example, the minor version of Windows 8 is 2.
EventLog	nvarchar (255)	Name of the log from which events were retrieved.
RecordNumber	int	Number of the record in the event log, used for storing the position of the last gathered event.
TimeWritten	int	Time when the event was written to the log.
GMT	datetime	Event generation time in GMT format.
LocalTime	datetime	Time when the event was written to the log; this time is local to the computer where the event was logged.
IGMD	image	Stands for Incremental Gathering MetaData. This is arbitrary binary data written and read by the data source that is used for the gathering. For example, a data source can store and query lists of file paths.
filterhash	int	Hash of the combined filter used for the gathering.
filter	image	Combined filter used for the gathering.
PositionVersion	int	Contains one of the following values: • 1 (agent-side audit log backup was used during the gathering) • 0 (agent-side audit log backup was not used)
PositionFlag	int	When cached data is collected for the first time to the new storage, data from the corresponding event log also captured (to prevent data loss). For the second cached data gathering to the same storage data from the corresponding event log is not needed and this option indicates this.

Name	Type	Description
		Contains one of the following values: - 0 (Cached data and data from the corresponding event are not collected) - 1 (Cached data have been collected for the first time to the new storage together with data from the corresponding event log)

GatheringSessions

Match	Field	Description
ID	int	Gathering session ID.
Computer	nvarchar(150)	Name of the InTrust Server computer that ran the gathering job.
CollectionName	nvarchar(255)	Name of the gathering job.
GMT	datetime	Session start time in GMT format.
LocalTime	datetime	Session start time; this time is local to the InTrust server.
UniqueID	nvarchar(255)	Unique ID of the gathering session.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product