

Quest® InTrust 11.4.2

Preparing for Auditing Microsoft SQL Server



© 2020 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

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

InTrust Preparing for Auditing Microsoft SQL Server

Updated - September 2020

Version - 11.4.2

Contents

SQL Server Auditing Overview	4
Requirements	5
Auditing Requirements	5
C2 Log Requirements	5
Gathering from Multiple Servers	6
Error Log Requirements	6
Setup	7
InTrust Objects	7
Report Pack	8
Collecting SQL Server Data	9
Collecting the C2 Log	9
Collecting C2 Logs from Multiple Default SQL Server Instances	10
Collecting C2 Logs from Multiple Named SQL Server Instances	10
CollectC2LoadBalancing	10
Cleaning Up After Gathering	13
Collecting the Error Log	14
Collecting Replication Agent History	14
Using the Collection Task	15
Reporting	16
Viewing Reports in Knowledge Portal	16
About us	18
Contacting Quest	18
Technical support resources	18

SQL Server Auditing Overview

The SQL Server Knowledge Pack expands the auditing and reporting capabilities of InTrust to SQL Server. It lets you gather events from the SQL Server C2 log, the Error log and replication agent history, and make reports on these events.

Requirements

The Knowledge Pack is compatible with the following versions of Microsoft SQL Server Reporting Services:

- 2005
- 2008
- 2008 R2
- 2012
- 2014

Auditing Requirements

To gather the C2 log and the Error log with InTrust for reporting, configure SQL Server audit as described in the related topics:

- [C2 Log Requirements](#)
- [Error Log Requirements](#)

C2 Log Requirements

C2 logging is the more comprehensive of the two logging options in SQL Server. However, it is also more resource-intensive than Error log writing, and it is turned off by default. If C2 logging is disabled on your SQL servers for performance reasons, then you can only audit events from the Error log.

If you need to collect more information than the Error log can provide, then enable C2 logging for your SQL servers.

To enable C2 logging

1. In SQL Analyzer, run the following query to the relevant SQL server to enable advanced options:

```
EXEC sp_configure 'show advanced options', 1  
RECONFIGURE
```

2. Enable C2 audit mode:

```
EXEC sp_configure 'c2 audit mode', 1  
RECONFIGURE
```

The setting “1” establishes the C2 audit trace and turns on the option to fail the server should the server be unable to write to the audit file for any reason.

3. Run the following command:

```
EXEC sp_configure 'xp_cmdshell', 1  
RECONFIGURE
```
4. Restart the SQL server.

To successfully turn on C2 logging, you must be a member of the **sysadmin** role.

Gathering from Multiple Servers

To ensure correct operation when gathering C2 logs from several SQL servers

1. 1 On the InTrust server that performs the C2 log gathering, click **Start | Programs | Administrative Tools | Data Sources (ODBC)**.
2. 2 On the **Connection Pooling** tab, double-click the name of the driver that is used for gathering, and select **Don't pool connections to this driver**. If you are unsure which driver you need, check in the properties of the database events data source used during the gathering.

Error Log Requirements

Unlike the C2 log, the Error log is always enabled.

To prepare the SQL Server Error log for gathering

1. In SQL Server Management Studio, open the properties of the SQL server you need.
2. On the Security page, select the **Both failed and successful logins** option under Login Auditing.

The Knowledge Pack is installed as part of the extended InTrust deployment.

InTrust Objects

InTrust setup includes the following InTrust objects related to SQL Server:

- Data sources:
 - Microsoft SQL server C2 log
 - Microsoft SQL server C2 log (events for reporting)
 - Microsoft SQL Server Error log
 - Microsoft SQL server replication agents history
 - Microsoft SQL server miscellaneous replication agents history
- Gathering policies:
 - SQL Server C2 log
 - SQL Server Error log
 - SQL Server replication agents history
- Import policies:
 - SQL Server C2 log
 - SQL Server Error log
 - SQL Server replication agents history
- “SQL Server logs daily collection” task
- “All SQL servers in the domain” site

After installation, the site, the task and the policies do not require modification and are immediately ready for use. However, you can change the default settings to make the workflow fit your environment better. For instance, you may want to automate report creation by adding a reporting job to the “SQL Server logs daily collection” task.

Data sources must be configured for your environment, as described in the next chapter.

Report Pack

After you have completed the InTrust installation wizard, the reports appear in a new "InTrust | InTrust for Servers and Applications | SQL Server" report set in the Knowledge Portal.

Collecting SQL Server Data

[Collecting the C2 Log](#)

[Collecting the Error Log](#)

[Collecting Replication Agent History](#)

[Using the Collection Task](#)

Collecting the C2 Log

The “SQL Server C2 log (events for reporting)” data source, included in the “SQL Server C2 log gathering” policy, is used for collecting the C2 log. This is a lean data source designed strictly for reporting purposes. It helps you save bandwidth, database storage and processing time. This data source is used by default.

The other C2 log data source, “SQL Server C2 log”, lets you gather all events. Use it for purposes other than reporting, for example audit data archiving. This data source is not used by default.

Before you can start gathering, you must edit the data source you are using so that it suits your environment, as follows:

1. In InTrust Manager, expand **Configuration** and select **Data Sources**.
2. Open the data source’s properties in the right pane.
3. On the **Connection String** tab, click **Create** to specify the correct SQL ODBC driver, SQL server and credentials.

i **NOTE:** Note the following possible issues:

- InTrust gathering jobs expect C2 logs to be unlocked. The log can become locked, for example, if you open it in SQL Profiler or if a gathering job that started earlier is still processing it. To gather the C2 log successfully, make sure you avoid situations when it gets locked.
- You cannot gather events from the current C2 log file. Events from the file are accessible only after a newer file is created.
- When you gather replication agent history, you may get warning messages that result in duplicate “No replicated transactions are available” events in reports. To work around this problem, you can exclude these events from reports using report filters.

If you want to collect C2 logs from several SQL servers, your course of action depends on whether they are default instances or named instances.

Collecting C2 Logs from Multiple Default SQL Server Instances

Specify the “All SQL servers in the domain” site in the gathering job.

In the connection string of the C2 log data source that you are using, insert the variable %COMPUTER_NAME%, as follows:

```
SERVER = %COMPUTER_NAME%;
```

This variable is resolved as the name of the SQL server from which data is gathered. The list of SQL servers is obtained from the site.

i | **NOTE:** These actions will be successful only if the same credentials are required by all the relevant SQL servers.

Collecting C2 Logs from Multiple Named SQL Server Instances

The following table shows differences between gathering with and without agents.

	Agents	No agents
What to include in the site	One computer with the appropriate ODBC driver is enough for the InTrust site specified in the gathering job. It does not matter much what computer that is, as long as the computer has a reliable connection with the InTrust server on the one hand, and with all necessary SQL servers on the other hand.	If the InTrust server itself is connected to the SQL servers, it is a good idea to create and use a site that includes only the InTrust server.
How to configure data sources, jobs and policies	<p>InTrust gathers from one SQL server instance at a time, so there is no point in creating many jobs.</p> <p>Take the following steps:</p> <ol style="list-style-type: none">1. Make a copy of the appropriate C2 log data source for each named instance that you want to collect from.2. Configure their connection strings accordingly.3. Specify these copied data sources in the appropriate gathering policy. <p>You can also use a separate copy of the gathering policy for this purpose.</p>	<p>InTrust gathers from all specified SQL server instances at once if you have a separate gathering job for each SQL server instance, each using a separate gathering policy based on a separate data source.</p> <p>However, SQL servers are processed one by one if you configure data sources, jobs and policies as for gathering with agents.</p>

For more information about configuring database events data sources, see [Auditing Custom Logs](#).

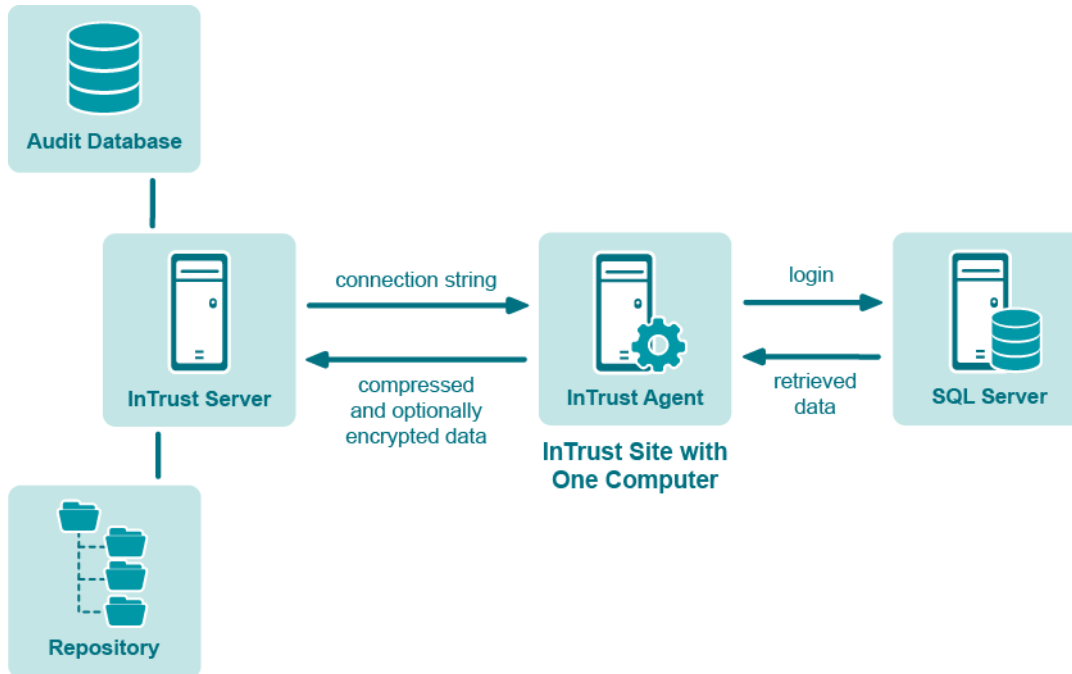
CollectC2LoadBalancing

Depending on how you organize gathering of SQL Server audit data, the SQL server, The InTrust server or the InTrust agent computer gets the most load. When planning the gathering, consider the following:

- What you include in the site or sites
- Whether or not to use agents

Method 1

You can use a site that includes one InTrust agent computer connected to one SQL server. To collect from multiple SQL servers in this way, create a similar site for each SQL server.



Gathering takes place as follows:

1. The InTrust server passes the SQL connection string to the agent. This connection string explicitly specifies the SQL server that data must come from.
2. The agent uses the connection string with the local ODBC driver to connect to the SQL server.
3. The agent retrieves C2 log data and packs it.
4. The collected data is compressed and forwarded to the InTrust server. Optionally, the data is encrypted.

! CAUTION: When you use an agent for data gathering and `trusted_connection` is set to true in the connection string, then the connection to the SQL server will be created under the agent account.

In most environments, this is the preferred way to organize C2 log gathering. The InTrust agent computer gets the most load in the process without significantly affecting SQL server and InTrust server performance.

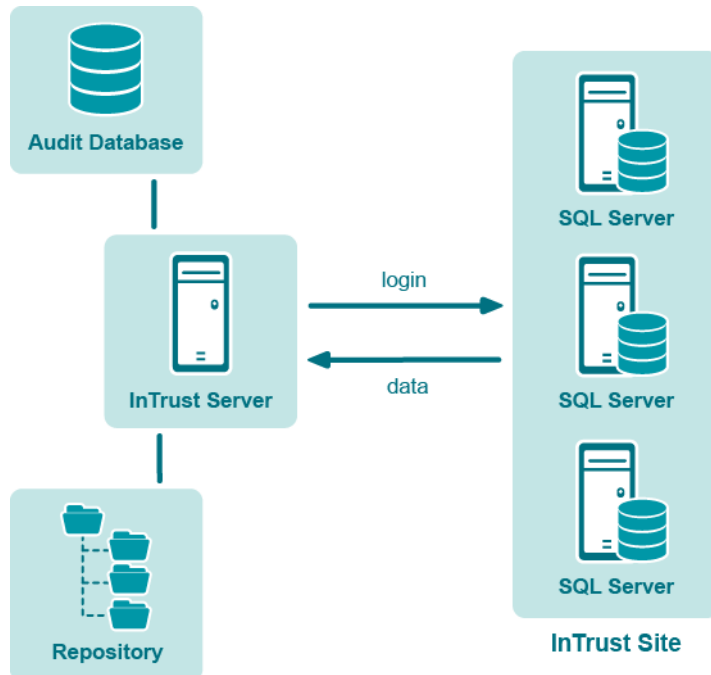
i NOTE: The following measures can help you improve gathering performance in this scenario:

- Running the agent on a powerful multi-core computer
- Adding RAM to the agent computer—however, this helps only if the available RAM is insufficient

With regard to performance, it does not matter whether the agent computer runs a workstation operating system or server operating system.

Method 2

You can use a site that includes multiple SQL servers and gather from them without agents. The following figure shows this workflow:



If you organize gathering like this, include the `%COMPUTER_NAME%` variable in the connection string of the data source that you use. The variable will be resolved for each computer in the site, and all computers in the site will be processed one by one.

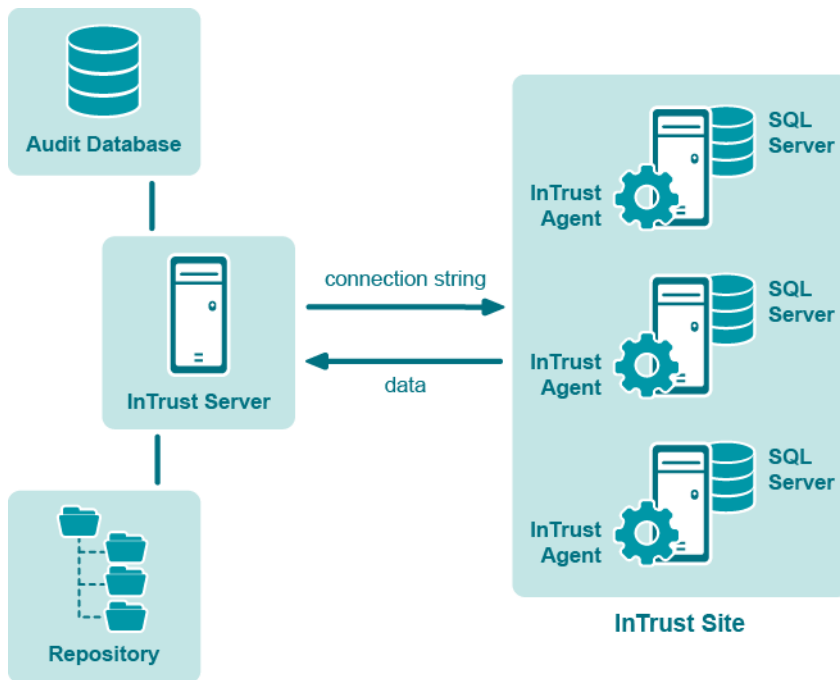
The following is a sample connection string for this gathering method:

```
DRIVER = SQL Server; SERVER = %COMPUTER_NAME%; UID = sa; PWD = %PASSWORD%; APP = Quest  
InTrust; WSID = InTrustServer
```

The InTrust server gets the most load in this case. Note that sequential gathering can take very long.

Method 3

You can use a site that includes multiple InTrust agents installed on SQL servers, as shown in the following figure:



In this workflow, include the %COMPUTER_NAME% variable in the connection string of the data source that you use. The variable will be resolved by each agent, and all agents will gather data simultaneously. See the description of Method 2 for a sample connection string.

In this case, the SQL servers get the most load.

Cleaning Up After Gathering

Cleanup is performed by running a cleanup SQL query. This query is specified in the data source properties on the SQL Cleanup Query tab. By default, cleanup is disabled. However, it is recommended that you enable it, unless you must retain all audit data. Cleanup helps reduce gathering time and saves disk space on your SQL servers.

To enable cleanup

1. Expand the node of the policy that uses the data source.
2. Open the properties of the data source.
3. On the **General** tab, select the **Clear log files after gathering** check box.
4. Commit the changes you have made.

The “Microsoft SQL Server C2 log” and “Microsoft SQL Server C2 log (events for reporting)” data sources are configured to delete C2 trace files after they have been gathered. If you want to keep the files, do the following:

1. Open the properties of the data source and switch to the **SQL Cleanup Query** tab.
2. Comment out the following line:

```
set @HowToClean = 'delete'
```

Now, instead of removing the files, InTrust will keep them and append the extension “.que” to their names.

Collecting the Error Log

The “Microsoft SQL Server Error log” data source, included in the “SQL Server Error log” policy, is used for collecting the Error log. The data source properties contain the absolute path to the Error log file. You need to edit the path for your particular environment; the default path specified there is just an example.

If the Error log is written to a location other than the default, then do as follows:

1. Make a copy of the “Microsoft SQL Server Error log” data source.
2. Open the properties of the new data source and, on the **Settings** tab, click **Edit**.
3. On the Path to Custom Text Log step of the wizard, correct the path.
4. Make a copy of the “SQL Server Error log” gathering policy, and include the new data source in it. Use the new policy in your Error log gathering job.

If you want to gather Error logs of named SQL server instances, then do as follows for each named instance:

1. Make a copy of the “Microsoft SQL Server Error log” data source.
2. Open the properties of the new data source and, on the Settings tab, click **Edit**.
3. On the Path to Custom Text Log step of the wizard, correct the path.
4. Continue to the next step of the wizard, select the regular expression and click **Edit**.
5. On the dialog box that appears, click **Add** next to the Field Mapping list box, and name the new field “Insertion String #2”.
6. Specify the name of the named instance as the value of “Insertion String #2”.
7. Complete the wizard.
8. Make a copy of the “SQL Server Error log” gathering policy, and include the new data source in it. Use the new policy in your Error log gathering job.

i **NOTE:** The log name is specified in the Log name field on the Settings tab in data source properties. For the SQL Server Error log, make sure “SQL Server Error log” is specified in that field. Otherwise, your Error log-based reports will not work properly.

Collecting Replication Agent History

To prepare for replication agent history gathering

1. Make as many copies of the necessary data source as there are distributor SQL servers.
2. For each distributor, do the following:
 - Open the properties of the corresponding data source.
 - In the connection string, specify the name of the distributor SQL server.

Using the Collection Task

The “SQL Server logs daily collection” includes jobs that gather all of the data that the Knowledge Pack is designed for.

i | **NOTE:** If C2 logging is turned off in your environment, disable the “SQL Server C2 log collection” job.

The task’s schedule is disabled by default. To enable the schedule, open the task’s properties and select the **Schedule enabled** option. The default schedule specifies that collection takes place daily. If necessary, adjust the schedule and rename the task appropriately.

The site from which data is collected includes only SQL servers from the same domain as the InTrust server by default.

If you want to automatically create and store reports on schedule, add a final reporting job to the task and include the reports you need.

For more information about working with tasks and jobs, refer to the [Auditing Guide](#).

Reporting

Reports provided with the Knowledge Pack are grouped by source as follows:

Source	Report Details
C2 log	<p>These reports cover users' login, account management and database management activity. Events for the reports can be gathered with two data sources:</p> <ol style="list-style-type: none">1 "All events in C2 log (events for reporting)" This data source specifies all events required for reports other than "All events in C2 log". The data source is used by default.2 "All events in C2 log" This data source specifies all events in the C2 log. Use the data source to gather events for the "All events in C2 log" report.
Error log	<p>These reports cover SQL Server maintenance and logons. If you need reports based on other events, use the "All events in Error log" report with appropriate filters. Reports on Error log events are based on the "SQL Server Error log" data source, which gathers all Error log events.</p>
Replication	<p>These reports cover the history of replication agents (both general and miscellaneous).</p>

Viewing Reports in Knowledge Portal

Knowledge Portal lets you work with reports interactively. This data view application enables you to:

- Organize the structure of the folders that reports are stored in
- Apply report properties to a number of reports at a time
- Customize reports view by modifying sort order within reports

To start working with the Knowledge Portal it is required to specify some of the security settings and data source properties.

Before you can view reports, you have to configure the data source to connect to the product database. Data sources are databases that store the information used in the reports.

It is also required to configure access rights to provide the report users with access to reports they need. These rights are assigned through specifying appropriate SQL Reporting Services role to a user or group account.

After the Knowledge Portal is properly configured open the InTrust Manager and launch a chosen task to create reports you need. Make sure that a reporting job is included in this task. Then in the Knowledge Portal click the **Reports** tab in the left tabbed pane and select the corresponding report. To view a report, select the **View Report** option in the right pane.

For detailed information, see [Leveraging Microsoft SQL Server Reporting Services Integration for Advanced Reporting](#).

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