Quest

Quest® InTrust 11.6.0

Preparing for Auditing Oracle Database

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 Oracle Database
Updated - November 2023
Version - 11.6.0

Contents

Oracle Auditing Overview

The Oracle Knowledge Pack expands the auditing and reporting capabilities of InTrust to Oracle. It lets you collect and report on the audit data from your Oracle database system. Featuring a fully automated workflow, InTrust helps you:

- Gather and consolidate a variety of data from the Oracle hosts running on different platforms
- Consolidate, store, and analyze this information
- Generate the reports on various aspects of your Oracle system operation

The following Oracle database system versions are supported:

- 18c
- 19c
- 21c

Data can be collected from the Oracle hosts running on the following platforms:

- Microsoft Windows 2012 and higher
- Redhat Enterprise Linux version 7 or above

Other platforms are also supported; however, reports on administrative users' activity will not be generated for them (all other reports will be created).

Reports on your Oracle database system cover the following areas:

- Activity of users with administrative privileges (logged on as SYSOPER or SYSDBA)
- Other users' activity, in particular, logons and logoffs
- User and role management activity
- Rights management
- Data retrieval and modification activity
- Data structure modification activity

Installing the Oracle Knowledge Pack

Support for Oracle auditing is provided by the Oracle Knowledge Pack. The Knowledge Pack must be installed on top of an existing InTrust installation.

Auditing Administrative User Activity

Gathering from Windows-Based Computers

Events from Oracle administrative users (users logged on to Oracle as SYSOPER or SYSDBA) are written into the Windows Application log of the Windows-based computers hosting Oracle database. This data is collected by InTrust in the traditional way, by retrieving events from the event logs on the specified computers.

In particular, to gather this data, you need to do the following:

1. On the target machine, turn auditing on by setting the AUDIT_SYS_OPERATIONS parameter in the SPFILE file to TRUE. To do that, either use Oracle Enterprise Manager or run an SQL query. For example, you can take following steps:
    a. Connect to the necessary database as SYSDBA and run the following query:
    ```
    select name, value from v$parameter where name like 'audit%'
    ```
    b. Then check whether the AUDIT_SYS_OPERATIONS parameter value is set to TRUE. If not, run the following query:
    ```
    ALTER SYSTEM SET audit_sys_operations = TRUE SCOPE=SPFILE;
    ```
    c. Wait for the system to report that the value has been altered, and restart Oracle database.
    d. Check whether administrative user events appear in the log.
2. Populate the 'Oracle for Windows servers in the domain' site with the machines you want to collect data from.
3. In the Oracle daily collection task, make sure that the 'Oracle administrative users audit collection' job involves the 'Oracle administrative user events from Application log' gathering policy, and that the job processes the 'Oracle for Windows servers in the domain' site.

Gathering from Unix-Based Computers

On a Unix-based computer hosting Oracle database, events from administrative users are written to the Oracle audit log files in text format. You can use InTrust to collect this data from Oracle hosts running on Linux or Unix machines. The InTrust gathering policy is named 'Oracle for Unix administrative users events' and treats the Oracle audit log as a Oracle Text Log data source of Custom Text Log type. You will have to customize the corresponding template, as described later in this section.

It is recommended that you use InTrust agents for gathering. Agents should be installed manually on target Unix machines. Install the agent and establish connection with InTrust Server as described in detail in Installing Agents Manually.

After you have deployed the agent on the target computer, include this computer in the Oracle for Unix Servers site.

To collect Oracle audit log from Unix-based computer

1. Find the path to the Oracle audit log file you want to collect. For that:
    a. Run the following command from the command prompt (SQLPlus must be installed on your computer):
    `sqlplus /nolog`
    b. Connect to the database, using the following command:
    `connect username/password@TNSName as SYSDBA`
    where
        - Username, password—credentials for database connection
        - TNSName—database you want to connect to
    c. Next, run the following query:
    `select name, value from v$parameter where name='audit_file_dest'`
    The Oracle log path will look like the following example:
    /u01/app/oracle/product/10.2.0/db_1/rdbms/audit
2. Check whether the log files are generated as a result of administrative activity.
3. In InTrust Manager, select **Configuration | Data Sources**, on the right pane, select Oracle Text Log, and create a copy of it. Right-click the copy and select **Properties**.
4. On the **General** tab, supply a name and description for the new data source.
5. On the **Settings** tab, make sure the log name is **Oracle Audit Log**. Click **Edit**.
In the **Path to text log** file text box, supply the path you obtained on step 2.
Click **Next**.
6. In the **Regular Expressions** list, select the first expression (it is of Data type), and click **Edit**.
7. In the **Field mapping** list, click **Add**, and add Insertion String #7. Specify your Oracle database name as the value for this field. Click **OK**, and then finish the wizard.
8. If you are gathering with agents, configure the “Oracle for Unix administrative users events” gathering policy, specifying the Custom Text Log you customized on steps 3 through 6 as the data source.
9. Configure the “Oracle Daily Collection” task, as follows:
    a. Disable all unnecessary jobs by clearing the **Enabled** check box on the job’s **General** tab.
    b. Make sure that the “Oracle for Unix administrative users audit collection” job is enabled.
    c. Go to the job’s **Gathering** tab, and specify the site you configured on step 8. Select the **Use agents to execute this job on target computers** check box.
    d. From the task’s shortcut menu, select **Properties**, and modify them as necessary.

Gathering logs from a Unix computer without an agent has the following differences from the workflow described above:

- The directory with the log must be available as an SMB share.
- The path to this SMB share must be specified in the using the %COMPUTER_NAME% variable and the share name (**\\%COMPUTER_NAME%*share_name***).

- The host must be a member of an InTrust site in the **Configuration | Sites | Microsoft Windows Network** container. InTrust currently supports gathering from network shares only in Microsoft Windows Environment sites; this workaround makes InTrust aware of the share even though the processed computer is not actually running Windows.
- A separate InTrust gathering policy under the **Gathering | Gathering Policies | Microsoft Windows Network** node must be created.
- The gathering job must use the custom site and gathering policy described above, instead of the predefined Oracle-related site and policy, which are intended for gathering with agents.
- The **Use agents to execute this job on target computers** check box must be turned off in the gathering job.

Auditing the Standard Audit Trail

Oracle database logs are retrieved from the SYS.AUD$ table in the database and communicated using the ODBC driver installed on the Windows-based computer that performs the InTrust gathering process. In other words, this computer operates like an “Oracle ODBC proxy”.

Generally, an Oracle ODBC proxy (with ODBC driver installed) can be one of the following:

- A computer where InTrust Server runs
- A dedicated Windows-based computer—in this case you need to deploy an InTrust agent on it

It is recommended that you use a dedicated machine for this purpose. Otherwise, the InTrust server is responsible for both communication with Oracle and gathering events, and this can lead to server overload.

> **CAUTION: If you need to collect Oracle database logs from Unix-based computers, you must always use a dedicated Windows machine (with InTrust agent installed) as an Oracle ODBC proxy.**

Consider organizing Oracle ODBC proxy computers into the “Oracle ODBC computers” site; InTrust agents will run the gathering service on them.

To gather Oracle database log data, take the following steps:

1. Turn on auditing of the Oracle hosts, as described in the following section.
2. In InTrust Manager, customize the Database Log Template by setting up the data source and connection settings for Oracle ODBC proxy, as described below.
3. Verify the connection settings.
4. Modify the InTrust predefined objects (site, policy, and task) for Oracle database log collection, as described below.

Turning on Auditing of an Oracle Host

1. 1 Connect to Oracle database as SYSDBA (use Oracle Enterprise Manager, or run an SQL query described below). For example, if you have SQLPlus installed on your computer, you can run the following command in the command prompt:
   ```
   sqlplus /nolog
   ```
   Then run the following command:
   ```
   connect username/password@TNSName as SYSDBA
   ```
   where
   - username, password—credentials for the database connection
   - TNSName—the database you want to connect to
2. Then you can run the following query:
   select name, value from v$parameter where name like ‘audit%’
3. Check the AUDIT_TRAIL value returned by the query. It must be set to the following:
   - For Oracle 18c, 19c, 21c: **DB_EXTENDED**

   If not, run the corresponding query, as follows:

- For Oracle 18c, 19c, 21c:
  ```
  ALTER SYSTEM SET AUDIT_TRAIL = 'DB','EXTENDED' SCOPE=SPFILE;
  ```

4. Wait for the system to report that it has been altered, and restart Oracle database.
5. Run the command necessary to provide the data for the report you need. For details, see the following section.

Fine-Tuning Audit Options for Reports

Oracle has a very flexible auditing configuration system with many options. To see what audit options are currently enabled, run:

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS;
```

The output should be similar to the following:

```
AUDIT_OPTION SUCCESS FAILURE

---------------------------------------- ---------- ----------

ALTER SYSTEM BY ACCESS BY ACCESS

SYSTEM AUDIT BY ACCESS BY ACCESS

CREATE SESSION BY ACCESS BY ACCESS

TABLE BY ACCESS BY ACCESS

CLUSTER BY ACCESS BY ACCESS

TABLESPACE BY ACCESS BY ACCESS

USER BY ACCESS BY ACCESS

ROLLBACK SEGMENT BY ACCESS BY ACCESS

TYPE BY ACCESS BY ACCESS

INDEX BY ACCESS BY ACCESS

CREATE USER BY ACCESS BY ACCESS
```

Add and remove audit options as necessary. For example, to start getting data for the "User Logons and Logoffs" report, run:

```
AUDIT SESSION
```

To disable auditing of a particular feature, run something like the following:

```
NOAUDIT CLUSTER
```

If you want to create your audit option configuration from scratch, you can start by turning off all audit options, as follows:

```
NOAUDIT ALL
```

See the descriptions of the reports you need to find out their auditing requirements.

Configuring the Oracle ODBC Proxy

Oracle ODBC driver (8.0.5 or later) must be installed on the Oracle ODBC proxy (that is, the computer where gathering process will run).

- If the process is agentless, then the Oracle ODBC proxy is the computer where InTrust Server resides.
- If agents are used (recommended), then the Oracle ODBC proxy is the computer where the InTrust agent is installed.

Setting Up ODBC
Configuring Database Log Template

Configuring Database Log Template

To simplify the database log gathering process, InTrust Manager offers a number of predefined data sources, in particular, the Oracle log gatherer templates: "Oracle 18c DB-based log", "Oracle 19c DB-based log" and "Oracle 21c DB-based log" for the corresponding Oracle versions.

A data source contains the following:

- Connection settings that the ODBC driver will use when accessing the Oracle database (connection string, password for database access, and so on)
- The SQL query that will be used to retrieve data from the database
- The SQL Cleanup query that will be used to clear data already gathered

You can customize the existing data source or create a new one. For useful details about the procedures briefly outlined here, see Custom Text Log Data Sources.

To customize a data source

1. In InTrust Manager, select **Configuration | Data Sources**, select the data source you need, and from its shortcut menu, select Copy.
2. Then modify the copy: select **Properties** from the shortcut menu, click **General**.
3. Edit the data source name and description.
4. Open the **Connection String** tab. The Log name is the one that InTrust will give to the log with gathered events (**InTrust for Oracle Audit log**). This descriptive name will be used to identify corresponding events in the InTrust audit database (for example, to create custom filters for the DB-based log). This name does not need to be modified.
5. Edit the ODBC connection string. If InTrust Manager is running on your Oracle ODBC proxy (that is, the computer with Oracle ODBC driver installed), the connection string will be generated automatically. If InTrust Manager and Oracle ODBC proxy are running on different computers, you will need to create the connection string manually. Make sure you have specified the ODBC driver name, database access credentials, and the TNS name. For details, see Specifying a Connection String below.
   You can use the **Keyword** button to insert predefined keywords.
6. Specify the password for connection.

NOTE: If you enter the password explicitly in the connection string, it will be stored as plain text and appear to other users of InTrust Manager. To prevent unauthorized access to this data, it is recommended that you use the **%PASSWORD%** keyword instead. This keyword stands for the password to be used for connection. Supply the password in the text box on the same step of the wizard. It will be securely kept in the InTrust configuration database and substituted at connection time.

7. Decide on the database field that will be used for data sorting. It is strongly recommended that you choose the field that contains the date and time, because InTrust storage is designed for data sorted by date.
8. On the **SQL Query** tab, enter the SQL query that retrieves necessary data from the database. Ensure ordering by the field you chose on step 7. For example, if the field is called **TIMESTAMP**, include this: `order by "TIMESTAMP"`
9. In the **Field mapping** list, configure the matching between the original database fields and those that InTrust stores. This governs how the retrieved data is arranged for storage. Map the **LAST_GATHERED_EVENT** InTrust field to the database field you chose on step 7.
10. On the **SQL Cleanup Query** tab, supply an SQL query to be executed after gathering. This query should clear gathered events from the database. The query is not run by default. To make it run, you will have to enable the **Clear log files after gathering** option for the DB-based log data provider in the gathering policy that uses the template.
11. Click **OK** to save the changes.

To create a new data source

1. In InTrust Manager, select **Configuration | Data Sources**, and from the shortcut menu, select **New Data Source**.
2. On the first step of the New Data Source Wizard you are prompted for the ODBC connection string. Specify the connection string, as described in the previous procedure.
   For details, see the Specifying a Connection String below.
3. Follow the steps of the wizard. You will be prompted for the same data as if you were modifying the data source. Refer to the procedure above for details.

Specifying a Connection String

A connection string must contain the following:

- A driver name—your Oracle ODBC driver (for example, Microsoft ODBC for Oracle)
- A server to communicate with—the TNS name you configured in the TNSNAMES.ORA file
- A UID (user name)—a user name to be used when connecting to the database
- A password—the user's password for connecting to the database

The connection string can be created automatically if the ODBC driver is installed on the same computer as InTrust Manager. Here is a sample procedure:

1. When creating a new data source, you will be prompted for connection string on the first step of the New Data Source Wizard. When modifying a connection string for the existing data source, in **InTrust Manager | Configuration | Data Sources**, select the data source, and from its shortcut menu, select **Properties**. Go to the **Connection String** tab.
2. Click **Create**.

3. From the list of drivers, select your Oracle ODBC driver; specify user credentials for database connection and the TNS name.
4. After the connection string is generated and verified, it appears in the **ODBC connection string** text box of the Properties dialog.

If you decide to create or modify the connection string manually when creating or modifying a data source, make sure you have specified the ODBC driver name, database access credentials, and the TNS name. You can use the **Keyword** button to insert predefined keywords.

InTrust Applications - Oracle 64-bit Server Communication

For 18C, 19C and 21c Oracle 64-bit servers, download the corresponding 32-bit oracle client software and follow the steps as described below:

1. Oracle 32-bit client should be installed along with
    - InTrust Server.
    - InTrust Manager (if it is installed on a separate machine instead of a server machine)
    - Oracle Server (if you want to create a site for Oracle server PC
      NOTE: Here "**ORCL**" is used as a Service name during the oracle server installation. If any different name is used during the installation, please use that name in the below-mentioned procedure instead of "**ORCL**".

Oracle Server Configuration changes

Edit listener.ora & tnsnames.ora files as mentioned below.

listener.ora:

1. Open ..\network\admin\listener.ora file.
2. Modify HOST to 0.0.0.0 IP and save it.

tnsnames.ora:

1. Open ..\network\admin\tnsnames.ora file.
2. Modify HOST to Local machine IP address under Listener_ORCL.
3. Modify HOST to IT2019.diana.local and SERVICE_NAME to orcl.diana.local under ORCL.
4. Here, IT2019 is the oracle server installed computer name, orcl is the Oracle service name and diana is the domain name. Make sure all details are correct as per the working environment.

Oracle 21c 32-bit client installation

Download and install 32-bit oracle 21c client **NT_213000_client_home.zip**

Oracle 19c 32-bit client installation

Download and install 32-bit oracle 19c client **NT_193000_client_home.zip**

Oracle 18c 32-bit client installation

1. Download “Instant Client Package—Basic” and “Instant Client Package—ODBC” for Microsoft Windows from https://www.oracle.com/in/database/technologies/instant-client/microsoft-windows-32-downloads.html
2. Unpack both Instant Client packages into a target directory, for example, c:\InstantClient.
3. In the PATH system environment variable, specify the target directory name.
4. In a command shell window (DOS-like), run the odbc_install.exe file from the package.
5. After its execution, add ORACLE_HOME and TNS_ADMIN system environment variables and specify the target directory name (C:\InstantClient for our example).
6. Copy TNSNAMES.ORA and LISENER.ORA in (C:\InstantClient) directory from Oracle server \network\admin\ location.

InTrust Manager Configuration Changes

1. Restart the oracle services.
2. In **Quest InTrust Manager | Configuration | Data Sources**, add a new Oracle 21c/19c/18c DB-based log data source, or if available copy the existing oracle data source and rename it to Oracle 21c/19c/18c DB-based log.
3. Right-click on the Oracle log and select Properties.
4. On the **Connection String** tab, click **Create** and select **Oracle ODBC driver** and click **OK**.
5. Enter Service Name, User Name, and Password, and click OK.
6. Please enter the correct oracle server machine name, port, and oracle service name as per the installed environment.
    - **Service Name Format**: oracle server machine name:port/oracle service name.
    - **Example**: IT2019:1521/orcl
7. 7. Create a New Site and Policy for Oracle 19c, add New Task, and run this job.

Gathering Data from Multiple Databases

To gather data from multiple Oracle databases, you can either use a separate data source for each database, or use a single data source. When tuning the data collection process, consider the following:

- You will need a separate Oracle ODBC proxy for each database. Include these computers in the ‘Oracle ODBC computers’ site.
- In the **TNSNAMES.ORA** file, configure the TNS Name for each Oracle ODBC proxy as its computer name.
- When configuring the connection string in the Database Log template, specify the server name using the keyword:
  `SERVER=%COMPUTER_NAME%`
  When you connect to the database, this keyword will be replaced with the Oracle ODBC proxy name.
- Since the data source will use the same connection string (and, thus, the same credentials for database access) for all databases, make sure this user account is granted access rights to these databases.

It is recommended that you verify the connection string on the Oracle ODBC proxy side. To test the connection string, you can use, for example, ODBC Data Source Administration.

Configuring Sites

It is recommended that you gather data using agents running on the Oracle ODBC proxy computers. Configure the InTrust site in the following way:

1. In InTrust Manager, create a copy of the existing 'Oracle ODBC computers' site. By default, this site contains all computers from the current domain where Oracle ODBC driver is installed. Clear the site.
2. Populate this site with Oracle ODBC proxy computers. Note that if you are going to gather data without agents, you have to include each computer in a separate site and assign a separate job to process it.

Setting Up a Gathering Policy

The following procedure describes how to set up a gathering policy to collect Oracle 21c audit trails. You can set up a policy for collecting Oracle 18c and Oracle 19c audit trails in a similar way.

NOTE: It is recommended that you create a copy of each predefined object (policy, task, or job) you need and then modify it as necessary.

1. In InTrust Manager, select **Gathering | Gathering policies | Microsoft Windows Network | Oracle 21c audit trail (ODBC)**.
2. Create a copy of this policy. From the shortcut menu, select **Add Data Source** and follow the wizard to add the data source you have prepared.
3. Under the policy node, select the old data source, and from its shortcut menu, select **Delete**.
4. Open the policy's properties, and on the **Filter** tab specify the filters you need.

Setting Up a Scheduled Task

1. In InTrust Manager, select the **Workflow | Tasks | Oracle Daily Collection and Reporting** task.
2. For each gathering job you need, go to the **General** tab and make sure the job is enabled.

NOTE: The task contains jobs for Oracle audit trail collection: "Oracle 18c audit trail collection (via ODBC)", "Oracle 19c audit trail collection (via ODBC)" and "Oracle 21c audit trail collection (via ODBC)". Select the job you need and make sure it is enabled. Disable the unnecessary jobs by clearing the **Enable** check box on the **General** tab (for example, you may not need the 'Oracle for Unix administrative users audit collection' job.)

3. For the Oracle audit trail collection job you need, on the **Gathering** tab select **Use agents to execute this job on target computers**.
4. From the task's shortcut menu, select **Properties** and modify the properties as necessary.

InTrust Configuration Objects for Oracle

- Gathering policies:
  - Oracle administrative user events from Application log
  - Oracle for Unix administrative user events
  - Oracle 21c audit trail (ODBC)
  - Oracle 19c audit trail (ODBC)
  - Oracle 18c audit trail (ODBC)
- Import policies:
  - Oracle administrative user events from Application log
  - Oracle for Unix administrative user events
  - Oracle 21c audit trail (ODBC)
  - Oracle 19c audit trail (ODBC)
  - Oracle 18c audit trail (ODBC)
- Jobs:
  - Oracle administrative users audit collection
  - Oracle for Unix administrative users audit collection
  - Oracle 21c audit trail collection (via ODBC)
  - Oracle 19c audit trail collection (via ODBC)
  - Oracle 18c audit trail collection (via ODBC)
  - Oracle reporting
- “Oracle daily collection and reporting” task
- Sites:
  - Oracle for Windows servers in the domain
  - Oracle for Unix servers
  - Oracle ODBC computers
- Data Sources:
  - Oracle 21c DB-based log
  - Oracle 19c DB-based log
  - Oracle 18c DB-based log
  - Oracle Text log

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