Netsurion. | EventTracker

How to Configure Oracle DB for EventTracker Integration

EventTracker v9.x and above

Publication Date: September 13, 2019

Abstract

This guide provides instructions to configure/ retrieve **Oracle database** events using “**Unified Audit Trail**”. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **Oracle database**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Oracle database v12c and above**.

Audience

Administrators who are assigned the task to monitor **Oracle database unified audit trail** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview

Oracle Database Service is just one of the Oracle offerings that provide Oracle Database. Users can create databases on DB systems, which are either bare-metal servers or virtual machines with block volumes.

EventTracker, when integrated with the Oracle database, enables users to view critical information related to activities performed in the Oracle database. This information is represented in the form of report, alert and graphical/ pictorial representation(dashboard).

In this integration guide, logging of an audit trail in the Oracle database is set using “**Unified Audit Trail**”.

Unified auditing enables you to capture audit records from the following sources:

- Audit records (including SYS audit records) from unified audit policies and AUDIT settings
- Fine-grained audit records from the DBMS_FGA PL/SQL package
- Oracle Database Real Application Security audit records
- Oracle Recovery Manager audit records
- Oracle Database Vault audit records
- Oracle Label Security audit records
- Oracle Data Mining records
- Oracle Data Pump
- Oracle SQL*Loader Direct Load

2. Prerequisites

- EventTracker agents should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- Users should have administrative privileges on the host system/ server to run PowerShell.
- Read access to the unified audit trail (Login credentials).
- Oracle Wallet, which includes “**tnsnames.ora**” (includes connection string).

3. Integrating Oracle Database with EventTracker

3.1 Setting Unified Audit Trail

Oracle Database provides predefined unified audit policies that cover commonly used security-relevant audit settings. These policies are not enabled for databases that were upgraded from earlier versions, except if the user had created a new database from the previous release and then upgraded it to the current release.

However, for new databases, these policies are enabled by default for both pure unified auditing environments. Default audit policies:

1. `ORA_LOGON_FAILURES`
2. `ORA_SECURECONFIG`
3. `ORA_DATABASE_PARAMETER`
4. `ORA_ACCOUNT_MGMT`
5. `ORA_CIS_RECOMMENDATIONS`
6. `ORA_RAS_POLICY_MGMT`
7. `ORA_RAS_SESSION_MGMT`
8. `ORA_DV_AUDPOL`
9. `ORA_DV_AUDPOL2`

Before setting up a unified audit trail, create a user “**EventTracker**” and grant the “**AUDIT_VIEWER**” role to it.

1. Check if Unified auditing is enabled. If yes, unified auditing is enabled.

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';

PARAMETER         VALUE

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

Unified Auditing  TRUE
```

2. If unified auditing has not been enabled, then the output is `FALSE`. Perform the below steps to enable it:

2.1 Log in to your SQL database. E.g. using SQL*Plus:

```
sqlplus sys as sysdba

Enter password: password
```

2.2 Stop all Oracle processes: databases, listener and Enterprise Manager (if necessary)**:**

a. **Stopping Oracle database:**

```
SQL> shutdown immediate

SQL> exit
```

b. **Stopping listener service:**

```
$ lsnrctl stop
```

c. **Stopping Enterprise Manager (if necessary):**

```
$ cd /u01/app/oracle/product/middleware/oms

$ export OMS_HOME=/u01/app/oracle/product/middleware/oms

$ $OMS_HOME/bin/emctl stop oms
```

2.3 Relink the oracle binaries to turn pure Unified Auditing on:

```
$ cd $ORACLE_HOME/rdbms/lib

$ make -f ins_rdbms.mk uniaud_on ioracle
```

2.4 Restart all Oracle processes: Enterprise Manager, listener, databases**.**

```
$ lsnrctl start

$ sqlplus / as sysoper

SQL> startup
```

2.5 Verify:

```
SQL> select VALUE from V$OPTION where PARAMETER='Unified
Auditing';

VALUE
--------------------
TRUE
```

3. Enable a Unified Audit Policy:

The `AUDIT POLICY` statement can enable a unified audit policy. The following command format is used to enable desired predefined unified audit policy:

```
SQL> AUDIT POLICY { policy_auditing } [WHENEVER [NOT]
SUCCESSFUL]

OR

SQL> AUDIT POLICY { policy_auditing }
```

e.g.

```
SQL> AUDIT POLICY ORA_LOGON_FAILURES WHENEVER NOT SUCCESSFUL;
```

To find all existing policies, query the `AUDIT_UNIFIED_POLICIES` data dictionary view. To find currently enabled policies, query `AUDIT_UNIFIED_ENABLED_POLICIES`.

e.g.

```
SQL> select distinct POLICY_NAME from AUDIT_UNIFIED_POLICIES;

SQL> select distinct POLICY_NAME from AUDIT_UNIFIED_ENABLED_POLICIES;
```

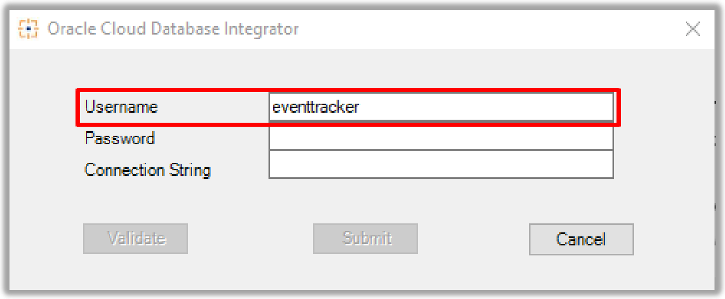
(**NOTE** – Please select the oracle audit policy as desired. The above-mentioned default policies are a point of reference.)

3.2 Forwarding Unified audit Logs to EventTracker

Once Unified auditing is enabled in Oracle database,

- Request the EventTracker support team for the "**Oracle database Integrator"** executable file.
- Once the executable application is received, right-click on the file and select "**Run as Administrator**".
- Running the Integrator, fill in the given fields.

3.1 Enter the DB "**username**":



Oracle Cloud Database Integrator

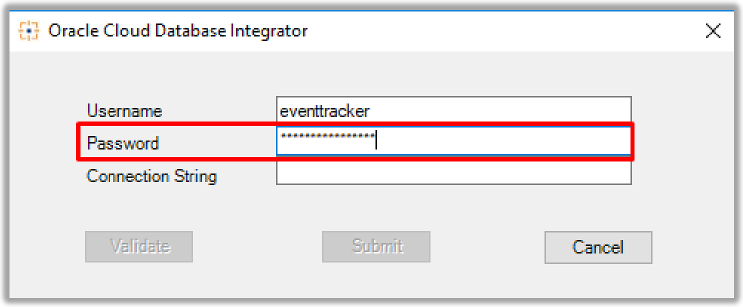
Username: eventtracker

Password:

Connection String:

Figure 1

3.2 Enter the DB "**password**":



Oracle Cloud Database Integrator

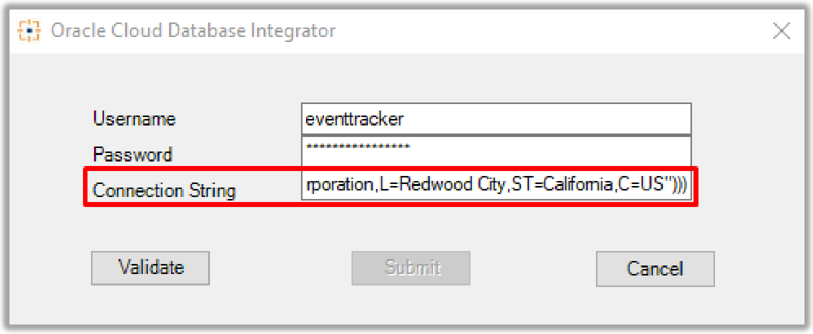
Username: eventtracker

Password: ****************

Connection String:

Figure 2

3.3 Enter the "**connection string**" as mentioned in "**tnsnames.ora**" file:



Username eventtracker

Password ****************

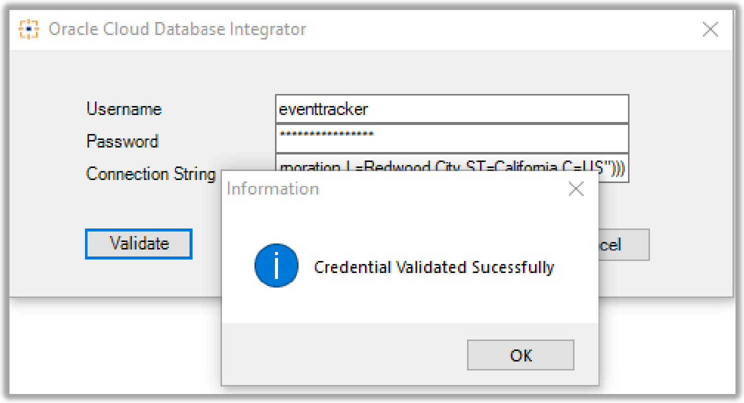
Connection String rporation,L=Redwood City,ST=California,C=US")))

Figure 3

e.g.

```
(description=
(address=(protocol=tcps)(port=1522)(host=adb.eu-frankfurt-
1.oracle.com))(connect_data=(service_name=xxxxxxxxxxxxx5o_u
adw_low.adwc.oracle.com))(security=(ssl_server_cert_dn="CN=
adwc.eucom-central-1.oracle.com,OU=Oracle BMCS
FRANKFURT,O=Oracle Corporation,L=Redwood
City,ST=California,C=US")))
```

3.4 Now, click on the “**validate**” button to verify the credentials:



Username eventtracker

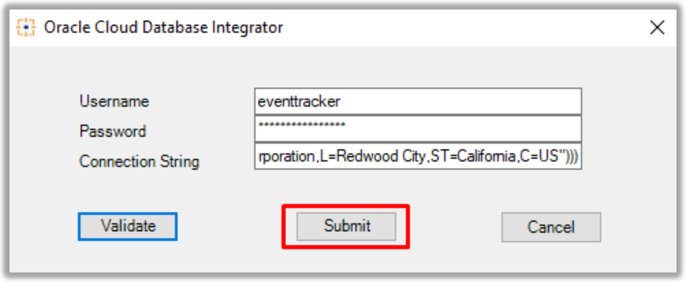
Password ****************

Connection String rporation,L=Redwood City,ST=California,C=US")))

Credential Validated Sucessfully

Figure 4

3.5 Click on the “**Ok**” button and then click on the “**submit**” button to complete the integration process.



Username eventtracker

Password ****************

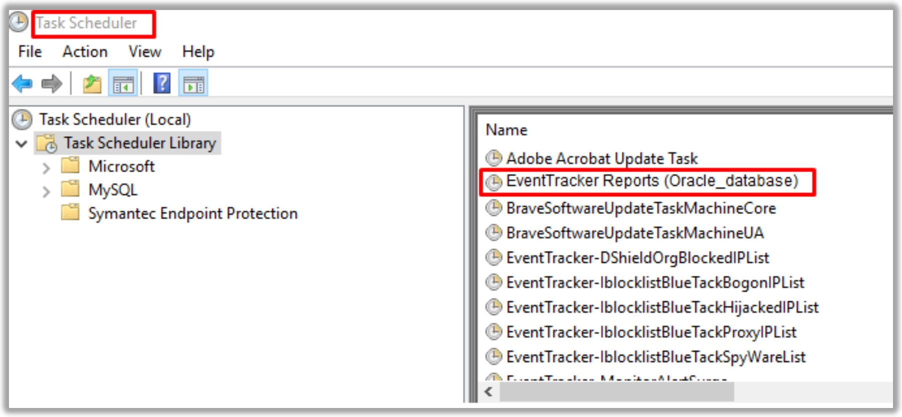
Connection String rporation,L=Redwood City,ST=California,C=US")))

Figure 5

3.3 Verification of Oracle database Integration

If the Integration is successful, the action can be verified in two ways:

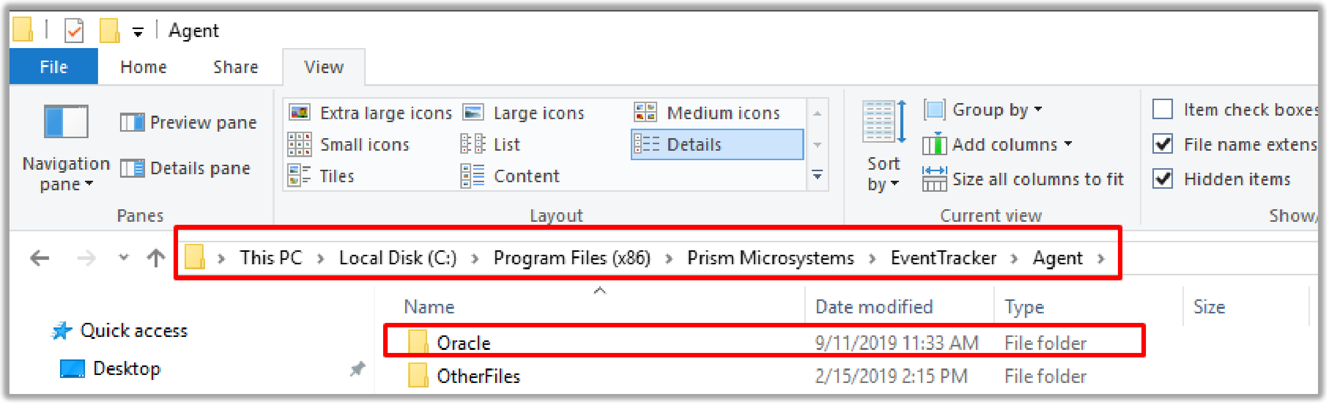
1. A scheduled task, named “**EventTracker Integrator (Oracle_database)**” is created in “**Task Scheduler**”.



Adobe Acrobat Update Task
EventTracker Reports (Oracle_database)
BraveSoftwareUpdateTaskMachineCore
BraveSoftwareUpdateTaskMachineUA
EventTracker-DShieldOrgBlockedIPList
EventTracker-IblocklistBlueTackBogonIPList
EventTracker-IblocklistBlueTackHijackedIPList
EventTracker-IblocklistBlueTackProxyIPList
EventTracker-IblocklistBlueTackSpyWareList

Figure 6

2. A new folder is created in EventTracker agent folder [“C:\Program Files (x86)\Prism Microsystems\EventTracker\Agent”], named “Oracle”.



This PC › Local Disk (C:) › Program Files (x86) › Prism Microsystems › EventTracker › Agent ›

Name	Date modified	Type	Size
Oracle	9/11/2019 11:33 AM	File folder	
OtherFiles	2/15/2019 2:15 PM	File folder	

Figure 7