1

Auditing Database Users, Privileges, and Objects

Objectives

After completing this lesson, you should be able to do the following:

- Implement basic database auditing
- Implement auditing of the privileged user
- Implement data manipulation language (DML) and data definition language (DDL) auditing
- Send audit records to the operating system (OS) files
- Configure audit trail purging

Monitoring for Suspicious Activity

- Monitoring or auditing should be an integral part of your security procedures.
- The audit tools in Oracle Database include:
  - Database auditing
  - Audit privileged user operations
  - Fine-grained auditing (FGA)
- You can create custom value-based auditing.

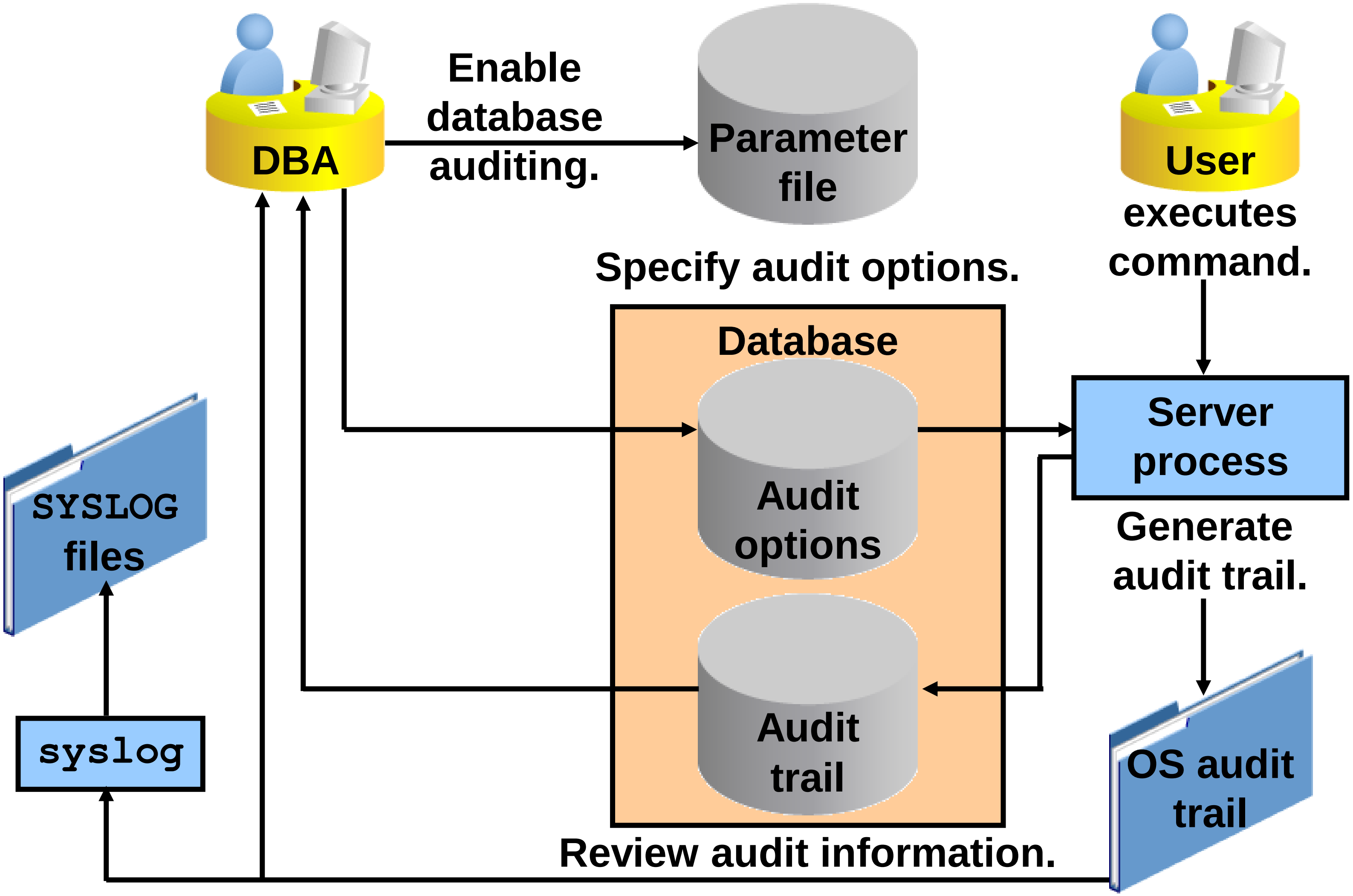
Audit Tool Comparisons

Type of Audit	What Is Audited?	What Can Be in the Audit Trail?
Standard database auditing	Privilege use, including object access	Fixed set of data, including the SQL statement and bind
Privileged user auditing	Connections by default When enabled, all the statements that are issued	Fixed set of data
Fine-grained auditing (FGA)	SQL statements (`INSERT`, `UPDATE`, `DELETE`, and `SELECT`) based on content	Fixed set of data, including the SQL statement and bind; extensible through event handlers

Standard Database Auditing: Overview

- Is enabled through the `AUDIT_TRAIL` parameter
- Can audit:
  - Login events
  - Exercise of system privileges
  - Exercise of object privileges
  - Use of SQL statements

Standard Database Auditing



Setting the `AUDIT_TRAIL` Parameter

The parameter values can be:

- `NONE`: Disables collection of audit records
- `DB`: Enables auditing with records stored in the database
- `DB,EXTENDED`: Populates `SQLBIND` and `SQLTEXT` columns
- `XML`: Enables auditing with records stored in XML format OS files
- `XML,EXTENDED`: Includes `SQLBIND` and `SQLTEXT` information
- `OS`: Enables auditing with records stored in the OS audit trail

Audit Log Location Options

Who has access?

- The database audit table is accessible to:
  - `SYSDBA`
  - The `DBA` role
  - Anyone with the `* ANY TABLE` privileges
- Optionally, Database Vault can protect database audit tables from the privileged users.
- OS audit files are accessible to:
  - The `root` user on the repository machine
  - Any user depending on directory permissions
- Audit Vault records are accessible to:
  - Configured users
  - Records protected by Database Vault

11.2

Moving the Database Audit Trail from the `SYSTEM` Tablespace

- The database audit trail (`SYS.AUD$` and `SYS.FGA_LOG$` tables) can be moved from the `SYSTEM` tablespace to:
  - `SYSAUX` tablespace
  - User-created tablespace
- Use the `DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION` procedure to move the audit trail tables from the current tablespace to a user-specified tablespace:

```
DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
   AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_DB_STD,
   AUDIT_TRAIL_LOCATION_VALUE => 'AT_TBS')
```

11.2

Limiting the Size of the Operating System Audit Trail

- The DBMS_AUDIT_MGMT.OS_FILE_MAX_SIZE property specifies the maximum size to which an operating system or XML audit file can grow before a new file is opened.
- Set the property by using the DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY procedure:

```
DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(
 AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_OS,
 AUDIT_TRAIL_PROPERTY=>DBMS_AUDIT_MGMT.OS_FILE_MAX_SIZE,
 AUDIT_TRAIL_PROPERTY_VALUE=>100)
```

- Query DBA_AUDIT_MGMT_CONFIG_PARAMS to view current settings.
- The default value is 10 MB.

11.2

Limiting the Age of the Operating System Audit Trail

- The `DBMS_AUDIT_MGMT.OS_FILE_MAX_AGE` property specifies the maximum age in days that an operating system or XML audit file is open before a new file is created.
- Set the property by using the `DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY` procedure:

```
DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(
 AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_OS,
 AUDIT_TRAIL_PROPERTY=>DBMS_AUDIT_MGMT.OS_FILE_MAX_AGE,
 AUDIT_TRAIL_PROPERTY_VALUE=>14)
```

- The default value is `5` days.

11.2

Clearing the Size and Age Properties

- Use the `DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY` procedure to clear the `DBMS_AUDIT_MGMT.OS_FILE_MAX_SIZE` and `DBMS_AUDIT_MGMT.OS_FILE_MAX_AGE` properties.
- Setting `USE_DEFAULT_VALUES` to:
  - `TRUE` sets the property to the default value
  - `FALSE` clears the property so that no file size or age is set

```
DBMS_AUDIT_MGMT.CLEAR_AUDIT_TRAIL_PROPERTY(
 AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_OS,
 AUDIT_TRAIL_PROPERTY=>DBMS_AUDIT_MGMT.OS_FILE_MAX_SIZE,
 USE_DEFAULT_VALUES=>TRUE)
```

Specifying Audit Options

- SQL statement auditing (nonfocused and focused):

```
AUDIT table;
AUDIT SELECT TABLE BY SCOTT BY ACCESS;
```

- System-privilege auditing (nonfocused and focused):

```
AUDIT select any table, create any trigger;
AUDIT select any table BY hr BY ACCESS;
```

- Object-privilege auditing (nonfocused and focused):

```
AUDIT ALL on hr.employees;
AUDIT UPDATE,DELETE on hr.employees BY ACCESS;
```

Auditing Sessions

- Audit unsuccessful attempts to connect:

```
AUDIT CREATE SESSION BY ACCESS
       WHENEVER NOT SUCCESSFUL;
```

- Monitor DBA_AUDIT_SESSION:

```
USERNA ACTION_NAME                    RETURNCODE LOGOFF
------ -------------------- ---------- ----------
FRED   LOGON                                1017
FRED   LOGOFF                                  0 0829 22:39
FRED   LOGOFF BY CLEANUP                       0 0829 22:40
FRED   LOGON                                   0
```

- Check DBA_AUDIT_TRAIL.COMMENT_TEXT.

Viewing Auditing Options

Data Dictionary View	Description
`ALL_DEF_AUDIT_OPTS`	Default audit options
`DBA_STMT_AUDIT_OPTS`	Statement auditing options
`DBA_PRIV_AUDIT_OPTS`	Privilege auditing options
`DBA_OBJ_AUDIT_OPTS`	Schema object auditing options

Viewing Auditing Results

Audit Trail View	Description
DBA_AUDIT_TRAIL	All audit trail entries
DBA_AUDIT_EXISTS	Records produced by the NOT EXISTS audit
DBA_AUDIT_OBJECT	Records concerning the schema objects
DBA_AUDIT_SESSION	All connect and disconnect entries
DBA_AUDIT_STATEMENT	Auditing records at the statement level

Quiz

To use standard database auditing to audit the use of object privileges, you need to set only the `AUDIT_TRAIL` parameter to `DB, EXTENDED` to generate audit records.

a. True

b. False

11.2

Purging Audit Trail Records

- Use the procedures in `DBMS_AUDIT_MGMT` to purge audit trail records after they have been archived.
- To configure automatic purging of archived audit trail records, perform the following steps:
  1. Initialize the audit trail for purging by executing the `INIT_CLEANUP` procedure.
  2. Set the "last archive timestamp" for the audit records by using the `SET_LAST_ARCHIVE_TIMESTAMP` procedure.
  3. Purge audit trail records by using the `CREATE_PURGE_JOB` to create and schedule a purge job.

11.2

Initializing the Audit Trail for Purging

- Configure the audit trail purging infrastructure and a default cleanup interval by executing `DBMS_AUDIT_MGMT.INIT_CLEANUP`:

```
DBMS_AUDIT_MGMT.INIT_CLEANUP(
 AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
 DEFAULT_CLEANUP_INTERVAL=>8)
```

- `INIT_CLEANUP` needs to be executed only once.
- Cleanup interval can be modified by using the `DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY` procedure.

11.2

Setting an Archive Timestamp for Audit Records

- DBMS_AUDIT_MGMT_SET_LAST_ARCHIVE_TIMESTAMP is used to specify when the audit records were last archived.
- DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL uses the timestamp to determine which audit records to purge.
- Time zone of the timestamp must be:
  - Coordinated Universal Time (UTC) for database audit trail tables
  - Local time zone time when the audit trail types are AUDIT_TRAIL_OS or AUDIT_TRAIL_XML

```
DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP(
 AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
 LAST_ARCHIVE_TIME=>'2010-01-13 2:00:00')
```

Manually Purging the Audit Trail

- You can manually purge the audit trail by using DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL.
- The USE_LAST_ARCH_TIMESTAMP parameter indicates whether to purge records created only before the last archive timestamp (TRUE) or all records (FALSE):

```
DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
 AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
 USE_LAST_ARCH_TIMESTAMP=>TRUE)
```

Scheduling an Automatic Purge Job for the Audit Trail

- Use `DBMS_AUDIT_MGMT.CREATE_PURGE_JOB` to automate audit trail purging.
- Modify the status of the purge job (enable/disable) by using `DBMS_AUDIT_MGMT.SET_PURGE_JOB_STATUS`.
- Modify the purge interval of the purge job by using `DBMS_AUDIT_MGMT.SET_PURGE_JOB_INTERVAL`.

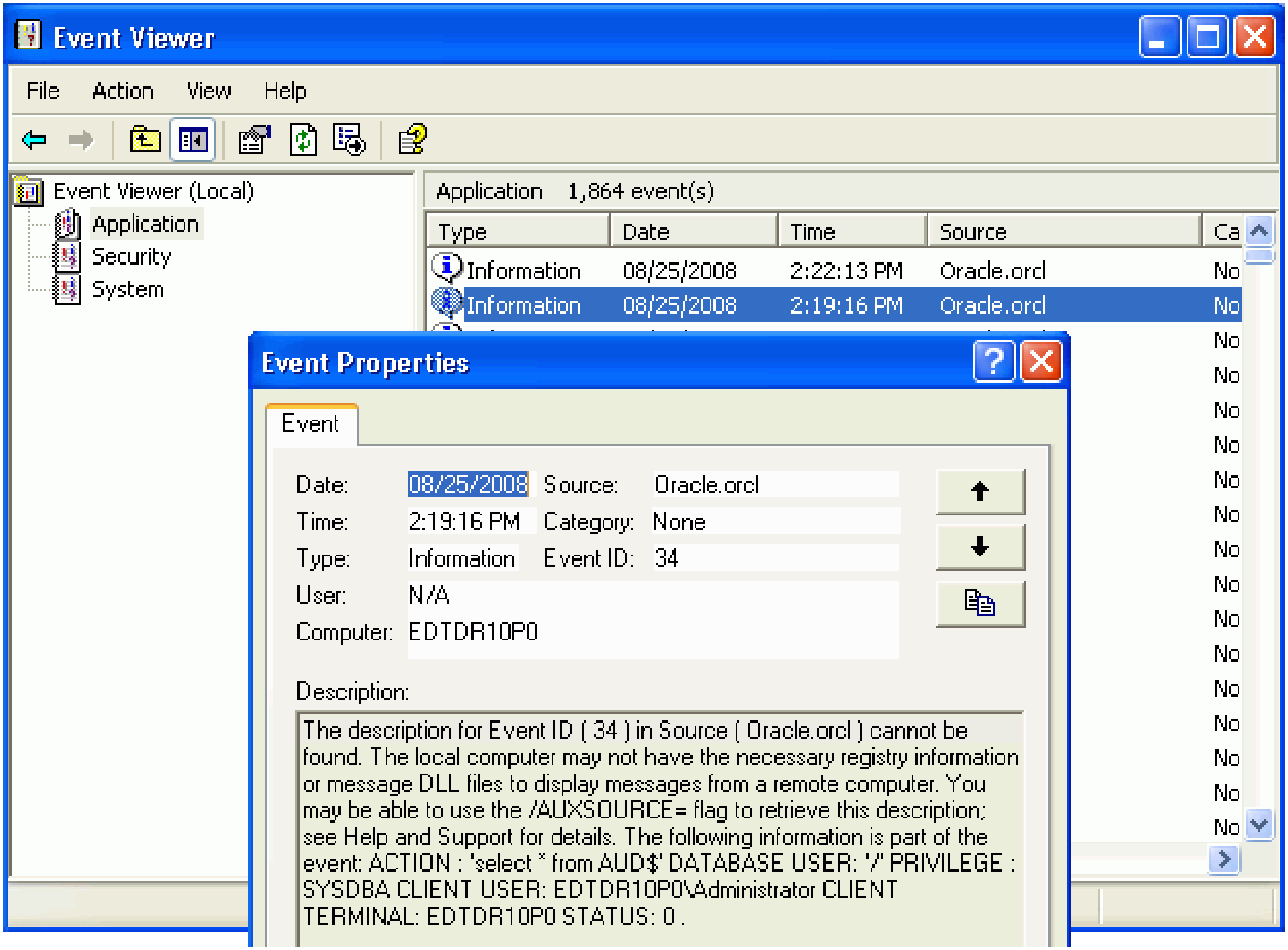
```
DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(
 AUDIT_TRAIL_TYPE=>DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
 AUDIT_TRAIL_PURGE_INTERVAL=>8,
 AUDIT_TRAIL_PURGE_NAME=>'AT_PURGE',
 USE_LAST_ARCH_TIMESTAMP=>TRUE)
```

Auditing the `SYSDBA` and `SYSOPER` Users

Control auditing of privileged users with the following parameters:

- `AUDIT_SYS_OPERATIONS` enables additional auditing of the `SYSDBA` or `SYSOPER` actions.
- `AUDIT_FILE_DEST` controls the location of the audit trail. The default is:
  - (UNIX or Linux)
    - First: `$ORACLE_BASE/admin/<ORACLE_SID>/adump`
    - Second: `$ORACLE_HOME/rdbms/audit`
  - On Windows: Windows Application Event Log

Viewing the `SYSDBA` Audit Trails



Application 1,864 event(s)

Type	Date	Time	Source	Ca
Information	08/25/2008	2:22:13 PM	Oracle.orcl	No
Information	08/25/2008	2:19:16 PM	Oracle.orcl	No

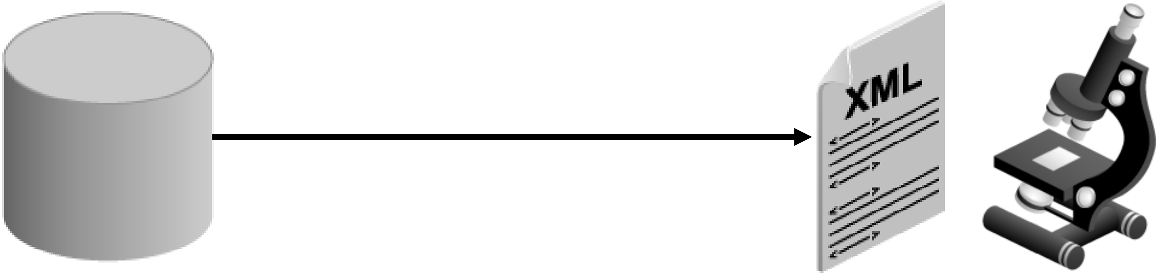
Date: 08/25/2008 Source: Oracle.orcl
Time: 2:19:16 PM Category: None
Type: Information Event ID: 34
User: N/A
Computer: EDTDR10P0

Description:

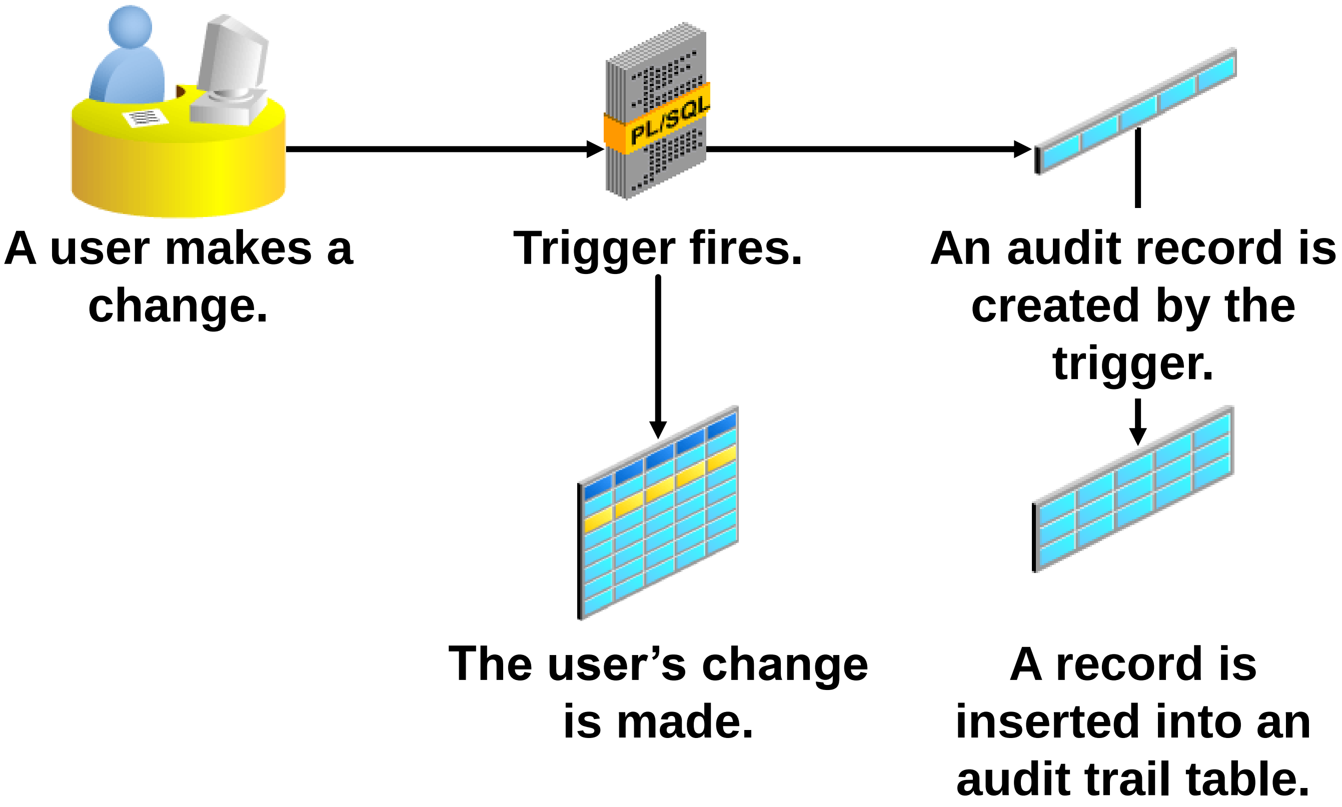
The description for Event ID (34) in Source (Oracle.orcl) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. You may be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details. The following information is part of the event: ACTION : 'select * from AUD$' DATABASE USER: '/' PRIVILEGE : SYSDBA CLIENT USER: EDTDR10P0\Administrator CLIENT TERMINAL: EDTDR10P0 STATUS: 0 .

Audit to XML Files

- Audit records can be sent to XML format files.
  - Standard audit
  - `SYS` operations audit records
  - Fine-grained audit (FGA) records
- XML files can be read with a variety of readers.
- XML files can be protected by the OS.



Value-Based Auditing



A user makes a change.

Trigger fires.

An audit record is created by the trigger.

The user's change is made.

A record is inserted into an audit trail table.

Triggers and Autonomous Transactions

Further enhance and protect the auditing by:

- Capturing DML changes to the shadow table
- Replicating audit records to another table
- Capturing attempts to change audit records

Summary

In this lesson, you should have learned how to:

- Implement basic database auditing
- Implement auditing of the privileged user
- Implement DML and DDL auditing
- Send audit records to the OS files
- Configure audit trail purging