CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

HOWTO Secure and Audit Oracle 10g and 11g

Ron Ben Natan

Foreword by Pete Finnigan

Chapter 10

Mandatory and Administrator Auditing

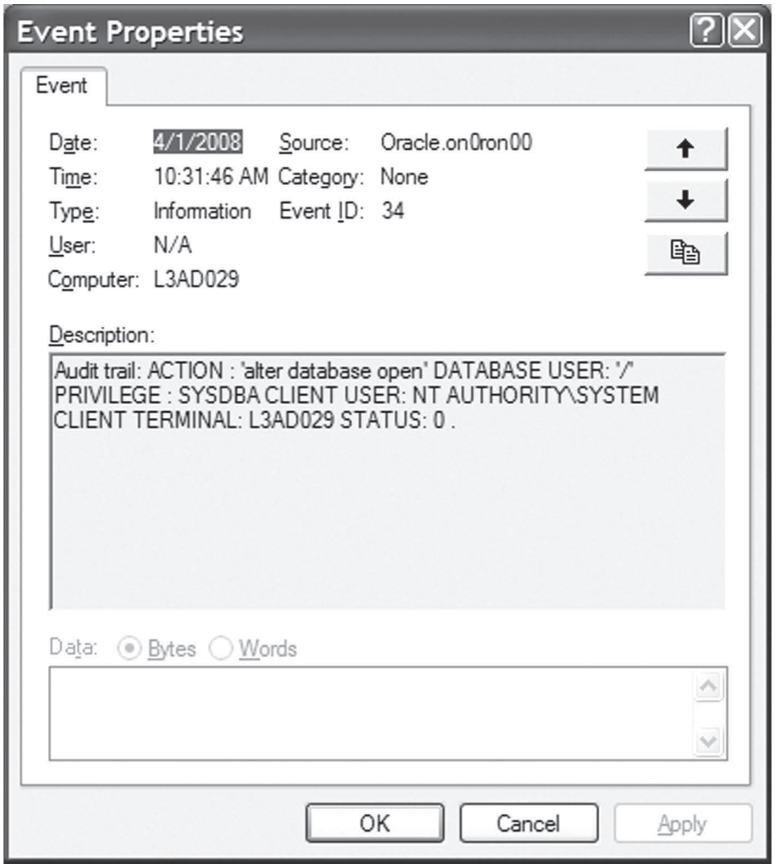
This is the shortest chapter in the book and it covers two simple categories of auditing. Although simple, they are of utmost importance. In all initiatives you will implement or you will be required to audit privileged user activity—and who more privileged than SYS or other users with SYSDBA privileges? This chapter shows you how to audit SYS activities and other important activities such as system startup and shutdown.

These HOWTOs were not included in Chapter 9 because administrator and mandatory auditing are indeed separate mechanisms; they are not part of standard auditing nor part of fine-grained auditing. You can enable standard auditing and you will still not get any audit records related to SYS activity. On the flip side, you can disable all auditing using NOAUDIT, but if you're auditing administrators then all SYS activities will still be logged. Finally, irrespective of where you choose to store the standard audit trail (DB or OS files) and what format you choose (e.g., XML), SYS auditing is always generated in files using a fixed format or sent to operating system log daemons such as syslog on Unix and the event log on Windows.

10.1 HOWTO Use Mandatory Auditing

Some activities are always audited even if you don't explicitly ask for them. These activities include all database startups, all database shutdowns, and all sysdba or sysoper logons. This is called mandatory auditing. On Unix these audit records go into the adump directory (by default) and on Windows these audit records are written to the Windows event log regardless of what you set the AUDIT_TRAIL parameter to.

Figure 10.1 shows a sample event in the Windows Event Viewer, in this case for a database startup. Figure 10.2 shows as event generated for a "/ as sysdba" connection on Windows. On Unix a shutdown after connecting as sysdba will produce the following two audit records in a single file in the adump directory:



Date: 4/1/2008 Source: Oracle.on0ron00
Time: 10:31:46 AM Category: None
Type: Information Event ID: 34
User: N/A
Computer: L3AD029

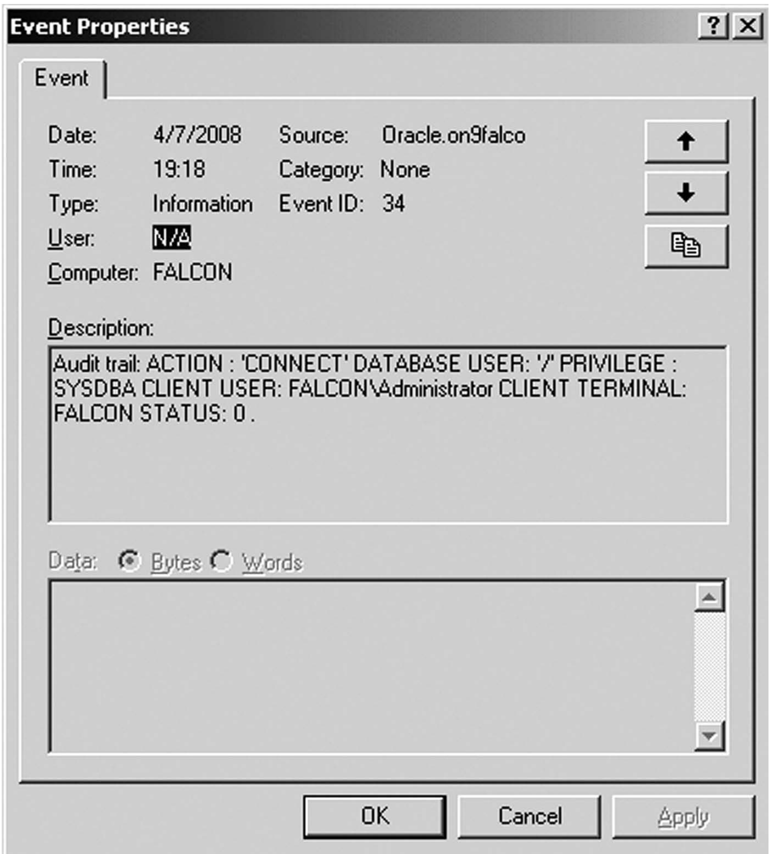
Description:

Audit trail: ACTION : 'alter database open' DATABASE USER: '/' PRIVILEGE : SYSDBA CLIENT USER: NT AUTHORITY\SYSTEM CLIENT TERMINAL: L3AD029 STATUS: 0 .

Figure 10.1 Mandatory auditing—Windows event for database startup.

```
Audit file /home/oracle10/admin/on0jumbo/adump/ora_25953.aud
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0              -   Production
With the Partitioning, OLAP and Data Mining options
ORACLE_HOME = /home/oracle10/product/10.2.0/db_1
System name:     Linux
Node name:        jumbo.guardium.com
Release:          2.6.9-55.0.2.ELsmp
Version:          #1 SMP Tue Jun 12 17:59:08 EDT 2007
Machine:           i686
Instance name:   on0jumbo
Redo thread mounted by this instance: 1
Oracle process number: 17
Unix process pid: 25953, image: oracle@jumbo.guardium.com

Mon Apr 7 19:13:02 2008
ACTION : 'CONNECT'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle10
CLIENT TERMINAL: pts/1
STATUS: 0
```



Date: 4/7/2008
Time: 19:18
Type: Information
User: N/A
Computer: FALCON
Source: Oracle.on9falco
Category: None
Event ID: 34

Description:

Audit trail: ACTION : 'CONNECT' DATABASE USER: '/' PRIVILEGE : SYSDBA CLIENT USER: FALCON\Administrator CLIENT TERMINAL: FALCON STATUS: 0 .

Figure 10.2 Mandatory auditing—Windows event for sysdba logon.

```
Mon Apr 7 19:15:12 2008
ACTION : 'SHUTDOWN'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle10
CLIENT TERMINAL: pts/1
STATUS: 0
```

Connecting using "/ as sysoper" produces an audit record of the form:

```
Audit file /home/oracle10/admin/on0jumbo/adump/ora_26182.aud
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options
ORACLE_HOME = /home/oracle10/product/10.2.0/db_1
System name:     Linux
Node name:       jumbo.guardium.com
Release:         2.6.9-55.0.2.ELsmp
Version:         #1 SMP Tue Jun 12 17:59:08 EDT 2007
Machine:         i686
Instance name:   on0jumbo
Redo thread mounted by this instance: 1
Oracle process number: 15
Unix process pid: 26182, image: oracle@jumbo.guardium.com (TNS V1-V3)
```

```
Mon Apr 7 19:17:15 2008
ACTION : 'CONNECT'
DATABASE USER: '/'
PRIVILEGE : SYSOPER
CLIENT USER: oracle10
CLIENT TERMINAL: pts/1
STATUS: 0
```

Note that these audit records do not include any details on the activity done by those connected with sysdba or sysoper privileges, just the fact that the connections occurred. For this you will have to turn to the next HOWTO.

Other Audit Records That Are Always Written

Another set of activities that are always recorded no matter what you configure are changes to the audit trail itself. Any Data Manipulation Language (DML) statements performed on SYS.AUD$ and SYS.FGA_LOG$ (see Chapter 11) are logged to SYS.AUD$.

Four Things to Remember about Mandatory Audit:

1. Startup of the database, shutdown, and logon using sysdba and sysoper privileges are always logged in OS files regardless of what audit trail you configure.
2. In Windows, these audit records are written to the application event log.
3. Mandatory auditing only audits the fact that an administrator logged on, it does not audit what they did.
4. Although these audit files are small, they can add up. Make sure to rotate these files and archive/purge them on a regular basis.

10.2 HOWTO Enable Administrator Auditing

Mandatory auditing logs SYS connections but does not show you what the user SYS did. Standard auditing itself does not write audit records for SYS. For example, set an audit trail:

```
SQL> show parameter audit_trail

NAME                                         TYPE       VALUE
-------------------------------------------  --------   -------------------------------
audit_trail                                  string     DB
```

Now logon as SYS and see how many audit records are there

```
-bash-3.00$ sqlplus / as sysdba
SQL*Plus: Release 11.1.0.6.0 - Production on Mon Apr 7 19:35:13 2008
Copyright (c) 1982, 2007, Oracle. All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
SQL> select count(*) from aud$;
COUNT(*)
------------
   1578
```

Set an audit rule:

```
SQL> audit all on scott.emp;
Audit succeeded.
```

Now access the table (still as the user SYS):

```
SQL> select count(*) from scott.emp;
COUNT(*)
--------
     14
```

The audit trail will not be updated:

```
SQL> select count(*) from aud$;
COUNT(*)
--------
   1578
```

To enable administrator auditing you need to set another parameter:

```
SQL> show parameter audit;

NAME                                        TYPE         VALUE
------------------------------------------ ------------ -------------------------------
audit_file_dest                             string       /var/oracle11/admin/on1condo/a
                                                         dump
audit_sys_operations                        boolean      FALSE
audit_syslog_level                          string
audit_trail                                 string       DB
```

Enable administrator auditing by setting AUDIT_SYS_OPERATIONS:

```
SQL> alter system set audit_sys_operations=true scope=spfile;
System altered.
```

Then, shutdown and startup the database. At this point ALL SYS-issued statements are audited indiscriminately. The data is not going to the standard audit trail, it is going to separate files in the audit_file_dest directory. For example, if after setting AUDIT_SYS_OPERATIONS to TRUE and restarting the database you perform:

```
SQL> select count(*) from aud$;
COUNT(*)
------------
   1582
SQL> select count(*) from scott.emp;
COUNT(*)
------------
     14
```

```
SQL> select count(*) from aud$;
COUNT(*)
-------------
   1582
```

However, you get the audit trail shown in Listing 10.1.

Three Things to Remember about Mandatory Audit:

1. Both mandatory auditing and standard auditing do not log activity performed by SYS. To enable SYS auditing set AUDIT_SYS_OPERATIONS to TRUE and restart the database.
2. SYS auditing is always logged to operating system files and defaults to the adump directory.
3. SYS auditing logs indiscriminately—make sure that you have enough space in AUDIT_FILE_DEST, that you don't run heavy batches or jobs using sysdba or sysoper privileges, and that you rotate these files periodically.

10.3 HOWTO Use Syslog Auditing

Syslog is a standard for forwarding log messages in an Internet Protocol (IP) network. The term "syslog" is often used for both the actual syslog protocol, as well as the application or library sending syslog messages. Syslog is often used for system management and security auditing. It is supported by a wide variety of devices and receivers across multiple platforms and is therefore often used to integrate log data from many different types of systems into a central repository.

On Unix you can send administrator audit records (as well as standard audit records) to syslog. This is the Unix equivalent to the use of the Windows event log. The advantage of using syslog is that the adump files can be modified by the instance account owner whereas syslog files are usually owned by root. Moreover, syslog is often used by Security Event Managers (SEMs) and other log aggregators and correlation engines.

The syslog protocol is a client/server protocol. The syslog client sends a small textual message (less than 1024 bytes) to the syslog server. The receiver is commonly called "syslogd," "syslog daemon," or "syslog server." Syslog messages can be sent via User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). The data is sent in cleartext however although wrappers such as Stunnel, sslio, or sslwrap can be used to encrypt syslog messages. You can also use syslog-ng to encrypt the messages. When you configure Oracle to use syslog, Oracle calls a syslog library to write its audit records. From a syslog perspective Oracle is acting as a client and syslogd is acting as the server.

Before you configure syslog auditing you should know what you have configured in /etc/syslog.conf. Syslog.conf controls how the syslog daemon logs events. Every syslog message has two attributes—a facility and a priority. Syslogd.conf defines what to do with messages per facility and priority. A sample config file is shown below:

```
# cat /etc/syslog.conf
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
kern.*                                                   /dev/console
```

```
Audit file /var/oracle11/admin/on1condo/adump/ora_1060894.aud
Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
ORACLE_HOME = /var/oracle11/product/11.1.0/db_1
System name:   AIX
Node name:     condor
Release:       3
Version:       5
Machine:       0000853F4C00
Instance name: on1condo
Redo thread mounted by this instance: 1
Oracle process number: 18
Unix process pid: 1060894, image: oracle@condor (TNS V1-V3)

Mon Apr 7 19:51:47 2008
ACTION : 'CONNECT'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle11
CLIENT TERMINAL: pts/0
STATUS: 0

Mon Apr 7 19:52:22 2008
ACTION : 'ALTER DATABASE OPEN'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle11
CLIENT TERMINAL: pts/0
STATUS: 0

Mon Apr 7 19:52:29 2008
ACTION : 'select count(*) from aud$'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle11
CLIENT TERMINAL: pts/0
STATUS: 0

Mon Apr 7 19:52:38 2008
ACTION : 'select count(*) from scott.emp'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle11
CLIENT TERMINAL: pts/0
STATUS: 0

Mon Apr 7 19:52:44 2008
ACTION : 'select count(*) from aud$'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: oracle11
CLIENT TERMINAL: pts/0
STATUS: 0
```

Listing 10.1 Sample administrator audit trail.

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                    /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                                  /var/log/secure

# Log all the mail messages in one place.
mail.*                                                      -/var/log/maillog

# Log cron stuff
cron.*                                                      /var/log/cron

# Everybody gets emergency messages
*.emerg                                                     *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                              /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                    /var/log/boot.log
```

Each line in this file starts with a selector. A selector specifies a combination of a facility and a priority and then specifies where the messages are to be written. In this example, each line specifies a file but syslog can also redirect messages to remote syslog servers. For example, the first line specifies that all messages sent to the KERN facility are logged to the console no matter what their priority. The next line specifies that all messages sent to any facility with the info priority and that all messages sent to the mail, cron, or authpriv facilities with no priority are written to /var/log/messages. Priorities (also called severities) include EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, and DEBUG. Facilities include AUTH, AUTHPRIV, CRON, DAEMON, FTP, KERN, LPR, MAIL, MARK, NEWS, SECURITY, SYSLOG, USER, UUCP, and LOCAL0–LOCAL7. To configure syslog auditing for Oracle you simply specify which facility and which priority Oracle should use for its messages.

Audit records in Oracle are written to syslog in two cases. For standard auditing you can set AUDIT_TRAIL to OS and then set AUDIT_SYSLOG_LEVEL to a value specifying a facility and a priority. For administrator auditing (AUDIT_SYS_OPERATIONS = TRUE) just set the AUDIT_SYSLOG_LEVEL. For example, if your syslog.conf has a line of the form:

```
*.info;mail.none                              /var/adm/syslog/syslog.log
```

Logon to the database, set the two initialization parameters and restart the database:

```
-bash-3.2$ sqlplus / as sysdba
SQL*Plus: Release 11.1.0.6.0 - Production on Tue Apr 8 17:55:24 2008
Copyright (c) 1982, 2007, Oracle. All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
SQL> alter system set audit_sys_operations=true scope=spfile;
System altered.
SQL> alter system set audit_ syslog_level='local1.info' scope=spfile;
System altered.
SQL> shutdown
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup
ORACLE instance started.
Total System Global Area 521936896 bytes
Fixed Size                 2124664 bytes
Variable Size            406848648 bytes
Database Buffers         109051904 bytes
Redo Buffers               3911680 bytes
Database mounted.
Database opened.
```

If you made a mistake in the facility or priority you get the following error:

```
SQL> startup
ORA-32028: Syslog facility or level not recognized
```

At this point, all SYS activity will be recorded by syslog, e.g.,

```
-bash-3.2$ sqlplus / as sysdba
SQL*Plus: Release 11.1.0.6.0 - Production on Tue Apr 8 18:41:12 2008
Copyright (c) 1982, 2007, Oracle. All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
SQL> delete from aud$;
3460 rows deleted.
```

In the syslog file you get an audit record of the form:

```
Apr 4 09:44:59 vireo Oracle Audit: SESSIONID: "6784"
ENTRYID: "1" STATEMENT: "6" USERID: "SYS" USERHOST: "vireo"
TERMINAL: "pts/2" ACTION: "7" RETURNCODE: "0" OBJ$CREATOR: "SYS" OBJ$NAME:
"AUD$" SES$TID: "4564" OS$USERID: "oracle11"
```

Database security

HOWTO Secure and Audit Oracle 10g and 11g

Ron Ben Natan

Foreword by Pete Finnigan

Oracle is the number one database engine in use today. The fact that it is the choice of military organizations and agencies around the world is part of the company's legacy and is evident in the product. Oracle has more security-related functions, products, and tools than almost any other database engine. Unfortunately, the fact that these capabilities exist does not mean that they are used correctly or even used at all. In fact, most users are familiar with less than 20 percent of the security mechanisms within Oracle.

Written by Ron Ben Natan, one of the most respected and knowledgeable database security experts in the world, ***HOWTO Secure and Audit Oracle 10g and 11g*** shows readers how to navigate the options, select the right tools and avoid common pitfalls. The text is structured as *HOWTOs* — addressing each security function in the context of Oracle 11g and Oracle 10g.

Among a long list of *HOWTOs*, readers will learn to —

- Choose configuration settings that make it harder to gain unauthorized access
- Understand when and how to encrypt data-at-rest and data-in-transit and how to implement strong authentication
- Use and manage audit trails, and advanced techniques for auditing
- Assess risks that may exist and determine how to address them
- Make use of advanced tools and options such as Advanced Security Options, Virtual Private Database, Audit Vault, and Database Vault

The text also provides an overview of cryptography, covering encryption and digital signatures and shows readers how Oracle Wallet Manager and orapki can be used to generate and manage certificates and other secrets.

While the book's 17 chapters follow a logical order of implementation, each *HOWTO* can be referenced independently to meet a user's immediate needs. Providing authoritative and succinct instructions highlighted by examples, this ultimate guide to security best practices for Oracle bridges the gap between those who install and configure security features and those who secure and audit them.

CRC Press
Taylor & Francis Group
an **informa** business
www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

AU4127
ISBN: 978-1-4200-8412-2
90000
9 781420 084122

www.auerbach-publications.com