```
##
## SPDX-FileCopyrightText: 2021 Splunk, Inc. <sales@splunk.com>
## SPDX-License-Identifier: LicenseRef-Splunk-8-2021
##
##

[oracle_audit_type_lookup]
filename = oracle_audit_type.csv

[oracle_action_lookup]
filename = oracle_audit_action_410.csv

[oracle_returncode_lookup]
filename = oracle_returncode.csv
min_matches = 1
max_matches = 1
default_match = failure
match_type = WILDCARD(RETURNCODE)

[oracle_privilege_lookup]
filename = oracle_system_privilege_map.csv

[oracle_statementtype_lookup]
filename = oracle_fga_statement_type.csv

[oracle_login_failure_reason_lookup]
filename = oracle_login_failure_reason.csv

[oracle_ora_code_lookup]
filename = oracle_ora_codes.csv
min_matches = 1
max_matches = 1
default_match = Unknown
match_type = WILDCARD(ORACODE)


[COMMENTTEXT_text]
REGEX = COMMENT\$TEXT\s*\:\[?\d*\]?\s+"([^"]+)
FORMAT = COMMENTTEXT::$1

[CLIENTIP_text]
REGEX = COMMENT\$TEXT\s*\:\[?\d*\]?\s+".*\(HOST=([^\r\n)]*)\)
FORMAT = CLIENTIP::$1

[CLIENTPORT_text]
REGEX = COMMENT\$TEXT\s*\:\[?\d*\]?\s+".*\(PORT=(\d+)\)
FORMAT = CLIENTPORT::$1

[SESSIONID_text]
REGEX = SESSIONID\s*\:\[?\d*\]?\s+['|"]?(\d+)
```

```
FORMAT = SESSIONID::$1

[ENTRYID_text]
REGEX = ENTRYID\s*\:\[?\d*\]?\s+['|"]?(\d+)
FORMAT = ENTRYID::$1

[STATEMENT_text]
REGEX = STATEMENT\s*\:\[?\d*\]?\s+['|"]?(\d+)
FORMAT = STATEMENT::$1

[ACTION_text]
REGEX = ACTION\s*\:\[?\d*\]?\s+['|"]?([^"'\r\n]*)
FORMAT = ACTION::"$1"

[ORACLE_AUDIT_ACTION_text]
REGEX = ACTION\s*\:\[?\d*\]?\s+['|"]?([^"'\r\n]*)
FORMAT = oracle_audit_action::"$1"

[ACTION_NUMBER_text]
REGEX = ACTION\s+NUMBER\s*\:\[?\d*\]?\s+['|"]?([^'"\r\n]+)
FORMAT = ACTION_NUMBER::"$1"

[object_text]
REGEX = ACTION\s*\:\[?\d*\]?\s+['|"]?alter\s+user\s+(.+)account
FORMAT = object::"$1"

[STATUS_text]
REGEX = STATUS\s*\:\[?\d*\]?\s+['|"]?([^'"\r\n]+)
FORMAT = STATUS::"$1"

[CLIENT_USER_text]
REGEX = CLIENT\s+USER\s*\:\[?\d*\]?\s+['|"]?([^'"\r\n]+)
FORMAT = CLIENT_USER::"$1"

[CLIENT_TERMINAL_text]
REGEX = TERMINAL\s*\:\[?\d*\]?\s+['|"]?([^'":\r\n]+)
FORMAT = CLIENT_TERMINAL::"$1"

[DATABASE_USER_text]
REGEX = DATABASE\s+USER\s*\:\[?\d*\]?\s+['|"]?([^'"\r\n]+)
FORMAT = DATABASE_USER::"$1"

[PRIVILEGE_text]
REGEX = PRIVILEGE\s*\:\[?\d*\]?\s+['|"]?([^'"\r\n]+)
FORMAT = PRIVILEGE::"$1"

[PRIVUSED_text]
REGEX = PRIV\$USED\s*\:\[?\d*\]?\s+["|']?(\d+)
FORMAT = PRIVUSED::$1
```

```
[RETURNCODE_text]
REGEX = RETURNCODE\s*\:\[?\d*\]?\s+["|']?(\d+)
FORMAT = RETURNCODE::$1

[USERHOST_text]
REGEX = USERHOST\s*\:\[?\d*\]?\s+["|']?([^"']*)
FORMAT = USERHOST::$1

[USERID_text]
REGEX = USERID[\s*]?\:\[?\d*\]?\s+["|']?([^'"]*)
FORMAT = USERID::$1

[OSUSERID_text]
REGEX = OS\$USERID\s*\:\[?\d*\]?\s+["|']?([^"']*)
FORMAT = OSUSERID::$1

[OBJNAME_text]
REGEX = OBJ\$NAME\s*\:\[?\d*\]?\s+["|']?([^"']*)
FORMAT = OBJNAME::"$1"

[OBJCREATOR_text]
REGEX = OBJ\$CREATOR\s*\:\[?\d*\]?\s+["|']?([^"']*)
FORMAT = OBJCREATOR::$1

[DBID_text]
REGEX = DBID\s*\:\[?\d*\]?\s+["|']?([^"']+)
FORMAT = DBID::$1

[LOGOFFPREAD_text]
REGEX = LOGOFF\$PREAD\s*\:\[?\d*\]?\s+["|']?(\d+)
FORMAT = LOGOFFPREAD::$1

[LOGOFFLWRITE_text]
REGEX = LOGOFF\$LWRITE\s*\:\[?\d*\]?\s+["|']?(\d+)
FORMAT = LOGOFFLWRITE::$1

[LOGOFFDEAD_text]
REGEX = LOGOFF\$DEAD\s*\:\[?\d*\]?\s+["|']?(\d+)
FORMAT = LOGOFFDEAD::$1

[SESSIONCPU_text]
REGEX = SESSIONCPU\s*\:\[?\d*\]?\s+["|'](\d+)
FORMAT = SESSIONCPU::$1


[AUDITTYPE_xml]
REGEX = <Audit_Type>(\d+)</Audit_Type>
FORMAT = AUDITTYPE::$1

[SESSIONID_xml]
```

```
REGEX = <Session_Id>(\d+)</Session_Id>
FORMAT = SESSIONID::$1

[STATEMENT_xml]
REGEX = <StatementId>(\d+)</StatementId>
FORMAT = STATEMENT::$1

[ENTRYID_xml]
REGEX = <EntryId>(\d+)</EntryId>
FORMAT = ENTRYID::$1

[USERID_xml]
REGEX = <DB_User>(.*)</DB_User>
FORMAT = USERID::$1

[CLIENT_USER_xml]
REGEX = <Client_Id>(.*)</Client_Id>
FORMAT = CLIENT_USER::$1

[CURRENT_USER_xml]
REGEX = <Current_User>(.*)</Current_User>
FORMAT = CURRENT_USER::$1

[OSUSERID_xml]
REGEX = <OS_User>(.*)</OS_User>
FORMAT = OSUSERID::$1

[USERHOST_xml]
REGEX = <Userhost>(.*)</Userhost>
FORMAT = USERHOST::$1

[OSPROCESS_xml]
REGEX = <OS_Process>(.*)</OS_Process>
FORMAT = OSPROCESS::"$1"

[CLIENT_TERMINAL_xml]
REGEX = <Terminal>(.*)</Terminal>
FORMAT = CLIENT_TERMINAL::"$1"

[INSTANCE_xml]
REGEX = <Instance_Number>(\d+)</Instance_Number>
FORMAT = INSTANCE_NUM::$1

[OBJCREATOR_xml]
REGEX = <Object_Schema>(.*)</Object_Schema>
FORMAT = OBJCREATOR::$1

[OBJNAME_xml]
REGEX = <Object_Name>(.*)</Object_Name>
FORMAT = OBJNAME::$1
```

```
[POLICYNAME_xml]
REGEX = <Policy_Name>(.*)</Policy_Name>
FORMAT = POLICYNAME::$1

[NEWOWNER_xml]
REGEX = <New_Owner>(.*)</New_Owner>
FORMAT = NEWOWNER::$1

[ACTION_xml]
REGEX = <Action>(\d+)</Action>
FORMAT = ACTION::$1


[ORACLE_AUDIT_ACTION_xml]
REGEX = <Action>(\d+)</Action>
FORMAT = oracle_audit_action::$1


[STMTTYPE_xml]
REGEX = <Stmt_Type>(\d+)</Stmt_Type>
FORMAT = STMTTYPE::$1

[RETURNCODE_xml]
REGEX = <Returncode>(-?\d+)</Returncode>
FORMAT = RETURNCODE::$1

[AUTHPRIVILEGE_xml]
REGEX = <AuthPrivileges>(.*)</AuthPrivileges>
FORMAT = AUTHPRIVILEGE::$1

[OSPRIVILEGE_xml]
REGEX = <OSPrivilege>(.*)</OSPrivilege>
FORMAT = OSPRIVILEGE::$1

[GRANTEE_xml]
REGEX = <Grantee>(.*)</Grantee>
FORMAT = GRANTEE::$1

[PRIVUSED_xml]
REGEX = <Priv_Used>(\d+)</Priv_Used>
FORMAT = PRIVUSED::$1

[PRIVGRANTED_xml]
REGEX = <Priv_Granted>(\d+)</Priv_Granted>
FORMAT = PRIVGRANTED::$1

[DBID_xml]
REGEX = <DBID>(.*)</DBID>
FORMAT = DBID::$1
```

```
[SQLTEXT_xml]
REGEX = <Sql_Text>(.*)</Sql_Text>
FORMAT = SQLTEXT::$1

[COMMENTTEXT_xml]
REGEX = <Comment_Text>(.*)</Comment_Text>
FORMAT = COMMENTTEXT::$1

[CLIENTIP_xml]
REGEX = <Comment_Text>.*\(HOST=([^\r\n)]*)\)
FORMAT = CLIENTIP::$1

[CLIENTPORT_xml]
REGEX = <Comment_Text>.*\(PORT=([\d]+)\)
FORMAT = CLIENTPORT::$1


[ALERTORGID_xml]
REGEX = org_id='([^']*)'
FORMAT = ORGID::$1

[ALERTCOMPID_xml]
REGEX = comp_id='([^']*)'
FORMAT = COMPID::$1

[ALERTTYPE_xml]
REGEX = type='([^']*)'
FORMAT = TYPE::$1

[ALERTLEVEL_xml]
REGEX = level='([^']*)'
FORMAT = LEVEL::$1

[ALERTHOST_xml]
REGEX = host_id='([^']*)'
FORMAT = HOSTID::$1

[ALERTMSG_xml]
REGEX = <txt>([^<]*)
FORMAT = MSG::$1

[ALERTMSGID_xml]
REGEX = msg_id='([^']*)'
FORMAT = MSGID::$1

[ORACODE]
REGEX = (ORA-\d+)
FORMAT = ORACODE::$1
MV_ADD = true
```

```
REPEAT_MATCH = true

[PROGRAM_listener]
REGEX = \(PROGRAM=([^)]*)\)\(HOST=[^)]*\)\(USER=[^)]*\)
FORMAT = PROGRAM::$1

[CLIENTIP_listener]
REGEX = \(PROGRAM=[^)]*\)\(HOST=([^)]*)\)\(USER=[^)]*\)
FORMAT = CLIENTIP::$1

[CLIENTUSER_listener]
REGEX = \(PROGRAM=[^)]*\)\(HOST=[^)]*\)\(USER=([^)]*)\)
FORMAT = CLIENT_USER::$1

[USER_listener]
REGEX = \(PROGRAM=[^)]*\)\(HOST=[^)]*\)\(USER=([^)]*)\)
FORMAT = user::$1

[DESTIP_listener]
REGEX = \(HOST=([^)]*)\)\(PORT=\d+\)
FORMAT = DESTIP::$1

[DESTPORT_listener]
REGEX = \(HOST=[^)]*\)\(PORT=(\d+)\)
FORMAT = DESTPORT::$1

[STATUS_listener]
REGEX = \(HOST=[^)]*\)\(PORT=\d+\)[^\r\n]*\s*\*\s*(\d+)
FORMAT = STATUS::$1

[ORACLE_SUFFIX]
REGEX = ([^\s^,]+#?)="?([^,"]+)"?
FORMAT = $1::$2

# Perf
# If you are using DBX 1.0, please copy all of the DELIMS and FIELDS lines for
# ORACLE_SYS_PERF, ORACLE_OS_PERF, ORACLE_LIB_CACHE, ORACLE_DBFILEIO_PERF stanzas to
the local/transforms.conf and uncomment these lines.

#[ORACLE_SYS_PERF]
#DELIMS = ","
#FIELDS = BEGIN_TIME,INTSIZE_CSEC,METRIC_NAME,VALUE,METRIC_UNIT

#[ORACLE_OS_PERF]
#DELIMS = ","
#FIELDS = STAT_NAME,VALUE,CUMULATIVE

#[ORACLE_LIB_CACHE]
#DELIMS = ","
#FIELDS =
```

```
NAMESPACE,GETS,GETHITS,GETHITRATIO,PINS,PINHITS,PINHITRATIO,RELOADS,INVALIDATIONS,DL
M_LOCK_REQUESTS,DLM_PIN_REQUESTS,DLM_PIN_RELEASES,DLM_INVALIDATION_REQUESTS,DLM_INVA
LIDATIONS

#[ORACLE_DBFILEIO_PERF]
#DELIMS = ","
#FIELDS = TYPE,FILE_NAME,PHYRDS,PHYWRTS,AVGIOTIM,MINIOTIM,MAXIOWTM,MAXIORTM

[ORACLE_QUERY]
REGEX = SQL_FULLTEXT="(.*)", PLAN_HASH_VALUE=
FORMAT = query::$1

[setnull]
# The `Dump file` is for Oracle version 19c and higher
REGEX = (?:(?:Trace|Dump) file *.+\.trc|<\?xml)
DEST_KEY = queue
FORMAT = nullQueue
```