Database Security and Auditing: Protecting Data Integrity and Accessibility

Auditing Database Activities

Objectives

- Use Oracle database activities
- Learn how to create DLL triggers with Oracle
- Audit database activities using Oracle

Objectives (continued)

- Audit server activities with Microsoft SQL Server 2000
- Audit database activities using Microsoft SQL Profiler
- Use SQL Server for security auditing

Using Oracle Database Activities

- Several types of activities:
  - Application activities: SQL statements issued against application tables
  - Administration activities: commands issued for maintenance and administrative purposes
  - Database events: events that occur when a specific activity occurs

Creating DDL Triggers with Oracle

- Audit program provides:
  - Audit trail for all activities
  - Opportunity for using process controls
- Database activities statements (in addition to DML):
  - Data Definition Language (DDL)
  - Data Control Language
  - Database events
  - SQL statements audit trail

Creating DDL Triggers with Oracle (continued)

- Use CREATE TRIGGER:
  - DDL statements
  - Database events

Example of LOGON and LOGOFF Database Events

- Steps:
  - Log on as SYSTEM
  - Create the APP_AUDIT_LOGINS table
  - Create two triggers:
    - One that fires after the logon event
    - One that fires before the logoff event
  - Log on as DBSEC; disconnect after a few minutes
  - Log on as SYSTEM to check the auditing table

DDL Event Example

- Steps:
  - Log on as SYSTEM
  - Create a trigger that fires before an ALTER statement is completed
  - Log on as DBSEC and alter a table
- Pseudocolumns:
  - ora_dict_obj_name
  - ora_dict_obj_owner
  - ora_sysevent

Auditing Code with Oracle

- Steps:
  - Log on as DBSEC
  - Create an auditing table
  - Create a table and populate it with two records
  - Create a trigger to track code
  - Update the new table
  - Look at the contents of the APP_AUDIT_SQLS table

Auditing Database Activities with Oracle

- Oracle provides mechanisms for auditing all:
  - Who creates or modifies the structure
  - Who is granting privileges to whom
- Two types of activities based on the type of SQL command statement used:
  - Defined by DDL (Data Definition Language)
  - Defined by DCL (Data Control Language)

Auditing DDL Activities

- Use a SQL-based AUDIT command
- Verify auditing is on:
  - Check the AUDIT_TRAIL parameter
  - Values:
    - DB
    - DB_EXTENDED
    - OS
    - NONE

Auditing DDL Activities (continued)

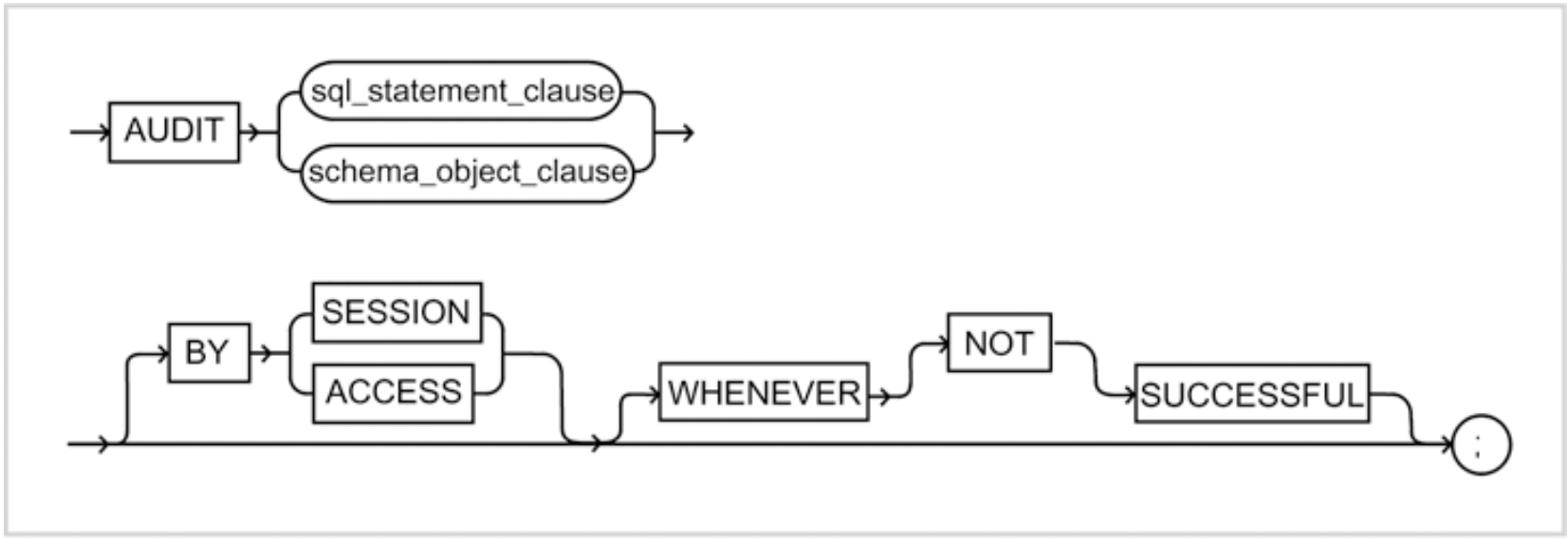

FIGURE 9-1 Audit command syntax diagram

DDL Activities Example 1

- Steps:
  - Use any user other than SYS or SYSTEM to create a table
  - Add three rows into the table
  - Log on as SYSTEM or SYS to enable auditing: For ALTER and DELETE
  - Log in as DBSEC:
    - Delete a row
    - Modify the structure of the table

DDL Activities Example 1 (continued)

- Steps (continued):
  - Check the audit records
  - Log in as SYSTEM and view the DBA_AUDIT_TRAIL table
  - Turn off the auditing option
  - Check the content of the DBA_AUDIT_OBJECT to see auditing metadata

DDL Activities Example 1 (continued)

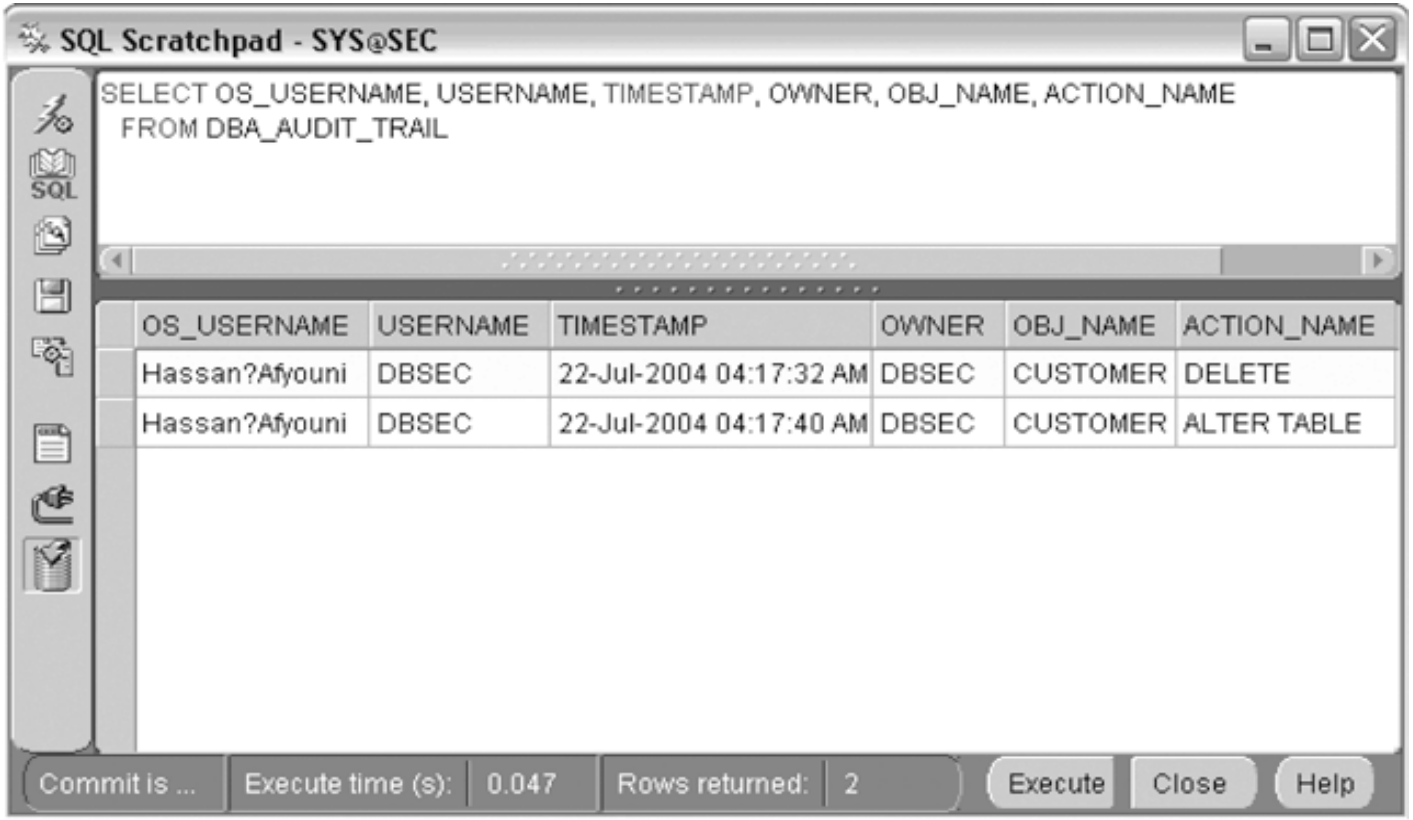

FIGURE 9-2 Contents of DBA_AUDIT_TRAIL

DDL Activities Example 1 (continued)

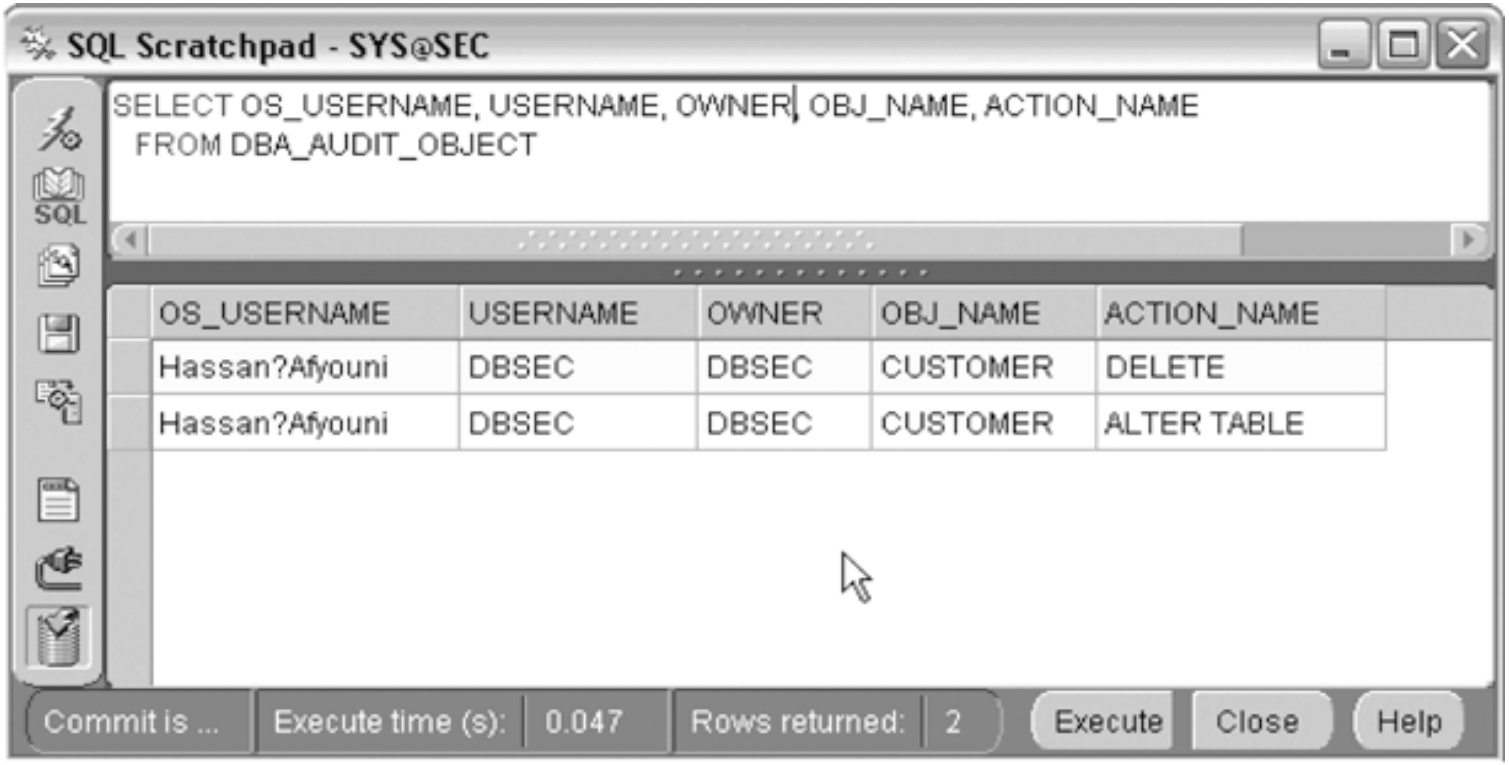

FIGURE 9-3 Contents of DBA_AUDIT_OBJECT

DDL Activities Example 2

- Steps:
  - Log in as SYSTEM or SYS to enable auditing for the TABLE statement; ALTER, CREATE, and DROP TABLE statements
  - Log on as DBSEC and create a table, then drop the table
  - Log on as SYSTEM; view the content of DBA_AUDIT_TRAIL
  - Turn off auditing for the TABLE statement

DCL Activities Example

- Steps:
  - Log on as SYSTEM or SYS and issue an AUDIT statement
  - Log on as DBSEC and grant SELECT and UPDATE to SYSTEM
  - Log on as SYSTEM and display the contents of DBA_AUDIT_TRAIL
  - Review audit data dictionary

DCL Activities Example (continued)

Table 9-1 Audit data dictionary views

Table name	Description of contents
DBA_AUDIT_TRAIL	All audit trail records when the AUDIT_TRAIL initialization parameter is set to DB or DB_EXTENDED
DBA_AUDIT_OBJECT	All audit trail records for database objects
DBA_AUDIT_SESSION	All audit trail records for session connections and disconnections
DBA_AUDIT_STATEMENT	All audit trail records for GRANT, REVOKE, AUDIT, NOAUDIT, and ALTER SYSTEM

Note: The information in this table is derived from the online documentation that Oracle provides at the Oracle Technology Network site: *www.otn.oracle.com*. To find the relevant information search on DBA_AUDIT.

Example of Auditing User Activities

- Steps:
  - Log on as SYSTEM or SYS, to issue an audit statement
  - Log on as DBSEC and create a temporary table
  - Go back to SYSTEM to view the contents of DBA_AUDIT_TRAIL

Audit Trail File Destination

- Steps:
  - Modify the initialization parameter file, INIT.ORA; set parameter AUDIT_TRAIL to the value OS
  - Create a folder/directory
  - Set AUDIT_FILE_DEST to the new directory
  - Shut down and restart the database
  - Connect as DBSEC

Oracle Alert Log

- Audits database activities:
  - Errors:
    - Errors related to physical structure are recorded in the Alert log
    - Monitor errors every five to ten minutes; can be done using a Windows or UNIX script
    - Syntactical errors are not recorded
  - Startup and shutdown
    - Date and time of each occurrence

Oracle Alert Log (continued)

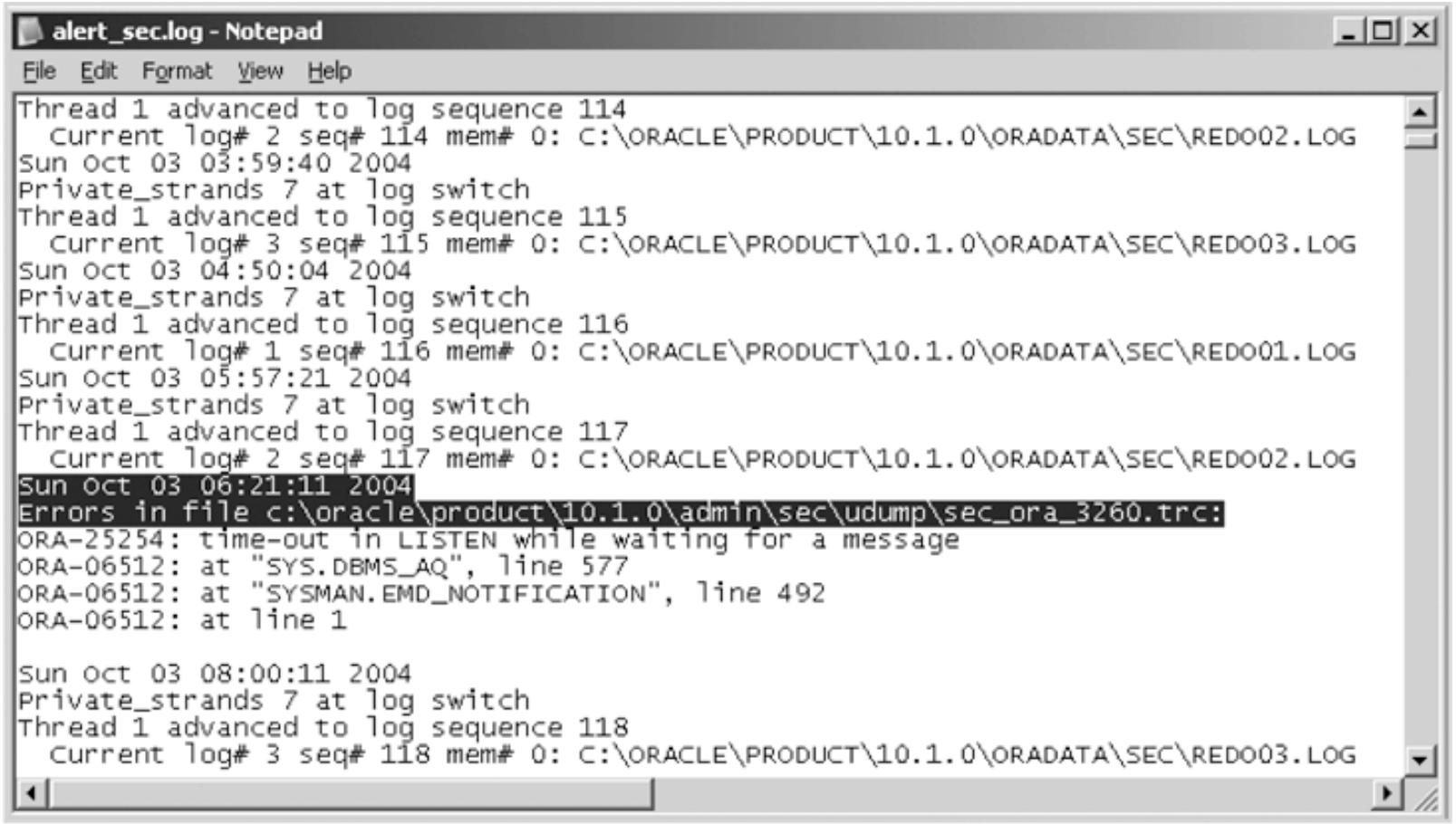

FIGURE 9-4 Sample contents of the Alert log file

Oracle Alert Log (continued)

- Database activities (continued):
  - Modified initialization parameters, each time a database is started
  - Checkpoints: configure Oracle to record checkpoint time
  - Archiving: view the timing for all redo log sequences, as well as archiving times
  - Physical database changes

Oracle Alert Log (continued)

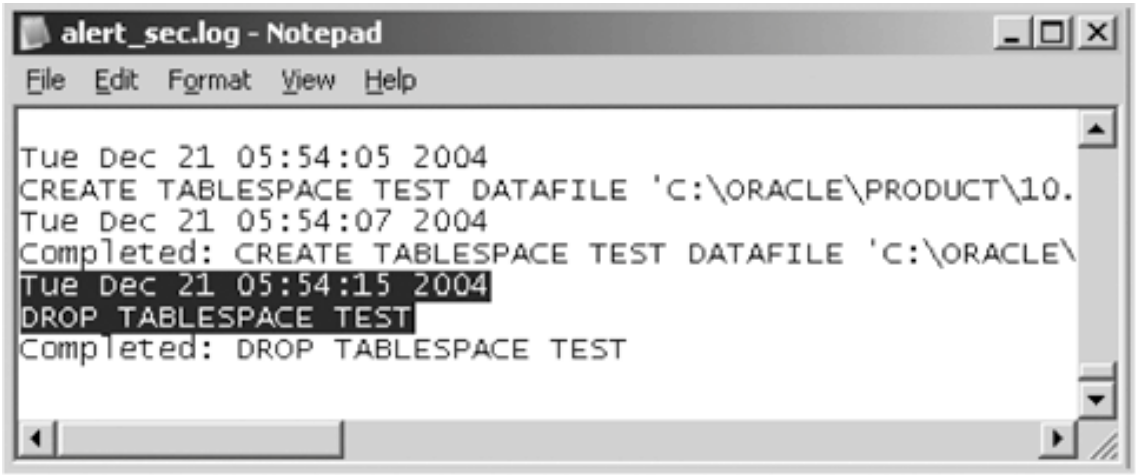

FIGURE 9-5 Alert log example showing an entry for tablespace changes

Auditing Server Activity with Microsoft SQL Server 2000

- Way to track and log activity for each SQL Server occurrence
- Must be a member of the sysadmin fixed server role
- Two types of auditing for server events:
  - Auditing
  - C2 auditing
- Auditing affects performance and can be costly

Implementing SQL Profiler

- User interface for auditing events
- For each event you can audit:
  - Date and time of the event
  - User who caused the event to occur
  - Type of event
  - Success or failure of the event
  - Origin of the request
  - Name of the object accessed
  - Text SQL statement

Implementing SQL Profiler (continued)

Table 9-2 SQL Server event descriptions

Event	Description
End user events	All SQL commands, LOGOUT/LOGIN, enabling of application roles
DBA events	DDL (other than security events), configuration (DB or server)
Security events	GRANT/REVOKE/DENY, LOGIN USER/ROLE ADD/REMOVE/CONFIGURE
Utility events	BACKUP/RESTORE/BULK INSERT/BCP/DBCC commands
Server events	SHUTDOWN, PAUSE, START
Audit events	ADD AUDIT, MODIFY AUDIT, STOP AUDIT

Security Auditing with SQL Server

- Steps for setting security auditing level:
  - Open Enterprise Manager
  - Expand the appropriate SQL Server group
  - Right-click on the desired server
  - Click Properties
  - On the security tab, select the desired security level

Security Auditing with SQL Server (continued)

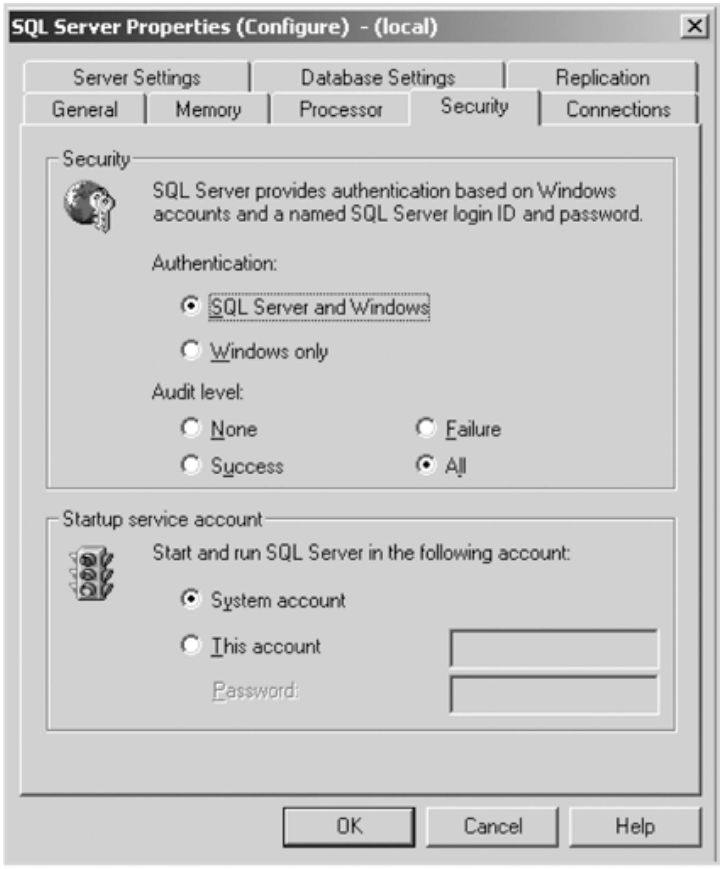

FIGURE 9-6 SQL Server configuration

Security Auditing with SQL Server (continued)

- Auditable events:
  - ADD DB USER
  - ADD LOGIN TO SERVER ROLE
  - ADD MEMBER TO DB ROLE
  - ADD ROLE
  - APP ROLE CHANGE PASSWORD
  - BACKUP/RESTORE
  - CHANGE AUDIT

Security Auditing with SQL Server (continued)

- Auditable events (continued):
  - DBCC
  - LOGIN
  - LOGOUT
  - LOGIN CHANGE PASSWORD
  - LOGIN CHANGE PROPERTY
  - LOGIN FAILED
  - Login GDR (GRANT, DENY, REVOKE)

Security Auditing with SQL Server (continued)

- Auditable events (continued):
  - Object Derived Permissions
  - Object GDR
  - Object Permissions
  - Server Start and Stop
  - Statement GDR
  - Statement Permission

Security Auditing with SQL Server (continued)

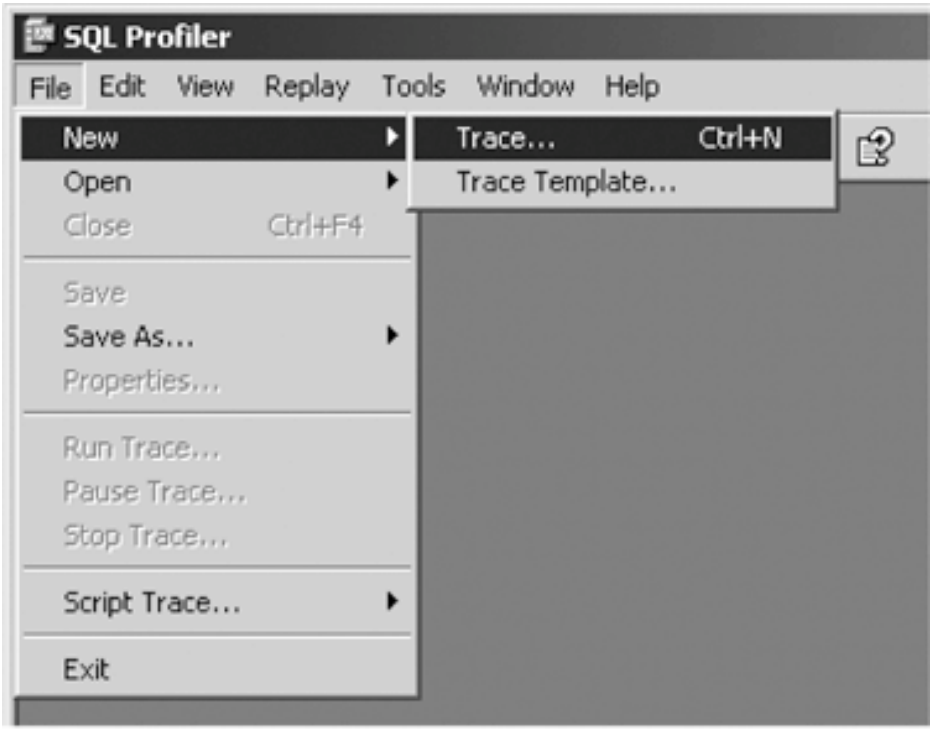

FIGURE 9-7 SQL Profiler main menu

Security Auditing with SQL Server (continued)

- New trace information:
  - A name for the trace
  - The server you want to audit
  - The base template to start with
  - Where to save the audit data, either to a file or to a database table
  - A stop time, if you don't want the trace to run indefinitely

Security Auditing with SQL Server (continued)

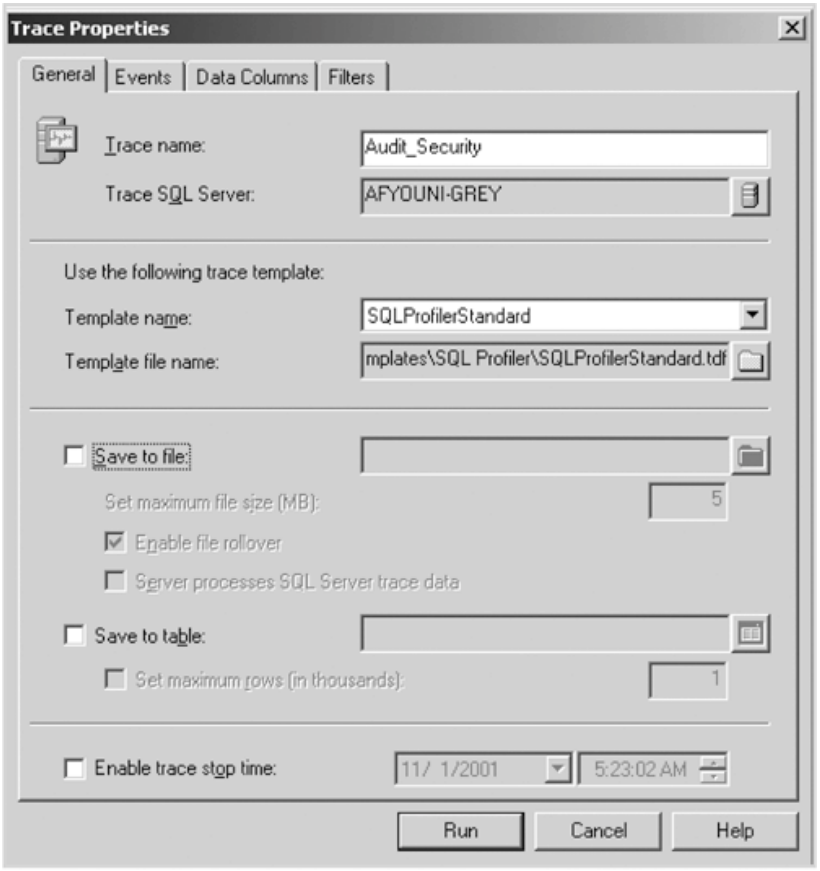

FIGURE 9-8 SQL Server Trace Properties dialog box

Security Auditing with SQL Server (continued)

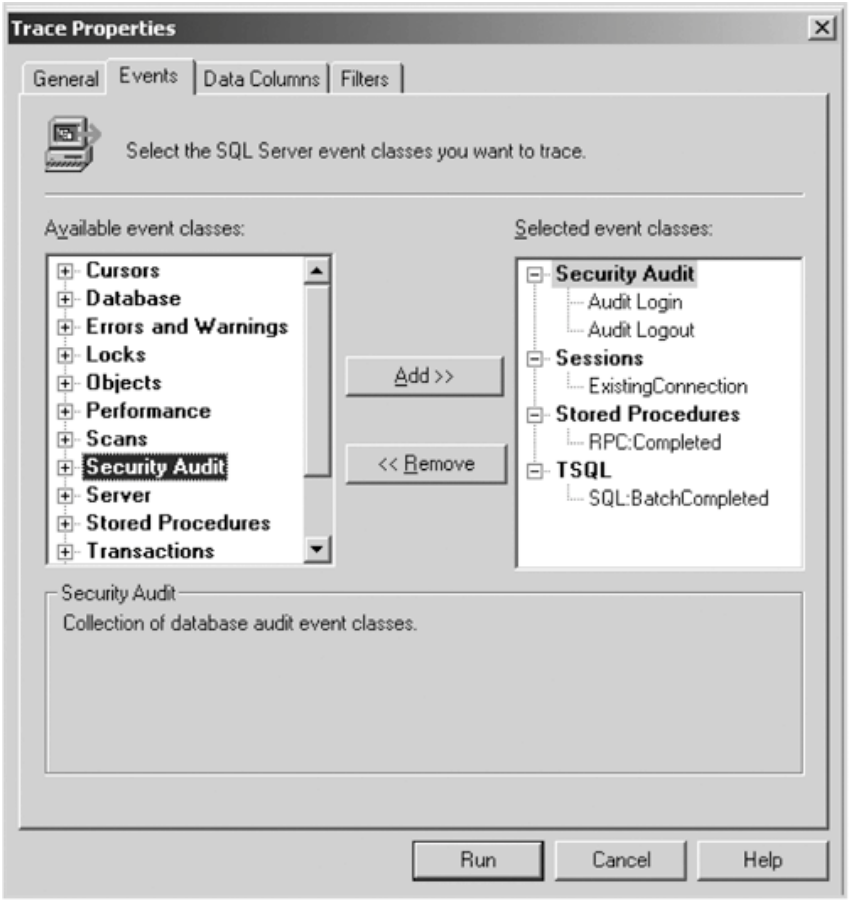

FIGURE 9-9 SQL Server trace configuration screen showing security audit selection

Security Auditing with SQL Server (continued)

- Steps to add Login Change Password event
  - Expand the Security Audit node under Available event classes
  - Click Audit Login Change Password Event
  - Click the Add button

Security Auditing with SQL Server (continued)

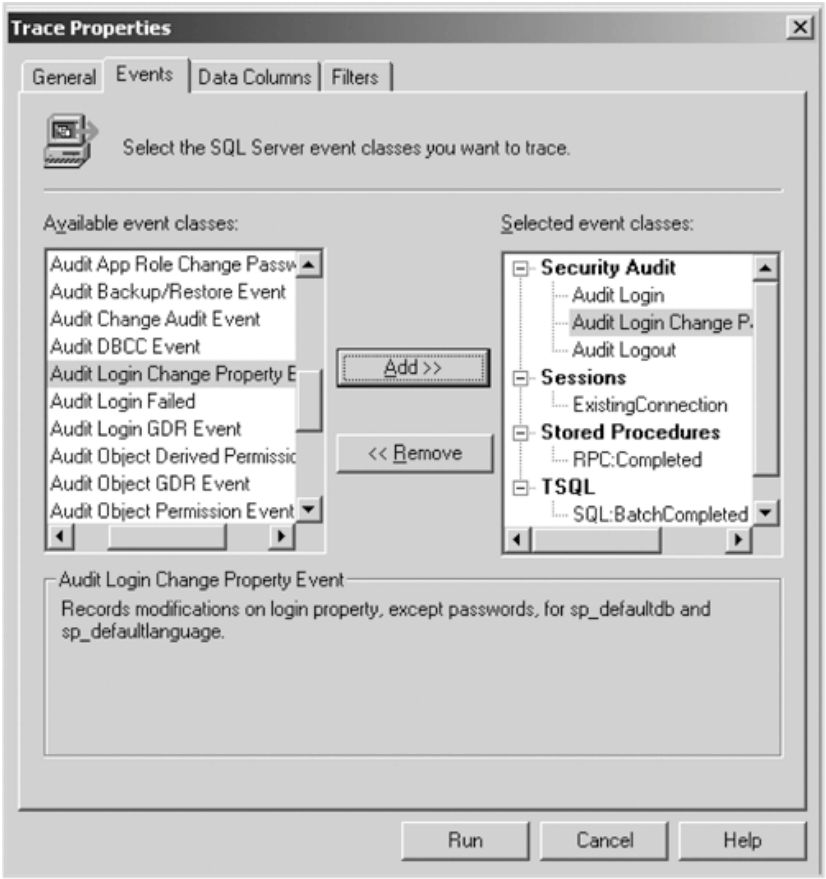

FIGURE 9-10 SQL Server trace configuration screen showing all available auditing options for security audit selection

Data Definition Auditing

- Audit DDL statements:
  - Object:Created
  - Object:Deleted
  - Will audit all CREATE and DROP statements

Data Definition Auditing (continued)

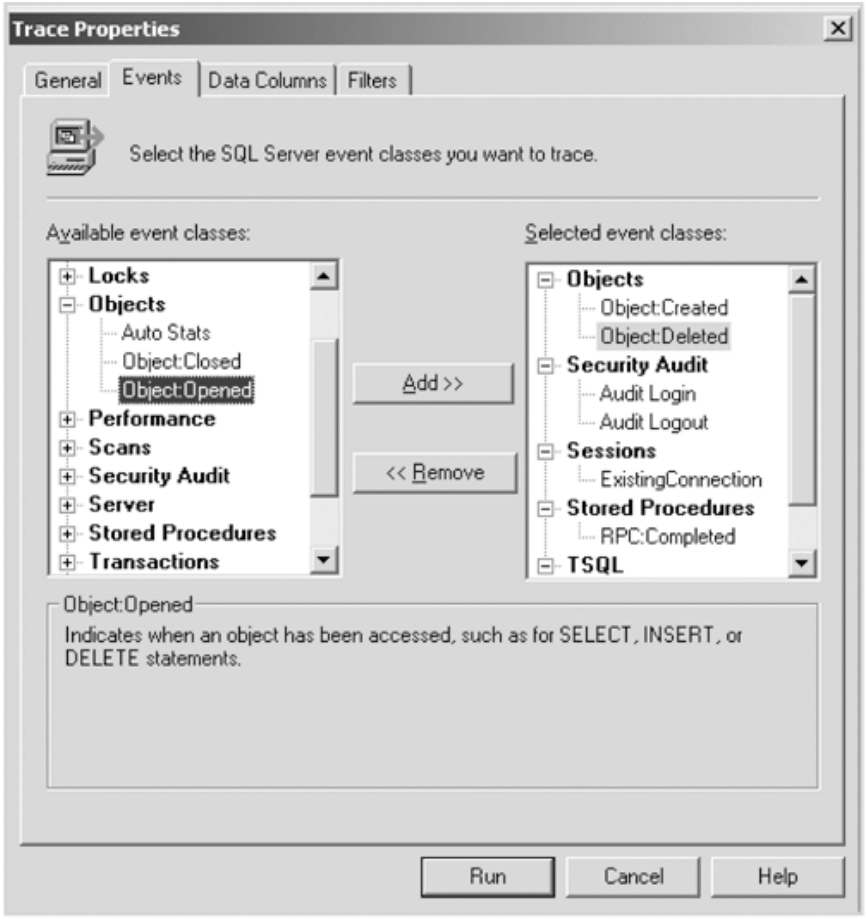

FIGURE 9-11 SQL Server trace configuration screen showing Object: Created by audit selection

Database Auditing with SQL Server

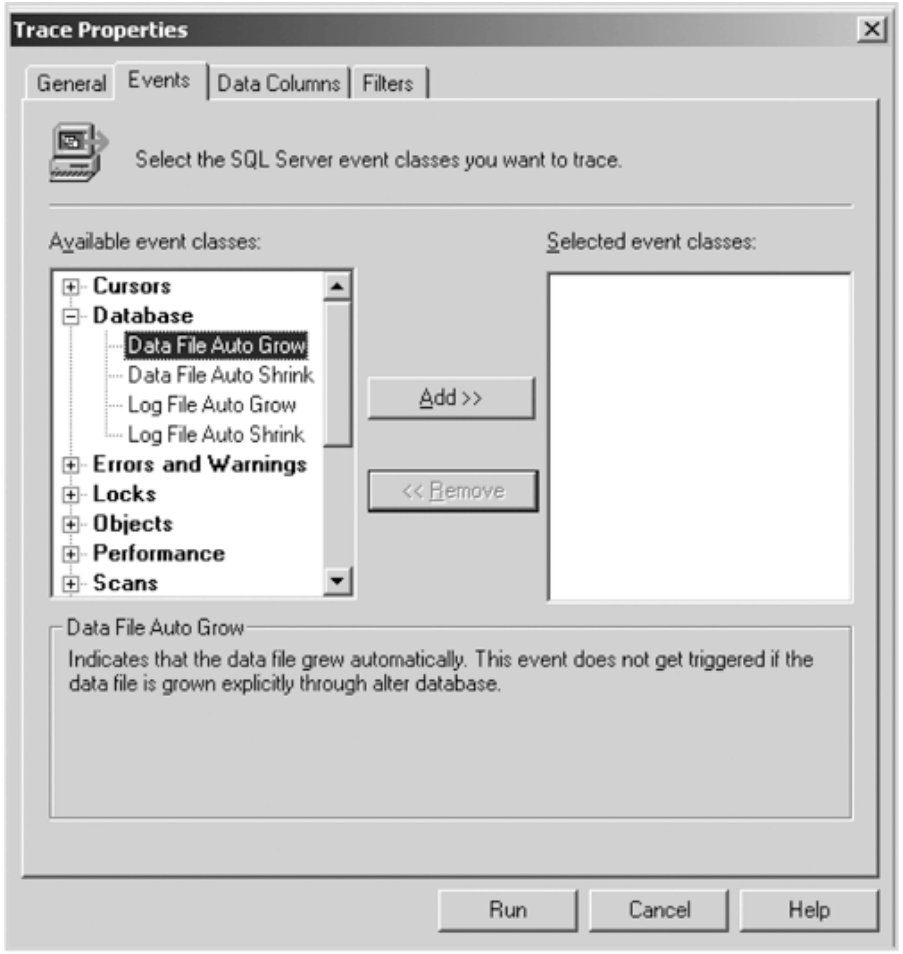

FIGURE 9-12 SQL Server trace configuration screen showing database audit selection

Database Errors Auditing with SQL Server

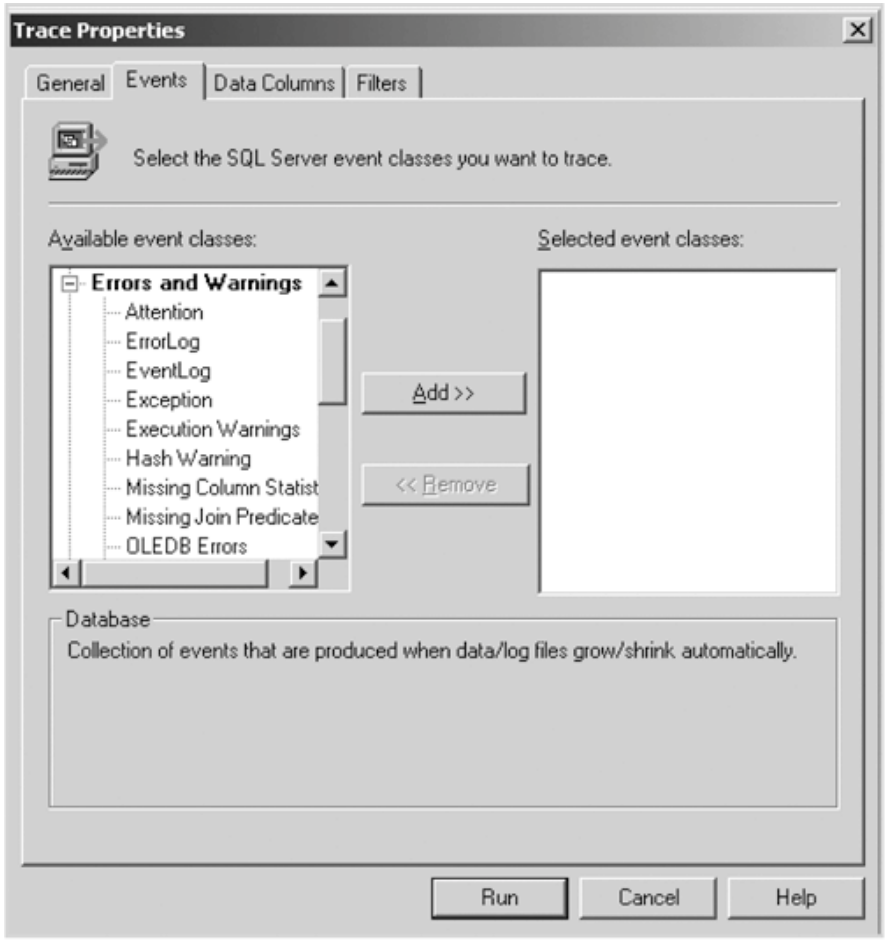

FIGURE 9-13 SQL Server trace configuration for adding events to be traced

Summary

- Activities types:
  - Application activities
  - Administration activities
  - Database events
- Oracle triggers provide a way to create an audit trail
- Auditable Oracle database activities: logon, logoff, startup and shutdown

Summary (continued)

- Oracle provides the SQL AUDIT command: initialization parameter AUDIT_TRAIL
- NOAUDIT used to stop auditing
- DBA_AUDIT_TRAIL data dictionary view
- Oracle Alert Log:
  - Database errors
  - Modified initialization parameters
  - Checkpoints

Summary (continued)

- Microsoft SQL Server 2000: way to track and log SQL Server activity
- Must be a member of sysadmin fixed role to enable or modify auditing
- SQL Profiler:
  - Visualization tool
  - Audit errors that occur within the database