Database Security and Auditing: Protecting Data Integrity and Accessibility

Administration of Users

Objectives

- Explain the importance of administration documentation
- Outline the concept of operating system authentication
- Create users and logins using both Oracle10*g* and SQL Server
- Remove a user from Oracle10*g* and SQL servers

Objectives (continued)

- Modify an existing user using both Oracle10*g* and SQL servers
- List all default users on Oracle10*g* and SQL servers
- Explain the concept of a remote user
- List the risks of database links

Objectives (continued)

- List the security risks of linked servers
- List the security risks of remote servers
- Describe best practices for user administration

Documentation of User Administration

- Part of the administration process
- Reasons to document:
  - Provide a paper trail
  - Ensure administration consistency
- What to document:
  - Administration policies, staff and management
  - Security procedures
  - Procedure implementation scripts or programs
  - Predefined roles description

Documentation of User Administration (continued)

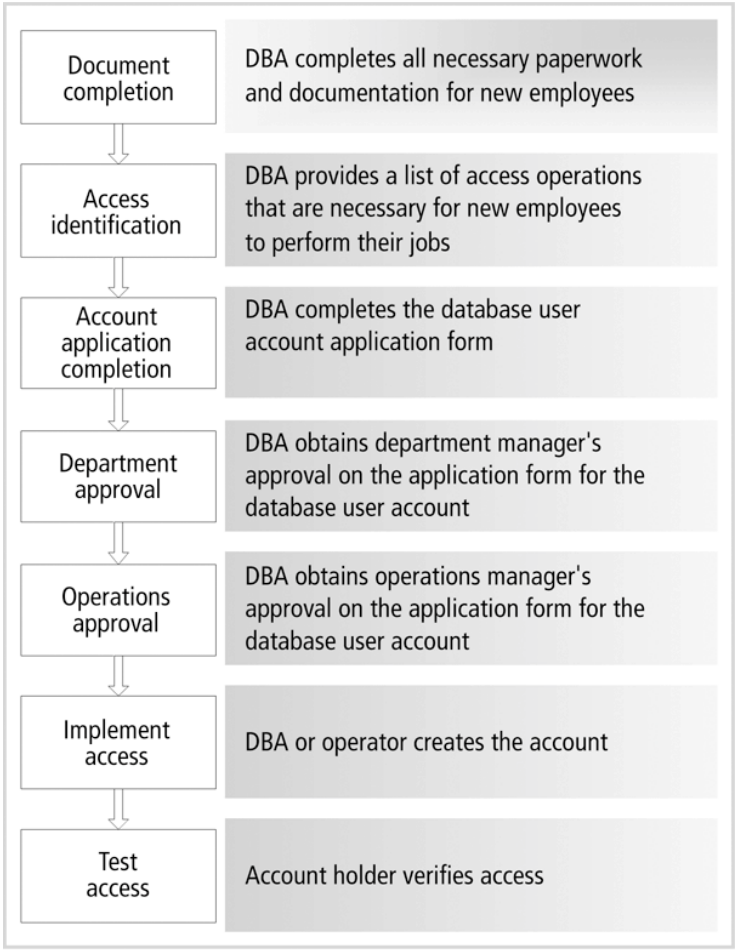

FIGURE 3-1 Database account access procedure

Documentation of User Administration (continued)

Acme Pharmaceutical Company
Database User Account Form

Requested For	
Name (First, MI, Last)	
Employee Type	☐ Employee ☐ Contractor ☐ Temporary ☐ Intern
Title	
Employee# (if available)	

Requested By			
Name (First, MI, Last)			
E-mail		Telephone Ext.	

Date			
Requested		Expected	

Action
☐ Add ☐ Modify ☐ Password Change ☐ Lock ☐ Unlock ☐ Remove

Location & Department	
Location	
Department	

Database Application

Database Role
☐ Operations Manager ☐ Business Manager ☐ Analyst ☐ Administrator ☐ Developer ☐ Operator ☐ Clerk ☐ QA ☐ Other:

Reason for the request

Approved by	
Requester Manager:	
Operation Manager:	

Comments

Completed by			
Administrator		Date	

FIGURE 3-2 Database user account application form

Operating System Authentication

- Many databases (including Microsoft SQL Server 2000) depend on OS to authenticate users
- Reasons:
  - Once an intruder is inside the OS, it is easier to access the database
  - Centralize administration of users
- Users must be authenticated at each level

Operating System Authentication (continued)

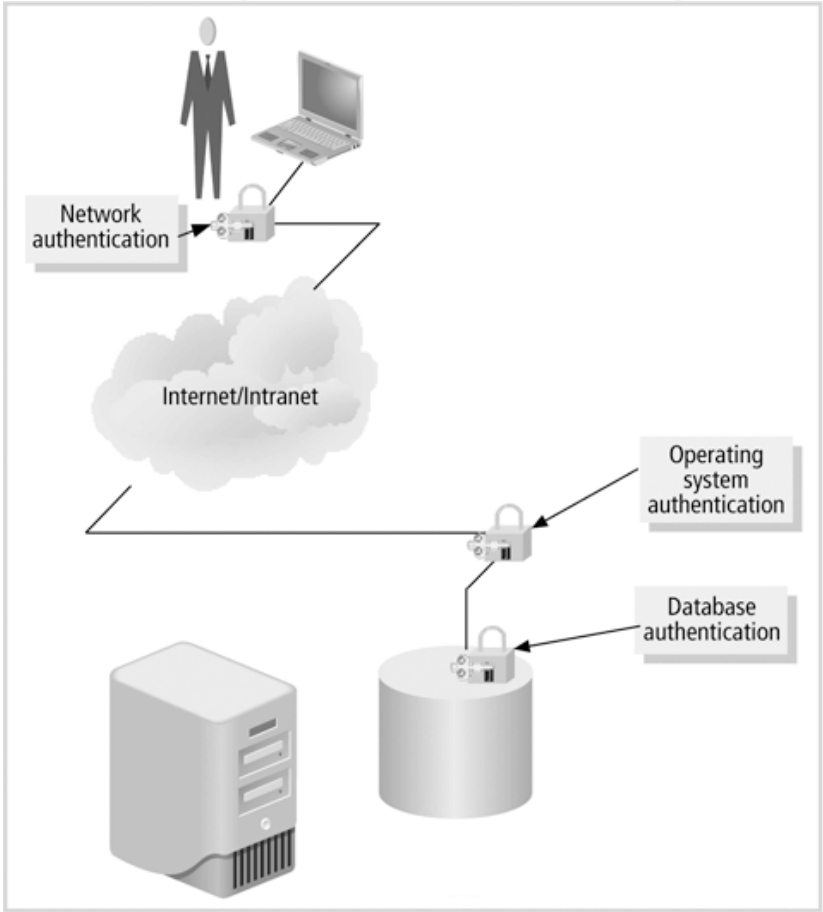

FIGURE 3-3 Ideal authentication levels for database applications

Creating Users

- Must be a standardized, well-documented, and securely managed process
- In Oracle10*g*, use the CREATE USER statement:
  - Part of the a Data Definition Language (DDL)
  - Account can own different objects

Creating an Oracle10*g* User

- IDENTIFIED clause
  - Tells Oracle how to authenticate a user account
  - BY PASSWORD option: encrypts and stores an assigned password in the database
  - EXTERNALLY option: user is authenticated by the OS
  - GLOBALLY AS option: depends on authentication through centralized user management method

Creating an Oracle10*g* User (continued)

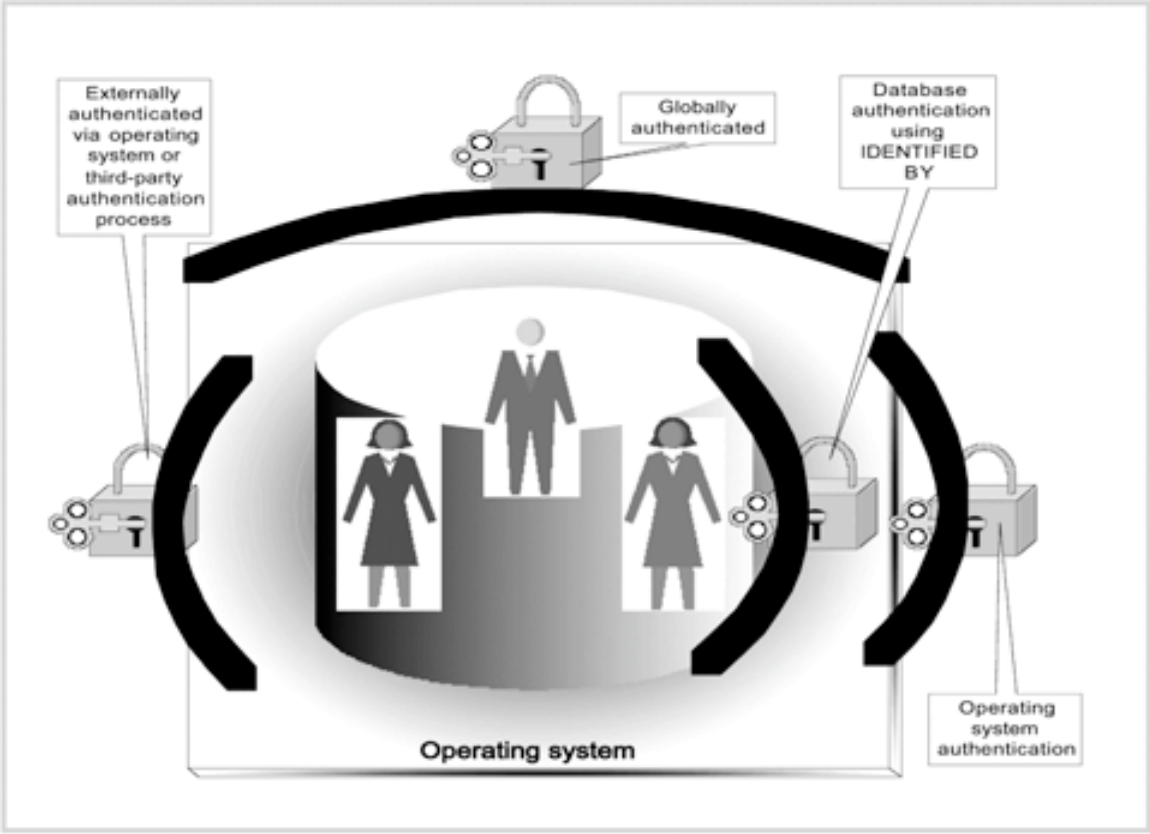

FIGURE 3-4 Architecture of Oracle authentication methods

Creating an Oracle10*g* User (continued)

- DEFAULT TABLESPACE clause: specifies default storage for the user
- TEMPORARY TABLESPACE clause
- QUOTA clause: tells Oracle 10*g* how much storage space a user is allowed for a specified tablespace
- PROFILE clause: indicates the profile used for limiting database resources and enforcing password policies

Creating an Oracle10*g* User (continued)

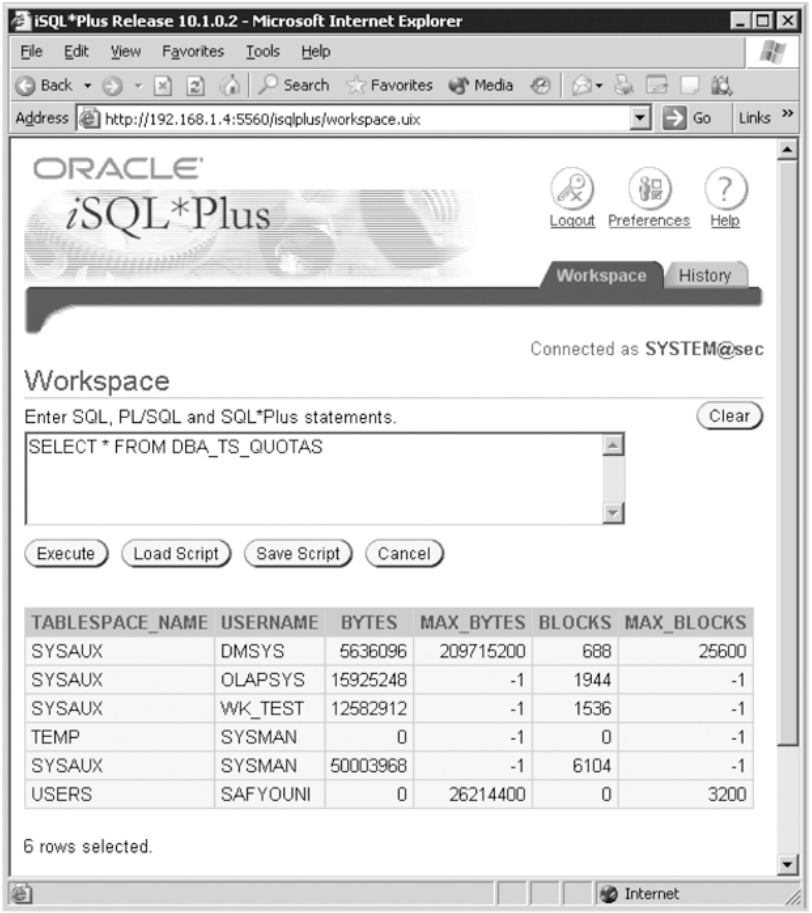

FIGURE 3-5 Contents of data dictionary view DBA_TS_QUOTAS

Creating an Oracle10*g* User (continued)

- PASSWORD EXPIRE clause: tells Oracle to expire the user password and prompts the user to enter a new password
- ACCOUNT clause: enable or disable account
- ALTER USER: modifies a user account
- Oracle Enterprise Manager: GUI administration tool

Creating an Oracle10*g* User (continued)

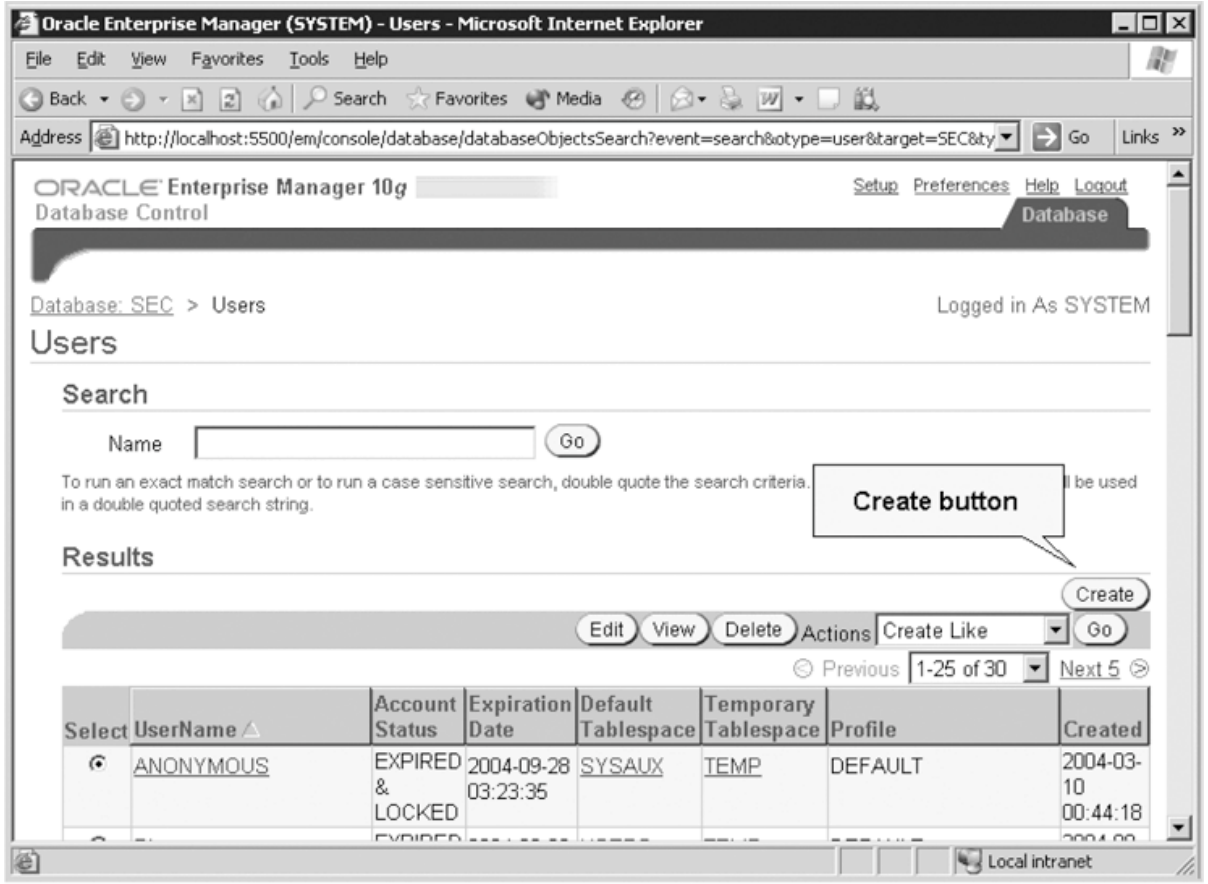

FIGURE 3-7 Oracle Enterprise Manager Console showing the Create Objects button

Creating an Oracle10*g* User (continued)

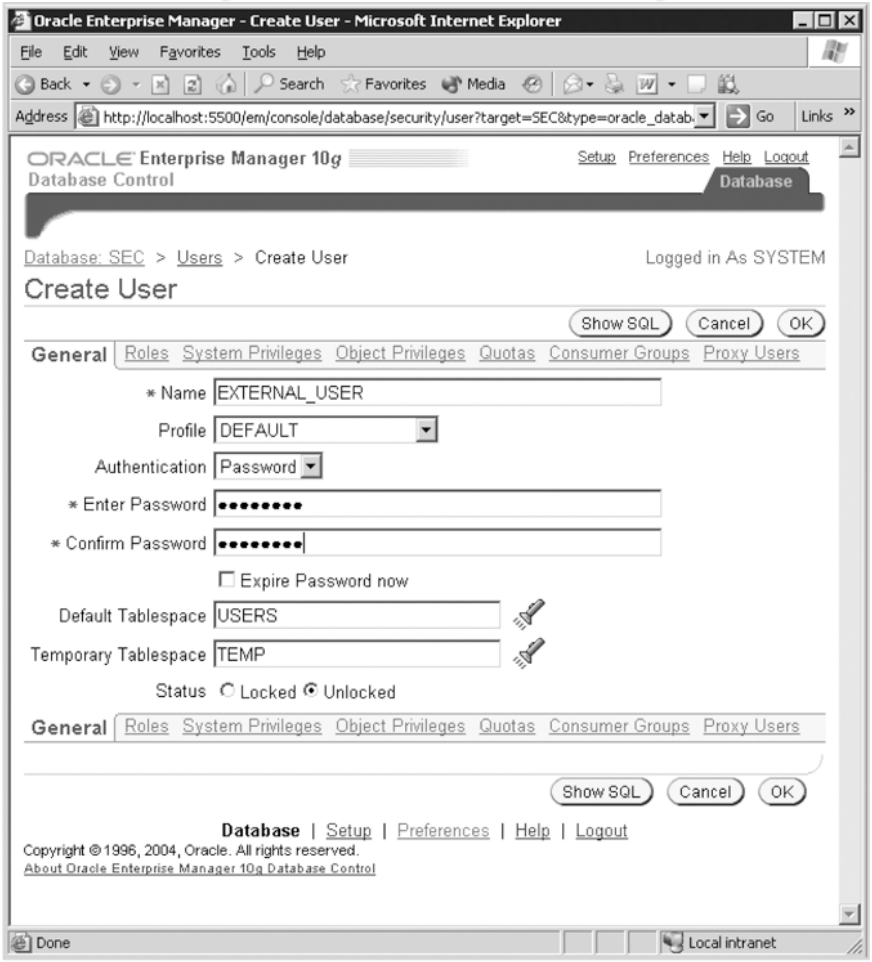

FIGURE 3-8 Creating a new user

Creating an Oracle10*g* User Using External (Operating System) Authentication

- Depends on an external party to authenticate the user
- Steps:
  - Verify account belongs to ORA_DBA group
  - Set the Windows registry string OSAUTH_PREFIX_DOMAIN to FALSE
  - View setting of the OS_AUTHENT_PREFIX initialization parameter
  - Change OS_AUTHENT_PREFIX to NULL

Creating an Oracle10*g* User Using External (Operating System) Authentication (continued)

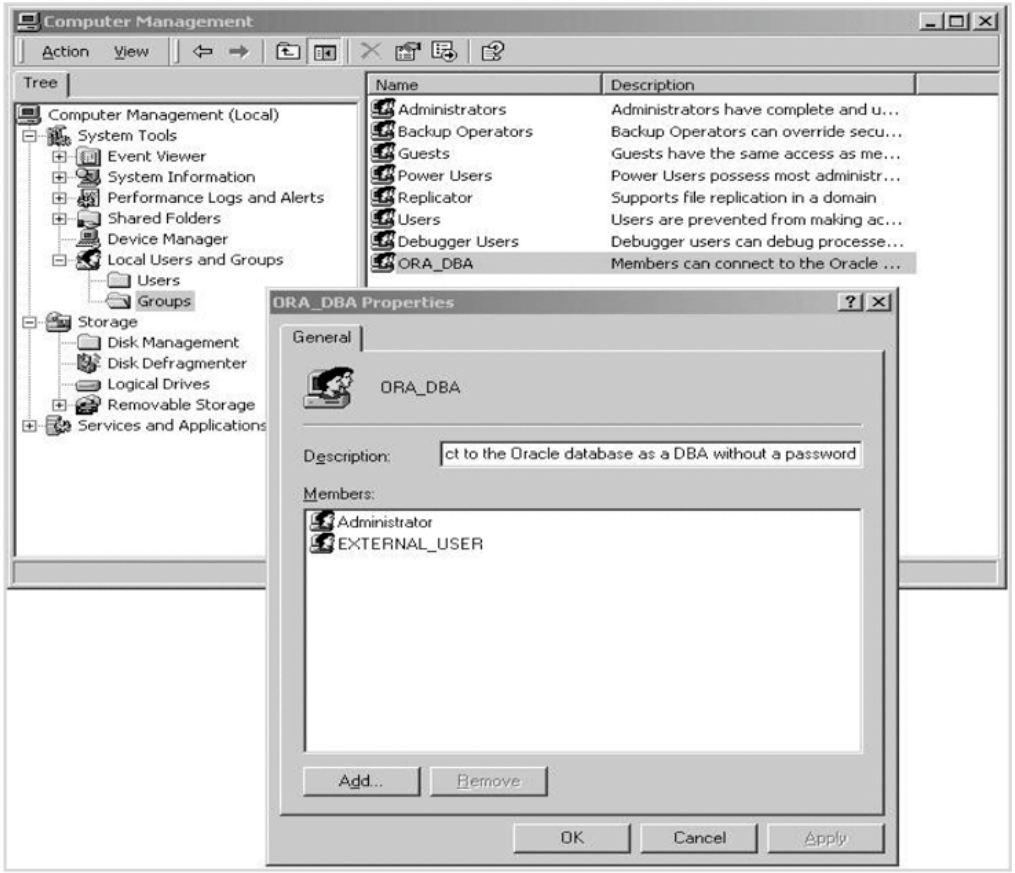

FIGURE 3-11 Computer management tool showing the ORA_DBA group properties

Creating an Oracle10*g* User Using External (Operating System) Authentication (continued)

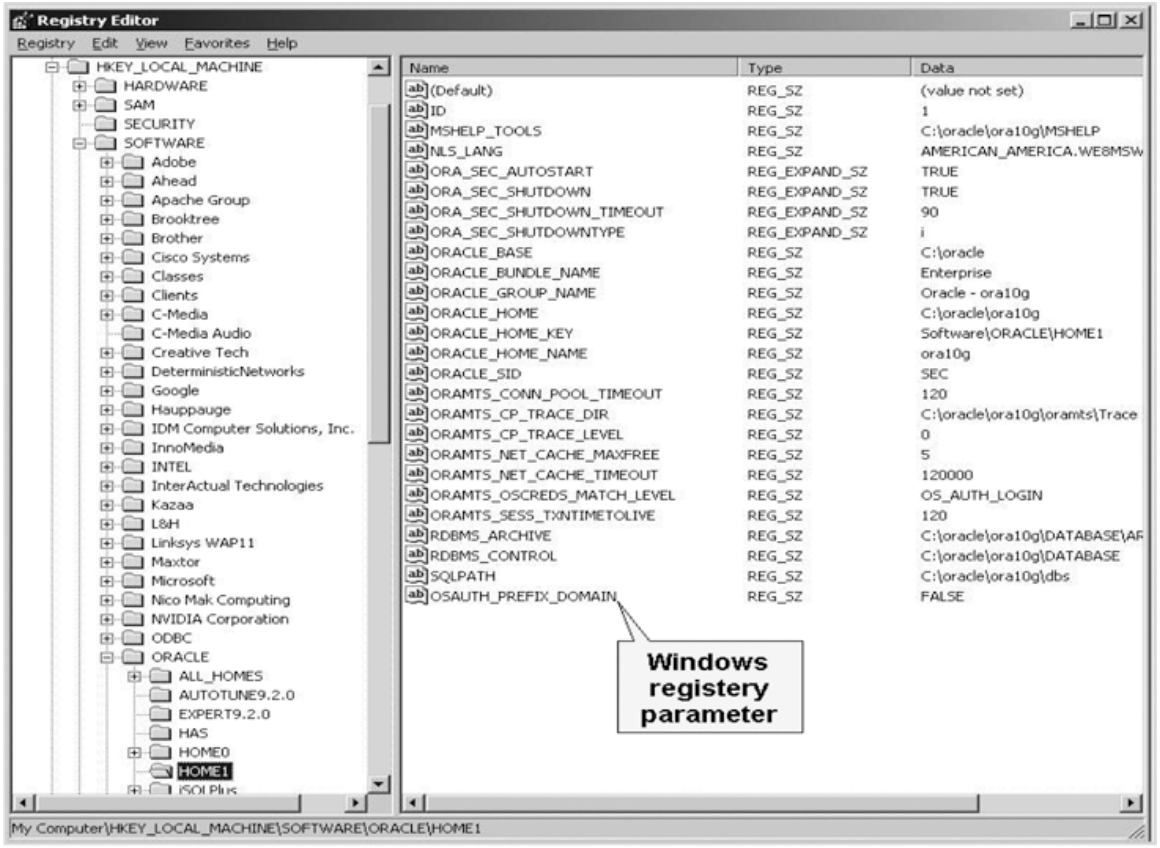

FIGURE 3-12 Windows registry showing the OSAUTH_PREFIX_DOMAIN parameter

Creating an Oracle10*g* User Using External (Operating System) Authentication (continued)

- Steps (continued):
  - Create an Oracle user
  - Provide new user with CREATE SESSION privilege
- Advantage: allows administrators to use one generic user to run maintenance scripts without a password

Creating an Oracle User Using Global Authentication

- Enterprise-level authentication solution
- Use the CREATE USER statement
- DBA_USERS view: contains information about all accounts

Creating an Oracle User Using Global Authentication (continued)

Table 3-1 Columns of DBA_USERS view

Column Name	Description
USERNAME	Name of the database user; name is used to log on to the database; Oracle10*g* does not allow duplicate values of this column
USER_ID	Unique identification number to identify a user; this column is not used as frequently as USERNAME; used most commonly for auditing
PASSWORD	Keeps encrypted password for a database-authenticated user; use EXTERNAL for externally authenticated users and GLOBAL for globally authenticated users
ACCOUNT_STATUS	Indicates whether the user account is EXPIRED, LOCKED, EXPIRED and LOCKED, or OPEN

Creating an Oracle User Using Global Authentication (continued)

Table 3-1 Columns of DBA_USERS view (continued)

Column Name	Description
LOCK_DATE	Date and time the account was locked
EXPIRY_DATE	Date and time the account password expired
DEFAULT_TABLESPACE	Name of the tablespace assigned to this user account
TEMPORARY_TABLESPACE	Name of the temporary tablespace assigned to this user account
CREATED	Date and time this user account was created
PROFILE	Name of the profile assigned to this user account (for more details on profiles see Chapter 4)
INITIAL_RSRC_CONSUMER_GROUP	Name of the resources group to which this account belongs
EXTERNAL_NAME	External name for a GLOBAL authenticated user

Creating a SQL Server User

- Create a login ID first; controls access to SQL Server system
- Associate login ID with a database user
- Must be member of fixed server roles (SYSADMIN or SECURITYADMIN)
- Two types of login IDs:
  - Windows Integrated (trusted) login
  - SQL Server login

Creating Windows Integrated Logins

- Command line:
  - SP_GRANTLOGIN system stored procedure
  - Can be associated local, domain, group usernames
- Enterprise Manager:
  - Use the Security container
  - Logins -> New Login

Creating Windows Integrated Logins (continued)

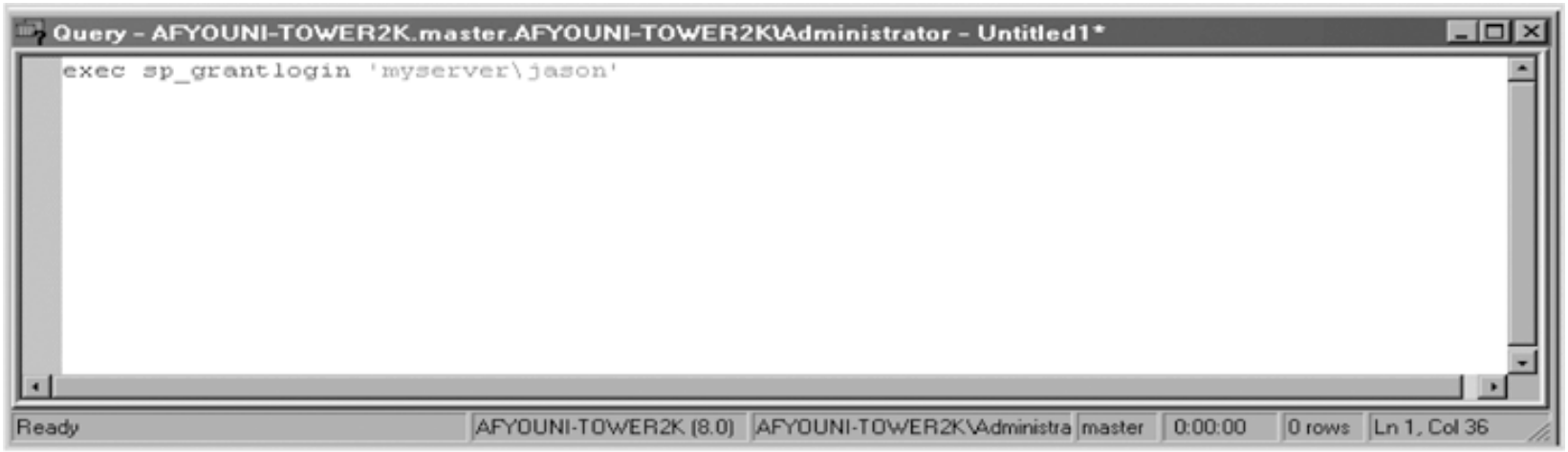

FIGURE 3-14 Microsoft SQL Server 2000 Query Analyzer tool used as a command line interface

Creating Windows Integrated Logins (continued)

FIGURE 3-16 SQL Server Enterprise Manager showing action menu

Creating Windows Integrated Logins (continued)

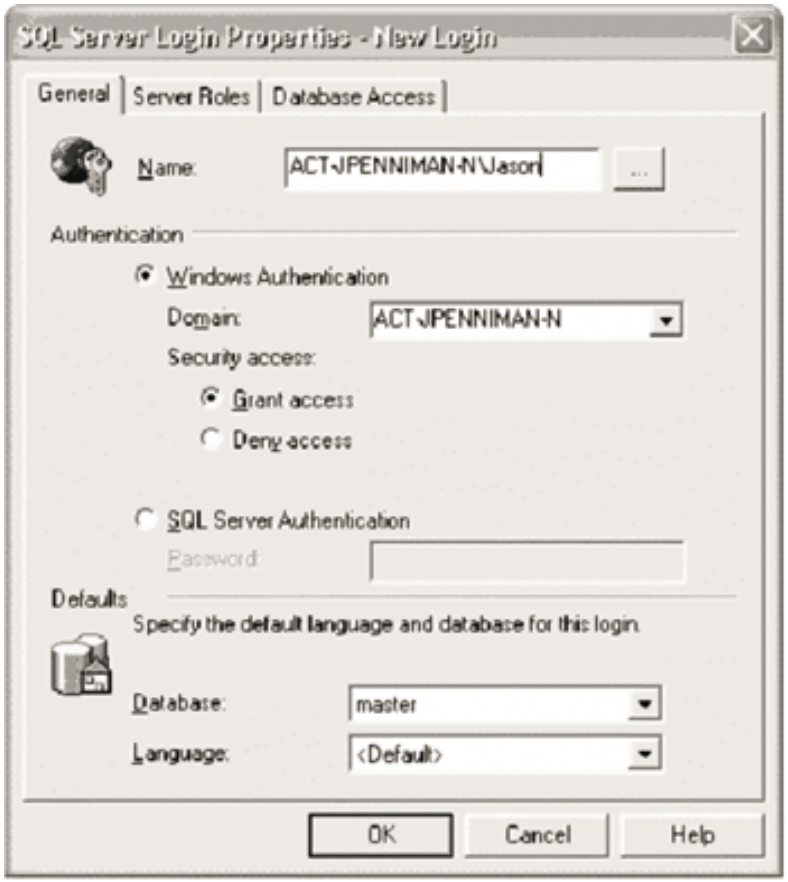

FIGURE 3-17 SQL Server login properties

Creating SQL Server Logins

- Command line:
  - SP_ADDLOGIN system stored procedure
  - Password is encrypted by default
  - Specify a default database
- Enterprise Manager:
  - Security container
  - Logins -> New Login
  - SQL Server Authentication option

Creating SQL Server Logins (continued)

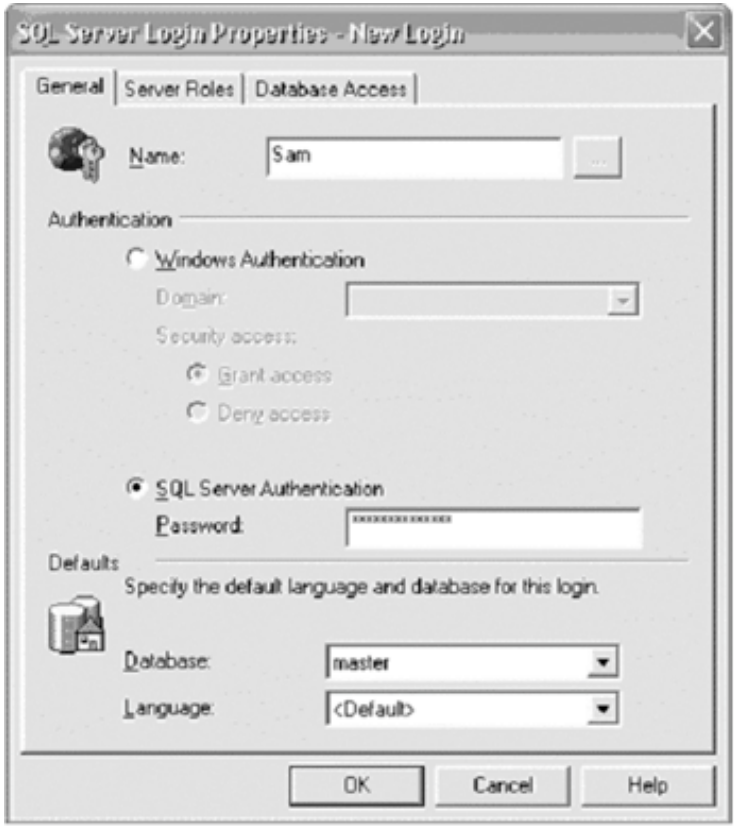

FIGURE 3-18 Server login properties—new login screen

Removing Users

- Simple process
- Make a backup first
- Obtain a written request (for auditing purposes)

Removing an Oracle User

- DROP command
- CASCADE option: when user owns database objects
- Recommendations:
  - Backup the account for one to three months
  - Listing all owned objects
  - Lock the account or revoke the CREATE SESSION privilege

SQL Server: Removing Windows Integrated Logins

- Command line: SP_DENYLOGIN system stored procedure
- Enterprise Manager:
  - Highlight the desired login
  - Choose Delete from the Action menu

Modifying Users

- Modifications involve:
  - Changing passwords
  - Locking an account
  - Increasing a storage quota
- ALTER USER DDL statement

Modifying an Oracle User

- ALTER USER statement
- Oracle Enterprise Manager: graphical tool

Modifying an Oracle User (continued)

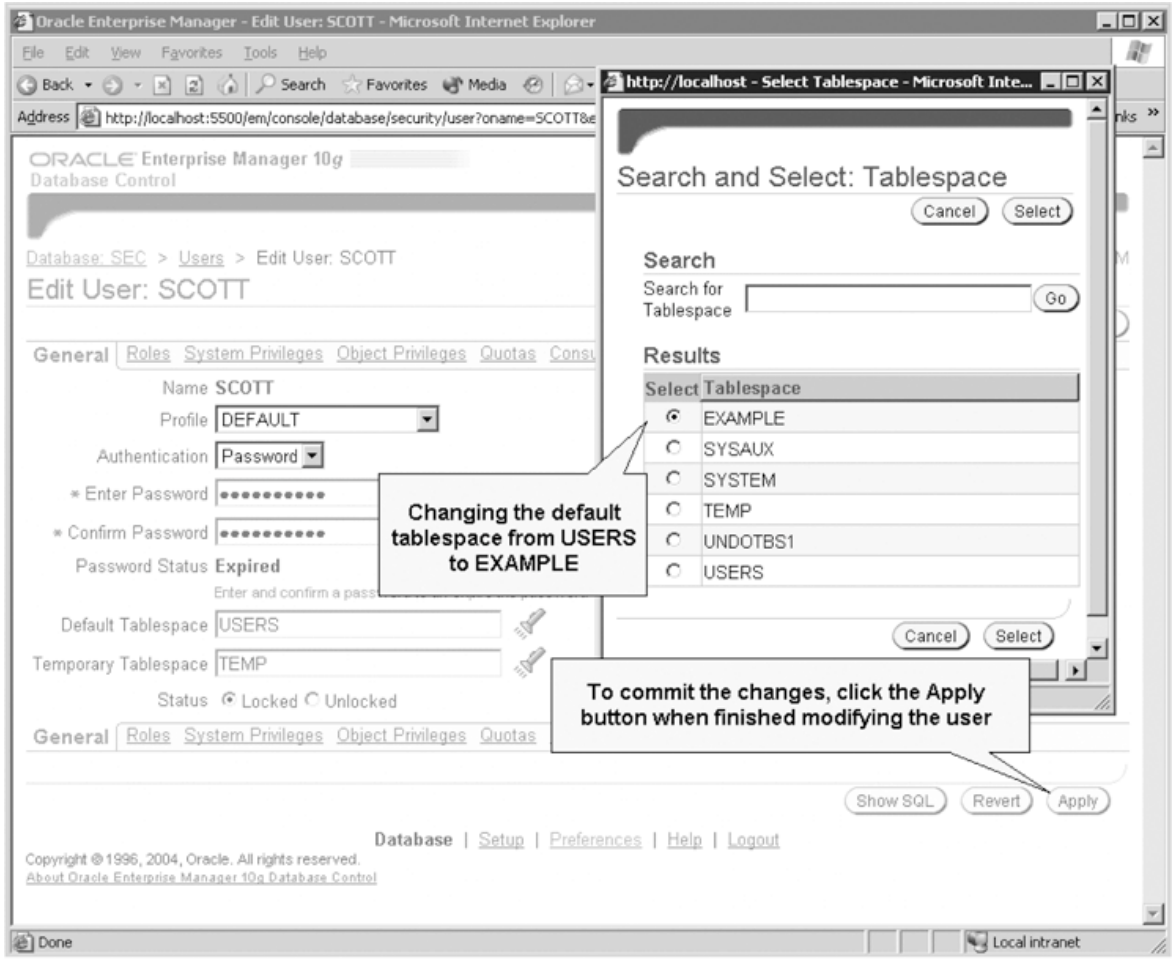

FIGURE 3-20 Illustration of modifying an existing Oracle user account

SQL Server: Modifying Windows Integrated Login Attributes

- Command line:
  - SP_DEFAULTDB system stored procedure
  - SP_DEFAULTLANGUAGE stored procedure
- Enterprise Manager:
  - Expand the security container
  - Select desired login
  - Properties (on the Action Menu)

Default Users

- Oracle default users:
  - SYS, owner of the data dictionary
  - SYSTEM, performs almost all database tasks
  - ORAPWD, creates a password file
- SQL Server default users:
  - SA, system administrator
  - BUILT_IN\Administrators

Remote Users

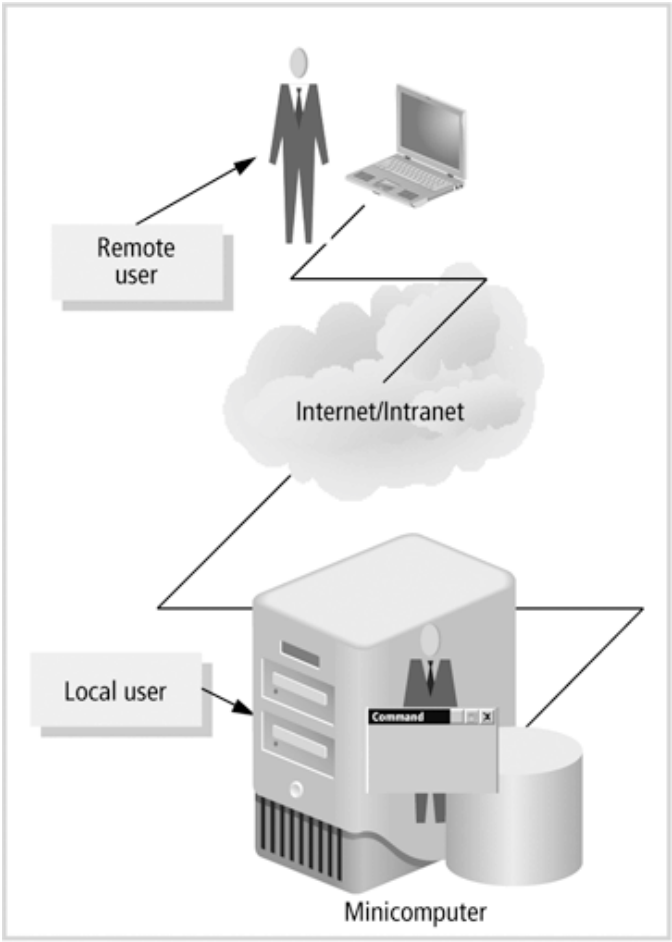

FIGURE 3-22 Local and remote users

Database Links

- Connection from one database to another: allow DDL and SQL statements
- Types: PUBLIC and PRIVATE
- Authentication Methods:
  - CURRENT USER
  - FIXED USER
  - CONNECT USER

Database Links (continued)

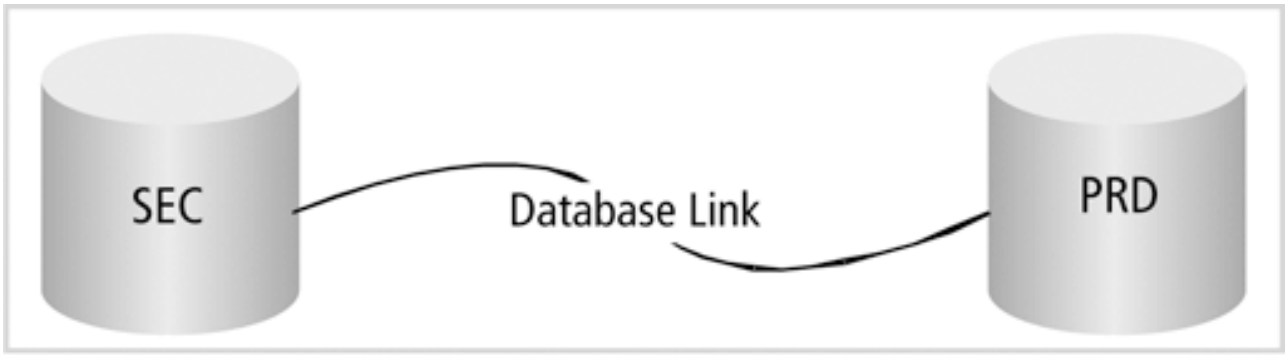

FIGURE 3-23 Database link architecture

Linked Servers

- Allow you to connect to almost any:
  - Object Linking and Embedding Database (OLEDB)
  - Open Database Connectivity (ODBC)
- OPENQUERY function
- Map logins in your SQL Server instance to users in the linked database
- Remote servers: allow communication using RPC

Linked Servers (continued)

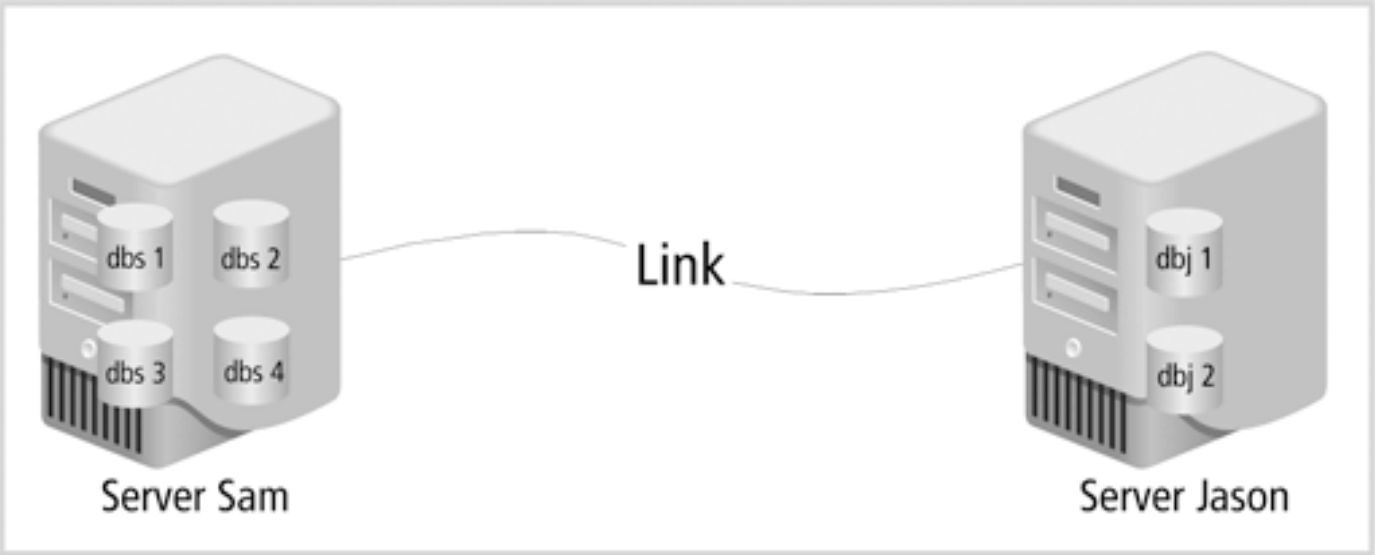

FIGURE 3-24 Linked servers architecture using SQL Server

Practices for Administrators and Managers

- Manage:
  - Accounts
  - Data files
  - Memory
- Administrative tasks:
  - Backup
  - Recovery
  - Performance tuning

Best Practices

- Follow company's policies and procedures
- Always document and create logs
- Educate users
- Keep abreast of database and security technology
- Review and modify procedures

Best Practices (continued)

- For SQL server:
  - Mimic Oracle's recommended installation for UNIX
  - Use local Windows or domain Windows accounts
- Block direct access to database tables
- Limit and restrict access to the server
- Use strong passwords
- Patches, patches, patches

Summary

- Document tasks and procedures for auditing purposes
- Creating users:
  - CREATE USER statement in Oracle
  - Login ID in SQL Server
- Removing users:
  - SQL DROP statement
  - SP_DENYLOGIN Windows system stored procedure

Summary (continued)

- Modifying user attributes: ALTER USER DDL statement
- Local database and users
- Remote users
- Database links
- Linked servers