

Index

Symbols

"all permissions", [A-3](#)

Numerics

12C password hash version
about, [3-34](#)
12C password version
recommended by Oracle, [3-34](#)

A

about, [6-2](#), [9-22](#), [B-4](#), [B-5](#)
about connection, [6-6](#)
ACCEPT_MD5_CERTS sqlnet.ora parameter,
[B-21](#)
ACCEPT_SHA1_CERTS sqlnet.ora parameter,
[B-21](#)
access configuration, DBCA, [6-20](#)
access configuration, silent mode, [6-22](#)
access configuration, system parameters, [6-19](#)
access control
encryption, about manual, [18-1](#)
encryption, problems not solved by, [18-2](#)
enforcing, [A-15](#)
object privileges, [4-72](#)
password encryption, [3-3](#)
access control list (ACL), [10-2](#), [10-4](#)
examples
external network connection for email
alert, [31-12](#)
external network connections, [10-14](#)
wallet access, [10-14](#)
external network services
about, [10-2](#)
advantages, [10-2](#)
affect of upgrade from earlier release,
[10-3](#)
email alert for audit violation tutorial,
[31-12](#)
finding information about, [10-23](#)
network hosts, using wildcards to specify,
[10-18](#)
ORA-06512 error, [10-22](#)
ORA-24247 error, [10-22](#)

access control list (ACL) (*continued*)
external network services (*continued*)
ORA-24247 errors, [10-3](#)
order of precedence, hosts, [10-18](#)
port ranges, [10-19](#)
privilege assignments, about, [10-20](#)
privilege assignments, database
administrators checking, [10-20](#)
privilege assignments, users checking,
[10-21](#)
revoking privileges, [10-7](#)
wallet access
about, [10-3](#)
advantages, [10-3](#)
client certificate credentials, using, [10-8](#)
finding information about, [10-23](#)
non-shared wallets, [10-8](#)
password credentials, [10-8](#)
password credentials, using, [10-8](#)
revoking, [10-13](#)
revoking access, [10-13](#)
shared database session, [10-8](#)
wallets with sensitive information, [10-8](#)
wallets without sensitive information, [10-8](#)
account locking
example, [3-11](#)
explicit, [3-11](#)
password management, [3-10](#)
PASSWORD_LOCK_TIME profile parameter,
[3-10](#)
accounting, RADIUS, [26-17](#)
activating checksumming and encryption, [20-8](#)
ad hoc tools
database access, security problems of, [4-56](#)
adapters, [22-6](#)
ADG_ACCOUNT_INFO_TRACKING initialization
parameter
guideline for securing, [A-15](#)
ADM_PARALLEL_EXECUTE_TASK role
about, [4-40](#)
ADMIN OPTION
about, [4-93](#)
revoking privileges, [4-98](#)
revoking roles, [4-98](#)
roles, [4-55](#)
system privileges, [4-19](#)

- ADMINISTER FINE GRAINED AUDIT POLICY
 - system privilege, [4-26](#)
- ADMINISTER REDACTION POLICY system
 - privilege, [4-26](#)
- ADMINISTER ROW LEVEL SECURITY POLICY
 - system privilege, [4-26](#)
- administrative accounts
 - about, [2-39](#)
 - predefined, listed, [2-39](#)
- administrative privileges
 - about, [4-13](#)
 - granting to users, [4-13](#)
 - SYSBACKUP privilege, [4-14](#)
 - SYSDBA privilege, [4-13](#)
 - SYSDBG privilege, [4-16](#)
 - SYSKM privilege, [4-17](#)
 - SYSOPER privilege, [4-13](#)
 - SYSRAC privilege, [4-17](#)
- administrative user passwords
 - default, importance of changing, [A-7](#)
- administrative users
 - auditing, [30-9](#)
 - last successful login time, [3-49](#)
 - locked or expired accounts, [3-49](#)
 - mandatorily audited, [29-3](#)
 - password complexity verification functions, [3-51](#)
 - password files, managing, [3-49](#)
 - password files, multitenant environment, [3-51](#)
 - password management, [3-49](#)
 - password profile limits, [3-49](#)
- administrator privileges
 - access, [A-15](#)
 - operating system authentication, [3-55](#)
 - passwords, [3-55](#), [A-7](#)
 - SYSDBA and SYSOPER access, centrally controlling, [3-52](#)
 - write, on listener.ora file, [A-15](#)
- Advanced Encryption Standard (AES)
 - about, [20-2](#)
- Advanced Networking Option (ANO) (Oracle native encryption), [20-15](#)
- AES256 algorithm
 - converting to in Oracle wallets, [B-13](#)
- alerts, used in fine-grained audit policy, [31-12](#)
- algorithms
 - weaker keys, [C-12](#)
- ALTER ANY LIBRARY statement
 - security guidelines, [A-3](#)
- ALTER DATABASE DICTIONARY DELETE CREDENTIALS statement, [12-20](#)
- ALTER DATABASE DICTIONARY ENCRYPT CREDENTIALS statement, [12-20](#)
- ALTER DATABASE DICTIONARY REKEY CREDENTIALS statement, [12-20](#)
- ALTER PROCEDURE statement
 - used for compiling procedures, [4-85](#)
- ALTER PROFILE statement
 - altering profile limits with, [3-8](#)
 - password management, [3-5](#)
- ALTER RESOURCE COST statement, [2-29](#)
- ALTER ROLE statement
 - changing authorization method, [4-51](#)
- ALTER SESSION statement
 - schema, setting current, [12-26](#)
- ALTER USER privilege, [2-18](#)
- ALTER USER statement
 - changing SYS password with, [2-21](#)
 - default roles, [4-107](#)
 - explicit account unlocking, [3-11](#)
 - profiles, changing, [3-13](#)
 - REVOKE CONNECT THROUGH clause, [3-76](#)
- altering users, [2-18](#)
- ANO encryption
 - configuring with SSL authentication, [20-15](#)
- ANONYMOUS user account, [2-39](#)
- ANSI operations
 - Oracle Virtual Private Database affect on, [14-45](#)
- ANY system privilege
 - guidelines for security, [A-11](#)
- application common users
 - about, [2-3](#)
- application containers
 - application contexts, [13-3](#)
 - Virtual Private Database policies, [14-5](#)
- application contexts, [13-6](#), [13-28](#), [13-52](#)
 - about, [13-2](#)
 - application containers, [13-3](#)
 - as secure data cache, [13-3](#)
 - benefits of using, [13-3](#)
 - bind variables, [14-4](#)
 - components, [13-2](#)
 - creating session based, [13-8](#)
 - DBMS_SESSION.SET_CONTEXT procedure, [13-13](#)
 - driving context, [13-54](#)
 - editions, affect on, [13-3](#)
 - finding errors by checking trace files, [13-54](#)
 - finding information about, [13-54](#)
 - global application contexts
 - authenticating user for multiple applications, [13-35](#)
 - creating, [13-30](#)
 - logon trigger, creating, [13-15](#)
 - Oracle Virtual Private Database, used with, [14-4](#)
 - performance, [14-36](#)
 - policy groups, used in, [14-16](#)
 - returning predicate, [14-4](#)
 - session information, retrieving, [13-11](#)

- application contexts (*continued*)
 - support for database links, [13-21](#)
 - types, [13-4](#)
 - users, nondatabase connections, [13-29](#), [13-36](#)
 - where values are stored, [13-2](#)
 - See also client session-based application contexts, database session-based application contexts, global application contexts
- application developers
 - CONNECT role change, [A-27](#)
 - managing privileges for, [12-4](#)
- application security
 - finding privilege use by users, [5-2](#)
 - restricting wallet access to current application, [10-8](#)
 - revoking access control privileges from Oracle wallets, [10-13](#)
 - sharing wallet with other applications, [10-8](#)
 - specifying attributes, [13-9](#)
- application users who are database users
 - Oracle Virtual Private Database, how it works with, [14-52](#)
- applications
 - about security policies for, [12-2](#)
 - database users, [12-2](#)
 - DB_DEVELOPER_ROLE role, [12-4](#)
 - enhancing security with, [4-36](#)
 - object privileges, [12-28](#)
 - object privileges permitting SQL statements, [12-28](#)
 - One Big Application User authentication
 - security considerations, [12-3](#)
 - security risks of, [12-2](#)
 - Oracle Virtual Private Database, how it works with, [14-45](#)
 - password handling, guidelines, [12-8](#)
 - password protection strategies, [12-7](#)
 - privileges, managing, [12-21](#)
 - roles
 - multiple, [4-38](#)
 - privileges, associating with database roles, [12-25](#)
 - security, [4-56](#), [12-3](#)
 - security considerations for use, [12-2](#)
 - security limitations, [14-45](#)
 - security policies, [14-17](#)
 - validating with security policies, [14-18](#)
- APPQOSSYS user account, [2-39](#)
- architecture, [6-3](#)
- archiving
 - operating system audit files, [32-10](#)
 - standard audit trail, [32-11](#)
 - timestamping audit trail, [32-15](#)
- ASMSNMP user account, [2-39](#)
- asymmetric key operations, [18-15](#)
- asynchronous authentication mode in RADIUS, [26-5](#)
- attacks
 - See security attacks
- audit files
 - operating system audit trail
 - archiving, setting timestamp, [32-15](#)
 - operating system file
 - archiving, [32-10](#)
 - standard audit trail
 - archiving, setting timestamp, [32-15](#)
 - records, archiving, [32-11](#)
- audit policies, [28-1](#)
 - about, [29-2](#)
 - about predefined, [29-5](#)
 - what to audit, [29-1](#)
 - See also unified audit policies
- audit policies, application contexts
 - about, [30-43](#)
 - appearance in audit trail, [30-45](#)
 - configuring, [30-43](#)
 - disabling, [30-44](#)
 - examples, [30-44](#)
- audit records
 - when written to OS files, [32-7](#)
- audit trail
 - archiving, [32-11](#)
 - capturing syslog records, [32-5](#)
 - capturing Windows Event Viewer records, [32-5](#)
 - finding information about audit management, [32-25](#)
 - finding information about fine-grained audit usage, [31-18](#)
 - finding information about usage, [29-17](#)
 - finding information about usage in custom audit policies, [30-91](#)
 - SYSLOG records, [32-4](#)
 - unified
 - archiving, [32-11](#)
- AUDIT_ADMIN role, [4-40](#)
- AUDIT_VIEWER role, [4-40](#)
- auditing, [29-14](#)
 - administrators, Database Vault, [30-48](#)
 - audit configurations, [29-16](#), [30-37](#)
 - audit options, [29-14](#)
 - audit policies, [29-16](#), [30-37](#)
 - audit trail, sensitive data in, [A-20](#)
 - CDBs, [28-9](#)
 - committed data, [A-21](#)
 - common objects, [29-16](#), [30-37](#)
 - cursors, affect on auditing, [32-10](#)
 - database user names, [3-65](#)
 - Database Vault administrators, [30-48](#)
 - databases, when unavailable, [32-7](#)
 - disk space size for unified audit records, [32-3](#)

auditing (*continued*)

- distributed databases and, [28-10](#)
- DV_ADMIN role user, [30-48](#)
- DV_OWNER role user, [30-48](#)
- finding information about audit management, [32-25](#)
- finding information about fine-grained auditing, [31-18](#)
- finding information about usage, [29-17](#)
- finding information about usage in custom audit policies, [30-91](#)
- fine-grained
 - See fine-grained auditing, [31-2](#)
- functions, [30-16](#)
- functions, Oracle Virtual Private Database, [30-18](#)
- general steps
 - commonly used security-relevant activities, [29-15](#)
 - specific fine-grained activities, [29-16](#)
 - SQL statements and other general activities, [29-15](#)
- general steps for, [29-14](#)
- guidelines for security, [A-20](#)
- historical information, [A-21](#)
- INHERIT PRIVILEGE privilege, [9-8](#)
- keeping information manageable, [A-21](#)
- loading audit records to unified audit trail, [32-7](#)
- mandatory auditing, [29-3](#)
- multitier environments
 - See standard auditing, [30-33](#)
- One Big Application User authentication, compromised by, [12-2](#)
- operating-system user names, [3-65](#)
- Oracle Virtual Private Database policy functions, [30-18](#)
- packages, [30-16](#)
- performance, [28-4](#)
- PL/SQL packages, [30-16](#)
- predefined policies
 - general steps for using, [29-15](#)
- privileges required, [28-6](#)
- procedures, [30-16](#)
- purging records
 - example, [32-24](#)
 - general steps for on-demand, [32-13](#)
 - general steps for scheduled purges, [32-13](#)
- range of focus, [29-14](#)
- READ object privileges in policies, [30-19](#)
- READ privileges
 - about, [30-19](#)
 - how recorded in audit trail, [30-19](#)
- recommended settings, [A-23](#)

auditing (*continued*)

- Sarbanes-Oxley Act
 - auditing, meeting compliance through, [28-1](#)
- SELECT privileges
 - about, [30-19](#)
 - how recorded in audit trail, [30-19](#)
- sensitive data, [A-23](#)
- suspicious activity, [A-22](#)
- triggers, [30-16](#)
- unified audit trail
 - about, [28-5](#)
- VPD predicates
 - fine-grained audit policies, [31-4](#)
 - unified audit policies, [30-16](#)
 - when audit options take effect, [32-2](#)
 - when records are created, [32-2](#)
 - See also unified audit policies
- auditing, purging records
 - about, [32-12](#)
 - cancelling archive timestamp, [32-23](#)
 - creating audit trail
 - purge job, [32-14](#)
 - creating the purge job, [32-17](#)
 - DBMS_SCHEDULER package, [32-14](#)
 - deleting a purge job, [32-22](#)
 - disabling purge jobs, [32-21](#)
 - enabling purge jobs, [32-21](#)
 - general steps for, [32-13](#)
 - purging audit trail manually, [32-18](#)
 - roadmap, [32-13](#)
 - scheduling the purge job, [32-17](#)
 - setting archive timestamp, [32-15](#)
 - time interval for named purge job, [32-22](#)
- AUDSYS user account, [2-39](#)
- AUTHENTICATEDUSER role, [4-40](#)
- authentication, [3-3](#), [22-6](#)
 - about, [3-1](#)
 - administrators
 - operating system, [3-55](#)
 - passwords, [3-55](#)
 - SYSDBA and SYSOPER access, centrally controlling, [3-52](#)
 - by database, [3-57](#)
 - client, [A-15](#)
 - client-to-middle tier process, [3-77](#)
 - configuring multiple methods, [27-4](#)
 - database administrators, [3-52](#)
 - databases, using
 - about, [3-57](#)
 - advantages, [3-59](#)
 - procedure, [3-59](#)
 - Enterprise User Security, [3-69](#)
 - external with local database authorization, [3-64](#), [3-68](#), [3-69](#)
 - methods, [22-3](#)

authentication (*continued*)

- middle-tier authentication
 - proxies, example, [3-79](#)
- modes in RADIUS, [26-3](#)
- multitier, [3-69](#)
- One Big Application User, compromised by, [12-2](#)
- operating system authentication, [3-62](#)
 - about, [3-65](#)
 - advantages, [3-65](#)
 - disadvantages, [3-65](#)
- operating system user in PDBs, [3-62](#)
- ORA-28040 errors, [3-37](#)
- PDBs, [3-62](#)
- proxy user authentication
 - about, [3-73](#)
 - expired passwords, [3-76](#)
- public key infrastructure, [3-66](#)
- RADIUS, [3-67](#)
- remote, [A-15](#)
- schema-only accounts, [3-60](#)
 - about, [3-60](#)
 - altering, [3-61](#)
 - creating users, [3-61](#)
- schema-only accounts, users created with, [3-60](#)
- security guideline, [A-10](#)
- specifying when creating a user, [2-9](#)
- strong, [A-7](#)
- SYSDBA on Windows systems, [3-55](#)
- Windows native authentication, [3-55](#)
 - See also passwords, proxy authentication

authentication types, [6-4](#)

AUTHID DEFINER clause

- used with Oracle Virtual Private Database functions, [14-4](#)

authorization

- about, [4-1](#)
- changing for roles, [4-51](#)
- local database for external authentication, [3-64](#), [3-68](#), [3-69](#)
- multitier, [3-69](#)
- omitting for roles, [4-48](#)
- operating system, [4-53](#)
- roles, about, [4-51](#)

automatic reparse

- Oracle Virtual Private Database, how it works with, [14-46](#)

AVTUNE_PKG_ROLE role, [4-40](#)

B

banners

- auditing user actions, configuring, [12-32](#)
- unauthorized access, configuring, [12-32](#)

BDSQL_ADMIN role, [4-40](#)

BDSQL_USER role, [4-40](#)

BFILES

- guidelines for security, [A-11](#)

bind variables

- application contexts, used with, [14-4](#)
- sensitive columns, [15-17](#)

BLOBS

- encrypting, [18-8](#)

C

CAPTURE_ADMIN role, [4-40](#)

cascading revokes, [4-101](#)

catpvt.sql script (password complexity functions), [3-26](#)

CDB common users

- about, [2-3](#)
- plug-in operations, [2-4](#)

CDB_DBA role, [4-40](#)

CDBs, [2-3](#)

- auditing
 - how affects, [28-9](#)
- CBAC role grants with DELEGATE option, [9-15](#)
- common mandatory profiles for CDB root, about, [2-30](#)
- common mandatory profiles for CDB root, creating, [2-31](#)
- common mandatory profiles for CDB root, example, [2-32](#)
- common privilege grants, [4-6](#), [4-8](#), [4-29](#)
- common roles, [4-59](#)
- common users, [4-6](#), [4-8](#)
- granting common roles and privileges, [4-7](#)
- granting privileges and roles, [4-5](#), [4-31](#)
- local privilege grants, [4-29](#)
- local roles, [4-5](#), [4-62](#)
- object privileges, [4-30](#)
- PDB lockdown profiles, [4-64](#), [4-67](#)
- PDB lockdown profiles, features that benefit from, [4-66](#)
- principles of grants, [4-4](#)
- privilege management, [4-29](#)
- privilege profiles, [5-4](#)
- revoking privileges, [4-31](#)
- roles
 - altering, [4-51](#)
 - creating common, [4-61](#)
 - creating local, [4-62](#)
 - granting common, [4-6](#), [4-8](#), [4-62](#)
 - how common roles work, [4-60](#)
 - managing, [4-58](#)
 - privileges required to manage, [4-60](#)
 - rules for creating common, [4-60](#)
- security isolation guideline, [A-14](#)

- CDBs (*continued*)
 - SYSLOG capture of unified audit records, [32-5](#)
 - system privileges, [4-30](#)
 - transparent sensitive data protection, [15-4](#)
 - user accounts
 - creating, [2-14](#)
 - local, [2-5](#)
 - user privileges, how affects, [4-12](#)
 - users
 - CDB common, [2-3](#)
 - common, [2-3](#)
 - viewing information about, [4-32](#)
 - Virtual Private Database
 - policies, [14-5](#)
- Center for Internet Security (CIS), [29-8](#)
 - ORA_CIS_PROFILE user profile, [2-27](#)
 - ORA_LOGIN_LOGOUT predefined unified audit policy, [29-10](#)
- centrally managed users
 - Oracle Autonomous Database, [6-38](#)
- certificate authority (CA), [B-5](#)
- certificate key algorithm
 - Transport Layer Security, [A-19](#)
- certificate revocation list (CRL)
 - deleting, [B-29](#)
 - displaying, [B-29](#)
 - displaying list of, [B-31](#)
 - hash value generation, [B-30](#)
 - uploading, [B-31](#)
- certificate revocation lists
 - manipulating with orapki tool, [21-47](#)
 - uploading to LDAP directory, [21-47](#)
 - where to store them, [21-43](#)
- certificate revocation status checking
 - disabling on server, [21-45](#), [21-46](#)
- certificate store location
 - system wallet, [B-15](#)
- certificate validation error message
 - CRL could not be found, [21-52](#)
 - CRL date verification failed with RSA status, [21-52](#)
 - CRL signature verification failed with RSA status, [21-52](#)
 - Fetch CRL from CRL DP
 - No CRLs found, [21-52](#)
 - OID hostname or port number not set, [21-52](#)
- certificates, [6-16](#), [B-4](#)
 - adding to wallet using orapki, [B-22](#)
 - creating SHA-2 with orapki, [B-17](#)
 - creating signed with orapki, [B-16](#)
 - general process of management, [B-6](#)
 - Oracle Real Application Clusters components that need certificates, [21-56](#)
 - tools to manage, [B-6](#)
- challenge-response authentication in RADIUS, [26-5](#)
- change_on_install default password, [A-7](#)
- character sets
 - role names, multibyte characters in, [4-48](#)
 - role passwords, multibyte characters in, [4-51](#)
- Cipher Block Chaining (CBC) mode, defined, [20-2](#)
- cipher suites
 - Transport Layer Security, [A-19](#)
- ciphertext data
 - defined, [20-2](#)
- client connections
 - guidelines for security, [A-15](#)
 - secure external password store, [3-43](#)
 - securing, [A-15](#)
- client identifier
 - setting for applications that use JDBC, [3-84](#)
- client identifiers, [13-29](#)
 - about, [3-82](#)
 - auditing users, [30-33](#)
 - consistency between DBMS_SESSION.SET_IDENTIFIER and DBMS_APPLICATION_INFO.SET_CLIENT_INFO, [3-85](#)
 - global application context, independent of, [3-83](#)
 - setting with DBMS_SESSION.SET_IDENTIFIER procedure, [13-29](#)
 - See also nondatabase users
- client session-based application contexts, [13-52](#)
 - about, [13-52](#)
 - CLIENTCONTEXT namespace, clearing value from, [13-54](#)
 - CLIENTCONTEXT namespace, setting value in, [13-52](#)
 - retrieving CLIENTCONTEXT namespace, [13-53](#)
 - See also application contexts
- CLIENT_IDENTIFIER USERENV attribute, [3-83](#)
 - setting and clearing with DBMS_SESSION package, [3-85](#)
 - setting with OCI user session handle attribute, [3-84](#)
 - See also USERENV namespace
- CLIENTID_OVERWRITE event, [3-85](#)
- CMU_WALLET database property
 - about, [6-11](#)
 - wallet creation, [6-17](#)
- code based access control (CBAC)
 - about, [9-11](#)
 - granting and revoking roles to program unit, [9-16](#)
 - how works with definers rights, [9-14](#)
 - how works with invoker's rights, [9-12](#)
 - privileges, [9-12](#)
 - tutorial, [9-17](#)

- column masking behavior, [14-14](#)
 - column specification, [14-15](#)
 - restrictions, [14-15](#)
- columns
 - auditing, [30-11](#), [30-14](#)
 - granting privileges for selected, [4-97](#)
 - granting privileges on, [4-97](#)
 - INSERT privilege and, [4-97](#)
 - listing users granted to, [4-113](#)
 - privileges, [4-97](#)
 - pseudo columns
 - USER, [4-83](#)
 - revoking privileges on, [4-100](#)
- command line recall attacks, [12-7](#), [12-10](#)
- committed data
 - auditing, [A-21](#)
- common privilege grants, [4-6](#), [4-8](#)
 - about, [4-29](#)
 - granting, [4-31](#)
 - revoking, [4-31](#)
 - with object privileges, [4-30](#)
 - with system privileges, [4-30](#)
- common roles, [4-59](#)
 - about, [4-59](#)
 - auditing, [30-5](#)
 - creating, [4-61](#)
 - granting, [4-6](#), [4-8](#), [4-62](#)
 - how they work, [4-60](#)
 - privileges required to manage, [4-60](#)
 - rules for creating, [4-60](#)
- common user accounts
 - creating, [2-14](#)
 - enabling access to other PDBs, [4-31](#)
 - granting privileges to, [4-6](#), [4-8](#), [4-29](#)
- common users
 - accessing data in PDBs, [4-33](#)
 - altering, [2-18](#)
- configuration
 - guidelines for security, [A-13](#)
- configuration files
 - Kerberos, [24-6](#)
 - listener.ora, [A-15](#)
 - RADIUS, [26-7](#)
 - sample listener.ora file, [A-15](#)
 - server.key encryption file, [A-19](#)
 - tsnames.ora, [A-19](#)
 - typical directory, [A-19](#)
- configuring
 - Kerberos authentication service parameters, [24-12](#)
 - RADIUS authentication, [26-9](#)
- CONNECT role
 - about, [A-25](#)
 - applications
 - account provisioning, [A-26](#)
 - affects of, [A-25](#)
- CONNECT role (*continued*)
 - applications (*continued*)
 - database upgrades, [A-26](#)
 - installation of, [A-26](#)
 - script to create, [4-40](#)
 - users
 - application developers, impact, [A-27](#)
 - client-server applications, impact, [A-27](#)
 - general users, impact, [A-27](#)
 - how affects, [A-26](#)
 - why changed, [A-25](#)
- connecting
 - with username and password, [27-1](#)
- connection pooling
 - about, [3-69](#)
 - finding unnecessarily granted privileges, [5-2](#)
 - global application contexts, [13-29](#)
 - nondatabase users, [13-36](#)
 - proxy authentication, [3-77](#)
- container data objects
 - about, [4-32](#)
- container database (CDB)
 - See CDBs
- CONTAINER_DATA objects
 - viewing information about, [4-31](#)
- context profiles
 - privilege analysis, [5-3](#)
- controlled step-in procedures, [9-3](#)
- CPU time limit, [2-24](#)
- CREATE ANY LIBRARY statement
 - security guidelines, [A-3](#)
- CREATE ANY PROCEDURE system privilege, [4-84](#)
- CREATE CONTEXT statement
 - example, [13-8](#)
- CREATE LOCKDOWN PROFILE statement, [4-64](#), [4-68](#)
- CREATE PROCEDURE system privilege, [4-84](#)
- CREATE PROFILE statement
 - password aging and expiration, [3-12](#)
 - password management, [3-5](#)
 - passwords, example, [3-13](#)
- CREATE ROLE statement, [4-59](#)
 - IDENTIFIED EXTERNALLY option, [4-52](#)
- CREATE SCHEMA statement
 - securing, [12-26](#)
- CREATE SESSION statement
 - CONNECT role privilege, [A-10](#)
 - securing, [12-26](#)
- CREATE USER statement
 - explicit account locking, [3-11](#)
 - IDENTIFIED BY option, [2-9](#)
 - IDENTIFIED EXTERNALLY option, [2-9](#)
 - creating Oracle service directory user account, [6-7](#)

credentials
 SQL*Loader object store, [3-47](#)
 CRLAdmins directory administrative group, [B-31](#)
 CRLs
 disabling on server, [21-45](#), [21-46](#)
 where to store them, [21-43](#)
 cryptographic libraries
 FIPS 140-2, [C-1](#)
 CTXAPP role, [4-40](#)
 CTXSYS user account, [2-39](#)
 cursors
 affect on auditing, [32-10](#)
 reparsing, for application contexts, [13-15](#)
 shared, used with Virtual Private Database, [14-4](#)

D

data definition language (DDL)
 roles and privileges, [4-39](#)
 data dictionary
 about, [16-1](#)
 data dictionary views, [16-6](#)
 deleting, [16-4](#)
 encrypting sensitive information in, [16-1–16-6](#)
 multitenant environment, [16-2](#)
 procedure, [16-2](#)
 protecting, [A-11](#)
 rekeying, [16-3](#)
 restoring lost keystore, [16-5](#)
 data encryption and integrity parameters
 about, [20-4](#)
 data files, [A-11](#)
 guidelines for security, [A-11](#)
 data manipulation language (DML)
 privileges controlling, [4-81](#)
 data security
 encryption, problems not solved by, [18-4](#)
 database administrators (DBAs)
 access, controlling, [18-3](#)
 authentication, [3-52](#)
 malicious, encryption not solved by, [18-3](#)
 Database Configuration Assistant (DBCA)
 default passwords, changing, [A-7](#)
 user accounts, automatically locking and expiring, [A-3](#)
 database links, [6-5](#)
 application context support, [13-21](#)
 application contexts, [13-13](#)
 authenticating with Kerberos, [3-66](#)
 definer's rights procedures, [9-22](#)
 object privileges, [4-72](#)
 operating system accounts, care needed, [3-65](#)
 Oracle DBaaS-to-IAM connections, [7-37](#)
 RADIUS not supported, [26-1](#)

database links (*continued*)
 sensitive credential data
 about, [16-1](#)
 data dictionary views, [16-6](#)
 deleting, [16-4](#)
 encrypting, [16-2](#)
 multitenant environment, [16-2](#)
 rekeying, [16-3](#)
 restoring functioning of after lost keystore, [16-5](#)
 session-based application contexts,
 accessing, [13-13](#)
 database session-based application contexts, [13-6](#)
 about, [13-6](#)
 cleaning up after user exits, [13-6](#)
 components, [13-7](#)
 database links, [13-13](#)
 dynamic SQL, [13-12](#)
 externalized, using, [13-27](#)
 how to use, [13-5](#)
 initializing externally, [13-21](#)
 initializing globally, [13-23](#)
 ownership, [13-8](#)
 parallel queries, [13-12](#)
 PL/SQL package creation, [13-9](#)
 session information, setting, [13-13](#)
 SYS_CONTEXT function, [13-11](#)
 trusted procedure, [13-2](#)
 tutorial, [13-17](#)
 See also application contexts
 database upgrades and CONNECT role, [A-26](#)
 databases
 access control
 password encryption, [3-3](#)
 additional security products, [1-3](#)
 authentication, [3-57](#)
 database user and application user, [12-2](#)
 default password security settings, [3-9](#)
 DBCA-created databases, [3-9](#)
 manually-created databases, [3-9](#)
 default security features, summary, [1-1](#)
 granting privileges, [4-92](#)
 granting roles, [4-92](#)
 limitations on usage, [2-23](#)
 schema-only accounts, [3-60](#)
 security and schemas, [12-26](#)
 security embedded, advantages of, [12-3](#)
 security policies based on, [14-3](#)
 DATAPUMP_EXP_FULL_DATABASE role, [4-40](#)
 DATAPUMP_IMP_FULL_DATABASE role, [4-40](#)
 DB_DEVELOPER_ROLE role
 about, [4-40](#), [12-4](#)
 DBA role
 about, [4-40](#)

- DBA_CONTAINER_DATA data dictionary view, [4-32](#)
- DBA_ROLE_PRIVS view
 - application privileges, finding, [12-22](#)
- DBA_ROLES data dictionary view
 - PUBLIC role, [4-21](#)
- DBFS_ROLE role, [4-40](#)
- DBJAVASCRIPT role, [4-40](#)
- DBMS_CREDENTIAL package, [3-62](#), [4-66](#)
- DBMS_CREDENTIAL.CREATE_CREDENTIAL procedure, [12-18](#)
- DBMS_CRYPTO
 - FIPS-supported cipher suites, [C-5](#)
- DBMS_CRYPTO package
 - asymmetric key operations, [18-15](#)
 - data encryption storage, [18-9](#)
 - examples, [18-16](#)
 - supported cryptographic algorithms, [18-9](#)
- DBMS_CRYPTO PL/SQL package
 - enabling for FIPS 140-2, [C-8](#)
- DBMS_FGA package
 - about, [31-6](#)
 - DISABLE_POLICY procedure, [31-11](#)
 - DROP_POLICY procedure, [31-11](#)
 - editions, [31-5](#)
 - ENABLE_POLICY procedure, [31-10](#)
- DBMS_MDX_INTERNAL role, [4-40](#)
- DBMS_NETWORK_ACL_ADMIN.REMOVE_HOST_ACE procedure, [10-7](#)
- DBMS_PRIVILEGE_CAPTURE PL/SQL package, [5-5](#)
- DBMS_RLS.ADD_POLICY
 - sec_relevant_cols parameter, [14-12](#)
 - sec_relevant_cols_opt parameter, [14-15](#)
- DBMS_RLS.ADD_POLICY procedure
 - transparent sensitive data protection policies, [15-22](#)
- DBMS_SESSION package
 - client identifiers, using, [3-85](#)
 - global application context, used in, [13-31](#)
 - SET_CONTEXT procedure
 - about, [13-13](#)
- DBMS_SESSION.SET_CONTEXT procedure
 - about, [13-13](#)
 - syntax, [13-13](#)
 - username and client_id settings, [13-32](#)
- DBMS_SESSION.SET_IDENTIFIER procedure
 - client session ID, setting, [13-29](#)
 - DBMS_APPLICATION.SET_CLIENT_INFO value, overwritten by, [3-85](#)
- DbNest
 - about, [17-1](#)
 - architecture, [17-4](#)
 - configuration file, [17-5](#)
 - enabling, [17-7](#)
 - file system isolation for nest, [17-8](#)
- DbNest (*continued*)
 - how Oracle Database manages nest, [17-7](#)
 - initialization parameters, [17-5](#)
 - Linux namespaces, [17-2](#)
 - properties of, [17-3](#)
 - purpose of, [17-2](#)
- DBNEST_ENABLE initialization parameter, [17-5](#)
- DBNEST_PDB_FS_CONF initialization parameter, [17-5](#)
- DBSFUSER user account, [2-39](#)
- DBSNMP user account
 - about, [2-39](#)
 - password usage, [A-7](#)
- DDL
 - See data definition language
- debugging
 - Java stored procedures, [10-22](#)
 - PL/SQL stored procedures, [10-22](#)
- decryption
 - number strings using DBMS_CRYPTO, [18-21](#)
- default command rules
 - ORA_DV_DEFAULT_PROTECTION predefined audit policy for, [29-13](#)
- default passwords, [A-7](#)
 - change_on_install or manager passwords, [A-7](#)
 - changing, importance of, [3-6](#)
 - finding, [3-6](#)
- default permissions, [A-11](#)
- default profiles
 - about, [3-7](#)
- default realms
 - ORA_DV_DEFAULT_PROTECTION predefined audit policy for, [29-13](#)
- default roles
 - setting for user, [2-17](#)
 - specifying, [4-107](#)
- default users
 - accounts, [A-3](#)
 - Enterprise Manager accounts, [A-3](#)
 - passwords, [A-7](#)
- defaults
 - tablespace quota, [2-11](#)
 - user tablespaces, [2-9](#)
- definer's rights
 - about, [9-2](#)
 - code based access control
 - about, [9-11](#)
 - granting and revoking roles to program unit, [9-16](#)
 - how code based access control works, [9-14](#)
 - compared with invoker's rights, [9-1](#)
 - example of when to use, [9-2](#)
 - procedure privileges, used with, [9-2](#)
 - procedure security, [9-2](#)

- definer's rights (*continued*)
 - schema privileges for, [9-2](#)
 - secure application roles, [12-23](#)
 - used with Oracle Virtual Private Database functions, [14-4](#)
 - views, [9-9](#)
- definer's rights, database links
 - revokes of INHERIT [ANY] REMOTE PRIVILEGES, [9-24](#)
 - grants of INHERIT ANY REMOTE PRIVILEGES, [9-24](#)
 - grants of INHERIT ANY REMOTE PRIVILEGES on connected user to current user, example, [9-23](#)
 - grants of INHERIT REMOTE PRIVILEGES to other users, [9-23](#)
 - revoking INHERIT REMOTE PRIVILEGES from PUBLIC, example, [9-25](#)
 - revoking INHERIT REMOTE PRIVILEGES on connecting user from procedure owner, example, [9-25](#)
 - tutorial, [9-26](#)
- definers's rights, database links
 - about, [9-22](#)
 - ORA-25433 error, [9-22](#)
- denial of service (DoS) attacks
 - about, [8](#)
- denial-of-service (DoS) attacks
 - bad packets, preventing, [12-30](#)
 - networks, securing, [A-15](#)
 - password concurrent guesses, [3-3](#)
- Department of Defense Database Security
 - Technical Implementation Guide, [3-26](#), [3-27](#)
- DGPDB_INT user account, [2-39](#)
- DGPDB_ROLE role, [4-40](#)
- diagnostics
 - DIAGNOSTICS_CONTROL initialization parameter, [4-28](#)
 - restricting use to SYSDBA and ENABLE DIAGNOSTICS, [4-28](#)
- dictionary privileges
 - about, [4-79](#)
- dictionary protection
 - disabling for Oracle-maintained schema, [4-80](#)
 - enabling for Oracle-maintained schema, [4-80](#)
- dictionary tables
 - auditing, [30-13](#)
- Diffie-Hellman key negotiation algorithm, [20-7](#)
- DIP user account, [2-42](#)
- direct path load
 - fine-grained auditing effects on, [31-2](#)
- directories
 - auditing, [30-11](#)
- directory authentication, configuring for SYSDBA or SYSOPER access, [3-53](#)
- directory objects
 - granting EXECUTE privilege on, [4-93](#)
- disabling unnecessary services
 - FTP, TFTP, TELNET, [A-15](#)
- dispatcher processes (Dnnn)
 - limiting SGA space for each session, [2-25](#)
- distributed databases
 - auditing and, [28-10](#)
- DML
 - See data manipulation language
- driving context, [13-54](#)
- DROP PROFILE statement
 - example, [2-29](#)
- DROP ROLE statement
 - example, [4-55](#)
 - security domain, affected, [4-55](#)
- DROP USER statement
 - about, [2-37](#)
 - schema objects of dropped user, [2-38](#)
- dsi.ora file
 - about, [6-11](#)
 - changing contents of, [6-11](#)
 - CMU_WALLET database property, [6-11](#)
 - compared with ldap.ora, [6-10](#)
 - multitenant environment, [6-11](#)
 - placement of, [6-11](#)
 - search order for, [6-11](#)
 - WALLET_LOCATION parameter and, [6-11](#)
 - when to use, [6-11](#)
- DV_role, [4-40](#)
- DV_ACCTMGR role, [4-40](#)
- DV_ADMIN role, [4-40](#)
- DV_AUDIT_CLEANUP role, [4-40](#)
- DV_DATAPUMP_NETWORK_LINK role, [4-40](#)
- DV_GOLDENGATE_ADMIN role, [4-40](#)
- DV_GOLDENGATE_REDO_ACCESS role, [4-40](#)
- DV_MONITOR role, [4-40](#)
- DV_OWNER role, [4-40](#)
- DV_PATCH_ADMIN role, [4-40](#)
- DV_POLICY_OWNER role, [4-40](#)
- DV_SECANALYST role, [4-40](#)
- DV_STREAMS_ADMIN role, [4-40](#)
- DV_XSTREAMS_ADMIN role, [4-40](#)
- DVF schema
 - ORA_DV_SCHEMA_CHANGES predefined audit policy for, [29-13](#)
- DVSYS schema
 - ORA_DV_SCHEMA_CHANGES predefined audit policy for, [29-13](#)
- dynamic Oracle Virtual Private Database policy
 - types, [14-20](#)
- DYNAMIC policy type, [14-20](#)

E

- editions
 - application contexts, how affects, [13-3](#)
 - fine-grained auditing packages, results in, [13-32](#)
 - global application contexts, how affects, [13-32](#)
 - Oracle Virtual Private Database packages, results in, [13-32](#)
- EJBCLIENT role, [4-40](#)
- email alert example, [31-12](#)
- enable_fips.py script, [C-4](#)
- encrypting information in, [16-1](#)
- encryption
 - access control, [18-2](#)
 - BLOBS, [18-8](#)
 - challenges, [18-4](#)
 - data security, problems not solved by, [18-4](#)
 - data transfer, [A-15](#)
 - deleted encrypted data, [A-11](#)
 - examples, [18-16](#)
 - indexed data, [18-4](#)
 - key generation, [18-5](#)
 - key storage, [18-6](#)
 - key transmission, [18-5](#)
 - keys, changing, [18-8](#)
 - malicious database administrators, [18-3](#)
 - network encryption, [20-7](#)
 - network traffic, [A-15](#)
 - number strings using DBMS_CRYPTO, [18-21](#)
 - on-demand encryption, [18-1](#)
 - problems not solved by, [18-2](#)
 - Transparent Data Encryption, [18-8](#)
 - transparent tablespace encryption, [18-8](#)
- encryption and checksumming
 - activating, [20-8](#)
 - negotiating, [20-9](#)
 - parameter settings, [20-11](#)
- encryption of data dictionary sensitive data, [16-1](#)
- ENFORCE_CREDENTIAL configuration
 - parameter
 - security guideline, [A-20](#)
- enterprise directory service, [4-53](#)
- enterprise roles, [4-53](#)
- enterprise user management, [12-2](#)
- Enterprise User Security
 - application context, globally initialized, [13-25](#)
 - proxy authentication
 - Oracle Virtual Private Database, how it works with, [14-52](#)
- enterprise users
 - global role, creating, [4-53](#)
 - One Big Application User authentication, compromised by, [12-2](#)
 - proxy authentication, [3-73](#)
 - shared schemas, protecting users, [12-27](#)
- error messages
 - ORA-12650, [20-8](#), [20-10](#)
 - ORA-25433, [9-22](#)
- errors
 - ORA-00036, [31-7](#)
 - ORA-01720, [4-82](#)
 - ORA-01994, [2-21](#)
 - ORA-06512, [10-22](#), [31-16](#)
 - ORA-06598, [9-6](#)
 - ORA-1000, [31-7](#)
 - ORA-1536, [2-11](#)
 - ORA-24247, [10-3](#), [10-22](#), [31-16](#)
 - ORA-28017, [2-21](#)
 - ORA-28040, [3-37](#), [3-57](#)
 - ORA-28046, [2-21](#)
 - ORA-28144, [31-7](#)
 - ORA-28575, [12-18](#)
 - ORA-45622, [15-12](#)
- example, basic, [30-22](#)
- example, comparison, [30-23](#)
- examples, [13-17](#), [14-27](#)
 - access control lists
 - external network connections, [10-14](#)
 - wallet access, [10-14](#)
 - account locking, [3-11](#)
 - audit trail, purging unified trail, [32-24](#)
 - auditing GRANT operations, [30-13](#)
 - auditing REVOKE operations, [30-13](#)
 - auditing user SYS, [30-8](#)
 - data encryption
 - encrypting and decrypting BLOB data, [18-17](#)
 - encrypting and decrypting procedure with AES 256-Bit, [18-17](#)
 - decrypting a number using DBMS_CRYPTO, [18-21](#)
 - directory objects, granting EXECUTE privilege on, [4-93](#)
 - encrypting a number using DBMS_CRYPTO, [18-21](#)
 - encrypting procedure, [18-16](#)
 - Java code to read passwords, [12-11](#)
 - locking an account with CREATE PROFILE, [3-11](#)
 - login attempt grace period, [3-13](#)
 - nondatabase user authentication, [13-36](#)
 - passwords
 - aging and expiration, [3-13](#)
 - changing, [2-19](#)
 - creating for user, [2-9](#)
 - privileges
 - granting ADMIN OPTION, [4-93](#)
 - views, [4-110](#)
 - procedure privileges affecting packages, [4-86](#)
 - profiles, assigning to user, [2-13](#)

examples (*continued*)

roles

- altering for external authorization, [4-51](#)
- creating for application authorization, [4-52](#)
- creating for external authorization, [4-52](#)
- creating for password authorization, [4-49](#), [4-50](#)

- default, setting, [4-107](#)

- external, [4-50](#)

- global, [4-50](#)

- using SET ROLE for password-authenticated roles, [4-51](#)

- views, [4-110](#)

- secure external password store, [3-42](#)

- session ID of user

- finding, [2-37](#)

- system privilege and role, granting, [4-93](#)

- tablespaces

- assigning default to user, [2-10](#)

- quota, assigning to user, [2-11](#)

- temporary, [2-13](#)

- type creation, [4-89](#)

- users

- account creation, [2-6](#)

- creating with GRANT statement, [4-93](#)

- dropping, [2-38](#)

- middle-tier server proxying a client, [3-75](#)

- object privileges granted to, [4-94](#)

- proxy user, connecting as, [3-75](#)

- See also tutorials

exceptions

- WHEN NO DATA FOUND, used in application context package, [13-18](#)

- WHEN OTHERS, used in triggers

- development environment (debugging)

- example, [13-16](#)

- production environment example, [13-16](#)

Exclusive Mode

- SHA-2 password hashing algorithm, enabling, [3-35](#)

EXECUTE ANY LIBRARY statement

- security guidelines, [A-3](#)

EXECUTE_CATALOG_ROLE role

- SYS schema objects, enabling access to, [4-20](#)

EXEMPT ACCESS POLICY privilege

- Oracle Virtual Private Database enforcements, exemption, [14-47](#)

EXP_FULL_DATABASE role

- about, [4-40](#)

expiring a password

- explicitly, [3-13](#)

exporting data

- direct path export impact on Oracle Virtual Private Database, [14-47](#)
- policy enforcement, [14-47](#)

extended data objects

- views and Virtual Private Database, [14-10](#)

external network services

- enabling listener for, [10-6](#)

- external network services, fine-grained access to
- See access control list (ACL)

- external network services, syntax for, [10-4](#)

external procedures

- configuring extproc process for, [12-18](#)

- credentials, [12-16](#)

- DBMS_CREDENTIAL.CREATE_CREDENTIAL procedure, [12-18](#)

- legacy applications, [12-19](#)

- security guideline, [A-20](#)

- external roles, [4-50](#)

- external tables, [A-11](#)

extproc process

- about, [12-16](#)

- configuring credential for, [12-18](#)

- legacy applications, [12-19](#)

F

failed login attempts

- account locking, [3-10](#)

- password management, [3-10](#)

- resetting, [3-10](#)

- fallback authentication, Kerberos, [24-28](#)

Federal Information Processing Standard (FIPS)

- DBMS_CRYPTO package, [C-8](#)

- FIPS 140-2

- postinstallation checks, [C-10](#)

- SQLNET.FIPS_140, [C-9](#)

- SSLFIPS_140, [C-9](#)

- SSLFIPS_LIB, [C-9](#)

- verifying connections for

- DBMS_CRYPTO, [C-11](#)

- verifying connections for network native encryption, [C-11](#)

- verifying connections for TLS, [C-11](#)

- verifying connections when using FIPS_140 parameter, [C-10](#)

- Transparent Data Encryption, [C-8](#)

files

BFILES

- operating system access, restricting, [A-11](#)

BLOB, [18-8](#)

- keys, [18-7](#)

listener.ora file

- guidelines for security, [A-15](#), [A-19](#)

- restrict listener access, [A-15](#)

- server.key encryption file, [A-19](#)

- symbolic links, restricting, [A-11](#)

- tnsnames.ora, [A-19](#)

fine grained auditing
 Data Redaction
 schema system privileges, [4-26](#)
 schema system privileges, [4-26](#)
 fine-grained access control
 See Oracle Virtual Private Database (VPD)
 fine-grained auditing
 about, [31-2](#)
 alerts, adding to policy, [31-12](#)
 archiving audit trail, [32-11](#)
 columns, specific, [31-10](#)
 direct loads of data, [31-2](#)
 edition-based redefinitions, [31-5](#)
 editions, results in, [13-32](#)
 finding errors by checking trace files, [29-17](#),
 [31-18](#)
 how audit records are generated, [31-3](#)
 how to use, [31-2](#)
 policies
 adding, [31-6](#)
 disabling, [31-11](#)
 dropping, [31-11](#)
 enabling, [31-10](#)
 modifying, [31-6](#)
 policy creation syntax, [31-7](#)
 privileges required, [31-3](#)
 records
 archiving, [32-11](#)
 transparent sensitive data protection policy
 settings, [15-31](#)
 TSDP policies and, [15-30](#)
 VPD predicates, [31-4](#)
 FIPS
 weaker deprecated algorithm keys, [C-12](#)
 FIPS 140-2
 approved DBMS_CRYPTO cipher suites, [C-5](#)
 approved network native encryption
 algorithms, [C-7](#)
 approved TDE algorithms, [C-4](#)
 approved TLS cipher suites, [C-6](#)
 FIPS 140-2 cryptographic libraries
 about, [C-1](#)
 FIPS_140 parameter
 about, [C-3](#), [C-8](#)
 DBMS_CRYPTO, [C-3](#), [C-8](#)
 Java applications, enabling in, [C-4](#)
 Java applications, enabling using orapki and
 java.security file, [C-4](#)
 network native encryption, [C-3](#), [C-8](#)
 TDE, [C-3](#), [C-8](#)
 TLS, [C-3](#)
 Transport Layer Security, [C-8](#)
 fips.ora file, [C-3](#), [C-9](#)
 firewalls
 advice about using, [A-15](#)
 database server location, [A-15](#)

firewalls (*continued*)
 ports, [A-19](#)
 supported types, [A-15](#)
 flashback query
 Oracle Virtual Private Database, how it works
 with, [14-46](#)
 forcetcp parameter in krb5.conf, [24-16](#)
 foreign keys
 privilege to use parent key, [4-81](#)
 FTP protocol messages, auditing, [30-75](#)
 FTP service, [A-15](#)
 functions
 auditing, [30-11](#), [30-16](#)
 granting roles to, [4-55](#)
 Oracle Virtual Private Database
 components of, [14-6](#)
 privileges used to run, [14-4](#)
 privileges for, [4-84](#)
 roles, [4-38](#)

G

GATHER_SYSTEM_STATISTICS role, [4-40](#)
 GDS_CATALOG_SELECT role, [4-40](#)
 global application contexts, [13-28](#)
 about, [13-28](#)
 authenticating nondatabase users, [13-36](#)
 checking values set globally for all users,
 [13-34](#)
 clearing values set globally for all users,
 [13-34](#)
 components, [13-29](#)
 editions, affect on, [13-32](#)
 example of authenticating nondatabase users,
 [13-37](#)
 example of authenticating user moving to
 different application, [13-35](#)
 example of setting values for all users, [13-34](#)
 Oracle RAC environment, [13-30](#)
 Oracle RAC instances, [13-28](#)
 ownership, [13-30](#)
 PL/SQL package creation, [13-31](#)
 process, lightweight users, [13-49](#)
 process, standard, [13-48](#)
 sharing values globally for all users, [13-33](#)
 system global area, [13-28](#)
 tutorial for client session IDs, [13-44](#)
 used for One Big Application User scenarios,
 [14-52](#)
 uses for, [14-52](#)
 See also application contexts
 global authorization
 role creation, [4-53](#)
 global roles, [4-50](#)
 about, [4-53](#)
 GLOBAL_AQ_USER_ROLE role, [4-40](#)

GLOBAL_EXTPROC_CREDENTIAL
 configuration parameter
 security guideline, [12-19](#)
 grace period for login attempts
 example, [3-13](#)
 grace period for password expiration, [3-13](#)
 gradual database password rollover
 about, [3-17](#)
 actions permitted during, [3-22](#)
 changing password during rollover period, [3-21](#)
 changing password to begin rollover period, [3-20](#)
 enabling, [3-19](#)
 finding users who use old passwords, [3-24](#)
 manually ending the password before rollover period, [3-22](#)
 Oracle Data Guard, [3-24](#)
 Oracle Data Pump exports, [3-24](#)
 password change life cycle, [3-18](#)
 passwords, compromised, [3-23](#)
 server behavior after rollover ends, [3-23](#)
 GRANT ALL PRIVILEGES statement
 SELECT ANY DICTIONARY privilege, exclusion of, [A-11](#)
 GRANT ANY PRIVILEGE system privilege, [4-19](#)
 GRANT CONNECT THROUGH clause
 consideration when setting FAILED_LOGIN_ATTEMPTS parameter, [3-7](#)
 for proxy authorization, [3-75](#)
 GRANT statement, [4-92](#)
 ADMIN OPTION, [4-93](#)
 creating a new user, [4-93](#)
 object privileges, [4-94](#), [12-28](#)
 system privileges and roles, [4-92](#)
 when takes effect, [4-106](#)
 WITH GRANT OPTION, [4-95](#)
 granting privileges and roles
 about, [4-21](#)
 specifying ALL, [4-74](#)
 GRAPH_ADMINISTRATOR role, [4-40](#)
 GRAPH_DEVELOPER role, [4-40](#)
 GRAPH_USER role, [4-40](#)
 GSM_OGG_CAPTURE role, [4-40](#)
 GSM_POOLADMIN_ROLE role, [4-40](#)
 GSMADMIN_ROLE role, [4-40](#)
 GSMCATUSER_ROLE role, [4-40](#)
 GSMROOTUSER user account, [2-39](#)
 GSMROOTUSER_ROLE role, [4-40](#)
 GSMUSER_ROLE role, [4-40](#)
 guidelines
 handling compromised passwords, [3-23](#)
 guidelines for security
 auditing, [A-20](#)
 custom installation, [A-13](#)

guidelines for security (*continued*)
 data files and directories, [A-11](#)
 encrypting sensitive data, [A-11](#)
 guidelines for security
 custom installation, [A-13](#)
 installation and configuration, [A-13](#)
 networking security, [A-14](#)
 operating system accounts, limiting privileges, [A-11](#)
 operating system users, limiting number of, [A-11](#)
 Oracle home default permissions, disallowing modification, [A-11](#)
 ORACLE_DATAPUMP access driver, [A-12](#)
 passwords, [A-7](#)
 PDBs, [A-14](#)
 products and options
 install only as necessary, [A-13](#)
 sample schemas, [A-13](#)
 Sample Schemas
 remove or relock for production, [A-13](#)
 test database, [A-13](#)
 symbolic links, restricting, [A-11](#)
 Transport Layer Security
 mode, [A-19](#)
 TCPS protocol, [A-19](#)
 user accounts and privileges, [A-3](#)
 Windows installations, [A-10](#)

H

hackers
 See security attacks
 how it works, [6-3](#)
 HS_ADMIN_EXECUTE_ROLE role
 about, [4-40](#)
 HS_ADMIN_ROLE role
 about, [4-40](#)
 HS_ADMIN_SELECT_ROLE role
 about, [4-40](#)
 HTTP authentication
 See access control lists (ACL), wallet access
 HTTP protocol messages, auditing, [30-75](#)
 HTTP verifier removal, [A-7](#)
 HTTPS
 port, correct running on, [A-19](#)

I

IMP_FULL_DATABASE role
 about, [4-40](#)
 inactive user accounts, locking automatically, [3-9](#)
 INACTIVE_ACCOUNT_TIME profile parameter, [3-9](#)
 indexed data
 encryption, [18-4](#)

indirectly granted roles, [4-35](#)

INHERIT ANY PRIVILEGES privilege

- about, [9-6](#)
- managing, [9-8](#)
- revoking from powerful users, [9-7](#)
- when it should be granted, [9-7](#)

INHERIT ANY REMOTE PRIVILEGES, [9-22](#)

INHERIT PRIVILEGES privilege

- about, [9-6](#)
- auditing, [9-8](#)
- managing, [9-8](#)
- when it should be granted, [9-6](#)

INHERIT REMOTE PRIVILEGES

- about, [9-22](#)

initial ticket, defined, [24-17](#)

initialization parameter file

- parameters for clients and servers using Kerberos, [24-6](#)
- parameters for clients and servers using RADIUS, [26-7](#)

initialization parameters

- application protection, [12-29](#)
- MAX_ENABLED_ROLES, [4-107](#)
- OS_ROLES, [4-53](#)
- SEC_MAX_FAILED_LOGIN_ATTEMPTS, [12-31](#)
- SEC_RETURN_SERVER_RELEASE_BANNER, [12-32](#)
- SEC_USER_AUDIT_ACTION_BANNER, [12-32](#)
- SEC_USER_UNAUTHORIZED_ACCESS_BANNER, [12-32](#)

INSERT privilege

- granting, [4-97](#)
- revoking, [4-100](#)

installation

- guidelines for security, [A-13](#)

intruders

- See security attacks

invoker's rights

- about, [9-3](#)
- code based access control
 - about, [9-11](#)
 - granting and revoking roles to program unit, [9-16](#)
 - how code based access control works, [9-12](#)
 - tutorial, [9-17](#)
- compared with definer's rights, [9-1](#)
- controlled step-in, [9-3](#)
- procedure privileges, used with, [9-2](#)
- procedure security, [9-3](#)
- secure application roles, [12-23](#)
- secure application roles, requirement for enabling, [12-23](#)
- security risk, [9-5](#)
- views
 - about, [9-9](#)

invoker's rights (*continued*)

- views (*continued*)
 - finding user who invoked invoker's right view, [9-10](#)

IP addresses

- falsifying, [A-15](#)

J

Java Debug Wire Protocol (JDWP)

- network access for debugging operations, [10-22](#)

Java schema objects

- auditing, [30-11](#)

Java stored procedures

- network access for debugging operations, [10-22](#)

JAVA_ADMIN role, [4-40](#)

JAVA_RESTRICT initialization parameter

- security guideline, [A-11](#)

java.security file, [C-4](#)

JAVADEBUGPRIV role, [4-40](#)

JVAIDPRIV role, [4-40](#)

JAVASYSPRIV role, [4-40](#)

JVAUSERPRIV role, [4-40](#)

JDBC connections

- JDBC Thin Driver proxy authentication
 - configuring, [3-73](#)
 - with real user, [3-77](#)
- JDBC/OCI proxy authentication, [3-73](#)
 - multiple user sessions, [3-77](#)
 - Oracle Virtual Private Database, [14-52](#)

JDeveloper

- debugging using Java Debug Wire Protocol, [10-22](#)

JMXSERVER role, [4-40](#)

K

Kerberos, [22-4](#)

- authentication adapter utilities, [24-18](#)
- authentication fallback behavior, [24-28](#)
- authentication in Oracle Database, [24-6](#)
- components, [24-2](#)
- configuring authentication, [24-9](#), [24-12](#)
- configuring for database server, [24-10](#)
- configuring for Windows Server Domain Controller KDC, [24-22](#)
- connecting to database, [24-22](#)
- how Oracle Database works with, [24-5](#)
- interoperability with Windows Server Domain Controller KDC, [24-23](#)
- Kerberos server (KDC), [24-4](#)
- kinstance, [24-10](#)
- kservice, [24-10](#)
- Oracle Database parameters, [24-6](#)

Kerberos (*continued*)

- realm, [24-10](#)
- sqlnet.ora file sample, [20-5](#)
- system requirements, [22-7](#)
- tickets
 - client service ticket, [24-4](#)
 - client ticket granting ticket, [24-3](#)
- Kerberos authentication, [3-66](#)
 - configuring for SYSDBA or SYSOPER
 - access, [3-54](#)
 - password management, [A-7](#)
- Kerberos Key Distribution Center (KDC), [24-22](#)
- key generation
 - encryption, [18-5](#)
- key storage
 - encryption, [18-6](#)
- key transmission
 - encryption, [18-5](#)
- kinstance (Kerberos), [24-10](#)
- krb5.conf
 - configuring TCP or UDP connection, [24-16](#)
- kservice (Kerberos), [24-10](#)

L

large objects (LOBs)

- about securing, [12-20](#)
- encryption management, [12-20](#)
- LBAC_DBA role, [4-40](#)
- LBACSYS schema
 - ORA_DV_SCHEMA_CHANGES predefined
 - audit policy for, [29-13](#)
- LBACSYS user account, [2-39](#)
- LBACSYS.ORA_GET_AUDITED_LABEL function
 - about, [30-70](#)
- ldap.ora
 - which directory SSL port to use for no
 - authentication, [21-48](#)
- ldap.ora file
 - about, [6-15](#)
 - benefit of, [6-15](#)
 - changing contents of, [6-15](#)
 - compared with dsi.ora, [6-10](#)
 - creating for Microsoft Active Directory
 - services, [6-13](#), [6-16](#)
 - placement of, [6-15](#)
 - search order for, [6-15](#)
- least privilege principle, [A-3](#)
 - about, [A-3](#)
 - granting user privileges, [A-3](#)
 - middle-tier privileges, [3-78](#)
- libraries
 - auditing, [30-11](#)
- lightweight users
 - example using a global application context,
 - [13-44](#)

lightweight users (*continued*)

- Lightweight Directory Access Protocol (LDAP), [14-36](#)
- listener
 - not an Oracle owner, [A-15](#)
 - preventing online administration, [A-15](#)
 - restrict privileges, [A-15](#)
 - secure administration, [A-15](#)
- listener.ora file
 - administering remotely, [A-15](#)
 - default location, [A-19](#)
 - online administration, preventing, [A-15](#)
 - TCPS, securing, [A-19](#)
- lists data dictionary
 - data dictionary views
 - See views
 - granting privileges and roles
 - finding information about, [4-110](#)
 - privileges, [4-18](#)
 - finding information about, [4-110](#)
 - roles, [12-23](#)
 - finding information about, [4-110](#)
 - views, [4-110](#)
 - privileges, [4-82](#), [4-110](#)
 - roles, [4-110](#)
- LOB_SIGNATURE_ENABLE initialization
 - parameter, [12-20](#)
- LOBs
 - about securing, [12-20](#)
 - encryption management, [12-20](#)
- local privilege grants
 - about, [4-29](#)
 - granting, [4-31](#)
 - revoking, [4-31](#)
- local privileges
 - granting, [4-5](#)
- local roles, [4-5](#), [4-62](#)
 - about, [4-59](#)
 - creating, [4-62](#)
 - granting, [4-5](#)
 - rules for creating, [4-61](#)
- local user accounts
 - creating, [2-16](#)
- local users
 - about, [2-5](#)
- lock and expire
 - default accounts, [A-3](#)
 - predefined user accounts, [A-3](#)
- lockdown profiles
 - example, [4-64](#)
- lockdown profiles, PDB, [4-64](#)
- locking inactive user accounts automatically, [3-9](#)
- log files
 - owned by trusted user, [A-11](#)
- logical reads limit, [2-24](#)

logon triggers
 externally initialized application contexts,
 [13-15](#)
 for application context packages, [13-15](#)
 running database session application context
 package, [13-15](#)
 secure application roles, [4-57](#)
 LOGSTDBY_ADMINISTRATOR role, [4-40](#)

M

malicious database administrators, [18-3](#)
 See also security attacks
 manager default password, [A-7](#)
 managing roles with RADIUS server, [26-19](#)
 materialized views
 auditing, [30-11](#)
 MD5 message digest algorithm, [20-6](#)
 MDDATA user account, [2-42](#)
 MDSYS user account, [2-39](#)
 memory
 users, viewing, [2-46](#)
 MERGE INTO statement, affected by
 DBMS_RLS.ADD_POLICY
 statement_types parameter, [14-11](#)
 metadata links
 privilege management, [4-77](#)
 methods
 privileges on, [4-87](#)
 Microsoft Active Directory services, [6-3](#), [6-4](#), [6-6](#),
 [6-7](#), [6-16](#), [6-19](#), [6-20](#)
 about configuring connection, [6-19](#)
 about password authentication, [6-24](#)
 access configuration, Oracle wallet
 verification, [6-22](#)
 access configuration, testing integration, [6-23](#)
 access, Kerberos authentication, [6-29](#)
 access, PKI authentication, [6-30](#)
 account policies, [6-38](#)
 administrative user configuration, exclusive
 mapping, [6-34](#)
 administrative user configuration, shared
 access accounts, [6-34](#)
 dsi.ora file, about, [6-11](#)
 dsi.ora file, compared with ldap.ora, [6-10](#)
 extending Active Directory schema, [6-8](#)
 ldap.ora file, about, [6-15](#)
 ldap.ora file, compared with dsi.ora, [6-10](#)
 ldap.ora file, creating, [6-13](#), [6-16](#)
 logon user name with password
 authentication, [6-27](#)
 multitenant users, how affected, [6-5](#)
 user authorization, about, [6-31](#)
 user authorization, mapping Directory user
 group to global role, [6-32](#)
 user authorization, verifying, [6-35](#)

Microsoft Active Directory services (*continued*)
 user management, altering mapping
 definition, [6-33](#)
 user management, exclusively mapping
 Directory user to database global
 user, [6-33](#)
 user management, mapping group to shared
 global user, [6-32](#)
 user management, migrating mapping
 definition, [6-33](#)
 Microsoft Active Directory services integration,
 [6-2](#), [6-3](#), [6-5](#)
 Microsoft Active Directory services proxy
 authentication, [6-29](#)
 about, [6-28](#)
 configuring, [6-28](#)
 Microsoft Directory Access services, [6-22](#)
 Microsoft Entra ID token
 checking version of, [8-48](#)
 Microsoft Windows
 Kerberos
 configuring for Windows Server Domain
 Controller KDC, [24-22](#)
 middle-tier systems
 client identifiers, [3-82](#)
 enterprise user connections, [3-81](#)
 password-based proxy authentication, [3-80](#)
 privileges, limiting, [3-78](#)
 proxies authenticating users, [3-79](#)
 proxying but not authenticating users, [3-79](#)
 reauthenticating user to database, [3-80](#)
 USERENV namespace attributes, accessing,
 [13-22](#)
 mining models
 auditing, [30-11](#)
 mkstore utility
 create command, [B-48](#)
 createALO command, [B-49](#)
 createCredential command, [B-49](#)
 createEntry command, [B-50](#)
 createUserCredential command, [B-50](#)
 delete command, [B-51](#)
 deleteCredential command, [B-51](#)
 deleteEntry command, [B-52](#)
 deleteSSO command, [B-52](#)
 deleteUserCredential command, [B-53](#)
 list command, [B-53](#)
 listCredential command, [B-54](#)
 modifyCredential command, [B-54](#)
 modifyEntry command, [B-55](#)
 modifyUserCredential command, [B-55](#)
 SQL*Loader object store credentials, [3-47](#)
 viewEntry command, [B-56](#)
 monitoring user actions, [28-1](#)
 See also auditing, standard auditing, fine-
 grained auditing

multiplex multiple-client network sessions, [A-15](#)
 multitenant container database (CDB)
 See CDBs
 multitenant option
 centrally managed users, how affected, [6-5](#)
 My Oracle Support, [A-2](#)
 security patches, downloading, [A-2](#)
 user account for logging service requests,
 [2-42](#)

N

native network encryption
 checking if enabled in current session, [20-16](#)
 compared with Transport Layer Security, [20-2](#)
 FIPS library location setting (SSLFIPS_LIB),
 [C-9](#)
 FIPS mode setting (FIPS_140), [C-9](#)
 troubleshooting, [20-16](#)
 native network encryption and integrity
 how it works, [20-2](#)
 native network encryption
 disabling, [27-2](#)
 Net8
 See Oracle Net
 network authentication
 guidelines for securing, [A-7](#)
 roles, granting using, [4-103](#)
 smart cards, [A-7](#)
 token cards, [A-7](#)
 X.509 certificates, [A-7](#)
 network connections
 denial-of-service (DoS) attacks, addressing,
 [A-15](#)
 guidelines for security, [A-14](#), [A-15](#)
 securing, [A-15](#)
 network encryption
 about, [20-7](#)
 configuring, [20-7](#)
 troubleshooting, [20-16](#)
 network IP addresses
 guidelines for security, [A-15](#)
 network native encryption
 FIPS-supported algorithms, [C-7](#)
 network traffic encryption, [A-15](#)
 nondatabase users, [13-28](#), [13-29](#)
 about, [13-29](#)
 auditing, [30-88](#)
 clearing session data, [13-39](#)
 creating client session-based application
 contexts, [13-52](#)
 global application contexts
 package example, [13-37](#)
 reason for using, [13-29](#)
 setting, [13-36](#)
 tutorial, [13-44](#)

nondatabase users (*continued*)
 One Big Application User authentication
 about, [14-52](#)
 features compromised by, [12-2](#)
 security risks, [12-2](#)
 Oracle Virtual Private Database
 how it works with, [14-52](#)
 tutorial for creating a policy group, [14-38](#)
 See also application contexts, client identifiers

O

object privileges, [4-72](#), [A-3](#)
 about, [4-72](#)
 granting on behalf of the owner, [4-95](#)
 managing, [12-27](#)
 revoking, [4-98](#)
 revoking on behalf of owner, [4-99](#)
 schema object privileges, [4-72](#)
 synonyms, [4-75](#)
 with common privilege grants, [4-30](#)
 See also schema object privileges
 object types
 auditing, [30-11](#)
 objects
 applications, managing privileges in, [12-27](#)
 granting privileges, [12-28](#)
 privileges
 applications, [12-28](#)
 managing, [4-87](#)
 protecting in shared schemas, [12-27](#)
 protecting in unique schemas, [12-26](#)
 SYS schema, access to, [4-20](#)
 OEM_ADVISOR role, [4-40](#)
 OEM_MONITOR role, [4-40](#)
 OGG_APPLY role, [4-40](#)
 OGG_APPLY_PROCREP role, [4-40](#)
 OGG_SHARED_CAPTURE role, [4-40](#)
 OJMSYS user account, [2-39](#)
 okcreate
 Kerberos adapter utility, [24-18](#)
 okcreate options, [24-21](#)
 okdstry
 Kerberos adapter utility, [24-18](#)
 okdstry options, [24-21](#)
 okinit
 Kerberos adapter utility, [24-18](#)
 okinit utility options, [24-18](#)
 oklist
 Kerberos adapter utility, [24-18](#)
 OLAPSYS user account, [2-39](#)
 One Big Application User authentication
 See nondatabase users
 operating system
 audit files written to, [32-7](#)

- operating system users
 - configuring for PDBs, [3-62](#)
 - setting default credential, [3-63](#)
- operating systems, [3-62](#)
 - accounts, [4-104](#)
 - authentication
 - about, [3-65](#)
 - advantages, [3-65](#)
 - disadvantages, [3-65](#)
 - operating system user for PDB, [3-62](#)
 - roles, using, [4-103](#)
 - default permissions, [A-11](#)
 - enabling and disabling roles, [4-105](#)
 - operating system account privileges, limiting, [A-11](#)
 - role identification, [4-104](#)
 - roles and, [4-40](#)
 - roles, granting using, [4-103](#)
 - users, limiting number of, [A-11](#)
- OPTIMIZER_PROCESSING_RATE role, [4-40](#)
- ORA_ACCOUNT_MGMT predefined unified audit policy, [29-7](#)
- ORA_ALL_TOPLEVEL_ACTIONS predefined unified audit policy, [29-10](#)
- ORA_CIS_RECOMMENDATIONS predefined unified audit policy, [29-8](#)
- ORA_DATABASE_PARAMETER predefined unified audit policy, [29-7](#)
- ORA_DV_DEFAULT_PROTECTION predefined unified audit policy, [29-13](#)
- ORA_DV_SCHEMA_CHANGES predefined unified audit policy, [29-13](#)
- ORA_LOGIN_LOGOUT predefined unified audit policy, [29-10](#)
- ORA_OLS_SCHEMA_CHANGES predefined unified audit policy, [29-14](#)
- ORA_SECURECONFIG predefined unified audit policy, [29-6](#)
- ORA_STIG_PROFILE profile, [3-26](#)
- ORA_STIG_RECOMMENDATIONS predefined unified audit policy, [29-9](#)
- ORA-01017 errors in Oracle Cloud Infrastructure-IAM integration, [7-41](#)
- ORA-01017 errors in Oracle DBaaS-IAM integration
 - client-side, [7-38](#)
 - IAM administrator actions to remedy, [7-43](#)
 - IAM user configurations, [7-42](#)
- ORA-01720 error, [4-82](#)
- ORA-01741 error, [31-6](#)
- ORA-01994, [2-21](#)
- ORA-03114 error, [7-43](#), [8-47](#)
- ORA-06512 error, [10-22](#), [31-16](#)
- ORA-06598 error, [9-6](#)
- ORA-12008 error, [31-6](#)
- ORA-12599 error, [7-43](#), [8-47](#)
- ORA-1536 error, [2-11](#)
- ORA-24247 error, [10-3](#), [10-22](#), [31-16](#)
- ORA-28017 error, [2-21](#)
- ORA-28040 error, [3-37](#), [3-57](#)
- ORA-28046 error, [2-21](#)
- ORA-28575 error, [12-18](#)
- ORA-29024 error, [10-13](#)
- ORA-45622 errors, [15-12](#)
- ORA-64219: invalid LOB locator encountered, [12-20](#)
- ORA\$DEPENDENCY profile, [5-4](#)
- ORA\$DICTIONARY_SENS_COL_ACCESS predefined unified audit policy, [29-11](#)
- Oracle Advanced Security
 - checksum sample for sqlnet.ora file, [20-5](#)
 - encryption sample for sqlnet.ora file, [20-5](#)
 - network authentication services, [A-7](#)
 - TLS features, [25-1](#)
 - user access to application schemas, [12-27](#)
- Oracle Audit Vault and Database Firewall
 - schema-only accounts, [3-60](#)
- Oracle Autonomous Database
 - centrally managed users, [6-38](#)
- Oracle Call Interface (OCI)
 - application contexts, client session-based, [13-52](#)
 - proxy authentication, [3-73](#)
 - Oracle Virtual Private Database, how it works with, [14-52](#)
 - proxy authentication with real user, [3-77](#)
 - security-related initialization parameters, [12-29](#)
- Oracle Connection Manager
 - securing client networks with, [A-15](#)
- Oracle Data Guard
 - gradual database password rollover, [3-24](#)
 - SYSDG administrative privilege, [4-16](#)
- Oracle Data Pump
 - audit events, [30-71](#)
 - exported data from VPD policies, [14-48](#)
 - exports during gradual database password rollover, [3-24](#)
 - unified audit trail, [32-9](#)
- Oracle Database Enterprise User Security
 - password security threats, [3-34](#)
- Oracle Database Real Application Clusters
 - archive timestamp for audit records, [32-15](#)
 - global contexts, [13-28](#)
- Oracle Database Real Application Security
 - ALL audit events, [30-62](#)
 - auditing, [30-56](#)
 - security class and ACL audit events, [30-59](#)
 - session audit events, [30-60](#)
 - user, privilege, and role audit events, [30-58](#)
- Oracle Database Vault
 - auditing, [30-47](#)

- Oracle Database Vault (*continued*)
 - command rules, audit events, [30-51](#)
 - Data Pump, audit events, [30-53](#)
 - enable and disable, audit events, [30-54](#)
 - factors, audit events, [30-51](#)
 - OLS, audit events, [30-53](#)
 - realms, audit events, [30-49](#)
 - rule sets and rules, audit events, [30-50](#)
 - secure application roles, audit events, [30-52](#)
- Oracle Database-to-Entra ID authorizations
 - disabling, [8-17](#)
 - enabling, [8-16](#)
- Oracle Database-to-IAM
 - trace files for client side, [8-47](#)
- Oracle Database-to-Microsoft Azure Active Directory client connections
 - network proxies, [8-37](#)
- Oracle Database-to-Microsoft Azure Entra ID
 - creating Entra ID app roles, [8-14](#)
- Oracle Database-to-Microsoft Entra ID
 - about, [8-2](#)
 - architecture, [8-4](#)
 - assigning app role to service principal, [8-15](#)
 - assigning users and groups to Entra ID app roles, [8-15](#)
 - configuring v2 tokens, [8-13](#)
 - Entra ID token, checking version of, [8-48](#)
 - exclusive mapping between database schema and Azure user, [8-18](#)
 - mapping Oracle roles with Entra ID roles, [8-19](#)
 - on-premises requirements, [8-8](#)
 - operational flow, [8-21](#)
 - Oracle schema-to-Entra ID application role mapping, [8-18](#)
 - registering database instance to Microsoft Azure tenancy, [8-9](#)
 - trace files for client, levels, [8-46](#)
 - trace files for client, setting, [8-47](#)
 - use cases, [8-6](#)
 - user and group mappings, [8-5](#), [8-7](#)
- Oracle Database-to-Microsoft Entra ID client connections
 - about, [8-20](#)
 - confidential client registration, [8-25](#)
 - configuring to work with Entra ID token, [8-27](#)
 - creating a client app registration, [8-25](#)
 - direct token retrievals, [8-28](#)
 - enabling client to retrieve token from file location, [8-33](#)
 - example using Python script for MSAL library, [8-35](#)
 - examples of retrieving OAuth2 tokens, [8-34](#)
 - net naming for Azure, [8-41](#)
 - net naming for IAM, [7-22](#)
 - network proxy for default database, [8-39](#)
- Oracle Database-to-Microsoft Entra ID client connections (*continued*)
 - network proxy for Oracle Real Application Clusters, [8-39](#)
 - network proxy for Windows, [8-40](#)
 - public client registration, [8-25](#)
 - requesting tokens using Azure CLI, [8-36](#)
 - retrieving token using Entra ID CLI, [8-35](#)
 - secrets for Azure, [8-41](#)
 - secrets for IAM, [7-22](#)
 - supported drivers, [8-24](#)
 - testing Azure endpoint accessibility, [8-37](#)
- Oracle DBaaS client connections
 - supported drivers, [7-22](#)
- Oracle DBaaS-to-Entra ID proxy authentication
 - about, [8-41](#)
 - configuring, [8-42](#)
 - validating, [8-42](#)
- Oracle DBaaS-to-IAM
 - about, [7-2](#), [7-22](#)
 - about token requests using passwords or SEPS, [7-23](#)
 - architecture, [7-4](#)
 - cross-tenancy access examples, [7-35](#)
 - cross-tenancy, about, [7-32](#)
 - database clients for cross-tenancy access, [7-37](#)
 - parameters for setting password or SEPS token requests, [7-24](#)
 - requesting cross-tenancy tokens, [7-37](#)
 - trace files for client side, [7-40](#)
 - troubleshooting client side, [7-40](#)
- Oracle DBaaS-to-IAM authorizations
 - about, [7-10](#)
 - altering, [7-13](#)
 - creating IAM database password, [7-20](#)
 - creating policies for authenticating users, [7-19](#)
 - enabling, [7-8](#)
 - IAM group to database global role, [7-12](#)
 - IAM user to database global user, [7-12](#)
 - instance principals, [7-13](#)
 - mapping schemas and roles to users and groups in another tenancy, [7-36](#)
 - migrating, [7-13](#)
 - resource principals, [7-13](#)
 - shared database global user, [7-11](#)
 - source user tenancy, [7-34](#)
 - target database resource tenancy, [7-34](#)
 - token requested by IAM user name and password, [7-27](#)
 - token requested by IAM user name and secure external password store (SEPS), [7-26](#)
 - user authorization, verifying, [7-14](#)
- Oracle DBaaS-to-IAM client connections
 - IAM token, [7-30](#)
 - password verifier, [7-23](#)

- Oracle DBaaS-to-IAM client connections (*continued*)
 - SQL*Plus using an IAM database password, [7-29](#)
 - token, [7-27](#)
- Oracle DBaaS-to-IAM connections
 - about, [7-8](#)
 - connection pools using instance or resource principals, [7-20](#)
 - database links, [7-37](#)
 - direct token retrievals, [7-28](#)
 - walletless connections, [7-28](#)
- Oracle DBaaS-to-IAM proxy authentication
 - about, [7-17](#)
 - configuring, [7-18](#)
 - validating, [7-18](#)
- Oracle DBaaS-to-Power BI SSO
 - about, [8-43](#)
- Oracle Developer Tools For Visual Studio (ODT)
 - debugging using Java Debug Wire Protocol, [10-22](#)
- Oracle E-Business Suite
 - schema-only accounts, [3-60](#)
- Oracle Enterprise Manager
 - PDBs, [11-1](#)
 - statistics monitor, [2-25](#)
- Oracle Flashback Data Archive
 - Oracle Virtual Private Database, [14-49](#)
- Oracle home
 - default permissions, disallowing modification, [A-11](#)
- Oracle Internet Directory
 - Diffie-Hellman TLS port, [21-48](#)
- Oracle Internet Directory (OID)
 - SYSDBA and SYSOPER access, controlling, [3-52](#)
 - Transport Layer Security authentication, [25-2](#)
- Oracle Java Virtual Machine
 - JAVA_RESTRICT initialization parameter
 - security guideline, [A-11](#)
- Oracle Java Virtual Machine (OJVM)
 - permissions, restricting, [A-3](#)
- Oracle Label Security
 - audit events, [30-66](#)
 - auditing, [30-65](#)
 - auditing internal predicates in policies, [30-16](#)
 - user session label audit events, [30-68](#)
- Oracle Label Security (OLS)
 - Oracle Virtual Private Database, using with, [14-47](#)
- Oracle Machine Learning for SQL
 - audit events, [30-77](#)
- Oracle native encryption
 - configured with SSL authentication, [20-15](#)
- Oracle Net, [A-15](#)
 - firewall support, [A-15](#)
- Oracle parameters
 - authentication, [27-5](#)
- Oracle RAC
 - Transport Layer Security, [21-54](#)
- Oracle Real Application Clusters
 - components that need certificates, [21-56](#)
 - global application contexts, [13-30](#)
 - SYSRAC administrative privilege, [4-17](#)
- Oracle Real Application Security
 - auditing internal predicates in policies, [30-16](#)
- Oracle Recovery Manager
 - audit events, [30-64](#)
 - auditing, [30-63](#)
 - SYSBACKUP administrative privilege, [4-14](#)
- Oracle Scheduler
 - sensitive credential data
 - about, [16-1](#)
 - data dictionary views, [16-6](#)
 - deleting, [16-4](#)
 - encrypting, [16-2](#)
 - multitenant environment, [16-2](#)
 - rekeying, [16-3](#)
 - restoring functioning of lost keystore, [16-5](#)
- Oracle SQL*Loader
 - Direct Load Path audit events, [30-73](#)
- Oracle Technology Network
 - security alerts, [A-2](#)
- Oracle Virtual Private Database, [14-2](#)
 - exporting data using Data Pump Export, [14-48](#)
 - Oracle Flashback Data Archive, [14-49](#)
- Oracle Virtual Private Database (VPD), [14-3](#)
 - about, [14-2](#)
 - ANSI operations, [14-45](#)
 - application containers, [14-5](#)
 - application contexts
 - tutorial, [14-31](#)
 - used with, [14-4](#)
 - applications
 - how it works with, [14-45](#)
 - users who are database users, how it works with, [14-52](#)
 - applications using for security, [12-3](#)
 - automatic reparsing, how it works with, [14-46](#)
 - benefits, [14-3](#)
 - CDBs, [14-5](#)
 - column level, [14-12](#)
 - column masking behavior
 - enabling, [14-14](#)
 - restrictions, [14-15](#)
 - column-level display, [14-12](#)
 - components, [14-6](#)
 - configuring, [14-8](#)
 - cursors, shared, [14-4](#)
 - edition-based redefinitions, [14-44](#)
 - editions, results in, [13-32](#)

Oracle Virtual Private Database (VPD) *(continued)*

- Enterprise User Security proxy authentication,
 - how it works with, [14-52](#)
- exporting data, [14-47](#)
- extended data objects in views, [14-10](#)
- finding information about, [14-53](#)
- flashback query, how it works with, [14-46](#)
- function
 - components, [14-6](#)
 - how it is run, [14-4](#)
- JDBC proxy authentication, how it works with, [14-52](#)
- JSON, [14-53](#)
- nondatabase user applications, how works with, [14-52](#)
- OCI proxy authentication, how it works with, [14-52](#)
- Oracle Label Security
 - exceptions in behavior, [14-47](#)
 - using with, [14-47](#)
- outer join operations, [14-45](#)
- performance benefit, [14-3](#)
- policies, Oracle Virtual Private Database
 - about, [14-9](#)
 - applications, validating, [14-18](#)
 - attaching to database object, [14-10](#)
 - column display, [14-12](#)
 - column-level display, default, [14-13](#)
 - dynamic, [14-20](#)
 - multiple, [14-18](#)
 - optimizing performance, [14-20](#)
 - privileges used to run, [14-4](#)
 - SQL statements, specifying, [14-11](#)
- policy groups
 - about, [14-16](#)
 - benefits, [14-16](#)
 - creating, [14-17](#)
 - default, [14-17](#)
 - tutorial, implementation, [14-38](#)
- policy types
 - context sensitive, about, [14-23](#)
 - context sensitive, altering existing policy, [14-25](#)
 - context sensitive, creating, [14-24](#)
 - context sensitive, refreshing, [14-24](#)
 - context sensitive, restricting evaluation, [14-23](#)
 - context sensitive, when to use, [14-26](#)
 - context-sensitive, audited, [30-18](#)
 - DYNAMIC, [14-20](#)
 - dynamic, audited, [30-18](#)
 - shared context sensitive, about, [14-25](#)
 - shared context sensitive, when to use, [14-26](#)
 - shared static, about, [14-22](#)
 - shared static, when to use, [14-23](#)

Oracle Virtual Private Database (VPD) *(continued)*

- policy types *(continued)*
 - static, about, [14-21](#)
 - static, audited, [30-18](#)
 - static, when to use, [14-23](#)
 - summary of features, [14-26](#)
 - privileges required to create policies, [14-4](#)
 - SELECT FOR UPDATE statements in
 - policies, [14-45](#)
 - tutorial, simple, [14-28](#)
 - user models, [14-52](#)
 - Web-based applications, how it works with, [14-52](#)
- ## Oracle Virtual Private Database (VPD)
- predicates
 - audited in fine-grained audit policies, [31-4](#)
 - audited in unified audit policies, [30-16](#)
- ## Oracle wallets
- authentication method, [3-66](#)
 - search order for TLS, [21-30](#)
- ## ORACLE_DATAPUMP access driver
- guidelines for security, [A-12](#)
- ## ORACLE_OCM user account, [2-42](#)
- ## OracleMetaLink
- See My Oracle Support
- ## orapki
- running in FIPS mode, [C-3](#)
- ## orapki utility
- adding a certificate request to a wallet with, [B-15](#)
 - adding a root certificate to a wallet with, [B-19](#)
 - adding a trusted certificate to a wallet with, [B-19](#)
 - adding certificate to wallet, [B-22](#)
 - adding user certificates to a wallet with, [B-20](#)
 - adding user-supplied certificate to wallet, [B-22](#)
 - cert create command, [B-28](#)
 - cert display command, [B-28](#)
 - certificate revocation lists, [21-47](#)
 - changing the wallet password with, [B-12](#)
 - converting wallet to use AES256 algorithm, [B-13](#)
 - creating a local auto-login wallet with, [B-11](#)
 - creating a wallet with, [B-10](#)
 - creating an auto-login only wallet with, [B-11](#)
 - creating an auto-login wallet with, [B-11](#)
 - creating SHA-2 certificates for testing, [B-17](#)
 - creating signed certificates for testing, [B-16](#)
 - crl delete command, [B-29](#)
 - crl display command, [B-29](#)
 - crl hash command, [B-30](#)
 - crl list command, [B-31](#)
 - crl upload command, [B-31](#)
 - examples, [B-23](#)
 - exporting a certificate from a wallet with, [B-22](#)

orapki utility (*continued*)

- exporting a certificate request from a wallet with, [B-22](#)
 - importing a wallet with, [B-10](#)
 - managing certificate revocation lists, [B-23](#)
 - secretstore create_credential command, [B-32](#)
 - secretstore create_entry command, [B-33](#)
 - secretstore create_user_credential command, [B-33](#)
 - secretstore delete_credential command, [B-34](#)
 - secretstore delete_entry command, [B-34](#)
 - secretstore delete_user_credential command, [B-35](#)
 - secretstore list_credentials command, [B-35](#)
 - secretstore list_entries command, [B-35](#), [B-38](#)
 - secretstore list_entries_unsorted command, [B-36](#)
 - secretstore modify_credential command, [B-36](#)
 - secretstore modify_entry command, [B-37](#)
 - secretstore modify_user_credential command, [B-37](#)
 - syntax, [B-9](#)
 - viewing a certificate with, [B-21](#)
 - viewing a wallet with, [B-12](#)
 - wallet add command, [B-38](#)
 - wallet change_pwd command, [B-41](#)
 - wallet convert command, [B-41](#)
 - wallet create command, [B-42](#)
 - wallet delete command, [B-42](#)
 - wallet display command, [B-43](#)
 - wallet export command, [B-44](#)
 - wallet export_private_key command, [B-44](#)
 - wallet import_pkcs12 command, [B-45](#)
 - wallet import_private_key command, [B-45](#)
 - wallet jks_to_pkcs12 command, [B-46](#)
 - wallet pkcs12_to_jks command, [B-46](#)
 - wallet remove command, [B-47](#)
- ORAPWD utility
- case sensitivity in passwords, [3-32](#)
 - changing SYS password, [2-22](#)
 - changing SYS password with, [2-21](#)
- ORDDATA user account, [2-39](#)
- ORDPLUGINS user account, [2-39](#)
- ORDSYS user account, [2-39](#)
- OS_AUTHENT_PREFIX parameter, [27-6](#)
- OS_ROLES initialization parameter
- operating system role grants, [4-105](#)
 - operating-system authorization and, [4-53](#)
 - REMOTE_OS_ROLES and, [4-105](#)
 - using, [4-104](#)
- OSAK_ADMIN_ROLE role, [4-40](#)
- outer join operations
- Oracle Virtual Private Database affect on, [14-45](#)
- OUTLN user account, [2-39](#)

P

packages

- auditing, [30-11](#), [30-16](#)
- examples, [4-86](#)
- examples of privilege use, [4-86](#)
- granting roles to, [4-55](#)
- privileges
 - divided by construct, [4-85](#)
 - executing, [4-84](#), [4-85](#)
- parallel execution servers, [13-12](#)
- parallel query, and SYS_CONTEXT, [13-12](#)

parameters

- authentication
 - Kerberos, [24-6](#)
 - RADIUS, [26-7](#)
- encryption and checksumming, [20-11](#)

pass phrase

- read and parse server.key file, [A-19](#)

PASSWORD command

- about, [2-20](#)
- changing SYS password with, [2-21](#)

password complexity functions

- about, [3-26](#)
- administrative users, for, [3-51](#)
- customizing, [3-28](#)
- enabling, [3-28](#)
- how database checks password complexity, [3-26](#)
- ora12c_stig_verify_function, [3-27](#)
- ora12c_strong_verify_function, [3-27](#)
- ora12c_verify_function, [3-26](#)
- privileges required, [3-26](#)

password files

- how used to authenticate administrators, [3-55](#)
- migration of for administrative users, [3-50](#)

password limits

- administrative logins, [3-55](#)

password management

- inactive user accounts, locking automatically, [3-9](#)

password versions

- target databases that run earlier releases, [3-38](#)
- using 12C exclusively, [3-37](#)

PASSWORD_LIFE_TIME profile parameter, [3-12](#)

PASSWORD_LOCK_TIME profile parameter, [3-10](#)

PASSWORD_REUSE_MAX profile parameter, [3-11](#)

PASSWORD_REUSE_TIME profile parameter, [3-11](#)

PASSWORD_ROLLOVER_TIME parameter, [3-19](#)

passwords, [3-3](#)

- 10G password version, finding and resetting, [3-30](#)

passwords (*continued*)

- about managing, [3-5](#)
- account locking, [3-10](#)
- administrator
 - authenticating with, [3-55](#)
 - guidelines for securing, [A-7](#)
- aging and expiration, [3-12](#)
- ALTER PROFILE statement, [3-5](#)
- altering, [2-19](#)
- application design guidelines, [12-8](#)
- applications, strategies for protecting
 - passwords, [12-7](#)
- brute force attacks, [3-3](#)
- changing for roles, [4-51](#)
- changing SYS with ORAPWD utility, [2-22](#)
- complexity verification
 - about, [3-26](#)
- complexity, guidelines for enforcing, [A-7](#)
- compromised, how to handle, [3-23](#)
- connecting without, [3-65](#)
- CREATE PROFILE statement, [3-5](#)
- danger in storing as clear text, [A-7](#)
- database user authentication, [3-57](#)
- default profile settings
 - about, [3-7](#)
- default user account, [A-7](#)
- default, finding, [3-6](#)
- delays for incorrect passwords, [3-3](#)
- duration, [A-7](#)
- encrypting, [3-3](#), [A-7](#)
- examples of creating, [3-4](#)
- expiring
 - explicitly, [3-13](#)
 - procedure for, [3-12](#)
 - proxy account passwords, [3-76](#)
 - with grace period, [3-13](#)
- failed logins, resetting, [3-10](#)
- finding users who use old passwords, [3-24](#)
- forcing oracle user to enter when logging in as
 - SYSDBA, [4-14](#)
- grace period, example, [3-13](#)
- gradual database rollover, [3-17](#)
- guidelines for security, [A-7](#)
- history, [3-11](#), [A-7](#)
- Java code example to read passwords, [12-11](#)
- length, [A-7](#)
- life time set too low, [3-15](#)
- lifetime for, [3-12](#)
- lock time, [3-10](#)
- management rules, [A-7](#)
- managing, [3-4](#)
- maximum reuse time, [3-11](#)
- ORAPWD utility, [3-32](#)
- password complexity verification, [3-26](#)
 - how database checks, [3-26](#)
 - ora12c_stig_verify_function, [3-27](#)

passwords (*continued*)

- password complexity verification (*continued*)
 - ora12c_verify_function function, [3-26](#)
 - privileges required, [3-26](#)
- password file risks, [3-56](#)
- PASSWORD_LOCK_TIME profile parameter, [3-10](#)
- PASSWORD_REUSE_MAX profile
 - parameter, [3-11](#)
- PASSWORD_REUSE_TIME profile
 - parameter, [3-11](#)
- policies, [3-4](#)
- privileges for changing for roles, [4-51](#)
- privileges to alter, [2-18](#)
- protections, built-in, [3-3](#)
- proxy authentication, [3-80](#)
- requirements
 - additional, [A-7](#)
 - minimum, [3-4](#)
- reusing, [3-11](#), [A-7](#)
- reusing passwords, [3-11](#)
- role password case sensitivity, [3-29](#)
- roles authenticated by passwords, [4-48](#)
- roles enabled by SET ROLE statement, [4-51](#)
- secure external password store, [3-41](#)
- security risks, [3-56](#)
- SYS account, [2-21](#)
- SYS and SYSTEM, [A-7](#)
- used in roles, [4-36](#)
- utlpwmg.sql password script
 - password management, [3-26](#)
- verified using SHA-512 hash function, [3-37](#)
- versions, management of, [3-30](#)
 - See also authentication, and access control list (ACL), wallet access

PDB lockdown profiles

- about, [4-64](#)
- creating, [4-68](#)
- default, [4-67](#)
- disabling, [4-69](#)
- dropping, [4-71](#)
- enabling, [4-69](#)
- features that benefit from, [4-66](#)
- inheritance, [4-67](#)

PDB_DBA role, [4-40](#)

PDB_OS_CREDENTIAL initialization parameter, [3-62](#), [4-66](#)

PDBs

- application common users
 - about, [2-3](#)
- auditing
 - types of audit settings allowed, [28-9](#)
 - unified audit policy syntax, [30-2](#)
 - what can be audited, [28-1](#)
- CDB common users
 - about, [2-3](#)

PDBs (*continued*)

common roles

- about, [4-59](#)
- creating, [4-61](#)
- granting, [4-62](#)
- how they work, [4-60](#)
- privileges required for management, [4-60](#)
- revoking, [4-62](#)
- rules for creating, [4-60](#)

common users

- accessing data in PDBs, [4-33](#)
- creating, [2-14](#)
- viewing privilege information, [4-32](#)

Enterprise Manager

- about, [11-1](#)
- creating common roles, [11-7](#)
- creating common users, [11-3](#)
- creating local roles, [11-9](#)
- creating local users, [11-5](#)
- dropping common roles, [11-9](#)
- dropping common users, [11-5](#)
- dropping local roles, [11-10](#)
- dropping local users, [11-6](#)
- editing common roles, [11-8](#)
- editing common users, [11-4](#)
- editing local roles, [11-10](#)
- editing local users, [11-6](#)
- logging in, [11-1](#)
- revoking common privilege grants, [11-9](#)
- revoking local privilege grants, [11-11](#)
- switching to different container, [11-2](#)

fine-grained audit policies, [31-4](#)granting privileges and roles, [4-4](#)

local roles

- about, [4-59](#)
- creating, [4-62](#)
- rules for creating, [4-61](#)

local users

- about, [2-5](#)
- creating, [2-16](#)

lockdown profiles, [4-64](#)operating system user configuration, [3-62](#)operating system user for, setting, [3-62](#)privilege analysis, [5-4](#)

privileges

- common, [4-30](#)
- granting, [4-31](#)
- how affected, [4-12](#)
- object, [4-30](#)
- revoking, [4-31](#)
- viewing information about, [4-32](#)

PUBLIC role, [4-60](#)security isolation guideline, [A-14](#)setting default credential, [3-63](#)sqlnet.ora settings, [3-37](#)transparent sensitive data protection, [15-4](#)PDBs (*continued*)

- viewing information about, [4-32](#)
- Virtual Private Database policies, [14-5](#)

performance

- application contexts, [13-2](#)
- auditing, [28-4](#)
- Oracle Virtual Private Database policies, [14-3](#)
- Oracle Virtual Private Database policy types, [14-20](#)
- resource limits and, [2-23](#)

permissions

- default, [A-11](#)
- run-time facilities, [A-3](#)

PGX_SERVER_GET_INFO role, [4-40](#)PGX_SERVER_MANAGE role, [4-40](#)PGX_SESSION_ADD_PUBLISHED_GRAPH role, [4-40](#)PGX_SESSION_COMPILE_ALGORITHM role, [4-40](#)PGX_SESSION_CREATE role, [4-40](#)PGX_SESSION_GET_PUBLISHED_GRAPH role, [4-40](#)PGX_SESSION_MODIFY_MODEL role, [4-40](#)PGX_SESSION_NEW_GRAPH role, [4-40](#)PGX_SESSION_READ_MODEL role, [4-40](#)

PKI

- See public key infrastructure (PKI)

PL/SQL

- roles in procedures, [4-38](#)

PL/SQL packages

- auditing, [30-11](#), [30-16](#)

PL/SQL procedures

- setting application context, [13-10](#)

PL/SQL stored procedures

- network access for debugging operations, [10-22](#)

plaintext data

- defined, [20-2](#)

PMON background process

- application contexts, cleaning up, [13-6](#)

positional parameters

- security risks, [12-10](#)

predefined schema user accounts, [2-38](#)principle of least privilege, [A-3](#)

- about, [A-3](#)

- granting user privileges, [A-3](#)

- middle-tier privileges, [3-78](#)

privilege analysis

- about, [5-2](#)
- accessing reports in Cloud Control, [5-13](#)
- benefits, [5-2](#)
- CDBs, [5-4](#)
- creating, [5-6](#)
- creating role in Cloud Control, [5-15](#)
- data dictionary views, [5-30](#)
- DBMS_PRIVILEGE_CAPTURE PL/SQL package, [5-5](#)

privilege analysis (*continued*)

- disabling, [5-10](#)
- dropping, [5-14](#)
- enabling, [5-9](#)
- examples of creating and enabling, [5-8](#)
- general steps for managing, [5-6](#)
- generating regrant scripts, [5-17](#)
- generating reports
 - about, [5-11](#)
 - in Cloud Control, [5-13](#)
 - using DBMS_PRIVILEGE_CAPTURE.GENERATE_REPORT, [5-12](#)
- generating revoke scripts, [5-16](#)
- logon users, [5-3](#)
- multiple named capture runs, [5-11](#)
- pre-compiled database objects, [5-4](#)
- privilege uses captured, [5-3](#)
- requirements for using, [5-3](#)
- restrictions, [5-3](#)
- revoking and re-granting in Cloud Control, [5-15](#)
- revoking and regranting using scripts, [5-16](#)
- tutorial, [5-22](#)
- tutorial for ANY privileges, [5-18](#)
- tutorial for schema privileges, [5-27](#)
- use cases, [5-2](#)
 - finding application pool privileges, [5-2](#)
 - finding overly privileged users, [5-3](#)

privileges, [4-18](#)

- about, [4-2](#)
- access control lists, checking for external
 - network services, [10-20](#)
- altering
 - passwords, [2-19](#)
 - users, [2-18](#)
- altering role authentication method, [4-51](#)
- applications, managing, [12-21](#)
- auditing use of, [30-6](#)
- auditing, recommended settings for, [A-23](#)
- cascading revokes, [4-101](#)
- column, [4-97](#)
- compiling procedures, [4-85](#)
- creating or replacing procedures, [4-84](#)
- creating users, [2-6](#)
- data links
 - privilege management, [4-77](#)
- diagnostics, [4-28](#)
- dropping profiles, [2-29](#)
- extended data links
 - privilege management, [4-78](#)
- granted locally, [4-6](#)
- granting
 - about, [4-21](#), [4-92](#)
 - examples, [4-86](#)
 - object privileges, [4-73](#), [4-94](#)
 - system, [4-92](#)
 - system privileges, [4-92](#)

privileges (*continued*)

- granting common, [4-6–4-8](#)
- granting in a CDB, [4-4](#)
- grants, listing, [4-112](#)
- grouping with roles, [4-33](#)
- local, [4-5](#)
- managing, [12-27](#)
- metadata links, [4-77](#)
- middle tier, [3-78](#)
- object, [4-72](#), [4-74](#), [12-28](#)
- granting and revoking, [4-73](#)
- on selected columns, [4-100](#)
- procedures, [4-84](#)
 - creating and replacing, [4-84](#)
 - executing, [4-84](#)
 - in packages, [4-85](#)
- READ ANY TABLE system privilege
 - about, [4-75](#)
 - restrictions, [4-75](#)
- READ object privilege, [4-74](#)
- read-only configuration, [4-108](#)
- reasons to grant, [4-11](#)
- revoking privileges
 - about, [4-21](#)
 - object, [4-98](#)
 - object privileges, cascading effect, [4-101](#)
 - object privileges, requirements for, [4-98](#)
 - schema object, [4-73](#)
- revoking system privileges, [4-98](#)
- roles
 - creating, [4-48](#)
 - dropping, [4-55](#)
 - restrictions on, [4-39](#)
- roles, why better to grant, [4-11](#)
- schema grants, listing, [4-112](#)
- schema object, [4-72](#)
 - DML and DDL operations, [4-81](#)
 - packages, [4-85](#)
 - procedures, [4-84](#)
- SELECT system privilege, [4-74](#)
- SQL statements permitted, [12-28](#)
- synonyms and underlying objects, [4-75](#)
- system
 - granting and revoking, [4-21](#)
 - SELECT ANY DICTIONARY, [A-11](#)
- SYSTEM and OBJECT, [A-3](#)
- system privileges
 - about, [4-19](#)
- trigger privileges, [9-2](#)
- used for Oracle Virtual Private Database
 - policy functions, [14-4](#)
- view privileges
 - creating a view, [4-82](#)
 - using a view, [4-83](#)
- views, [4-82](#)

privileges (*continued*)

See also access control list (ACL) and system privileges, privilege captures

procedures

auditing, [30-11](#), [30-16](#)

compiling, [4-85](#)

definer's rights

about, [9-2](#)

roles disabled, [4-38](#)

examples of, [4-86](#)

examples of privilege use, [4-86](#)

granting roles to, [4-55](#)

invoker's rights

about, [9-3](#)

roles used, [4-39](#)

privileges for procedures

create or replace, [4-84](#)

executing, [4-84](#)

executing in packages, [4-85](#)

privileges required for, [4-84](#)

security enhanced by, [9-2](#)

process monitor process (PMON)

cleans up timed-out sessions, [2-25](#)

PRODUCT_USER_PROFILE table

SQL commands, disabling with, [4-57](#)

profile limits

modifying, [3-8](#)

profile parameters

FAILED_LOGIN_ATTEMPTS, [3-7](#)

INACTIVE_ACCOUNT_TIME, [3-7](#), [3-9](#)

PASSWORD_GRACE_TIME, [3-7](#), [3-13](#)

PASSWORD_LIFE_TIME, [3-7](#), [3-13](#), [3-15](#)

PASSWORD_LOCK_TIME, [3-7](#), [3-10](#)

PASSWORD_REUSE_MAX, [3-7](#), [3-11](#)

PASSWORD_REUSE_TIME, [3-7](#), [3-11](#)

PASSWORD_ROLLOVER_TIME, [3-19](#)

profiles, [2-26](#)

about, [2-26](#)

application, [2-29](#)

assigning to user, [2-29](#)

CDB, [2-29](#)

common, [2-29](#)

common mandatory for CDB root, about, [2-30](#)

common mandatory for CDB root, creating, [2-31](#)

common mandatory for CDB root, example, [2-32](#)

creating, [2-28](#)

dropping, [2-29](#)

finding information about, [2-43](#)

finding settings for default profile, [2-45](#)

managing, [2-26](#)

ORA_CIS_PROFILE user profile, [2-27](#)

ORA_STIG_PROFILE user profile, [2-27](#)

privileges for dropping, [2-29](#)

specifying for user, [2-13](#)

profiles (*continued*)

viewing, [2-45](#)

program units

granting roles to, [4-55](#)

PROVISIONER role, [4-40](#)

proxy authentication

about, [3-73](#)

advantages, [3-73](#)

auditing operations, [3-70](#)

auditing users, [30-33](#)

client-to-middle tier sequence, [3-77](#)

creating proxy user accounts, [3-74](#)

middle-tier

authorizing but not authenticating users, [3-79](#)

authorizing to proxy and authenticate users, [3-79](#)

limiting privileges, [3-78](#)

reauthenticating users, [3-80](#)

passwords, expired, [3-76](#)

privileges required for creating users, [3-74](#)

secure external password store, used with, [3-76](#)

security benefits, [3-73](#)

users, passing real identity of, [3-77](#)

proxy user accounts

privileges required for creation, [3-74](#)

PROXY_USERS view, [3-76](#)

pseudo columns

USER, [4-83](#)

public and private key pair, defined, [22-5](#)

public key infrastructure (PKI), [3-66](#), [22-5](#)
about, [3-66](#)

PUBLIC role

about, [4-21](#)

granting and revoking privileges, [4-102](#)

grants to in a CDB, [4-8](#)

procedures and, [4-102](#)

security domain of users, [4-38](#)

PUBLIC role, CDBs, [4-60](#)

PUBLIC_DEFAULT profile

profiles, dropping, [2-29](#)

Q

quotas

tablespace, [2-11](#)

temporary segments and, [2-11](#)

unlimited, [2-12](#)

viewing, [2-45](#)

R

RADIUS, [22-4](#)

accounting, [26-17](#)

asynchronous authentication mode, [26-5](#)

RADIUS (*continued*)

- authentication modes, [26-3](#)
- challenge-response
 - authentication, [26-5](#)
 - user interface, [26-20](#), [26-21](#)
- configuring, [26-9](#)
- database links not supported, [26-1](#)
- initialization parameter file setting, [26-8](#)
- minimum parameters to set, [26-8](#)
- older clients, [26-15](#)
- RADIUS_SECRET parameter, [26-13](#)
- smartcards and, [22-4](#), [26-14](#), [26-20](#)
- SQLNET.AUTHENTICATION_SERVICES
 - parameter, [26-9](#), [26-11](#)
- sqlnet.ora file sample, [20-5](#)
- SQLNET.RADIUS_ALLOW_WEAK_CLIENTS, [26-15](#)
- SQLNET.RADIUS_ALLOW_WEAK_PROTOCOL, [26-15](#)
- SQLNET.RADIUS_ALTERNATE parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_PORT parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_RETRIES
 - parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_TIMEOUT
 - parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_TLS_HOST
 - parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_TLS_PORT
 - parameter, [26-15](#)
- SQLNET.RADIUS_AUTHENTICATION_PORT
 - parameter, [26-13](#)
- SQLNET.RADIUS_AUTHENTICATION_RETRIES
 - parameter, [26-13](#)
- SQLNET.RADIUS_AUTHENTICATION_TIMEOUT
 - parameter, [26-13](#)
- SQLNET.RADIUS_AUTHENTICATION_TLS_HOST
 - parameter, [26-11](#)
- SQLNET.RADIUS_AUTHENTICATION_TLS_PORT
 - parameter, [26-11](#)
- SQLNET.RADIUS_SEND_ACCOUNTING
 - parameter, [26-18](#)
- SQLNET.RADIUS_TRANSPORT_PROTOCOL
 - parameter, [26-11](#)
- synchronous authentication mode, [26-3](#)
- system requirements, [22-7](#)
- RADIUS authentication, [3-67](#)
- RADIUS SQLNET.RADIUS_AUTHENTICATION
 - parameter
 - SQLNET.RADIUS_AUTHENTICATION
 - parameter, [26-11](#)
- RADIUS_SECRET parameter, [26-13](#)
- READ ANY TABLE system privilege
 - about, [4-75](#)
 - restrictions, [4-75](#)

READ object privilege

- about, [4-74](#)
- guideline for using, [A-3](#)
- SQL92_SECURITY initialization parameter, [4-75](#)
- read-only user configuration, [4-108](#)
- reads
 - limits on data blocks, [2-24](#)
- realm (Kerberos), [24-10](#)
- RECOVERY_CATALOG_OWNER_VPD role, [4-40](#)
- RECOVERY_CATALOG_USER role, [4-40](#)
- REDACT_AUDIT transparent sensitive data
 - protection default policy, [15-17](#)
- redo log files
 - auditing committed and rolled back
 - transactions, [A-21](#)
- REFERENCES privilege
 - CASCADE CONSTRAINTS option, [4-100](#)
 - revoking, [4-100](#)
- remote authentication, [A-15](#)
- remote debugging
 - configuring network access, [10-22](#)
- REMOTE_OS_AUTHENT initialization parameter
 - guideline for securing, [A-15](#)
- REMOTE_OS_ROLES initialization parameter
 - OS role management risk on network, [4-105](#)
 - setting, [4-53](#)
- REMOTE_SCHEDULER_AGENT user account, [2-39](#)
- resource limits
 - about, [2-23](#)
 - call level, limiting, [2-24](#)
 - connection time for each session, [2-25](#)
 - CPU time, limiting, [2-24](#)
 - determining values for, [2-25](#)
 - idle time in each session, [2-25](#)
 - logical reads, limiting, [2-24](#)
 - private SGA space for each session, [2-25](#)
 - profiles, [2-26](#)
 - session level, limiting, [2-24](#)
 - sessions
 - concurrent for user, [2-25](#)
 - elapsed connection time, [2-25](#)
 - idle time, [2-25](#)
 - SGA space, [2-25](#)
 - types, [2-23](#)
- RESOURCE privilege
 - CREATE SCHEMA statement, needed for, [12-26](#)
- RESOURCE role, [4-88](#)
 - about, [4-40](#)
- restrictions, [22-8](#)
- REVOKE CONNECT THROUGH clause
 - revoking proxy authorization, [3-76](#)

- REVOKE statement
 - system privileges and roles, [4-98](#)
 - when takes effect, [4-106](#)
- revoking privileges and roles
 - cascading effects, [4-101](#)
 - on selected columns, [4-100](#)
 - REVOKE statement, [4-98](#)
 - specifying ALL, [4-74](#)
 - when using operating-system roles, [4-105](#)
- role identification
 - operating system accounts, [4-104](#)
- ROLE_SYS_PRIVS view
 - application privileges, [12-22](#)
- ROLE_TAB_PRIVS view
 - application privileges, finding, [12-22](#)
- roles, [12-23](#)
 - about, [4-2](#), [4-35](#)
 - ADM_PARALLEL_EXECUTE_TASK role, [4-40](#)
 - ADMIN OPTION and, [4-93](#)
 - advantages in application use, [12-22](#)
 - application, [4-38](#), [4-56](#), [12-25](#), [12-27](#)
 - application privileges, [12-22](#)
 - applications, for user, [12-25](#)
 - AUDIT_ADMIN role, [4-40](#)
 - AUDIT_VIEWER role, [4-40](#)
 - AUTHENTICATEDUSER role, [4-40](#)
 - authorization, [4-51](#)
 - authorized by enterprise directory service, [4-53](#)
 - AVTUNE_PKG_ROLE role, [4-40](#)
 - BDSQL_ADMIN role, [4-40](#)
 - BDSQL_USER role, [4-40](#)
 - CAPTURE_ADMIN role, [4-40](#)
 - CDB_DBA role, [4-40](#)
 - changing authorization for, [4-51](#)
 - changing passwords, [4-51](#)
 - common, [4-7](#)
 - common, auditing, [30-5](#)
 - common, granting, [4-62](#)
 - CONNECT role
 - about, [4-40](#)
 - create your own, [A-10](#)
 - CTXAPP role, [4-40](#)
 - database role, users, [12-25](#)
 - DATAPUMP_EXP_FULL_DATABASE role, [4-40](#)
 - DATAPUMP_IMP_FULL_DATABASE role, [4-40](#)
 - DB_DEVELOPER_ROLE role, [4-40](#)
 - DBA role, [4-40](#)
 - DBFS_ROLE role, [4-40](#)
 - DBJAVASCRIPT role, [4-40](#)
 - DBMS_MDX_INTERNAL role, [4-40](#)
 - DDL statements and, [4-39](#)
 - default, [4-107](#)
- roles (*continued*)
 - default, setting for user, [2-17](#)
 - definer's rights procedures disable, [4-38](#)
 - dependency management in, [4-39](#)
 - DGPDB_ROLE role, [4-40](#)
 - disabling, [4-106](#)
 - dropping, [4-55](#)
 - DV_ACCTMGR role, [4-40](#)
 - DV_ADMIN role, [4-40](#)
 - DV_AUDIT_CLEANUP role, [4-40](#)
 - DV_DATAPUMP_NETWORK_LINK role, [4-40](#)
 - DV_GOLDENGATE_ADMIN role, [4-40](#)
 - DV_GOLDENGATE_REDO_ACCESS role, [4-40](#)
 - DV_MONITOR role, [4-40](#)
 - DV_OWNER role, [4-40](#)
 - DV_PATCH_ADMIN role, [4-40](#)
 - DV_POLICY_OWNER role, [4-40](#)
 - DV_SECANALYST role, [4-40](#)
 - DV_STREAMS_ADMIN role, [4-40](#)
 - DV_XSTREAMS_ADMIN role, [4-40](#)
 - EJBCLIENT role, [4-40](#)
 - enabled or disabled, [4-35](#), [4-54](#)
 - enabling, [4-106](#), [12-25](#)
 - enterprise, [4-53](#)
 - EXP_FULL_DATABASE role, [4-40](#)
 - external, [4-50](#)
 - FSQL_FIREWALL_VIEWER role, [4-40](#)
 - functionality, [4-11](#), [4-35](#)
 - functionality of, [4-35](#)
 - GATHER_SYSTEM_STATISTICS role, [4-40](#)
 - GDS_CATALOG_SELECT role, [4-40](#)
 - global authorization, [4-53](#)
 - about, [4-53](#)
 - global roles
 - creating, [4-53](#)
 - example, [4-50](#)
 - external sources, and, [4-52](#)
 - GLOBAL_AQ_USER_ROLE role, [4-40](#)
 - GRANT statement, [4-105](#)
 - granted locally, [4-6](#)
 - granted to other roles, [4-35](#)
 - granting and revoking to program units, [9-16](#)
 - granting in a CDB, [4-4](#)
 - granting roles
 - about, [4-92](#)
 - methods for, [4-54](#)
 - system, [4-92](#)
 - system privileges, [4-21](#)
 - granting to program units, [4-55](#)
 - GRAPH_ADMINISTRATOR role, [4-40](#)
 - GRAPH_DEVELOPER role, [4-40](#)
 - GRAPH_USER role, [4-40](#)
 - GSM_POOLADMIN_ROLE role, [4-40](#)
 - GSMADMIN_ROLE role, [4-40](#)
 - GSMCATUSER_ROLE role, [4-40](#)

roles (*continued*)

- GSMROOTUSER_ROLE role, [4-40](#)
- GSMUSER_ROLE role, [4-40](#)
- guidelines for security, [A-10](#)
- HS_ADMIN_EXECUTE_ROLE role, [4-40](#)
- HS_ADMIN_ROLE role, [4-40](#)
- HS_ADMIN_SELECT_ROLE role, [4-40](#)
- IMP_FULL_DATABASE role, [4-40](#)
- in applications, [4-36](#)
- indirectly granted, [4-35](#)
- invoker's rights procedures use, [4-39](#)
- JAVA_ADMIN role, [4-40](#)
- JAVADEBUGPRIV role, [4-40](#)
- JAVAIDPRIV role, [4-40](#)
- JAVASYSPRIV role, [4-40](#)
- JAVAUERPRIV role, [4-40](#)
- JMXSERVER role, [4-40](#)
- job responsibility privileges only, [A-10](#)
- LBAC_DBA role, [4-40](#)
- listing grants, [4-112](#)
- listing privileges and roles in, [4-114](#)
- listing roles, [4-114](#)
- local, [4-5](#), [4-62](#)
- LOGSTDBY_ADMINISTRATOR role, [4-40](#)
- management using the operating system, [4-103](#)
- managing roles
 - about, [4-33](#)
 - categorizing users, [12-27](#)
- managing through operating system, [4-40](#)
- managing with RADIUS server, [26-19](#)
- maximum number a user can enable, [4-107](#)
- multibyte characters in names, [4-48](#)
- multibyte characters in passwords, [4-51](#)
- naming, [4-35](#)
- network authorization, [4-53](#)
- network client authorization, [4-53](#)
- OEM_ADVISOR role, [4-40](#)
- OEM_MONITOR role, [4-40](#)
- OGG_APPLY role, [4-40](#)
- OGG_APPLY_PROCREP role, [4-40](#)
- OGG_CAPTURE role, [4-40](#)
- OGG_SHARED_CAPTURE role, [4-40](#)
- One Big Application User, compromised by, [12-2](#)
- operating system, [4-104](#)
- operating system authorization, [4-53](#)
- operating system granting of, [4-105](#)
- operating system identification of, [4-104](#)
- operating system management and the shared server, [4-105](#)
- operating system-managed, [4-105](#)
- operating-system authorization, [4-52](#)
- OPTIMIZER_PROCESSING_RATE role, [4-40](#)
- OSAK_ADMIN_ROLE role, [4-40](#)
- password case sensitivity, [3-29](#)

roles (*continued*)

- PDB_DBA role, [4-40](#)
- PGX_SERVER_GET_INFO role, [4-40](#)
- PGX_SERVER_MANAGE role, [4-40](#)
- PGX_SESSION_ADD_PUBLISHED_GRAPH role, [4-40](#)
- PGX_SESSION_COMPILE_ALGORITHM role, [4-40](#)
- PGX_SESSION_CREATE role, [4-40](#)
- PGX_SESSION_GET_PUBLISHED_GRAPH role, [4-40](#)
- PGX_SESSION_MODIFY_MODEL role, [4-40](#)
- PGX_SESSION_NEW_GRAPH role, [4-40](#)
- PGX_SESSION_READ_MODEL role, [4-40](#)
- predefined, [4-40](#)
- privilege analysis, [5-3](#)
- privileges for creating, [4-48](#)
- privileges for dropping, [4-55](#)
- privileges, changing authorization method for, [4-51](#)
- privileges, changing passwords, [4-51](#)
- PROVISIONER role, [4-40](#)
- RECOVERY_CATALOG_OWNER_VPD role, [4-40](#)
- RECOVERY_CATALOG_USER role, [4-40](#)
- RESOURCE role, [4-40](#)
- restricting from tool users, [4-56](#)
- restrictions on privileges of, [4-39](#)
- REVOKE statement, [4-105](#)
- revoking, [4-54](#), [4-98](#)
- SAGA_ADM_ROLE role, [4-40](#)
- SAGA_CONNECT_ROLE role, [4-40](#)
- SAGA_PARTICIPANT_ROLE role, [4-40](#)
- SCHEDULER_ADMIN role, [4-40](#)
- schemas do not contain, [4-35](#)
- security domains of, [4-38](#)
- SET ROLE statement
 - about, [4-51](#)
 - example, [4-51](#)
 - OS_ROLES parameter, [4-105](#)
- setting in PL/SQL blocks, [4-39](#)
- SHARDED_SCHEMA_OWNER role, [4-40](#)
- SODA_APP role, [4-40](#)
- SQL_FIREWALL_ADMIN role, [4-40](#)
- unique names for, [4-48](#)
- use of passwords with, [4-36](#)
- user, [4-38](#), [12-27](#)
- users capable of granting, [4-55](#)
- uses of, [4-35](#), [4-36](#)
- WITH GRANT OPTION and, [4-95](#)
- without authorization, [4-48](#)
- WM_ADMIN_ROLE role, [4-40](#)
- XDB_SET_INVOKER roles, [4-40](#)
- XDB_WEBSERVICES role, [4-40](#)
- XDB_WEBSERVICES_OVER_HTTP role, [4-40](#)

roles (*continued*)

- XDB_WEBSERVICES_WITH_PUBLIC role, [4-40](#)
- XDBADMIN role, [4-40](#)
- XS_CACHE_ADMIN role, [4-40](#)
- XS_NAMESPACE_ADMIN role, [4-40](#)
- XS_NSATTR_ADMIN role, [4-40](#)
- XS_RESOURCE role, [4-40](#)
- XSTREAM_APPLY role, [4-40](#)
- XSTREAM_CAPTURE role, [4-40](#)
 - See also secure application roles
- root container
 - viewing information about, [4-32](#)
- root file paths
 - for files and packages outside the database, [A-3](#)
- row level security
 - schema system privileges, [4-26](#)
- row-level security
 - See fine-grained access control, Oracle Virtual Private Database (VPD)
- RSA private key, [A-19](#)
- run-time facilities, [A-3](#)
 - restriction permissions, [A-3](#)

S

- SAGA_ADM_ROLE role, [4-40](#)
- SAGA_CONNECT_ROLE role, [4-40](#)
- SAGA_PARTICIPANT_ROLE role, [4-40](#)
- salt, [3-34](#)
- Sarbanes-Oxley Act
 - auditing to meet compliance, [28-1](#)
- SCHEDULER_ADMIN role
 - about, [4-40](#)
- schema object privileges, [4-72](#)
- schema objects
 - cascading effects on revoking, [4-101](#)
 - default tablespace for, [2-9](#)
 - dropped users, owned by, [2-37](#)
 - granting privileges, [4-94](#)
 - privileges
 - DML and DDL operations, [4-81](#)
 - granting and revoking, [4-73](#)
 - view privileges, [4-82](#)
 - privileges on, [4-72](#)
 - privileges to access, [4-74](#)
 - privileges with, [4-74](#)
 - revoking privileges, [4-98](#)
- schema privileges
 - about, [4-22](#)
 - ADMINISTER FINE GRAINED AUDIT
 - POLICY system privilege, [4-26](#)
 - ADMINISTER REDACTION POLICY system privilege, [4-26](#)

schema privileges (*continued*)

- ADMINISTER ROW LEVEL SECURITY
 - POLICY system privilege, [4-26](#)
- administrative privileges excluded from, [4-23](#)
- granting, [4-25](#)
- revoking, [4-26](#)
- system privileges excluded from, [4-23](#)
- system privileges for security policies, about, [4-26](#)
- system privileges for security policies, granting, [4-27](#)
- system privileges for security policies, revoking, [4-27](#)
- tutorial using privilege analysis, [5-27](#)
- schema user accounts, predefined, [2-38](#)
- schema-independent users, [12-27](#)
- schema-only accounts, [3-60](#)
- schemas
 - auditing, recommended settings for, [A-23](#)
 - shared, protecting objects in, [12-27](#)
 - unique, [12-26](#)
 - unique, protecting objects in, [12-26](#)
- SCOTT user account
 - restricting privileges of, [A-10](#)
- SEC_MAX_FAILED_LOGIN_ATTEMPTS
 - initialization parameter, [12-31](#)
- SEC_PROTOCOL_ERROR_FURTHER_ACTION
 - initialization parameter, [12-30](#)
- sec_relevant_cols_opt parameter, [14-15](#)
- SEC_RETURN_SERVER_RELEASE_BANNER
 - initialization parameter, [12-32](#)
- SEC_USER_AUDIT_ACTION_BANNER
 - initialization parameter, [12-32](#)
- SEC_USER_UNAUTHORIZED_ACCESS_BANNER
 - initialization parameter, [12-32](#)
- seconf.sql script
 - password settings, [3-9](#)
- secret key
 - location in RADIUS, [26-13](#)
- secure application roles, [12-23](#)
 - about, [4-57](#)
 - creating, [12-22](#)
 - creating PL/SQL package, [12-23](#)
 - finding with DBA_ROLES view, [4-110](#)
 - invoker's rights, [12-23](#)
 - invoker's rights requirement, [12-23](#)
 - package for, [12-23](#)
 - user environment information from
 - SYS_CONTEXT SQL function, [12-23](#)
 - using to ensure database connection, [4-57](#)
- secure external password store
 - about, [3-41](#)
 - client configuration, [3-43](#)
 - examples, [3-42](#)
 - how it works, [3-42](#)
 - proxy authentication, used with, [3-76](#)

Secure Sockets Layer on Oracle RAC
 remote client, testing configuration, [21-60](#)

SecurID, [26-4](#)
 token cards, [26-4](#)

security, [A-3](#)
 application enforcement of, [4-36](#)
 default user accounts
 locked and expired automatically, [A-3](#)
 locking and expiring, [A-3](#)
 domains, enabled roles and, [4-54](#)
 enforcement in application, [12-3](#)
 enforcement in database, [12-3](#)
 multibyte characters in role names, [4-48](#)
 multibyte characters in role passwords, [4-51](#)
 passwords, [3-57](#)
 policies
 applications, [12-2](#)
 SQL*Plus users, restricting, [4-56](#)
 tables or views, [14-3](#)
 procedures enhance, [9-2](#)
 products, additional, [1-3](#)
 roles, advantages in application use, [12-22](#)
 See also security risks

security alerts, [A-2](#)

security attacks, [3-3](#), [3-76](#), [18-3](#), [A-15](#)
 access to server after protocol errors,
 preventing, [12-30](#)
 application context values, attempts to
 change, [13-8](#)
 application design to prevent attacks, [12-7](#)
 command line recall attacks, [12-7](#), [12-10](#)
 denial of service, [A-15](#)
 denial-of-service
 bad packets, addressing, [12-30](#)
 denial-of-service attacks through listener,
 [A-15](#)
 disk flooding, preventing, [12-30](#)
 eavesdropping, [A-15](#)
 encryption, problems not solved by, [18-3](#)
 falsified IP addresses, [A-15](#)
 falsified or stolen client system identities, [A-15](#)
 hacked operating systems or applications,
 [A-15](#)
 intruders, [18-3](#)
 password cracking, [3-3](#)
 password protections against, [3-3](#)
 preventing malicious attacks from clients,
 [12-29](#)
 preventing password theft with proxy
 authentication and secure external
 password store, [3-76](#)
 session ID, need for encryption, [13-42](#)
 shoulder surfing, [12-10](#)
 SQL injection attacks, [12-8](#)
 unlimited authenticated requests, preventing,
 [12-31](#)

security attacks (*continued*)
 user session output, hiding from intruders,
 [13-16](#)
 See also security risks

security domains
 enabled roles and, [4-35](#)

security isolation
 guidelines for, [A-14](#)

security patches
 about, [A-2](#)
 downloading, [A-2](#)

security policies
 See Oracle Virtual Private Database, policies

security risks, [3-76](#), [A-3](#)
 ad hoc tools, [4-56](#)
 application users not being database users,
 [12-2](#)
 applications enforcing rather than database,
 [12-3](#)
 bad packets to server, [12-30](#)
 database version displaying, [12-32](#)
 encryption keys, users managing, [18-8](#)
 invoker's rights procedures, [9-5](#)
 password files, [3-56](#)
 passwords exposed in large deployments,
 [3-41](#)
 passwords, exposing in programs or scripts,
 [12-10](#)
 positional parameters in SQL scripts, [12-10](#)
 privileges carelessly granted, [4-21](#)
 remote user impersonating another user, [4-53](#)
 sensitive data in audit trail, [A-20](#)
 server falsifying identities, [A-19](#)
 users with multiple roles, [12-25](#)
 See also security attacks

security settings scripts
 password settings
 seconf.sql, [3-9](#)

Security Technical Implementation Guide (STIG)
 ORA_ALL_TOPLEVEL_ACTIONS predefined
 unified audit policy, [29-10](#)
 ORA_LOGIN_LOGOUT predefined unified
 audit policy, [29-10](#)
 ORA_STIG_PROFILE user profile, [2-27](#)
 ORA_STIG_RECOMMENDATIONS
 predefined unified audit policy, [29-9](#)
 ora12c_stig_verify_function password
 complexity function, [3-27](#)

SELECT ANY DICTIONARY privilege
 data dictionary, accessing, [A-11](#)
 exclusion from GRANT ALL PRIVILEGES
 privilege, [A-11](#)

SELECT FOR UPDATE statement in Virtual
 Private Database policies, [14-45](#)

SELECT object privilege
 guideline for using, [A-3](#)

- SELECT object privilege (*continued*)
 - privileges enabled, [4-74](#)
- SELECT_CATALOG_ROLE role
 - SYS schema objects, enabling access to, [4-20](#)
- sensitive data, auditing of, [A-23](#)
- separation of duty concepts, [23](#)
- sequences
 - auditing, [30-11](#)
- server.key file
 - pass phrase to read and parse, [A-19](#)
- SESSION_ROLES data dictionary view
 - PUBLIC role, [4-21](#)
- SESSION_ROLES view
 - queried from PL/SQL block, [4-38](#)
- sessions
 - listing privilege domain of, [4-113](#)
 - memory use, viewing, [2-46](#)
 - time limits on, [2-25](#)
 - when auditing options take effect, [32-2](#)
- SET ROLE statement
 - application code, including in, [12-26](#)
 - associating privileges with role, [12-25](#)
 - disabling roles with, [4-106](#)
 - enabling roles with, [4-106](#)
 - when using operating-system roles, [4-105](#)
- SGA
 - See System Global Area (SGA)
- SHA-512 cryptographic hash function
 - enabling exclusive mode, [3-37](#)
- SHARED_SCHEMA_OWNER role, [4-40](#)
- Shared Global Area (SGA)
 - See System Global Area (SGA)
- shared server
 - limiting private SQL areas, [2-25](#)
 - operating system role management restrictions, [4-105](#)
- shoulder surfing, [12-10](#)
- SI_INFORMTN_SCHEMA user account, [2-39](#)
- single sign-on (SSO)
 - defined, [22-2](#)
- smart cards
 - guidelines for security, [A-7](#)
- smartcards, [22-4](#)
 - and RADIUS, [22-4](#), [26-14](#), [26-20](#)
- SODA_APP role, [4-40](#)
- SQL Developer
 - debugging using Java Debug Wire Protocol, [10-22](#)
- SQL Firewall
 - appearance of events in audit trail, [30-46](#)
 - auditing, about, [30-46](#)
- SQL injection attacks, [12-8](#)
- SQL statements
 - dynamic, [13-12](#)
- SQL statements (*continued*)
 - object privileges permitting in applications, [12-28](#)
 - privileges required for, [4-72](#), [12-28](#)
 - resource limits and, [2-24](#)
 - restricting ad hoc use, [4-56](#)
- SQL statements, top-level in unified audit policies, [30-22](#)
- SQL_FIREWALL_ADMIN role, [4-40](#)
- SQL_FIREWALL_VIEWER role, [4-40](#)
- SQL*Loader
 - object store credential creation, [3-47](#)
- SQL*Net
 - See Oracle Net Services
- SQL*Plus
 - connecting with, [3-65](#)
 - restricting ad hoc use, [4-56](#)
 - statistics monitor, [2-25](#)
- SQL92_SECURITY initialization parameter
 - READ object privilege impact, [4-75](#)
- SQLNET.ALLOWED_LOGON_VERSION_CLIENT
 - target databases from earlier releases, [3-38](#)
- SQLNET.ALLOWED_LOGON_VERSION_SERVER
 - target databases from earlier releases, [3-38](#)
 - using only 12C password version, [3-37](#)
- SQLNET.ALLOWED_LOGON_VERSION_SERVER
 - parameter
 - effect on role passwords, [3-29](#)
- SQLNET.AUTHENTICATION_KERBEROS5_SER
 - VICE parameter, [24-12](#)
- SQLNET.AUTHENTICATION_SERVICES
 - parameter, [24-12](#), [26-9](#), [26-11](#), [27-2](#), [27-4](#), [A-19](#)
- SQLNET.CRYPTO_CHECKSUM_CLIENT
 - parameter, [20-13](#)
- SQLNET.CRYPTO_CHECKSUM_SERVER
 - parameter, [20-13](#)
- SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT
 - T parameter, [20-13](#)
- SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
 - parameter, [20-13](#)
- SQLNET.ENCRYPTION_CLIENT
 - with ANO encryption and TLS authentication, [20-15](#)
- SQLNET.ENCRYPTION_CLIENT parameter, [20-11](#), [27-2](#)
- SQLNET.ENCRYPTION_SERVER
 - with ANO encryption and TLS authentication, [20-15](#)
- SQLNET.ENCRYPTION_SERVER parameter, [20-11](#), [27-2](#)
- SQLNET.ENCRYPTION_TYPES_CLIENT
 - parameter, [20-11](#)
- SQLNET.ENCRYPTION_TYPES_SERVER
 - parameter, [20-11](#)

- SQLNET.IGNORE_ANO_ENCRYPTION_FOR_TCPS
 - setting, [20-15](#)
 - with ANO encryption and TLS authentication, [20-15](#)
- SQLNET.KERBEROS5_CC_NAME parameter, [24-14](#)
- SQLNET.KERBEROS5_CLOCKSKEW
 - parameter, [24-14](#)
- SQLNET.KERBEROS5_CONF parameter, [24-14](#)
- SQLNET.KERBEROS5_REALMS parameter, [24-14](#)
- sqlnet.ora file
 - Common sample, [20-5](#)
 - Kerberos sample, [20-5](#)
 - Oracle Advanced Security checksum sample, [20-5](#)
 - Oracle Advanced Security encryption sample, [20-5](#)
 - parameters for clients and servers using Kerberos, [24-6](#)
 - parameters for clients and servers using RADIUS, [26-7](#)
 - PDBs, [3-37](#)
 - RADIUS sample, [20-5](#)
 - sample, [20-5](#)
 - SQLNET.AUTHENTICATION_KERBEROS5_SERVICE
 - parameter, [24-12](#)
 - SQLNET.AUTHENTICATION_SERVICES parameter, [24-12](#), [27-2](#), [27-4](#), [A-19](#)
 - SQLNET.CRYPTO_CHECKSUM_CLIENT parameter, [20-13](#)
 - SQLNET.CRYPTO_CHECKSUM_SERVER parameter, [20-13](#)
 - SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT
 - parameter, [20-13](#)
 - SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
 - parameter, [20-13](#)
 - SQLNET.ENCRYPTION_CLIENT parameter, [27-2](#)
 - SQLNET.ENCRYPTION_SERVER parameter, [20-11](#), [27-2](#)
 - SQLNET.ENCRYPTION_TYPES_CLIENT parameter, [20-11](#)
 - SQLNET.ENCRYPTION_TYPES_SERVER parameter, [20-11](#)
 - SQLNET.KERBEROS5_CC_NAME parameter, [24-14](#)
 - SQLNET.KERBEROS5_CLOCKSKEW parameter, [24-14](#)
 - SQLNET.KERBEROS5_CONF parameter, [24-14](#)
 - SQLNET.KERBEROS5_REALMS parameter, [24-14](#)
 - SSL sample, [20-5](#)
 - Trace File Set Up sample, [20-5](#)
- SQLNET.RADIUS_ALTERNATE parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_PORT
 - parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_RETRIES
 - parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_TIMEOUT
 - parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_TLS_HOST
 - parameter, [26-15](#)
- SQLNET.RADIUS_ALTERNATE_TLS_PORT
 - parameter, [26-15](#)
- SQLNET.RADIUS_AUTHENTICATION_PORT
 - parameter, [26-13](#)
- SQLNET.RADIUS_AUTHENTICATION_RETRIES
 - parameter, [26-13](#)
- SQLNET.RADIUS_AUTHENTICATION_TIMEOUT
 - parameter, [26-13](#)
- SQLNET.RADIUS_AUTHENTICATION_TLS_HOST
 - parameter, [26-11](#)
- SQLNET.RADIUS_AUTHENTICATION_TLS_PORT
 - parameter, [26-11](#)
- SQLNET.RADIUS_SEND_ACCOUNTING
 - parameter, [26-18](#)
- SQLNET.RADIUS_TRANSPORT_PROTOCOL
 - parameter, [26-11](#)
- SSL_VERSION
 - See [SSL_VERSION](#)
- standard audit trail
 - records, purging, [32-10](#)
- standard auditing
 - affected by editions, [30-18](#)
 - archiving audit trail, [32-11](#)
 - privilege auditing
 - about, [30-6](#)
 - multitier environment, [30-33](#)
 - records
 - archiving, [32-11](#)
 - statement auditing
 - multitier environment, [30-33](#)
- statement_types parameter of
 - DBMS_RLS.ADD_POLICY procedure, [14-11](#)
- storage
 - quotas and, [2-11](#)
 - unlimited quotas, [2-12](#)
- stored procedures
 - using privileges granted to PUBLIC role, [4-102](#)
- strong authentication
 - centrally controlling SYSDBA and SYSOPER access to multiple databases, [3-52](#)
 - disabling, [27-2](#)
 - guideline, [A-7](#)
- symbolic links
 - restricting, [A-11](#)
- synchronous authentication mode, RADIUS, [26-3](#)
- synonyms
 - object privileges, [4-75](#)
 - privileges, guidelines on, [A-3](#)
- SYS account
 - auditing, [30-83](#)
 - changing password, [2-21](#)
 - policy enforcement, [14-47](#)

SYS account (*continued*)
 privilege analysis, [5-3](#)
 SYS and SYSTEM
 passwords, [A-7](#)
 SYS and SYSTEM accounts
 auditing, [30-83](#)
 SYS objects
 auditing, [30-13](#)
 SYS schema
 objects, access to, [4-20](#)
 SYS user
 auditing example, [30-8](#)
 SYS user account
 about, [2-39](#)
 SYS_CONTEXT function
 about, [13-10](#)
 auditing nondatabase users with, [30-89](#)
 Boolean expressions used in privilege
 analysis, [5-6](#)
 database links, [13-13](#)
 dynamic SQL statements, [13-12](#)
 example, [13-14](#)
 parallel query, [13-12](#)
 syntax, [13-11](#)
 unified audit policies, [30-29](#)
 used in views, [9-9](#)
 validating users, [12-23](#)
 SYS_DEFAULT Oracle Virtual Private Database
 policy group, [14-17](#)
 SYS_SESSION_ROLES namespace, [13-10](#)
 SYS.AUD\$ table
 archiving, [32-11](#)
 SYS.FGA_LOG\$ table
 archiving, [32-11](#)
 SYS.LINK\$ system table, [16-1](#)
 SYS.SCHEDULER\$_CREDENTIAL system table,
 [16-1](#)
 SYS\$UMF user account, [2-39](#)
 SYSASM privilege
 password file, [3-55](#)
 SYSBACKUP privilege
 operations supported, [4-14](#)
 password file, [3-55](#)
 SYSBACKUP user account
 about, [2-39](#)
 SYSDBA administrative privilege
 forcing oracle user to enter password, [4-14](#)
 SYSDBA privilege, [4-13](#)
 directory authentication, [3-53](#)
 Kerberos authentication, [3-54](#)
 password file, [3-55](#)
 TLS authentication, [25-3](#)
 SYSDG privilege
 operations supported, [4-16](#)
 password file, [3-55](#)

SYSDG user account
 about, [2-39](#)
 SYSKM privilege
 operations supported, [4-17](#)
 password file, [3-55](#)
 SYSKM user account
 about, [2-39](#)
 SYSLOG
 audit trail records, [32-4](#)
 capturing audit trail records, [32-5](#)
 SYSMAN user account, [A-7](#)
 SYSOPER privilege, [4-13](#)
 directory authentication, [3-53](#)
 password file, [3-55](#)
 SYSRAC privilege
 operations supported, [4-17](#)
 System Global Area (SGA), [13-2](#)
 application contexts, storing in, [13-2](#)
 global application context information location,
 [13-28](#)
 limiting private SQL areas, [2-25](#)
 system privileges, [A-3](#)
 about, [4-19](#)
 ADMIN OPTION, [4-19](#)
 ANY
 guidelines for security, [A-11](#)
 CDBs, [4-30](#)
 GRANT ANY PRIVILEGE, [4-19](#)
 granting, [4-92](#)
 granting and revoking, [4-21](#)
 granting as a schema privilege, [4-22](#)
 power of, [4-19](#)
 preventing from being used on schemas, [4-79](#)
 restriction needs, [4-20](#)
 revoking, cascading effect of, [4-101](#)
 SELECT ANY DICTIONARY, [A-11](#)
 with common privilege grants, [4-30](#)
 system requirements
 Kerberos, [22-7](#)
 RADIUS, [22-7](#)
 strong authentication, [22-7](#)
 TLS, [22-7](#)
 SYSTEM user account
 about, [2-39](#)

T

table encryption
 transparent sensitive data protection policy
 settings, [15-34](#)
 tables
 auditing, [30-11](#)
 privileges on, [4-81](#)
 tablespaces
 assigning defaults for users, [2-9](#)
 default quota, [2-11](#)

- tablespaces (*continued*)
 - quotas for users, [2-11](#)
 - quotas, viewing, [2-45](#)
 - temporary
 - assigning to users, [2-12](#)
 - unlimited quotas, [2-12](#)
- TCP connection
 - Kerberos krb5.conf configuration, [24-16](#)
- TCPS protocol
 - tnsnames.ora file, used in, [A-19](#)
 - Transport Layer Security, used with, [A-15](#)
- TELNET service, [A-15](#)
- TFTP service, [A-15](#)
- token cards, [22-4](#), [A-7](#)
- trace file
 - set up sample for sqlnet.ora file, [20-5](#)
- trace files
 - access to, importance of restricting, [A-11](#)
 - bad packets, [12-30](#)
 - location of, finding, [13-54](#)
 - Oracle DBaaS-to-IAM client side tracing, [7-40](#)
- traditional auditing
 - desupport, [28-8](#)
- Transparent Data Encryption
 - about, [18-8](#)
 - enabling for FIPS 140-2, [C-8](#)
 - FIPS-supported algorithms, [C-4](#)
 - SYSKM administrative privilege, [4-17](#)
- Transparent Data Encryption (TDE), [16-1](#)
 - TSDP with TDE column encryption, [15-33](#)
- transparent sensitive data protection (TSDP)
 - unified auditing
 - general steps, [15-28](#)
- transparent sensitive data protection (TSDP)
 - about, [15-2](#)
 - altering policies, [15-13](#)
 - benefits, [15-2](#), [15-3](#)
 - bind variables
 - about, [15-17](#)
 - expressions of conditions, [15-18](#)
 - creating policies, [15-5](#)
 - disabling policies, [15-14](#)
 - disabling REDACT_AUDIT policy, [15-20](#)
 - dropping policies, [15-15](#)
 - enabling REDACT_AUDIT policy, [15-20](#)
 - finding information about, [15-35](#)
 - fine-grained auditing
 - general steps, [15-30](#)
 - general steps, [15-2](#)
 - PDBs, [15-4](#)
 - privileges required, [15-4](#)
 - REDACT_AUDIT policy, [15-17](#)
 - sensitive columns in INSERT or UPDATE
 - operations, [15-19](#)
 - sensitive columns in same SELECT query, [15-19](#)
- transparent sensitive data protection (TSDP) (*continued*)
 - sensitive columns in views, [15-20](#)
 - TDE column encryption
 - general steps, [15-33](#)
 - settings used, [15-34](#)
 - unified auditing: settings used, [15-29](#)
 - Virtual Private Database
 - DBMS_RLS.ADD_POLICY parameters, [15-22](#)
 - general steps, [15-22](#)
 - tutorial, [15-24](#)
- transparent sensitive data protection (TSDP);
 - fine-grained auditing
 - settings used, [15-31](#)
- transparent tablespace encryption
 - about, [18-8](#)
- Transport Layer Security
 - compared with native network encryption, [20-2](#)
 - FIPS-supported cipher suites, [C-6](#)
- Transport Layer Security (SSL)
 - sqlnet.ora file sample, [20-5](#)
- Transport Layer Security (TLS), [22-5](#)
 - allowing certificates from earlier algorithms, [21-42](#)
 - ANO encryption and, [20-15](#)
 - certificate key algorithm, [A-19](#)
 - cipher suites, [A-19](#)
 - combining with other authentication methods, [21-36](#)
 - configuration files, securing, [A-19](#)
 - configuration troubleshooting, [21-61](#)
 - configuring ANO encryption with, [20-15](#)
 - FIPS library location setting (SSLFIPS_LIB), [C-9](#)
 - FIPS mode setting (SSLFIPS_140), [C-9](#)
 - guidelines for security, [A-19](#)
 - listener, administering, [A-15](#)
 - MD5 certification, [B-21](#)
 - mode, [A-19](#)
 - Oracle Internet Directory, [25-2](#), [25-16](#)
 - pass phrase, [A-19](#)
 - RSA private key, [A-19](#)
 - securing TLS connection, [A-19](#)
 - server.key file, [A-19](#)
 - SHA-1 certification, [B-21](#)
 - system requirements, [22-7](#)
 - TCPS, [A-19](#)
 - wallet search order, [21-30](#)
- Transport Layer Security (TLS) troubleshooting
 - checking connection, [25-22](#)
 - checking sqlnet.ora and listener.ora wallet
 - settings, [25-24](#)
 - checking SSL_VERSION parameter, [25-23](#)
 - checking wallet file permissions, [25-23](#)
 - SQL*Net and listener tracing, [25-25](#)

Transport Layer Security on Oracle RAC

- cluster node, testing configuration, [21-60](#)
- listener.ora, [21-59](#)
- local_listener startup parameter, [21-55](#)
- restarting instances, [21-60](#)
- restarting listeners, [21-60](#)
- sqlnet.ora, [21-59](#)
- TCPs protocol endpoints, [21-54](#)
- wallet and certificate creation, [21-56](#)
- wallet creation in nodes, [21-59](#)

Transport Layer Security, X.509 Certificates

- about, [25-5](#)
- about configuring MCS on client, [25-12](#)
- configuring MCS on client, [25-14](#)
- configuring sqlnet.ora on client, [25-11](#)
- configuring sqlnet.ora on server, [25-8](#)
- configuring TNS_NAMES on client, [25-13](#)
- configuring tnsnames.ora on client, [25-12](#)
- creating and configuring server wallet, [25-6](#)
- external user, [25-10](#)
- Grid Infrastructure, listener.ora on server, [25-9](#)
- initialization parameters on server, [25-10](#)
- logical volume management, listener.ora on server, [25-8](#)
- restarting and checking listener on server, [25-10](#)
- shutting down listener on server, [25-7](#)
- testing MCS configuration, SQL*Plus, [25-15](#)
- testing MCS configuration, tnspring, [25-14](#)

Transport Layer Security(TLS)

- configuring for SYSDBA or SYSOPER access, [25-3](#)

triggers

- auditing, [30-11](#), [30-16](#)
- CREATE TRIGGER ON, [12-28](#)
- logon
 - examples, [13-15](#)
 - externally initialized application contexts, [13-15](#)
- privileges for executing, [9-2](#)
- roles, [4-38](#)
- WHEN OTHERS exception, [13-16](#)

troubleshooting, [24-30](#)

- finding errors by checking trace files, [13-54](#)
- Kerberos common configuration problems, [24-29](#)
- ORA-01017 connection errors in CMU configuration, [6-39](#)
- ORA-01017 errors in Kerberos configuration, [24-30](#)
- ORA-12631 errors in Kerberos configuration, [24-30](#)
- ORA-12650 and ORA-12660 errors in native network encryption configuration, [20-17](#)

troubleshooting (*continued*)

- ORA-28030 connection errors in CMU configuration, [6-41](#)
- ORA-28274 connection errors in CMU configuration, [6-39](#)
- ORA-28276 connection errors in CMU configuration, [6-40](#)
- trace files for in CMU connection errors, [6-41](#)

trusted procedure

- database session-based application contexts, [13-2](#)

tsnames.ora configuration file, [A-19](#)

tutorials, [13-17](#), [14-27](#)

- application context, database session-based, [13-17](#)
- auditing
 - creating policy to audit nondatabase users, [30-88](#)
 - creating policy using email alert, [31-12](#)
- definer's rights, database links, [9-26](#)
- external network services, using email alert, [31-12](#)
- global application context with client session ID, [13-44](#)
- invoker's rights procedure using CBAC, [9-17](#)
- nondatabase users
 - creating Oracle Virtual Private Database policy group, [14-38](#)
 - global application context, [13-44](#)
- Oracle Virtual Private Database
 - policy groups, [14-38](#)
 - policy implementing, [14-31](#)
 - simple example, [14-28](#)
- privilege analysis, [5-22](#)
- privilege analysis for ANY privileges, [5-18](#)
- schema privilege use, [5-27](#)
- TSDP with VPD, [15-24](#)
- See also* examples

types

- creating, [4-89](#)
- privileges on, [4-87](#)
- user defined
 - creation requirements, [4-89](#)

U

UDP and TCP ports

- close for ALL disabled services, [A-15](#)

UDP connection

- Kerberos krb5.conf configuration, [24-16](#)

UGA

- See* User Global Area (UGA)

unified audit policies, [28-1](#), [29-14](#)

- about custom, [30-1](#)
- best practices for creating, [30-2](#)

unified audit policies (*continued*)

dropping

about, [30-87](#)procedure, [30-88](#)location of, [30-2](#)

predefined

ORA_ACCOUNT_MGMT, [29-7](#)ORA_ALL_TOPLEVEL_ACTIONS, [29-10](#)ORA_CIS_RECOMMENDATIONS, [29-8](#)ORA_DATABASE_PARAMETER, [29-7](#)ORA_DV_DEFAULT_PROTECTION, [29-13](#)ORA_DV_SCHEMA_CHANGES, [29-13](#)ORA_LOGIN_LOGOUT, [29-10](#)ORA_OLS_SCHEMA_CHANGES, [29-14](#)ORA_SECURECONFIG, [29-6](#)ORA_STIG_RECOMMENDATIONS, [29-9](#)ORA\$DICTIONARY_SENS_COL_ACCESS,
[29-11](#)syntax for creating, [30-2](#)top-level statements, [30-22](#)users, applying to, [30-83](#)users, excluding, [30-83](#)users, success or failure, [30-83](#)

unified audit policies, administrative users

configuring, [30-10](#)example, [30-10](#)users that can be audited, [30-9](#)

unified audit policies, altering

about, [30-80](#)configuring, [30-81](#)examples, [30-82](#)unified audit policies, application common policies,
[30-38](#)

unified audit policies, application containers

example, [30-41](#)

unified audit policies, CDBs

about, [30-36](#)appearance in audit trail, [30-42](#)configuring, [30-38](#)examples, [30-40](#), [30-41](#)unified audit policies, column level auditing, [30-12](#)

unified audit policies, conditions

about, [30-29](#)configuring, [30-29](#)examples, [30-31](#)

unified audit policies, disabling

about, [30-83](#), [30-86](#)configuring, [30-86](#)

unified audit policies, enabling

about, [30-83](#)configuring, [30-85](#)for groups of users through roles, [30-83](#)

unified audit policies, object actions

about, [30-11](#)actions that can be audited, [30-11](#)appearance in audit trail, [30-15](#)unified audit policies, object actions (*continued*)columns, [30-14](#)configuring, [30-13](#)

dictionary tables

auditing, [30-13](#)examples, [30-13](#)GRANT operations, [30-13](#)SYS objects, [30-13](#)

unified audit policies, objects actions

REVOKE operations, [30-13](#)

unified audit policies, Oracle Data Miner

about, [30-77](#)

unified audit policies, Oracle Data Pump

about, [30-71](#)appearance in audit trail, [30-72](#), [30-74](#)configuring, [30-71](#)examples, [30-71](#)how events appear in audit trail, [30-72](#)

unified audit policies, Oracle Database Real

Application Security

about, [30-57](#)configuring, [30-62](#)events to audit, [30-57](#)examples, [30-62](#)how events appear in audit trail, [30-63](#)

predefined

about, [29-11](#)ORA_RAS_POLICY_MGMT, [29-12](#)ORA_RAS_SESSION_MGMT, [29-12](#)

unified audit policies, Oracle Database Vault

about, [30-48](#)appearance in audit trail, [30-56](#)attributes to audit, [30-49](#)configuring, [30-54](#)data dictionary views, [30-48](#)example of auditing factors, [30-55](#)example of auditing realm, [30-55](#)example of auditing rule set, [30-55](#)example of auditing two events, [30-55](#)how events appear in audit trail, [30-56](#)

unified audit policies, Oracle Firewall

example, [30-46](#)

unified audit policies, Oracle Label Security

about, [30-65](#)appearance in audit trail, [30-70](#)configuring, [30-68](#)examples, [30-69](#)how events appear in audit trail, [30-70](#)

LBACSYS.ORA_GET_AUDITED_LABEL

function, [30-70](#)unified audit policies, Oracle Machine Learning for
SQLconfiguring, [30-78](#)how events appear in audit trail, [30-79](#)

unified audit policies, Oracle Recovery Manager

about, [30-63](#)

- unified audit policies, Oracle Recovery Manager (*continued*)
 - how events appear in audit trail, [30-64](#)
- unified audit policies, Oracle SQL*Loader
 - about, [30-73](#)
 - configuring, [30-74](#)
 - example, [30-74](#)
 - how events appear in audit trail, [30-74](#)
- unified audit policies, Oracle XML DB HTTP and FTP protocols
 - about, [30-75](#)
 - configuring, [30-75](#)
 - example of policy for 401 AUTH HTTP errors, [30-76](#)
 - example of policy for all FTP messages, [30-76](#)
 - example of policy for failed HTTP messages, [30-75](#)
 - how appears in audit trail, [30-76](#)
- unified audit policies, privileges
 - about, [30-6](#)
 - appearance in audit trail, [30-8](#)
 - configuring, [30-8](#)
 - examples, [30-8](#)
 - privileges that can be audited, [30-7](#)
 - privileges that cannot be audited, [30-7](#)
- unified audit policies, roles
 - about, [30-5](#)
 - configuring, [30-5](#)
 - examples, [30-6](#)
- unified audit policies, SQL Firewall
 - how events appear in audit trail, [30-46](#)
- unified audit policies, top-level statements, [30-22](#)
 - appearance in audit trail, [30-28](#)
 - how events appear in audit trail, [30-28](#)
- unified audit policies, virtual columns, [30-12](#)
- unified audit session ID, finding, [30-32](#)
- unified audit trail
 - about, [28-5](#)
 - archiving, [32-11](#)
 - disk space size, [32-3](#)
 - improving performance of, [32-8](#)
 - loading audit records to, [32-7](#)
 - Oracle Data Pump, [32-9](#)
 - partition management, [32-8](#)
 - when records are created, [32-2](#)
 - writing audit trail records to AUDSYS
 - about, [32-3](#)
 - immediate-write mode, [32-3](#)
 - minimum flush threshold for queues, [32-2](#)
 - queued-write mode, [32-3](#)
- unified audit trail, object actions
 - READ object actions, [30-19](#)
 - SELECT object actions, [30-19](#)
- unified audit trail, Oracle Machine Learning for SQL
 - examples, [30-78](#)
- unified audit trail, top-level statements, [30-22](#), [30-23](#)
- unified audit trial
 - Oracle Data Pump audit events, [30-71](#)
 - Oracle Database Real Application Security
 - ALL audit events, [30-62](#)
 - Oracle Database Real Application Security security class and ACL audit events, [30-59](#)
 - Oracle Database Real Application Security session audit events, [30-60](#)
 - Oracle Database Real Application Security user, privilege, and role audit events, [30-58](#)
 - Oracle Database Vault command rule events, [30-51](#)
 - Oracle Database Vault Data Pump events, [30-53](#)
 - Oracle Database Vault enable and disable events, [30-54](#)
 - Oracle Database Vault factor events, [30-51](#)
 - Oracle Database Vault OLS events, [30-53](#)
 - Oracle Database Vault realm events, [30-49](#)
 - Oracle Database Vault rule set and rule events, [30-50](#)
 - Oracle Database Vault secure application role events, [30-52](#)
 - Oracle Label Security audit events, [30-66](#)
 - Oracle Label Security user session label events, [30-68](#)
 - Oracle Machine Learning for SQL audit events, [30-77](#)
 - Oracle Recovery Manager audit events, [30-64](#)
 - Oracle SQL*Loader Direct Load Path audit events, [30-73](#)
- unified auditing
 - benefits, [28-5](#)
 - purging records
 - example, [32-24](#)
 - general steps for on-demand purges, [32-13](#)
 - general steps for scheduled purges, [32-13](#)
 - traditional audit desupport, [28-8](#)
 - transparent sensitive data protection policy settings, [15-29](#)
 - tutorial, [30-88](#)
- unified auditing
 - TSDP policies and, [15-28](#)
- UNIFIED_AUDIT_COMMON_SYSTEMLOG
 - initialization parameter
 - using, [32-5](#)
- UNIFIED_AUDIT_SYSTEMLOG initialization
 - parameter
 - about, [32-4](#)
 - using, [32-5](#)

- UNIFIED_AUDIT_TRAIL data dictionary view
 - best practices for using, [A-24](#)
- UNLIMITED TABLESPACE privilege, [2-12](#)
- UPDATE privilege
 - revoking, [4-100](#)
- user accounts
 - administrative user passwords, [A-7](#)
 - application common user
 - about, [2-3](#)
 - CDB common user
 - about, [2-3](#)
 - common
 - creating, [2-14](#)
 - default user account, [A-7](#)
 - local
 - creating, [2-16](#)
 - local user
 - about, [2-5](#)
 - password guidelines, [A-7](#)
 - passwords, encrypted, [A-7](#)
 - predefined
 - administrative, [2-39](#)
 - non-administrative, [2-42](#)
 - predefined sample schemas, [2-42](#)
 - predefined schema, [2-38](#)
 - privileges required to create, [2-6](#)
 - proxy users, [3-74](#)
- user accounts, predefined
 - ANONYMOUS, [2-39](#)
 - ASMSNMP, [2-39](#)
 - AUDSYS, [2-39](#)
 - CTXSYS, [2-39](#)
 - DBSFUSER, [2-39](#)
 - DBSNMP, [2-39](#)
 - DGPDB_INT, [2-39](#)
 - DIP, [2-42](#)
 - GSMROOTUSER, [2-39](#)
 - LBACSYS, [2-39](#)
 - MDDATA, [2-42](#)
 - MDSYS, [2-39](#)
 - OJVM SYS, [2-39](#)
 - OLAP SYS, [2-39](#)
 - ORACLE_OCM, [2-42](#)
 - ORDDATA, [2-39](#)
 - ORDPLUGINS, [2-39](#)
 - ORDSYS, [2-39](#)
 - OUTLN, [2-39](#)
 - REMOTE_SCHEDULER_AGENT, [2-39](#)
 - SI_INFORMTN_SCHEMA, [2-39](#)
 - SYS, [2-39](#)
 - SYS\$UMF, [2-39](#)
 - SYSBACKUP, [2-39](#)
 - SYSDG, [2-39](#)
 - SYSKM, [2-39](#)
 - SYSTEM, [2-39](#)
 - WMSYS, [2-39](#)
- user accounts, predefined (*continued*)
 - XDB, [2-39](#)
 - XS\$NULL, [2-42](#)
- User Global Area (UGA), [13-2](#)
 - application contexts, storing in, [13-2](#)
- user names
 - schemas, [12-26](#)
- user privileges
 - CDBs, [4-12](#)
- USER pseudo column, [4-83](#)
- user sessions, multiple within single database
 - connection, [3-77](#)
- USERENV function
 - used in views, [9-9](#)
- USERENV namespace, [3-83](#)
 - about, [13-11](#)
 - See also CLIENT_IDENTIFIER USERENV attribute
- users
 - administrative option (ADMIN OPTION), [4-93](#)
 - altering, [2-18](#)
 - altering common users, [2-18](#)
 - altering local users, [2-18](#)
 - application users not known to database, [3-82](#)
 - assigning unlimited quotas for, [2-12](#)
 - auditing, [30-83](#)
 - database role, current, [12-25](#)
 - default roles, changing, [2-17](#)
 - default tablespaces, [2-9](#)
 - dropping, [2-37](#)
 - dropping profiles and, [2-29](#)
 - dropping roles and, [4-55](#)
 - enabling roles for, [12-25](#)
 - enterprise, [4-53](#)
 - enterprise, shared schema protection, [12-27](#)
 - external authentication
 - assigning profiles, [2-29](#)
 - finding information about, [2-43](#)
 - finding information about authentication, [3-86](#)
 - global
 - assigning profiles, [2-29](#)
 - hosts, connecting to multiple
 - See external network services, fine-grained access to, [10-2](#)
 - information about, viewing, [2-44](#)
 - listing roles granted to, [4-112](#)
 - memory use, viewing, [2-46](#)
 - names
 - case sensitivity, [2-8](#)
 - how stored in database, [2-8](#)
 - nondatabase, [13-29](#), [13-36](#)
 - objects after dropping, [2-37](#)
 - password encryption, [3-3](#)
 - privileges
 - for changing passwords, [2-18](#)
 - for creating, [2-6](#)

users (*continued*)

- privileges (*continued*)
- granted to, listing, [4-112](#)
- of current database role, [12-25](#)

profiles

- assigning, [2-29](#)
- creating, [2-28](#)
- specifying, [2-13](#)

profiles, CDB or application, [2-29](#)proxy authentication, [3-73](#)proxy users, connecting as, [3-73](#)PUBLIC role, [4-38](#), [4-102](#)quota limits for tablespace, [2-11](#)read-only configuration, [4-108](#)restricting application roles, [4-56](#)restrictions on user names, [2-8](#)roles and, [4-36](#)

- for types of users, [4-38](#)

schema-independent, [12-27](#)security domains of, [4-38](#)security, about, [2-1](#)tablespace quotas, [2-11](#)tablespace quotas, viewing, [2-45](#)user accounts, creating, [2-6](#)user models and Oracle Virtual Private Database, [14-52](#)user name, specifying with CREATE USER statement, [2-8](#)views for finding information about, [2-43](#)users supported, [6-4](#)

utlpwmg.sql

about, [3-26](#)

V

valid node checking, [A-15](#)validating, [6-29](#)views, [4-110](#)about, [4-82](#)

access control list data

- external network services, [10-23](#)

- wallet access, [10-23](#)

application contexts, [13-54](#)audit management settings, [32-25](#)audit trail usage, [29-17](#)audit trail usage for fine grained auditing, [31-18](#)audited activities, [29-17](#)audited activities from custom audit policies, [30-91](#)auditing, [30-11](#)authentication, [3-86](#)bind variables in TSDP sensitive columns, [15-20](#)custom audit policy audit trail usage, [30-91](#)DBA_COL_PRIVS, [4-113](#)views (*continued*)DBA_HOST_ACES, [10-23](#)DBA_HOST_ACLs, [10-23](#)DBA_ROLE_PRIVS, [4-112](#)DBA_ROLES, [4-114](#)DBA_SCHEMA_PRIVS, [4-112](#)DBA_SYS_PRIVS, [4-112](#)DBA_TAB_PRIVS, [4-113](#)DBA_USERS_WITH_DEFPWD, [3-6](#)DBA_WALLET_ACES, [10-23](#)DBA_WALLET_ACLs, [10-23](#)definer's rights, [9-9](#)fine-grained audited activities, [31-18](#)invoker's rights, [9-9](#)Oracle Virtual Private Database policies, [14-53](#)privileges, [4-82](#), [4-110](#)privileges to query views in other schemas, [4-83](#)profiles, [2-43](#)ROLE_SYS_PRIVS, [4-114](#)ROLE_TAB_PRIVS, [4-114](#)security applications of, [4-83](#)SESSION_PRIVS, [4-113](#)SESSION_ROLES, [4-113](#)transparent sensitive data protection, [15-35](#)USER_HOST_ACES, [10-23](#)USER_WALLET_ACES, [10-23](#)users, [2-43](#)

Virtual Private Database

See Oracle Virtual Private Database

VPD

See Oracle Virtual Private Database

vulnerable run-time call, [A-3](#)made more secure, [A-3](#)

W

wallets, [10-2](#)about, [B-2](#)adding certificate to, [6-17](#)authentication method, [3-66](#)

certificates

- adding to wallet, [6-17](#)

deleting, [B-13](#)general process of management, [B-6](#)search paths, [B-7](#)system wallet, [B-15](#)tools to manage, [B-6](#)

- See also access control lists (ACL), wallet access

Web applications

user connections, [13-29](#), [13-36](#)

Web-based applications

Oracle Virtual Private Database, how it works with, [14-52](#)

WHEN OTHERS exceptions
 logon triggers, used in, [13-16](#)
Windows Event Viewer
 capturing audit trail records, [32-5](#)
Windows installations
 security guideline, [A-10](#)
Windows native authentication, [3-55](#)
WITH GRANT OPTION clause
 about, [4-95](#)
 user and role grants, [4-73](#)
WM_ADMIN_ROLE role, [4-40](#)
WMSYS user account, [2-39](#)

X

X.509 certificates, [25-5](#)
 guidelines for security, [A-7](#)

XDB user account, [2-39](#)
XDB_SET_INVOKER role, [4-40](#)
XDB_WEBSERVICES role, [4-40](#)
XDB_WEBSERVICES_OVER_HTTP role
 about, [4-40](#)
XDB_WEBSERVICES_WITH_PUBLIC role, [4-40](#)
XDBADMIN role, [4-40](#)
XS_CACHE_ADMIN role, [4-40](#)
XS_NAMESPACE_ADMIN role, [4-40](#)
XS_NSATTR_ADMIN role, [4-40](#)
XS_RESOURCE role, [4-40](#)
XS\$NULL user account, [2-42](#)
XSTREAM_APPLY role, [4-40](#)
XSTREAM_CAPTURE role, [4-40](#)