Oracle Database Security and Audit

Beyond Checklists

Copyright © 2014, Reidy Database Consulting, LLC

Learning objectives

- Understand
  - Oracle architecture
    - Database
    - Listener
  - Oracle connection handshake
  - Client/server architecture
  - Authentication methods
  - Password protection

Copyright © 2014, Reidy Database Consulting, LLC

Oracle architecture

- Architecture of an Oracle database instance
  - Oracle Real Application Cluster (RAC)
  - Oracle Automatic Storage Management (ASM)
  - Oracle Enterprise Manager (OEM) 12c Cloud Control
- Oracle networking architecture

Copyright © 2014, Reidy Database Consulting, LLC

Oracle RDBMS Architecture

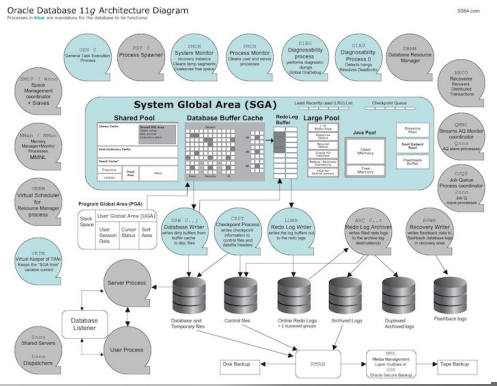
- Oracle database is not just a data store
- Complex system - like an operating system
- Networking services (FIFO pipes, etc.) and support for many protocols (TCP, etc.)
- File subsystem (space allocation, deletion, reuse, recovery, corruption detection, etc.)
- Job schedulers
- Kernel interrupts and instrumentation
- XML storage and processing
- Shared memory and memory pools
- Interprocess communication (IPC) and threading
- Large object storage and processing
- Encryption support at the data storage and network layers (strong algorithms, SSL support)
- Multiple authentication methods (database, Kerberos, LDAP, etc.)

Copyright © 2014, Reidy Database Consulting, LLC

What is an Oracle instance?

- Composed of many subsystems
  - This is same regardless if you are speaking of a single instance database, RAC database, or ASM database
- Based on UNIX architecture
- Software (executables, shared libraries, JAR files, etc)
- Disk files (database files, log files, control files)
- Shared memory

Copyright © 2014, Reidy Database Consulting, LLC

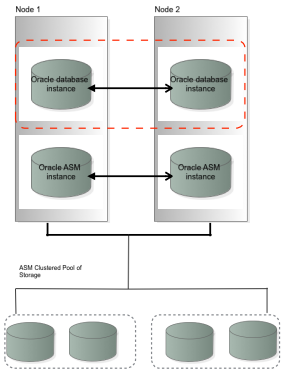


Copyright © 2014, Reidy Database Consulting, LLC

RAC Architecture

- High availability solution
- Multiple computers open and access one database instance
- Transparent application failover (network layer)

Copyright © 2014, Reidy Database Consulting, LLC



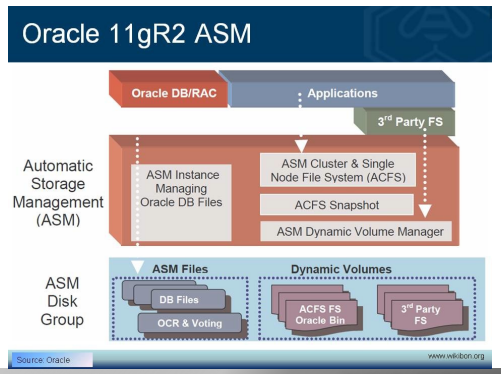
Copyright © 2014, Reidy Database Consulting, LLC

ASM Architecture

- Disk volume manager for Oracle database
- Commonly used in Real Application Cluster (RAC) configurations
  - But, it can be used in a stand-alone single instance system
- Implemented with a small Oracle companion database

ASM database instance is not used to store client data - ever!

Copyright © 2014, Reidy Database Consulting, LLC

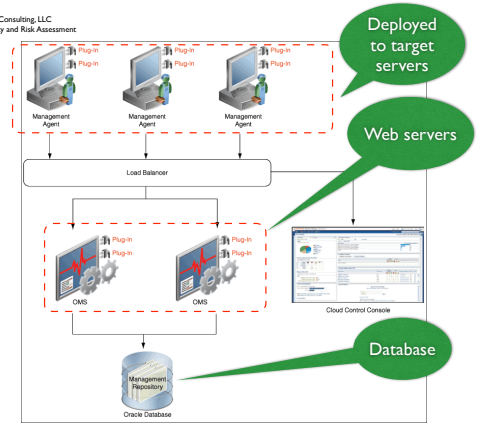


Copyright © 2014, Reidy Database Consulting, LLC

OEM 12c

- Infrastructure to manage, monitor, provision, and baseline enterprise computing platforms
  - Oracle database repository (OMR)
  - Web and application servers (OMS)
  - Management agent (OMA)
  - Console (OMC)
- Operating system configuration
- Database - single instance, RAC, and ASM services
  - non-Oracle databases via plugins
- Sensitive data discovery and mapping (Real Application Testing - RAT)
- Really, anything you want to monitor and/or manage and/ or test

Copyright © 2014, Reidy Database Consulting, LLC



Copyright © 2014, Reidy Database Consulting, LLC

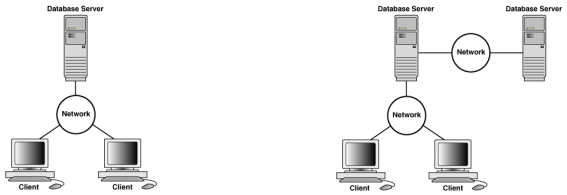
Oracle networking

- Database and database application are separated into a client/server architecture
  - Client runs the database application
    - SQL*Plus, Desktop programs, web applications, etc.
  - Server runs the Oracle database software
    - Functions for concurrent, shared data access

Copyright © 2014, Reidy Database Consulting, LLC

http://docs.oracle.com/cd/E11882_01/server.112/e16508/dist_pro.htm#CNCPT006

Client/server architecture



Copyright © 2014, Reidy Database Consulting, LLC

Oracle listener

- Server side process
  - Traffic manager
  - Incoming client connection requests
  - Establishes a pathway to the database instance

Copyright © 2014, Reidy Database Consulting, LLC

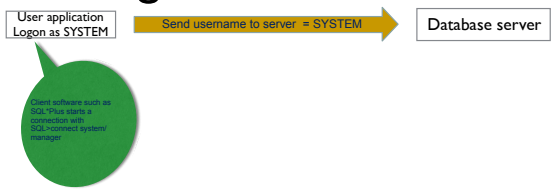
Connection handshake

- 03Logon pre-11g
- 05Logon

Essentially the same process regardless of database version.

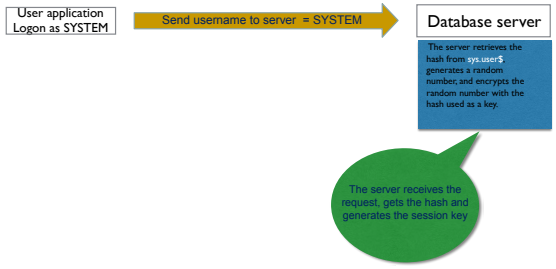
Copyright © 2014, Reidy Database Consulting, LLC

03Logon



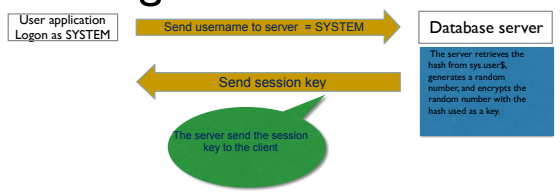
Copyright © 2014, Reidy Database Consulting, LLC

03Logon



Copyright © 2014, Reidy Database Consulting, LLC

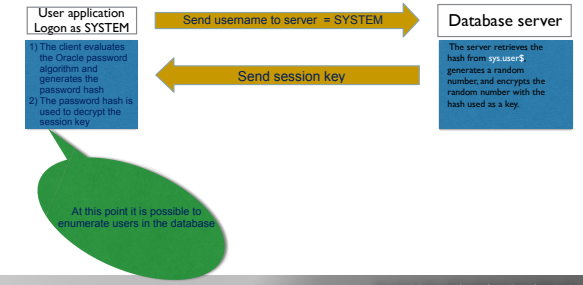
03Logon



Copyright © 2014, Reidy Database Consulting, LLC

Reidy Database Consulting, LLC
Database Security and Risk Assessment

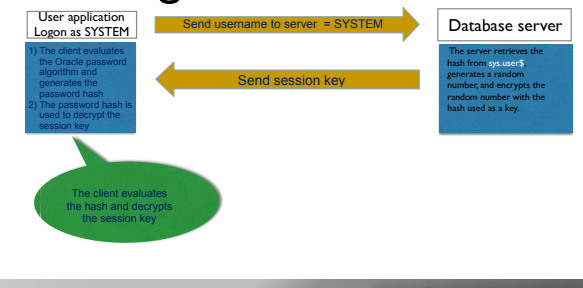
03Logon



Copyright © 2014, Reidy Database Consulting, LLC

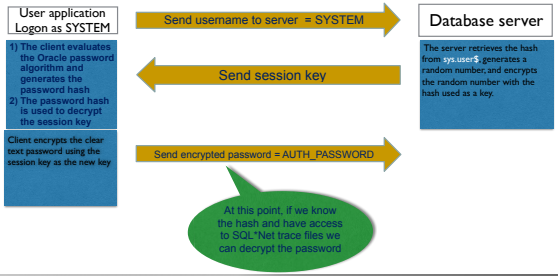
Reidy Database Consulting, LLC
Database Security and Risk Assessment

03Logon



Copyright © 2014, Reidy Database Consulting, LLC

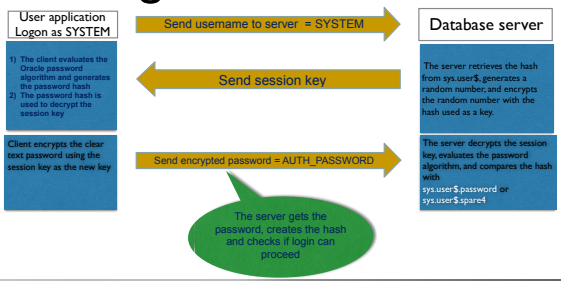
03Logon



Copyright © 2014, Reidy Database Consulting, LLC

Reidy Database Consulting, LLC
Database Security and Risk Assessment

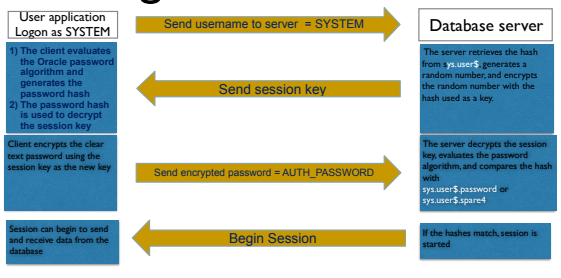
03Logon



Copyright © 2014, Reidy Database Consulting, LLC

Reidy Database Consulting, LLC
Database Security and Risk Assessment

03Logon



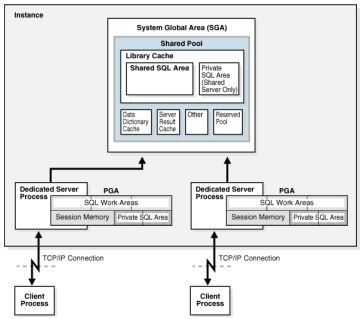
Copyright © 2014, Reidy Database Consulting, LLC

Client/server architectures

- Dedicated server architecture
  - Server process created on behalf of each client process
- Shared server architecture
  - Dispatcher directs incoming requests to pool of shared server processes
- Database resident connection pooling
  - Connection pool of dedicated servers for typical Web application scenarios

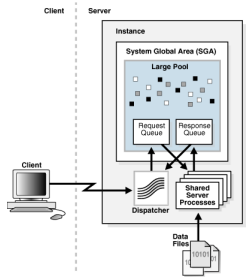
Copyright © 2014, Reidy Database Consulting, LLC

Dedicated server process



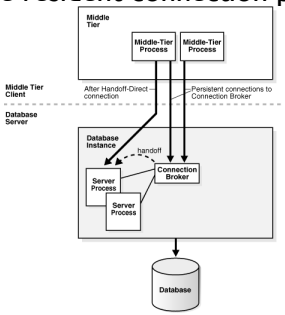
Copyright © 2014, Reidy Database Consulting, LLC

Shared server process



Copyright © 2014, Reidy Database Consulting, LLC

Database resident connection pooling



Copyright © 2014, Reidy Database Consulting, LLC

Oracle networking

- Establish and maintain connection between client and database
- Based on the OSI architecture
  - Stack based architecture
- 3 basic type of connections
  - Client/Server Connections
  - Java Connections
  - Web client connections

Copyright © 2014, Reidy Database Consulting, LLC

http://docs.oracle.com/cd/B28359_01/network.111/b28316/architecture.htm#i1048731

http://en.wikipedia.org/wiki/OSI_model

Q&A

Copyright © 2014, Reidy Database Consulting, LLC