Oracle Database Security and Audit

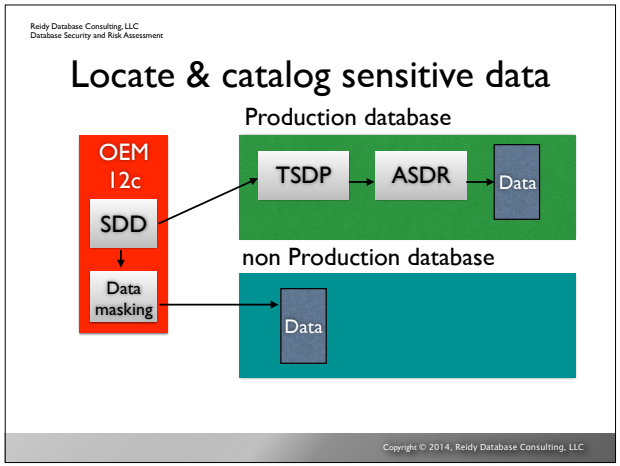
Beyond Checklists

The future - Oracle 12c

- Oracle 12c

12c new security features

http://www.oracle.com/technetwork/database/security/security-compliance-wp-12c-1896112.pdf

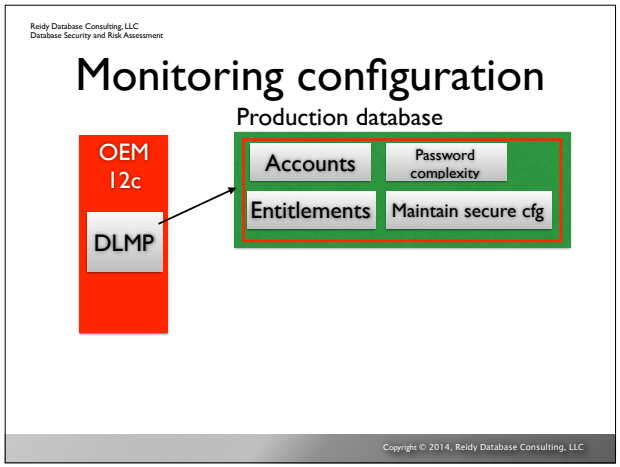


SDD – Sensitive data discovery and modeling

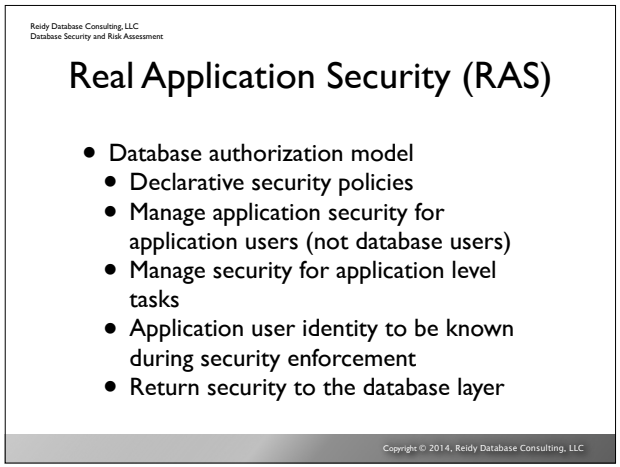
Data masking provides end to end automation for provisioning test databases from production in compliance with regulations. Single source can apply data privacy rules to sensitive data across enterprise-wide databases.

TSDP – Transparent sensitive data protection

Advanced security data redaction (ASDR) makes the business need-to-know decision based on declarative policy conditions.

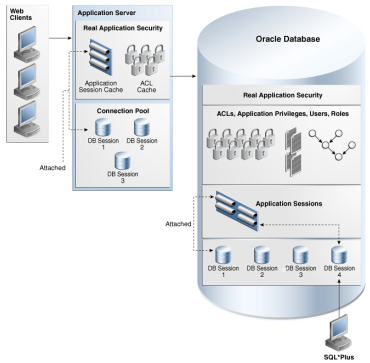


DLMP – Data lifecycle management pack



Provide a uniform security model across all tiers and support multiple application user stores, including the associated roles, authentication credentials, database attributes, and application-defined attributes.

The database can natively support the application security context. The database supports integrated policy specification and enforcement for both the application and the database, so the application does not need to do this through application code. Because the database stores the application security context information, this also reduces network traffic.



Database vault

- Mandatory realms
  - Seal off application objects from all access
- Block or enforce checks on SQL commands
- Additional layer of rules and checks
  - Ad-hoc creation of database links
  - Copy tables (CTAS, copy table)

Others

- Code based access control
  - Grant roles to stored code
- New roles
  - SYSDG (data guard)
  - SYSBACKUP (RMAN)
  - SYSKM (advanced key management)
  - AUDIT_ADMIN, AUDIT_VIEWER (unified conditional auditing)
- Role reduction (RESOURCE is removed)
- System privilege reduction (UNLIMITED TABLESPACE removed)

Q&A

Reidy Database Consulting, LLC
Database Security and Risk Assessment

Thank you!

ron.reidy@gmail.com

Copyright © 2014, Reidy Database Consulting, LLC