Database Security

Oracle Database 12c - New Features and Planning Now

Michelle Malcher

- Oracle ACE Director
- Data Services Team Lead at DRW
- IOUG, Board of Directors
- Author, *Oracle Database Administration for the Microsoft SQL Server DBA*, *Oracle 11g Database Beginner's Guide*
- Wanted to be the San Diego Chicken when I was growing up, but ended up as a DBA and wouldn't want it any other way

Agenda

- Why is security important?
- Review 11g security options
- New Features of Oracle Database 12c
- Practical features to implement now to prepare

Why is security important?

"Overall, two-thirds of companies either expect a data security incident they will have to deal with in the next 12 months, or simply don't know what to expect."

Source:

2012 IOUG DATA SECURITY SURVEY

Produced by Unisphere Research, a division of Information Today, Inc. October 2012

Why is security important?

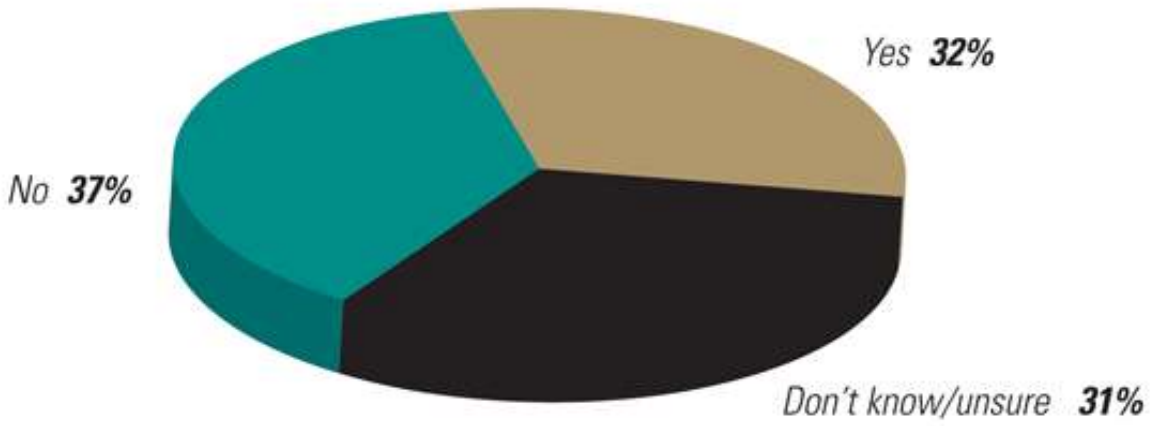
- Protect Company Assets
- Security Breeches
- Protect Data Privacy
- Regulation requirements
- Secret Stuff

Why is security important?

Security from the DBA perspective

- Reduce Risk of Unauthorized Access
- Protect Data Assets
- Be able to Maintain Secure Environment
- Simplify Access and Changes
- Validate and Report on Security

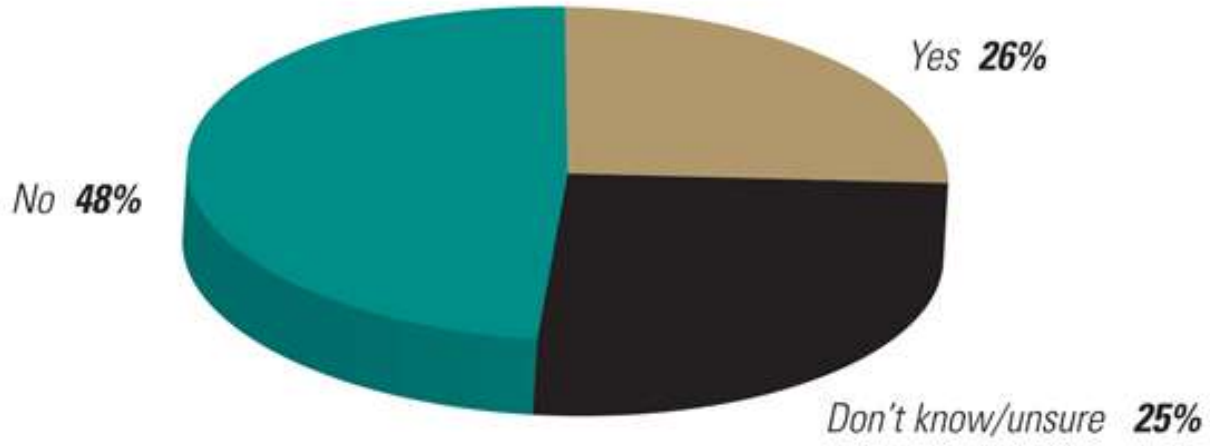
Can you prevent database administrators and other privileged database users from reading or tampering with sensitive information in financial, HR, or other business applications?



Source:
2012 IOUG DATA SECURITY SURVEY
Produced by Unisphere Research, a division of Information Today, Inc. October 2012

IOUG
independent oracle users group

Could you prove database administrators & other privileged database users at your company are not abusing their super-user privileges?



Source:
2012 IOUG DATA SECURITY SURVEY
Produced by Unisphere Research, a division of Information Today, Inc. October 2012

Current Security Options

- Secure Configuration
- User Management
- Least Privileged
- Encryption
- CPU Patching
- Auditing
- Database Vault
- Virtual Private Database

Current Security Options

- Combination of Security Features
  - Database Vault
  - Encryption
    - stored data
    - data files
  - Virtual Private Database
    - Application
    - Ad-hoc queries
  - Auditing
  - Role Management

New Features

- Privilege Analysis
- Additional Roles for Separation of Duties
- Key Management
- Redaction
- Auditing
- Database Vault

New Features

Privilege Analysis

- Getting to the Least Privilege Model
- Captures and Reports on Permissions Used
- Shows Unused Privileges
- DBMS_PRIVILEGE_CAPTURE
  - Enable Policies
  - Generate Reports
- DBA_ Tables
  - DBA_USED … (PRIVS, OBJPRIVS)
  - DBA_UNUSED … (PRIVS, OBJPRIVS)

New Features

Privilege Analysis

- Gather Information to then Revoke Permissions
- Gather Information to Maintain Permissions in Different Environments
- Support for Applications Claiming they need DBA roles

New Features

- Additional Roles for Separation of Duties
  - Existing Roles
    - SYSOPER
    - SYSASM
  - New Roles
    - SYSBACKUP
      - Setup User for backing up databases
    - SYSKM
      - Key Management Role
    - SYSDG
      - Data Guard Role

New Features

- Key Management
  - Manage Key Store
  - Backups of Keys
  - New Role
  - Changing of Keys

New Features

- Redaction
  - Mask Data
    - Full
      - XXXXX *******
    - Partial
      - XXX XX 1234
    - Random
      - 123 45 6789 -> 344 45 2211
  - Online and independent of application code

New Features

- Redaction
  - Policies
    - Users
    - Applications
    - Label Security

New Features

- Auditing
  - Unified Audit Policies

    CREATE AUDIT POLICY

    ACTIONS

    WHEN
    - Can be applied to SYS roles
  - Unified Audit Trail
    - Enabled by default
  - DBMS_AUDIT_MGMT

New Features

- Database Vault
  - Simple Configuration
    - Installed with database
      - Configure users
      - Enable
    - Management in OEM
  - Mandatory Realms
    - Highly sensitive data protected from all users
    - Patching and maintenance available without object access
  - Performance

Getting there

- Start using 11g Security Features
  - Vault
  - Tablespace Encryption
  - Virtual Private Databases
  - Auditing
  - Roles
  - CPUs and PSUs

Getting There

- Install Database Vault for 11g
  - Administration tools
    - Create and Edit Realms
    - Add and Manage Users
    - Security Team can use to grant access
    - Another team can manage Realms
- Validate Install
  - Check that it is enabled in the database, run the following command:

    SQLPLUS> select * from v$option where

    parameter = 'Oracle Database Vault';
  - Bring up Vault Administration in OEM

Getting There

- Database Vault
  - Create Realms
  - Using Roles
- New Release will have Database Vault Installed
  - Configure users
  - Enable

Getting There

- Encryption
- Transparent Data Encryption (TDE)
  - Column data
  - Tablespace level
  - Wallet
    - Master Encryption key
    - Table Encryption key
    - Password protected
  - Transparent to application

Getting There

- Encryption
- Column Encryption

```
CREATE TABLE CUSTOMER
(CUST_ID        NUMBER                          NOT NULL,
FIRST_NAME      VARCHAR2(50)    NOT NULL,
LAST_NAME       VARCHAR2(50)    NOT NULL,
ACCOUNT_ID      NUMBER ENCRYPT using 'AES128',
CC_NUMBER       NUMBER ENCRYPT using 'AES128',
CUST_TYPE       VARCHAR2(30),
CREATED         DATE,
UPDATED         DATE)
```

Getting There

- External Table Encryption

```
create table account_ext
organization external
(
  type oracle_datapump
  default directory dump_dir
  location ('accounts_ext.dmp')
)
as
select
ACCOUNT_NUMBER,
FIRST_NAME,
LAST_NAME,
SSN        ENCRYPT IDENTIFIED BY "Pass123",
ACCOUNT_TAX_ID     ENCRYPT IDENTIFIED BY "Pass123",
ACCOUNT_TYPE,
CREATED,
UPDATED
from accounts;
```

Getting There

- Encryption
- Tablespace level encryption
  - Wallet needs to be open to view data
  - Remains encrypted in RMAN backup
  - Transparent to application
  - Not for system tablespaces
    - SYSTEM, SYSAUX, UNDO, TEMP
  - DBA_TABLESPACES – ENCRYPTED column
  - V$ENCRYPTED_TABLESPACES

Getting There

- Encryption

Create Encrypted Tablespace:

```
CREATE TABLESPACE DATA_ENCRYPT01 DATAFILE
'/u01/oracle/oradata/mmtest/data_encrypt01.dbf' SIZE 100M
ENCRYPTION DEFAULT STORAGE (ENCRYPT);
```

Getting There

- Virtual Private Databases
  - Based on Policies to restrict access to data
  - Examples:
    - By Job Title
    - By Department
    - By other

Getting There

- Virtual Private Databases
  - Triggers and Policies in the database
  - Protects and Restricts the data
    - Inside Applications
    - Ad-Hoc Queries
  - Restrict Columns or other values even with permissions on objects

Getting There

- Virtual Private Databases
  - Creating policies
  - Database trigger on login
  - Procedure to set the context

Create Policy

```
BEGIN
 SYS.DBMS_RLS.ADD_POLICY   (
   object_schema       => 'HR'
   ,object_name        => 'EMP_DETAILS'
   ,policy_name        => 'EMP_IU'
   ,function_schema    => 'HR'
   ,policy_function    => 'MANAGER_ROLE_ONLY'
   ,statement_types    => 'SELECT'
   ,policy_type        => dbms_rls.dynamic
   ,long_predicate     => FALSE
   ,update_check       => TRUE
   ,static_policy      => FALSE
   ,enable             => TRUE );
END;
/
```

Create Procedure

```
CREATE OR REPLACE PROCEDURE HR.set_role_mgr
as
var_role varchar2(30);
begin
select rolename into var_role
from HR_ROLES
where upper(username)=upper(sys_context ('userenv','session_user'));
dbms_session.set_context (namespace => 'realm_role_ctx', attribute =>
'rolename', value => var_role);
end;
/
```

Create Trigger

```
CREATE OR REPLACE TRIGGER SYS.set_user_role
after logon on database
begin
hr. set_role_mgr;
exception
when no_data_found
then
null;
end;
/
```

Getting There

- AUDITING
- Events are audited and stored in the DVYS.AUDIT_TRAIL$ table
- Not part of the database audit trail
  - Database auditing disabled
  - Vault auditing still on
- DV_OWNER, DV_ADMIN, and DV_SECANALYST role have access to the DVYS.AUDIT_TRAIL$ table

Getting There

- Security Patching
  - Oracle CPUs cover Oracle products, application, tools and of course database.
  - Released quarterly
  - Security fixes
  - Released in order of severity
  - Scored accordingly to security standards
  - Documented

Getting There

- Security Patching
- PSU versus CPU
  - Patch Set Update (PSU)
    - Critical bug fixes
    - Apply to most customers
    - Contain security patches
    - Regression testing
  - Critical Patch Update (CPU)
    - Security patches
    - Security fixes in CPU advisory
    - Regression testing

Getting There

- Security Patching
- Develop process
  - Quarterly activity
  - Repeatable process
- Include review of CPU documentation
  - Oracle releases documents the Thursday before patch released
- Include risk assessment
- Include testing plans

Getting There

- User Roles
- Permissions Granted
  - Dictionary Tables
    - DBA_TAB_PRIVS
    - DBA_ROLE_PRIVS
- Changes in permissions
  - Information to compare to
  - Review of changes

Getting There

- User Roles
- Revoking Permissions
- Verifying Current Permissions against Planned Permissions
  - Save table permissions
  - Compare

Getting There

- User Roles
- Review Plan for Access
- Validate that Access is Updated
- Least Privilege User
  - Verify against least privilege
  - Verify what is needed

Summary

- Security Important
- New Features worth upgrading for
- Starting using now for secure database configurations

Questions

????

Additional Information

www.ioug.org

www.oracle.com/security

Michelle_malcher@ioug.org