WELLS FARGO

Protecting Data Using Oracle Database Vault – Wells Fargo Bank Customer Experience

Michael Anderson
Database Analyst

Rohit Goyal
Database Analyst

October 2017

Wells Fargo: Who we are

- Wells Fargo & Company (NYSE: WFC) is a diversified, community-based financial services company with $1.9 trillion in assets. Founded in 1852, Wells Fargo provides banking, insurance, investments, mortgage, and consumer and commercial financial services through 8,600 locations, 13,000 ATMs, online (wellsfargo.com), and mobile devices.
- We're headquartered in San Francisco, but we're decentralized, so every local Wells Fargo location is a headquarters for satisfying our customers' financial needs and helping them succeed financially. We do business with 70 million customers and one in three U.S. households. Wells Fargo has approximately 273,000 team members in 42 countries across our more than 90 businesses.
- At the end of first quarter 2017, Wells Fargo ranked third in assets among U.S. banks.

Information above from the 1st QTR 2017 Wells Fargo Quarterly Fact Sheet

For additional information about Wells Fargo visit the "About Wells Fargo" page on the corporate site.

EDM / DVE at Wells Fargo

Introduction to Enterprise Database Management (EDM) – Database Virtualization and Engineering (DVE)

- Long history of managing Oracle RAC-hosted consolidation environments
- Establishes standards for multiple database products
- Sets infrastructure standards for Oracle hosting
- Responsible for database product certifications
- Manages multiple Oracle Exadata Engineered Systems

Agenda

- Introduction
- Separation of Duties
- DB Vault Configuration
- Job Scheduling
- DB Vault Support By DBA
- GoldenGate Setup with DBV
- Task That Need Realm Disabled
- Issues/Bugs/Resolution
- Special Consideration for enterprise applications
- Recommendation / Lessons Learned / Tips

Intro - Requirements

- Isolate user/application data from privileged users (DBAs)
- No impact to the application or to application users
- Allow DBAs to do their job
- No noticeable effect on performance
- Standard configuration for all databases
- Write-protect job scripts

Intro - Scope

- DBAs in scope...all other users assumed to be app users.
- 11g and 12c Databases – all 9400+ of them
- Initial scope limited to shared environment. Later expanded to all DBs.
- Traditional and multi-tenant databases
- Vaulting whole schema vs objects.

Intro - Assumptions

- All DBAs use Enterprise User Security to connect to DBs. (Using Oracle Virtual Directory)
- No physical DBA accounts
- User provisioning handled by EAM prior to vaulting
- All databases registered with Oracle Internet Directory (OID)

Separation of Duties

- DBA w/o Privileged Temporary Access (PTA)
  - Stats gathering
  - Performance tuning
  - RMAN
  - Tablespace maint
- DBA w/ PTA
  - Sometimes, DBAs need access to app objects
  - The Key...privileged access is temporary
  - Access is requested through enterprise breakglass system
  - Change request, work request or problem ticket required
  - App updates/upgrades, schema changes, Data Pump, etc.

Separation of Duties

- Job Control DBA
  - Only group with write access to job scripts
  - Reviews and deploys scripts
  - More details later…
- Database Vault Owner (DV Owner)
  - Needed for DV admin tasks
    - Enable/disable DB Vault
    - Realm add/removal of schemas and/or roles
    - Realm authorization add/removal of users and/or roles
    - Grant data pump/scheduler authorization
    - Certain 'ALTER SYSTEM' commands for tracing, init.ora params

Separation of Duties

- Database Vault Owner (DV Owner) - continued
  - Need a team of DV Owners (9400+ DBs after all!)
  - 2-3 DV Owners per LOB

- User Provisioning (Enterprise Access Management)
  - Create/Alter/Delete User no longer allowed by DBA
  - Create/Alter/Delete Profile, too
  - DV_ACCTMGR role used for these tasks and granted to EAM staff

DB Vault Configuration

- Realms
- Rules & Rule Sets
- Command Rules
- Secure Application Roles
- Auditing

DV Config - Realms

- Realms
  - One realm vs multiple
    - Didn't want 100s of realms in a database
  - Identifying app users/roles
    - ORACLE_MAINTAINED = 'N'
    - Not in known accounts/roles list
    - Shouldn't have any physical DBA accts
  - All users added as schemas
  - All users and roles have realm owner authorization

DV Config – Rules & Rule Sets

- Rules & Rule Sets
  - Used for Command Rules and Secure App Roles
  - Used to identify SYS sessions for special tasks
  - Used to prevent grants on global users and roles
  - Multiple rules per rule set
  - Rules can be reused in multiple rule sets

DV Config – Command Rules

- Command Rules
  - GRANT
    - Allow the granting of DV_OWNER or DV_ADMIN roles from DV Owner sessions other than SYS
    - Don't allow grants to standard global EUS roles or global EUS user
    - Allow grants by user with DV_PATCH_ADMIN role
    - Still want to allow DBAs to grant appropriate roles and privs
  - SELECT & INSERT (11g only)
    - Used to prevent access by users that may have direct object privileges, unless they are authorized in the realm
    - Mandatory realms used in 12c

DV Config – Secure Application Roles

- Secure App Roles
  - Used to identify special sessions that need extra privileges
    - Inventory/Compliance data gathering
    - Password change process
    - Patching
    - DB Automated build process

DV Config – Auditing

- Auditing
  - Objects are set with ‘Audit on Failure’
  - Using third party tool to collect DV audit trail
  - Data sent into enterprise audit data repository
  - Can be matched up with change management records to help track any unauthorized access attempts

Scheduled Jobs

- Scheduled Jobs
  - Only for jobs that access application objects
    - RMAN, Stats gathering, DB Monitoring unaffected by DV
  - Separate, write-protected location for job scripts once deployed
  - JC DBAs review job scripts for attempted data exfiltration
  - Jobs connect as different OPS$ account that has realm authorization
  - Ideally, jobs that access application objects should be owned by application teams
  - DBMS_SCHEDULER not Enterprise standard
    - If necessary, job should NOT be owned by SYS or DBA user

DB Vault Support by DBA

- DV Support User
  - Contains Package/procedures for DBA Activities
  - User is always locked and protected by Realm

- DV Support APIs
  - DataPump API
    - Calling DBMS_DATAPUMP package
    - Can be run by DBAs with Privileged Temporary Access
    - Cannot do Full export/import
  - Procedure to change tablespace Quota
  - Check Database Vault Status

DB Vault Support by DBA (cont.)

- APIs to support DB Vault Owner Tasks
  - Soft-Disable/Enable DB Vault
  - Remove Role from Realm (Workaround for BUG in 11G)
  - Add users/Roles to realm

- Health Check Script
  - 300+ Checks with 3000+ lines of code and still growing !!
  - Detects failure for many DBVault configuration and setups
  - Provides details of failure
  - Tool as a first step in any troubleshooting

DB Vault Support by DBA (cont.)

- Many other custom scripts
  - Goldengate User
  - Global Role mapping
  - Disable/Enable Vault

GoldenGate Setup with DBV

- Issues in 11g with DBV option enabled
  - OGG-08221 Cannot register or unregister EXTRACT xxxx because of the following SQL error:

    OCI Error 26,723 - Doc ID 2148255.1

    OCI Error 1,950 - Doc ID 1983621.1
  - Solution: Fully install DV components and disable realms to make it work.

- DV Roles for Goldengate
  - DV_GOLDENGATE_ADMIN
  - DV_GOLDENGATE_REDO_ACCESS

GoldenGate Setup with DBV (cont.)

- Realm Access
  - Realm authorization to access protected objects
  - Realm authorization for Oracle Default realm

    11G - Oracle Data Dictionary

    12c - Oracle Default Component Protection Realm

    Error: OGG-00663 Oracle GoldenGate Capture for Oracle, xxx: OCI Error ORA-01031: insufficient privileges

    ORA-06512: at "SYSTEM.LOGMNR$GSBA_GG_TABF_PUBLIC", DV Roles for Goldengate

GoldenGate Setup with DBV (cont.)

- Heartbeat Table
  - GG 12.2 has built in Heartbeat table support
  - Pre12.2 custom health-check script
    - Heartbeat table in App schema

      DBMS JOB or external job to update the table
  - Solution: Move job to owned by application user or move table out of the realm.

Tasks That Need Realm Disabled

- CSSCAN (Character Set Scanner)
- Application upgrade having build in script to create accounts and objects
- WebLogic upgrade RCU (Repository Creation Utility)
- Products not able to work with DBVault
  - CDC - Change Data Capture
  - Advance Replication Master-Master

Issues/Bugs/Resolution

- Change Data Capture (CDC)

  BUG 20774259 - ORA-47401 REALM VIOLATION USING CDC SUBSCRIBE

  Patch: 20774259

- ORA-600 during dropping a realm protected role (11g)

  BUG 9894259 - ORA-600 WITH DROPPING A REALM PROTECTED ROLE BY REALM OWNER

  Patch: 9894259

Issues/Bugs/Resolution (cont.)

- Multiple Bugs related to EUS (ENTERPRISE USER SECURITY)
  - ORA-01031 received when EUS user tries to create a common user in CDB$ROOT

    BUG 25457579 - EUS - EXEC DBMS_STATS.SET_PARAM FAILS WITH ORA-20000 CONNECTED AS GLOBAL USER
    Awaiting Patch
  - Database Vault does not recognize role granted through EUS

    Bug 18733351 - DATABASE VAULT DOES NOT RECOGNIZE ROLES GRANTED THROUGH EUS

    Patch: 18733351
  - DataPump authorization doesn't recognize global roles

    Enhancement Request : 18907613

Special Consideration for enterprise applications

- Oracle E-Business Suite

  Integrating Oracle E-Business Suite Release 12.2 with Oracle Database Vault 12c (Doc ID 2131435.1)

- PeopleSoft Application

  No application specific change for DBV.

Recommendation/Lessons Learned/Tips

- Reduce / prevent full database outage
  - Rolling outage for RAC DB
  - Pre-Configure DBV in new databases

- Not make DBAs enemy
  - DB Vault Support Tools
  - Provide them access for Application support
  - Easy access to check vault status
  - Involve in discussion / Training / How to Sessions

Recommendation/Lessons Learned/Tips (cont.)

- Securing scripts and version control
  - DBV configuration details should be Confidential
  - Protect DBV super accounts

- DB upgrade from 11g to 12c
  - Realms are changed in 12c

    11g Realm "Oracle Data Dictionary" got split into 3 realms in 12c

    - Oracle Default Component Protection Realm
    - Oracle Default Schema Protection Realm
    - Oracle System Privilege and Role Management Realm
  - Post upgrade script to fix the realm access

Recommendation/Lessons Learned/Tips (cont.)

- Custom Monitoring Scripts / Reports
  - Application jobs - move to Application owner
  - DBA scripts - move to OEM

- What could have been done differently?
  - Number of application Realms on databases supporting multiple applications
  - Separate realm for DV supports utilities
  - Instead of protecting whole schema, protect only specific objects.
  - Use of Factors

Thank You