Wells Fargo Bank: Protecting Data Using Oracle Database Vault

Michael Anderson
Database Analyst
Rohit Goyal
Database Analyst
Ken Chestnut
Database Analyst

October 2018

© 2018 Wells Fargo Bank, N.A. All rights reserved. For public use.

Wells Fargo Bank: Who we are

- Wells Fargo & Company (NYSE: WFC) is a diversified, community-based financial services company with $1.9 trillion in assets. Wells Fargo's vision is to satisfy our customers' financial needs and help them succeed financially.
- Founded in 1852 and headquartered in San Francisco, Wells Fargo provides banking, investments, mortgage, and consumer and commercial finance through 8,050 locations, 13,000 ATMs, the internet (wellsfargo.com), and mobile banking, and has offices in 38 countries and territories to support customers who conduct business in the global economy.
- With approximately 265,000 team members, Wells Fargo serves one in three households in the United States. Wells Fargo & Company was ranked No. 26 on Fortune's 2018 rankings of America's largest corporations.
- News, insights and perspectives from Wells Fargo are also available at Wells Fargo Stories.

Information above from the 2nd Quarter 2018 Quarterly Fact Sheet

EDM at Wells Fargo

Introduction to Enterprise Database Management (EDM)

- EDM provides a range of database management oriented services
  - product selection and strategy
  - tooling support
  - standards establishment
  - risk management and compliance oversight
  - database design, administration, and management for multiple primary DBMS platforms installed across Wells Fargo's footprint
- Manages multiple Oracle Exadata Engineered Systems and a large Oracle RAC-hosted consolidation environment

Agenda

- Project Introduction
- DB Vault Configuration
- Operational Impact to DBAs and Applications
- Integration with Existing Processes
- Recommendations / Lessons Learned / Tips
- Final Project Results
- Q & A (after session outside room)

Project Introduction

Requirements / Assumptions

- Requirements
  - Isolate user/application data from privileged users (DBAs)
  - No impact to the application or application users
  - Allow DBAs to do their job
  - No noticeable effect on performance
  - Standard, scripted configuration for all databases
  - Write-protect job scripts
- Assumptions
  - All DBAs connect using Enterprise User Security (EUS)
  - No physical DBA accounts
  - Required support by Enterprise Access Management

Project Introduction

Scope

- DBAs in scope
  - all other users assumed to be application users.
- Project rollout to 11g and 12c databases
  - all tiers
- Traditional and multitenant databases
- Initial scope limited to shared environment
  - Later expanded to all DBs.

DB Vault Configuration

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

DB Vault Configuration

Realms

- One realm for all application schemas
- Scripted way to identify all application users & roles to add to the realm
  - ORACLE_MAINTAINED = 'N' (12c and later)
  - 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

DB Vault Configuration

Rules & Rule Sets

- Used for Command Rules and Secure Application Roles
- Used to identify SYS sessions for special tasks
- Used to prevent unauthorized grants on global users and roles
- Can have multiple rules per rule set
- Each rule can be reused in multiple rule sets

DB Vault Configuration

Command Rules

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

DB Vault Configuration

Secure Application Roles

- Used to identify special sessions requiring additional privileges
  - Inventory and compliance data collection
  - Automated monthly password change process
  - Patching
  - Automated DB provisioning

DB Vault Configuration

Auditing

- Objects are set with 'Audit on Failure'
- Use DBMS_SCHEDULER job to control retention of DV audit trail
- Looking into using third party tool to collect the DV audit trail entries into an enterprise audit data repository
- Audit trail entries can be compared up with change management records to help track any unauthorized access attempts

Operational Impact to DBAs and Applications

Separation of Duties

- Enterprise Access Management is responsible for creating, dropping and altering database users.
  - Nothing enforced this.
- Oracle Database Vault enforces separation of duties in these 5 areas
  - User provisioning
  - Non-privileged DBA access
  - Privileged DBA access
  - Automated jobs
  - DB Vault administration

Operational Impact to DBAs and Applications

Separation of Duties (cont)

- User Provisioning (Enterprise Access Management)
  - Create/Alter/Delete users and profiles
    - No longer allowed by DBA
  - DV_ACCTMGR role required for these tasks and granted to EAM staff
- Normal non-privileged DBA access
  - Stats gathering
  - Performance tuning
    - 'alter session' tracing ok, 'alter system' tracing needs DV Owner
  - RMAN backup and recovery
  - Tablespace maintenance

Operational Impact to DBAs and Applications

Separation of Duties (cont)

- Privileged Temporary Access (PTA) by DBA
  - The key…privileged access is temporary
  - Access is requested through enterprise breakglass system
  - Change request, work request or problem ticket is required
  - Sometimes, DBAs need access to application objects
    - Application updates/upgrades
    - Schema changes
    - Data Pump
    - Application troubleshooting

Operational Impact to DBAs and Applications

Separation of Duties (cont)

- Scheduled Job Control
  - Separate group of DBAs
  - 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

Operational Impact to DBAs and Applications

Separation of Duties (cont)

- Database Vault Owner (DV Owner) – continued
  - Need a team of DV Owners (9900+ DBs after all!)
  - 2-3 DV Owners per LOB
  - DV Owner on-call rotation providing 24 x 7 x 365 support

Operational Impact to DBAs and Applications

Organizational Impact

- Application support teams now have to:
  - Submit requests to create/drop/alter database users
  - Submit requests to create/drop/alter new, non-standard profiles
  - Create change requests, work orders, and work requests so DBAs can obtain PTA access
- Application DBAs also are encouraging 3rd party software vendors and internal development teams to develop application upgrades, new releases, etc. with separation of duties in mind

Operational Impact to DBAs and Applications

DBA Support Utilities

- Created a physical DB Vault support account
  - Contains packages and procedures for DBA activities
  - User is always locked and protected by realm
  - Packages and procedures created with definer's rights
- DV Support APIs
  - DataPump API
    - More details later…
  - Procedure to change tablespace quota
    - Needed since 'alter user' command restricted by DB Vault
  - Check DB Vault status

Operational Impact to DBAs and Applications

DBA Support Utilities

- APIs to support DV Owner Tasks
  - Soft-disable/enable DB Vault
    - Disables/enables all realms and command rules (no restart)
    - Used for special tasks where separation of duties is not practical, i.e. vendor application upgrades to database
    - Soft-enable process scans for any new users and roles to add to the realm
  - Remove Role from Realm (Workaround for bug in 11g)
  - Separate API to add users/roles to realm

Operational Impact to DBAs and Applications

DBA Support Utilities (cont)

- Health check script
  - 375+ checks with 3500+ lines of code and still growing!!
  - Detects failures in the expected DB Vault and related database configuration settings
  - Provides details of the failure
  - Used as a first step in any troubleshooting involving DB Vault
- DB Vault configuration repair script
  - Used to return to the standard configuration

Operational Impact to DBAs and Applications

DB Vault support matrices

- DBA Support Matrices
  - 1st matrix of common DBA tasks and shows who can perform the task, along with the access required. Categories group tasks that apply to multitenant, non-multitenant, and both.
  - 2nd matrix related to privileges affected by DB Vault, and who can grant and revoke them, with the access required. Categories are divided by whether the user/role is protected by DB Vault and whether the database is multitenant or non-multitenant.
- Serves as a quick lookup for DBAs

Integration with Existing Processes

Scheduled Jobs (more detail, as promised)

- Jobs that run as SYS can no longer access application objects
- Solution
  - Ideally, job ownership moved to application team and run as application user
  - Jobs that must run on DB server can run as OPS$ user with realm authorization
    - With multitenant, needed to create common account instead of OPS$ user
  - Job scripts deployed to write-protected shared network location.
  - RMAN, stats, DB monitoring jobs unaffected by DV

Integration with Existing Processes

DataPump (export/import) (more detail, as promised)

- Full export/import requires DV_OWNER grants
- Login to server as oracle software owner to run expdp/impdp
- DataPump authorization doesn't recognize global roles
- Solution
  - DataPump API – wrapper around DBMS_DATAPUMP package
  - Can be run by DBAs with Privileged Temporary Access (PTA)
  - Still can't do full export/import
  - Users/schema owners need to be pre-created

Integration with Existing Processes

User provisioning by DBA

- Massive deployments – creating multiple users/roles with scripts are now blocked by DV
- Datapump API can't create users
- Solution
  - DV Owner group has permission to create user (with PTA)
  - Soft-Enable/Soft-Disable API
  - Add users/roles to realm (API)
    - Scan through all users and roles in database
    - Exclude oracle default users/roles
    - Exclude known accounts
    - Add and authorize the remaining accounts to the realm

Integration with Existing Processes

Application Deployment

- App user is locked and protected by realm
- Vendor-provided deployments scripts blocked by DV
- Greater DDL restrictions in 12c
- Solution
  - Unlock and login as app user for deployment
  - Use Soft-Enable/Soft-Disable API for complex and vendor provided scripts
  - If using another application schema, make sure to grant DDL authorization (dbms_macadm.authorize_ddl)
  - If using proxy users, make sure proxy user authorization is granted (dbms_macadm.authorize_proxy_user)

Integration with Existing Processes

GoldenGate

- New DB Vault roles for GoldenGate
  - DV_GOLDENGATE_ADMIN
  - DV_GOLDENGATE_REDO_ACCESS
- Realm Access
  - GG user needs realm authorization to access protected objects
  - GG user needs realm authorization to following default realms
    - Oracle Data Dictionary (11g)
    - Oracle Default Component Protection Realm (12c)

Integration with Existing Processes

GoldenGate (cont)

- Heartbeat Table
  - GG 12.2 has built in Heartbeat table support
  - Pre-12.2 required a custom heartbeat table and job
    - Heartbeat table in App schema
    - DBMS_JOB or external job to update the table
    - Solution: Move job ownership to application user or move HB table out of the realm
- Issues in 11g with DB Vault binaries enabled
  - OGG-08221: Cannot register or unregister EXTRACT xxxx because of the following SQL error:
  - Solution: Fully install DV components and disable realms to allow extract registration

Integration with Existing Processes

RMAN Table Restore

- New RMAN table restore command doesn't work when DV fully enabled
  - RMAN uses expdp internally
  - Runs as SYS, which doesn't have datapump authorization
- Solution
  - Use traditional method of recovering table instead of rman table restore command
    - Restore full database, disable DV, then export table

Note: Other RMAN functionality works without issue

Integration with Existing Processes

Cloning/Refreshing CDB/PDB

- DV must be configured and enabled in CDB before configuring in PDB
- No impact if doing schema-level export/import to refresh PDB
- No impact if cloning one PDB to another within the same CDB. DV will be configured the same as original PDB.
- If cloning from PDB$SEED, DV will not be configured.
- PDB created from a non-CDB database will have old DV configuration and will need to be cleaned up. Check for common user vs. non-CDB local user conflicts.

Integration with Existing Processes

Cloning/Refreshing CDB/PDB (cont)

- For a full import, must ensure the components listed in DBA_REGISTRY match between the source non-CDB and target CDB.
  - Must disable DV before full import
  - May need cleanup and reconfigure DV
- PDB clone impact on EUS with Oracle Virtual Directory (OVD)
  - PDB clone assigned new GUID
  - EUS global role mapping uses PDB GUID
  - To preserve global role mapping, save and reuse old wallet

Integration with Existing Processes

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 changes for DV
- SAP
  - SAP note 2218115 – Oracle Database Vault 12c
  - SAP note 1355140 – Using Oracle Database Vault in an SAP environment
  - SAP note 1868094 – Overview: Oracle Security SAP Notes

Recommendations / Lessons Learned / Tips

- Reduce / prevent full database outages
  - Rolling instance restart for RAC DB
  - Pre-configure DV in new databases
- Try not to make DBAs too upset
  - DV support utilities
  - Provide DBAs temporary access for app support
  - Provide DBAs a way to check status of DV (soft disabled or fully enabled)
  - Involve DBAs in discussions, training and How-To sessions (repeat often)

Recommendations / Lessons Learned / Tips

- Securing scripts and version control
  - DV configuration details should be confidential
  - Protect DV super accounts
- Create a DV health check and config repair scripts
  - Ensures configuration is stable, nothing missing
- Move monitoring scripts to OEM or run as application jobs
- Stay up-to-date on all DV-related patches
- Full regression testing for each DB release
  - Things may work differently in the new release

Final Project Recap

- Project lasted 3.5 years
- Oracle versions 11.2, 12.1 & 12.2 (18c certification by 2019Q1)
- Number of Databases vaulted – 9900+
  - Normal (non-multitenant) – 1500+
  - Container DBs – ~3000
  - Pluggable DBs – ~5400
- Project involved diverse team
  - Engineering, operations, architecture, compliance, deployment, project management
  - US and India

Thank You