
ORACLE®

Oracle Database Vault for SAP NetWeaver

Oracle Database Vault 12c Release 1 (12.1)

Andreas Becker, Principal Member Technical Staff
Oracle Server Technologies
SAP Development
January 21, 2016

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Agenda

1. Oracle Database Security
2. Oracle Database Security for SAP
3. Oracle Database Vault
4. Oracle Database Vault 12c for SAP
5. Outlook

References

SAP Notes

SAP Notes
1868094 - Overview: Oracle Security SAP Notes
1355140 - Using Oracle Database Vault in an SAP environment
2218115 - Oracle Database Vault 12c

Source: SAP Support Portal https://support.sap.com/notes

References

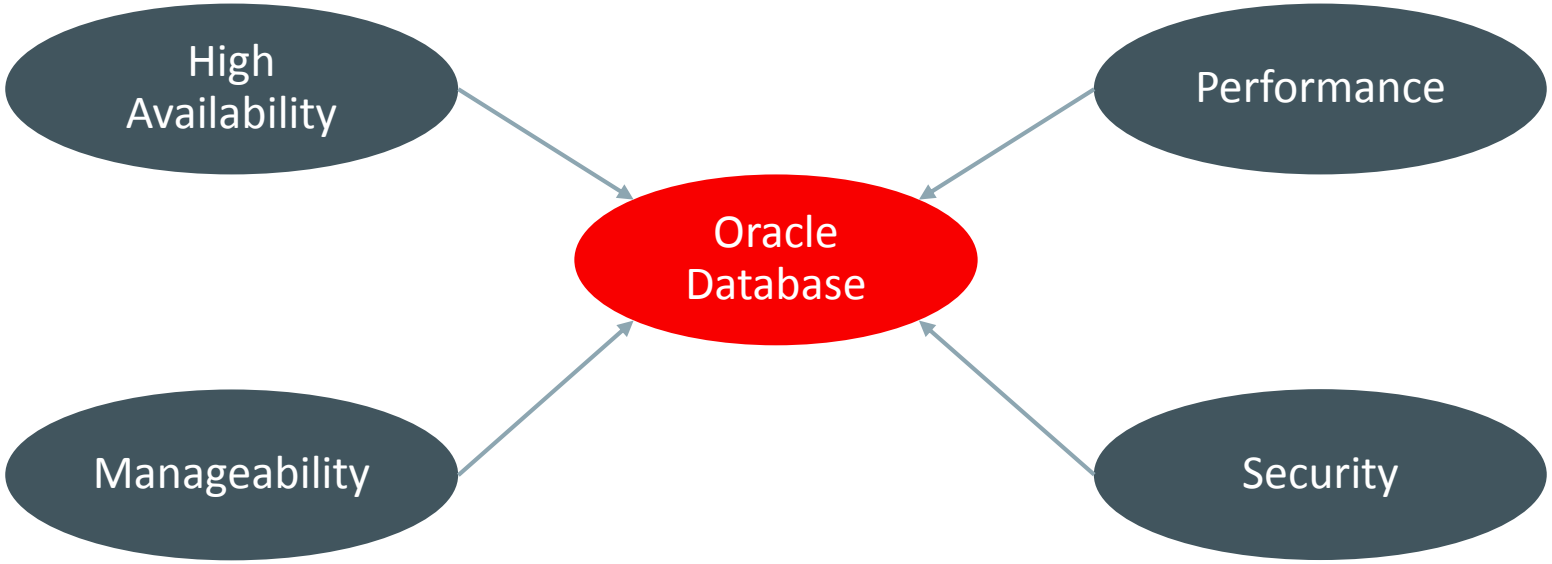
Oracle Database Online Documentation

Oracle Database Online Documentation 12c Release 1 (12.1) → Security
Security Guide - http://docs.oracle.com/database/121/DBSEG/toc.htm
Advanced Security Guide - http://docs.oracle.com/database/121/ASOAG/toc.htm
Database Vault Administrator's Guide - http://docs.oracle.com/database/121/DVADM/toc.htm

Source: Oracle Database Online Documentation 12c Release 1 (12.1) http://docs.oracle.com/database/121/index.html

Oracle Database Security

Oracle Database Security- Interesting Topic?



Example from Analogue World: Porsche Cayman GTS

Source: http://www.porsche.com/usa/models/cayman/cayman-gts/

Porsche Cayman GTS Safety

Safety Concept

Occupant protection is provided by the bodywork design, which has been optimized for stiffness, two full-size airbags fitted as standard and the Porsche Side Impact Protection System (POSIP) featuring two side airbags and steel side impact protection elements, respectively. To match the high engine power of the Cayman GTS, the front and rear axles are equipped with four-piston aluminum monobloc fixed brake calipers.

Source: http://www.porsche.com/usa/models/cayman/cayman-gts/safety/safety-concept/

Oracle Database Security for SAP NetWeaver

Oracle Database Security for SAP NetWeaver

SAP Guidelines

- Security Guidelines and Recommendations from SAP
  - SAP NetWeaver Security Guide http://help.sap.com/saphelp_nw73ehp1/helpdata/de/f3/780118b9cd48c7a668c60c3f8c4030/frameset.htm
  - General guidelines for installation and operation of SAP systems
  - For all operating systems
  - For all database systems

Oracle Database Security for SAP NetWeaver

Oracle Guidelines

- Generic recommendations from Oracle are available on
  - Oracle Database Online Documentations
  - Oracle My Oracle Support (MOS Notes)
  - Oracle Technology Network
    - http://www.oracle.com/technetwork/topics/security/articles/index.html
      - http://www.oracle.com/technetwork/database/security/twp-database-vault-bestpractices-132020.pdf

Oracle Database Security for SAP NetWeaver

Guidelines Specific for SAP NetWeaver on Oracle

- How to find specific recommendations for SAP on Oracle?
  - Do we have a complete checklist for Oracle Security for SAP NetWeaver? → No
  - Overview
    - SAP Note 1868094 - Overview: Oracle Security SAP Notes
  - Search internet 'sap security guidelines oracle':
    - Database Security for Oracle (White Paper Oracle Database Administration Feb 2012)
      - http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/9e626b1c-0d01-0010-b2ba-cfa2443c1cce?overridelayout=true
    - Oracle Security Solutions for SAP Environments (White Paper February 2014)
      - http://www.oracle.com/us/solutions/sap/oracle-security-for-sap-2148703.pdf
      - http://www.oracle.com/technetwork/server-storage/hardware-solutions/oos-sap-efficiency-performance-1849692.pdf

Oracle Database Security for SAP NetWeaver

SAP NetWeaver on Oracle Installation

- Standardized installation (path, users, components)
- Minimal Installation
  - Installs only Oracle software components needed by SAP application (until 11g)
  - Installs only Oracle database components needed by SAP application
    - Less components inside the database → less patching
    - Less components inside the database → faster upgrades
    - → No support for SAP on databases created by DBCA (with all components installed)

Oracle Database Security for SAP NetWeaver

SAP Oracle Database Configuration

- SAP Schema User (SAPSR3)
  - SAPSR3, SAP<SCHEMA_ID>
    - SAPCONN role, no DBA role → principle of least privilege
    - SAPUPROF user profile
- SAP database administration users for SAP BR*Tools
  - OPS$ accounts, BRT$ADM (with secure storage SSFS), BRTDBA
    - SAPDBA role, (DBA role) → principle of least privilege
    - SAPUPROF user profile

Oracle Database Security for SAP NetWeaver

SAP Oracle Database Configuration

- Locked Oracle Accounts
  - All database accounts except SYS, SYSTEM and SAP database accounts are locked by default
- Standardized database parameter
  - Security parameter are set to Oracle default (or according to SAP Notes)
  - Parameter REMOTE_OS_AUTHENT=FALSE (12c onwards)

Oracle Database Security for SAP NetWeaver

OS User concept for SAP NetWeaver on Oracle

- Windows platform:
  - Support for Oracle Home User in 12c (SAP Note 1915302)
- Unix platform:
  - User concept 'SAP CLASSIC' and 'ORACLE STANDARD' (SAP Note 1915323)
  - See DSAG / DOAG presentations from 2015

Oracle Database Security for SAP NetWeaver

Auditing

- Default is Oracle default
- No SAP-specific recommendations for configuration of auditing
- Customer-specific configuration possible
- As of 12c, unified auditing is possible to centralize audit records in a single place (see Database Security Guide, Introduction to Auditing).

Oracle Database Security for SAP NetWeaver

Oracle Transparent Data Encryption (TDE)

- Requires Advanced Security Option (ASO)
  - ASO is included in ASFU license
    - SAP Note 740897 - Info about the scope of the Oracle license; Required Oracle options
  - TDE Reference SAP Note: 974876 - Oracle Transparent Data Encryption (TDE)
  - Certified by SAP with Oracle Database 10g Release 2

Oracle Database Security for SAP NetWeaver

Database Vault (DV)

- Requires Database Vault Option
  - DV option is not included in ASFU license, requires additional license
    - SAP Note 740897 - Info about the scope of the Oracle license; Required Oracle options
  - DV reference SAP Note 1355140
  - Certified by SAP with Oracle Database 10g Release 2

Oracle Database Security for SAP NetWeaver

Patching

- Relevant from a security perspective (Critical Patch Update Program)
  - Critical Patch Update (CPU)
  - Security Patch Update (SPU)
  - Patch Set Update (PSU)
- Prevent errors proactively
- Oracle Critical Patch Updates and Security Alerts
  - http://www.oracle.com/technetwork/topics/security/alerts-086861.html
  - Example: Oracle Critical Patch Update Advisory – January 2016
  - http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

Oracle Database Vault

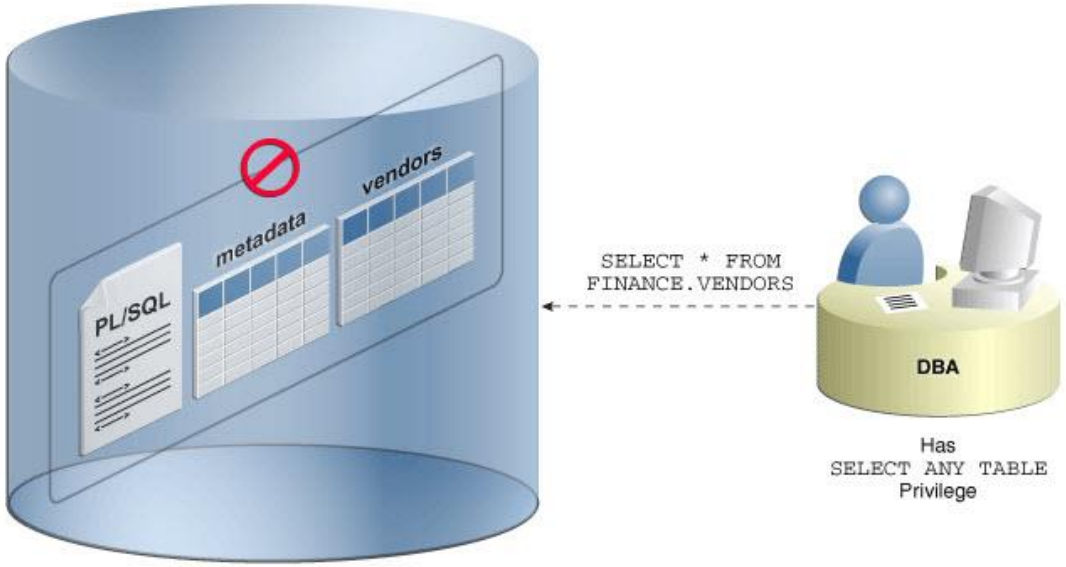
Oracle Database Vault Concept

Controls for Privileged Accounts

Privileged database accounts are one of the most commonly used pathways for gaining access to sensitive applications data in the database.

While their broad and unrestricted access facilitates database maintenance, the same access also creates a point of attack for gaining access to large amounts of data. Oracle Database Vault realms around application schemas, sensitive tables, and stored procedures provide controls to prevent privileged accounts from being exploited by intruders and insiders to access sensitive application data.

Figure 1-1 Oracle Database Vault Realm Blocking DBA Access to Data



Description of "Figure 1-1 Oracle Database Vault Realm Blocking DBA Access to Data"

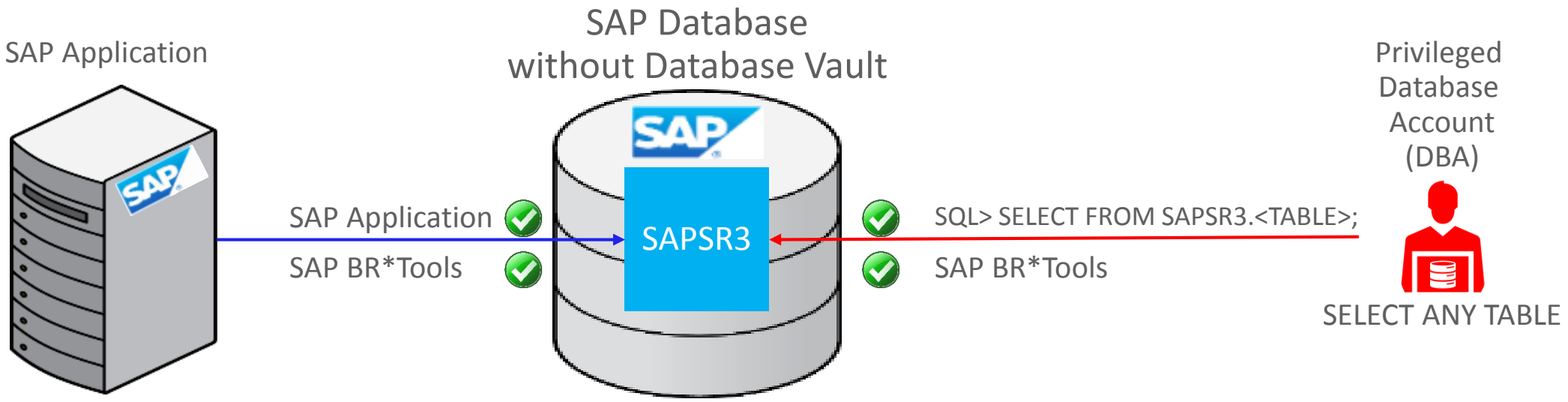
Source: Oracle Database Vault Administrator's Guide: 'Introducing Oracle Database Vault'

Oracle Database Vault Concept

- Goals:
  - Controlling access to sensitive SAP application data
  - Preventing unauthorized access to sensitive SAP application data
  - Preventing unauthorized changes to production environments

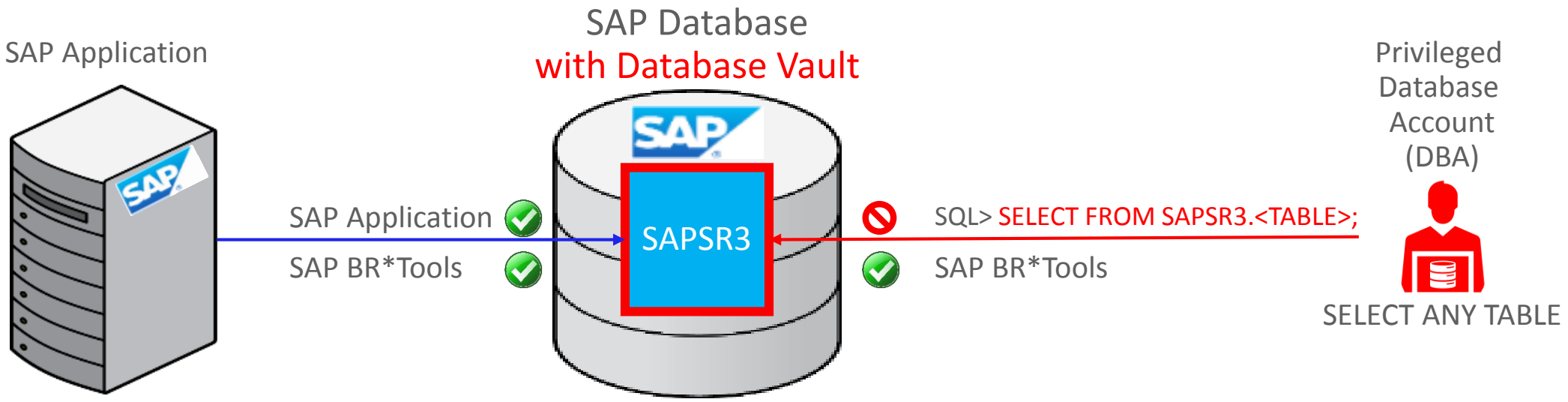
Source: Oracle Database Vault Administrator's Guide: 'Introducing Oracle Database Vault'

Oracle Database Vault Concept



Source: Oracle Database Vault Administrator's Guide: 'Introducing Oracle Database Vault'

Oracle Database Vault Concept



Source: Oracle Database Vault Administrator's Guide: 'Introducing Oracle Database Vault'

Oracle Database Vault Concept

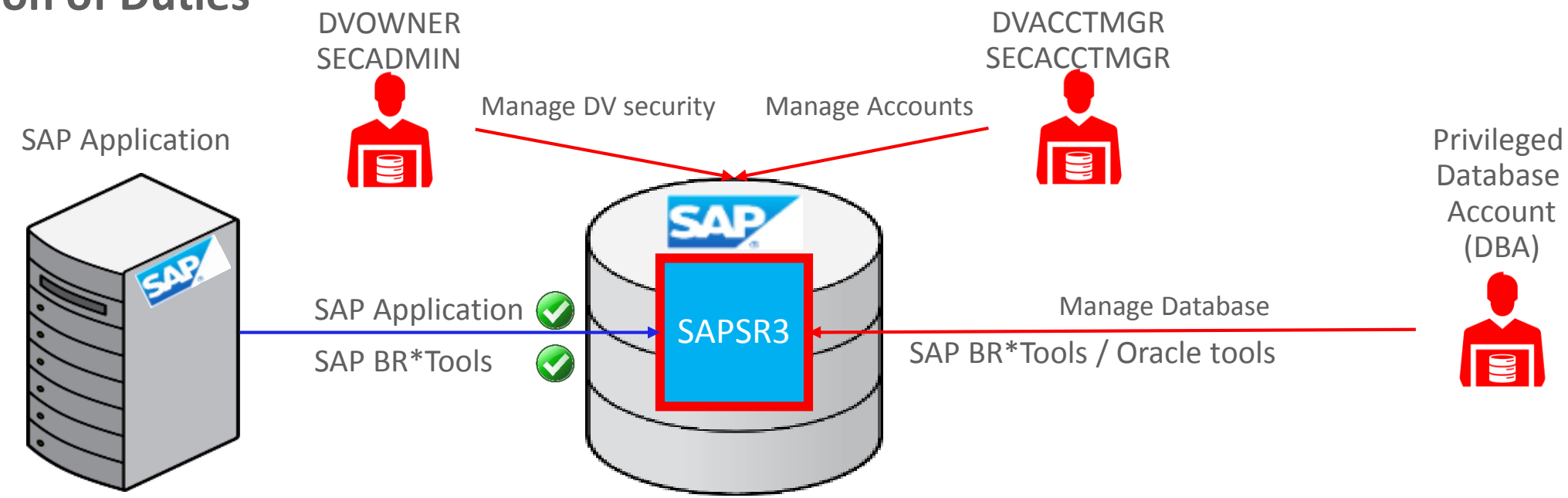
- Oracle Database Vault
  - is a Database Option that must be licensed
  - Is a Database Component that needs to be installed
- Oracle Database Vault
  - Implements an additional concept for controlling access to application data.
    - Classic concept is based on database roles and database system privileges.
    - Database Vault protection is based on realms, rules, factors.
- Oracle Database Vault
  - Is transparent for the SAP application
  - Is not transparent for all administration tasks

Oracle Database Vault Concept

- Oracle Database Vault
  - Is based on the concept of separation of duties (SoD).
    - Database Administration
      - SYS, SYSTEM, …
    - Database Vault Security Administration (DVOWNER)
      - SECADMIN
      - Administration of DV security policies (enable/disable DV, configure DV policies)
    - Database Vault Account Administration (DVACCTMGR)
      - SECACCTMGR
      - SAPACCTMGR
      - Administration of database accounts (CREATE USER/DROP USER/ALTER USER/PASSWORD)

Oracle Database Vault for SAP NetWeaver

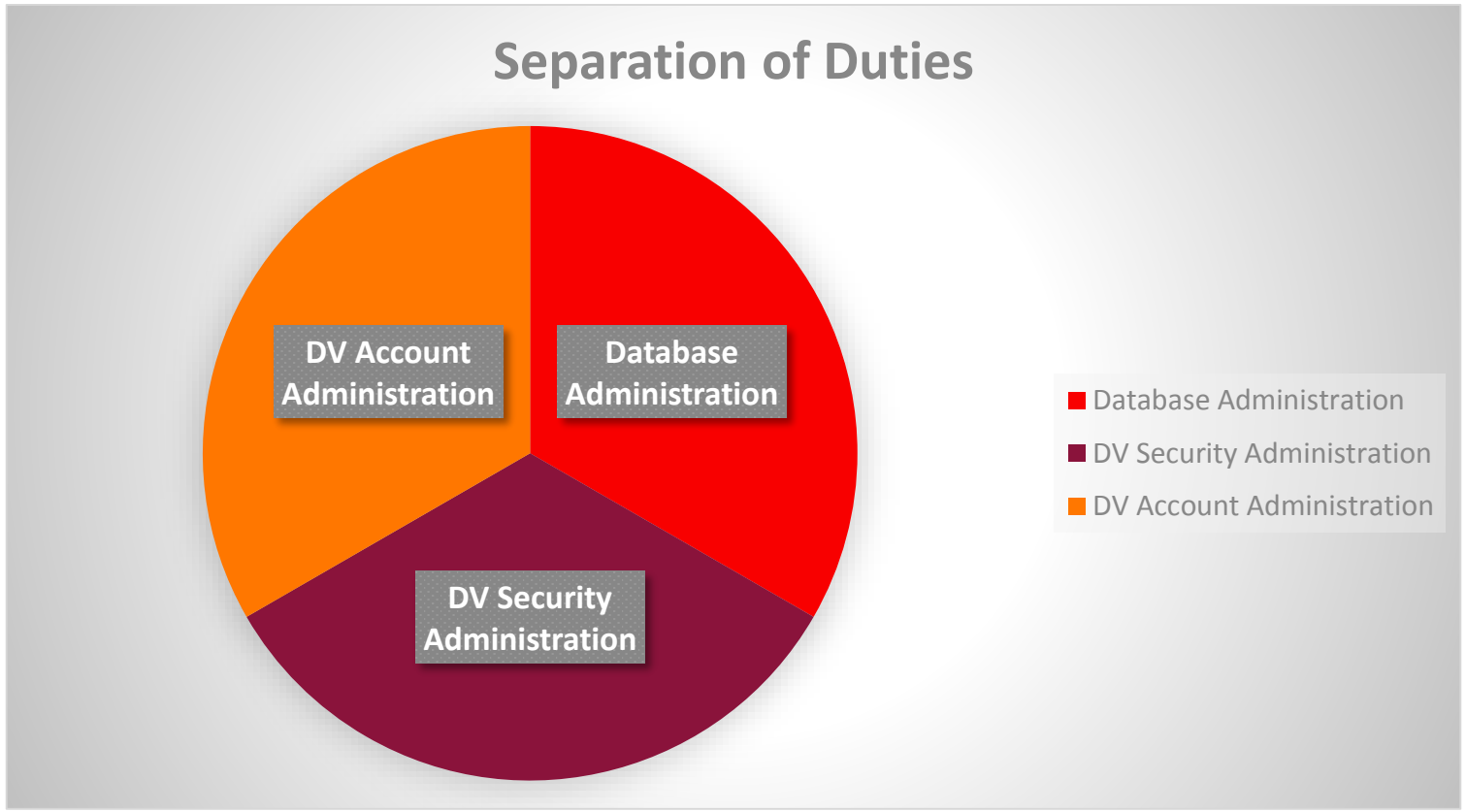
Separation of Duties



Separation of Duties: Security Administration, Account Management, Database Administration

Oracle Database Vault for SAP NetWeaver

Separation of Duties



Oracle Database Vault 12c for SAP

12c Release 1

Oracle Database Vault 12c R1 for SAP NetWeaver

Release Status and Technical Requirements

- Released for SAP in December 2015
  - Reference: SAP Note 1914631
- Requirements
  - same as for 12c R1 in general, see SAP Note 2218115
- Supported for all types of installations and all platforms
- Installation / Configuration
  - SAP-specific configuration scripts (SQL, PL/SQL) are shipped as database patch 9656644

Oracle Database Vault 12c for SAP

Installation

Oracle Database Vault 12c R1 for SAP NetWeaver

Database Vault Installation Steps

1. Install required Oracle Database Components (as SYS)
2. Create additional SAP-specific database users and roles (as SYS)
3. Enable Oracle Database Vault in the database (as SECADMIN)
4. Configure Oracle Database Vault for SAP (as SECADMIN)

Note: you could also run the steps in order 1., 2., 4., 3.

Oracle Database Vault 12c R1 for SAP NetWeaver

Installing Required Database Components

- Database components to install:
  - Database Vault (DV)
  - Label Security (OLS)
- Installation method
  - Script-based installation
  - DBCA

For details see SAP note 2218115.

Oracle Database Vault 12c R1 for SAP NetWeaver

Create additional SAP-specific database users and roles

- User / Roles to create:
  - SECADMIN → Database Vault Security Administrator (DVOWNER)
  - SECACCTMGR → Database Vault Account Manager (DVACCTMGR)
  - SAPACCTMGR → Account Manager for SAP application user
  - SAPSYS → Database role for segment administration in SAP realms
  - BRTDBA → Database user for BRSPACE for segment administration in SAP realms
  - BRT$ADM → Database user for BR*Tools (with SSFS, replaces OPS$ users)

For details see SAP note 2218115.

Oracle Database Vault 12c R1 for SAP NetWeaver

Enable Database Vault (11.2)

1. Stop the instance
2. In 11.2, enable DV in the software:
   Relink Oracle software (chopt) as software owner (SAP Note 1502377):
   OS> chopt enable lbac
   OS> chopt enable dv
3. Restart the instance

Oracle Database Vault 12c R1 for SAP NetWeaver

Enable Database Vault (12.1)

1. Stop the instance
2. Enable DV in the database (as DVOWNER or DVADMIN):
   For details see SAP note 2218115.
   SQL> EXEC DBMS_MACADM.ENABLE_DV
3. Restart the instance

For details see SAP note 2218115.

Oracle Database Vault 12c R1 for SAP NetWeaver

Configuring Database Vault for SAP NetWeaver

- As Database Vault security administrator (DVOWNER) SECADMIN, you can configure Database Vault for SAP NetWeaver (details see below)
  - SQL> @dv_policy policy create

    This command creates / configures the
    "SAP NetWeaver Database Vault Standard Policy"

For details see SAP note 2218115.

Oracle Database Vault 12c R1 for SAP NetWeaver

Installation and Configuration Scripts Overview (*)

Database Components	Users / Roles	Database Vault Policy	Others
dv_install_ols.sql	dv_create_sapsys.sql (role)	dv_policy.sql	dv_check.sql
dv_install_dv.sql	dv_create_dvowner.sql (user)	dv_enable_dv.sql	dv_recompile.sql
dv_configure_ols.sql	dv_create_dvacctmgr.sql (user)	dv_disable_dv.sql	dv_lock_accounts.sql
dv_configure_dv.sql	dv_create_sapacctmgr.sql (user)		
	dv_create_brtdba.sql (user)		
	dv_create_brtadm.sql (user)		

All scripts are included in generic database patch 9656644 and are installed into <ORACLE_HOME>/sap/ora_dbvault.
(*) All scripts mentioned above refer to the initial patch version. Note that contents of the patch including scripts and script names are subject to change

Oracle Database Vault 12c Release 1 for SAP

SAP NetWeaver Database Vault Standard Policy Design Principles

Oracle Database Vault 12c R1 for SAP NetWeaver

SAP NetWeaver Database Vault Standard Policy

- Configuration / design principles
  - Simple out-of-the-box base configuration
  - Considers SAP BR*Tools as SAP-standard administration tools for Oracle
  - DBAs should not be limited or blocked from their daily tasks
  - Extensible by customer (if needed)

Oracle Database Vault 12c R1 for SAP NetWeaver

SAP NetWeaver Database Vault Standard Policy

- Simple out-of-the-box base configuration
  - Design is not complex
  - Configuration step is easy (script based: dv_policy.sql)

Oracle Database Vault 12c R1 for SAP NetWeaver

SAP NetWeaver Database Vault Standard Policy

- Considers SAP BR*Tools as SAP-standard administration tools for Oracle
  - BR*Tools specific DV realms
  - BR*Tools specific database user (eg. BRTDBA)

Oracle Database Vault 12c R1 for SAP NetWeaver

SAP NetWeaver Database Vault Standard Policy

- DBAs should not be limited or blocked from their daily tasks
  - The following types of administrative tasks are affected by Database Vault:
    - Access to SAP Application data
      - Datapump Export / Datapump Import / SELECT * from <SAPSR3>.<table>
    - Applying database patches
      - Requires certain privileges (DV_PATCH_ADMIN role) that must be granted by security administrator
    - Management of database users → SECACCTMGR / SAPACCTMGR
      - CREATE/ALTER/DROP USER
      - Change password of database users
      - Change password of SAP schema user (eg. SAPSR3)

Oracle Database Vault 12c R1 for SAP NetWeaver

SAP NetWeaver Database Vault Standard Policy

- Extensible by customer (if needed)
  - Most SAP customers do not modify or extend the SAP-standard policy
  - Example for customer specific requirements
    - Use of non-standard administration accounts
    - Use of non-SAP tools or applications that need access to SAP application tables (or a subset of tables)

Oracle Database Vault 12c Release 1 for SAP

SAP NetWeaver Database Vault Standard Policy Internals

SAP NetWeaver Database Vault Standard Policy

Requirements

1. SAP application must be able to connect to the database and select and modify SAP application data (as SAP schema user)
2. SAP BR*Tools must be able to select and modify data of the SAP BR*Tools dictionary tables (SDBAH, SDBAD, …) (as different admin users)
3. For daily administration tasks, Oracle tools and SAP BR*Tools should work without configuration change.
4. For certain administration tasks, a change due to Database Vault is required and should be acceptable (must be accepted).

SAP NetWeaver Database Vault Standard Policy

Requirements

Daily Administration Tasks
Check database eg. brconnect -u / -f check
Backup database eg. brbackup -u / … -m all
Backup archive logs eg. brarchive -u / …
Update table statistics eg. brconnect -u / -f stats -t all

SAP NetWeaver Database Vault Standard Policy

Requirements

Infrequent Administration Tasks	
Applying patches	→ requires authorization from DV Security Administrator
Export / Import SAP application data (data pump)	→ requires authorization from DV Security Administrator
Access to an SAP application table (e.g. support)	→ requires authorization from DV Security Administrator
Changing the password of the SAP application user	→ requires special user: SAPACCTMGR
Online redefinition of SAP tables/indexes	→ requires special user: BRTDBA

SAP NetWeaver Database Vault Standard Policy Internals

Steps to define the Database Vault Policy for SAP NetWeaver

Step
1. Create realm "SAP NetWeaver Realm for ABAP stack" to protect all objects owned by SAP<SCHEMA_ID> (SAPSR3).
2. Create realm "SAP NetWeaver Realm for Java stack" to protect all objects owned by SAP<SCHEMA_ID>DB.
3. Create realm "SAP NetWeaver Realm for SAP BR*Tools" to allow access to SAP BR*Tools dictionary objects for SAP BR*Tools admin accounts. 'SDBAH', 'SDBAD', 'DBAML', 'DBARCL', 'DBAFID', 'DBAEXTL', 'DBAREOL', 'DBABARL', 'DBADFL', 'DBAOPTL', 'DBASPAL', 'DBABD', 'DBABL', 'DBATL', 'DBAOBJL', 'DBAPHAL', 'DBAGRP', 'DBAERR', 'DBATRIAL', 'DBSTATC', 'DBSTATTORA', 'DBSTATIORA', 'DBSTATHORA', 'DBSTAIHORA', 'DBMSGORA', 'DBCHECKORA', 'MLICHECK', 'TGORA', 'IGORA', 'TSORA', 'TAORA', 'IAORA', 'SVERS', 'CVERS', 'DD02L', 'DD09L', 'DDNTT', 'DDART', 'DARTT', 'DBCHK', 'DBDIFF', 'SAPLIKEY', 'RSNSPACE', 'RSPSPACE', 'DDLOG'
4. Identify SAP Standard Database Accounts used to run SAP BR*Tools SYS, SYSTEM, OPS$ORA<DBSID>, OPS$<SAPSID>ADM, OPS$ORACLE, OPS$SAPSERVICE<SAPSID>, BRT$ADM, BRTDBA
5. Authorize users for Database Vault Realms SAP NetWeaver Realm for ABAP stack : SAPSR3 + certain BR*Tools admin accounts SAP NetWeaver Realm for Java stack : SAPSR3DB + certain BR*Tools admin accounts SAP NetWeaver Realm for SAP BR*Tools: All BR*Tools administration accounts

SAP NetWeaver Database Vault Standard Policy

Comparison 11.2 <-> 12.1

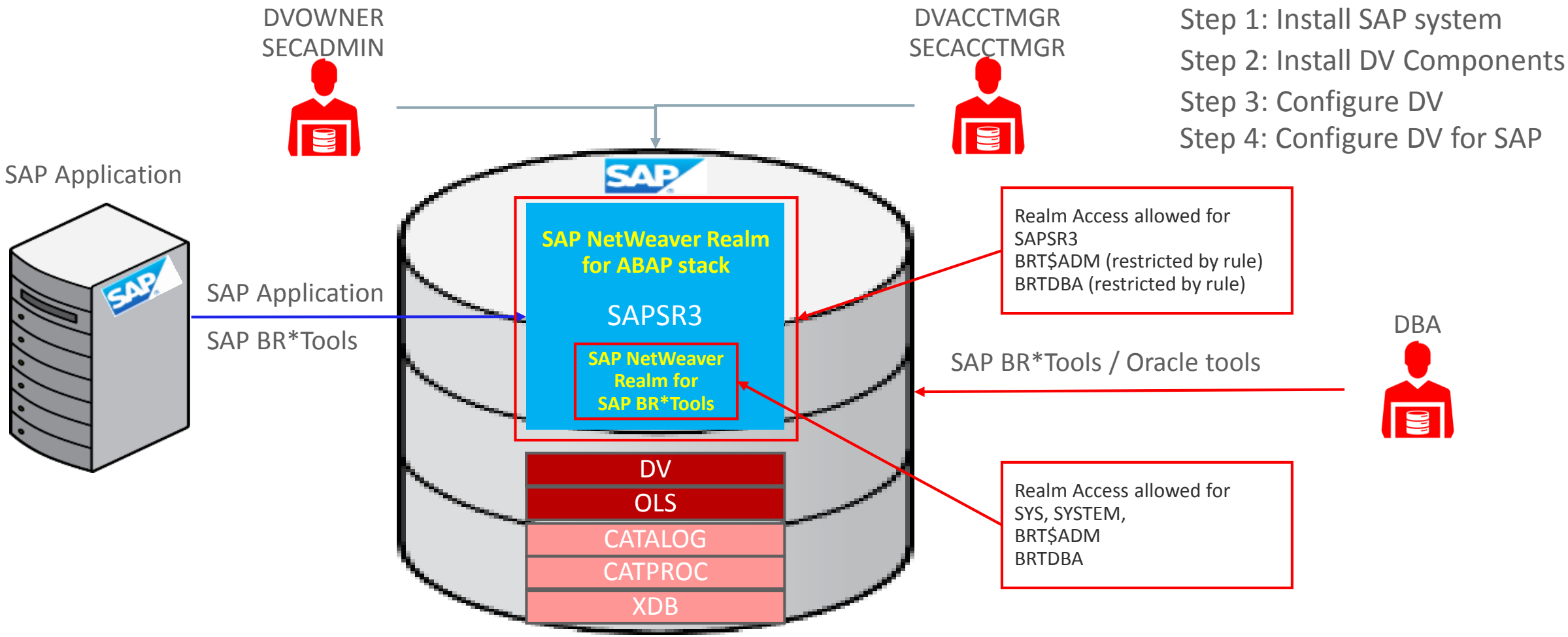
- In 11.2 there are rules to identify SAP programs by program name.
  - Requires CONNECT command rule in 11.2
  - For new programs the rule must be adapted.
- In 12c access to SAP tables is solely based on user/password authentication.
  - No CONNECT command rule required.
  - If a DBA knows the password of SAP application user SAPSR3, he can connect and access SAP application data.

SAP NetWeaver Database Vault Standard Policy

Comparison 11.2 <-> 12.1

- In 11.2 database roles (e.g. SAPDBA) are used for authentication to SAP realms.
  - Requires additional realm to control / prevent modification of these roles
  - Requires GRANT command rule to control GRANT operations
- In 12c authentication to SAP realms is based on user names.
  - DBA can update SAP-specific database roles (eg SAPCONN, SAPDBA)
  - Granting database role SAPDBA to another database user does not authorize this user for access to a realm.

SAP NetWeaver Database Vault Standard Policy Internals



Additional Recommendations

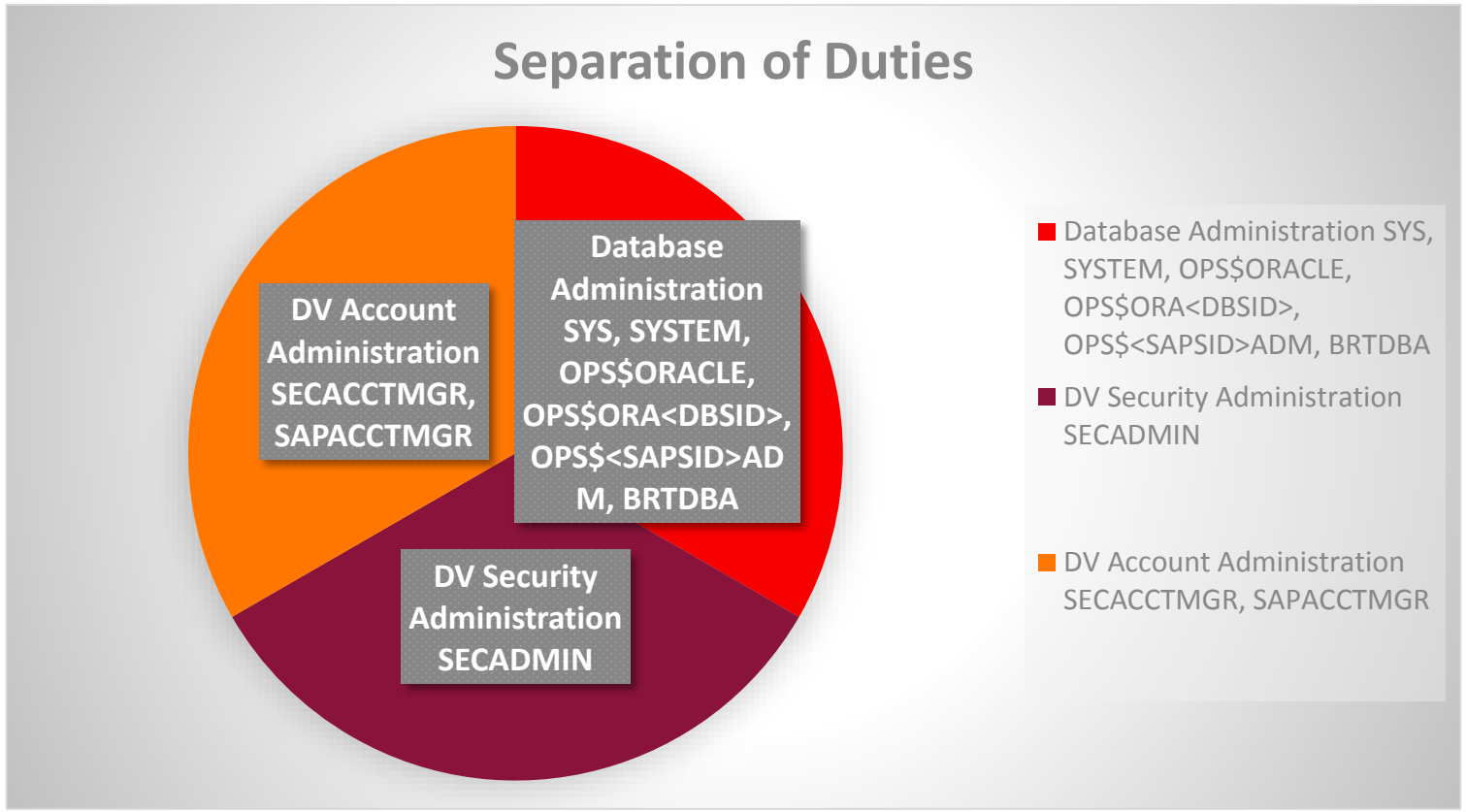
Recommendations

Reference: SAP Note 2218115 - Oracle Database Vault 12c

- Configure SAP BR*Tools with SSFS (SAP Note 1764043)
  - Database Vault policy for SAP NetWeaver becomes more simple
  - More secure (no local OPS$ connects)
  - BRT$ADM replaces OPS$ users
  - Starting 12c SSFS must be configured for the SAP application
    - Reference: SAP Note 1914631 (SSFS: SAP Notes 1639578 and 1622837)

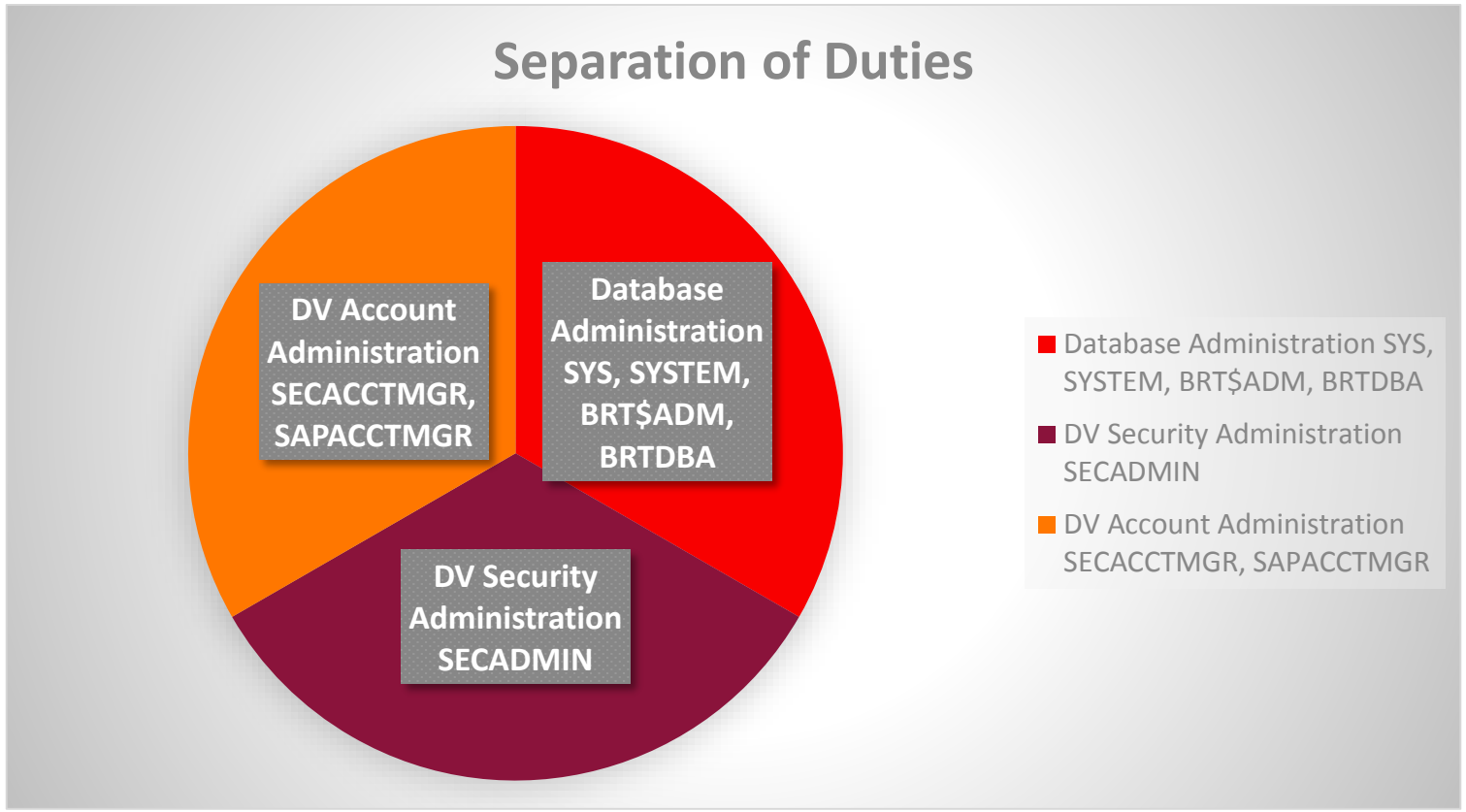
Oracle Database Vault for SAP NetWeaver

Administrative Database Accounts without SSFS for BR*Tools



Oracle Database Vault for SAP NetWeaver

Administrative Database Accounts with SSFS for BR*Tools



Outlook

Future plans

Outlook

Fine-tuning for SAP NetWeaver Database Vault Standard Policy

- Extending dv_policy.sql for Security Administrator
  - Authorizing additional administrators for SAP realms
    - SQL> @dv_policy authorize <user>
    - SQL> @dv_policy unauthorize <user>
  - Authorizing for datapump operations
    - SQL> @dv_policy authorize_dp <user> [<schema> [<table>]]
    - SQL> @dv_policy unauthorize_dp <user> [<schema> [<table>]]

Outlook

Upgrade from 11g R2 → 12c R1 with Database Vault

- SAP NetWeaver Database Vault Standard Policy 11g differs from SAP NetWeaver Database Vault Standard Policy 12c
  - It is planned to smoothly upgrade the policy when you upgrade to 12c

References

References

SAP Notes

Oracle Database Security
1868094 - Overview: Oracle Security SAP Notes

Oracle Database Vault 12c Release 1
1355140 - Using Oracle Database Vault in an SAP environment
2218115 - Oracle Database Vault 12c

References

Oracle Database Online Documentation

Oracle Database Online Documentation 12c Release 1 (12.1) http://docs.oracle.com/database/121/index.html
Security Guide - http://docs.oracle.com/database/121/DBSEG/toc.htm
Advanced Security Guide - http://docs.oracle.com/database/121/ASOAG/toc.htm
Oracle Database Vault Administrator's Guide - http://docs.oracle.com/database/121/DVADM/toc.htm

Oracle Technology Network (OTN) http://otn.oracle.com/ or http://www.oracle.com/technetwork/index.html
Security Articles & Whitepapers - http://www.oracle.com/technetwork/topics/security/articles/index.html
Best Practices - http://www.oracle.com/technetwork/database/security/twp-database-vault-bestpractices-132020.pdf

References

SAP Notes

Oracle Database Vault 12c Release 1
2218115 - Oracle Database Vault 12c
1355140 - Using Oracle Database Vault in an SAP environment

Oracle Database Security
1868094 - Overview: Oracle Security SAP Notes

Hardware and Software
Engineered to Work Together


ORACLE®