Recent Database Security Innovations You Might Not Be Using, But Should Be

TIP4112

Alan Williams, Senior Principal Product Manager
Russ Lowenthal, Director Product Management

Oracle Database Security
October 2018

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

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.

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Data Breaches are Growing and Databases are the Target

Database is the most common asset involved in a breach attack.

#1

Stolen credentials were the #1 cyberattack method used in 2017 breaches

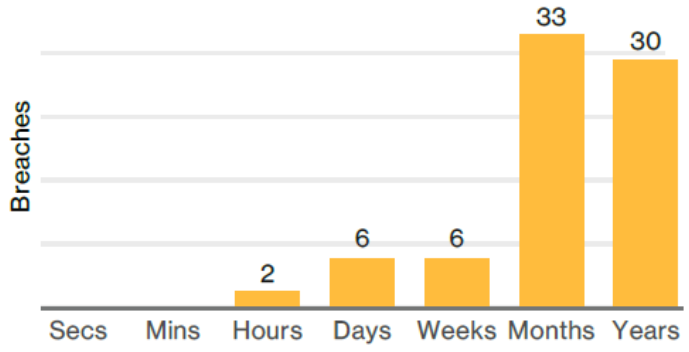


Figure 45: Breach discovery timeline within Insider and Privilege Misuse (n=77)

Good

78% will not click any phishing emails

Bad

4% will click on any phishing email

Source: Privacyrights.org; 2017-2018 Verizon Data Breach Investigations Report

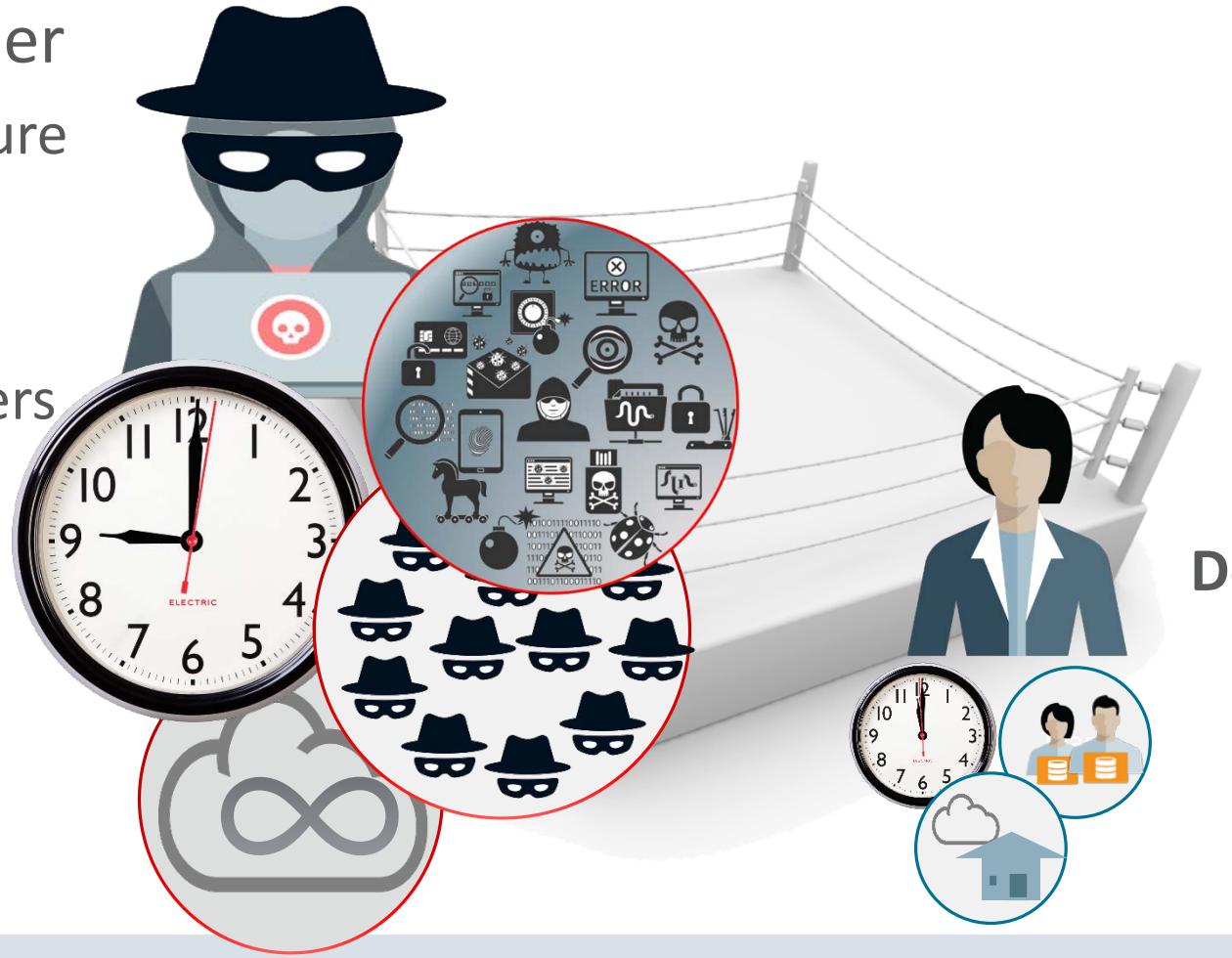
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

This is an Asymmetric Battle

The Bad Guys Have the Advantage

Challenger's Corner

- All the infrastructure
- All the tools
- All the time
- A legion of attackers



Defender's Corner

- Not enough people
- Not enough resources
- Not enough time

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Oracle Has Been Doing Database Security for a Long Time

Oracle8i

Database Auditing

Network Encryption

Database Encryption API

Virtual Private Database

Strong authentication

Label Security

Oracle Database 9i

Fine Grained Auditing

Secure Configuration Scanning

Transparent Data Encryption

Database Vault

Oracle Database 10g

Data Masking and Subsetting

Audit Vault and Database Firewall

Privilege Analysis

Oracle Database 11g

Data Redaction

Real Application Security

Conditional Auditing

Key Vault

Oracle Database 12c

DBSAT

CMU-AD

Oracle Database 18c

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Let’s Look at Your Security Concerns

- How do I protect against database misconfigurations?
- How can I convert an unencrypted database to TDE?
- How do I manage database users with my enterprise’s directory service?
- How do I guard against unauthorized access through application schemas?
- How do I minimize the attack surface associated with privileged users?
- How can I design effective Database Vault policies for my application?
- How can I control which SQL commands users can run, and when?
- How can I manage audit data across multiple processes and activities?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Database Security Assessment Tool (DBSAT)

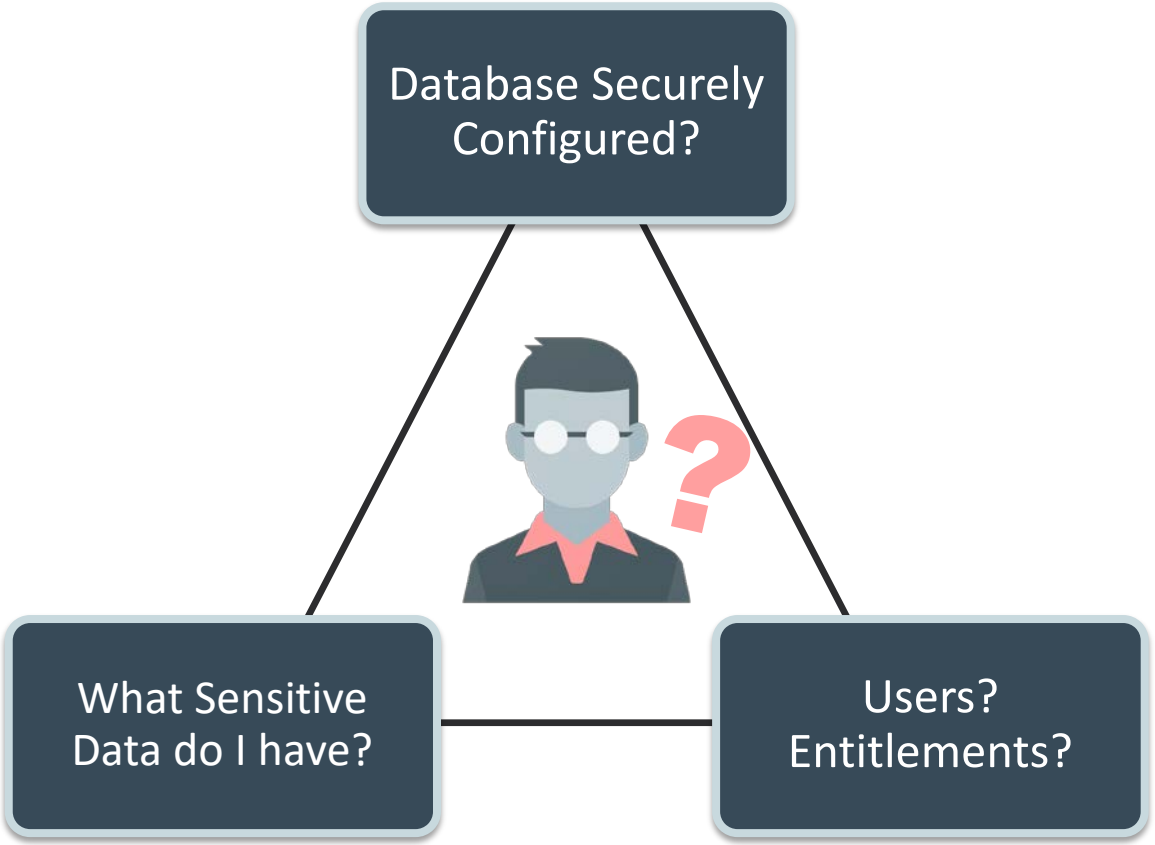
How do I know if my database is securely configured?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Oracle Database Security Assessment Tool (DBSAT)

Know Your Security Posture Before Hackers Do

- Understand how (in)secure your database is
  - Report on overall security status
  - Find the users, entitlements, and risks
  - Discover sensitive data in English, German, Dutch, French, Italian, Spanish & Portuguese *
- Actionable Assessment Reports
  - Summary and detailed information
  - Prioritized recommendations
  - Mapping to EU GDPR, CIS Benchmark and STIG *
- Stand-alone light weight tool: Quick, Easy
- **FREE** to current Oracle customers



* In upcoming release

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

DBSAT: Security Assessment Finding

Category of the Finding

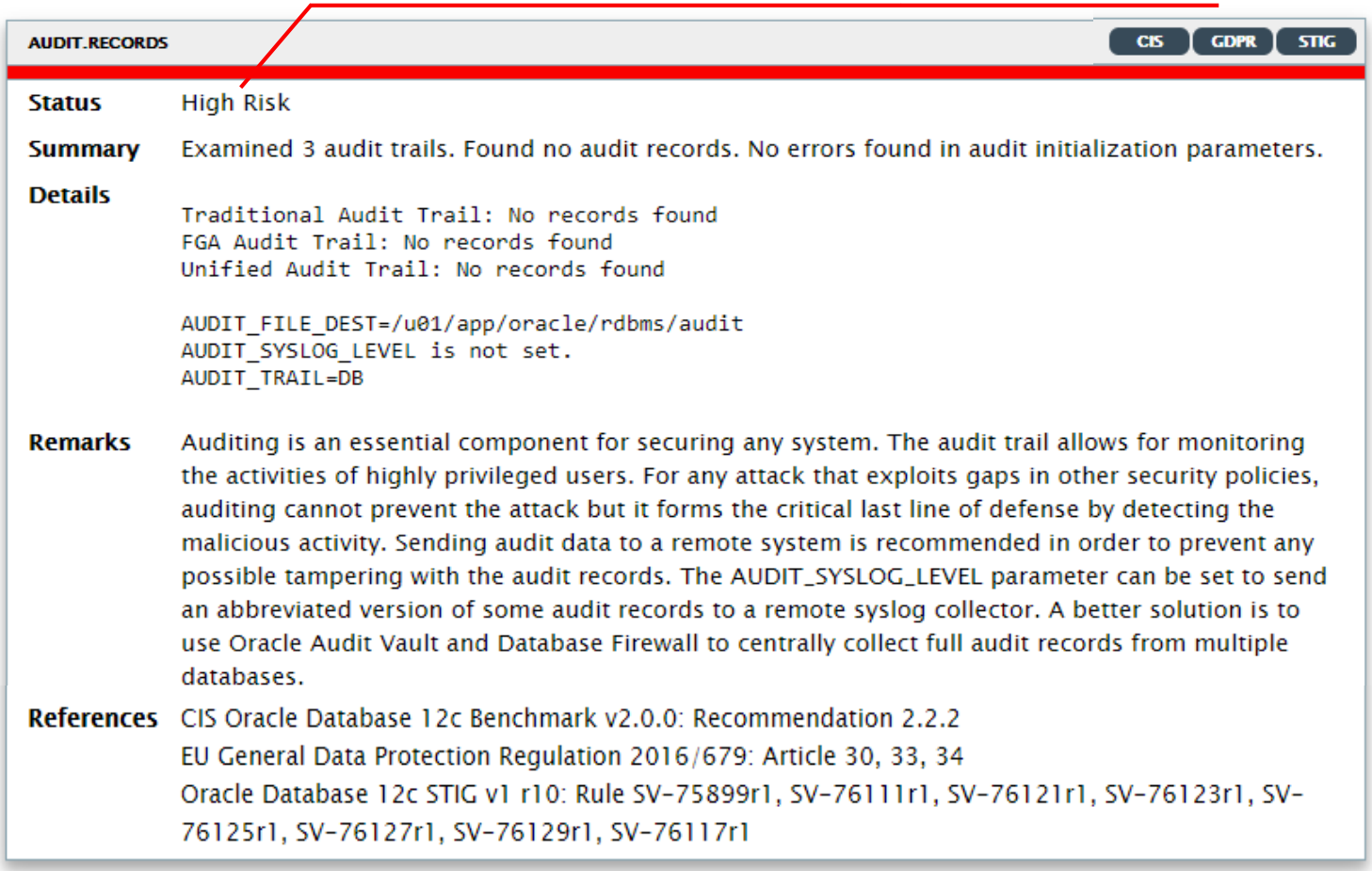
Evaluate, Advisory, Pass, Low Risk, Medium Risk, High Risk

Applicability to Standards & Regulations

Details of the Finding

Rationale and Recommendations

Mapping to Regulations



AUDIT.RECORDS CIS GDPR STIG

Status High Risk

Summary Examined 3 audit trails. Found no audit records. No errors found in audit initialization parameters.

Details

```
Traditional Audit Trail: No records found
FGA Audit Trail: No records found
Unified Audit Trail: No records found

AUDIT_FILE_DEST=/u01/app/oracle/rdbms/audit
AUDIT_SYSLOG_LEVEL is not set.
AUDIT_TRAIL=DB
```

Remarks Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity. Sending audit data to a remote system is recommended in order to prevent any possible tampering with the audit records. The AUDIT_SYSLOG_LEVEL parameter can be set to send an abbreviated version of some audit records to a remote syslog collector. A better solution is to use Oracle Audit Vault and Database Firewall to centrally collect full audit records from multiple databases.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 2.2.2
EU General Data Protection Regulation 2016/679: Article 30, 33, 34
Oracle Database 12c STIG v1 r10: Rule SV-75899r1, SV-76111r1, SV-76121r1, SV-76123r1, SV-76125r1, SV-76127r1, SV-76129r1, SV-76117r1

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

DBSAT: Sensitive Data Assessment Report

Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
PII – ADDRESS	8	12	1024
PII – BIOMETRIC DATA	1	1	4
PII – CATEGORIZATION DATA	1	2	630
PII – CONTACT DETAILS	3	6	1056
PII – IT DATA	1	1	288
PII – JOB DATA	7	15	1217
PII – NAMES	3	6	1056
TOTAL	15*	43	1584**

Sensitive Column Details

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type
HR	COUNTRIES	COUNTRY_NAME	Country name	PII – ADDRESS	COUNTRY
HR	DEPARTMENTS	MANAGER_ID	Manager_id of a...	PII – JOB DATA	EMPLOYEE IDENTIFICATION NUMBER
HR	EMPLOYEES	COMMISSION_PCT	Commission per...	PII – JOB DATA	VARIABLE INCOME
HR	EMPLOYEES	EMAIL	Email id of the e...	PII – CONTACT DETAILS	EMAIL
HR	EMPLOYEES	EMPLOYEE_ID	Primary key of e...	PII – JOB DATA	EMPLOYEE IDENTIFICATION NUMBER

Schemas with Sensitive Data

Risk Levels	High Risk, Medium Risk
Summary	Found 5 schemas with sensitive data.
Location	Schemas with sensitive data: HR, IX, OE, PM, SH

Risk Level: High Risk

Security for Environments with High Value Data: Detective plus Strong Preventive Controls
Highly sensitive and regulated data should be protected from privileged users, and from users without a business need for the data. Activity of privileged accounts should be controlled to protect against insider threats, stolen credentials, and human error. Who can access the database and what can be executed should be controlled by establishing a trusted path and applying command rules. Sensitive data should be redacted on application read only screens. A Database Firewall ensures that only approved SQL statements or access by trusted users reaches the database – blocking unknown SQL injection attacks and the use of stolen login credentials.

Recommended controls include:

- **Audit all sensitive operations including privileged user activities**
- **Audit access to application data that bypasses the application**
- **Encrypt data to prevent out-of-band access**
- **Mask sensitive data for test and development environments**
- **Restrict database administrators from accessing highly sensitive data**
- **Block the use of application login credentials from outside of the application**
- **Monitor database activity for anomalies**
- **Detect and prevent SQL Injection attacks**
- ***Evaluate: Oracle Audit Vault and Database Firewall, Oracle Advanced Security, Oracle Data Masking and Subsetting, Oracle Database Vault***

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

NEW

DBSAT version (2.0.3) New Features

- STIG rules highlighting
- New findings on password file, global names, instance name RMAN backups and more
- Simplify identification of directly granted System Privileges.
  - Now marked with (<-)

- Now includes sensitive pattern files for Portuguese, Spanish, Italian, French, German and Dutch
- New Sensitive Types, Categories and Subcategories
- Sensitive Data Categories now grouped by Risk Level
- Report include remarks and recommended controls for different Risk Levels

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Unified Audit

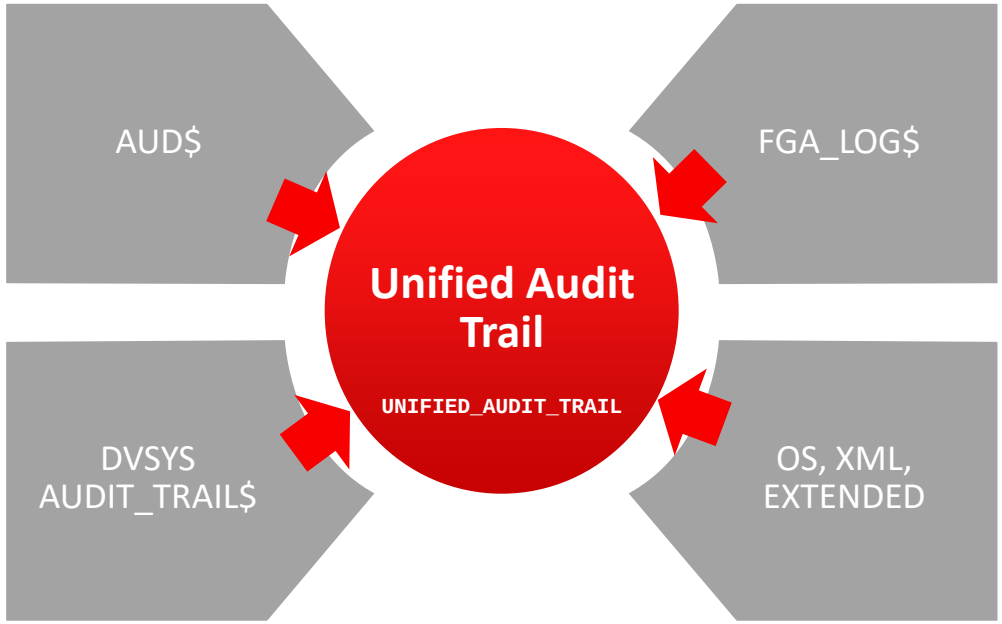
How can I pull together the various audit trails in the database and create fine grained audit policies?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Unified Audit

Advantages

- Superior Performance
- More Secure Audit Trail
- Improved Separation of Duties
- More Efficient Storage

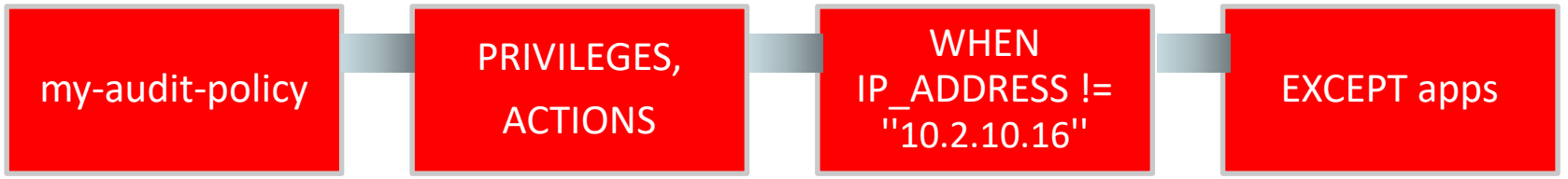


Audit Viewer Role

- View audit data

Audit Admin Role

- Manage policies
- Manage audit data



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

A few Unified Audit Capabilities

- Audit based on conditions like client IP address or program module

```
CREATE AUDIT POLICY from_application  ACTIONS ALL
    WHEN '(upper(sys_context (''userenv'', ''module'')) 
!= ''MYAPPNAME'') OR (sys_context(''userenv'', 
''ip_address'') != ''10.2.10.16'')' EVALUATE PER SESSION;
```

- Audit based on role membership

```
CREATE AUDIT POLICY privileged_actions ACTIONS ALL
ONLY TOPLEVEL;

AUDIT POLICY privileged_actions BY USERS WITH
GRANTED ROLES dba;
```

- Extend the audit trail to include additional information

```
AUDIT CONTEXT NAMESPACE ebusiness_context
ATTRIBUTES form, action, active_responsibility;
```

- Exception-based auditing

```
CREATE AUDIT POLICY application_bypass ACTIONS
SELECT ON hr.employees;

AUDIT POLICY application_bypass EXCEPT apps;
```

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

A few more Unified Audit Capabilities (there are MANY more!)

- Audit based on the component used

```
CREATE AUDIT POLICY dp_operations ACTIONS
COMPONENT = DATAPUMP IMPORT, EXPORT;

AUDIT POLICY dp_operations BY system;
```

Supported components include:

- FGA
- Database Vault
- Real Application Security
- OLS
- Data Pump
- RMAN
- Direct Path Load
- KSACL (Kernel Service Access Control List)
- Protocol (HTTP, FTP)

- Use predefined (default) audit policies

```
AUDIT POLICY ora_logon_failures WHENEVER NOT
SUCCESSFUL;
```

Predefined policies include:

- ORA_SECURECONFIG replicates the historical Oracle "Secure Configuration" audit recommendations
- ORA_LOGON_FAILURES audits failed logons
- ORA_DATABASE_PARAMETER audits changes to Oracle Database parameters
- ORA_ACCOUNT_MGMT audits changes to user accounts and grants of privileges
- ORA_CIS_RECOMMENDATIONS audits using Center for Internet Security (CIS) recommendations

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

TDE On-line/Off-line Tablespace Encryption Conversion

How can I encrypt my database files without downtime?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Why Transparent Data Encryption (TDE)?

- Encrypts columns or entire tablespaces
- Protects the database files on disk and on backups
- High-speed performance
- Transparent to applications, no changes required
- Integrated with Oracle DB technologies
- Ability to scale TDE deployments with OKV

- Many production applications have large (multi TB) schemas
- Resource requirements for conversion can be significant
- Many production applications cannot afford downtime

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Why Use Tablespace Conversion Features?

- Migrating existing clear data to encrypted data without downtime or with minimal downtime was a major impediment to TDE adoption
- Online/offline tablespace conversion options removes this impediment
- Two options:
  - Online tablespace conversion to migrate with no downtime
  - Fast offline tablespace conversion to migrate with minimal incremental storage requirements
  - Offline capabilities back ported in 11gR2 and 12c

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Online vs. Fast Offline Tablespace Conversion

Functionality	Offline Encryption	Online Encryption
When can I run the conversion?	Offline tablespace OR Database in mount stage	Online tablespace AND Database is open in read write mode
Do I need to plan for downtime?	Requires temporarily taking the tablespace offline, unless using Data Guard	No, encrypts tablespace in background with no downtime
Do I need additional storage space?	No	Yes, storage overhead is only 2x the largest tablespace file
Can I run encryption operations in parallel?	Yes, enables simultaneous encryption of multiple data files across multiple cores	Yes, at the tablespace level with multiple sessions running
Can data encryption keys be rekeyed or rotated?	No	Yes, supports live re-encryption of tablespace data (a.k.a. data key rotation)
Which encryption is supported?	AES128 only	AES128 and AES256
Backported to earlier release	Releases 12.1.0.2 and 11.2.0.4	No (only DB 12c Release 2 and higher)

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Centrally Managed Users

I need to authenticate and authorize my database users with Active Directory easily.

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Oracle Database Authentication and Authorization

Method	Authentication	Authorization
Password	Password verifier	Database Built-In (privileges and roles)
Kerberos	Kerberos ticket	Database Built-In
PKI Certificate	PKI certificate	Database Built-In
Operating System	Operating System	OS Groups, Database Built-In
RADIUS	RADIUS	RADIUS, Database Built-In
Enterprise User Security – directory services	Password, Kerberos, and Certificate	Directory sub-tree, enterprise roles, Database Built-In

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Oracle Database Authentication and Authorization

Method	Authentication	Authorization
Password	Password verifier	Database Built-In (privileges and roles)
Kerberos	Kerberos ticket	Database Built-In
PKI Certificate	PKI certificate	Database Built-In
Operating System	Operating System	OS Groups, Database Built-In
RADIUS	RADIUS	RADIUS, Database Built-In
Enterprise User Security – directory services	Password, Kerberos, and Certificate	Directory sub-tree, enterprise roles, Database Built-In

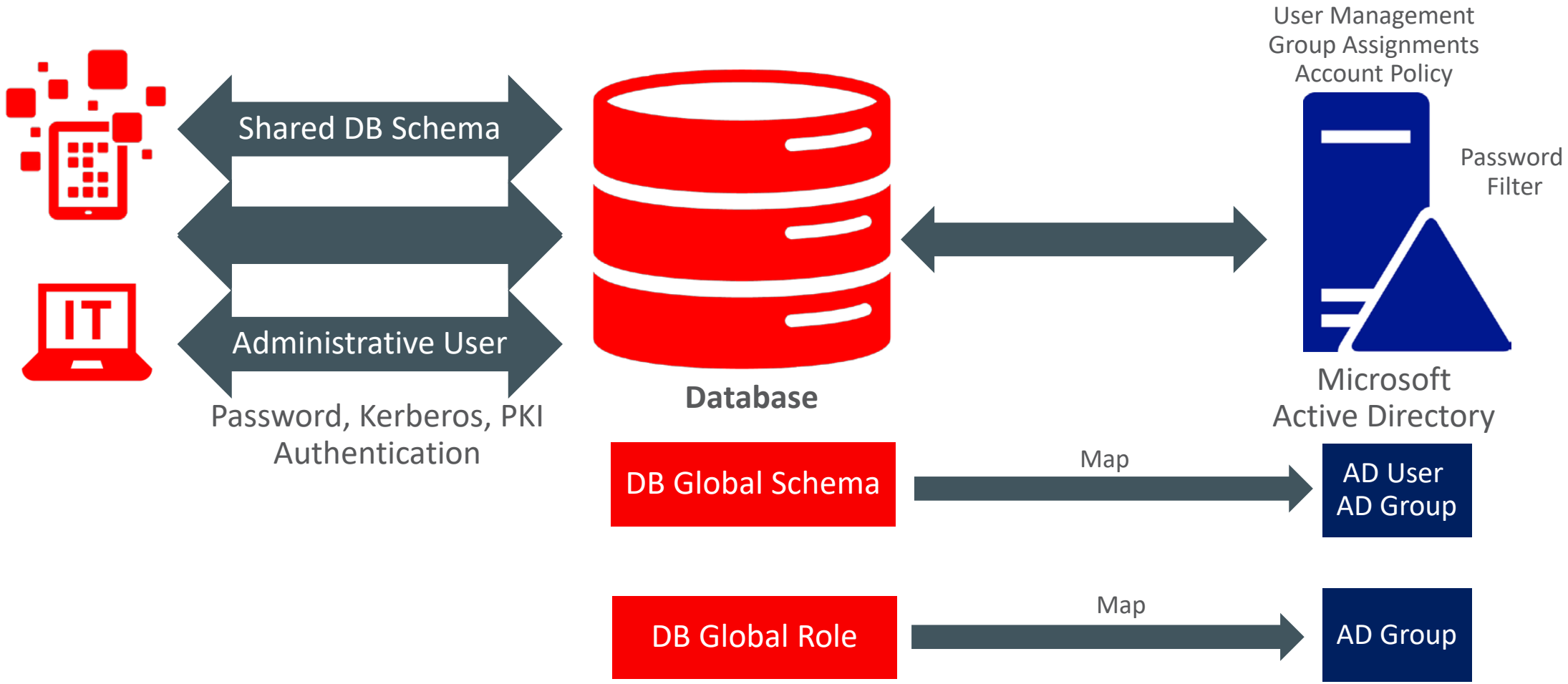
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Oracle Database Authentication and Authorization

Method	Authentication	Authorization
Password	Password verifier	Database Built-In (privileges and roles)
Kerberos	Kerberos ticket	Database Built-In
PKI Certificate	PKI certificate	Database Built-In
Operating System	Operating System	OS Groups, Database Built-In
RADIUS	RADIUS	RADIUS, Database Built-In
Enterprise User Security – directory services	Password, Kerberos, and Certificate	Directory sub-tree, enterprise roles, Database Built-In
Centrally Managed Users with Active Directory (New with 18c)	Password, Kerberos, and Certificate	Active Directory Groups, Database Built-In

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

New Active Directory Integration with Oracle Database 18c



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

18c Feature

Authorization using Active Directory Groups and DB Roles

Database

Global user:
HR_RUNTIME

Map:
Global user HR_RUNTIME to AD Group hr-rep

Directory

Domain (dc=examplecorp, dc=com)
cn = Users

Users:
Susan, Diana, Jennifer

Groups:
– hr–rep {*Susan, Diana, Jennifer*}

CREATE USER HR_RUNTIME IDENTIFIED GLOBALLY AS
'cn=hr-rep,ou=hr,dc=examplecorp,dc=com';

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

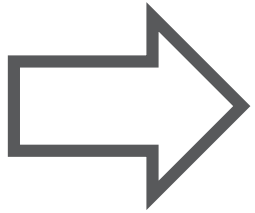
18c Feature

Authorization using Active Directory Groups and DB Roles

Database

Global user:
HR_RUNTIME

Global Role:
HR_MGR



Directory

Domain (dc=examplecorp, dc=com)
cn = Users

Users:
Susan, Diana, Jennifer

Groups:
- hr-rep {*Susan, Diana, Jennifer*}
- hr-mgr {*Susan*}

Map:
Global user HR_RUNTIME to AD Group hr-rep
Global role HR_MGR to AD Group hr-mgr

```
CREATE ROLE HR_MGR IDENTIFIED GLOBALLY AS
'cn=hr-mgr,ou=hr,dc=examplecorp,dc=com';
```

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Schema Only Accounts

I don’t need to login to most of the Oracle supplied database accounts – why are there passwords associated with them?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

18c Feature

Schema Only Accounts

- Problem
  - Database user accounts came with password authentication whether or not it was used as a login account
  - Some accounts will never be used for login, but passwords still need to be maintained
- Solution
  - Remove passwords (and all authentication) from these accounts
  - CREATE USER auxapp NO AUTHENTICATION;
  - Use ALTER USER to add/remove authentication
- 19c Update
  - On fresh 19c Database installations, Oracle Database accounts will be installed without passwords. Only SYS will have a password provided during the installation process.

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Privilege Analysis

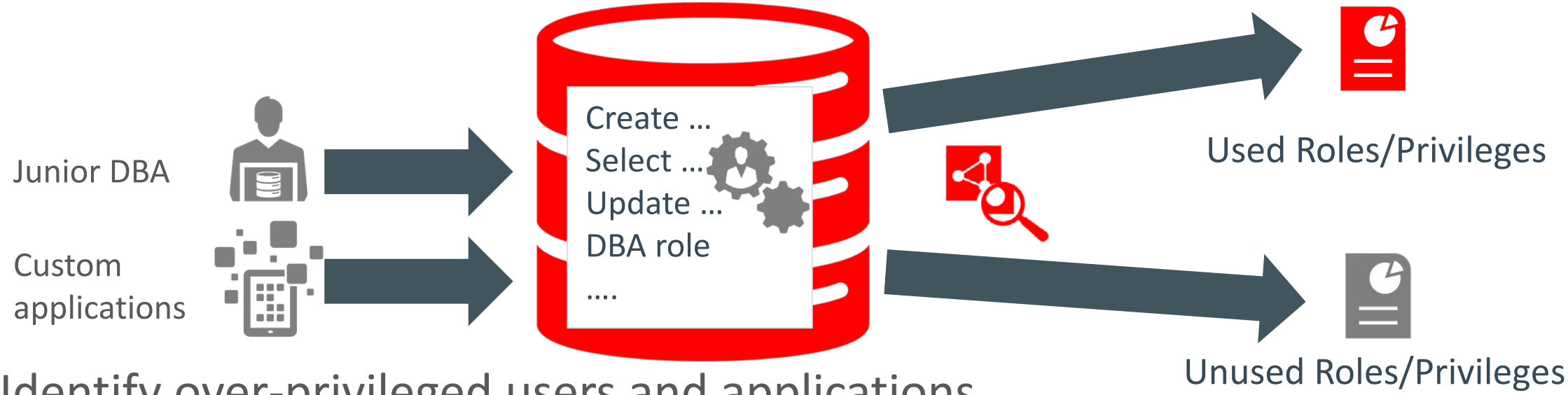
How can I tell which privileges and roles are used by a user – and more importantly, which ones aren't used?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

12c Feature

Privilege Analysis

Runtime Privilege Analysis Supports Least Privileges Model



- Identify over-privileged users and applications
- Report on actual privileges / roles used in the database
- Identify unnecessary privileges / roles
- Run on Production and Test systems – minimal performance impact

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

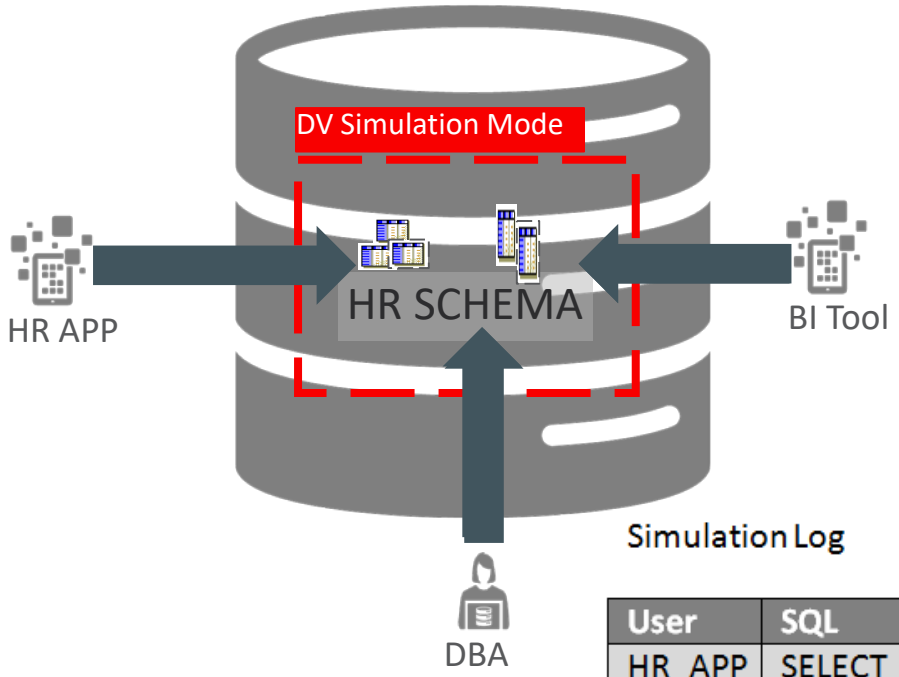
Database Vault Simulation Mode

How can I introduce new security access blocking controls into the database and minimize impact to 24x7 operations?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

12.2c Feature

Database Vault Simulation Mode

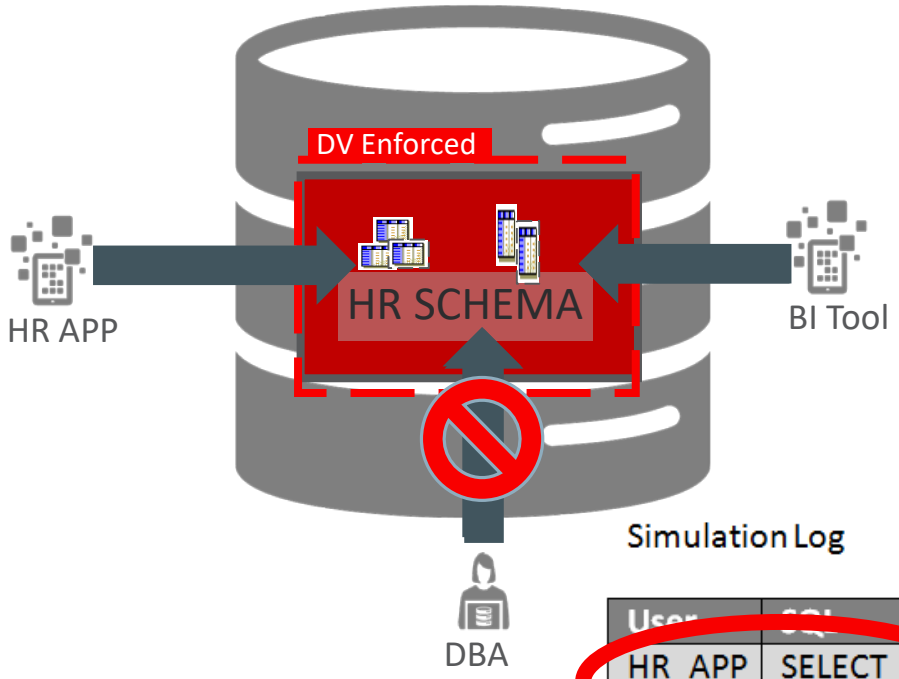


User	SQL	IP	Client	Object
HR_APP	SELECT	10.55.27.100	HRAPPv6	HR.EMPLOYEES
HR_APP	UPDATE	10.55.27.105	HRAPPv6	HR.EMPLOYEES
DBA	CREATE INDEX	10.55.68.3	SQLPLUS	HR.EMP_INDEX
DBA	SELECT	10.55.68.3	SQLPLUS	HR.EMPLOYEES
BI	SELECT	10.55.103.1	BI_TOOL	HR.EMPLOYEES

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

12.2c Feature

Database Vault Simulation Mode



Simulation Log

User	SQL	IP	Client	Object
HR_APP	SELECT	10.55.27.100	HRAPPv6	HR.EMPLOYEES
HR_APP	UPDATE	10.55.27.105	HRAPPv6	HR.EMPLOYEES
DBA	CREATE INDEX	10.55.68.3	SQLPLUS	HR.EMP_INDEX
DBA	SELECT	10.55.68.3	SQLPLUS	HR.EMPLOYEES
BI	SELECT	10.55.103.1	BI_TOOL	HR.EMPLOYEES

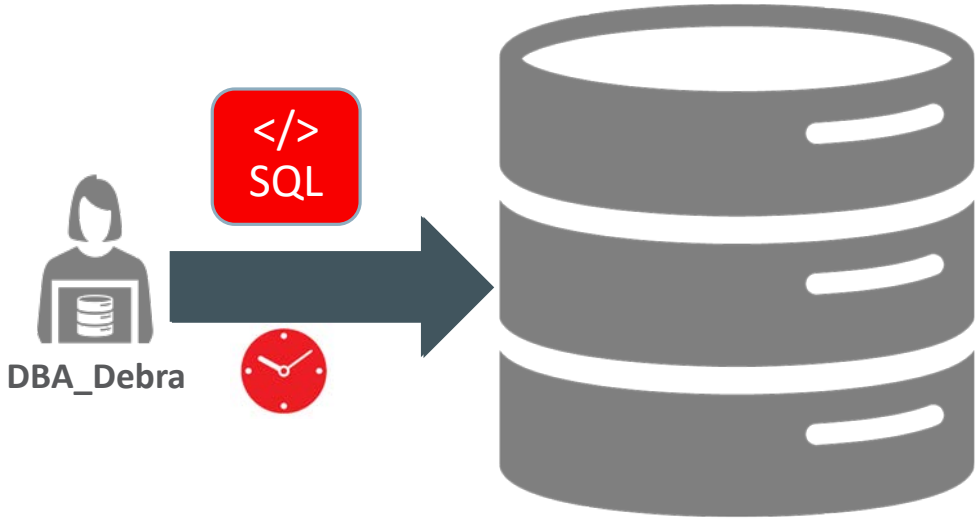
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Database Vault Command Rules

How do I prevent accidental or malicious SQL changes to my production database?

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Database Vault Command Rules



Command Rule
Rule Set
Rule – Username
Rule – IP
Rule – Time of Day
Rule – Client Tool

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Restricted

Customer Concerns and Solutions

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Summary: Solutions for Your Security Concerns

How do I protect against database misconfigurations?	• Run DBSAT against your databases
How can I convert an unencrypted database to TDE?	• Take advantage of online or fast offline conversion
How do I manage database users with my enterprise's directory service?	• Use Centrally Managed Users to integrate with Active Directory
How do I guard against unauthorized access through application schemas?	• Use password-less schemas
How do I minimize the attack surface associated with privileged users?	• Use Privilege Analysis to identify privileges users need
How can I design effective Database Vault policies for my application?	• Use Database Vaults simulation mode to validate policies
How can I control which SQL commands users can run, and when?	• Use command rules to limit user activities
How can I manage audit data across multiple processes and activities?	• Use unified auditing to manage data through a single audit trail

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Q&A

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Safe Harbor Statement

The preceding 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.

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018

Integrated Cloud

Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. | Oracle OpenWorld 2018