Oracle Database Auditing

Best practices for improving performance and security

Angeline Dhanarani,

Principal Product Manager,

Oracle Database Security Product Management

Agenda

1. Why do you need to audit Database activity ?
2. Oracle Database Auditing Journey
3. Unified Auditing Deep-Dive
4. Unified Auditing Performance
5. Fine-tuning audit for better performance

Why do you need to audit Database activity ?

Why do you need to audit Database Activity ?

Regulatory Compliance

- Provides assurance that data is used only in intended and appropriate ways
- Provides documented record of user activity

Anomaly Detection

- Detects suspicious database access patterns
- Shrinks detection time, can mitigate data breaches quickly

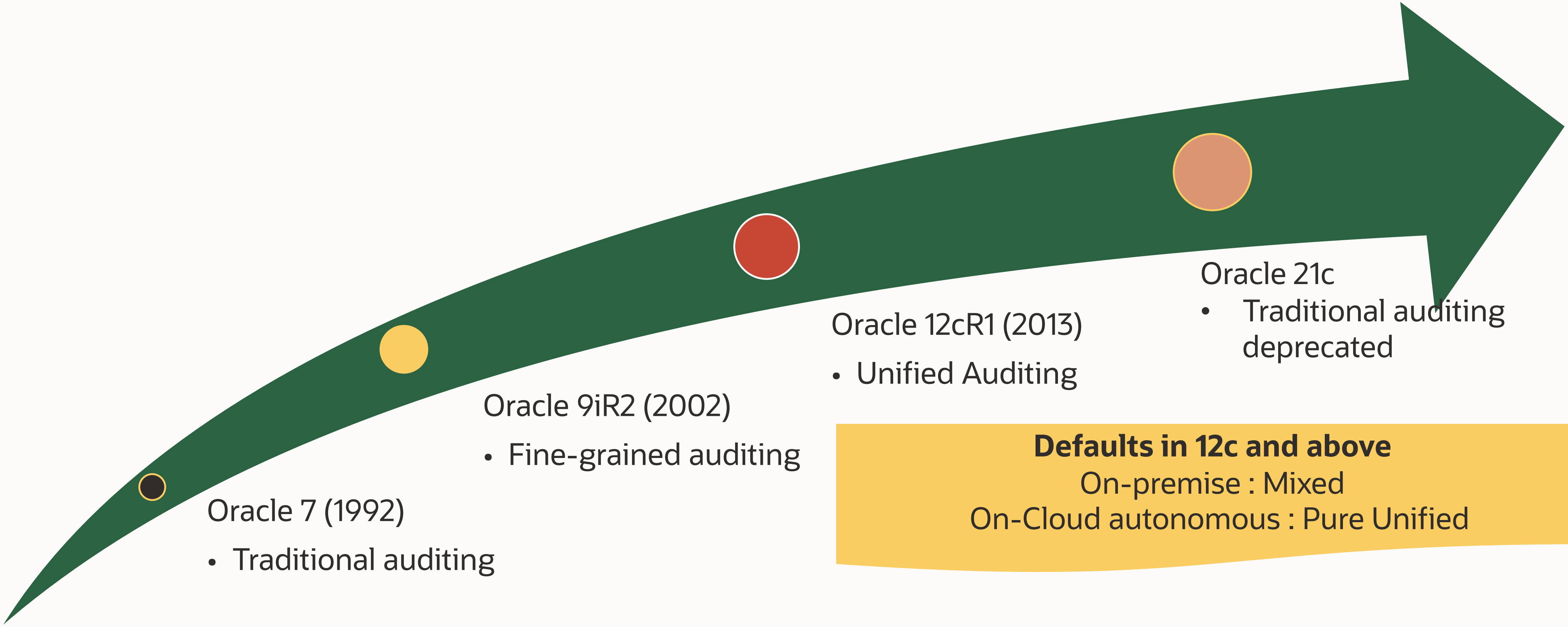
Support Forensic Analysis

- Provides wealth of information about data access – ability to track who did what to which piece of data, and when they did it
- Identifies an unauthorized access from an authorized user

Oracle Database Auditing Journey

Oracle Database Auditing Journey

Characterizing almost three decades of evolution



Oracle 7 (1992)

- Traditional auditing

Oracle 9iR2 (2002)

- Fine-grained auditing

Oracle 12cR1 (2013)

- Unified Auditing

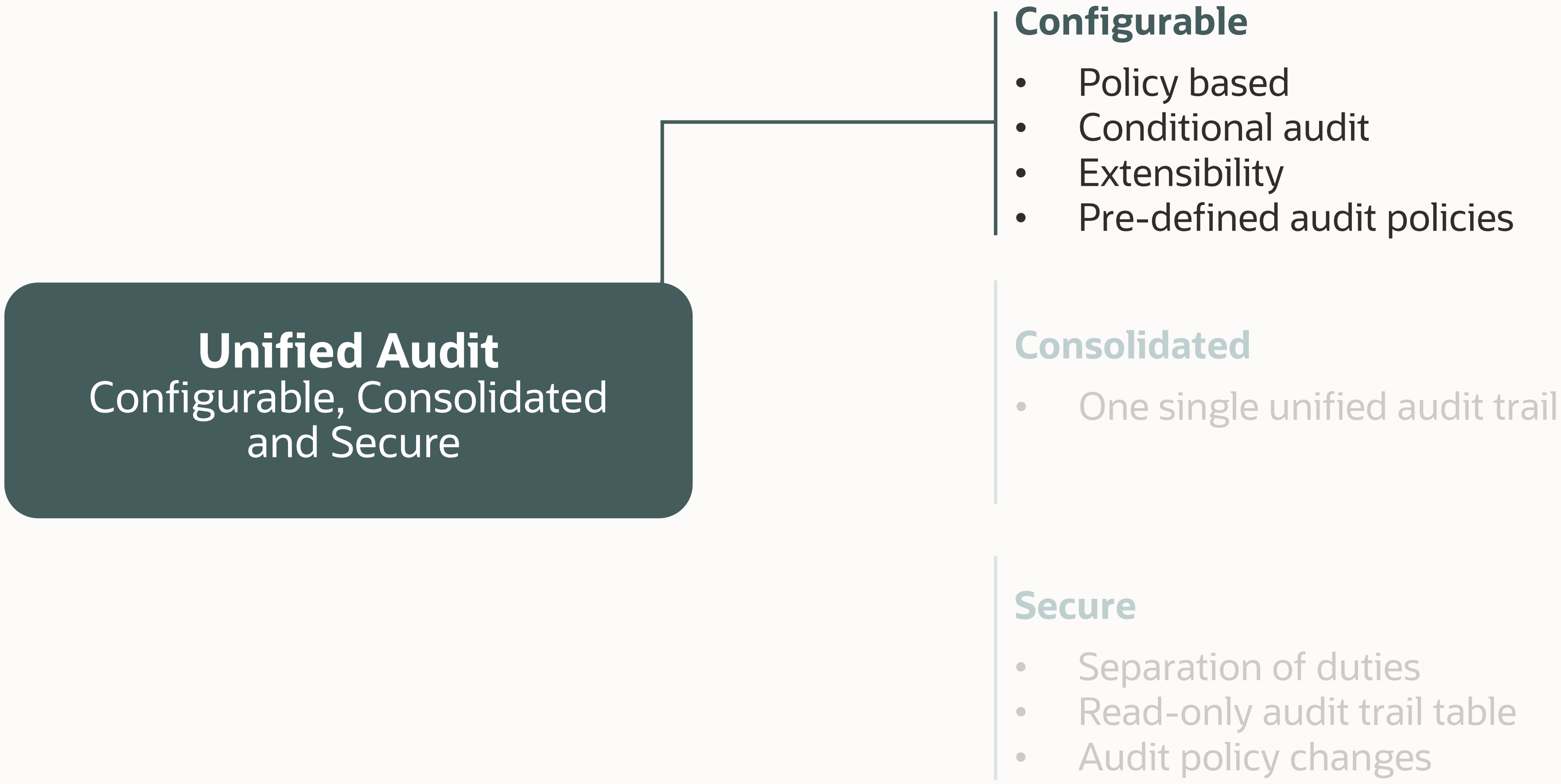
Oracle 21c

- Traditional auditing deprecated

Defaults in 12c and above
On-premise : Mixed
On-Cloud autonomous : Pure Unified

Unified Auditing Deep-Dive

Unified Audit Features



Unified Audit
Configurable, Consolidated and Secure

Configurable

- Policy based
- Conditional audit
- Extensibility
- Pre-defined audit policies

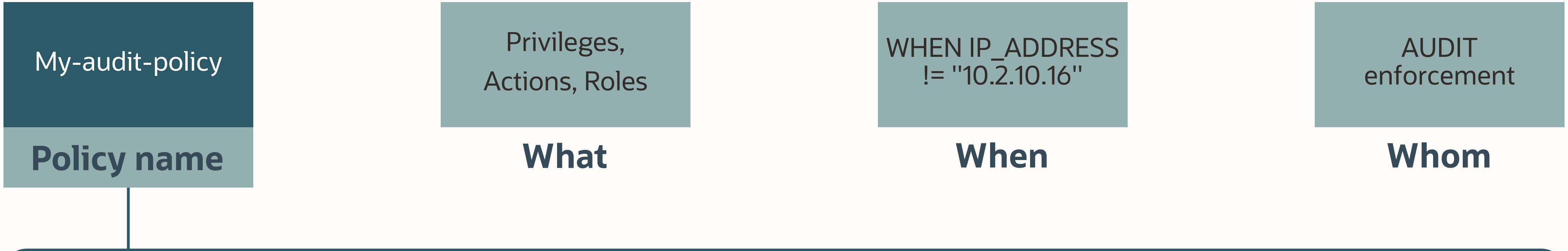
Consolidated

- One single unified audit trail

Secure

- Separation of duties
- Read-only audit trail table
- Audit policy changes

Unified Audit – Configuring Named Policies



My-audit-policy

Policy name

Privileges, Actions, Roles

What

WHEN IP_ADDRESS != "10.2.10.16"

When

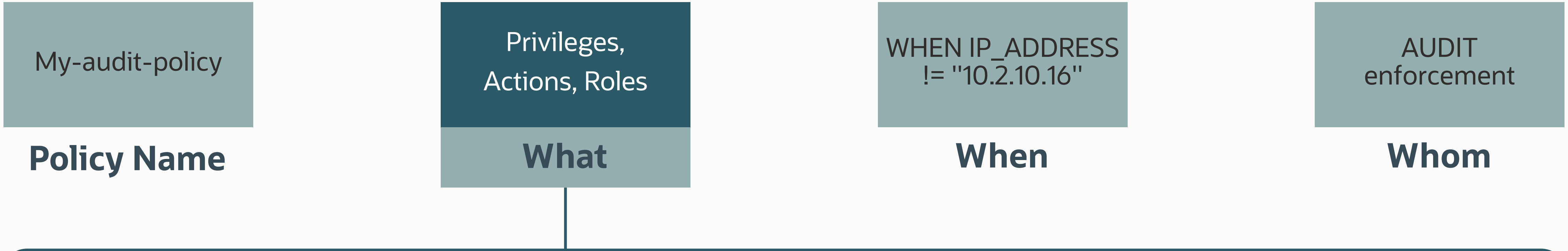
AUDIT enforcement

Whom

CONFIGURATION:

- Supports definition of Unified Audit Policy
- Defines audit-options using qualifiers “ACTIONS, PRIVILEGES, ROLES”
- CREATE AUDIT POLICY *policy_name*
  - *privilege_audit_clause* | *action_audit_clause* | *role_audit_clause*
  - WHEN *audit_condition* EVALUATE PER {STATEMENT|SESSION|INSTANCE}
  - CONTAINER = {CURRENT | ALL}
- Out-of-box policies are available which cannot be altered or dropped

Unified Audit – Simpler Policy Configuration



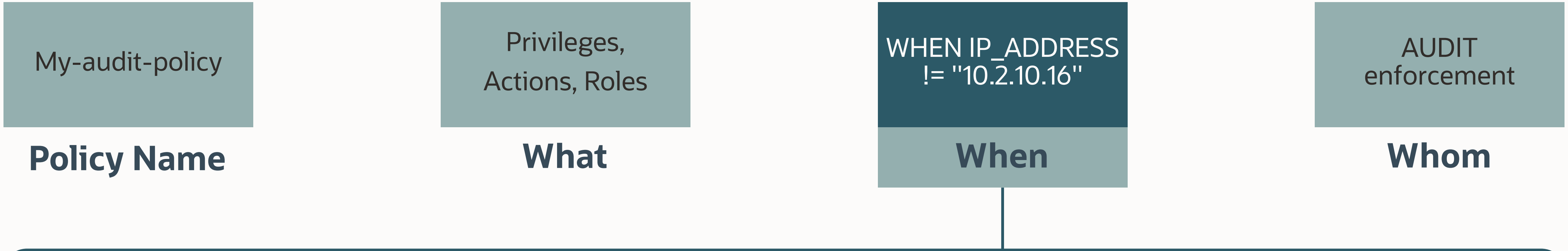
WHAT :

- System Privilege Auditing audits activities that use a system privilege
- Audit actions on specific objects
- Audits all system privileges that are directly granted to the role (user-defined, pre-defined)
- Audit system actions
- Top level auditing
- Sample

Audit based on role membership:

```
CREATE AUDIT POLICY ALL_ACTIONS_ON_EMPLOYEES ACTIONS ALL ON HR.EMPLOYEES;
AUDIT POLICY ALL_ACTIONS_ON_EMPLOYEES BY USERS WITH GRANTED ROLES DBA;
```

Unified Audit – Precision with Conditional Configuration



My-audit-policy

Policy Name

Privileges, Actions, Roles

What

WHEN IP_ADDRESS != "10.2.10.16"

When

AUDIT enforcement

Whom

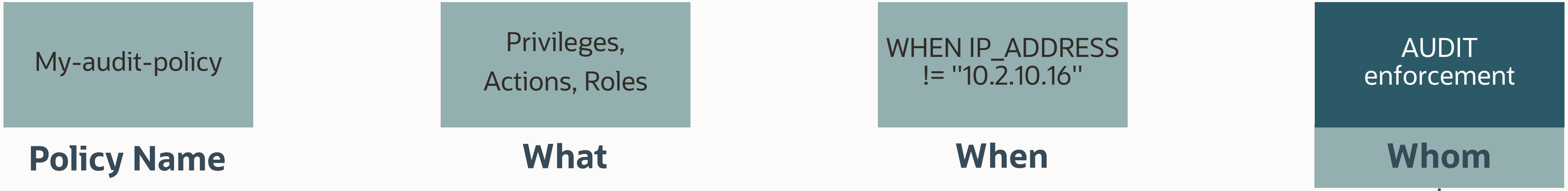
CONDITIONS:

- SYSDATE,CURRENT_DATE, and CURRENT_TIME
- SYS_CONTEXT (‘userenv’,….)
- Character functions that return character values, such as CONCAT, LOWER, and UPPER
- Character functions that return numeric values, such as LENGTH or INSTR
- AND, OR, IN, NOT IN, =, <, >, <>
- Sample

Audit based on conditions:

CREATE AUDIT POLICY **ALL_ACTIONS_ON_EMPLOYEES** ACTIONS ALL ON HR.EMPLOYEES
WHEN 'INSTR(UPPER(SYS_CONTEXT("USERENV", "AUTHENTICATION_METHOD")), "SSL") = 0‘ EVALUATE PER SESSION;

Unified Audit – Enforcement Flexibility



My-audit-policy

Policy Name

Privileges, Actions, Roles

What

WHEN IP_ADDRESS != "10.2.10.16"

When

AUDIT enforcement

Whom

CONDITIONS:

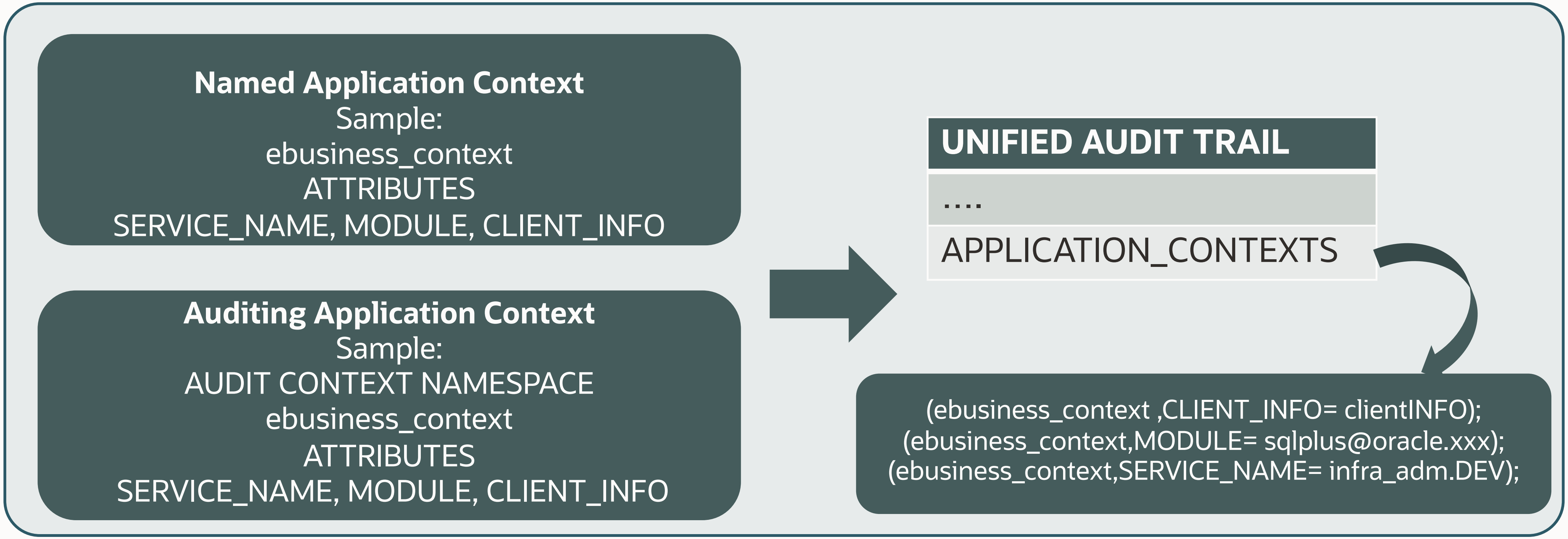
- Enable and apply unified audit policies to users using AUDIT POLICY statement.
- Whether to apply the unified audit policy to one or more users , including SYS.
- Whether to exclude few users from the unified audit policy with EXCEPT clause.
- Whether to create an audit record if the activity succeeds or fails or both.
- Whether to include users with specific granted role (BY USERS WITH GRANTED ROLE)
- Sample

Exception-based auditing

CREATE AUDIT POLICY **APP_BYPASS** ACTIONS SELECT ON HR.EMPLOYEES;
 AUDIT POLICY **APP_BYPASS** EXCEPT apps;

Unified Audit – Extensibility

Unified Auditing is extensible to include application attributes



Named Application Context
Sample:
ebusiness_context
ATTRIBUTES
SERVICE_NAME, MODULE, CLIENT_INFO

Auditing Application Context
Sample:
AUDIT CONTEXT NAMESPACE
ebusiness_context
ATTRIBUTES
SERVICE_NAME, MODULE, CLIENT_INFO

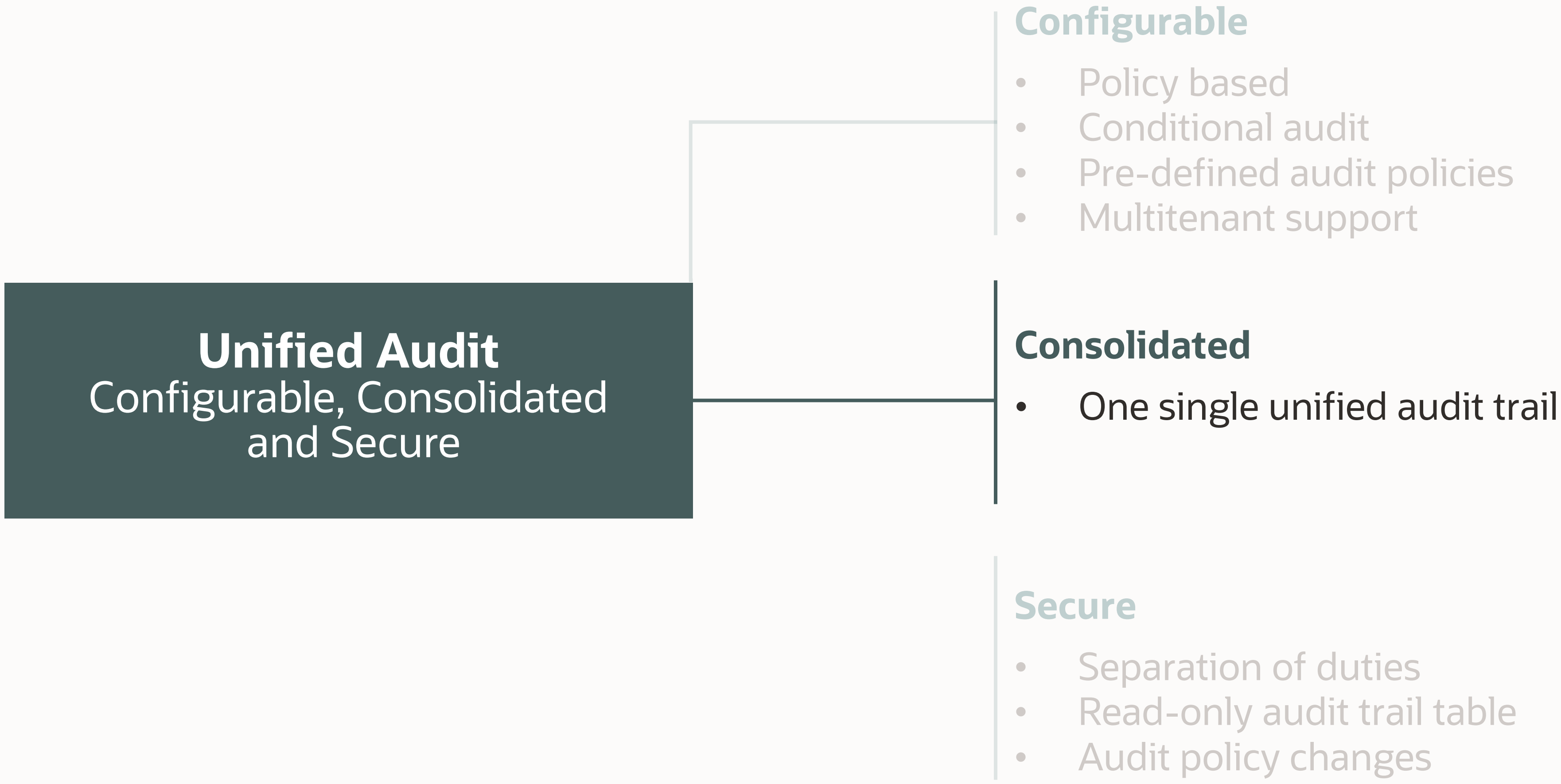
UNIFIED AUDIT TRAIL
….
APPLICATION_CONTEXTS

(ebusiness_context ,CLIENT_INFO= clientINFO);
(ebusiness_context,MODULE= sqlplus@oracle.xxx);
(ebusiness_context,SERVICE_NAME= infra_adm.DEV);

Pre-defined Audit Policies

No	Policy Name	What it does ?	Enabled by default ?
1	ORA_LOGON_FAILURES	Tracks failed logons only	Yes (for DBCA created databases)
2	ORA_SECURECONFIG	Provides all the secure configuration audit options	Yes (for DBCA created databases)
3	ORA_DATABASE_PARAMETER	Audits changes to Oracle Database parameter settings	No
4	ORA_ACCOUNT_MGMT	Audits modification to user account and privilege settings.	No
5	ORA_CIS_RECOMMENDATIONS	Audits that the Center for Internet Security (CIS) recommends	No
6	ORA_RAS_POLICY_MGMT, ORA_RAS_SESSION_MGMT	Oracle Database Real Application Security events	No
7	ORA_DV_AUDPOL	Audits Oracle Database Vault DVSYS and LBACSYS schema objects	No
8	ORA_DV_AUDPOL2	Audits the Oracle Database Vault default realms and command rules.	No
9	ORA_STIG_RECOMMENDATIONS, ORA_ALL_TOPLEVEL_ACTIONS, ORA_LOGON_LOGOFF	Audits that the Security Technical Implementation Guide (STIG) recommends	No

Unified Audit Features



Unified Audit
Configurable, Consolidated and Secure

Configurable

- Policy based
- Conditional audit
- Pre-defined audit policies
- Multitenant support

Consolidated

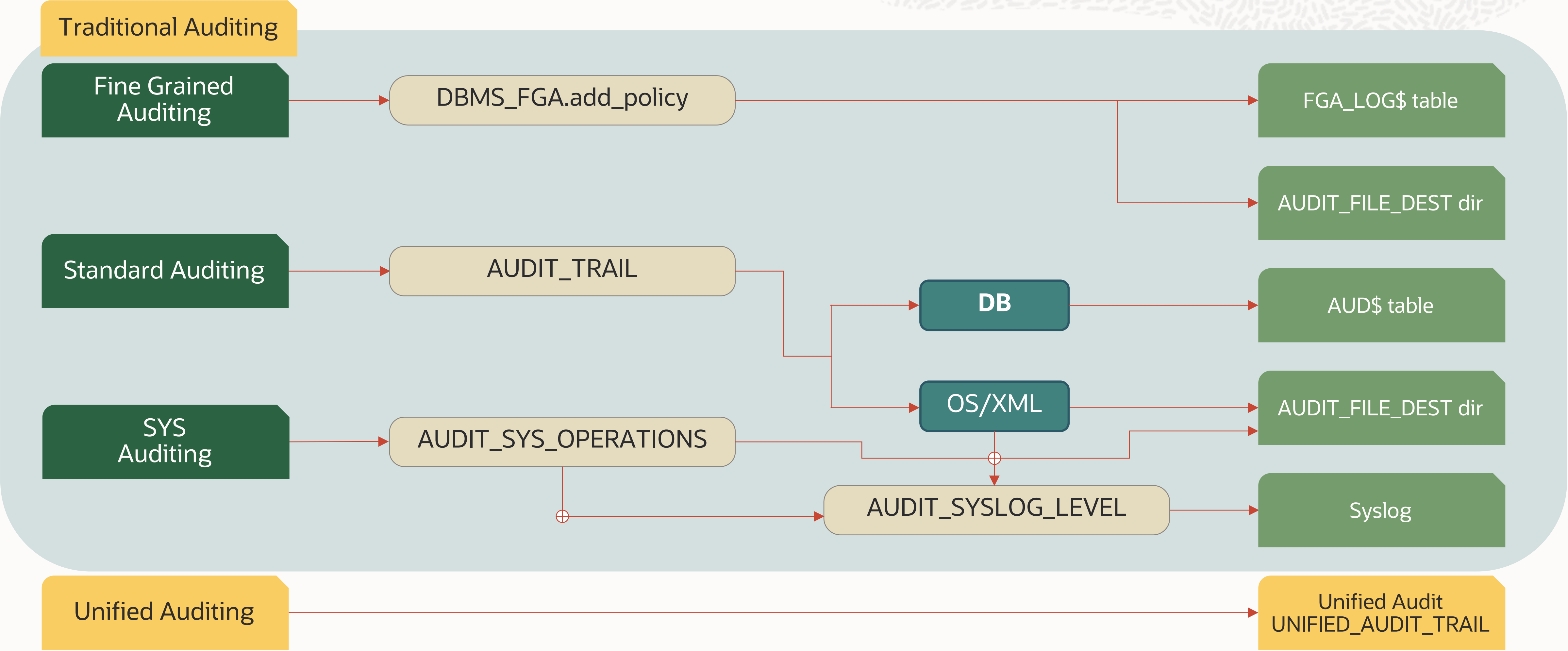
- One single unified audit trail

Secure

- Separation of duties
- Read-only audit trail table
- Audit policy changes

Mixed Mode Auditing (Default Oracle 12c onwards)

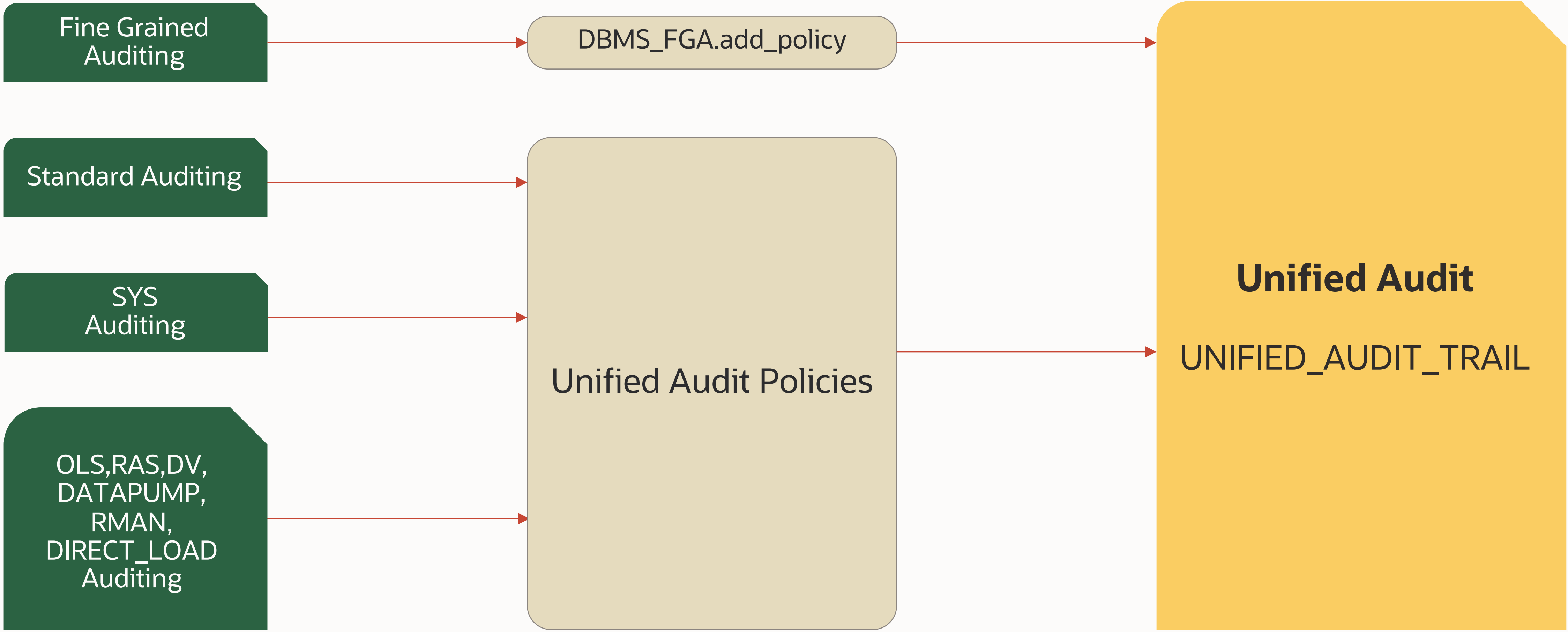
Multiple audit sources



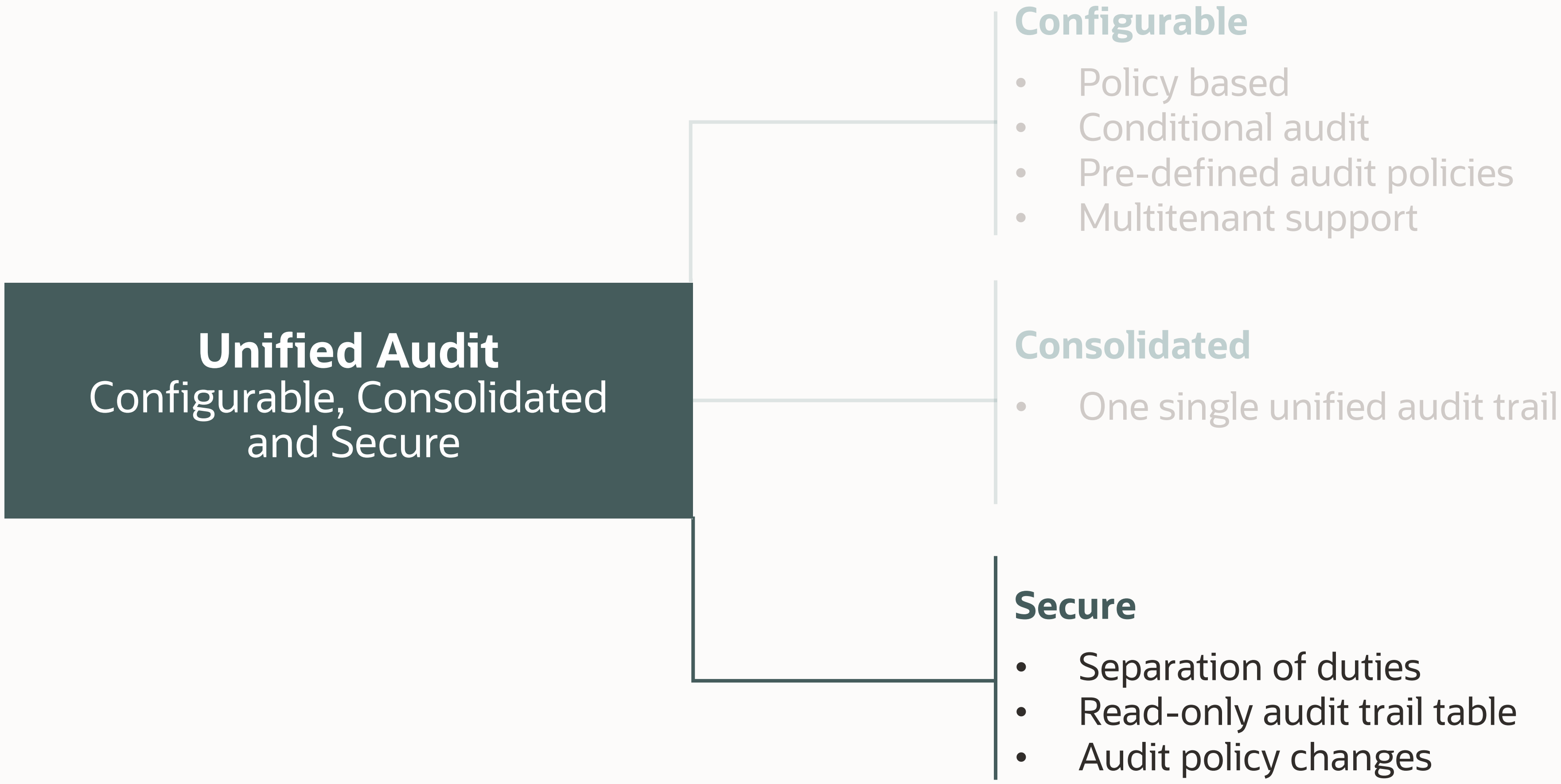
Pure Unified auditing (Available Oracle 12c onwards)

Unified source of audit

Default in Oracle Autonomous Databases



Unified Audit Features



Unified Audit
Configurable, Consolidated and Secure

Configurable

- Policy based
- Conditional audit
- Pre-defined audit policies
- Multitenant support

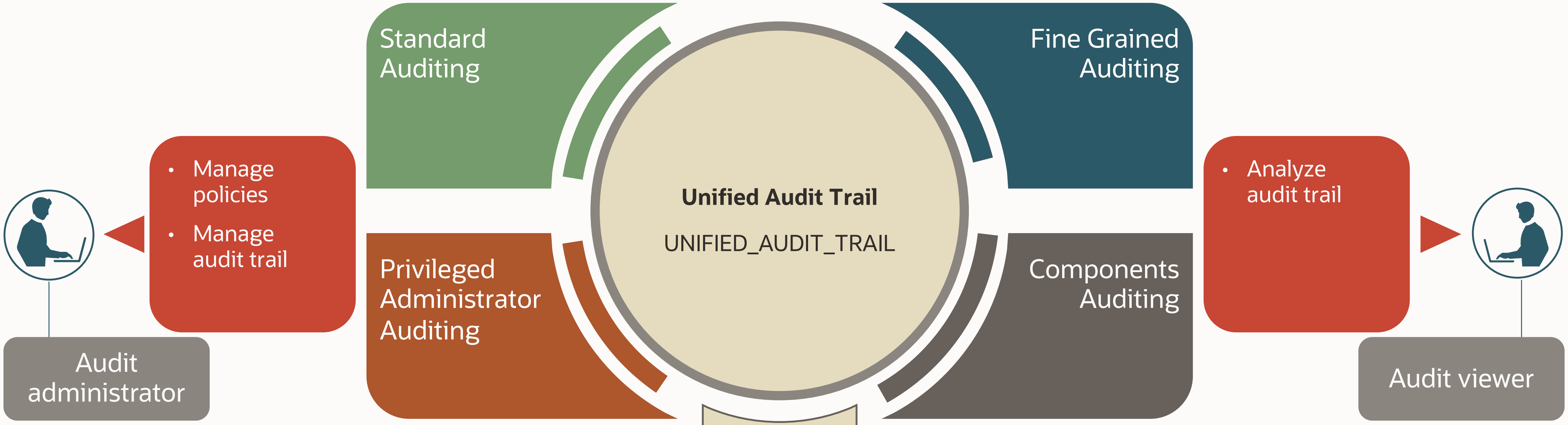
Consolidated

- One single unified audit trail

Secure

- Separation of duties
- Read-only audit trail table
- Audit policy changes

Secure and Reliable



Standard Auditing

Fine Grained Auditing

Unified Audit Trail

UNIFIED_AUDIT_TRAIL

Privileged Administrator Auditing

Components Auditing

- Manage policies
- Manage audit trail

Audit administrator

- Analyze audit trail

Audit viewer

Highly secured

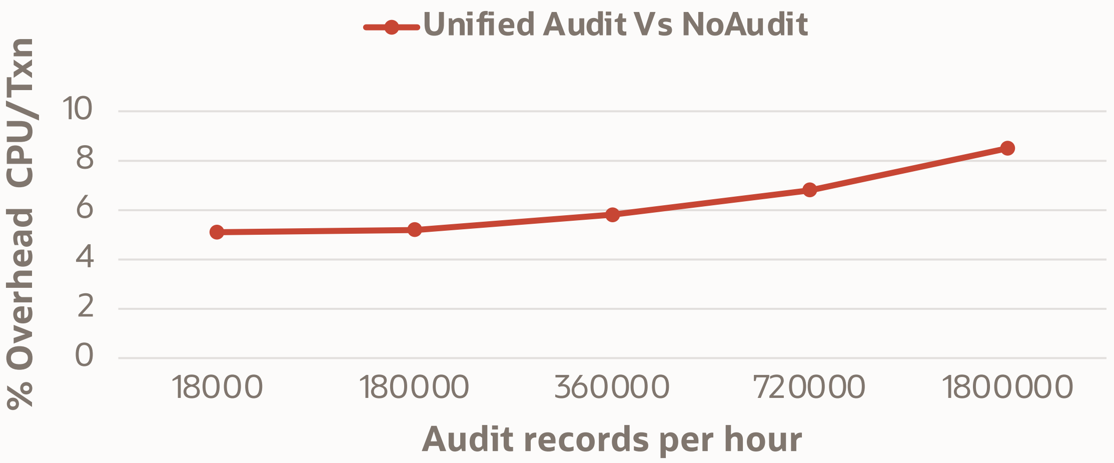
- Read Only Table
- DMLs /DDLs on underlying dictionary table not permitted
- All modification attempts on unified audit internal table audited
- Audit-related activities, such as modifications to audit policies and audit trail cleanup, are mandatorily audited

Unified Auditing Performance

Minimizing Performance Impact of Auditing

From Internal performance tests with TPC-C workload:

- CPU overhead is mid-single digit when auditing up to 3,60,000 audit records/hour
- For extreme audit loads up to 18,00,000 audit records/hour,   the additional overhead is still in a single digit.



Pure Unified Vs Mixed Mode Audit Performance:

- Further improvement of 1% with Pure Unified Audit as compared to Mixed Mode

Recommendation:

- For most typical use cases of auditing, the performance impact of Unified Auditing is so low
- As auditing is a transactional activity with typical ACID properties to guarantee record of database activities, fine-tune your audit policies
  - To collect audit data that is targeted to your needs
  - To further minimize performance impact

Fine-tuning Audit for Better Performance

Three Golden Principles of Fine-tuning Audit Policy Configuration

Privileged user activity monitoring

Privileged user accounts

- Soft targets for hackers
- Helps gain access to critical systems and data

Continuous **privileged user activity monitoring** helps

- Identify anomalous behavior
- Detect insider breaches

Security-relevant events auditing

Actions within the database that warrant greater scrutiny and constant monitoring like

- Failed login attempts
- Schema structural changes
- Privilege grants

Security-relevant events auditing helps

- Engage in strategic early warning detection

Sensitive data access auditing

Provides visibility into access and changes to sensitive data

Sensitive data access auditing helps

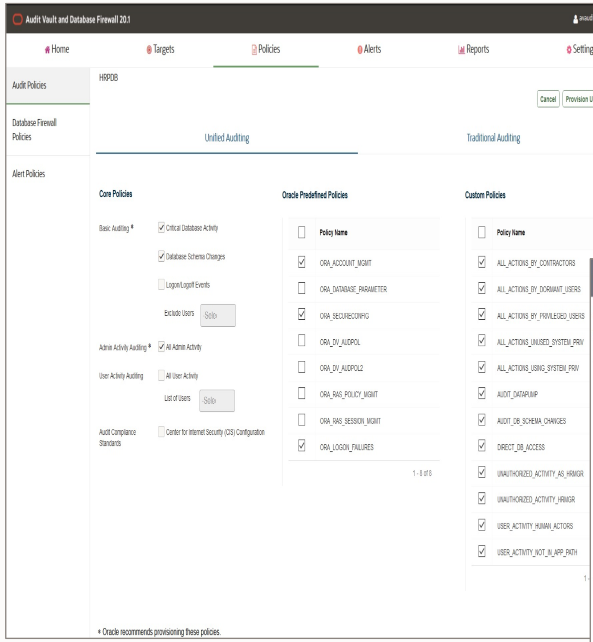
- Meet privacy regulations
- Stay alerted to prevent data loss
- Primary deterrence to those who do not have a business reason to access

Guidelines for Provisioning Audit Policies

- Do not duplicate **Always-on** Mandatory Audit configurations of Oracle Database
- Leverage **Pre-defined** Unified Audit policies
  - Defined in Oracle Database(ORA_%), provisionable from Oracle Data Safe/ Oracle Audit Vault and Database Firewall (AVDF)
  - Recommended and provisionable from Oracle Data Safe / Oracle AVDF
- Create custom Unified Audit policies for audit configurations that is unique to your scenario (e.g. sensitive data access)

Audit Policy Provisioning

Oracle AVDF



HRPDB

Core Policies

Basic Auditing *
☑ Critical Database Activity
☑ Database Schema Changes
□ Logon/Logoff Events
Exclude Users -Selec

Admin Activity Auditing * ☑ All Admin Activity

User Activity Auditing □ All User Activity
List of Users -Selec

Audit Compliance Standards □ Center for Internet Security (CIS) Configuration

Oracle Predefined Policies

□	Policy Name
☑	ORA_ACCOUNT_MGMT
□	ORA_DATABASE_PARAMETER
☑	ORA_SECURECONFIG
□	ORA_DV_AUDPOL
□	ORA_DV_AUDPOL2
□	ORA_RAS_POLICY_MGMT
□	ORA_RAS_SESSION_MGMT
☑	ORA_LOGON_FAILURES

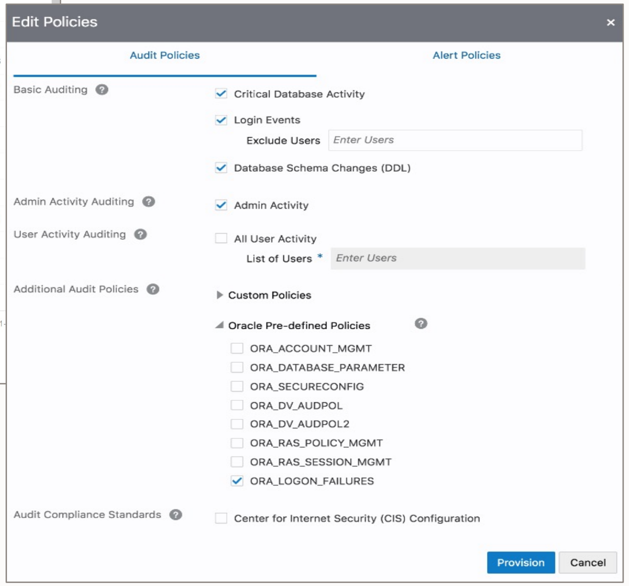
1 - 8 of 8

Custom Policies

□	Policy Name
☑	ALL_ACTIONS_BY_CONTRACTORS
☑	ALL_ACTIONS_BY_DORMANT_USERS
☑	ALL_ACTIONS_BY_PRIVILEGED_USERS
☑	ALL_ACTIONS_UNUSED_SYSTEM_PRIV
☑	ALL_ACTIONS_USING_SYSTEM_PRIV
☑	AUDIT_DATAPUMP
☑	AUDIT_DB_SCHEMA_CHANGES
☑	DIRECT_DB_ACCESS
☑	UNAUTHORIZED_ACTIVITY_AS_HRMGR
☑	UNAUTHORIZED_ACTIVITY_HRMGR
☑	USER_ACTIVITY_HUMAN_ACTORS
☑	USER_ACTIVITY_NOT_IN_APP_PATH

* Oracle recommends provisioning these policies.

Oracle Data Safe



Basic Auditing ?
☑ Critical Database Activity
☑ Login Events
Exclude Users Enter Users
☑ Database Schema Changes (DDL)

Admin Activity Auditing ? ☑ Admin Activity

User Activity Auditing ? □ All User Activity
List of Users * Enter Users

Additional Audit Policies ?
▸ Custom Policies
◢ Oracle Pre-defined Policies ?
□ ORA_ACCOUNT_MGMT
□ ORA_DATABASE_PARAMETER
□ ORA_SECURECONFIG
□ ORA_DV_AUDPOL
□ ORA_DV_AUDPOL2
□ ORA_RAS_POLICY_MGMT
□ ORA_RAS_SESSION_MGMT
☑ ORA_LOGON_FAILURES

Audit Compliance Standards ? □ Center for Internet Security (CIS) Configuration

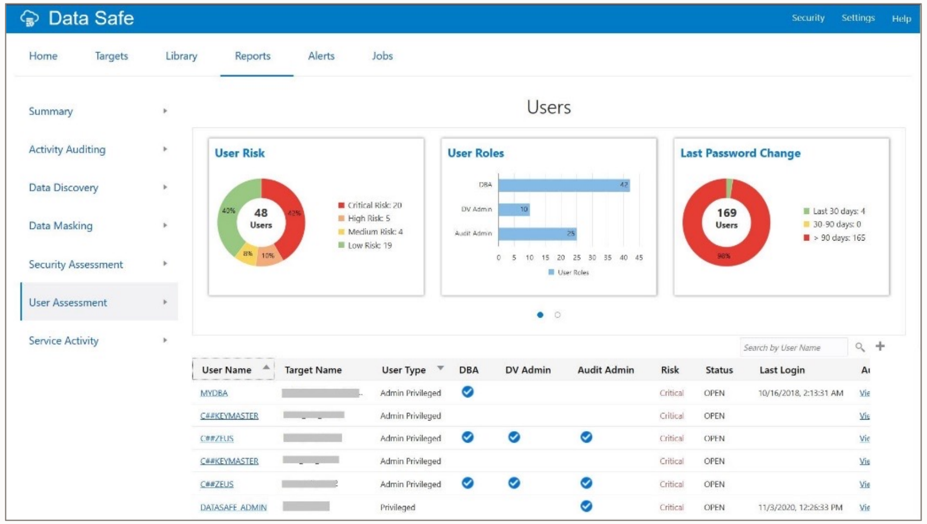
Privileged User Activity Monitoring Recommendations

Audit Recommendations:
Audit administrative database user accounts
Audit database user accounts with direct access
Audit individual high risk database user accounts

Audit Administrative Database User Accounts

Identify database user accounts with administrative privileges

- User Assessment report in Data Safe

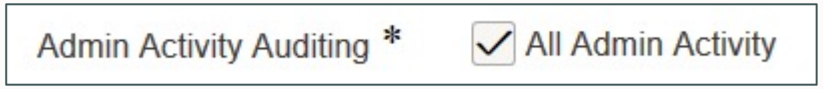


User Name	Target Name	User Type	DBA	DV Admin	Audit Admin	Risk	Status	Last Login	A
MYDBA	[redacted]	Admin Privileged	✓			Critical	OPEN	10/16/2018, 2:13:31 AM	Vie
C##KEYMASTER	[redacted]	Admin Privileged				Critical	OPEN		Vie
C##ZEUS	[redacted]	Admin Privileged	✓	✓	✓	Critical	OPEN		Vie
C##KEYMASTER	[redacted]	Admin Privileged				Critical	OPEN		Vie
C##ZEUS	[redacted]	Admin Privileged	✓	✓	✓	Critical	OPEN		Vie
DATASAFE_ADMIN	[redacted]	Privileged			✓	Critical	OPEN	11/3/2020, 12:26:33 PM	Vie

- DBSAT report

Recommendations:

- Top-level statements by administrative users (e.g. SYSDBA, SYSKM) are mandatorily audited when the database is in the closed or mount state
- Configure audit policies to capture all top-level actions of administrative user accounts, such as SYS or named DBA accounts during normal database operations.
- Provision audit policy **“Admin Activity Auditing”** to audit all activities by privileged administrators, including SYS



Admin Activity Auditing * ☑ All Admin Activity

Oracle Data Safe / Oracle AVDF

Audit Database User Accounts with Direct Access

- Direct access to databases is usually granted to only power-users like data analysts or application administrator

- Auditing local sessions is crucial because they bypass network monitoring

Recommendations:

- Configure audit policy to audit all top-level actions performed on local direct access (including bequeath connections):

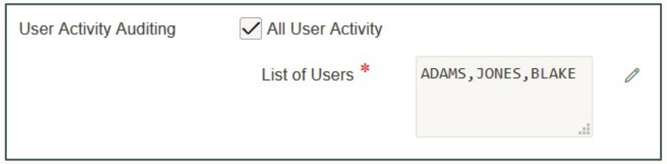
```
CREATE AUDIT POLICY DIRECT_DB_ACCESS
ACTIONS ALL
WHEN '(SYS_CONTEXT ("USERENV", "IP_ADDRESS") IS NULL)'
EVALUATE PER SESSION
ONLY TOPLEVEL;

AUDIT POLICY DIRECT_DB_ACCESS;
```

Audit Individual High Risk Database User Accounts

- Monitor all user-initiated activities of individual database accounts
  - With higher risk
  - Have access to sensitive data
  - Non-admin but privileged users

Recommendations:

- Option#1: Provision audit policy **“User Activity Auditing”** to audit all activities for a set of users



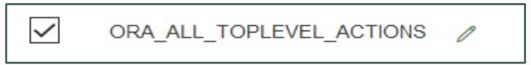
User Activity Auditing ☑ All User Activity

List of Users * ADAMS,JONES,BLAKE

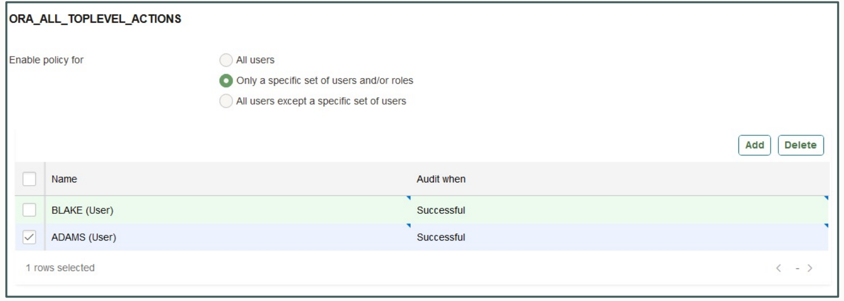
Oracle Data Safe / Oracle AVDF

- Option#2: Provision audit policy “**ORA_ALL_TOPLEVEL_ACTIONS**” to audit all top level activities for a set of users/ roles

Oracle Data Safe / Oracle AVDF



☑ ORA_ALL_TOPLEVEL_ACTIONS



ORA_ALL_TOPLEVEL_ACTIONS

Enable policy for
○ All users
● Only a specific set of users and/or roles
○ All users except a specific set of users

□	Name	Audit when
□	BLAKE (User)	Successful
☑	ADAMS (User)	Successful

1 rows selected

Security-Relevant Events Auditing Recommendations

Audit Recommendations:
Audit security-management events
Audit account-management events
Audit data-security events
Audit database-management events
Audit data-management events
Audit activities with system privileges
Audit activities with unused system privileges
Audit usage of components with data implications
Monitor suspicious user-activity events

Audit Security-Management/ Account-Management Events

- Audit any changes to the database-wide security policies

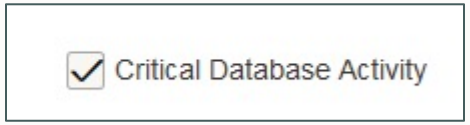
EVENTS	TYPICAL USER COMMANDS
Security parameters changes such as SEC_MAX_FAILED_LOGIN _ATTEMPTS	ALTER DATABASE, ALTER SYSTEM
Audit policies changes	ALTER AUDIT POLICY
Key rotation	ADMINISTER KEY MANAGEMENT

- Audit any changes to the database access

EVENTS	TYPICAL USER COMMANDS
USER SECURITY-PROFILE CHANGES	CREATE/ALTER/DELETE USER/ROLE/PROFILE GRANT/REVOKE

Recommendations:

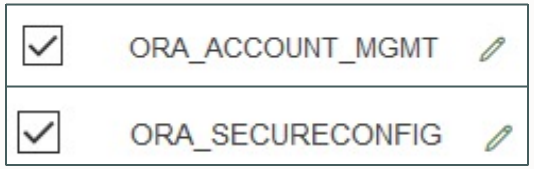
- Option#1: Provision audit policy “Critical Database Activity” to audit for all users



☑ Critical Database Activity

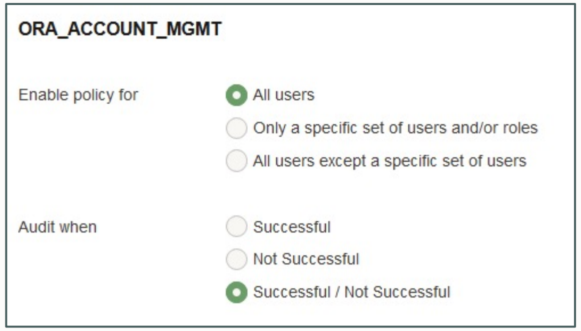
Oracle Data Safe / Oracle AVDF

- Option#2: Provision audit policy “ORA_SECURECONFIG” , “ORA_ACCOUNT_MGMT” to audit a set of users/ roles



☑ ORA_ACCOUNT_MGMT

☑ ORA_SECURECONFIG



ORA_ACCOUNT_MGMT

Enable policy for
- ● All users
- ○ Only a specific set of users and/or roles
- ○ All users except a specific set of users

Audit when
- ○ Successful
- ○ Not Successful
- ● Successful / Not Successful

Audit Data-Security Events

Audit security policy changes around protected objects or schemas

EVENTS	TYPICAL USER COMMANDS
Redaction policy changes	DBMS_REDACT procedures
VPD/OLS/RAS policy changes	DBMS_RLS procedures
Database Vault policy changes	DBMS_MACADM procedures
TSDP policies changes	DBMS_TSDP_MANAGE / DBMS_TSDP_PROTECT procedures
Exempt policies changes	EXEMPT ACCESS POLICY

Recommendations:

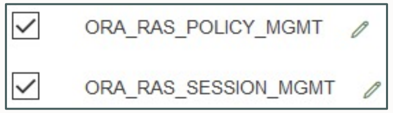
- Configure audit policy for redaction changes:

```
CREATE AUDIT POLICY redaction_policy_changes ACTIONS EXECUTE ON
DBMS_REDACT;
```

- Configure audit policy for VPD/OLS/RAS policy changes

```
CREATE AUDIT POLICY vpd_policy_changes ACTIONS EXECUTE ON
DBMS_RLS;
CREATE AUDIT POLICY ols_policy_changes ACTIONS COMPONENT=OLS
ALL;
```

  - Provision pre-defined audit policy for RAS



☑ ORA_RAS_POLICY_MGMT

☑ ORA_RAS_SESSION_MGMT

Oracle Data Safe /
Oracle AVDF

- DV policy changes are mandatorily audited
- Configure audit policy for TSDP changes

```
CREATE AUDIT POLICY tsdp_policy_changes ACTIONS EXECUTE ON
DBMS_TSDP_MANAGE, EXECUTE ON DBMS_TSDP_PROTECT;
```

- Provision pre-defined audit policy for Exempt policy changes

☑ ORA_SECURECONFIG

Oracle Data Safe /
Oracle AVDF

Audit Database-Management Events

Database-management events:

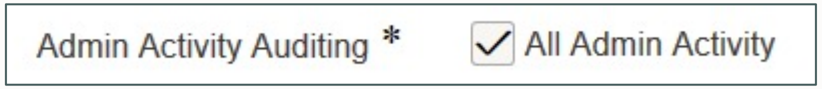
EVENTS	TYPICAL USER COMMANDS
Backup/ restore operations, Cloning PDBs	RMAN Operations
Creating/deleting tablespace	CREATE/ALTER/DROP TABLESPACE
Patching	opatch
Altering Database	ALTER DATABASE, ALTER SYSTEM

Recommendations:

- All RMAN events are mandatorily audited in Oracle Database
- Configure audit policy for tablespace changes

```
CREATE AUDIT POLICY tablespace_changes
ACTIONS
create tablespace, alter tablespace, drop tablespace;
```

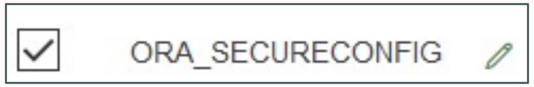
- Patching is typically a SYS activity
  - In unmounted state, SYS activities mandatorily audited
  - Pre-defined audit policy for SYS in mounted state:



Admin Activity Auditing * ☑ All Admin Activity

Oracle Data Safe / Oracle AVDF

- Pre-defined audit policy for alter database/ alter system:



☑ ORA_SECURECONFIG

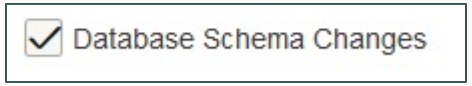
Oracle Data Safe / Oracle AVDF

Audit Data-Management Events

- Audit database schema structure modification events like create/alter/delete of tables/index/views
- All Data Definition Language (DDL) commands issued by any database user

Recommendations:

Provision audit policy **“Database Schema Changes”** to audit for all users



☑ Database Schema Changes

Oracle Data Safe / Oracle AVDF

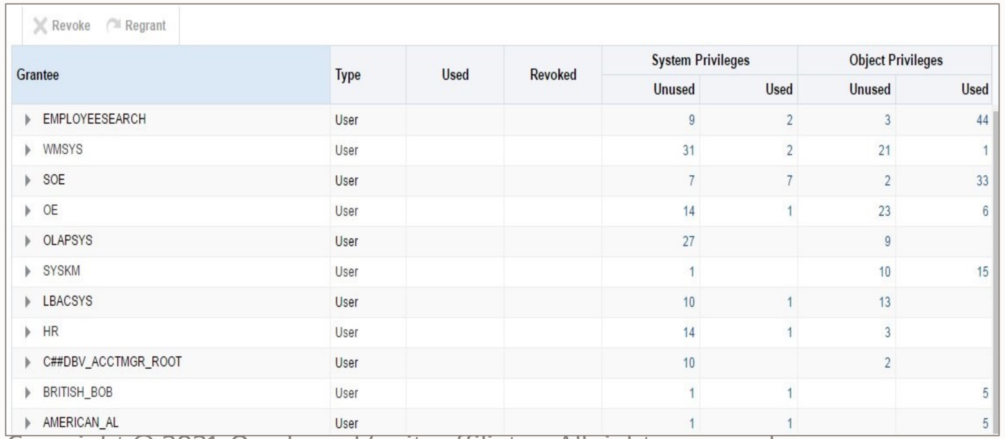
Audit Activities with Used/ UN-used System Privileges

Use of system privileges need to be monitored

- Can be potentially abused
- Can cause wide-spread impact
- Helps in implementing a least privilege model

Identify the system privileges granted to the database users currently in-use/ un-used

- Privilege Analysis (PA) of Oracle Database from Enterprise Manager:



Grantee	Type	Used	Revoked	System Privileges		Object Privileges	
				Unused	Used	Unused	Used
EMPLOYEESEARCH	User			9	2	3	44
WMSYS	User			31	2	21	1
SOE	User			7	7	2	33
OE	User			14	1	23	6
OLAPSYS	User			27		9	
SYSKM	User			1		10	15
LBACSYS	User			10	1	13	
HR	User			14	1	3	
C##DBV_ACCTMGR_ROOT	User			10		2	
BRITISH_BOB	User			1	1		5
AMERICAN_AL	User			1	1		5

Recommendations:

- Configure audit policy to audit activities using a system privilege for all users, that is currently in-use

```
CREATE AUDIT POLICY ALL_ACTIONS_USING_SYSTEM_PRIV
PRIVILEGES
SELECT ANY TABLE, UPDATE ANY TABLE, INSERT ANY TABLE, REDEFINE
ANY TABLE, DELETE ANY TABLE;
-- Include all the used system privileges from the Privilege Analysis (PA)
report

AUDIT POLICY ALL_ACTIONS_USING_SYSTEM_PRIV;
```

- Configure audit policy to audit activities using a system privilege that does not appear to be in-use

```
CREATE AUDIT POLICY ALL_ACTIONS_UNUSED_SYSTEM_PRIV
PRIVILEGES ALTER ANY ROLE, ALTER ANY TRIGGER, DROP ANY ROLE,
GRANT ANY PRIVILEGE;
-- Include all the unused system privileges from the Privilege Analysis (PA)
report that need to exist

AUDIT POLICY ALL_ACTIONS_UNUSED_SYSTEM_PRIV BY
secadmin_steve;
```

Audit Usage of Components with Data Implications

Consider auditing of database components such as the following when used:

- Oracle Data Pump
- Oracle SQL*Loader
- Oracle Label Security

Recommendations:

Configure audit policy for components usage

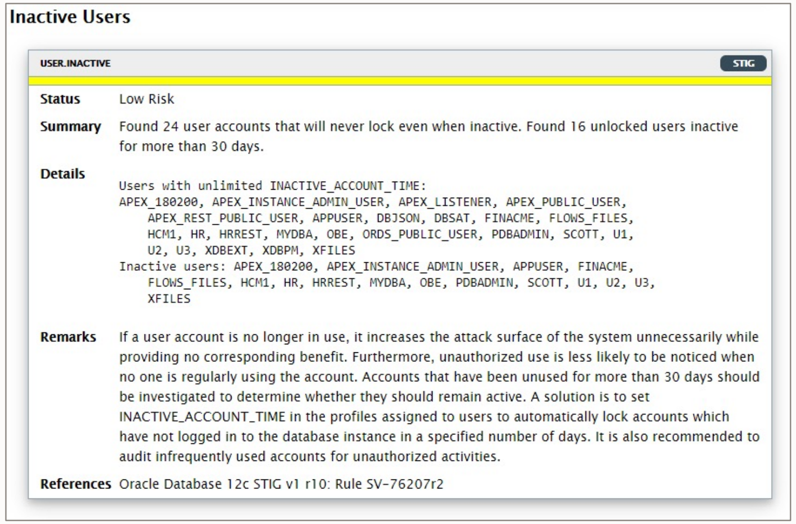
Sample audit policy for Oracle Data Pump component used:

```
CREATE AUDIT POLICY AUDIT_DATAPUMP
ACTIONS COMPONENT= datapump EXPORT, IMPORT;

AUDIT POLICY AUDIT_DATAPUMP ;
```

Monitor Suspicious User-Activity Events

Common abnormal access patterns indicating suspicious activity:

- Multiple failed login attempts
- Sudden activity in dormant accounts
  - Identify dormant accounts from DBSAT



Inactive Users

USER.INACTIVE STIG

Status Low Risk

Summary Found 24 user accounts that will never lock even when inactive. Found 16 unlocked users inactive for more than 30 days.

Details

```
Users with unlimited INACTIVE_ACCOUNT_TIME:
APEX_180200, APEX_INSTANCE_ADMIN_USER, APEX_LISTENER, APEX_PUBLIC_USER,
    APEX_REST_PUBLIC_USER, APPUSER, DBJSON, DBSAT, FINACME, FLOWS_FILES,
    HCM1, HR, HRREST, MYDBA, OBE, ORDS_PUBLIC_USER, PDBADMIN, SCOTT, U1,
    U2, U3, XDBEXT, XDBPM, XFILES
Inactive users: APEX_180200, APEX_INSTANCE_ADMIN_USER, APPUSER, FINACME,
    FLOWS_FILES, HCM1, HR, HRREST, MYDBA, OBE, PDBADMIN, SCOTT, U1, U2, U3,
    XFILES
```

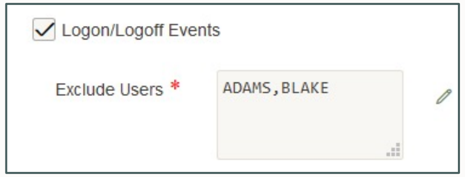
Remarks If a user account is no longer in use, it increases the attack surface of the system unnecessarily while providing no corresponding benefit. Furthermore, unauthorized use is less likely to be noticed when no one is regularly using the account. Accounts that have been unused for more than 30 days should be investigated to determine whether they should remain active. A solution is to set INACTIVE_ACCOUNT_TIME in the profiles assigned to users to automatically lock accounts which have not logged in to the database instance in a specified number of days. It is also recommended to audit infrequently used accounts for unauthorized activities.

References Oracle Database 12c STIG v1 r10: Rule SV-76207r2

- Non-business hour activities

Recommendations:

- Provision pre-defined audit policy for tracking logins
  - Audits logon and logoff activities for database users except for a specified list
  - Audits all unsuccessful logons and logoffs.

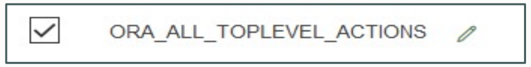


☑ Logon/Logoff Events

Exclude Users * ADAMS,BLAKE

Oracle Data Safe /
Oracle AVDF

- Provision audit policy "**ORA_ALL_TOPLEVEL_ACTIONS**" for dormant set of users:



☑ ORA_ALL_TOPLEVEL_ACTIONS

Oracle Data Safe /
Oracle AVDF

- For non-business hour operations, configure audit policy with application context representing date:

```
Sample:
CREATE AUDIT POLICY AUDIT_NON_BUSINESS_HOURS
ACTIONS update ON HR.EMPLOYEES
WHEN '((SYS_CONTEXT("DATE_CTX","DAY")  IN " SUNDAY")
EVALUATE PER STATEMENT;
```

Sensitive Data Access Auditing Recommendations

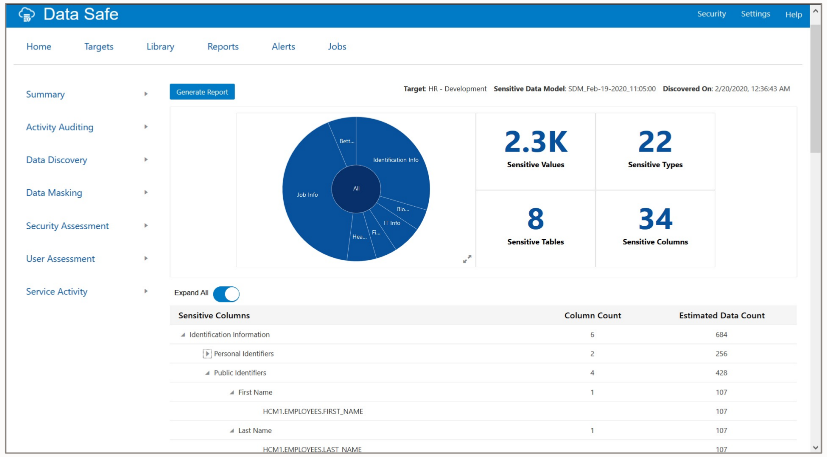
[Date]

Audit Recommendations:
Audit user access to sensitive data through untrusted path
Audit user access to sensitive data
Audit sensitive columns storing Personally Identifiable Information (PII) data

Identify Sensitive Data Landscape and Allow-list Users

Identify sensitive data landscape

- Sensitive data discovery feature in Data Safe



Target: HR - Development **Sensitive Data Model**: SDM_Feb-19-2020_11:05:00 **Discovered On**: 2/20/2020, 12:36:43 AM

2.3K Sensitive Values

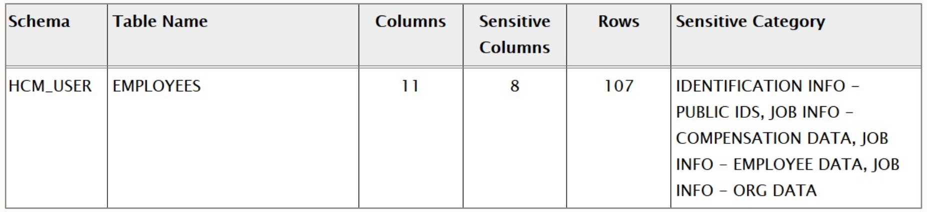
22 Sensitive Types

8 Sensitive Tables

34 Sensitive Columns

Sensitive Columns	Column Count	Estimated Data Count
Identification Information	6	684
Personal Identifiers	2	256
Public Identifiers	4	428
First Name	1	107
HCM1.EMPLOYEES.FIRST_NAME		107
Last Name	1	107
HCM1.EMPLOYEES.LAST_NAME		107

- DBSAT report



Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
HCM_USER	EMPLOYEES	11	8	107	IDENTIFICATION INFO – PUBLIC IDS, JOB INFO – COMPENSATION DATA, JOB INFO – EMPLOYEE DATA, JOB INFO – ORG DATA

- Enterprise Manager’s Application Data Modeling

Identify who can access your sensitive data

- Authorized users with valid business reason (Allow-list)
  - Application service accounts:
    - Used by an application to perform a defined set of standardized business functions;
    - Data access through trusted path -> Lower risk
    - Data access outside of trusted path -> Higher risk
  - Database users authorized to directly interact
    - For generating reports, performing ad-hoc queries or otherwise interact with data
    - Audit recommended
- Attempts by anyone else (Not in Allow-list, Watch-list)
    - Higher level of risk, must be audited

Audit User Access to Sensitive Data through Untrusted Path

For Application service accounts

- Audit all top-level actions on sensitive data
- Exclude trusted path

Sample:

```
CREATE AUDIT POLICY USER_ACTIVITY_NOT_IN_APP_PATH
ACTIONS ALL ON HR.EMPLOYEES
WHEN

'SYS_CONTEXT("APPUSER_CONTEXT", "APP_USER") NOT IN
("EMPLOYEE_USER","HR_USER","HR_MANAGER")'
EVALUATE PER STATEMENT
ONLY TOPLEVEL;

AUDIT POLICY USER_ACTIVITY_NOT_IN_APP_PATH by users with
granted roles EMP_ROLE,HR_ROLE,HR_MGR;
```

For users authorized to directly interact with sensitive data

- Minimally audit all top-level actions on sensitive data irrespective of trusted paths

Sample:

```
CREATE AUDIT POLICY USER_ACTIVITY_HUMAN_ACTORS
ACTIONS
ALL ON HR.EMPLOYEES
ONLY TOPLEVEL;

AUDIT POLICY USER_ACTIVITY_HUMAN_ACTORS by sophie, john;
```

Audit User Access to Sensitive Data

Attempts by **anyone else** should always be audited:

- Who is not authorized to access sensitive data(Not in allow-list)
- Who is in the watch-list

Track all Top-level actions of such users on sensitive objects

Sample:

```
CREATE AUDIT POLICY REJECT_LIST_ACTIVITY
ACTIONS
INSERT ON HR.DEPARTMENTS, UPDATE ON HR.DEPARTMENTS,
DELETE ON HR.DEPARTMENTS

WHEN 'SYS_CONTEXT(''APPUSER_CONTEXT'', ''APP_USER'') IN
(''HR_USER'')'
EVALUATE PER STATEMENT;

AUDIT POLICY REJECT_LIST_ACTIVITY EXCEPT hr_ann;
```

Audit Sensitive Columns storing Personally Identifiable Information (PII)

When do you require granular monitoring of sensitive data access ?

- Monitor access to security-relevant columns that hold sensitive PII information
- Monitor data access based on security-relevant column values
- Customize audit settings such as accessing a table between 9 p.m. and 6 a.m., or on Sunday
- Alert the security administrator when an audited column that should not be changed at midnight is updated

Configure Fine-grained auditing (FGA) policies to augment intrusion detection

Sample:

```
BEGIN
DBMS_FGA.ADD_POLICY(
object_schema     => 'HR',
object_name       => 'EMPLOYEES',
policy_name       => 'updates_on_salary_column',
audit_column      => 'SALARY',
enable            =>  TRUE,
statement_types   => 'UPDATE');
END;
```

Summarizing the Golden Principles of fine-tuning Audit

Oracle Database

Privileged
user activity monitoring

Security-relevant
events auditing

Sensitive data access
auditing

[Date]

Audit Trail Management Recommendations

- **Relocate Unified Audit trail table to a dedicated tablespace**
  - Create and designate a dedicated tablespace
- **Set manageable Unified Audit trail partition interval**
  - Partition interval frequency depends on the rate of audit record generation
  - Default is one day from 21c onwards
- **Archive audit records and purge the Unified Audit trail**
  - Consolidate audit data in a dedicated repository(Oracle AVDF, Oracle Data Safe) than the source
  - Purge old audit records at source
- **Plan your queries to fetch audit records from Unified Audit trail**
  - Ensure the statistics of unified audit internal table are up to date.
  - Load the unified audit records that are written to operating system spillover files.
  - Include EVENT_TIMESTAMP_UTC column in a WHERE clause when querying UNIFIED_AUDIT_TRAIL

Summary

- Database auditing is an integral component of an organization’s data security architecture
- Oracle Unified Auditing significantly enhances auditing functionality of the database
- Leverage the golden principles of fine-tuning audit policies based on the privileged user activity, security-relevant events, and sensitive data access

Call To Action

- Review technical report for more details:
  - https://www.oracle.com/a/tech/docs/dbsec/unified-audit-best-practice-guidelines.pdf

- Traditional auditing is deprecated in 21c, and will be de-supported in near release. Recommend to plan migrating to Unified Auditing for Oracle Database 12c and above

- If you would like Oracle to take a look at your existing Unified Audit policies and suggest recommendations to further fine-tune them, please log a Support Request with the title: **Fine-tuning Unified Audit Policies**

Thank You

Angeline Janet Dhanarani
Product Management,
Oracle Database Security