Upgrade to Unified Auditing

Auditing von 11g nach 12c

Sebastian Winkler
CarajanDB GmbH

© 2016 CarajanDB GmbH

CarajanDB

- Experten mit über 30 Jahren Oracle Erfahrung
- Firmensitz in Erftstadt bei Köln
- Spezialisten für
  - Oracle Datenbank Administration
  - Hochverfügbarkeit (RAC, Data Guard, Failsafe, etc.)
  - Einsatz der Oracle Standard Edition
  - Oracle Migrationen (HW, Unicode, Konsolidierung, Standard Edition)
  - Replikation (GoldenGate, SharePlex, Dbvisit)
  - Performance Tuning
  - Database Cloning (Actifio, Delphix, CloneDB)
- Fernwartung
- Schulung und Workshops (Oracle, Toad)

© 2016 CarajanDB GmbH

Agenda

- Überblick
  - New Unified Auditing in 12c
- Upgrade
  - Mixed und Pure Mode
- Unified Audit Policies
  - Anwendungsbeispiele
- Konfiguration
  - Management und Performance

© 2016 CarajanDB GmbH

CARAJANDB

Überblick

© 2016 CarajanDB GmbH

12c Auditing – Neues Konzept

- Was sagt Oracle?
  - Paul Needham, Senior Director, Product Management - Oracle Database Security

- Unified and Conditional Audit
  - Unified = vereinheitlicht, konsolidiert => Aufbau
  - Conditional = bedingt, abhängig => Prozess

- New Unified Audit
  - Policy Based => vereinfachte Handhabung
  - Conditional => effektiveres Auditing
  - User Exceptions => einfache Ausnahmen
  - Extensible Syntax => bezieht Database Vault, Label Security, RMAN und weiteres ein

© 2016 CarajanDB GmbH

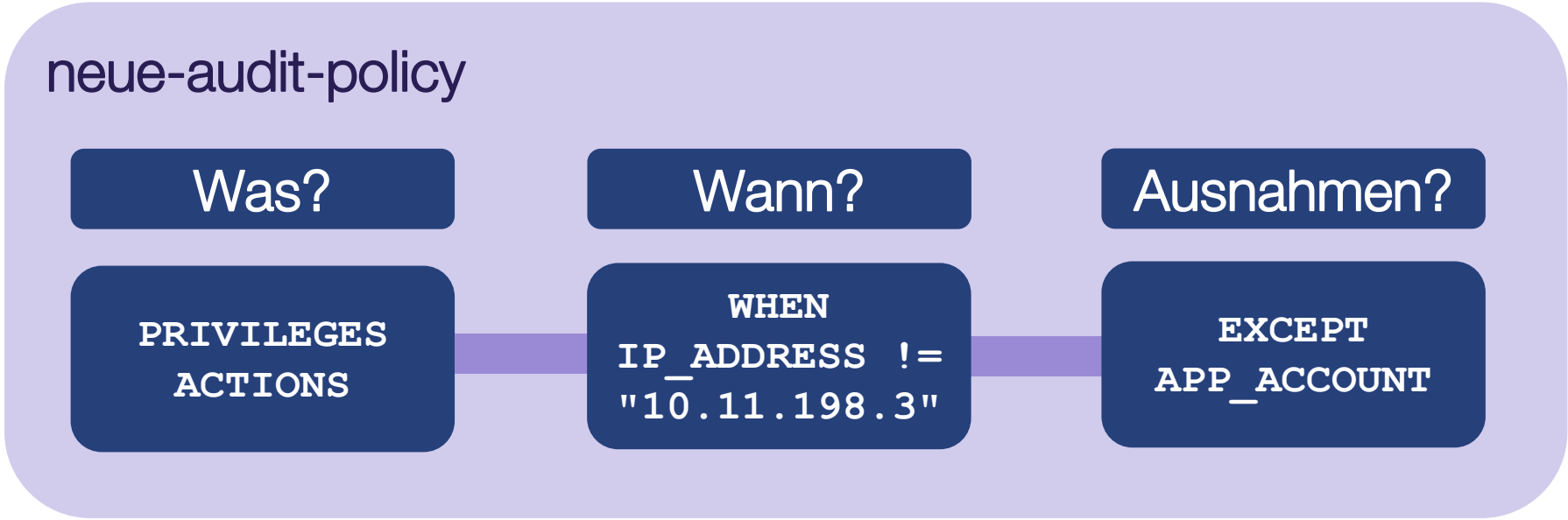
12c Auditing – Unified Audit Trail

- Unified Audit Trail
  - AUD$
  - FGA_LOG$
  - DVSYS.AUDIT_TRAIL$
  - OS, XML, EXTENDED

© 2016 CarajanDB GmbH

12c Auditing – Audit Policy

- Grundaufbau 12c Audit Policy



© 2016 CarajanDB GmbH

12c Auditing – Audit Schema und Rollen

- Schema AUDSYS
- Rollen
  - Audit Viewer Rolle
    - Audit Daten ansehen
  - Audit Admin Rolle
    - Policies verwalten
    - Audit Daten verwalten

Audit Viewer Role

`Audit Daten ansehen`

Audit Admin Role

`Audit Daten verwalten`

`Policies verwalten`

© 2016 CarajanDB GmbH

CARAJANDB

Upgrade

© 2016 CarajanDB GmbH

12c Auditing – Abwärtskompatibilität

- Oracle Online Documentation 12c Release 2
  - Administration
    - Database SQL Language Reference

„Beginning with Oracle 12c, Oracle introduces unified auditing, which provides a full set of enhanced auditing features. For backward compatibility, traditional auditing is still supported."

AUDIT (Traditional Auditing)

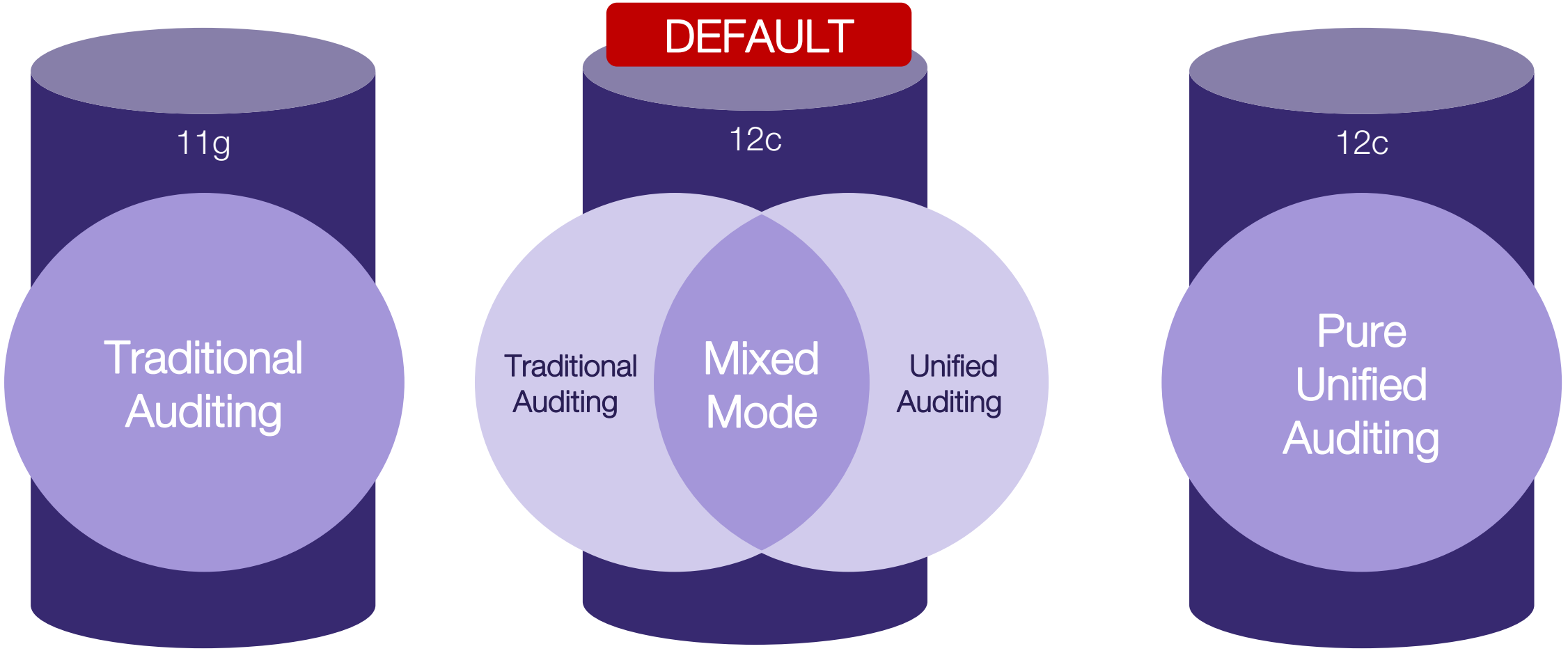
This section describes the `AUDIT` statement for **traditional auditing**, which is the same auditing functionality used in releases earlier than Oracle Database 12*c*.

Beginning with Oracle Database 12*c*, Oracle introduces **unified auditing**, which provides a full set of enhanced auditing features. For backward compatibility, traditional auditing is still supported. However, Oracle recommends that you plan the migration of your existing audit settings to the new unified audit policy syntax. For new audit requirements, Oracle recommends that you use the new unified auditing. Traditional auditing may be desupported in a future major release.

„However, Oracle recommends that you plan the migration of your existing audit settings to the new unified audit policy syntax."

© 2016 CarajanDB GmbH

12c Auditing - Abwärtskompatibilität



© 2016 CarajanDB GmbH

12c Auditing – Unified Audit Trail ???

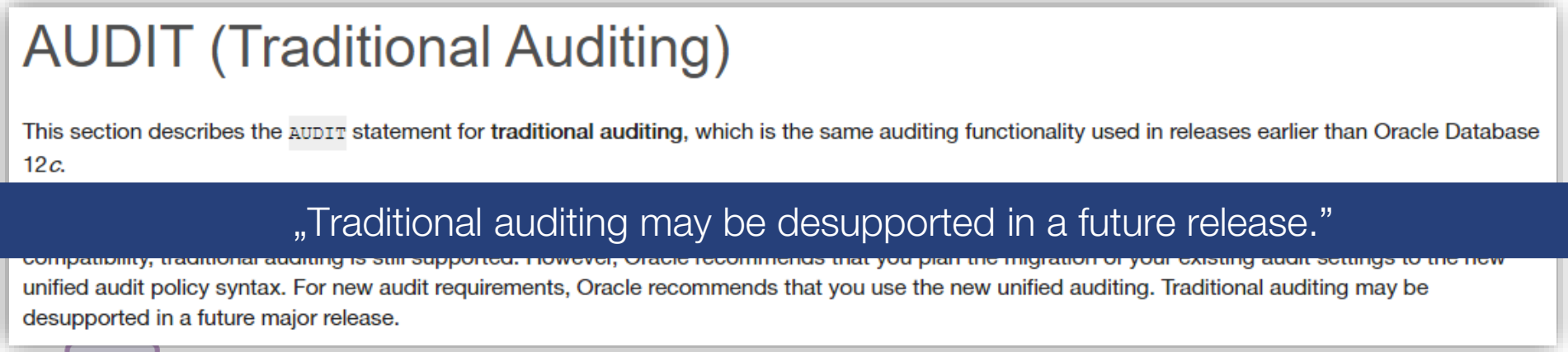
- Audit Trails ab 12c
  - *Unified Audit* *-> sys.unified_audit_trail*
  - Fine-Grained Audit -> sys.fga_log$
  - Standard Auditing -> sys.aud$
  - Sys User -> .aud Files
  - Mandatory Audit -> .aud Files
  - Trigger basiertes Audit -> …
  - Database Vault Audit -> dvsys.audit_trail$

© 2016 CarajanDB GmbH

12c Auditing – Mixed Mode vs. Pure Mode

- Mixed Mode = Unified Mode und Traditional Mode
  - Mixed Mode ist der Standard bei Upgrades und für neu erstellte Datenbanken
  - Alle „alten“ Audit Konfigurationen funktionieren weiterhin

- Pure Unified Mode
  - Oracle empfiehlt eine schrittweise Migration in den neuen Unified Mode
  - „Traditional“ Audit Features werden in künftigen Releases eingestellt – desupported



AUDIT (Traditional Auditing)

This section describes the `AUDIT` statement for **traditional auditing**, which is the same auditing functionality used in releases earlier than Oracle Database 12*c*.

„Traditional auditing may be desupported in a future release.”

unified audit policy syntax. For new audit requirements, Oracle recommends that you use the new unified auditing. Traditional auditing may be desupported in a future major release.

© 2016 CarajanDB GmbH

12c Auditing – Mixed Mode umstellen

- Mixed Mode
  - Unified Auditing deaktiviert?

```
SELECT parameter, value
FROM v$option
WHERE parameter = 'Unified Auditing';

PARAMETER            VALUE
-------------------  --------
Unified Auditing     FALSE
```

  - FALSE bedeutet: Unified Auditing wird nicht ausschließlich verwendet.

© 2016 CarajanDB GmbH

12c Auditing – Mixed Mode umstellen

- Pure Mode
  - Kernel relink

```
cd $ORACLE_HOME/rdbms/lib

make -f ins_rdbms.mk uniaud_on ioracle ORACLE_HOME=$ORACLE_HOME
```

  - Datenbank stoppen und Oracle Binary nach uniaud_on linken und wieder starten.

```
PARAMETER                 VALUE
------------------------  --------
Unified Auditing          TRUE
```


© 2016 CarajanDB GmbH

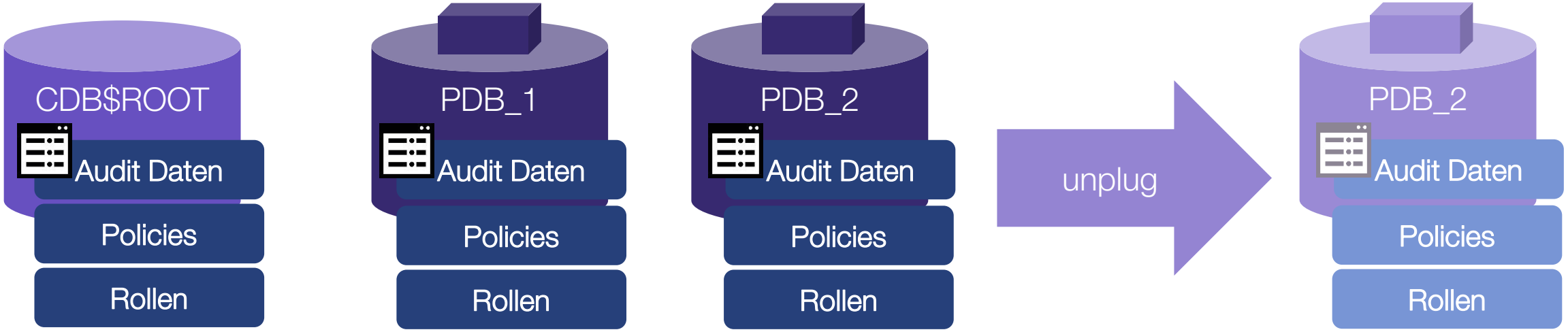
12c Auditing – Pure Mode

- Auswirkungen nach dem Kernel relink
  - Audit Einträge werden nur noch in Unified Audit Views abgelegt und in Oracle SecureFiles geschrieben
    - Logs können nicht mehr gelesen werden
  - Traditional Auditing Konfiguration wird nicht mehr genutzt
  - AUDIT_TRAIL, AUDIT_FILE_DEST, AUDIT_SYS_OPERATIONS, AUDIT_SYSLOG_LEVEL, … Parameter werden ignoriert
  - SYSLOG Auditing ist nicht mehr möglich!

© 2016 CarajanDB GmbH

12c Auditing – Multitenant Datenbanken

- Unified Audit von Pluggable Database (PDBs)
  - Jede PDB hat sein eigenes Audit Trail und eigene Policies
  - Jede PDB hat seine eigenen administrativen Rollen



  - Audit Trail und Policies wandern mit der PDB
    - Achtung: Common Policies, Roles, …

© 2016 CarajanDB GmbH

12c Auditing – Multitenant Datenbank

- Rollen Audit Admin + Audit Viewer
  - CDB + PDB

```
select *
from USER_ROLE_PRIVS
where GRANTED_ROLE='AUDIT_ADMIN' or GRANTED_ROLE='AUDIT_VIEWER';

USERNAME          GRANTED_ROLE
--------------    ------------------
SYS               AUDIT_ADMIN
SYS               AUDIT_VIEWER
```


© 2016 CarajanDB GmbH

12c Auditing - Neue Rollen

- Zwei neue Rollen für die Gewaltenteilung im Auditing

- Audit Admin (AUDIT_ADMIN)

- Audit Viewer (AUDIT_VIEWER)
  - Benutzer mit dieser Rolle können ausschließlich lesend auf die verschiedenen Audit Trails zugreifen (dba_audit_trail, dba_fga_audit_trail und unified_audit_trail)
    - GRANT SELECT ON …
  - Kein direkter Zugriff auf Basistabellen (sys.aud$, audsys.cli_swp…)
  - Geeignet für Auswertung, Revisoren

© 2016 CarajanDB GmbH

12c Auditing - Neue Rollen

- Audit Admin (AUDIT_ADMIN)
  - Benutzer mit dieser Rolle können ausschließlich lesend auf die verschiedenen Audit Trails zugreifen (dba_audit_trail, dba_fga_audit_trail und unified_audit_trail)
    - Zusätzlich noch dba_users und dba_objects
    - GRANT SELECT ON …
  - Systemprivilegien
    - GRANT AUDIT ANY
    - GRANT AUDIT SYSTEM
  - Zugriff auf dbms_audit_mgmt und dbms_fga
    - GRANT EXECUTE ON SYS.DBMS_AUDIT_MGMT
    - GRANT EXECUTE ON SYS.DBMS_FGA
  - Keine direkter Zugriff auf Basistabellen (sys.aud$, audsys.cli_swp…)
  - Nur für Security Admins geeignet – nicht DBA, da er sonst Audit-Daten löschen kann

© 2016 CarajanDB GmbH

12c Auditing – Multitenant Datenbank

- Audit Tablespace
  - CDB + PDB

```
select *
from dba_audit_mgmt_config_params
where parameter_name = 'DB AUDIT TABLESPACE';

PARAMETER_NAME                 PARAMETER_VALUE      AUDIT_TRAIL
------------------------------ -------------------- --------------------
DB AUDIT TABLESPACE            SYSAUX               STANDARD AUDIT TRAIL
DB AUDIT TABLESPACE            SYSAUX               FGA AUDIT TRAIL
DB AUDIT TABLESPACE            SYSAUX               UNIFIED AUDIT TRAIL
```


© 2016 CarajanDB GmbH

12c Auditing – Multitenant Datenbank

- Audit Tablespace
  - CDB + PDB

```
select owner, segment_type, tablespace_name
from dba_segments
where segment_name = 'CLI_SWP$%'
or segment_name = 'FGA_LOG$'
or segment_name = 'AUD$';

OWNER   SEGMENT_NAME          SEGMENT_TYPE     TABLESPACE_NAME
------  --------------------  ---------------  ---------------
SYS     AUD$                  TABLE            SYSTEM
SYS     FGA_LOG$              TABLE            SYSTEM
AUDSYS  CLI_SWP$7ab1f289$1$1  TABLE PARTITION  SYSAUX
```


© 2016 CarajanDB GmbH

12c Auditing – Multitenant Datenbank

- Audit Tablespace
  - CDB + PDB

```
select owner, segment_type, tablespace_name
from dba_segments
where segment_name = 'CLI_SWP$%'
or segment_name = 'FGA_LOG$'
or segment_name = 'AUD$';

OWNER   SEGMENT_NAME          SEGMENT_TYPE     TABLESPACE_NAME
------  --------------------  ---------------  ----------------
SYS     AUD$                  TABLE            SYSTEM
SYS     FGA_LOG$              TABLE            SYSTEM
AUDSYS  CLI_SWP$7ab1f289$1$1  TABLE PARTITION  SYSAUX
```


© 2016 CarajanDB GmbH

12c Auditing – Multitenant Datenbank

- Audit Tablespace
  - CDB + PDB

```
select owner, segment_type, tablespace_name
from dba_segments
where segment_name = 'CLI_SWP$%'
or segment_name = 'FGA_LOG$'
or segment_name = 'AUD$';

OWNER   SEGMENT_NAME          SEGMENT_TYPE      TABLESPACE_NAME
------  --------------------  ----------------  ---------------
SYS     AUD$                  TABLE             SYSTEM
SYS     FGA_LOG$              TABLE             SYSTEM
AUDSYS  CLI_SWP$7ab1f289$1$1  TABLE PARTITION   SYSAUX
```


© 2016 CarajanDB GmbH

12c Auditing – Audit Daten verschieben

- Neuen exklusiven Tablespace für Audit Daten erstellen

```
create tablespace AUDIT_DATA
   datafile size 1000M autoextend on next 100M maxsize 2000M;
```

- Initialisieren der Audit Trails zur Konfiguration mit dem dbms_audit_mgmt Package
  - Für Unified Audit Trail NICHT notwendig

```
BEGIN
  dbms_audit_mgmt.init_cleanup(
  audit_trail_type => dbms_audit_mgmt.audit_trail_all,
  default_cleanup_interval => 12 /* hours */);
END;
/
```


© 2016 CarajanDB GmbH

12c Auditing – Audit Daten verschieben

- Standard Auditing (AUD$) und Fine Grained Auditing (FGA_LOG$) verschieben

```
BEGIN
   dbms_audit_mgmt.SET_AUDIT_TRAIL_LOCATION(
    audit_trail_type => dbms_audit_mgmt.AUDIT_TRAIL_AUD_STD,
    audit_trail_location_value => 'AUDIT_DATA');
END;
/

BEGIN
   dbms_audit_mgmt.SET_AUDIT_TRAIL_LOCATION(
    audit_trail_type => dbms_audit_mgmt.AUDIT_TRAIL_FGA_STD,
    audit_trail_location_value => 'AUDIT_DATA');
END;
/
```


© 2016 CarajanDB GmbH

12c Auditing – Audit Daten verschieben

- Unified Audit Trail verschieben
  - Neue Audit Records werden in die neue Location geschrieben

```
BEGIN
   dbms_audit_mgmt.SET_AUDIT_TRAIL_LOCATION(
    audit_trail_type => dbms_audit_mgmt.AUDIT_TRAIL_UNIFIED,
    audit_trail_location_value => 'AUDIT_DATA');
END;
/
```

```
select segment_name from dba_segments where owner = 'AUDSYS';

SEGMENT_NAME
--------------------------------------------------------------------
SYS_LOB0000091756C00014$$
SYS_IL0000091756C00014$$
CLI_SCN$7ab1f289$1$1
CLI_TIME$7ab1f289$1$1
CLI_LOB$7ab1f289$1$1
CLI_SWP$7ab1f289$1$1
```


© 2016 CarajanDB GmbH

12c Auditing – Audit Daten verschieben

- Unified Audit Trail verschieben
  - Alte Audit Records werden nicht verschoben!

Archivierung => Cleanup

```
select owner, segment_type, tablespace_name
from dba_segments
where segment_name = 'CLI_SWP$%'
or segment_name = 'FGA_LOG$'
or segment_name = 'AUD$';

OWNER   SEGMENT_NAME          SEGMENT_TYPE      TABLESPACE_NAME
------  --------------------  ----------------  ---------------
SYS     AUD$                  TABLE             AUDIT_DATA
SYS     FGA_LOG$              TABLE             AUDIT_DATA
AUDSYS  CLI_SWP$7ab1f289$1$1  TABLE PARTITION   AUDIT_DATA
AUDSYS  CLI_SWP$7ab1f289$1$1  TABLE PARTITION   SYSAUX
```


© 2016 CarajanDB GmbH

CARAJAN DB

Unified Audit Policies

© 2016 CarajanDB GmbH

12c Auditing – Standard Policies

- Mitgelieferte Standard Policies
  - Account Management
    - Create User
    - Grant, Revoke
    - Create Role
    - Drop Role
  - Database Parameters
    - Create SPFILE
    - Alter System
    - Alter Database
  - Secure Configuration
    - Alter Any
    - Create Any
    - Alter User
    - Alter Profile

```
select distinct policy_name
from audit_unified_policies;

POLICY_NAME
------------------------------
ORA_ACCOUNT_MGMT
ORA_DATABASE_PARAMETER
ORA_SECURECONFIG
ORA_LOGON_FAILURES
ORA_CIS_RECOMMENDATIONS
ORA_RAS_POLICY_MGMT
ORA_RAS_SESSION_MGMT
ORA_DV_AUDPOL
```

CIS = Center for Internet Security
RAS = Real Application Security
DV = Database Vault

© 2016 CarajanDB GmbH

12c Auditing – Standard Policies

- Neu mitgelieferte Standard Policies
  - 2 Unified Audit Policies bereits aktiv für alle User

```
select policy_name, enabled_opt, user_name, success, failure
from audit_unified_enabled_policies;

POLICY_NAME          ENABLED_OPT   USER_NAME     SUCCESS       FAILURE
-------------------  ------------  ------------  ------------  --------
ORA_SECURECONFIG     BY            ALL USERS     YES           YES
ORA_LOGON_FAILURES   BY            ALL USERS     NO            YES
```

  - ORA_SECURECONFIG
    - Überwachung Audit-Konfiguration, Audit Trail und kritische Systemprivilegien

© 2016 CarajanDB GmbH

12c Auditing – Standard Policies

- Neu mitgelieferte Standard Policies
  - 2 Unified Audit Policies bereits aktiv für alle User

```
select policy_name, enabled_opt, user_name, success, failure
from audit_unified_enabled_policies;

POLICY_NAME          ENABLED_OPT   USER_NAME     SUCCESS       FAILURE
-------------------  ------------  ------------  ------------  --------
ORA_SECURECONFIG     BY            ALL USERS     YES           YES
ORA_LOGON_FAILURES   BY            ALL USERS     NO            YES
```

  - Bug 19383839 - UNIFIED AUDIT - NO LOGON OR FAILED LOGON ACTION CAPTURED
    - Unified Audit Trail - LOGON Action Not Captured (Doc ID 1940793.1) – Patch verfügbar

© 2016 CarajanDB GmbH

12c Auditing – Standard Policies

- Neu mitgelieferte Standard Policies
  - 2 Unified Audit Policies bereits aktiv für alle User

```
select policy_name, enabled_opt, user_name, success, failure
from audit_unified_enabled_policies;

POLICY_NAME          ENABLED_OPT   USER_NAME     SUCCESS       FAILURE
-------------------  ------------  ------------  ------------  --------
ORA_SECURECONFIG     BY            ALL USERS     YES           YES
ORA_LOGON_FAILURES   BY            ALL USERS     NO            YES
```

  - Policies deaktivieren

```
noaudit policy ORA_SECURECONFIG;
noaudit policy ORA_LOGON_FAILURES;
```


© 2016 CarajanDB GmbH

12c Auditing – Unified Audit Policies

- Grundaufbau 12c Audit Policy

  - Vorteile gegenüber „altem“ Standard Auditing
    - Umsetzung komplexerer Sicherheits- und Audit-Anforderungen einfacher
    - Explizite Überwachung für bestimmte Kontexte (Netzwerk, Anwender, Zeit)

© 2016 CarajanDB GmbH

12c Auditing – Unified Audit Policies

- Grundaufbau 12c Audit Policy

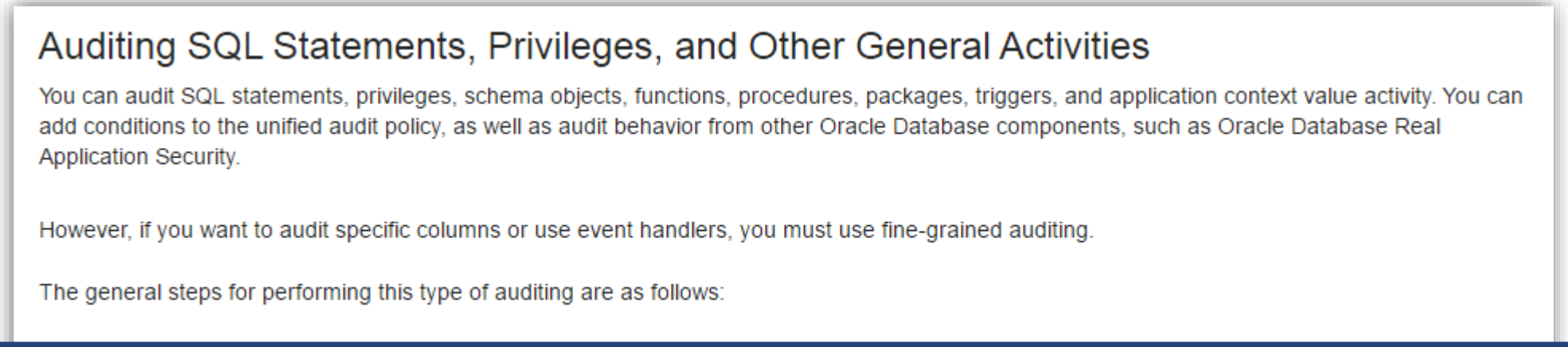
  - Auditieren von Aktionen, Objekten und Privilegien
    - Policy kann Bedingungen und / oder Rollen beinhalten
    - Policy kann aktiviert und deaktiviert werden

© 2016 CarajanDB GmbH

12c Auditing – UA Policies vs. Fine-Grained

- Oracle Online Documentation 12c Release 2
  - Database Security Guide
    - 22 Configuring Audit Policies

„You can configure unified auditing by creating custom unified audit policies, using predefined unified auditing policies, or using fine-grained auditing."



Auditing SQL Statements, Privileges, and Other General Activities

You can audit SQL statements, privileges, schema objects, functions, procedures, packages, triggers, and application context value activity. You can add conditions to the unified audit policy, as well as audit behavior from other Oracle Database components, such as Oracle Database Real Application Security.

However, if you want to audit specific columns or use event handlers, you must use fine-grained auditing.

The general steps for performing this type of auditing are as follows:

„However, if you want to audit specific columns or use event handlers, you must use fine-grained auditing."

© 2016 CarajanDB GmbH

12c Auditing – Policy Beispiel

- pol_connect_proxy

```
create audit policy pol_connect_proxy
actions all
when 'sys_context("userenv","proxy_user") is not NULL'
evaluate per session;
```

  - actions all: alle Aktionen werden auditiert
  - when: Bedingung – connect über proxy_user

```
sqlplus app_dba [app] / app_dba_password@appspdb    *** proxy connection ***
SQL> select sys_context('userenv', 'proxy_user') from dual;
-----------
app_dba
```


© 2016 CarajanDB GmbH

12c Auditing – Policy Beispiel

- pol_connect_dblink

```
create audit policy pol_connect_dblink
actions all
when 'sys_context("userenv","dblink_info") is not NULL'
evaluate per session;
```

  - actions all: alle Aktionen werden auditiert
  - when: connect über DB Link
  - Evaluate:
    - per statement: für jedes einzelne Statement
    - per session: einmalig für die Laufzeit einer Session
    - per instance: einmalig für die Laufzeit der Instanz

© 2016 CarajanDB GmbH

12c Auditing – Policy Beispiel

- pol_maint_user

```
create audit policy pol_maint_user
privileges create user, drop user
actions create user, drop user, execute on DBMS_AUDIT_MGMT;
```

  - Alle CREATE USER und DROP USER Aktionen auditieren

  - OBJECT ACTION => execute on SYS.DBMS_AUDIT_MGMT
    - Audit Record bei jeder Ausführung des Objekts
  - STANDARD ACTION => CREATE, ALTER, DROP USER
    - Audit Record bei jeder Ausführung des Befehls
  - SYSTEM PRIVILEGE => CREATE, ALTER, DROP USER
    - Audit Record wenn ein Benutzer der das Privileg gegranted hat den Befehl ausführt
    - SYS ist OWNER des Privilegs, daher kein Record!

© 2016 CarajanDB GmbH

12c Auditing – Policy Beispiel

- pol_maint_role_java

```
create audit policy pol_maint_role_java
role java_admin, java_deploy;
```

  - Rollen JAVA_ADMIN und JAVA_DEPLOY auditieren
    - Auditiert alle aus den Systemprivilegien resultierenden SQL Statements

- pol_maint_role_dbas

```
create audit policy pol_maint_role_dbas
role dba, cdb_dba, pdb_dba;
```

  - DBA‘s auditieren leicht gemacht

© 2016 CarajanDB GmbH

12c Auditing – Policy Beispiel

- pol_aud_booking

```
create audit policy pol_aud_booking
actions
   insert on app.booking, update on app.booking, delete on app.booking,
   select on app.booking
when 'sys_context("userenv","client_identifier") = "Sebastian"'
evaluate per statement;
```

  - INSERT, UPDATE, DELETE … eines bestimmten Anwenders auditieren

© 2016 CarajanDB GmbH

12c Auditing – Policy Beispiel

- pol_connect_app

```
create audit policy pol_connect_app
actions all
when '(upper(sys_context("userenv","module")) != "myappname") or
 sys_context("userenv","ip_address") != "127.0.0.1")'
evaluate per session;

audit policy pol_connect_app except hr;
```

  - Sicherstellung, dass nur Verbindungen über die Anwendung kommen
    - hier: Modulname, IP Adresse
    - Ausnahme: except HR

© 2016 CarajanDB GmbH

12c Auditing – Policy Bedingungen

- WHEN - Audit Condition - Bedingung
  - SYS_CONTEXT ('userenv',…), UID
  - Numerische Funktionen
    - BITAND, CEIL, FLOOR, POWER
  - Zeichenfunktionen, welche Zeichen zurückgeben
    - CONCAT, LOWER und UPPER
  - Zeichenfunktionen, welche Numerische Werte zurückgeben
    - LENGTH oder INSTR
  - Logisch und Vergleich
    - AND, OR, IN, NOT IN, =, <, >, <>, !=, >=, <=
  - IS [NOT] NULL, [NOT] BETWEEN, [NOT] IN
  - SYSDATE, SYSTIMESTAMP, CURRENT_DATE und CURRENT_TIME
  - (leider) keine beliebige PL/SQL-Funktion anwendbar

© 2016 CarajanDB GmbH

12c Auditing – Policy Syntax

- Komplette Syntax

```
CREATE AUDIT POLICY policy_name{{privilege_audit_options [action_audit_options]
[role_audit_options]}|{action_audit_options}[role_audit_options]}|{role_audit_opti
ons}}[WHEN audit_condition EVALUATE PER {STATEMENT|SESSION|INSTANCE}][CONTAINER =
{CURRENT|ALL}];

privilege_audit_options := PRIVILEGES privilege1 [,privilege2]

action_audit_options := {standard-actions | component-actions}[,component-actions]
standard-actions := ACTIONS action1 [ON{schema.obj_name | DIRECTORY directory_name | MINING
MODEL schema.obj_name}][,action2 [ON{schema.obj_name | DIRECTORY directory_name | MINING_MODEL
schema.obj_name}]
component-actions := ACTIONS COMPONENT=[DV|OLS|XS|DATAPUMP|DIRECT_LOAD] action1 [,action2]

role_audit_options := ROLES role1 [,role2]

audit_condition := function operation value_list
```


© 2016 CarajanDB GmbH

12c Auditing – Policy aktivieren

- Audit Policy aktivieren

```
AUDIT POLICY pol_connect_app;
```

  - Policies werden erst durch explizites „einschalten“ aktiv

```
AUDIT POLICY pol_aud_booking except HUGO;
```

  - Für alle Benutzer aktivieren oder mit `BY` oder `EXCEPT` auf bestimmte User einschränken

```
AUDIT POLICY pol_maint_role_dbas whenever successful;
```

  - mit `WHENEVER [NOT] SUCCESSFUL` nur wenn [nicht] erfolgreich, oder bei jedem = keine Angabe

Deaktivieren:

```
NOAUDIT POLICY pol_maint_role_dbas;
```


© 2016 CarajanDB GmbH

12c Auditing – Policies in Multitenant

- Traditional Auditing

```
AUDIT DROP ANY TABLE BY SYSTEM BY ACCESS CONTAINER = CURRENT;
```

```
AUDIT DROP ANY TABLE BY SYSTEM BY ACCESS CONTAINER = ALL;
```

- Unified

```
CREATE AUDIT POLICY policy_name
 action1 [,action2 ]
 [CONTAINER = {CURRENT | ALL}];

CREATE AUDIT POLICY pol_dict_updates
 ACTIONS UPDATE ON SYS.USER$, DELETE ON SYS.USER$
 CONTAINER = ALL;
```


© 2016 CarajanDB GmbH

12c Auditing – Policies in Multitenant

- Standardmäßig sind Audit Policies lokal und PDB bezogen
- Local Audit Policies
  - Verfügbar im Root Container oder der PDB
  - Local Audit Policies im Root können Local und Common Objects auditieren.
  - Local und Common User mit der AUDIT_ADMIN Rolle können Local Policies aktivieren
- Common Audit Policies
  - Common Policies können nur im Root Container angelegt werden
  - Für alle PDBs in der Multitenant Umgebung verfügbar
  - Ausschließlich Common User mit AUDIT_ADMIN Rolle können Common Audit Policies verwalten – sie können also nur Common Usern zugewiesen werden
  - kann Objekt Auditing nur für Common Objects

© 2016 CarajanDB GmbH

CARAJANDB

Konfiguration

© 2016 CarajanDB GmbH

12c Auditing – Audit Daten verwalten

- Management mit DBMS_AUDIT_MGMT Package
  - wurde um Unified Audit Funktionen erweitert
- Privilegien
  - Unified Audit Trail Management nur mit AUDIT_ADMIN Rolle
- Multitentant
  - Alle PDBs oder einzelne per CONTAINER Klausel verwalten
    - CONTAINER_ALL
    - CONTAINER_CURRENT

© 2016 CarajanDB GmbH

12c Auditing – Audit Daten verwalten

- Unified Audit Trail bereinigen

```
BEGIN
  DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP(
   AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
   LAST_ARCHIVE_TIME => SYSDATE);
END;
/

BEGIN
  DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
   AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
   USE_LAST_ARCH_TIMESTAMP => TRUE,
   CONTAINER => DBMS_AUDIT_MGMT.CONTAINER_CURRENT);
END;
/
```


© 2016 CarajanDB GmbH

12c Auditing – Performance

- 2 Modi zum Schreiben der Audit Records
  - Queued Mode
    - Audit Records werden in SGA gelagert und alle 3 Sekunden geflushed

```
AUDIT_TRAIL_QUEUED_WRITE
```

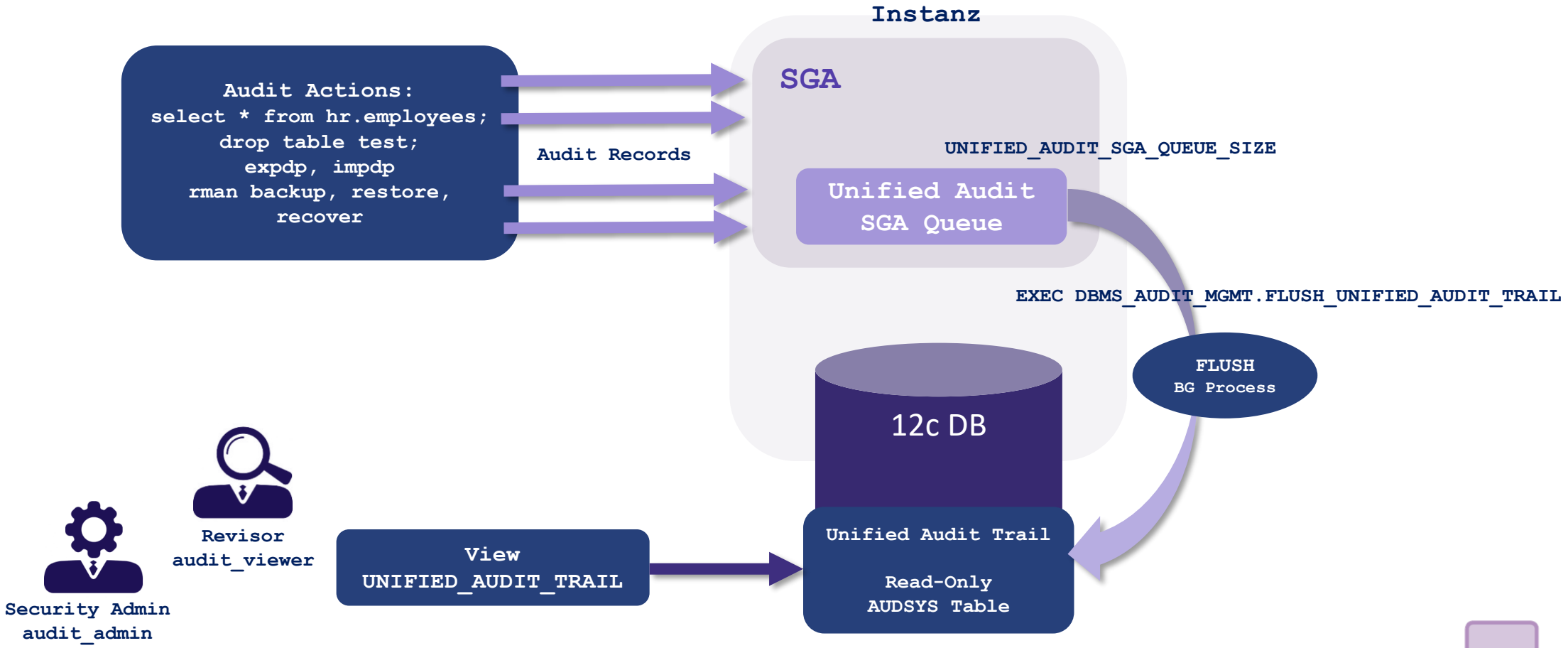
  - Immediate Mode
    - Audit Records werden direkt geschrieben - für hohe Sicherheit

```
EXECUTE DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_WRITE_MODE,
 DBMS_AUDIT_MGMT.AUDIT_TRAIL_IMMEDIATE_WRITE);
```


© 2016 CarajanDB GmbH

12 Auditing - Performance

- Unified Auditing – Queued Mode (Default)



© 2016 CarajanDB GmbH

12c Auditing – Performance

- UNIFIED_AUDIT_SGA_QUEUE_SIZE
  - Initialization Parameter for Queued Mode
  - Default value 1 MB (1048576)
  - Max value 30 MB

> **Note:**
> The `UNIFIED_AUDIT_SGA_QUEUE_SIZE` initialization parameter is deprecated in Oracle Database 12*c* Release 2 (12.2.0.1), and may be desupported in a future release.

  - Deprecated in 12.2, and may be desupported in a future release

- _UNIFIED_AUDIT_FLUSH_INTERVAL => 3 Sekunden
- _UNIFIED_AUDIT_FLUSH_THRESHOLD => 85 Prozent

```
EXEC SYS.DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL
```


© 2016 CarajanDB GmbH

12c Auditing – Performance

- Was wenn die Datenbank nicht verfügbar ist?

- Queued Mode (DEFAULT)
  - bei einem Shutdown Abort oder Instance Crash können Auditdaten verloren gehen
    - QUEUE SIZE + FLUSH INTERVAL

- Datenbank im Read-Only Mode oder nicht gemounted
  - Audit Records werden in OS Files geschrieben
    - `$ORACLE_BASE/audit/$ORACLE_SID`
  - Per DBMS_AUDIT_MGMT Package können die OS Daten ins Unified Audit Trail geschrieben werden

© 2016 CarajanDB GmbH

12c Auditing – AUDIT_TRAIL vs. UNIFIED_AUDIT_TRAIL

- AUDIT_TRAIL vs. UNIFIED_AUDIT_TRAIL

```
select count(*)
from dba_tab_columns
where table_name='DBA_COMMON_AUDIT_TRAIL';

  COUNT(*)
----------
        45
```

```
select count(*)
from dba_tab_columns
where table_name='UNIFIED_AUDIT_TRAIL';

  COUNT(*)
----------
        94
```

AUDIT_TYPE
SESSIONID
PROXY_SESSIONID
OS_USERNAME
USERHOST
TERMINAL
INSTANCE_ID
DBID
AUTHENTICATION_TYPE
DBUSERNAME
DBPROXY_USERNAME
EXTERNAL_USERID
GLOBAL_USERID
CLIENT_PROGRAM_NAME
DBLINK_INFO
XS_USER_NAME
XS_SESSIONID
ENTRY_ID
STATEMENT_ID
EVENT_TIMESTAMP
ACTION_NAME
RETURN_CODE
OS_PROCESS
TRANSACTION_ID
SCN
EXECUTION_ID
OBJECT_SCHEMA
OBJECT_NAME
SQL_TEXT
SQL_BINDS
APPLICATION_CONTEXTS
CLIENT_IDENTIFIER
NEW_SCHEMA
NEW_NAME
OBJECT_EDITION
SYSTEM_PRIVILEGE_USED
SYSTEM_PRIVILEGE
AUDIT_OPTION
OBJECT_PRIVILEGES
ROLE
TARGET_USER
EXCLUDED_USER
EXCLUDED_SCHEMA
EXCLUDED_OBJECT
ADDITIONAL_INFO
UNIFIED_AUDIT_POLICIES
FGA_POLICY_NAME
XS_INACTIVITY_TIMEOUT
XS_ENTITY_TYPE
XS_TARGET_PRINCIPAL_NAME
XS_PROXY_USER_NAME
XS_DATASEC_POLICY_NAME
XS_SCHEMA_NAME
XS_CALLBACK_EVENT_TYPE
XS_PACKAGE_NAME
XS_PROCEDURE_NAME
XS_ENABLED_ROLE
XS_COOKIE
XS_NS_NAME
XS_NS_ATTRIBUTE
XS_NS_ATTRIBUTE_OLD_VAL
XS_NS_ATTRIBUTE_NEW_VAL
DV_ACTION_CODE
DV_ACTION_NAME
DV_EXTENDED_ACTION_CODE
DV_GRANTEE
DV_RETURN_CODE
DV_ACTION_OBJECT_NAME
DV_RULE_SET_NAME
DV_COMMENT
DV_FACTOR_CONTEXT
DV_OBJECT_STATUS
OLS_POLICY_NAME
OLS_GRANTEE
OLS_MAX_READ_LABEL
OLS_MAX_WRITE_LABEL
OLS_MIN_WRITE_LABEL
OLS_PRIVILEGES_GRANTED
OLS_PROGRAM_UNIT_NAME
OLS_PRIVILEGES_USED
OLS_STRING_LABEL
OLS_LABEL_COMPONENT_TYPE
OLS_LABEL_COMPONENT_NAME
OLS_PARENT_GROUP_NAME
OLS_OLD_VALUE
OLS_NEW_VALUE
RMAN_SESSION_RECID
RMAN_SESSION_STAMP
RMAN_OPERATION
RMAN_OBJECT_TYPE
RMAN_DEVICE_TYPE
DP_TEXT_PARAMETERS1
DP_BOOLEAN_PARAMETERS1
DIRECT_PATH_NUM_COLUMNS_LOADED

© 2016 CarajanDB GmbH

12 Auditing - Performance

- Probleme mit dem Unified Audit Trail
  - Abfrage auf Unified Audit Trail View kann sich aufhängen
  - Bug 21119008 - POOR QUERY PERFORMANCE ON UNIFIED_AUDIT_TRAIL

„If there are a lot of audit records within unified audit trail, the query performance is extremely slow."

  - Performance Issues While Monitoring the Unified Audit Trail of an Oracle12c Database (Doc ID 2063340.1)
  - SELECT * FROM UNIFIED_AUDIT_TRAIL Blocks Other Sessions (Doc ID 2196171.1)

Workarounds:
- „Reduce the number of audit records in the Unified Audit trail, …"
- „Disable Unified Auditing and using Standard Auditing instead."

© 2016 CarajanDB GmbH

12c Auditing – Audit Daten archivieren

- Archivierung
  - nur manuell mit anschließendem löschen
    - Data Pump Export
    - Tabelle erstellen

```
INSERT INTO table SELECT ... FROM UNIFIED_AUDIT_TRAIL ...;
INSERT INTO table SELECT ... FROM SYS.AUD$ ...;
INSERT INTO table SELECT ... FROM SYS.FGA_LOG$ ...;
```

- Alternativ: Oracle Audit Vault and Database Firewall
  - Audit Daten von der Source zum Audit Vault Server verschieben

© 2016 CarajanDB GmbH

12c Auditing - Abschluss

- Planung
  - Ziele und Vorgaben?
    - Welche Ziele und Vorgaben will oder muss ich eigentlich erfüllen?
  - Datenschutz?
    - Darf ich im gewünschten Umfang überhaupt auditieren?
  - Kosten?
    - Habe ich genug Performance und Speicher?
  - Auswertung?
    - Wer wertet die auditierten Daten aus?
  - Archivierung?
    - Was passiert mit „alten“ Audit Daten?

© 2016 CarajanDB GmbH

12 Auditing – Praxis

- Auditing nur selektiv einschalten!
  - Nur das auditieren, was auch ausgewertet werden muss.
- Überwachung nicht vergessen!
  - Audit Daten auswerten und auf deren Größe achten.

© 2016 CarajanDB GmbH

Vielen Dank!

- Zeit für Ihre Fragen.

- Kontakt

Sebastian Winkler

CarajanDB GmbH
Siemensstraße 25
50374 Erftstadt

E-Mail: sebastian.winkler@carajandb.com
Fon: +49 2235 170 91 86
Mobil: +49 175 864 90 61
Twitter: sjw1011
Blog: www.carajandb.com/blogs/blog-swinkler

© 2016 CarajanDB GmbH