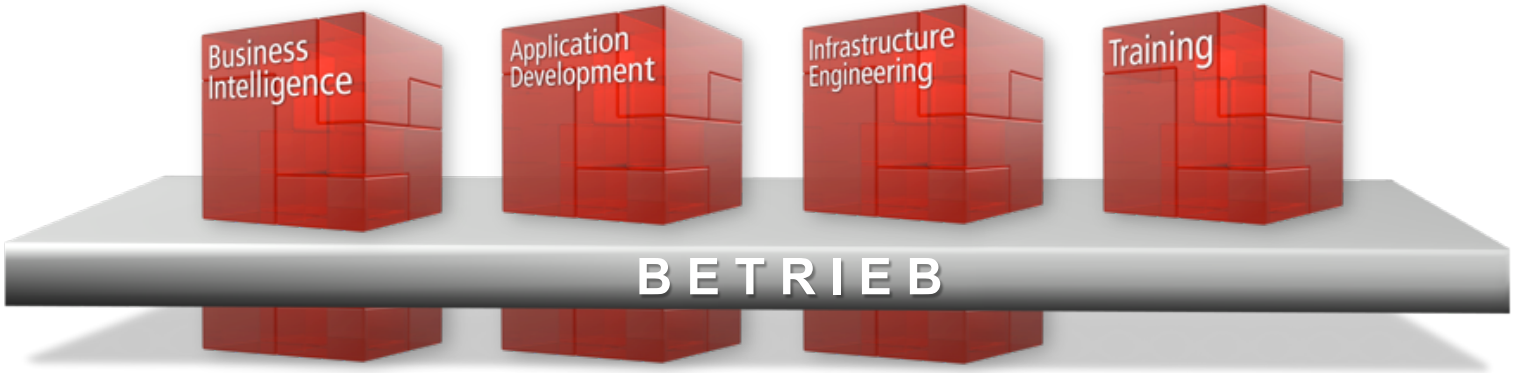
Oracle Unified Auditing

Migration der Audit-Konfiguration

Stefan Oehrli

Unser Unternehmen.

Trivadis ist führend bei der IT-Beratung, der Systemintegration, dem Solution Engineering und der Erbringung von IT-Services mit Fokussierung auf ORACLE - und Microsoft -Technologien in der Schweiz, Deutschland, Österreich und Dänemark. Trivadis erbringt ihre Leistungen aus den strategischen Geschäftsfeldern:



Trivadis Services übernimmt den korrespondierenden Betrieb Ihrer IT Systeme.

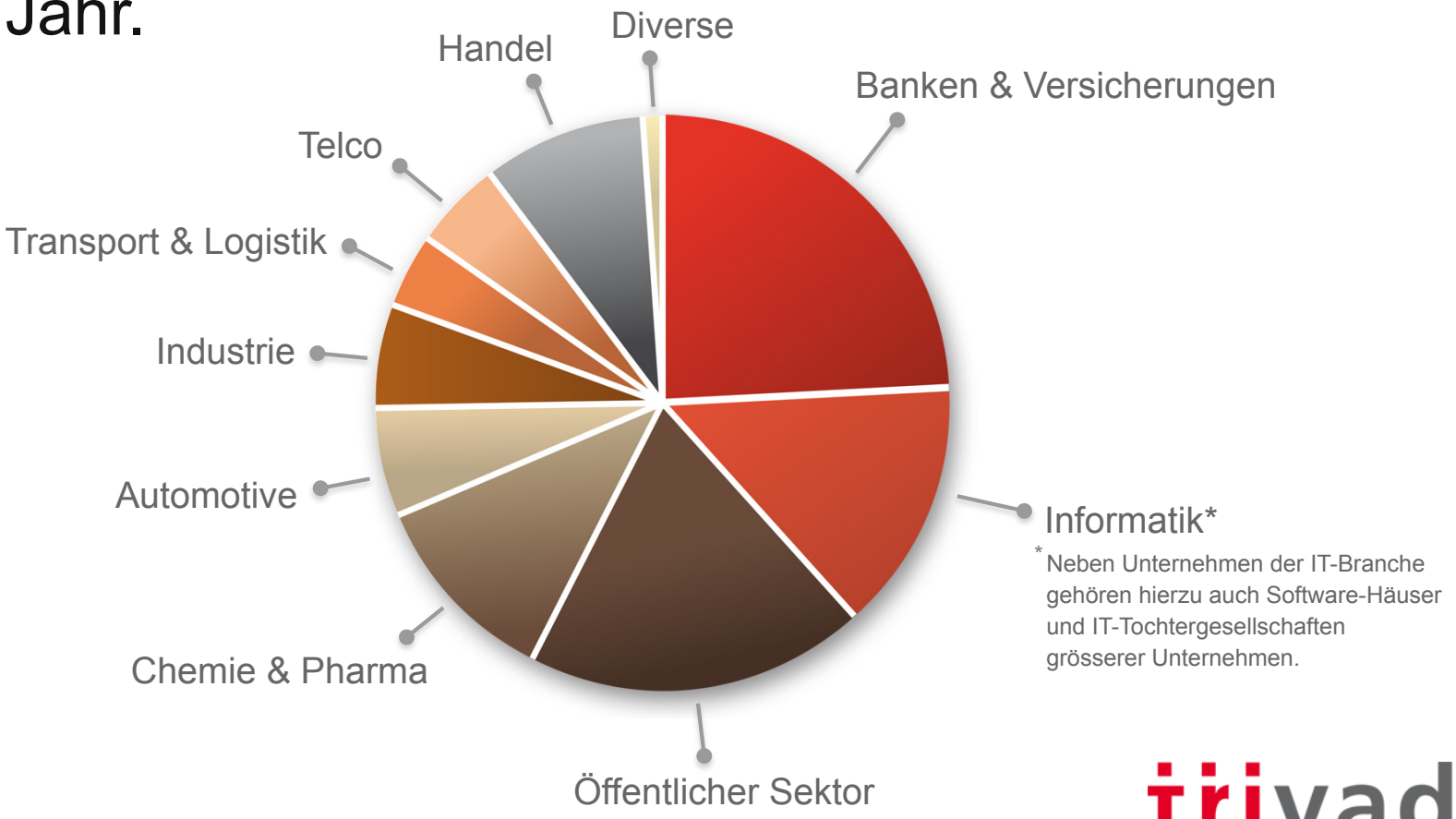
trivadis
makes IT easier.

Mit über 600 IT- und Fachexperten bei Ihnen vor Ort.

- 14 Trivadis Niederlassungen mit über 600 Mitarbeitenden.
- Über 200 Service Level Agreements.
- Mehr als 4'000 Trainingsteilnehmer.
- Forschungs- und Entwicklungs-budget: CHF 5.0 Mio. / EUR 4.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

trivadis
makes IT easier.

Unsere Fachkompetenz aus über 1'900 Projekten pro Jahr.



* Neben Unternehmen der IT-Branche gehören hierzu auch Software-Häuser und IT-Tochtergesellschaften grösserer Unternehmen.

trivadis
makes IT easier.

Stefan Oehrli

Solution Manager BDS SEC

- Seit 1997 IT-Bereich tätig
- Seit 2008 bei der Trivadis AG
- Seit 2010 Disziplin Manager SEC INFR
- Seit 2014 Solution Manager BDS Security

IT Erfahrung

- DB Administration und DB Security Lösungen
- Administration komplexer, heterogenen Umgebungen
- Datenbank Teamleiter

Spezialgebiet

- Datenbank Sicherheit Security und Betrieb
- Security Konzepte
- Security Reviews
- Oracle Backup & Recovery

Skills

- Backup & Recovery
- Oracle Advanced Security
- Audit Vault und Database Firewall, Database Vault
- Team / Projekt Management

trivadis makes IT easier.

trivadis
makes IT easier.

Agenda

1. Einleitung
2. Übersicht Unified Audit
3. Konfiguration und Verantwortlichkeiten
4. Audit Policies
5. Mixed Mode
6. Migrationsarbeiten
7. Unified Mode
8. Weitere Überlegungen
9. Fazit

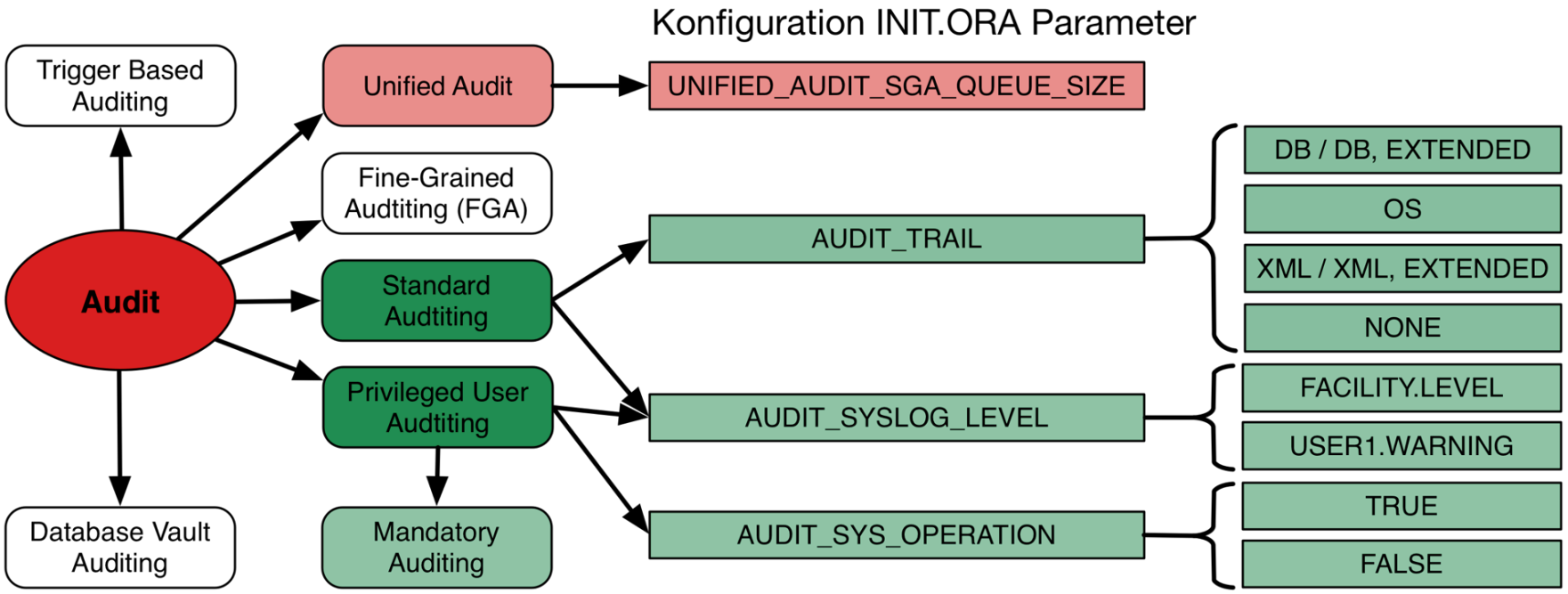
trivadis
makes IT easier.

Einleitung

- Audit relevante Informationen werden an unterschiedlichen Orte abgelegt
  - Keine Übersicht über die vorhanden Informationen
- Oracle 12c bringt einen neuen Audit Trail und Audit Kommandos
  - UNIFIED_AUDIT_TRAIL als einziger Audit Trail für alle Audit Daten
  - Ersetzt SYS.AUD$, SYS.FGA_LOGS$, DVSYS.AUDIT_TRAIL$, OS Audit Daten in adump, etc.
- Auditing ist immer eingeschaltet
  - Es werden Init.ora Parameter mehr benötigt
  - Kein Restart der Datenbank (ehm. Einmal schon für‘s relinken ☺)

trivadis makes IT easier.

Einleitung



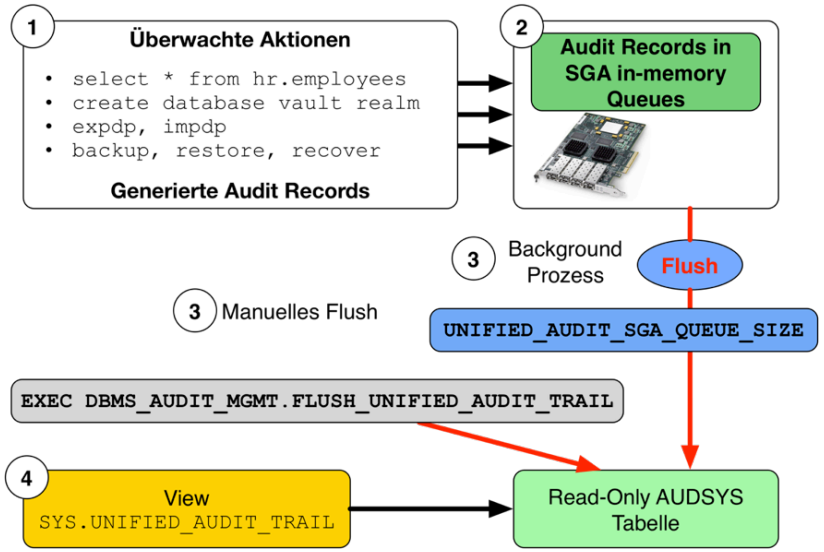
trivadis makes IT easier.

Übersicht Unified Audit

- Standardmässiges Auditing der Audit Konfiguration
  - Protokolieren jedes Events der die Audit Konfiguration modifiziert
  - Protokolieren jeder Modifikation des Audit Trails und der Einstellungen
- Schnelle Audit Engine, einfachere Kontrolle des Zugriffes, verbesserte Performance
  - Minimale Mehrbelastung bei der Verarbeitung (Audit Datensätze werden in einem Proprietären Format abgespeichert)
  - Minimale Mehrbelastung bei Transaktionen (Audit Datensätze werden in ein Buffer geschrieben)

trivadis
makes IT easier.

Übersicht Unified Audit – Fast Audit Engine

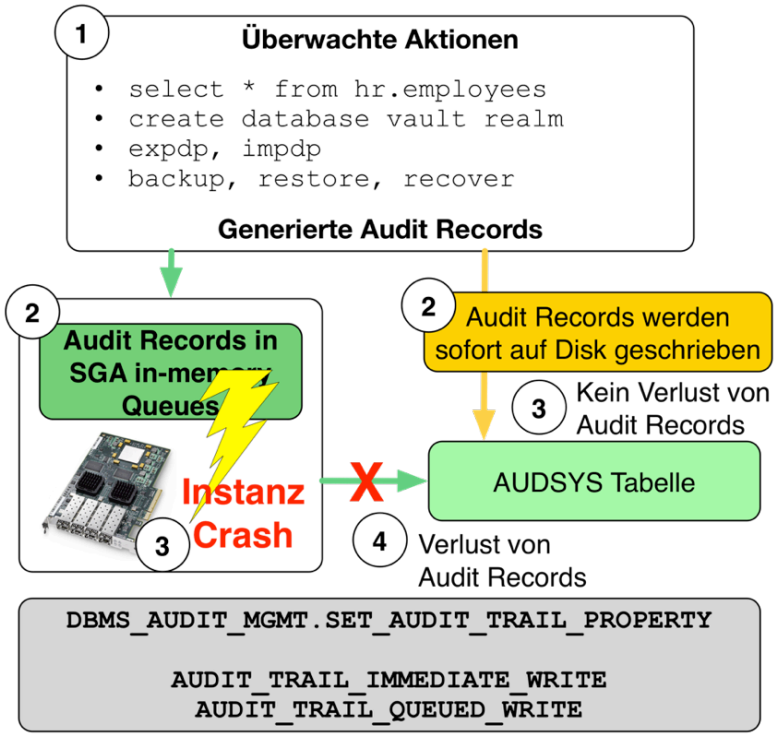


- **Queued** Mode
  - Standard Einstellung
  - Audit Datensätze werden in der SGA zwischen gespeichert
  - Konfigurierbar mit UNIFIED_AUDIT_SGA_QUEUE_SIZE (1MB bis 30MB)
- **Immediate** Mode
  - Audit Datensätze werden direkt in den Audit Trail geschrieben

trivadis makes IT easier.

Übersicht Unified Audit – Ups...

- Audit Datenverlust seit dem letzten Flush auf Disk
- Alternative bleibt der Immediate Write Mode
- Verhalten im Queued wird durch INIT.ORA Parameter gesteuert
  - `unified_audit_sga_queue_size`
  - `_unified_audit_flush_interval`
  - `_unified_audit_flush_threshold`



trivadis makes IT easier.

Übersicht Unified Audit

- Der Unified Audit Trail speichert auch Audit Informationen für:
  - Fine Grained Audit (FGA)
  - Data Pump
  - Oracle RMAN
  - Oracle Label Security (OLS)
  - Oracle Database Vault (DV)
  - Real Application Security (RAS)
- Verwenden von dedizierten Spalten
- Komponenten wie DataPump sind explizit mit einer Audit Policy zu definieren

trivadis makes IT easier.

Übersicht Unified Audit

- Auditing für Oracle Database Vault (DV)
  - Wird durch das DV Framework definiert
  - Änderungen an der DV Konfiguration werden auditiert
  - DV Verstösse werden mit DV Realm definiert etc.
- RMAN Operationen werden standardmässig überwacht
  - Erfolgreiche RMAN Backup‘s
  - Erfolgreiche RMAN Restores
  - List und Report Statements
  - Aber nicht alles … z.B. delete archivelog all;

trivadis
makes IT easier.

Übersicht Unified Audit

- Verwenden von dedizierten Spalten
  - RMAN_OPERATION, RMAN_OBJECT_TYPE, RMAN_DEVICE_TYPE
  - DP_TEXT_PARAMETERS1, DP_BOOLEAN_PARAMETERS1

```
SELECT event_timestamp, dbusername, rman_operation,
       rman_object_type, rman_device_type
  FROM unified_audit_trail
  WHERE action_name = 'RMAN ACTION'
  ORDER BY event_timestamp
```


trivadis makes IT easier.

Konfiguration und Verantwortlichkeiten

- INIT.ORA Parameter
- PL/SQL Package DBMS_AUDIT_MGMT

```
SELECT parameter_name,parameter_value,audit_trail
 FROM dba_audit_mgmt_config_params
 WHERE audit_trail='UNIFIED AUDIT TRAIL';

Name                    Value
-------------------- ------------------
AUDIT FILE MAX SIZE  10000
AUDIT FILE MAX AGE   5
DB AUDIT TABLESPACE  SYSAUX
AUDIT WRITE MODE     QUEUED WRITE MODE
```

trivadis makes IT easier.

Konfiguration und Verantwortlichkeiten

- DBA
  - Legt das Tablespace für die Audit Daten an
- AUDIT_ADMIN
  - Verwaltet die Audit Policies und definiert das Auditing
  - Verwaltet die Aufbewahrungsdauer der Audit Daten und ist verantwortlich für das Housekeeping

```
CREATE AUDIT POLICY ...
AUDIT POLICY ...
EXEC dbms_fga ...
EXEC dbms_audit_mgmt.move_dbaudit_tables
EXEC dbms_audit_mgmt.init_cleanup
```


trivadis makes IT easier.

Konfiguration und Verantwortlichkeiten

- AUDIT_VIEWER
  - Auswertung der Audit Daten

UNIFIED_AUDIT_TRAIL

SESSIONID	DBUSERNAME	ACTION_NAME
3493454563	HR	SELECT
2592425735	SYS	CREATE DIRECTORY
2359386095	SYS	CREATE AUDIT POLICY
2592425735	SYS	GRANT
2359386095	SYS	AUDIT

- Best Practice
  - Erstellen von dezidierten Benutzern mit den entsprechenden Rollen

```
GRANT audit_admin TO auditor_oehrli
GRANT audit_viewer TO auditor_meier
```


trivadis makes IT easier.

Audit Policies

- Audit Policies sind Container für Audit Einstellungen
  - Verwendet um ACTIONS, PRIVILEGES, OBJECTS zu Auditiren
  - Basieren auf Systemweiten oder Objekt Spezifischen Audit Optionen
  - Können direkt Rollen enthalten
  - Können Bedingungen, Ausnahmen enthalten
  - Werden mit dem Statement AUDIT und NOAUDIT Ein- bzw. Ausgeschaltet
- Bedingungen können aktuell nur Oracle Funktionen enthalten. Kundenspezifische PL/SQL Funktionen werden nicht unterstütz
- Audit Daten werden immer in den UNIFIED_AUDIT_TRAIL geschrieben

trivadis makes IT easier.

Audit Policies

- Erstellen einer Audit Policy mit Bedingung und Ausnahme

```
CREATE AUDIT POLICY dba_pol ROLE DBA;
CREATE AUDIT POLICY hr_employees_pol
  PRIVILEGES CREATE TABLE
  ACTIONS UPDATE ON HR.EMPLOYEES
  WHEN q'[SYS_CONTEXT('USERENV',
         'IDENTIFICATION_TYPE'='EXTERNAL']'
  EVALUATE PER STATEMENT;
```

- Aktivieren einer Audit Policy

```
AUDIT POLICY hr_employees_pol EXCEPT HR;
```


trivadis makes IT easier.

Audit Policies

- Aktive Audit Policies

```
SQL> SELECT * FROM audit_unified_enabled_policies;

USER_NAME    POLICY_NAME        ENABLED_ SUC FAI
----------- ------------------ -------- --- ---
SCOTT_DBA    ORA_ACCOUNT_MGMT   BY       YES YES
ALL USERS    ORA_SECURECONFIG   BY       YES YES
```


trivadis makes IT easier.

Audit Policies – Default Policies

- ORA_SECURECONFIG (aktiv)
  - Überwachung der Audit Konfiguration und des Audit Trails
- ORA_LOGON_FAILURES (aktiv)
  - Überwachung von Logon/Logoff
- ORA_ACCOUNT_MGMT
  - Erstellen von Benutzer und Rollen und Vergabe von Rechten
- ORA_DATABASE_PARAMETER
  - Änderung der Datenbank Parameter beziehungsweise SPFile
- Je nach Oracle 12c Release weitere Default Policies

trivadis makes IT easier.

Mixed Mode

- Standard bei Neuinstallationen
- Traditionelles und Unified Audit zusammen (Mixed Mode)
  - Traditionelles Audit (pre 12c) funktioniert weiterhin in 12c
  - All Audit Einstellungen die in 11g R2 Konfiguriert wurden bleiben
- Spezielle Unified Audit Feature funktionieren nicht
  - Z.B kein RMAN Audit
- Aktive Audit Policies schreiben Daten in UNIFIED_AUDIT_TRAIL
  - Gefahr der doppelten Datensammlung
  - z.B. AUDIT CREATE SESSION und ORA_LOGON_FAILURES

trivadis makes IT easier.

Migrationsarbeiten

- Gute Gelegenheit für die Definition eines „Audit Konzeptes“
  - Was soll überwacht werden?
  - Wie lange sollen die Rohdaten aufbewahrt werden?
  - Wer wertet die Audit Daten aus?
- Analyse der bestehenden Audit Konfiguration
  - Wird SYSLOG verwendet?
  - Welcher AUDIT_TRAIL wird verwendet
  - Kundenspezifisches Housekeeping und/oder Trigger basiertes Audit

trivadis
makes IT easier.

Migrationsarbeiten

- Analyse der bestehenden Audit Statements
  - Ältere MOS Note 1019552.6 Script to Show Audit Options/Audit Trail
  - Auswerten der Informationen aus DBA_PRIV_AUDIT_OPTS, DBA_OBJ_AUDIT_OPTS, DBA_STMT_AUDIT_OPTS, etc
- Erstellen neuer Audit Policies
  - Abdecken der Bestehenden Bedürfnisse
  - Ggf. direkt Rollen überwachen. Z.B die DBA Rolle
- Neue Audit Policies verifizieren
  - Wird alles wie gewünscht überwacht?
  - Achtung doppelte Datensammlung

trivadis makes IT easier.

Unified Mode

- Aktivieren den Unified Audit Mode benötig Neustart der Datenbank
- Option wird in die Binaries „gelinkt“
  - Siehe auch MOS Note 1567006.1

```
cd $ORACLE_HOME/rdbms/lib
make -f ins_rdbms.mk uniaud_on ioracle
```

- Kontrolle der Unified Audit Option

```
SELECT parameter,value FROM v$option
WHERE parameter='Unified Auditing';
PARAMETER           Value
------------------- ---------
Unified Auditing    TRUE
```

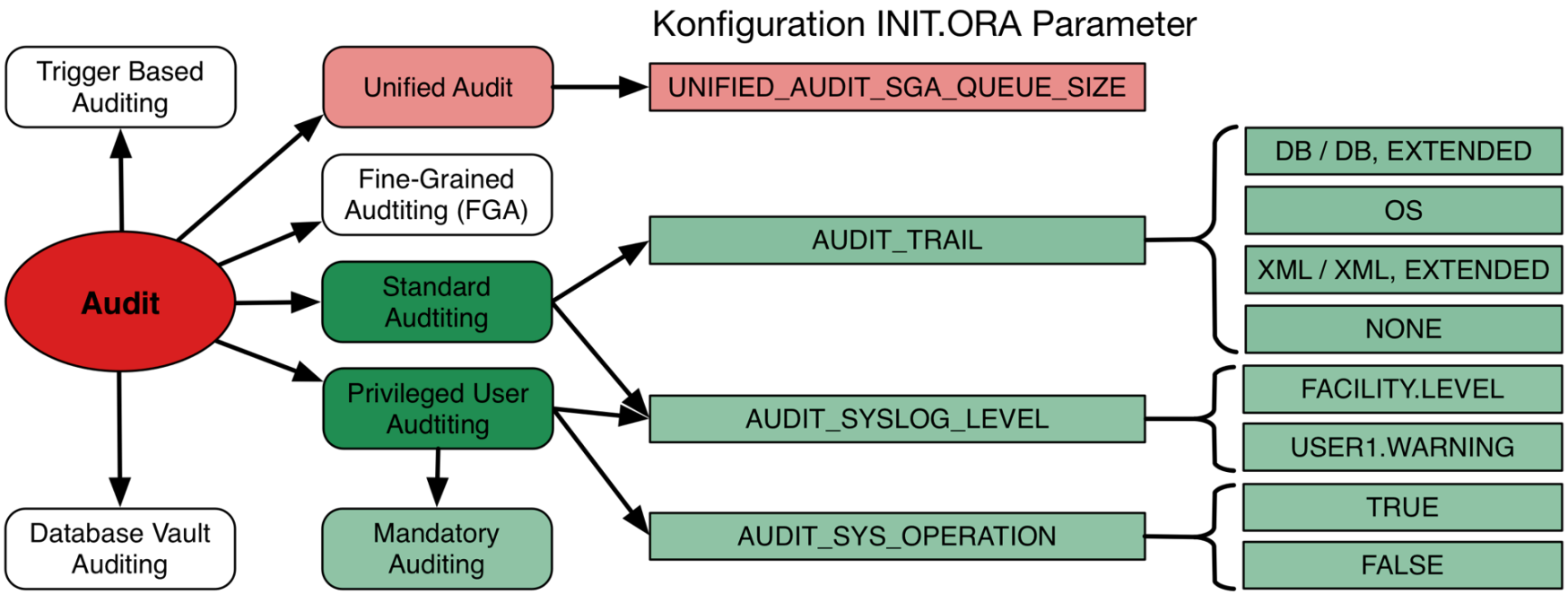

trivadis makes IT easier.

Unified Mode

- Aktivieren der neue Audit Policies
- Anpassen des Housekeeping mit DBMS_AUDIT_MGMT
  - Definition von Purge Jobs
- Bereinigung der altern Audit Statements
  - Löschen bzw. NOAUDIT xyz

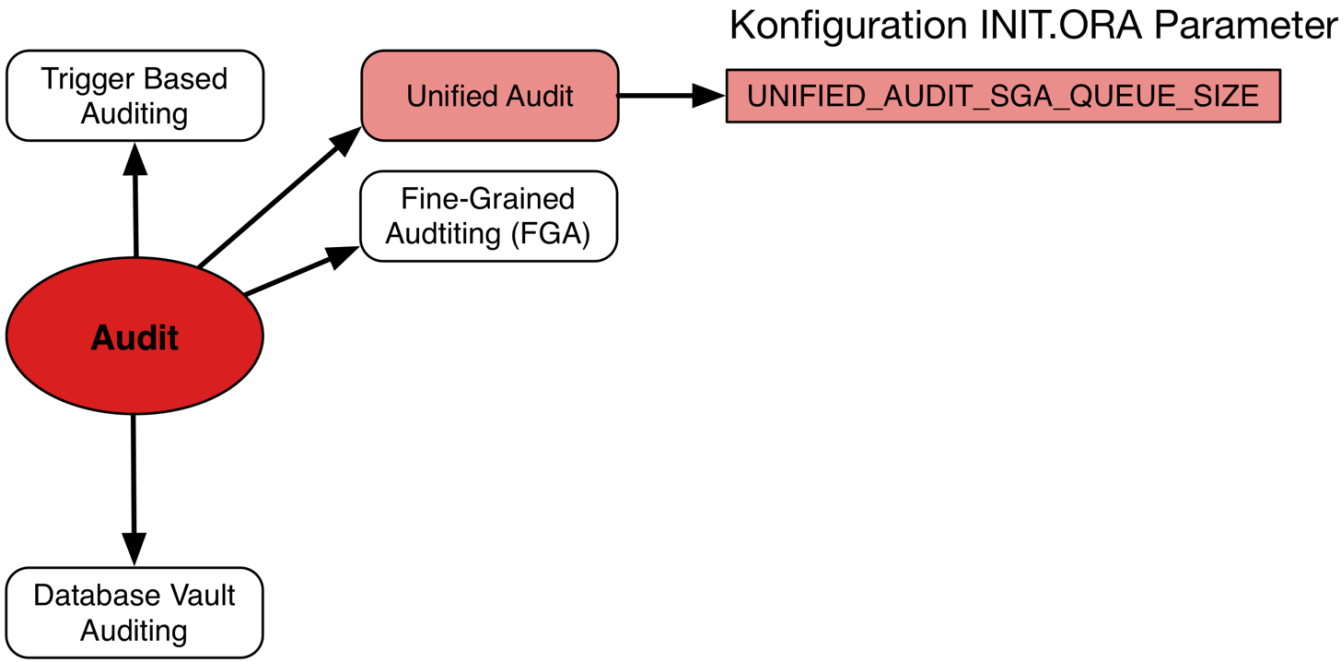
trivadis
makes IT easier.

Unified Mode



trivadis makes IT easier.

Unified Mode



trivadis makes IT easier.

Weitere Überlegungen – Manipulation der Audit Daten

- Unified Audit ist Teil des Oracle Kernels
  - Ausschalten benötigt ein Relink und ein DB Restart
  - Verwendung von andern Oracle Binaries zur Laufzeit z.B. um SQLPlus auszuführen, führen zu Fehlern und ORA-00600
  - Nach einem Relink mit uniaud_off ist Audit nicht ganz ausgeschaltet
- SGA Buffer kann Manipuliert werden
  - Immediate Mode verwenden um das Risiko zu minimieren
- ORADEBUG Statements werden standardmässig überwacht

trivadis makes IT easier.

Weitere Überlegungen – Manipulation der Audit Daten

- Mit oradebug SYS Audit oder Standard Audit ausschalten

```
SQL> oradebug setmypid
Statement processed.
SQL> oradebug dumpvar sga kzaflg
ub2 kzaflg_ [0600340E0, 0600340E4) = 00000001
SQL> oradebug setvar sga kzaflg_ 0
BEFORE: [0600340E0, 0600340E4) = 00000001
AFTER:  [0600340E0, 0600340E4) = 00000000
```

- Oder wieder einschalten

```
SQL> oradebug setvar sga kzaflg_ 1
BEFORE: [0600340E0, 0600340E4) = 00000000
AFTER:  [0600340E0, 0600340E4) = 00000001
```


trivadis makes IT easier.

Weitere Überlegungen – Standby / Read Only

- Unified Audit funktioniert auch bei:
  - Standby Datenbanken
  - Read only Datenbanken
- Unified Audit verwendet $ORACLE_BASE/audit um Binär Dateien anzulegen, wenn die DB nicht geöffnet oder schreibbar ist
  - Transparenter Zugriff durch den UNIFIED_AUDIT_TRAIL View
  - Dateien können mit DBMS_AUDIT_MGMT.LOAD_UNIFIED_AUDIT_FILES in die Datenbank geladen werden
  - Housekeeping mit DBMS_AUDIT_MGMT funktioniert auch für die Binär Dateien

trivadis
makes IT easier.

Weitere Überlegungen

- Unterstützung von Oracle Audit Vault und Database Firewall (AVDF)
  - Neuer Audit Trail wird gelesen / gesammelt
  - Neue Attribute werden z.Z noch nicht unterstützt
  - Keine zentrale Verwaltung der Audit Policies
  - Neuer Release 12.2 von AVDF geplant
- Neue Oracle 12c Release bringen teilweise neue Default Audit Policies
  - Verhalten kann sich ggf. ändern
- Vereinzelte Bugs bezüglich Unified Audit vorhanden

trivadis
makes IT easier.

Fazit

- Unified Audit Trail bietet bezüglich Administration, Sicherheit und Performance wesentliche Verbesserungen
- Auswertung erfolgt nur noch an einer Stelle
- Neue Audit Policies erlauben das einfach Zusammenfassen der Audit Bedingungen
- Mixed Mode bietet genügend Zeit für ein Review der bestehenden Audit Anforderungen

trivadis
makes IT easier.

Fragen und Antworten...

Stefan Oehrli
Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55
stefan.oehrli@trivadis.com

trivadis
makes IT easier.