Audit Vault – Erfahrungen aus der ersten deutschen Produktivumgebung?

Referent:
Volker Mach, Fachbereichsleiter RSS, MT AG, Ratingen

managing technology

MT AG Key Facts

MT AG MANAGING TECHNOLOGY – ENABLING THE ADAPTIVE ENTERPRISE

- Gründung 1994
- Inhabergeführte AG:
  Aktienkapital 1.500.000 €
- Hauptsitz Ratingen;
  Niederlassung Dortmund
- Mitarbeiter:
  > 200 Festangestellte
  > 65 Freie Mitarbeiter

- Full-Service-Dienstleistung für alle Phasen des Software-Lifecycle
- Herstellerunabhängige Expertise in den marktführenden Technologien wie Oracle, IBM, Microsoft, SAP und OpenSource
- Themen- und Lösungs-Know-how in den Kerndisziplinen des Adaptive Enterprise

AGENDA

- Definition Audit
- Projektanforderung
- Voraussetzungen für den Einsatz
- Oracle Audit Vault
- Organisatorische Rollen
- Methoden
- Skalierung
- Auswertung
- Bereinigung auf den Quellsystemen
- Fragen & Antworten

Definition Audit

„Audit; von lateinisch audit: „er/sie hört"; sinngemäß: „er/sie überprüft"; werden in der Informationstechnik (IT) Maßnahmen zur Risiko- und Schwachstellenanalyse (engl. Vulnerability Scan) eines IT-Systems oder Computerprogramms bezeichnet.

(Quelle: http://de.wikipedia.org/wiki/IT-Sicherheitsaudit)“

Projektanforderung

- Protokollierung aller administrativen Aktivitäten der relevanten Datenbanken
- Personalisierter Zugang der Datenbankadministratoren auf Betriebssystemebene
- Audit-Daten dürfen nicht mehr verändert oder gelöscht werden
- Regelmäßige interne Kontrolle
- Auswertungsmöglichkeit
- Sichere Aufbewahrung

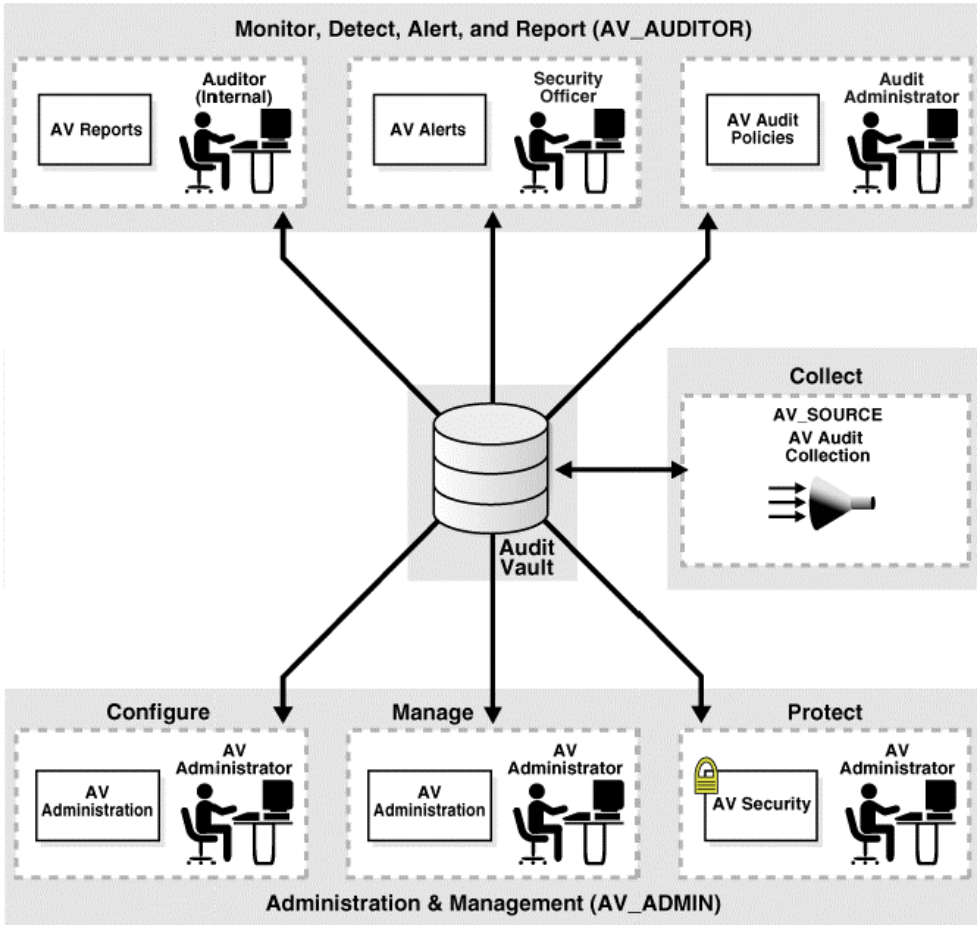
Voraussetzung für den Einsatz

- Personalisierte Zugänge auf Betriebssystemebene
  - Administrative Tätigkeiten sollen mit dem SUDO – Recht ausgeführt werden
- Organisatorische Trennung der Rollen

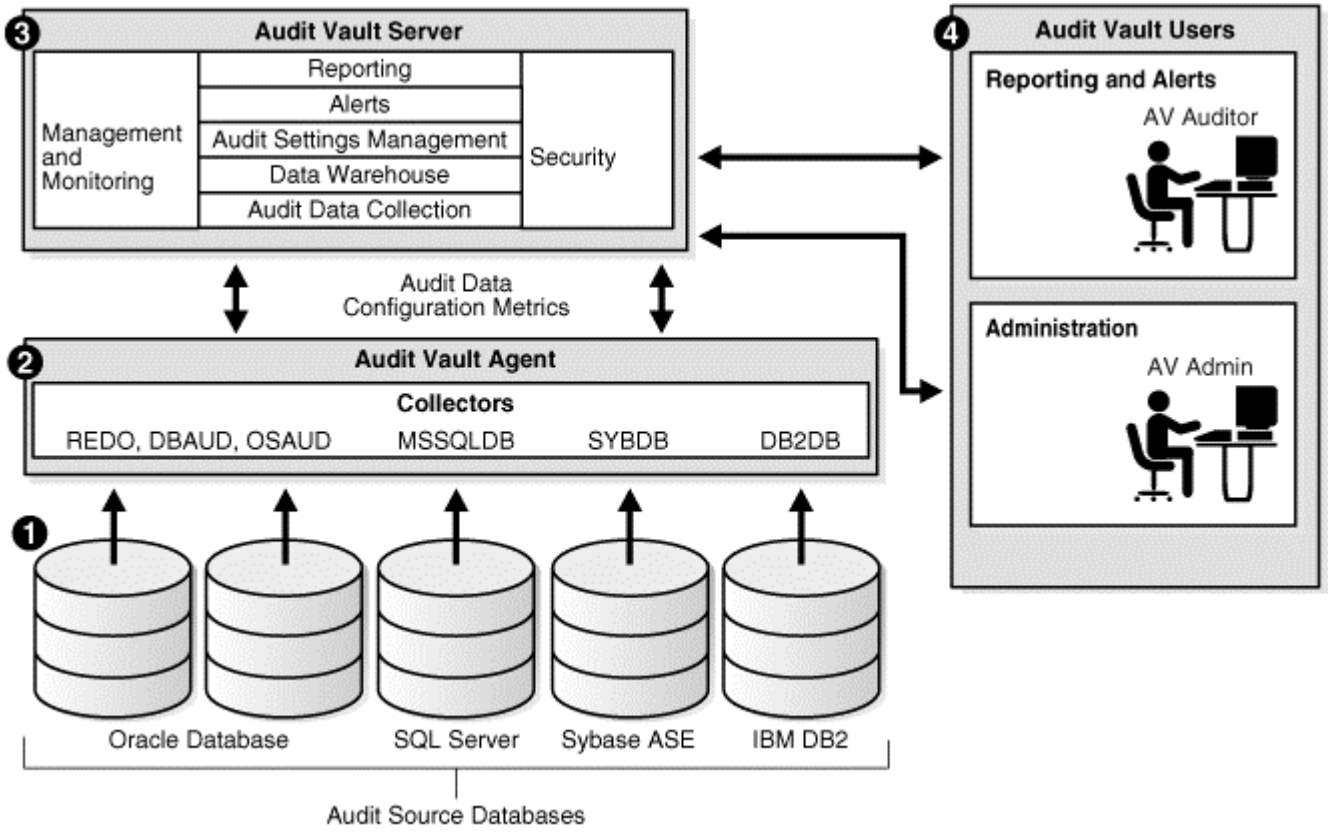
- Produktion darf nicht gefährdet sein, notfalls in Absprache mit der Revision

  Deaktivierung von Audit Vault
- Daten dürfen nicht ausgewertet oder Zweckentfremdet werden

Oracle Audit Vault (1)



Oracle Audit Vault (2)



Organisatorische Rollen

- Wer erstellt die Regeln und darf diese ändern?
  - Administration & Revision
- Wer wertet die Audit-Files aus?
  - Administration & Revision
- Wer entscheidet ob das Audit abgeschaltet werden kann ?
  - Nur in Absprache und Genehmigung durch die Revision

Methoden

- Auditing von Benutzer mit dem Privileg SYSDBA
  - Audit_sys_operations
- DDL
  - Änderung an den relevanten Tabellen
  - Benutzer- und Rollenmanagement
- DML
  - Lese- und Schreibzugriffe auf den relevanten Tabellen
- Audit Trail
  - XML, EXTENDED (ab 10g)
- Audit Vault Agent
  - OS Collector

Datenmenge

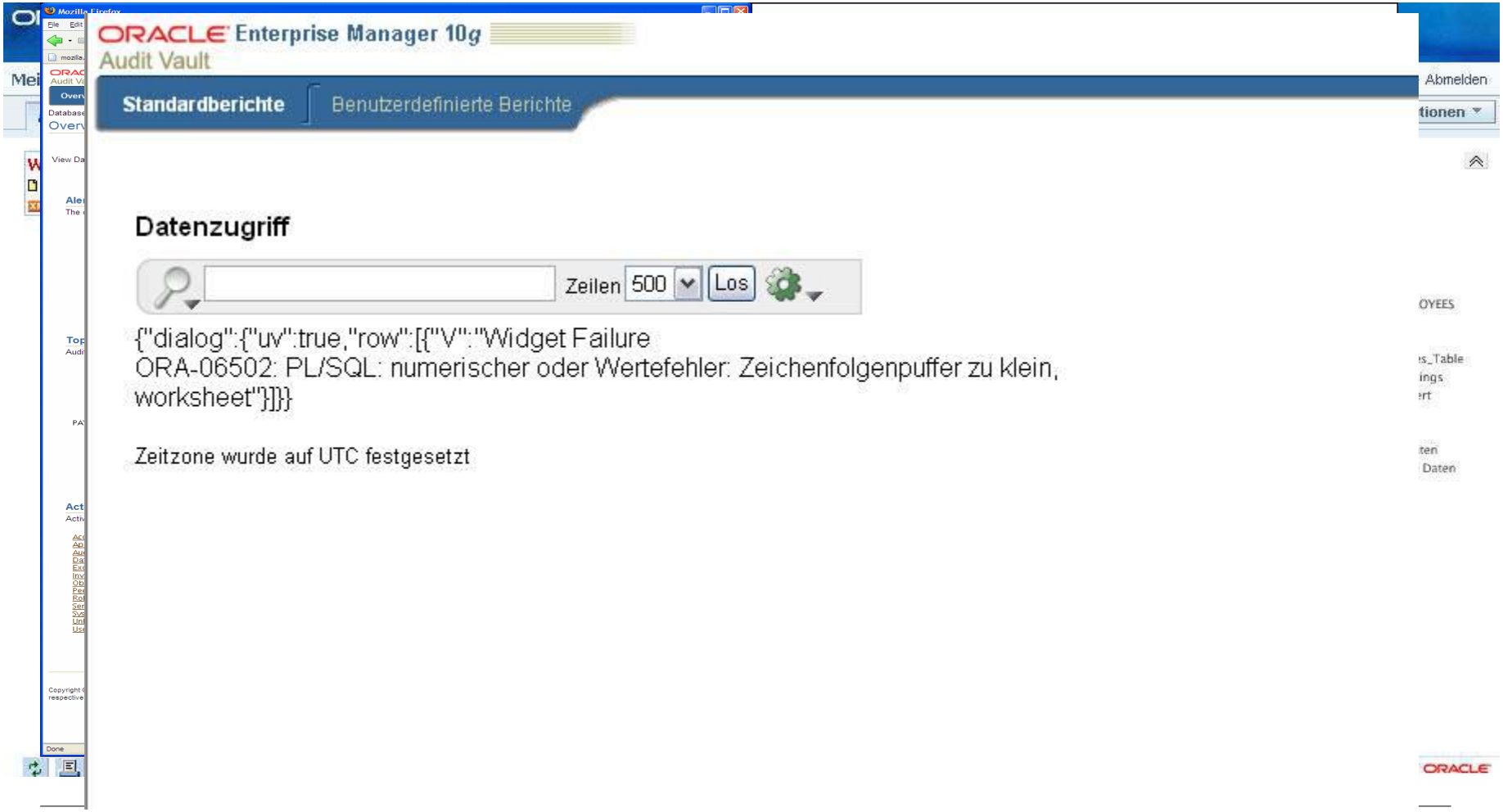
- Fine Grained Auditing

```
begin
dbms_fga.add_policy (
object_schema=>'BANK',
object_name=>'ACCOUNTS',
policy_name=>'ACCOUNTS_ACCESS',
audit_column => 'BALANCE',
audit_condition =>'User=„DBA_Mustermann“,
statement_types => 'UPDATE, DELETE, SELECT',
audit_trail => DBMS_FGA.XML + DBMS_FGA.EXTENDED);
end;
```

Skalierung

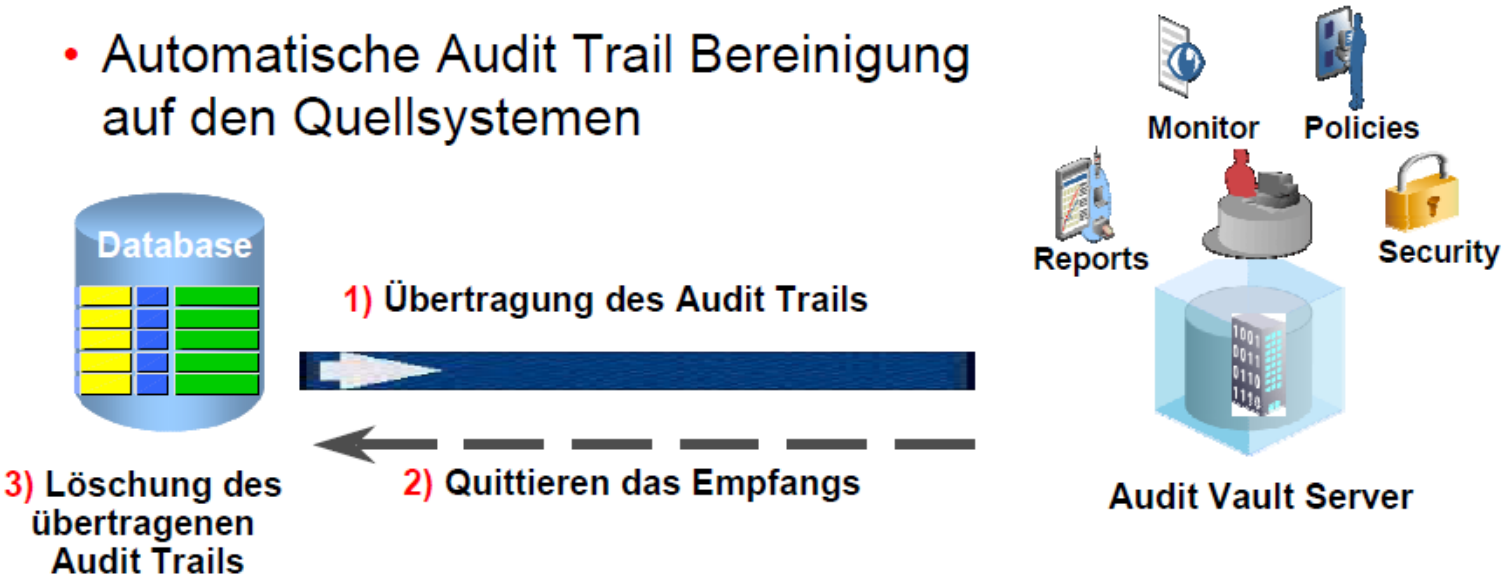
- Sun Solaris Server
  - Produktion
  - Integration
  - Test
- Hochverfügbar
  - Hardware Cluster
  - RAC
- Datenmenge
  - Durchschnittlicher Audit-Eintrag in Stage-Tabelle ca. 700 – 1.200 Bytes
  - Durchschnittlicher Audit-Eintrag in Star-Schema ca. 1,5 Fache von Stage
- Hohe CPU – Last nur bei täglichem Verdichtungsjob im DW

Auswertung


ORACLE Enterprise Manager 10g
Audit Vault
Standardberichte
Benutzerdefinierte Berichte
Datenzugriff
Zeilen 500 Los
{"dialog":{"uv":true,"row":[{"V":"Widget Failure
ORA-06502: PL/SQL: numerischer oder Wertefehler: Zeichenfolgenpuffer zu klein,
worksheet"}]}}
Zeitzone wurde auf UTC festgesetzt

Bereinigung auf den Quellsystemen

- Automatische Audit Trail Bereinigung auf den Quellsystemen



- Patch erforderlich für 10.2.0.3, 10.2.0.4, & 11.1.0.6
- Enthalten in 10.2.0.5+ & 11.1.0.7

Vielen Dank!

?!

MT AG managing technology I Balcke-Dürr-Alle 9 I 40882 Ratingen
Tel. +49 (0) 2102 309 61-0 I info@mt-ag.com I www.mt-ag.com

managing technology

MT AG – Vorträge auf der DOAG

ORACLE Platinum Partner

MT AG MANAGING TECHNOLOGY – ENABLING THE ADAPTIVE ENTERPRISE

Di. 16. Nov.	10:00 – 10:45	Clevere Web-Formulare mit APEX und jQuery	Andreas Wismann
Di. 16. Nov.	13:00 – 13:45	Oracle RMAN – beim Recovery das Disaster erleben?	Volker Mach
Di. 16. Nov.	13:00 – 13:45	Rollout Prozess für APEX Anwendungen	Oliver Lemm
Mi. 17. Nov.	13:00 – 13:45	Audit Vault - Erfahrungen aus der ersten deutschen Produktivumgebung	Volker Mach
Do. 18. Nov.	13:00 – 13:45	Das APEX Migrationsprojekt bei der Union Investment	Niels de Bruijn
Do. 18. Nov.	16:00 – 16:45	BPEL und Transaktionen	Arne Platzen Guido Neander
Stand-by		Rich-Internet-Applications mit jQuery und dem APEX Listener	Klaus Friemelt