Oracle Audit in a Nutshell - Database Audit but how?

DOAG + SOUG Security-Lounge

Stefan Oehrli
Senior Consultant
Discipline Manager
Trivadis AG

Basel 24. April 2012

trivadis
makes IT easier.

Trivadis facts & figures

11 Trivadis locations with more than 600 employees

Financially independent and sustainably profitable

Key figures 2011

- Revenue CHF 104 / EUR 84 Mio.
- Services for more than 800 clients in over 1,900 projects
- 200 Service Level Agreements
- More than 4,000 training participants
- Research and development budget: CHF 5.0 / EUR 4 Mio.

trivadis
makes IT easier.

Why we are special

Customer-specific solution competence and vendor independence	▪ offers substantiated techniques and skills as well as self-developed approaches ▪ guarantees repeatable quality and a safe execution
Technology competence	▪ offers more than 18 years of expertise in Oracle and Microsoft ▪ has its own Technology Center and strives for technological excellence
Solution and integration expertise	▪ has a wide and cross-sectorial customer basis and more than 1900 projects every year spanning a broad range of goals, complexity and corresponding framework conditions ▪ Combines technological expertise with an understanding of the specific business needs of the client
Support for the entire IT project lifecycle	▪ has a modular portfolio of services for the entire IT project lifecycle ▪ provides the appropriate combination of solutions and services for every „level of maturity“

AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

trivadis
makes IT easier.

Overview

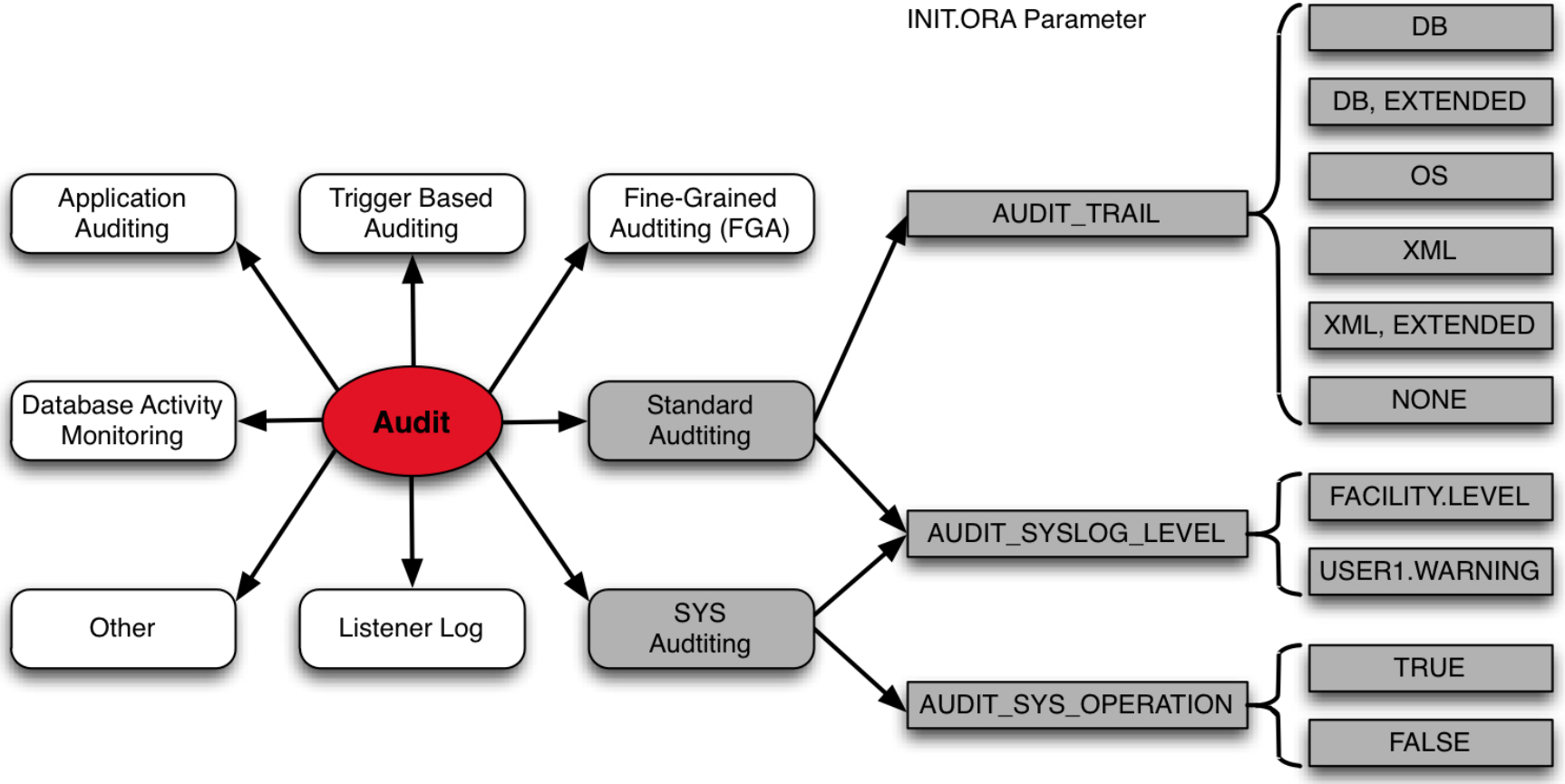
Database audit may be needed for very different reasons.

- General Security Requirements
  - Enable accountability for actions
  - Notify an auditor of actions by an unauthorized user
  - Investigate suspicious activity
  - Detect problems with an authorization or access control implementation
- Compliance Requirements
  - Sarbanes-Oxley Act (SOX)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Basel II
- Monitor Requirements
  - Monitor and gather data about specific database activities
  - E.g. Monitor changes during an update by an vendor

trivadis
makes IT easier.

Overview

Overview of audit facilities



AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

trivadis
makes IT easier.

Oracle audit facilities and options

Oracle standard audit

- Configured by init.ora parameter and audit statements
  - AUDIT_TRAIL defines the audit infrastructure resp *where* to store audit records
  - Audit statement defines *what* to audit
  - Since 11g default AUDIT_TRAIL is DB => *audit is enabled by default!*
  - Set AUDIT_TRAIL OS and AUDIT_SYSLOG_LEVEL to send audit to SYSLOG
- Audit possibilities / statements
  - By statement (CREATE,ALTER,DROP...)
  - By privilege (SELECT ANY, BECOME USER...)
  - Specific for a user (statement , privilege)
  - On objects
  - All statements
- Audit is used to record general database activity

Oracle audit facilities and options

Trigger based auditing

- Triggered at database events
  - Instance problems SERVERERROR
  - Connect, disconnect of sessions LOGON, LOGOFF
  - Start, stop of an instance STARTUP, SHUTDOWN
- Triggered at DML events
  - Get before update values
  - Who did what on a critical table/column
- Audit infrastructure must be developed individually
  - Triggers and table to store audit data
  - Reporting and housekeeping
- Reliability – did I covered all?

Oracle audit facilities and options

Fine grained auditing FGA - Policy-based auditing

- FGA policies are programmatically bound to the object (table, view) by using the DBMS_FGA package
  - WHO has WHEN accessed table HR.EMPLOYEES and list names of all employees with a salary of more than 10000CHF
- Audit of select and DML statements (INSERT, UPDATE, DELETES)
- One policy can be used to audit multiple columns
- There are some limitations
  - Audit records are create as well during a rollback
  - Potential access of sensitive data will cause an audit record as well
  - Updates on sensitive columns to no sensitive columns are not audited
    - Increase salary from 9000CHF to 11000CHF
  - Flashback queries, export, rule based optimizers etc.

Oracle audit facilities and options

SYS auditing – Audit for DBA's

- Standard audit does not cover SYSDBA, SYSOPER
- Available since Oracle 9i Release 2
  - Set through init.ora parameter AUDIT_SYS_OPERATIONS
  - Static parameter / instance restart required
- Audit records are always written to OS even if AUDIT_TRAIL=DB
  - AUDIT_FILE_DEST or AUDIT_SYSLOG_LEVEL
- Certain database-related operations are always reported MOS 308066.1
  - Connections to the instance with administrator privileges SYSOPER/SYSDBA
  - Database startup
  - Database shutdown

Oracle audit facilities and options

Application auditing

- Collect audit information within the application
  - Who logged in
  - Who accessed which object
  - Before / after values
- High integration with application
  - Must be part of the application architecture
  - Audit only what's necessary
  - Included reporting and housekeeping facilities
- Additional effort in application development
  - Will not be easily added at a later time

AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

trivadis
makes IT easier.

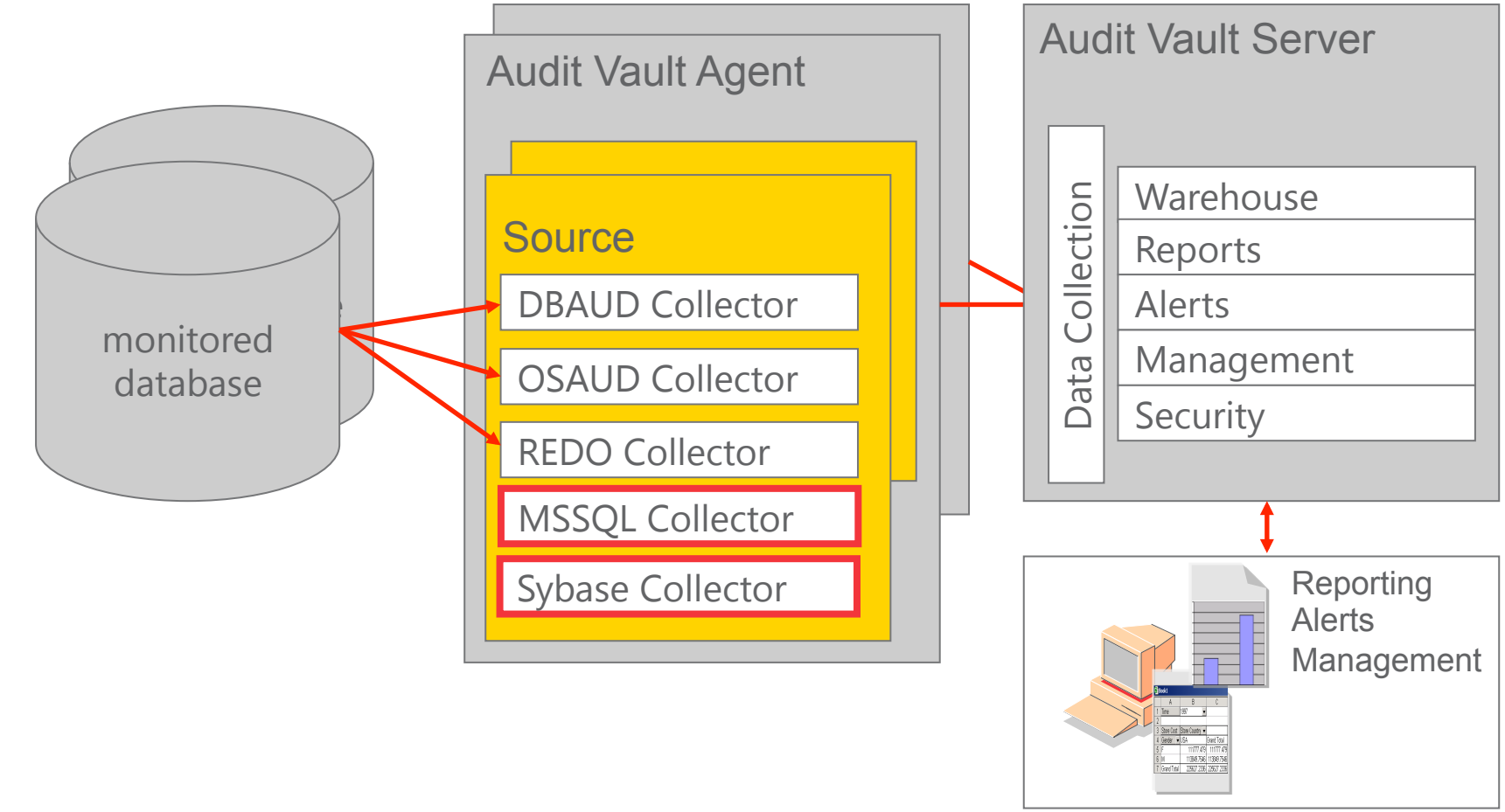
Audit Vault and third party tools

Beside classic audit there are alternatives and extensions available

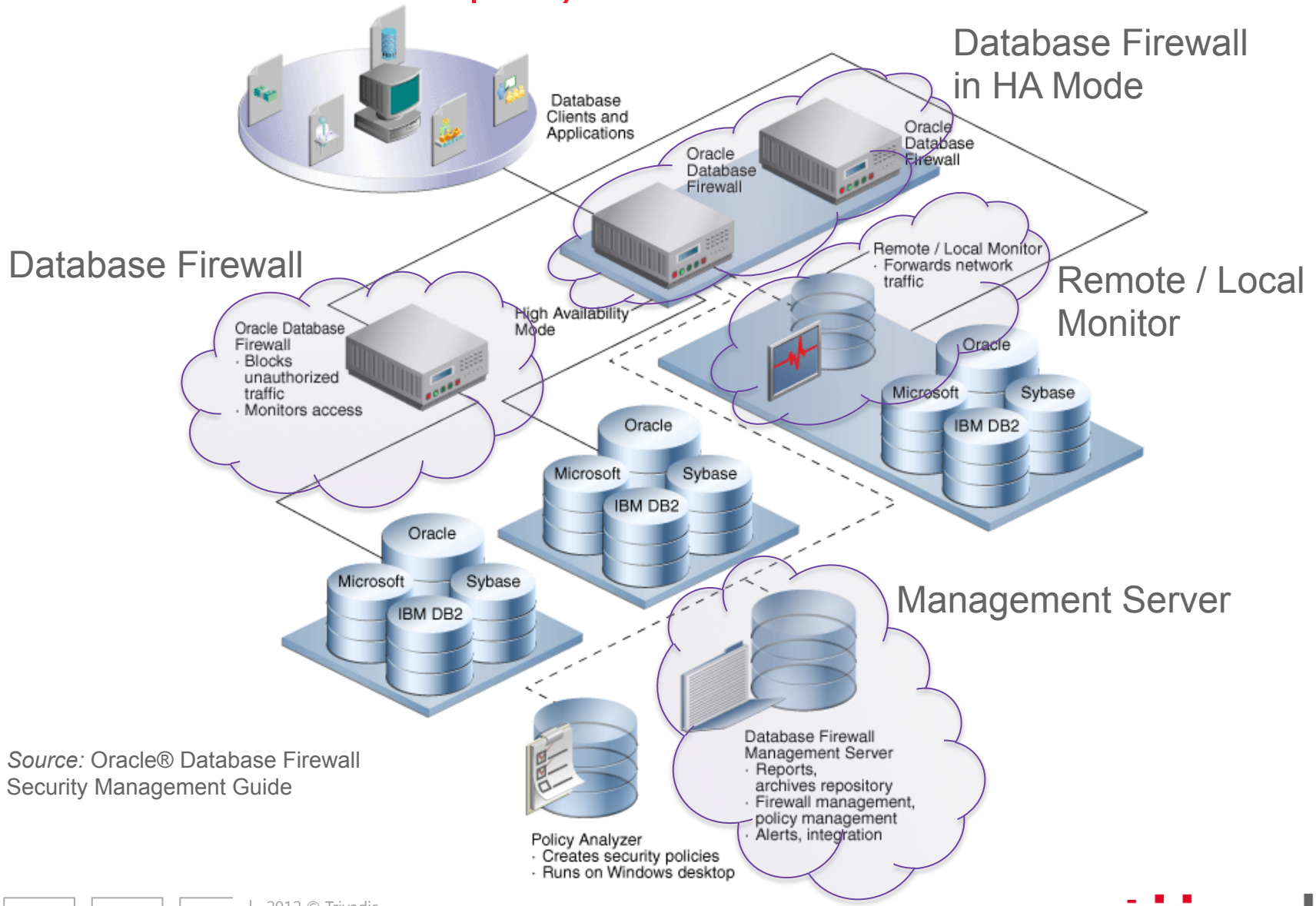
- Oracle Audit Vault
  - Oracle solution for central storage, management and reporting of audit data
  - Organize as audit warehouse
  - Data collection is partially based on standard and fine grained auditing
- Oracle Database Firewall
  - Building a “line of defense” between data and access level
  - Controlling and/or monitor how and who is accessing data
- McAfee database activity monitoring (DAM)
  - Collection audit information from the shared memory rather than through database audit
  - Allows other interesting functionalities

Audit Vault and third party tools

Audit Vault architecture



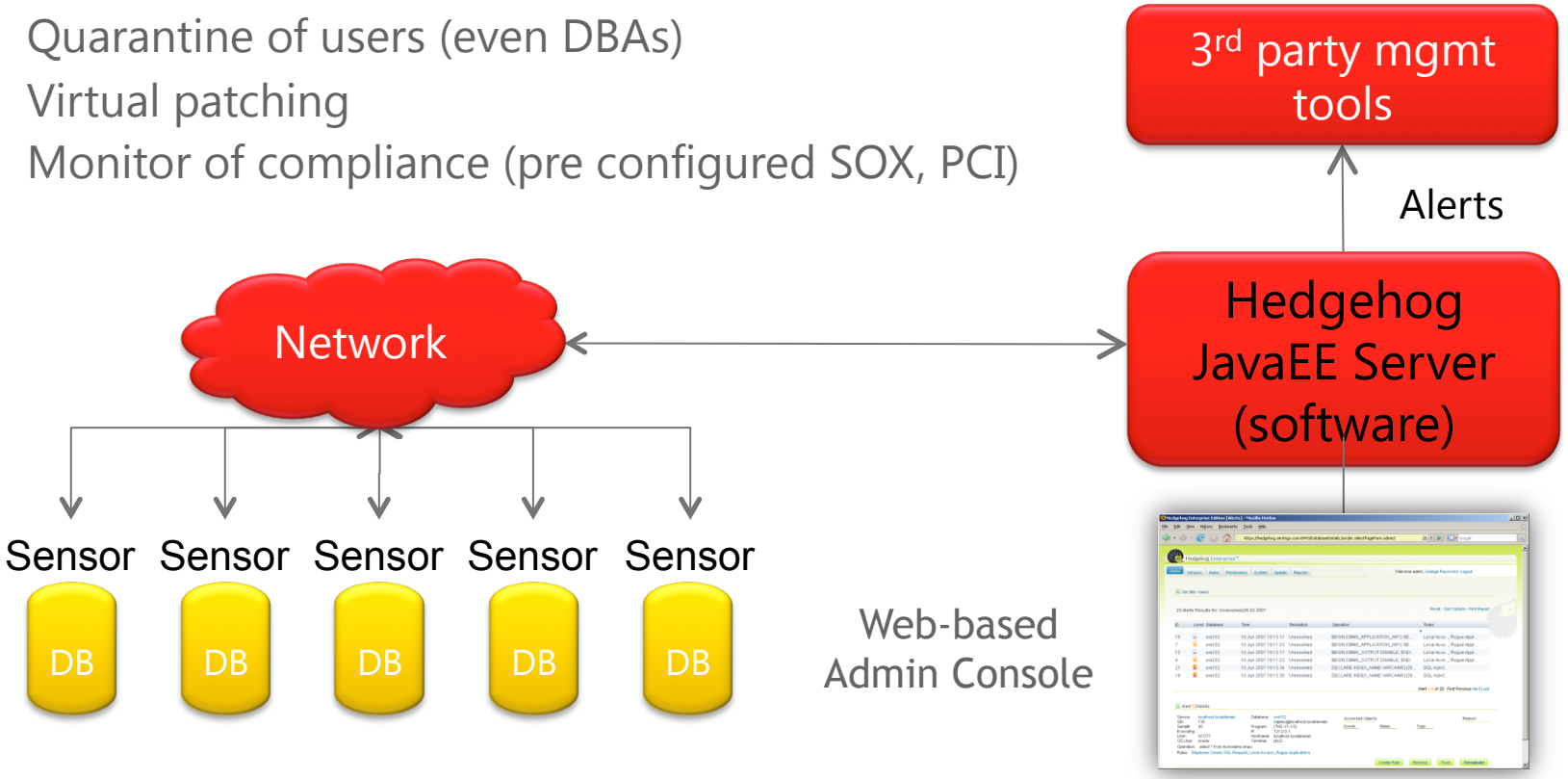
Audit Vault and third party tools



Source: Oracle® Database Firewall Security Management Guide

Audit Vault and third party tools

- McAfee database activity monitoring not just a central database audit
  - Kill sessions (thus indirect authorization)
  - Quarantine of users (even DBAs)
  - Virtual patching
  - Monitor of compliance (pre configured SOX, PCI)



AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

trivadis
makes IT easier.

Housekeeping and archiving

Any audit facility will generate a bunch of raw audit data

- Plan the storage of audit data
  - Separate table space for AUD$ and FGA_LOG$ (default SYSTEM)
  - Keep the audit files on a dedicated file system or central server
- Choose a appropriate retention for the raw audit data
  - Create regular reports to consolidate the data
  - E.g.. keep raw data up to 3 months and consolidated reports for 1 year
- Consolidate audit data on a central system
  - Oracle Audit Vault
  - SYSLOG Server
  - Custom solution

trivadis
makes IT easier.

Housekeeping and archiving

DBMS_AUDIT_MGMT a PL/SQL package to maintain any AUDIT_TRAIL's

- Part of 11g R2 or available as patch for 11g R1 and 10g R2
- Initially required by Oracle Audit Vault
- Provides a set of procedures and functions to
  - Initialize audit management infrastructure
  - Move AUD$ and FGA_LOG$ tables to an other location
  - Clean up any AUDIT_TRAIL and create purge jobs
  - Set AUDIT_TRAIL properties
- Provides a set of new views
  - DBA_AUDIT_MGMT_CLEANUP_JOBS
  - DBA_AUDIT_MGMT_CLEAN_EVENTS
  - DBA_AUDIT_MGMT_CONFIG_PARAMS
  - DBA_AUDIT_MGMT_LAST_ARCH_TS

Housekeeping and archiving

Initializing the audit management infrastructure

```
exec DBMS_AUDIT_MGMT.INIT_CLEANUP(AUDIT_TRAIL_TYPE =>
DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD, DEFAULT_CLEANUP_INTERVAL => 12 /
*hours*/);
```

Move AUD$ to a new location

```
BEGIN
  DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_DB_STD,
    AUDIT_TRAIL_LOCATION_VALUE => 'AUDIT_DATA');
END;
/
```

Purge audit records before archive timestamp

```
exec DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL( AUDIT_TRAIL_TYPE =>
DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD, USE_LAST_ARCH_TIMESTAMP => TRUE );
```

trivadis
makes IT easier.

Housekeeping and archiving

Setup a automatic clean job

```
BEGIN
  DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
    AUDIT_TRAIL_PURGE_INTERVAL => 24 /* hours */,
    AUDIT_TRAIL_PURGE_NAME => 'Daily_Purge_Job',
    USE_LAST_ARCH_TIMESTAMP => TRUE);
END;
/
```

Clean job as defined above

```
select JOB_NAME,JOB_STATUS,AUDIT_TRAIL,JOB_FREQUENCY
from DBA_AUDIT_MGMT_CLEANUP_JOBS;

JOB_NAME          JOB_STAT AUDIT_TRAIL            JOB_FREQUENCY
----------------- -------- ---------------------- -------------------------
DAILY_PURGE_JOB    ENABLED  STANDARD AUDIT TRAIL FREQ=HOURLY;INTERVAL=24
```

AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

Performance

Does audit impact Performance? It depends…

- How and what will be audited, but it will…
  - …generate additional redo information
  - …more CPU load
  - …more IO
- Only just as much as necessary but as much as possible.
  - Audit can be done in different ways by access, whenever not successfully, etc.
  - Only audit critical privileges, statements or objects
  - Do not just audit any or all
- The different AUDIT_TRAIL settings/ possibilities …
  - OS does have the lowest performance impact
  - XML, Extended and DB, Extended does have the most impact

trivadis
makes IT easier.

Performance

Audit Trail Setting	Additional Throughput Time	Additional CPU Usage
OS	1.39%	1.75%
XML	1.70%	3.51%
XML, Extended	3.70%	5.26%
DB	4.57%	8.77%
DB, Extended	14.09%	15.79%

- Oracle Database Auditing Performance Guideline: http://www.oracle.com/technetwork/database/audit-vault/learnmore/twp-security-auditperformance-166655.pdf

Performance

	AUDIT TRAIL	none	11g standard auditing OS	DB	XML
Wait times	CPU Time	78%	76%	75%	73%
	db file sequential read	17%	19%	20%	21%
AWR results	SwingBench Transactions/s	57,1	56,83	56,65	56,82
	Transactions/s	68,00	67,20	68,80	68,40
	Redo size/transaction (bytes)	1408	1493	1481	1473
	BlockChanges/transaction	10	10,3	10,2	10,3
	LogicalReads/transaction	344	357,3	345,6	337,1
	CPU Usage	67,10%	70,10%	68,20%	65,20%
Overhead	time/transaction (SwingBench)	0,00%	+0,47%	+0,79%	+0,49%
	time/transaction (AWR)	0,00%	1,18%	-1,18%	-0,59%
	redo generated/transaction	0%	6%	5%	5%
	block changes/transaction	0%	3%	2%	3%

- Trivadis article on Audit Performance
  http://www.trivadis.com/uploads/tx_cabagdownloadarea/TTC_Oracle_Auditing_Report_AMI_June2011-final.pdf

AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

Licensing

Overview of audit facilities / options and there licenses

Text	Oracle SE(O)	Oracle EE	Licenses / Comment
Oracle standard audit	✓	✓	Part of all supported oracle releases
Trigger based auditing	✓	✓	Trigger have to be developed, tested, maintained
Fine grained auditing FGA	✗	✓	EE License required
SYS auditing	✓	✓	SYSDBA connects are audited by default
DBMS_AUDIT_MGMT	11g R2	11g R2	For earlier release AV Agent licenses is required (see MOS Note 731908.1)
Audit Vault	✓	✓	AV Server / Agent licenses is required
Application auditing	✓	✓	Audit facilities have to be implemented within application
Database Activity Monitoring	✓	✓	Third Party Product

AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

Audit concept and principles

- Since Oracle 11g standard audit is enabled by default
  - Good starting point but needs to be extended depending on security level
  - Audit critical statements and privileges
  - Audit critical objects (tables, views, procedures)
- Define reporting of audit data before enabling auditing
- Define retention policies for raw and aggregated audit data
  - Eg keep raw data up to 6 months and reports 2 years
- Set AUDIT_TRAIL to DB,EXTENDED
  - Database is easier to query than OS files
  - Ensure that all information on SQL statements is written to the AUDIT_TRAIL
- Store audit data in a separate table space if DB or DB, EXTENDED or on a dedicated location if OS or XML is used

Audit concept and principles

- Keep audit data in a central database
  - Offline storage for long term archiving
- Define three different security levels INTERNAL, CONFIDENTIAL and SECRET
  - Each level should have it's own audit concept
  - INTERNAL => extended standard audit, 6 month retention
  - CONFIDENTIAL => extended standard audit plus critical tables and privileges, retention 2 years
  - SECRET => central audit solution, retention 7 years
- There are several My Oracle Support notes about auditing
  use *Master Note For Oracle Database Auditing* 1299033.1 to start

AGENDA

1. Overview
2. Oracle audit facilities and options
3. Audit Vault and third party tools
4. Housekeeping and archiving
5. Performance
6. Licensing
7. Audit concept and principles
8. One more thing

One more thing

Audit data could be manipulated on different levels

- Audit data could be manipulated
  - Change, remove audit files on the file system
  - Update audit records in AUD$ or FGA_LOG$
- Prevent tampering
  - Limit access to audit files (*.aud, *.xml)
  - Enable audit of the core audit tables AUD$, FGA_LOG$
- Keep your software / database up to date to avoid security vulnerabilities
  - Install latest patch set
  - Regularly install Oracle CPU (critical patch updates)

One more thing

Using oradebug to temporarily disable SYS audit or standard auditing

```
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
```

Auditing is disabled instance wide until next DB restart or manual reset

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

Limit access on OS and use personalized user accounts

Conclusion:

Oracle is providing audit facilities on different levels

It is important to know what should be audited

This is not always easy...

But we are happy to assist you ☺

?

Questions?

trivadis
makes IT easier.

THANK YOU.

Trivadis AG

Stefan Oehrli

Europa-Strasse 5
CH-8152 Glattbrugg

Tel. +41 44 808 70 20

stefan.oehrli@trivadis.com
www.trivadis.com
www.oradba.ch

BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

trivadis
makes IT easier.