# Table of Contents

1. INTRODUCTION ................................................................................................................................................. 1-1
   1.1 Scope............................................................................................................................................................... 1-1
   1.2 INTRODUCTION OF ORACLE AUDIT VAULT ......................................................................................... 1-1
      1.2.1 Advantages................................................................................................................................................. 1-1

2. REQUIREMENT OR PROBLEM STATEMENT ................................................................................................. 2-1

3. PREREQUISITES .................................................................................................................................................... 3-1
   3.1 SOFTWARE REQUIRED ................................................................................................................................. 3-1
   3.2 DATABASE SETTINGS REQUIRED .............................................................................................................. 3-1

4. ORACLE AUDIT VAULT COMPONENTS .......................................................................................................... 4-1
   4.1 AUDIT VAULT ARCHITECTURE .................................................................................................................... 4-1
   4.2 AUDIT VAULT SERVER ............................................................................................................................... 4-2
   4.3 AUDIT VAULT AGENT .................................................................................................................................. 4-3
   4.4 AUDIT VAULT SOURCE .................................................................................................................................. 4-3

5. ORACLE AUDIT VAULT – FEATURES WITH FLEXCUBE USE CASES ......................................................... 5-1
   5.1 APPROACH...................................................................................................................................................... 5-1
   5.2 ENVIRONMENT USED ......................................................................................................................................... 5-1
      5.2.1 Oracle Audit Vault Server........................................................................................................................ 5-1
      5.2.2 Oracle Audit Vault Agent and DB server ............................................................................................. 5-1
   5.3 COMPARISON MEASUREMENT RESULTS .................................................................................................. 5-1
1. Introduction

1.1 Scope

This document brings out the feasibility of auditing FLEXCUBE schema using Oracle Audit Vault feature. This document also presents observations made during the test done on FLEXCUBE with auditing operations and thus quantifies the benefits achieved in some of these operations.

1.2 Introduction of Oracle Audit Vault

Oracle Audit Vault is an audit solution that consolidates, detects, monitors, alerts, and reports on audit data for security auditing and compliance. Oracle Audit Vault provides mechanisms to collect audit data from various Oracle databases. It provides a means to automatically collect and analyze audit data (who connected, when, what they did, etc.) from multiple systems into a centralized location.

Audit Vault can collect data from the Oracle Database audit trail tables, database operating system audit files, and database redo logs to capture before or after value changes. Audit Vault is agent/server architecture having audit vault server is central repository and action console and individual audit vault collection agent are deployed to db/application server to collect the audit data and send to central repository for analysis. To collect DB audit data it is not necessary to have agent install on the source machine(audit db source).to collect the OS audit the agent should be install on the same machine whose OS related data needs to be gathered for analysis.

1.2.1 Advantages

- Consolidates audit trails by mapping various audit data to a common audit format
- Secures all audit data across the enterprise
- Offers centralized audit policy management
- Enables analysis of audit data, including timely detection of violations
- Facilitates regulatory compliance
2. Requirement or Problem Statement

The requirement is to enable the auditing feature for Oracle FLEXCUBE application to monitor the DML operations performed by user/application using redo collector of Oracle Audit Vault and observe feasibility, adoptability and the performance impact if any.
3. Prerequisites

3.1 Software Required

1. Oracle Audit vault Server (10.3.0.0)
   
   Download & install the Oracle Audit Vault Server (10.3.0.0) from the below link
   

2. Oracle Audit Vault Agent
   
   Download & install the Oracle Audit Vault Agent (10.3) from the below link
   

3. Oracle Database server
   
   Download & install the Oracle Database server 11g from the below link
   

3.2 Database Settings Required

Following settings are required to be done on the database servers:-

- Ensure that the source database has a password file setup and source DB is in archivelog mode.
- Parameter needs to be change to configure the Redo collector

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Recommended Value</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>_job_queue_interval</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>_spin_count</td>
<td>5000</td>
<td>2000</td>
</tr>
<tr>
<td>undo_retention</td>
<td>3600</td>
<td>900</td>
</tr>
<tr>
<td>job_queue_processes</td>
<td>4</td>
<td>1000</td>
</tr>
<tr>
<td>global_names</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>streams_pool_size</td>
<td>200M</td>
<td>0</td>
</tr>
</tbody>
</table>
4. Oracle Audit Vault Components

4.1 Audit Vault Architecture

Oracle Audit Vault primarily consists of Audit Vault Server, Agent and Source. Following diagram describes the architecture flow of it.

- **Audit Vault Server**
  - Management and Monitoring
  - Reporting
  - Alerts
  - Audit Settings Management
  - Data Warehouse
  - Audit Data Collection

- **Audit Vault Agent**
  - Collectors: REDO, DBAUD, OSAUD

- **Audit Sources**

4.2 Audit Vault Server

Audit Vault Server monitors Oracle Database audit trail tables, database operating system audit files, and database redo logs to capture before or after value changes. It can then generates reports and alerts showing where such unusual activity is occurring.

Audit Vault Server consists of:

- OC4J(Oracle container for Web applications) consist of:
- Audit vault console: it is a user interface to manage audit vault.
- Oracle Enterprise Manager Database Control console: it is a user interface to manage audit repository database.
- Management Framework – Sends management commands to the Audit Vault Agent to start or stop agent and collectors
- Audit Policy System: A service to retrieve and provision audit settings on the source; and a system to create and manage alerts raised by audit events
- Database Client is infrastructure to communicate to the audit repository consist of:
  - Oracle Wallet – Contains credentials to authenticate Audit Vault users
  - Configuration Files – Files used by Audit Vault for networking, preferences
- Configuration and Management Tools – Utilities used to configure and manage Oracle Audit Vault, such as the AVCA, AVCTL, and AVORCLDB command-line utilities.
- Logs: Informational and error messages for Oracle Audit Vault
- Audit repository: Oracle database to consolidate and manage audit trail records, consist of
  - Raw audit data store – A table space with a single data file where audit records are inserted as rows into a set of partitioned tables
  - Warehouse schema – Open schema of normalized audit trail records
  - Job scheduler – Database jobs used to populate and manage the warehouse
  - Alerts – Queue maintains alerts
  - Apply – Process used by the REDO collector to insert before or after values of data

4.3 **Audit Vault Agent**

It does provide run-time support for audit data collection by Audit Vault collectors. An agent loads the collectors, provides them with a connection to the Audit Vault audit service for sending audit data, it also handles calls from the Audit Vault management service and routes them to the appropriate collectors, and sends the Audit Vault management service run-time metrics on the collectors.

- OC4J (Oracle container for Web applications) consist of:
  - Audit Vault Collector Manager – Receives management commands from Audit Vault Server to start and stop collectors
  - Audit Settings Manager – Receives commands from Oracle Audit Vault to extract audit settings from a source
- Database Client: Infrastructure to communicate to the audit repository consist of:
  - Oracle Wallet – Contains credentials to authenticate Audit Vault
  - Configuration Files – Files used by Audit Vault for networking
- Configuration and Management Tools: Utilities used to configure and manage Audit Vault, such as the AVCA, AVCTL, and AVORCLDB command-line utilities
- Logs: Informational and error messages for Audit Vault
- Collectors: The type of collectors deployed by the Audit Vault Agents includes:
  - OSAUD – Collector to collect audit data from event logs. This collector will collect data from the source where the windows agent and this collector is running
  - DBAUD - Collector to extract audit records from the Oracle Database SYS.AUD$ dictionary table and SYS.FGA_LOG$ dictionary table
  - REDO – Collector using Oracle Streams technology to retrieve logical change records from the REDO logs

Following chart describes various feature supported by above said collectors.
4.4 **Audit Vault Source**

It is the db/application whose audit trail tables, database operating system audit files, and database redo logs to capture before or after value changes are being captured.

The audit data source consists of Oracle Database audit trails stored in:

- SYS.AUD$ dictionary table and SYS.FGA_LOG$ dictionary table that are collected by the DBAUD collector
- Operating system audit trail files stored on Linux and UNIX-based systems and event logs stored on Windows systems that are collected by the OSAUD collector
- Redo logs containing logical change records of before and after values in which a REDO collector using Oracle Streams technology utilizes a Capture process to read the data and a Propagate process to transmit it.
5. Oracle Audit Vault – Features with FLEXCUBE Use Cases

The FLEXCUBE data entry process has been chosen for the Oracle Audit Vault testing. The primary tables which are involved in this DE Upload were enabled with auditing using redo collector method (i.e. accounting table, Customer Account table & DE batch related tables). The use case of this feature could be extended to other application specific area based on customer needs.

Test case on the FLEXCUBE schema by enabling Redo collector feature of Oracle Audit Vault is described below.

5.1 Approach

- Enable DML and select operation auditing on FLEXCUBE schema for tables related to DE upload by using redo collector Feature of Oracle Audit vault.
- Monitor the Audit report generated from Oracle audit Vault server to get the details of the DML and select operations performed by user.
- Performance measurement was done for 16000 DEUPLOAD records.

5.2 Environment Used

5.2.1 Oracle Audit Vault Server

- Operating System - Linux x86_64 2.6.18-53.el5
- Number of CPU’s - 8
- Physical Memory - 16GB

5.2.2 Oracle Audit Vault Agent and DB server

- Operating System - Microsoft Windows XP [Version 5.1.2600]
- Number of CPU’s - 1
- Physical Memory - 2GB

5.3 Comparison Measurement Results

It is observed that about 22% of performance overhead caused by enablement of audit vault using redo collector to process 16,000 Data Entries with the commit frequency of 300 entries.