

## Oracle Database Security: Detective Controls Ed 1

Duration: 5 Days

### What you will learn

In the Oracle Database Security: Detective Controls course, students learn how they can use Oracle Database administration auditing features to meet the compliance requirements of their organization. The current regulatory environment requires better security at the database level. Students learn how to audit the access to their databases and how to use the auditing and compliance features to monitor data access and confidentiality. The course provides suggested Oracle solutions for common problems.

### Learn to:

Enumerate Oracle auditing solutions to monitor database security requirements. Implement Oracle Audit Vault and Oracle Database Firewall. Configure Oracle Audit Vault and Oracle Database Firewall. Explain Oracle Compliance Framework. Configure basic Compliance Framework rules.

### Benefits to You

Students will benefit by learning about the following security features of the database: Oracle Audit Vault, Oracle Database Firewall and Oracle Compliance Framework.

Hands-on practices and available demonstrations help students learn how to use detective control features of Oracle Database 12c to audit their database access using Oracle Enterprise Manager Cloud Control or other simple tools like SQL\*Plus.

### Related Training

Required Prerequisites

Create PL/SQL procedures

Good knowledge of Oracle Database Administration

Good understanding of SQL

Introduction to Oracle Database Security Ed 1

Suggested Prerequisites

Create and manage database users, roles, and privilege

Oracle Database 12c R2: Administration Workshop Ed 3

Oracle Database: Develop PL/SQL Program Units

Oracle Database: Develop PL/SQL Program Units Ed 2

### Course Objectives

Enumerate Oracle auditing solutions to monitor database security requirements

Implement Oracle Audit Vault and Database Firewall

Configure Oracle Audit Vault and Database Firewall

**TRUST-SYSTEMS CONSULTING SARL**

N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala

BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331

Email : [contact@trust-systems.net](mailto:contact@trust-systems.net) – site web : [www.trust-systems.net](http://www.trust-systems.net)

Explain Oracle Compliance Framework  
Configure basic Compliance Framework rules

## Course Topics

### Introduction

Course Objectives and Schedule  
Course Practices and Additional Information

### Using Unified Audit

Auditing Overview  
Unified Audit Management  
Specific Audit Situations

### Using Fine-Grained Audit

Comparison with Unified Auditing  
Overview  
FGA Implementation

### Introduction to Oracle Audit Vault and Database Firewall (AVDF)

Oracle Audit Vault and Database Firewall Features  
Oracle Audit Vault and Database Firewall Components  
Oracle Audit Vault and Database Firewall Architecture  
Supported Secured Targets  
Integrating Oracle AVDF with Third-party Products  
Oracle AVDF Administrator Tasks  
Oracle AVDF Auditor Tasks

### Planning the Oracle Audit Vault and Database Firewall Implementation

Evaluating Oracle AVDF Configuration Requirements  
Configuring Oracle AVDF and Deploying the Audit Vault Agent  
Configuring Oracle AVDF and Deploying the Database Firewall

### Installing the Audit Vault Server

Requirements for Installation of Oracle AVDF  
Network Interface Card Requirements  
Installing an Audit Vault Server  
Performing Audit Vault Server Post-Installation Tasks

### Configuring the Audit Vault Server

Specifying the Server Date and Time  
Setting or Changing the Audit Vault Server Network Settings  
Configuring or Changing the Audit Vault Server Service  
Configuring the Audit Vault Server Syslog Destinations  
Defining Datafile Archiving Locations  
Creating Archiving Policies

**TRUST-SYSTEMS CONSULTING SARL**  
N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala  
BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331  
Email : [contact@trust-systems.net](mailto:contact@trust-systems.net) – site web : [www.trust-systems.net](http://www.trust-systems.net)

Configuring the Email Notification Service  
Configuring Administrative Accounts for the Audit Vault Server

### **Configuring Oracle AVDF and Deploying the Audit Vault Agent**

Understanding Network Requirements for AV Server and AV Agent  
Registering Hosts in the Audit Vault Server  
Deploying and Activating the Audit Vault Agent on Host Computers  
Registering the Audit Vault Agent as a Windows Service  
Creating User Accounts for Oracle AVDF  
Registering Secured Targets  
Configuring Audit Trails for Secured Targets  
Configuring Stored Procedure Auditing

### **Networking and Oracle AVDF**

Overview of the OSI 7-level Network Model  
Overview of IPv4 Addressing and Routing  
Overview of MAC Addressing  
Overview of Virtual LANs (VLANs)  
Overview of Spanning Tree Protocol (STP)  
Oracle AVDF Deployment Models (inline, out of band, and proxy)  
Best Practices for Database Policy Enforcement (DPE) and Database Activity Monitoring (DAM) Modes

### **Installing a Database Firewall**

Requirements for Installation of a Database Firewall  
Network Interface Card (NIC) Requirements  
Installing a Database Firewall  
Performing Database Firewall Post-Installation Tasks

### **Configuring Oracle AVDF and Deploying Database Firewall**

Configuring Basic Settings for Database Firewall  
Configuring a Database Firewall on Your Network  
Associating a Database Firewall with the Audit Vault Server  
Registering Secured Targets  
Configuring Enforcement Points  
Configuring and Using Database Interrogation  
Configuring and Using Database Response Monitoring

### **Using Host Monitoring**

Overview of Host Monitoring  
Installing and Enabling Host Monitoring  
Checking the Status of the Host Monitor  
Stopping the Host Monitor

### **Configuring High Availability**

**TRUST-SYSTEMS CONSULTING SARL**  
N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala  
BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331  
Email : [contact@trust-systems.net](mailto:contact@trust-systems.net) – site web : [www.trust-systems.net](http://www.trust-systems.net)

Overview of Oracle AVDF High Availability Architecture (resilient pairs)  
Configuring a Resilient Pair of Audit Vault Servers  
Configuring a Resilient Pair of Database Firewalls

### **Creating Custom Collection Plug-ins**

Overview of Audit Collection Plug-ins  
General Procedure for Writing Audit Collection Plug-ins  
Setting Up Your Development Environment (downloading the SDK)  
Creating Audit Collection Plug-ins  
Packaging Audit Collection Plug-ins

### **Managing the Audit Vault Server**

Starting an Archive Job  
Restoring Audit Data  
Monitoring Jobs

### **Managing the Database Firewalls**

Viewing and Capturing Network Traffic in a Database Firewall  
Viewing the Status and Diagnostics Report for a Database Firewall  
Removing a Database Firewall from the Audit Vault Server

### **Overview of the Auditing and Reporting Features**

Overview of Database Firewall Policies  
Overview of Oracle Database Audit Policies  
Overview of Reports and Report Schedules  
Overview of Oracle Database Entitlement Auditing  
Overview of Oracle Database Stored Procedure Auditing  
Overview of Alerts and Email Notifications

### **Performing Administrative Tasks**

Viewing a List of Audit Trails and Audit Trail Status  
Viewing a List of Enforcement Points and Enforcement Point Status  
Specifying a Data Retention Policy  
Creating Secured Target Groups  
Assigning a Secured Target to a Compliance Group  
Managing User Accounts and Access  
Creating Templates and Distribution Lists for Email Notifications Monitoring Jobs

### **Creating Audit Policies for Oracle Databases**

Overview of Audit Policies and Audit Data Collection  
Overview of Oracle Database Auditing  
Recommended Audit Settings  
Creating Audit Policies for Oracle Database (overview)  
Retrieving and Modifying Audit Settings from an Oracle Database  
Creating Additional Audit Policy Settings for an Oracle Database

### **Creating Database Firewall Policies**

- Overview of Database Firewall Policies
- Creating a Firewall Policy
- Defining Firewall Policy Rules and Settings
- Using Profiles to Customize a Firewall Policy
- Publishing Firewall Policies
- Deploying Firewall Policies to Secured Targets

### **Oracle AVDF Reports**

- Using the Built-in Reports
- Managing Reports
- Customizing Built-in Reports
- Creating Custom Reports

### **Managing Entitlements**

- Overview of Entitlement Data (what is it?)
- Retrieving Entitlement Data from an Oracle Database (creating a snapshot)
- Creating Labels for Snapshots
- Assigning Labels to Snapshots
- Using Entitlement Reports

**TRUST-SYSTEMS CONSULTING SARL**  
N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala  
BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331  
Email : [contact@trust-systems.net](mailto:contact@trust-systems.net) – site web : [www.trust-systems.net](http://www.trust-systems.net)