THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

Oracle Audit Vault and Database Firewall: Install & Configure

Student Guide

D86587GC10

Edition 1.0

August 2014

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Authors

Donna K. Keesling
James L. Spiller

Technical Contributors & Reviewers

Paul Betteridge
Andrey Brozhko
Melody S. Liu
Pedro Lopes
Dinesh Rajasekharan

Graphic Editor

Seema Bopaiah

Editor

Malavika Jinka

Publishers

Nita Brozowski
Michael Sebastian Almeida

Copyright © 2014, Oracle and/or it affiliates. All rights reserved.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice. If you find any problems in the document, please report them in writing to: Oracle University, 500 Oracle Parkway, Redwood Shores, California 94065 USA. This document is not warranted to be error-free.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS
The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose these training materials are restricted by the terms of the applicable Oracle license agreement and/or the applicable U.S. Government contract.

Trademark Notice

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

Contents

1 Introduction to Oracle Audit Vault and Database Firewall
Objectives 1-2
Introducing Oracle Audit Vault and Database Firewall 1-3
Database Auditing and Activity Monitoring 1-4
Oracle AVDF Components 1-6
Oracle Audit Vault and Database Firewall Architecture 1-7
Audit Collection: Supported Secured Target Types 1-8
Database Firewall Protection: Supported Secured Target Types 1-10
Audit Vault Agent: Supported Platforms 1-11
Host Monitor: Supported Platforms 1-12
Configuring Network Firewalls to Enable Audit Vault and Database Firewall Deployment 1-13
Quiz 1-14
Using Enterprise Manager Cloud Control to Monitor Oracle AVDF 1-15
Integrating Oracle AVDF with Third-Party Products 1-16
Oracle AVDF Administrator Tasks 1-17
Oracle AVDF Auditor Tasks 1-18
Summary 1-19
Practice 1 1-20

2 Planning the Oracle Audit Vault and Database Firewall Implementation
Objectives 2-2
Planning the Oracle AVDF Implementation 2-3
Audit Vault Server Capacity Planning and Sizing Requirements 2-7
Database Firewall Capacity Planning and Sizing Requirements 2-9
Quiz 2-11
Implementation Workflow: AVDF and the Audit Vault Agent 2-12
Implementation Workflow: AVDF and the Database Firewall 2-13
Summary 2-14
Practice 2 2-15

3 Installing the Audit Vault Server
Objectives 3-2
Server Requirements 3-3
Network and Communication Requirements 3-4

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Client Software Requirements 3-5
Ports for Services Provided by the Audit Vault Server 3-6
Ports for External Network Access by the Audit Vault Server 3-7
Installing an Audit Vault Server 3-8
Performing Audit Vault Server Post-Installation Tasks 3-9
Quiz 3-10
Summary 3-11
Understanding the Classroom Configuration 3-12
Practice 3 3-13

4 Configuring the Audit Vault Server
Objectives 4-2
Configuring Administrative Accounts for the Audit Vault Server 4-3
Understanding AVDF Time Stamps 4-4
Specifying the Server Date and Time Settings 4-5
Setting or Changing the Audit Vault Server Network Settings 4-6
Configuring the Audit Vault Server Services 4-7
Configuring the Audit Vault Server Syslog Destinations 4-8
Defining Datafile Archiving Locations 4-9
Creating Archiving Policies 4-11
Configuring the Email Notification Service 4-12
Quiz 4-13
Summary 4-14
Practice 4 4-15

5 Configuring Oracle AVDF and Deploying the Audit Vault Agent
Objectives 5-2
Deploying and Activating the Audit Vault Agent on Host Computers 5-3
Registering Hosts in the Audit Vault Server 5-4
Deploying the Audit Vault Agent on the Host Computer 5-5
Activating and Starting the Audit Vault Agent 5-6
Registering the Audit Vault Agent as a Windows Service 5-7
Quiz 5-8
Creating User Accounts for Oracle AVDF 5-9
Creating User Accounts for an Oracle Database Secured Target 5-10
Creating User Accounts for a Sybase ASE Secured Target 5-11
Creating User Accounts for a Microsoft SQL Server Secured Target 5-12
Creating User Accounts for an IBM DB2 for LUW Secured Target 5-13
Registering Secured Targets 5-14
Configuring Audit Trails for Secured Targets 5-15
Configuring Stored Procedure Auditing 5-16

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing for an Oracle Database Secured Target 5-17
Configuring Stored Procedure Auditing for a Sybase ASE Secured Target 5-18
Configuring Stored Procedure Auditing for a Sybase SQL Anywhere Secured Target 5-19
Configuring Stored Procedure Auditing for a Microsoft SQL Server Secured Target 5-21
Configuring Stored Procedure Auditing for an IBM DB2 for LUW Secured Target 5-23
Configuring Stored Procedure Auditing for a MySQL Secured Target 5-24
Summary 5-25
Practice 5 5-26

6 Networking and Oracle AVDF
Objectives 6-2
OSI Seven-Layer Network Model: Overview 6-3
Layer Processing 6-4
OSI Networking Model Physical Layer 6-5
OSI Physical Layer 6-6
OSI Networking Model Data Link Layer 6-7
OSI Link Layer 6-8
Media Access Control (MAC) Addresses 6-9
Switches 6-10
Virtual Local Area Networks (VLANs) 6-11
Switches with VLAN Tags 6-12
Quiz 6-13
OSI Networking Model Network Layer 6-14
OSI Layer 3 (Network) 6-15
IPv4 Addresses 6-16
IPv4 Subnets 6-17
IPv4 Historical Class-Based Addressing 6-19
Classless Inter-Domain Routing (CIDR) 6-20
IP Version 6 6-21
OSI Networking Model Layer 4 6-22
Network Connections 6-23
Network Routing 6-24
Hostname Resolution 6-25
Quiz 6-26
OSI Networking Model Layer 5 6-27
OSI Networking Model Layer 6 6-28

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model Layer 7 6-29
Network Requirements 6-30
Spanning Tree Protocol 6-31
By-Pass Network Cards 6-32
Network Proxy 6-33
Network Firewall 6-34
Network Protection Techniques 6-35
Quiz 6-36
AVDF Supported Protocols 6-37
Oracle AVDF Deployment Models 6-38
Oracle Database Firewall Operational Modes 6-39
Database Firewall Bridge Configuration Basics 6-41
Basic Data Center Environment 6-42
Oracle Database Firewall Inline Deployment 6-43
Inline Networking Internals 6-44
Audit Vault Server and Database Firewall Link Layer Settings 6-45
AVDF Bridging 6-46
Oracle Audit Vault and Database Firewall and VLANs 6-47
Oracle Database Firewall Out-of-Band Monitoring 6-48
Out-of-Band Networking Internals 6-49
Oracle Database Firewall Proxy 6-50
Proxy Mode Networking Internals 6-51
Network Firewalls and Audit Vault and Database Firewall Deployment 6-52
Quiz 6-53
Summary 6-54
Practice 6 6-55

7 Installing a Database Firewall
Objectives 7-2
Installation Requirements: Hardware 7-3
NIC Requirements 7-4
Client Software Requirements 7-5
Ports for Services Provided by a Database Firewall 7-6
Ports for External Network Access by a Database Firewall 7-7
Installing a Database Firewall 7-8
Performing Database Firewall Post-Installation Tasks 7-9
Quiz 7-10
Summary 7-11
Understanding the Classroom Configuration 7-12
Practice 7 7-13

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

8 Configuring Oracle AVDF and Deploying Database Firewall
Objectives 8-2
Basic Database Firewall Configuration 8-3
Configuring Basic Settings for Database Firewall 8-4
Configuring a Database Firewall on Your Network 8-5
Configuring Traffic Sources 8-6
Configuring a Bridge in the Database Firewall 8-7
Configuring a Database Firewall as a Traffic Proxy 8-8
Associating the Database Firewall with an Audit Vault Server 8-9
Registering the Database Firewall with the Audit Vault Server 8-10
Secured Targets 8-11
Registering Secured Targets 8-12
Enforcement Point Architecture 8-13
Configuring Enforcement Points 8-15
Quiz 8-16
Configuring and Using Database Interrogation 8-17
Configuring Database Interrogation for Oracle Databases 8-18
Configuring Database Interrogation for SQL Server Databases 8-19
Configuring Database Interrogation for SQL Anywhere Databases 8-20
Configuring and Using Database Response Monitoring 8-21
Summary 8-22
Practice 8 8-23

9 Using Host Monitoring
Objectives 9-2
Host Monitoring: Overview 9-3
Operating System Prerequisites 9-4
Installing and Enabling Host Monitoring 9-5
Registering Hosts in the Audit Vault Server 9-6
Deploying the Audit Vault Agent on the Host Computer 9-7
Installing the Host Monitor 9-8
Registering Secured Targets 9-10
Configuring Enforcement Points 9-11
Configuring an Audit Trail for Host Monitoring 9-12
Checking the Status of the Host Monitor 9-13
Stopping the Host Monitor 9-14
Uninstalling the Host Monitor 9-15
Quiz 9-16
Summary 9-17
Practice 9 9-18

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

10 Configuring High Availability
Objectives 10-2
Oracle AVDF High Availability Architecture: Overview 10-3
A High Availability Pair of Database Firewalls Protecting a Single Secured Target 10-4
Pairs of Audit Vault Servers and Database Firewalls in High Availability Mode 10-5
Recommended Configuration Sequence 10-6
Configuring a Resilient Pair of Audit Vault Servers 10-7
Configuring a Resilient Pair of Database Firewalls 10-8
Quiz 10-9
Summary 10-10
Practice 10 10-11

11 Creating Custom Collection Plug-ins
Objectives 11-2
Custom Collection Plug-ins: Overview 11-3
Collector Plug-in 11-4
Deploying the Collector Plug-in 11-5
Database Table Collection Plug-in Requirements 11-6
XML File Collection Plug-in Requirements 11-7
Template-Based Customizable Collection 11-8
General Procedure for Creating Custom Collection Plug-ins 11-9
Setting Up Your Development Environment 11-11
Creating Custom Collection Plug-ins 11-13
Creating a Plug-in Manifest File 11-14
Creating an XML Mapper File 11-15
Creating the Collection Plug-in Package 11-16
Deploying a Custom Collection Plug-in 11-17
Setting Secured Target Collection Attributes 11-18
Best Practices Checklist 11-19
Quiz 11-20
Summary 11-21
Practice 11 11-22

12 Managing the Audit Vault Server
Objectives 12-2
Managing Audit Data Retention 12-3
Oracle AVDF Administrator's Role in Audit Data Management 12-4
Oracle AVDF Auditor's Role in Audit Data Management 12-5
Starting an Archive Job 12-6
Restoring Audit Data 12-7

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Monitoring Jobs 12-8
Managing the Audit Vault Agent 12-9
Deactivating and Removing the Audit Vault Agent 12-10
Backing Up and Restoring the Audit Vault Server 12-11
Quiz 12-12
Summary 12-13
Practice 12 12-14

13 Managing the Database Firewall
Objectives 13-2
Viewing and Capturing Network Traffic in a Database Firewall 13-3
Viewing Live Network Traffic 13-4
Capturing Network Traffic to a File 13-5
Viewing the Status and Diagnostics Report for a Database Firewall 13-6
Removing a Database Firewall from the Audit Vault Server 13-7
Quiz 13-8
Summary 13-9
Practice 13 13-10

14 Overview of the Auditing and Reporting Features
Objectives 14-2
Database Firewall Policies: Overview 14-3
Database Firewall Policy Enforcement 14-4
Database Firewall Policy Enforcement Flow 14-5
Configuring Policies 14-6
Oracle Database Firewall Preconfigured Policies 14-7
Audit Policies: Overview 14-8
Reports and Report Schedules: Overview 14-9
Oracle Database Entitlement Auditing: Overview 14-10
Oracle Database Entitlement Auditing Reports 14-11
Oracle Database Stored Procedure Auditing: Overview 14-12
Alerts and Email Notifications: Overview 14-13
Creating an Alert 14-14
Quiz 14-15
Summary 14-16
Practice 14 14-17

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

1

Introduction to Oracle Audit Vault and Database Firewall

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Describe the Oracle Audit Vault and Database Firewall (Oracle AVDF) components
- Explain the Oracle AVDF architecture and process flow
- List the secured targets that are supported by Oracle AVDF
- Describe integration with third-party products
- Describe the roles of the AVDF administrator and auditor

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Introducing Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (Oracle AVDF) provides:

- Comprehensive and flexible monitoring through consolidation of audit data from Oracle and non-Oracle databases, operating systems, directory, file systems, and application-specific audit data
- A first line of defense on the network, enforcing expected application behavior, helping prevent SQL injection, application bypass, and other malicious activity from reaching the database

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle AVDF provides a first line of defense for databases and consolidates audit data from databases, operating systems, and directories. A highly accurate SQL grammar-based engine monitors and blocks unauthorized SQL traffic before it reaches the database. Database activity data from the network is combined with detailed audit data for easy compliance reporting and alerting. With Oracle AVDF, auditing and monitoring controls can be easily tailored to meet enterprise security requirements.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Database Auditing and Activity Monitoring

	Database Auditing	Activity Monitoring (Database Firewall)
Information	Who, what, when, where Before/after values Full execution and application context	Who, what, when, where
Pathways	All: Stored procedures, direct connections, scheduled jobs, and operational activities	Network
Impact on database	Configure database audit policies	Completely independent
Purpose	Ensure compliance Provide guaranteed audit trail to enable control	Prevent SQL injections and other unauthorized activity Enforce compliance with corporate data security policy

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle AVDF is part of Oracle's comprehensive portfolio of Database Security products. It performs two main functions:

- Collects, stores, manages, and reports (or presents) information about user activity with respect to protected data assets
- Blocks SQL injection and other attacks on databases through the Database Firewall component

Database auditing is the recording, storing, and reporting on selected user actions in the database. It can be based on individual actions, such as the type of SQL statement that is executed, or on combinations of factors that can include name, application, time, and so on. Security policies can trigger auditing when specified elements in Oracle Database are accessed or altered, including content.

Auditing is generally used to:

- Enable future accountability for current actions taken in a particular schema, table, or row, or affecting specific content
- Investigate suspicious activity. For example, if an unauthorized user is deleting data from tables, the security administrator could audit all connections to the database and all successful and unsuccessful deletions of rows from all tables in the database.

Oracle University and Error : You are not a Valid Partner use only

- Gather statistics about specific database activities. For example, a database administrator can gather statistics about which tables are being updated, how many logical I/O operations are performed, or how many concurrent users connect at peak times.

Database auditing is a security function internal to the database. It is built into the core of RDBMSs. The key advantage is that native audit data provides a complete view of database activity along with full execution context irrespective of whether the statement was executed directly, through dynamic SQL, or through stored procedures.

By contrast, *activity monitoring* is performed outside of the database. Similar to database auditing, SQL commands sent to the database get recorded, stored, and reported on, including session attributes such as username, application, and so on. When an activity monitoring function is deployed on the network, monitoring is performed without impacting the database server and/or its clients, which are being monitored. Another important aspect of activity monitoring that stems from the fact that it is external to the database, is that the monitoring component can actively interfere in client-to-database interaction. It can firewall the database and prevent malicious SQL from ever reaching it. Oracle AVDF can block attempted attacks in real time by either stopping the statement on its way to the database or substituting it with a trivial “no-effect” statement returning no results.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

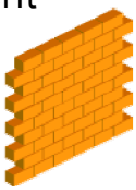
Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle AVDF Components

Oracle AVDF includes the following components:

- Audit Vault Server: The central, highly scalable and secure repository that stores consolidated audit data as well as event logs generated by the Database Firewall



- Database Firewall: The network monitoring component outside the database that monitors inbound SQL traffic and serves as a first line of defense against SQL injection threats and other unauthorized SQL statements

- Audit Vault Agent: The component that retrieves the audit trail data from a secured target database and sends it to the Audit Vault Server

ORACLE

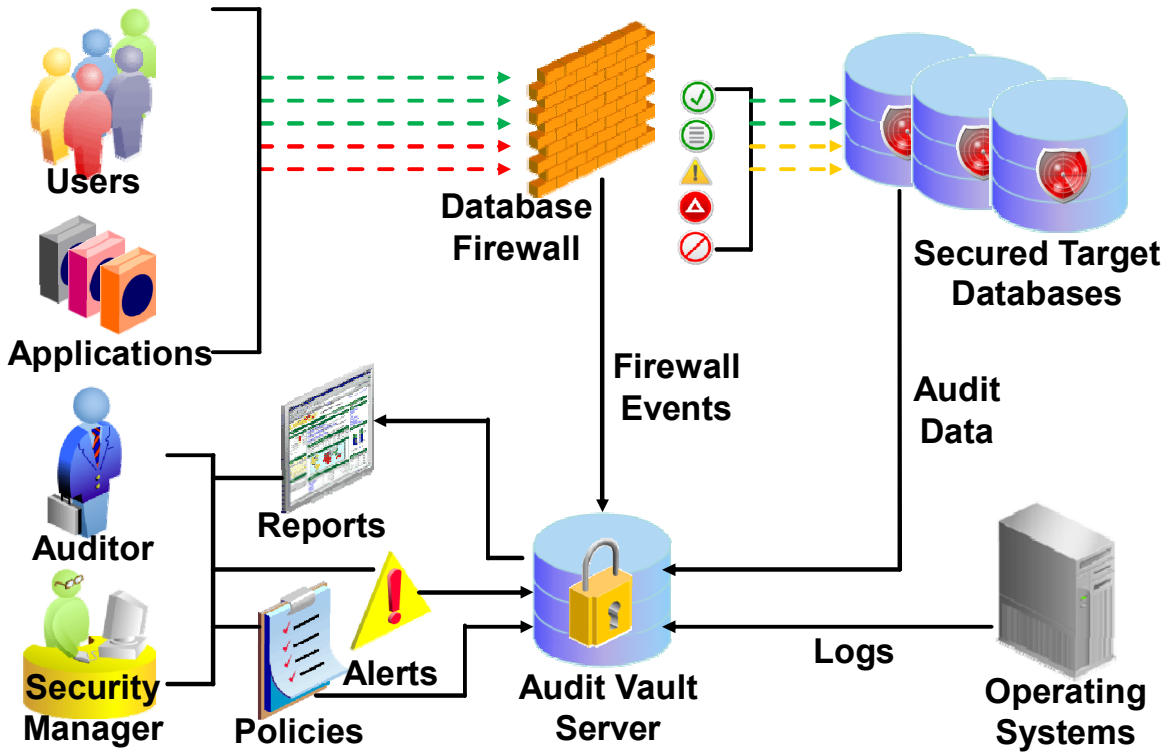
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle AVDF includes the components listed in the slide. Additional details on the components follows in this lesson.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Audit Vault and Database Firewall Architecture



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

For each secured target, you can deploy the Audit Vault Agent and/or place the Database Firewall in the network to protect the target.

If you deploy the Audit Vault Agent, it retrieves audit data from the audit trail of a secured target via built-in or custom collection plug-ins, and sends the data to the Audit Vault Server.

If you have deployed a Database Firewall to protect the target, a firewall policy is applied.

The Database Firewall monitors SQL traffic for secured targets and sends data to the Audit Vault Server based on the policies that have been configured.

The Database Firewall can be configured to monitor and raise alerts only, or to block SQL traffic and optionally substitute statements according to the defined policy.

The Audit Vault Server includes an internal database warehouse, which is used to store Oracle AVDF configuration data and collected audit data.

After audit data is stored in the data warehouse, an auditor can generate reports.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Audit Collection: Supported Secured Target Types

- Database management systems:
  - Oracle Database 10*g*, 11*g*, and 12*c*
  - IBM DB2 for LUW (Linux, UNIX, Windows) 9.x
  - Microsoft SQL Server 2000, 2005, 2008, 2008 R2, 2012
  - Sybase ASE 12.5.4 – 15.7
  - MySQL 5.5.29 – 5.6.12
- Operating systems:
  - Oracle Solaris on SPARC24 10, 11
  - Oracle Solaris x86-64 10, 11
  - Oracle Linux 5.8 and 6.0 – 6.4
  - Microsoft Windows Server on x86-64 2008, 2008 R2

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle AVDF supports different types of secured targets by providing a plug-in for each secured target type. Audit Vault Server software plug-ins enable the Audit Vault Agent to manage the collection of audit data from audit trails of secured targets. A set of out-of-the-box plug-ins is packaged and deployed with the Audit Vault Server to support the listed targets. You can develop your own plug-ins as described in the *Creating Custom Collection Plug-ins* lesson. You may also obtain new plug-ins from the Oracle Technology Network as they become available and add them to your Oracle AVDF installation.

Refer to *Appendix B, Plug-in Reference* of the *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on supported targets.

Refer to the My Oracle Support note for information on supported target types for previous releases: Doc ID 1536380.1

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Audit Collection: Supported Secured Target Types

- Directory Service:
  - Microsoft Active Directory 2008, 2008 R2
- File System:
  - Oracle ACFS 12*c*
- Hadoop System:
  - Oracle Big Data Appliance 2.3 and later

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Refer to *Appendix B, Plug-in Reference* of the *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on supported targets.

Refer to the My Oracle Support note for information on supported target types for previous releases: Doc ID 1536380.1

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Database Firewall Protection: Supported Secured Target Types

- Database management systems:
  - Oracle Database 9*i*, 10*g*, 11*g*, and 12*c*
  - IBM DB2 for LUW (Linux, UNIX, Windows) 9.x
  - Microsoft SQL Server 2000, 2005, 2008, 2008 R2, 2012
  - Sybase ASE 12.5.4 – 15.7
  - Sybase SQL Anywhere 10.0.1
  - MySQL 5.0, 5.1, 5.5, 5.6

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Refer to *Appendix B, Plug-in Reference* of the *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on supported targets.

Refer to the My Oracle Support note for information on supported target types for previous releases: Doc ID 1536380.1

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Audit Vault Agent: Supported Platforms

- Operating systems:
  - Linux x86-64: SLES11, RHEL 5 and 6, Asianux 3, Oracle Linux 5 and 6
  - Linux x86-32: SLES11, RHEL 5 and 6, Asianux 3, Oracle Linux 5 and 6
  - Microsoft Windows x86-64 7, 8, 8.1
  - Microsoft Windows Server on x86-64 2003, 2003R2, 2008, 2008R2
  - Microsoft Windows x86-32 7, 8, 8.1
  - Microsoft Windows Server on x86-32 2003, 2003R2, 2008
  - Oracle Solaris on x86-64 10, 11
  - Oracle Solaris on SPARC64 10, 11
  - IBM AIX on POWER Systems (64-bit) 6.1, 7.1
  - HP-UX on Itanium 11.31

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Refer to the My Oracle Support note for information on supported target types for previous releases: Doc ID 1536380.1

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Host Monitor: Supported Platforms

- Operating systems:
  - Linux x86-64: SLES11, RHEL 5 and 6, Asianux 3, Oracle Linux 5 and 6
  - Microsoft Windows Server x86-64 2008, 2008R2

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Refer to the My Oracle Support note for information on supported target types for previous releases: Doc ID 1536380.1

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Network Firewalls to Enable Audit Vault and Database Firewall Deployment

- Corporate networks are usually sectioned by network firewalls, which only allow specific traffic between zones.
- Audit Vault and Database Firewall components interact with each other and third-party enterprise systems.
- Ensure that required ports are open to enable Audit Vault and Database Firewall communication.
- Audit Vault Server and Database Firewall communication:

Port Number	Protocol Family	Protocol	Direction	Description
443	TCP	HTTPS	Connection initiated from Audit Vault Server	Management and traffic collections
1514	TCP	SSL	Connection initiated from Database Firewall	Event and status reporting

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The table in the slide lists the ports that are used for communication between Audit Vault Server and Database Firewall. Additional port information is provided in the “Installing the Audit Vault Server” and “Installing a Database Firewall” lessons.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Oracle AVDF provides two separate functions: database auditing and activity monitoring.

a. True
b. False

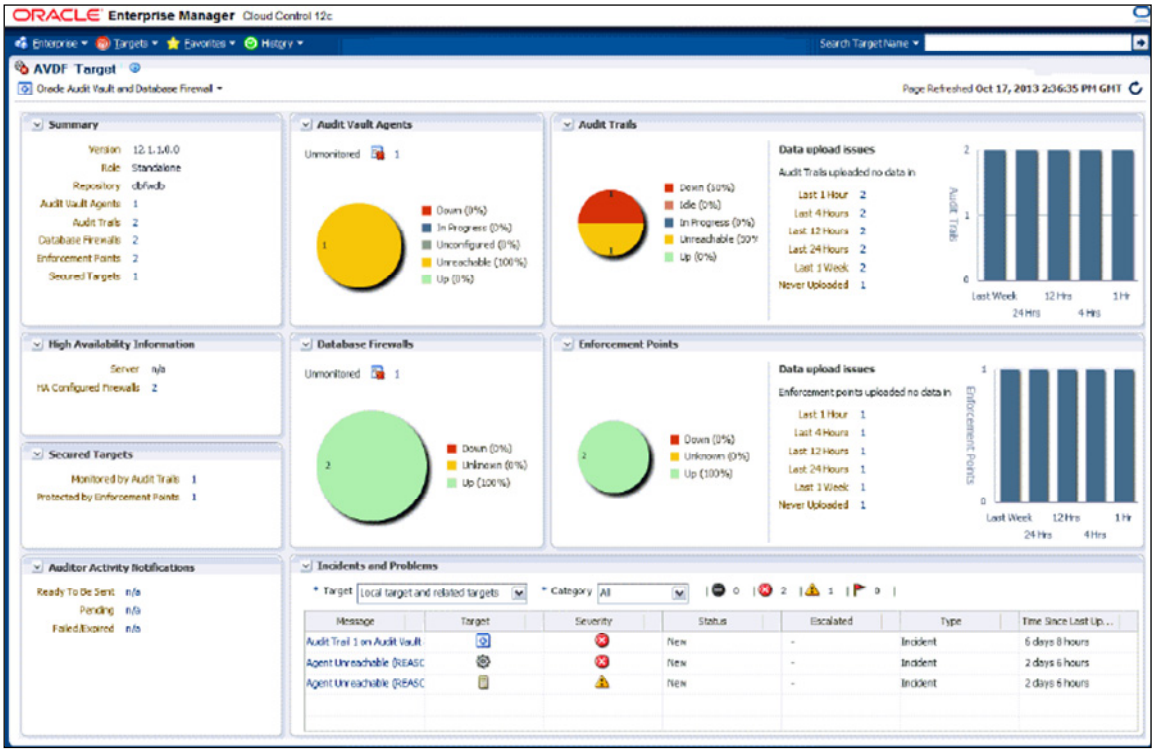
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Using Enterprise Manager Cloud Control to Monitor Oracle AVDF



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF plug-in provides an interface within Enterprise Manager Cloud Control for administrators to manage and monitor Audit Vault and Database Firewall components.

Perform the following steps to complete the installation and configuration so that you can use Enterprise Manager Cloud Control to monitor AVDF:

1. Install a Management Agent on the Audit Vault Server.
2. Install the Management Agent on the Database Firewall(s).
3. Deploy the AVDF plug-in on the Management Server and the Management Agent.
4. Discover the Audit Vault Server target.
5. Discover the Database Firewall target(s).
6. Discover the Audit Vault Agent target.

The screenshot shows the AVDF Target home page. This page enables you to monitor: Audit Vault Agents, secured targets, audit trails, Database Firewalls, and enforcement points. This page also provides summary, high availability, auditor activity notification, and incident and problem information.

Refer to the *Oracle Enterprise Manager System Monitoring Plug-in User's Guide* for details.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Integrating Oracle AVDF with Third-Party Products

You can integrate Oracle AVDF with the following third-party products:

- BIG-IP Application Security Manager (ASM) from F5 Networks, Inc.: An advanced Web Application Firewall (WAF) that provides comprehensive edge-of-network protection against a wide range of web-based attacks
- ArcSight Security Information Event Management (SIEM): A centralized system for logging, analyzing, and managing syslog messages from different sources

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Refer to Chapter 9, Configuring Integration with BIG-IP ASM of the *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on BIG-IP Application Security Manager (ASM).

Refer to Chapter 10, Configuring Integration with ArcSight SIEM of the *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on ArcSight Security Information Event Management (SIEM).

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle AVDF Administrator Tasks

The Oracle AVDF administrator's tasks include the following:

- Configuring system settings on the Audit Vault Server and Database Firewalls
- Configuring connections to host computers
- Creating secured targets in the Audit Vault Server for each monitored database or operating system
- Deploying and activating the Audit Vault Agent on the secured target host computers
- Configuring audit trails for secured targets
- Configuring Database Firewalls on your network
- Creating enforcement points for secured targets
- Backing up and archiving audit and configuration data
- Creating administrator users and managing access

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

An Oracle AVDF administrator is typically responsible for the configuration tasks outlined in the slide.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle AVDF Auditor Tasks

The Oracle AVDF auditor's tasks include the following:

- Designing and provisioning a firewall policy based on analyzed SQL statements from your secured targets
- Designing and provisioning audit policies
- Creating alerts for secured targets
- Specifying alert notifications by using email templates
- Monitoring the status of audit trails
- Scheduling and generating a variety of audit and firewall reports, including customized reports
- Creating report notifications

Auditor

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

An Oracle AVDF auditor is typically responsible for the tasks outlined in the slide. Detailed information on the tasks performed by an Oracle AVDF auditor is provided in the *Oracle Audit Vault and Database Firewall: Policies and Reports* course.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Describe the Oracle Audit Vault and Database Firewall (Oracle AVDF) components
- Explain the Oracle AVDF architecture and process flow
- List the secured targets that are supported by Oracle AVDF
- Describe integration with third-party products
- Describe the roles of the AVDF administrator and auditor

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 1

- 1-1: Identifying Audit Vault and Database Firewall Components
- 1-2: Identifying Supported Secured Targets
- 1-3: Identifying Third-Party Product Integration
- 1-4: Distinguishing Typical Tasks of Oracle AVDF Administrators and Auditors

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The practices for this lesson are all pen-and-paper practices.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

2

Planning the Oracle Audit Vault and Database Firewall Implementation

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Describe the steps you should perform to plan for the configuration and deployment of Oracle AVDF
- Describe the workflow for configuring Oracle AVDF and deploying the Audit Vault Agent
- Describe the workflow for configuring Oracle AVDF and deploying the Database Firewall

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Planning the Oracle AVDF Implementation

1. Plan for the Audit Vault Server configuration by considering your need for the following:
   - A resilient pair of servers (high availability)
   - Changes to network configuration settings made during the installation
   - Configuration of optional services

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To plan for your implementation of Oracle Audit Vault and Database Firewall (Oracle AVDF), you must plan the configuration of the components you intend to use.

The Audit Vault Server is required in all implementations of Oracle AVDF, so you must first consider the need for the following options related to it:

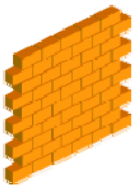
- Resilient pairs: You can configure a pair of Audit Vault Servers to provide a high-availability system architecture. These are known as resilient pairs. Refer to the lesson titled “Configuring High Availability” for detailed information.
- Network settings: The Oracle AVDF installer configures initial network settings for the Audit Vault Server during installation. Determine whether you need to make any changes to the initial network settings. This topic is covered in detail in the lesson titled “Configuring the Audit Vault Server.”
- Services: You may need to configure additional Audit Vault Server services such as host name resolution through DNS servers. This topic is also discussed in more detail in the lesson titled “Configuring the Audit Vault Server.”

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Planning the Oracle AVDF Implementation

2. Plan for the Database Firewall configuration by considering the following:
   - How many Database Firewalls you will need
   - Which secured target databases they will protect
   - Where should they be placed in the network
   - Will they be in Database Activity Monitoring (DAM) mode or Database Policy Enforcement (DPE) mode
   - Do you need to configure a resilient pair of firewalls
   - Whether to change the Database Firewall network configuration specified during installation



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

If you plan to deploy Database Firewalls as part of your implementation of Oracle AVDF, you need to determine the following:

- Which targets you plan to protect
- The number of Database Firewalls needed to protect the secured targets
- Mode of operation of the Database Firewalls:
  - Database Activity Monitoring (DAM)
  - Database Policy Enforcement (DPE)
- Need for resilient pairs
- Need to make changes to the network configuration settings specified during installation

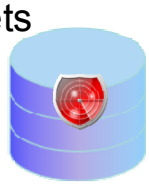
Detailed information on Database Firewall deployment and configuration is provided in the “Configuring Oracle AVDF and Deploying Database Firewall” lesson. Information about configuring resilient pairs is provided in the lesson titled “Configuring High Availability.”

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Planning the Oracle AVDF Implementation

3. Plan for the deployment of Audit Vault Agents by:
   - Determining which secured targets you want to collect audit data from
   - Identifying the host computers for the secured targets



4. Determine what type of audit trail will be collected.
5. Determine whether you need to integrate Oracle AVDF with the following third-party systems:
   - BIG-IP Application Security Manager (ASM), from F5 Networks, Inc.
   - ArcSight Security Information Event Management (SIEM)

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

If your implementation of Oracle AVDF includes the deployment of Audit Vault Agents, you need to determine which targets audit data will be collected from and identify the host computers of those targets.

If you are deploying the Audit Vault Agent to collect audit data, you will need to verify that audit trails are configured on the targets or configure audit trails. Refer to Table B–13 “Audit Trail Types Supported for Each Secured Target Type” in the *Oracle Audit Vault* and *Database Firewall Administrator’s Guide* for detailed information on the types of audit trails that data can be collected from.

If you are using BIG-IP Application Security Manager (ASM) or HP ArcSight Security Information Event Management (SIEM), determine whether you need to integrate Oracle AVDF with these products. Detailed implementation information is provided in the *Oracle Audit Vault and Database Firewall Administrator’s Guide*.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Planning the Oracle AVDF Implementation

6. Plan user accounts and access rights by determining:
   - How many super administrators and administrators you will create accounts for
   - Which secured targets the administrators will have access to

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Determine how many super administrators and administrators you will create accounts for, and to which secured targets the administrators will have access. Super administrators have access to and can modify any secured target. Administrators have access to only the secured targets they have been given access to.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Audit Vault Server Capacity Planning and Sizing Requirements

- Consider the following factors when planning for Audit Vault Server capacity:
  - Cumulative number of transactions per second logged on the server
  - Length of the retention policy for stored audit information
- Minimum required disk size is 150 GB. The two most important factors that affect disk requirements are:
  - Per-second rate of recording audit events
  - Length of the retention period as specified by the active retention policy for each secured target

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

A minimum of 150 GB of disk is required to install and run an Audit Vault Server. For most installations, disk requirements will be considerably larger.

The size of the audit event warehouse can be estimated by aggregating storage space requirements for event data from all protected secured targets. The calculation should include estimated audit event rates for all audit trails and enforcement points (for Database Firewalls) for the secured target. Detailed information on calculating storage requirements can be found in the *Oracle Audit Vault and Database Firewall 12.1 Sizing Best Practices* document.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Audit Vault Server Capacity Planning and Sizing Requirements

- CPU considerations:
  - Processing audit records from Audit Vault Agents: Allocate one core for every 1,000 audit records per second.
  - Processing SQL traffic records from Database Firewalls: Allocate one core for every 1,000 records per second, taking into account a complexity factor as necessary.
- Memory requirements:
  - 2 GB for the Audit Vault Server
  - Plus additional RAM of .1 GB - .5 GB per secured target depending on usage profile

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

CPU for Audit Vault Server is used by the following main functions:

- Recording audit events delivered by Audit Vault Agents
- Processing and storing SQL traffic records from Database Firewalls

Additional CPU is used to produce reports and generate alerts. The number of CPU cores required for processing audit records from Audit Vault Agents can be estimated by allocating one core for 1,000 audit records per second stored on the Audit Vault Server. This calculation assumes the average size of audit record to be approximately 512 bytes. CPU requirements for Database Firewalls can be calculated in a similar fashion and taking into account the complexity of the logged statements. Refer to the *Oracle Audit Vault and Database Firewall 12.1 Sizing Best Practices* document for detailed calculation formulas.

The minimum memory requirement for the Audit Vault Server is 2 GB. Additional memory must be provisioned for each secured target based on the usage profile:

- Moderate: 0.1 GB per secured target
- Medium: 0.2 GB per secured target
- High: 0.5 GB per secured target

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Database Firewall Capacity Planning and Sizing Requirements

- Consider the following factors when planning for Database Firewall capacity:
  - Cumulative number of transactions per second monitored by the Database Firewall
- Minimum required disk size: 130 GB (moderate use)
- CPU requirements:
  - One core for every 5,000 transactions per second monitored by Database Firewall
  - One core for all system management processes
- Memory requirements:
  - 2 GB for Database Firewall
  - Additional RAM per enforcement point depending on usage profile

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The primary factors in planning Database Firewall capacity is the cumulative number of transactions per second monitored by the Database Firewall.

A minimum of 130 GB of disk is required to install and run a Database Firewall. The disk space is used for temporary storage of captured SQL traffic and associated data before it is transferred to the Audit Vault Server. Estimated amount of disk space required based on usage profiles is as follows:

- Moderate: 130 GB
- Medium: 300 GB
- High: 500 GB

The number of required CPU cores can be estimated by allocating one core for every 5,000 transactions per second monitored by Database Firewall. In addition, one core is required for all system management processes. Refer to the *Oracle Audit Vault and Database Firewall 12.1 Sizing Best Practices* document for additional information based on secured target types.

Oracle University and Error : You are not a Valid Partner use only

The minimum memory requirement for Database Firewall is 2 GB. If there are multiple enforcement points, total memory requirements based on usage profiles are as follows:

- Moderate: .5 GB per enforcement point
- Medium: 1.0 GB per enforcement point
- High: 1.5 GB per enforcement point

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

The Audit Vault Server is required in all implementations of Oracle AVDF.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Implementation Workflow: AVDF and the Audit Vault Agent

1. Configure the Audit Vault Server.
2. Register the host computers where you will deploy the Audit Vault Agent, and then deploy and activate the Audit Vault Agent on those hosts.
3. Create user accounts on your secured targets for Oracle AVDF to use.
4. Register the secured targets you are monitoring with the agent in the Audit Vault Server, and configure audit trails for these secured targets.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

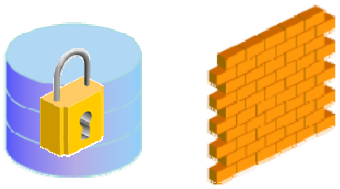
The steps in the slide are a general workflow for configuring Oracle AVDF and deploying the Audit Vault Agent. Detailed information about these steps is provided in later lessons of this course.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Implementation Workflow: AVDF and the Database Firewall

1. Configure the Audit Vault Server.
2. Configure the Database Firewall basic settings and associate the firewall with the Audit Vault Server. Then configure the firewall on your network.
3. Register the secured targets you are monitoring with the Database Firewall in the Audit Vault Server. Then configure enforcement points for these secured targets. Optionally, if you want to also monitor database response to SQL traffic, use the scripts and configuration steps to do so.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The steps in the slide are a general workflow for configuring Oracle AVDF and deploying the Database Firewall. Detailed information about these steps is provided in later lessons in this course.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Describe the steps you should perform to plan for the configuration and deployment of Oracle AVDF
- Describe the workflow for configuring Oracle AVDF and deploying the Audit Vault Agent
- Describe the workflow for configuring Oracle AVDF and deploying the Database Firewall

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 2

- 2-1: Implementing Oracle Audit Vault and Database Firewall
- 2-2: Configuring Oracle AVDF and Deploying the Audit Vault Agent
- 2-3: Configuring Oracle AVDF and Deploying the Database Firewall

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The practices for this lesson are all pen-and-paper practices.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

3

Installing the Audit Vault Server

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- List installation requirements (hardware, software, and privileges)
- Describe network configuration requirements, including network interface cards (NICs)
- Install an Audit Vault Server and perform Audit Vault Server post-installation tasks

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Server Requirements

- Each Audit Vault Server requires an x86 64-bit server with:
  - Minimum 2 GB of RAM
  - Minimum 150 GB of disk space
- Hardware must support Oracle Linux, Release 5 Update 10.
- Audit Vault Server can also be installed on Oracle VM Server for x86, version 3.x.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Each Audit Vault Server and each Database Firewall is installed on its own dedicated x86 64-bit server. Your hardware must be compatible with Oracle Linux, Release 5 Update 10.

The minimum memory requirement for the Audit Vault Server is 2 GB. Additional memory should be provisioned for each secured target based on the usage profile:

- Moderate: 0.1 GB per secured target
- Medium: 0.2 GB per secured target
- High: 0.5 GB per secured target

Detailed information on calculating storage requirements can be found in the *Oracle Audit Vault and Database Firewall 12.1 Sizing Best Practices* document.

Refer to this page for the Hardware Certification List for Oracle Linux:
http://linux.oracle.com/pls/apex/f?p=117:1:3906454051792461::NO:RP::

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network and Communication Requirements

- Before installation ensure that the AV Server host can communicate with the host(s) for the secured targets.
- Oracle recommends one network interface card (NIC) for the x86 64-bit server on which you install the Audit Vault Server.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Audit Vault Server must have a network connection for the interface that is used to manage Database Firewalls and to receive audit data from secured targets.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Client Software Requirements

The following requirements pertain to the client machines, which will be used for the utilities or consoles:

- Java SE version 6 or later for:
  - AVCLI command-line utility
  - AVPACK utility
- AVDF Administrator and Auditor GUIs support the following browsers:
  - Mozilla Firefox 14 or later
  - Microsoft Internet Explorer 8.0 or later
  - Google Chrome 21 or later
  - Apple Safari 5.0 or later
- Latest version of Adobe Flash plug-in to view charts and interactive reports

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The software requirements listed in the slide are applicable for the client machines, which will be used for management of the Oracle Audit Vault and Database Firewall components.

AVPACK is discussed in the lesson titled “Creating Custom Collection Plug-ins.”

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Ports for Services Provided by the Audit Vault Server

Port Number	Protocol Family	Protocol	Description
22	TCP	SSH	Command line access (disabled by default)
161	UDP	SNMP	SNMP access (disabled by default)
443	TCP	HTTPS	Administration Console
1521 1522	TCP	Oracle Database	Access for Audit Vault agents and access to Oracle Database for reporting

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The table in the slide lists the ports for services provided by the Audit Vault Server.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Ports for External Network Access by the Audit Vault Server

Port Number	Protocol Family	Protocol	Description
25	TCP	SMTP	Email delivery
53	UDP	DNS	Domain name service
123	UDP/TCP*	NTP	Time synchronization with external time servers
514	UDP/TCP*	Syslog	Policy and system alerts sent to syslog ArcSight integration
3260	TCP*	Software iSCSI	SAN server communication

*** TCP port is configurable through the Audit Vault Server console.**

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The table in the slide lists the ports for external services that may be used by the Audit Vault Server.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Installing an Audit Vault Server

- Reminder: An Audit Vault Server must be installed on its own dedicated server.
- Provide the following information during the installation:
  - An installation passphrase to be used again during post-installation tasks
  - The network interface to be used as the management interface
  - The IP address of the management interface
  - The network mask for the management interface
  - The gateway IP address for the management interface

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Audit Vault Server is an appliance. You must install it on its own dedicated server.

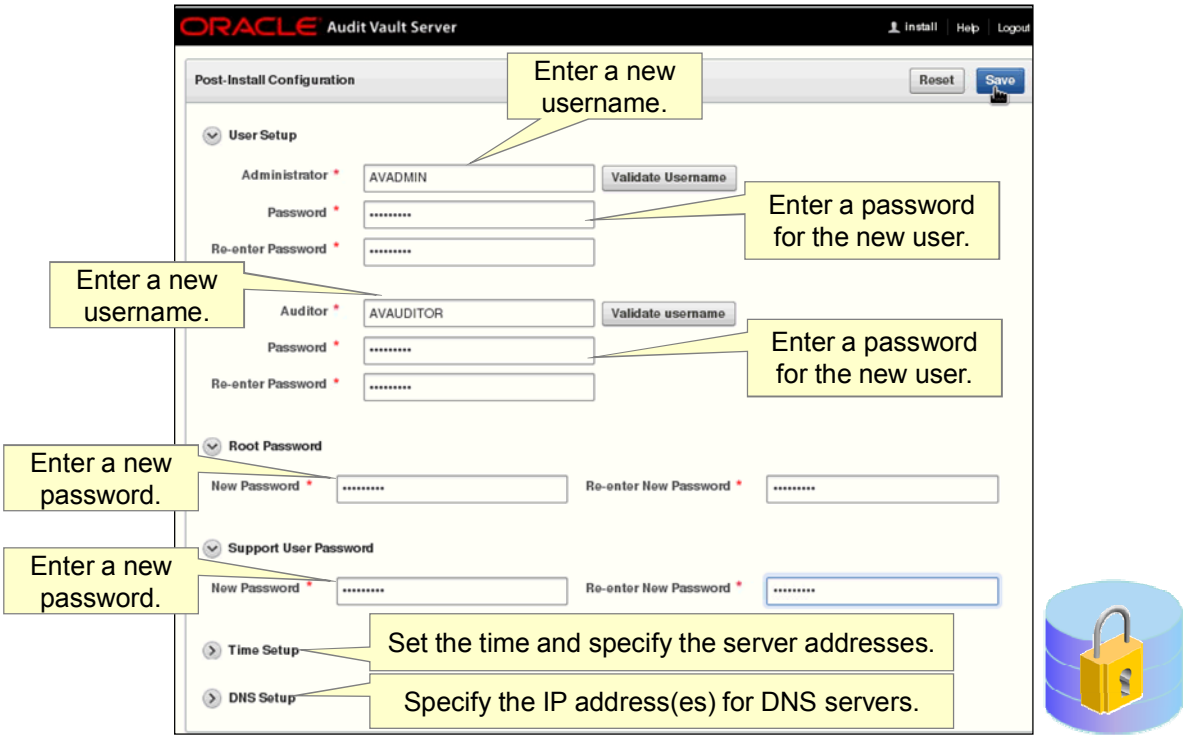
When you install the Audit Vault Server, you create an installation passphrase. You will use the installation passphrase for the post-installation configuration tasks. The installation passphrase protects the Audit Vault Server until you have completed configuration.

During installation, you supply information for the management interface. The subnet determined by the network mask must be the same subnet as the management interface for the firewall appliance management interface.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Performing Audit Vault Server Post-Installation Tasks



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must set the names and passwords for the Administrator and Auditor users with your first login to the Audit Vault Server Console.

Perform Audit Vault Server post-installation tasks as follows:

- Access the Audit Vault Server Console and enter the installation passphrase.
- On the Post-Install Configuration page:
  - Enter new names for the Administrator and Auditor users, and passwords for each.
  - Enter Passwords for the root and support users.
  - Set the time to “Use NTP” and specify the server addresses.
  - Specify the IP addresses for up to three DNS servers.

Note: You must set the names and passwords for the Administrator and Auditor users with your first login to the Audit Vault Server Console. You can perform the time and DNS setup at a later date as shown in the “Configuring the Audit Vault Server” lesson. Because you must re-enter all information on this page if any errors are encountered, you may find it easier to enter only the usernames and passwords initially, and then configure the other settings at a later time.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

You must have a separate, dedicated x86 64-bit server for each Audit Vault Server and Database Firewall.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

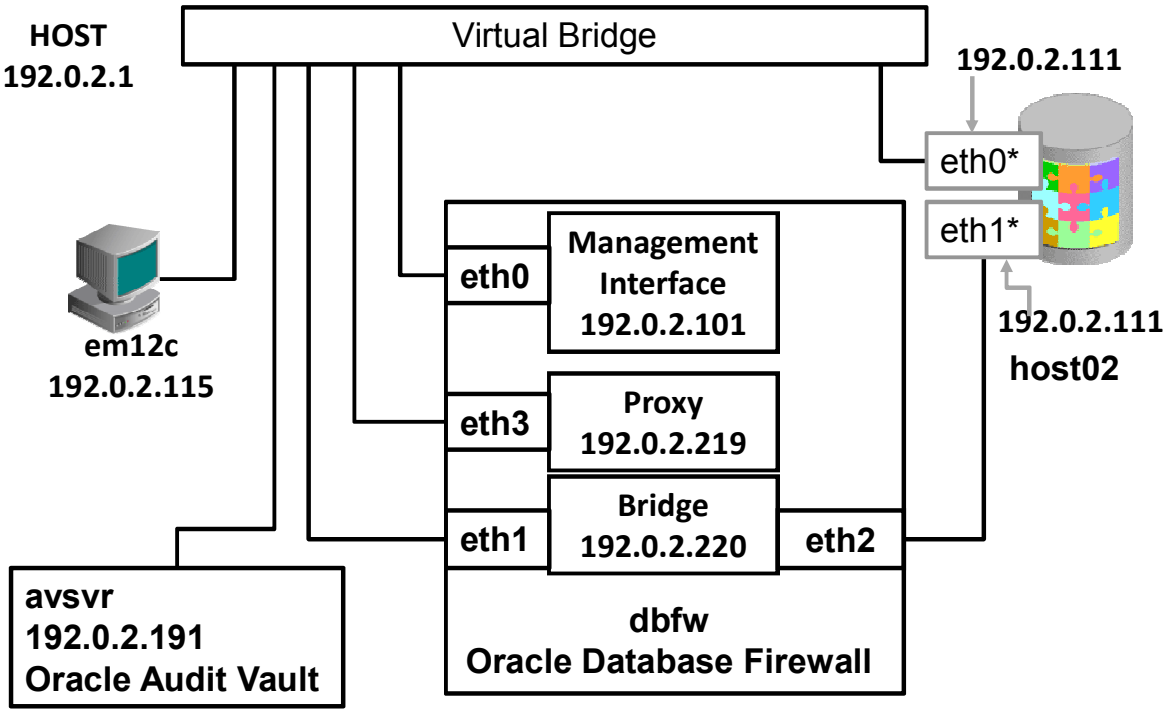
- List installation requirements (hardware, software, and privileges)
- Describe network configuration requirements, including network interface cards (NICs)
- Install an Audit Vault Server and perform Audit Vault Server post-installation tasks

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Understanding the Classroom Configuration



* **Note:** Only one of these interfaces may be active at any given time.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

There are four virtual machines in the classroom environment:

- em12c: The client machine
- host02: The database machine containing an Oracle Database 12*c* database
- avsvr: The Audit Vault Server appliance
- dbfw: The Database Firewall appliance

The host machine is the machine that contains the student desktop. You will connect to the virtual machines in your environment from here.

The database VM, `host02`, has two network devices that will use the same IP address. Only one can be active at any given time. The `eth0` device can connect to all the other VMs and will be used to demonstrate the traffic proxy configuration. The `eth1` device is connected to the Database Firewall `eth2` device and can communicate only with the `dbfw` VM.

The Database Firewall management link is set in the network configuration as part of the installation process. This is shown in the lesson titled "Deploying Oracle Database Firewall."

The bridge IP address is set to a default and is disabled by default on install. The IP address will be changed and enabled when you configure traffic sources in the Database Firewall Network Settings. Later, when the enforcement point is created, the connection between `dbfw eth2` and `host02 eth1` will be specified in the Administration Console as shown in the practice titled "Configuring Enforcement Points."

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 3

- 3-1: Performing Audit Vault Server Post-Installation Tasks

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

4

Configuring the Audit Vault Server

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Configure administrative accounts for the Audit Vault Server
- Specify the server date and time settings
- Set or change the Audit Vault Server network configuration
- Configure or change the Audit Vault Server services
- Configure the Audit Vault Server Syslog destinations
- Configure archive locations and retention policies
- Describe how to configure the email notification service

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Administrative Accounts for the Audit Vault Server

- Use Audit Vault and Database Firewall user accounts created during installation only as back-up accounts.
- Create new accounts of the following types:
  - *Super administrator:*
    - Grants access to all secured targets and secured target groups
    - Manages system-wide settings
    - Creates user accounts for super administrators and administrators
    - Grants access to secured targets or secured target groups to administrators
  - *Administrator*: Access to specific secured targets or secured target groups granted by a super administrator

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You should use the Audit Vault and Database Firewall user accounts that are defined at installation only as back-up accounts. Create new user accounts for the users who are responsible for the day-to-day Oracle Audit Vault and Database Firewall (Oracle AVDF) operations.

There are two types of Audit Vault Server user accounts. The Audit Vault Server Super Administrator has access to all secured targets and secured target groups. The Super Administrator manages system-wide settings, creates additional user accounts, and grants access to secured targets. The Audit Vault Server Administrator has access to specific secured targets or secured target groups as granted by a super administrator. Administrators cannot manage system-wide settings.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Understanding AVDF Time Stamps

- Audit Vault Server stores all data in UTC.
- For interactive data access, time stamps are in the user's time zone:
  - Audit Vault Server console: Time zone is derived from the user's browser time zone.
  - AVCLI command line: Time zone is derived from the "shell" time zone.
- For non-interactive data access (PDF reports or emails generated by the system), the time stamps displayed reflect the Time Zone Offset specified on the Audit Vault Server Manage page.
- If SSH is used to access the Audit Vault Server, time stamps are displayed in UTC.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Audit Vault Server stores all data in UTC.

If a user is accessing data interactively, all time stamps are in the user's time zone. For the Audit Vault Server console, the time zone is derived from the user's browser time zone. For the AVCLI interface, the time stamp is derived from the "shell" time zone.

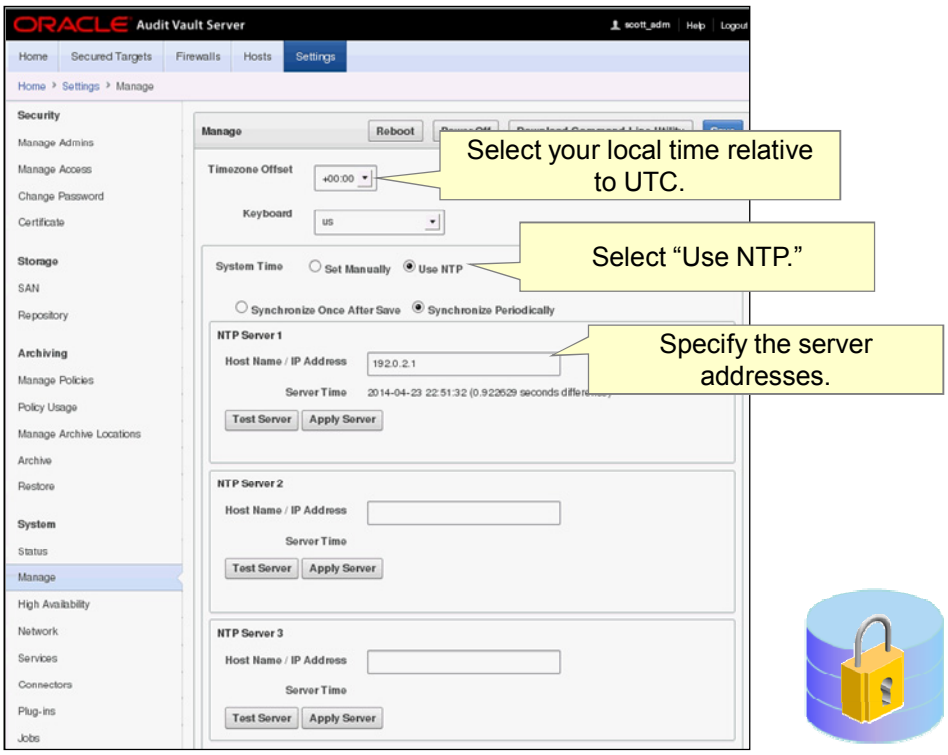
If a user is accessing data non-interactively, for example, looking at a PDF report or email generated by the system, time stamps displayed reflect the Time Zone Offset specified in the Audit Vault Server Manage page. The Audit Vault Server Manage page is described later in this lesson.

If a user uses SSH to access the Audit Vault Server as the support user, by default, time stamps are displayed in UTC.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Specifying the Server Date and Time Settings



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

On the Manage page in the Audit Vault Server console, you can specify the following settings:

- Timezone Offset: Use the Timezone Offset drop-down list to select your local time in relation to Coordinated Universal Time (UTC). Data in the Audit Vault Server database is stored in UTC. If a user accesses data non-interactively, the time stamp that is displayed reflects the timezone offset value specified on this page.
- System Time: In the System Time field, select Manually Set or NTP Synchronization. Specify the host name or IP address of the Network Time Protocol (NTP) server. You should ensure that the date and time for the Audit Vault Server are correct because the date and time are used when events are logged. Archiving occurs at intervals based on the time setting of the Audit Vault Server.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Setting or Changing the Audit Vault Server Network Settings

- During installation, the Oracle AVDF installer configures initial network settings for the Audit Vault Server.
- You can change the following network settings after installation:
  - IP address of the Audit Vault Server
  - Subnet mask of the Audit Vault Server
  - IP address of the default gateway
  - Audit Vault Server host

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

During installation, the Oracle AVDF installer configures initial network settings for the Audit Vault Server. If required, you can change the network settings after installation on the Settings page in the Audit Vault Server console.

If you change the Audit Vault Server network configuration, you must restart all audit trails. If you change the Audit Vault Server's IP address, you must update this information in the Database Firewall. If you configured a resilient pair of Database Firewalls, you must reconfigure the pair.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring the Audit Vault Server Services

You can configure the following on the Services page depending on your own requirements:

- DNS Servers: Used to specify IP addresses that are used to resolve host names used by Audit Vault Server
- Web Access: Used to specify IP addresses that are allowed to access to the Audit Vault Server console
- SSH Access: Used to specify IP addresses that are allowed to access the Audit Vault Server console from a remote server
- SNMP Access: Used to specify IP addresses that are allowed to access the network configuration of Audit Vault Server through SNMP

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

On the Services page in the Audit Vault Server console, you can configure the following based on your own requirements:

- DNS servers: You can configure up to three Domain Name Services (DNS) servers that will be used to resolve host names used by the Audit Vault Server.
- Web Access: You can select or enter specific IP addresses to restrict access to the Audit Vault Server console to only those computers. The default for this service is All, which allows access to the Audit Vault Server console from any computer.
- SSH Access: You can select or enter specific IP addresses to restrict access to the Audit Vault Server from a remote console. If you specify a value of All, any computer can access the Audit Vault Server. You can prevent access from any computer by specifying a value of Disabled.
- SNMP Access: You can specify IP addresses to allow access to the network configuration of Audit Vault Server through SNMP. The default value is Disabled, preventing any SNMP access. You can specify All to allow access from any computer.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

Configuring the Audit Vault Server Syslog Destinations

- Indicate whether you are using User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) to send syslog messages from the Audit Vault Server
- Specify the IP address of each machine that is permitted to receive the syslog messages.
- Specify the type of syslog messages to generate:
  - Alert: Based on alert conditions specified by an AVDF auditor
  - Debug: Debug messages for Oracle Support use only
  - Info: General Oracle AVDF messages and property changes
  - System: Messages generated by Oracle AVDF or other software that have a syslog priority level of at least “INFO”

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

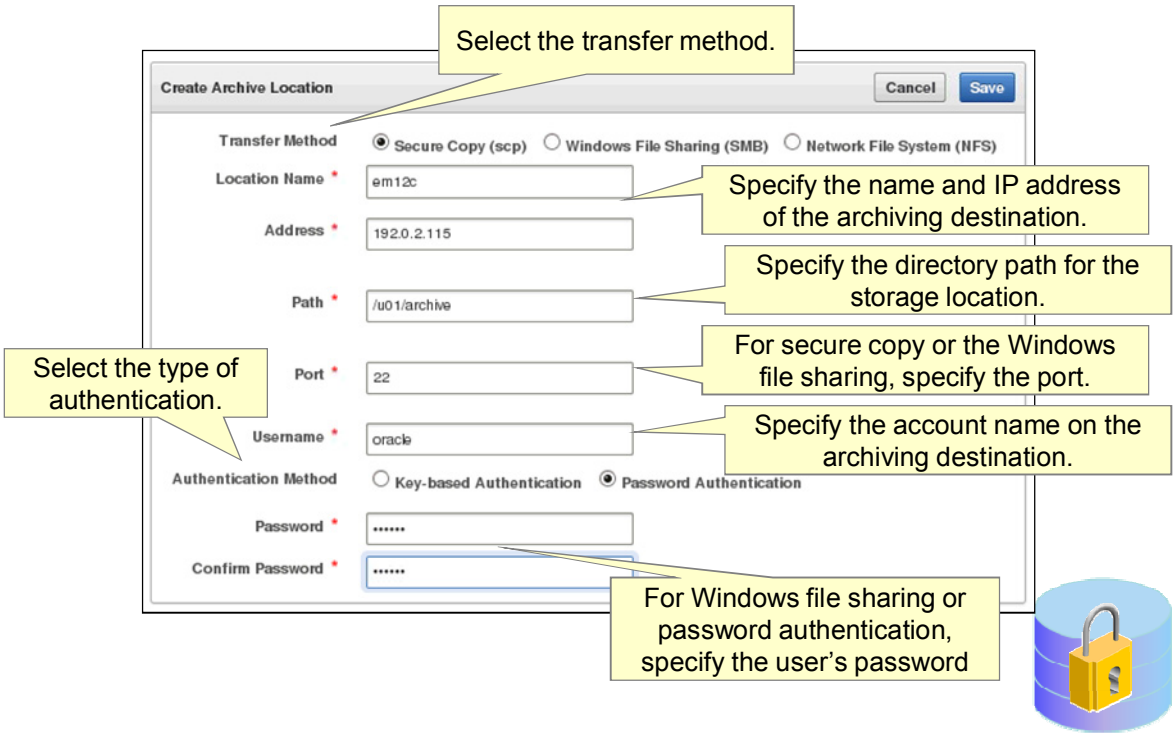
On the Connectors page in the Audit Vault Server console, you can configure the types of syslog messages to be sent from the Audit Vault Server by specifying the following:

- Syslog Destinations (UDP): Enter data in this area if you are using User Datagram Protocol (UDP) to communicate syslog messages from the Audit Vault Server. Specify the IP address of each machine that is permitted to receive the syslog messages, separated by spaces.
- Syslog Destinations (TCP): Enter data in this area if you are using Transmission Control Protocol (TCP) to communicate syslog messages from the Audit Vault Server. Specify the IP address and port combinations of each server that is permitted to receive the syslog messages, separated by spaces.
- Syslog Categories: Select the types of syslog messages to generate:
  - Alert: Based on alert conditions that an AVDF auditor specifies
  - Debug: Debug messages for Oracle support use only
  - Info: General Oracle AVDF messages and property changes
  - System: System messages generated by Oracle AVDF or other software that have a syslog priority level of at least “INFO”

Note: Syslog is a protocol that is used to convey event notification messages.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Defining Datafile Archiving Locations



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must define one or more archive locations before you can start an archive job. You define the archive location on the Create Archive Location page by selecting a transfer method and then specifying additional information about the archiving location.

The transfer method can be one of the following:

- Secure Copy (scp) if the data is to be archived on a Linux machine
- Windows File Sharing (SMB) if the data is to be archived on a Windows machine
- Network File Storage (NFS) if you are using a network file share or NAS

Specify information in the following fields to identify the archive location:

- Location Name: Name that you provide for the archiving destination and will use to select the destination when setting up an archive job
- Address: The name or IP address of the machine for the archive. If you selected Windows File Sharing as the transfer method, specify an IP address.
- Path: The directory path for the archive storage location.
- Port: The port number used by the secure copy or the Windows file sharing service on the archive location machine. You can normally use the default port number.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

- Username: The account name on the machine to which the archive data will be transferred.
- Authentication Method:
  - If you selected Secure Copy (scp) as the transfer method, you can select Password and specify the login password.
  - If the archive destination is a Linux machine, you can select Key Authentication.
- Password and Confirm Password: If you selected Windows File Sharing or you selected Password as the authentication method, specify the password for the archive destination user.
- Public Key: This field appears if you selected Key Authentication as the Authentication Method. Copy the public key and add it to the public keys file on the archive destination machine.

If you selected the Network File System (NFS) transfer method, the following fields appear:

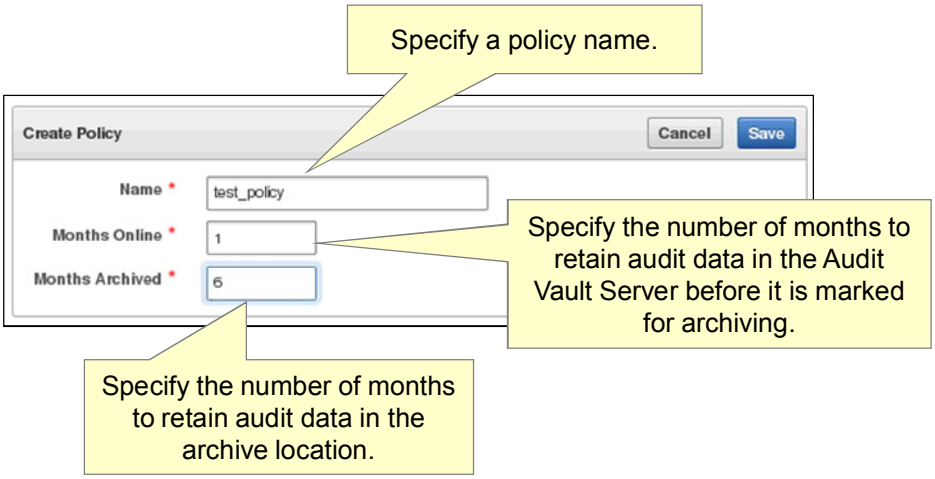
- Remote Filesystem: Select an existing filesystem or one will be created automatically based on the details of this archive location.
- Export Directory: Specify the NFS server's export directory.

Note: In AVDF 12.1.2, data files are first copied to a staging area in the Audit Vault Server when you select Secure Copy (scp) or Windows File Sharing as the transfer method. Ensure that there is space in the file system or the copy may fail.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating Archiving Policies



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

On the Create Policy page in the Audit Vault Server console, you can create an archiving policy by specifying the following information:

- Policy name: Provide a name for the archiving policy
- Months online: The number of months that audit data will be retained in the Audit Vault Server before it is marked for archiving. After this time, the data will no longer appear in reports.
- Months archived: The number of months that audit data will be available to be restored in the Audit Vault Server. This value does not affect the actual storage of the data in the archive location.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring the Email Notification Service

- Configure an SMTP server to enable email notifications for alerts and reports.
- Specify the following:
  - The IP address of the SMTP server
  - The SMTP server port
  - User name to be used as the sender of the email
  - The sender's address that appears in the email notifications
  - If required, username and password for the SMTP server
  - If required, authentication protocol

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You can configure email notifications so that messages are sent when alerts or reports are generated. Typically, the Audit Vault and Database Firewall auditor configures the email notifications, but the administrator must first configure a Simples Mail Transport Protocol (SMTP) server. You can configure one SMTP or ESMTP server for each installation of Oracle AVDF.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Which of the following Audit Vault Server administrators has access to all secured targets and secured target groups?

a. Administrator
b. Super Administrator

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Configure administrative accounts for the Audit Vault Server
- Specify the server date and time settings
- Set or change the Audit Vault Server network configuration
- Configure or change the Audit Vault Server services
- Configure the Audit Vault Server Syslog destinations
- Configure archive locations and retention policies
- Describe how to configure the email notification service

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 4

- 4-1: Creating Audit Vault Server Administrative Users
- 4-2: Verifying the Server Date and Time Settings
- 4-3: Verifying the Audit Vault Server Network Configuration
- 4-4: Verifying the Audit Vault Server Services
- 4-5: Configuring syslog Messages
- 4-6: Defining an Archiving Location
- 4-7: Creating Archive Policies

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In the hands-on practices for this lesson, you perform the following tasks:

- Create an Audit Vault Server administrative account.
- Verify the settings for the server date and time.
- Verify the Audit Vault Server network configuration.
- Verify that the Audit Vault Server services are configured appropriately for your needs.
- Configure syslog messages that will be sent from the Audit Vault Server.
- Define a location for archiving.
- Define the archiving policy.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

5

Configuring Oracle AVDF and Deploying the Audit Vault Agent

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Register the host computers where you will deploy the Audit Vault Agent
- Deploy and activate the Audit Vault Agent on the registered hosts
- Create user accounts on your secured targets for Oracle AVDF
- Register the secured targets with the agent in the Audit Vault Server
- Configure audit trails for the secured targets
- Configure stored procedure auditing

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

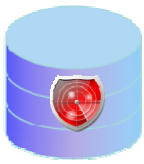
Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Deploying and Activating the Audit Vault Agent on Host Computers

Deploying and activating the Audit Vault Agent on a host machine consists of these steps:

1. Registering the host computer
2. Deploying the Audit Vault Agent on the host computer
3. Activating and starting the Audit Vault Agent



ORACLE

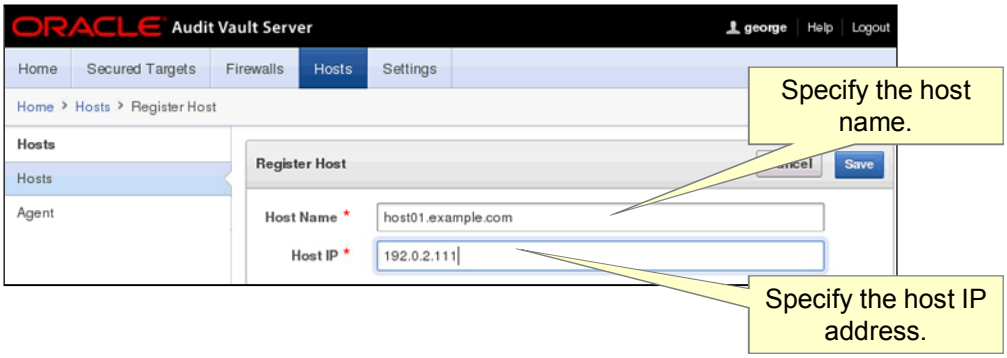
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To collect audit trail data from secured targets, you must deploy the Audit Vault Agent on a host computer, usually the same computer where the secured target resides.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Registering Hosts in the Audit Vault Server



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must configure a connection between the Audit Vault Server and the secured target host machine to enable audit data collection.

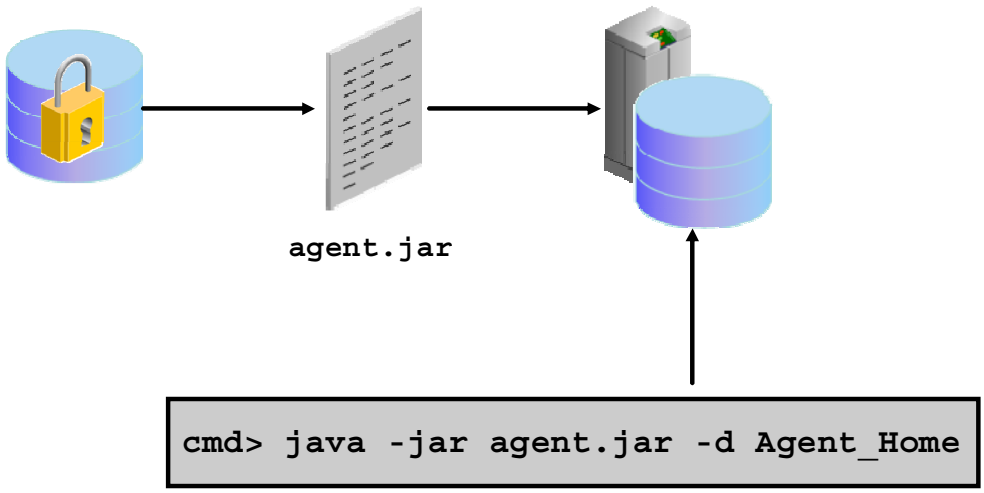
To register a host, log in to the Audit Vault Server console as an administrator and click the Hosts tab. Click register and enter the host name and host IP address.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Deploying the Audit Vault Agent on the Host Computer

Copy the `agent.jar` file from the Audit Vault Server and deploy this file on the host machine.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Perform the following steps to deploy the Audit Vault Agent on the host computer:

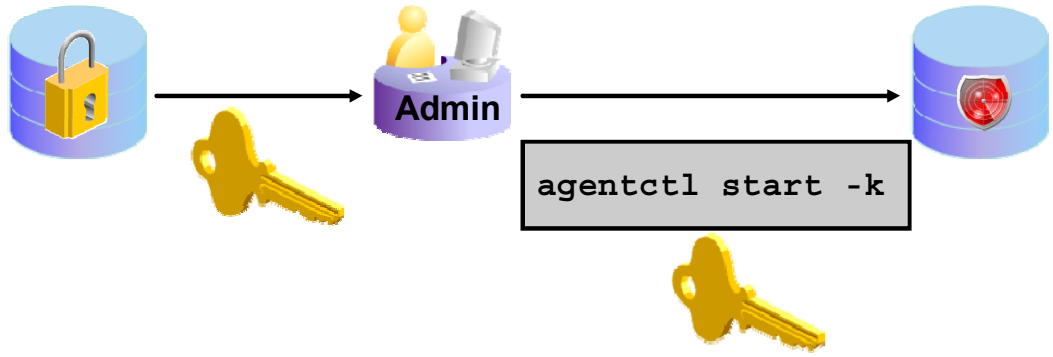
1. Log in to the Audit Vault Server console as an administrator.
2. Click the Hosts tab. Click Agent in the Hosts menu.
3. Click Download next to the Agent file. Save the `agent.jar` file to a location of your choice.
4. Using an operating system account, copy the `agent.jar` file to the secured target's host computer.
5. On the host machine, set `JAVA_HOME` to the installation directory of the jdk1.6 (or higher version), and make sure the Java executable corresponds to this `JAVA_HOME` setting.
6. Extract the agent by using the following command: `java -jar agent.jar -d Agent_Home`

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Activating and Starting the Audit Vault Agent

In this step, you activate the Audit Vault Agent with the Agent Activation Key and start the Agent.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Perform the following steps to activate the Audit Vault Agent with the Agent Activation Key and start the Agent:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the Hosts tab.
3. Note the Agent Activation Key for this host.
4. On the host machine, execute the following command to change to the `Agent_Home/bin` directory:

   ```
   cd Agent_Home/bin
   ```

5. Execute the following command and provide the Agent Activation Key when prompted:

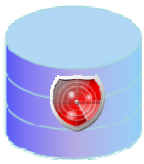
   ```
   agentctl start -k
   ```

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Registering the Audit Vault Agent as a Windows Service

- During agent deployment on a Microsoft Windows host computer a Windows service named OracleAVAgent is automatically registered.
- To manually register the Audit Vault Agent, execute the `agentctl registersvc` command from the `Agent_Home/bin` directory on the host machine.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

When the Audit Vault Agent is deployed on a Microsoft Windows host computer, a Windows service named OracleAVAgent is automatically registered during agent deployment. You can also register and unregister the agent service by using the `agentctl registersvc` command.

On the host machine, execute the following command from the `Agent_Home/bin` directory to register the Audit Vault Agent as a Windows Service:

```
agentctl registersvc
```

You can start or stop the service through the Windows Services applet in the Windows Control Panel.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Specify the correct order of the listed steps to deploy and activate the Audit Vault Agent on a host machine.

a. Deploy the Audit Vault Agent on the host computer.
b. Activate and start the Audit Vault Agent.
c. Register the host computer.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: c, a, b

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating User Accounts for Oracle AVDF

- Set up a user account with appropriate privileges on each secured target for Oracle Audit Vault and Database Firewall (Oracle AVDF) to use in performing functions related to monitoring and collecting audit data.
- Setup scripts are provided for database secured targets.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must set up a user account on each secured target for Oracle AVDF to use in performing functions related to monitoring and collecting audit data. Oracle AVDF includes setup scripts for a number of database secured targets.

The scripts set up user privileges that allow Oracle AVDF to do the following functions, depending on the type of target:

- Audit data collection
- Audit policy management
- Stored procedure auditing
- User entitlement auditing
- Database interrogation
- Audit trail cleanup (for some secured targets)

The setup scripts for user privileges are located in the following directory on the host computer on which you deployed the Audit Vault Agent:

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.secured_target_type/conf
ig/
```

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating User Accounts for an Oracle Database Secured Target

Perform the following steps:

1. Create a user account for Oracle AVDF on the Oracle Database.
2. Connect as **SYS** with the **SYSDBA** privilege.
3. Execute the following script to grant the necessary privileges:
   oracle_user_setup.sql <username> <mode>

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The setup script for an Oracle Database secured target is located in the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.oracle/config/` directory on Linux.

Create a user account in the Oracle Database and then execute the script to grant privileges:

```
@oracle_user_setup.sql <username> SETUP
```

`<username>` is the name of the user you created in the database.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating User Accounts for a Sybase ASE Secured Target

Perform the following steps:

1. Create a user account for Oracle AVDF in Sybase ASE with the username **avdf_sybuser**.
2. Execute the **sybase_auditcoll_user_setup.sql** script as follows:

```
isql -S server_name -U sa -P sa_password -i
sybase_auditcoll_user_setup.sql
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The setup script for a Sybase ASE secured target is located in the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.sybase/config/` directory on Linux.

To set up or revoke audit data collection privileges on a Sybase ASE secured target:

1. Create a user account in Sybase ASE with a username as `avdf_sybuser`.

   You will use the `avdf_sybuser` username and password when registering this Sybase ASE database as a secured target in the Audit Vault Server.
2. Execute the setup `sybase_auditcoll_user_setup.sql` script as follows:

```
isql -S server_name -U sa -P sa_password –i
sybase_auditcoll_user_setup.sql
```

Enter arguments as follows:

- `server_name`: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, omit the `-S server_name` argument.
- `sa`: Enter the system administrator username.
- `sa_password`: Enter the system administrator password.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating User Accounts for a Microsoft SQL Server Secured Target

Perform the following steps:

1. Create a user account for Oracle AVDF in SQL Server.
2. Execute the **mssql_user_setup.sql** script as follows:

```
sqlcmd -S server_name -U sa -P sa_password
-i mssql_user_setup.sql -v
username="username" mode="AUDIT_COLL"
all_databases="NA" database="NA"
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF setup script for a Microsoft SQL Server secured target is located in the `AGENT_HOME\av\plugins\com.oracle.av.plugin.mssql\config\` directory.

To set up Oracle AVDF user privileges for audit data collection, perform the following steps:

1. Create a user account for Oracle AVDF in SQL Server. You will use this username and password when registering the SQL Server database as a secured target in the Audit Vault Server.
2. Execute the `mssql_user_setup.sql` script as follows:

```
sqlcmd -S server_name -U sa -P sa_password -i
mssql_user_setup.sql -v username="username" mode="AUDIT_COLL"
all_databases="NA" database="NA"
```

The arguments are:

- `server_name`: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, omit the `-S server_name` argument.
- `sa`: Enter the system administrator username.
- `sa_password`: Enter the system administrator password.
- `username`: Enter the name of the user you created in step 1.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating User Accounts for an IBM DB2 for LUW Secured Target

Perform the following steps:

1. Create a new user account in DB2 to be used by Oracle AVDF for audit data collection.
2. Locate the **`db2_auditcoll_user_setup.sql`** script in the **`$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/`** directory and open it for editing.
3. Add the username of the account from step 1 to the **`grant`** statement and save the modified script.
4. Execute the modified script as follows:

```
db2 -tvf db2_auditcoll_user_setup.sql
```

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF setup scripts for a DB2 secured target are located in the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/` directory.

To set up Oracle AVDF user privileges for audit data collection, perform the following steps:

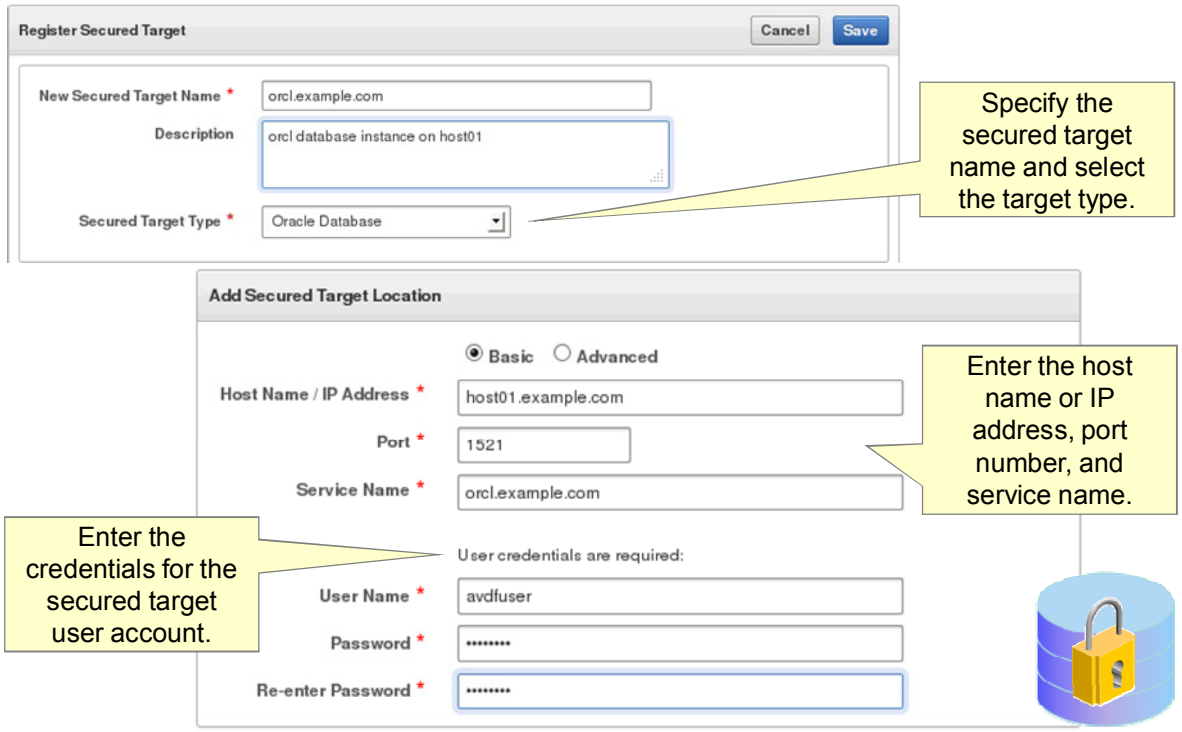
1. Create a new user account in DB2 to be used by Oracle AVDF for audit data collection. You will use this username and password when registering this DB2 database as a secured target in the Audit Vault Server.
2. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/` directory, locate the `db2_auditcoll_user_setup.sql` script and open it for editing.
3. In the grant statement in the script, enter the username for the user you created in step 1 and then save the modified script.
4. Execute the modified script as follows:

```
$> db2 -tvf db2_auditcoll_user_setup.sql
```

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Registering Secured Targets



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must register all secured targets in the Audit Vault Server, regardless of whether you are deploying the Audit Vault Agent, the Database Firewall, or both.

In Oracle Database 12*c*, if you are using a multitenant container database (CDB), you must register a secured target for the CDB, as well as each pluggable database (PDB).

If you know the exact connect string, you can click the Advanced radio button and enter the connect string in the Secured Target Location field. Refer to Appendix B in the *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information on secured target connect strings.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Audit Trails for Secured Targets

- On the Audit Trails page, specify the following to configure the audit trail:
  - Host computer where the Audit Vault Agent is deployed
  - Secured target's name
  - Audit trail type
  - Location of the audit trail on the secured target computer
  - Plug-in, if used
- After configuring the audit trail, start it on the Audit Trails page.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

So that Oracle AVDF can start collecting audit data, you must configure an audit trail for each secured target in the Audit Vault Server and then start the audit trail collection manually.

To start an audit trail, the Audit Vault Agent must be running on a host computer.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing

- Stored procedure auditing (SPA) enables Oracle AVDF auditors to audit changes to stored procedures on secured target databases.
- Enable SPA, by configuring the user account privileges necessary for Oracle AVDF, to perform stored procedure auditing on a secured target.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Stored procedure auditing (SPA) enables Oracle AVDF auditors to audit changes to stored procedures on secured target databases. Oracle AVDF connects to the database server at scheduled intervals and discovers any changes or additions that have been made to stored procedures. SPA is supported for all database secured targets supported by Oracle AVDF.

To enable SPA, configure the user account privileges by executing the setup script.

To set up Oracle AVDF user privileges, execute the setup script as follows:

```
oracle_user_setup.sql <username> SPA
```

`username` is the user you created for Oracle AVDF.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing for an Oracle Database Secured Target

Perform the following steps:

1. Create a user account for Oracle AVDF on the Oracle Database.
2. Connect as **SYS** with the **SYSDBA** privilege.
3. Execute the following script to grant the necessary privileges:
   oracle_user_setup.sql <username> SPA

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF setup script for an Oracle Database secured target is in the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.oracle/config/` directory.

To set up Oracle AVDF user privileges for SPA, execute the setup script as follows:

```
oracle_user_setup.sql <username> SPA
```

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing for a Sybase ASE Secured Target

Perform the following steps:

1. If you have not already done so, create a user account for Oracle AVDF in Sybase ASE with the username `avdf_sybuser`.
2. Execute the `sybase_spa_user_setup.sql` script as follows:

```
isql -S server_name -U sa -P sa_password -i
sybase_spa_user_setup.sql
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The script to set up user privileges for Oracle AVDF in a Sybase ASE secured target is located in the

`$AGENT_HOME/av/plugins/com.oracle.av.plugin.sybase/config/` directory.

To set up stored procedure auditing privileges on a Sybase ASE secured target, perform the following steps:

1. Create a user account for Oracle AVDF in Sybase ASE with the username `avdf_sybuser`. You will use the `avdf_sybuser` user and password when registering this Sybase ASE database as a secured target in the Audit Vault Server.
2. Execute the `sybase_spa_user_setup.sql` script as follows:

   ```
   isql -S server_name -U sa -P sa_password -i
   sybase_spa_user_setup.sql
   ```

   `server_name`: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, omit the `-S server_name` argument.

   `sa`: Enter the system administrator username.

   `sa_password`: Enter the system administrator password.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing for a Sybase SQL Anywhere Secured Target

Perform the following steps:

1. Log in to the database as a user who has privileges to create users and set user permissions.
2. Execute the **sqlanywhere_spa_user_setup.sql** script as follows:

```
isql -S server_name -U sa -P sa_password -i
sqlanywhere_spa_user_setup.sql -v
username="username" password="password"
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF setup scripts for a Sybase SQL Anywhere secured target are located in the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.sqlanywhere/config/` directory.

To set up or revoke stored procedure auditing for a SQL Anywhere secured target, perform the following steps:

1. Log in to the database as a user who has privileges to create users and set user permissions.
2. Execute the `sqlanywhere_spa_user_setup.sql` script as follows:

```
isql -S server_name -U sa -P sa_password -i
sqlanywhere_spa_user_setup.sql -v username="username"
password="password"
```

Specify argument values as follows:

- `server_name`: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, omit the `-S server_name` argument.
- `sa`: Enter the system administrator username.

Oracle University and Error : You are not a Valid Partner use only

- `sa_password`: Enter the system administrator password.
- `username`: Enter the name of the user you want to create for Oracle AVDF to use for SPA. Enclose this username in double quotation marks.
- `password`: Enter a password for the Oracle AVDF SPA user. Enclose the password in double quotation marks.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing for a Microsoft SQL Server Secured Target

Perform the following steps:

1. If you have not already done so, create a user account for Oracle AVDF in SQL Server.
2. Execute the **mssql_user_setup.sql** script as follows:

```
sqlcmd -S server_name -U sa -P sa_password
-i mssql_user_setup.sql -v
username="username" mode="SPA"
all_databases="Y/N"
database="NA/database_name"
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF setup script for a Microsoft SQL Server secured target is located in the `AGENT_HOME\av\plugins\com.oracle.av.plugin.mssql\config\` directory.

To set up or revoke Oracle AVDF user privileges for stored procedure auditing:

1. If you have not already done so, create a user account for Oracle AVDF in SQL Server. You will use this username and password when registering this SQL Server database as a secured target in the Audit Vault Server.
2. Execute the `mssql_user_setup.sql` script as follows:

```
sqlcmd -S server_name -U sa -P sa_password -i
mssql_user_setup.sql -v username="username" mode="SPA"
all_databases="Y/N" database="NA/database_name"
```

Enter arguments as follows:

- `server_name`: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, omit the `-S server_name` argument.
- `sa`: Enter the system administrator username.

Oracle University and Error : You are not a Valid Partner use only

- `sa_password`: Enter the system administrator password.
- `username`: Enter the name of the user you created in Step 1.
- `Y/N`: Enter Y if all databases should be audited for stored procedures. Enter N to specify one database name in the database parameter.
- `NA/database_name`: If you entered Y for `all_databases`, enter NA. If you entered N for `all_databases`, enter the database name that should be audited for stored procedures.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing for an IBM DB2 for LUW Secured Target

Perform the following steps:

1. Create a new user account in DB2 to be used by Oracle AVDF for stored procedure auditing.
2. Locate the **`db2_spa_user_setup.sql`** script in the **`$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/`** directory and open it for editing.
3. Add the username of the account from step 1 to the **`grant`** statement and save the modified script.
4. Execute the modified script as follows:

```
db2 -tvf db2_spa_user_setup.sql
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF setup script for a DB2 secured target is located in the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/` directory.

To set up Oracle AVDF user privileges for stored procedure auditing, perform the following steps:

1. Create a new user account in DB2 to be used by Oracle AVDF for stored procedure auditing. You will use this username and password when registering this DB2 database as a secured target in the Audit Vault Server.
2. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/` directory, locate the `db2_spa_user_setup.sql` script and open it for editing.
3. Enter the name of the user you created in step 1 in the grant statement in the script, and then save the modified script.
4. Execute the modified script as follows:

```
$> db2 -tvf db2_spa_user_setup.sql
```

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Stored Procedure Auditing for a MySQL Secured Target

Perform the following steps:

1. Log in to MySQL as a user who can create users and set user privileges.
2. Create a user for stored procedure auditing.
3. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/config/` directory, locate the `mysql_spa_user_setup.sql` script and open it for editing.
4. Modify the script to provide the same values for username, hostname, and password that you used in step 1.
5. Execute the `mysql_spa_user_setup.sql` script.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF setup script for a MySQL secured target is located in the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/config/` directory.

To set up or revoke stored procedure auditing for a MySQL secured target:

1. Log in to MySQL as a user who can create users and set user privileges.
2. Create a user for stored procedure auditing. You will use this username and password when registering this MySQL database as a secured target in the Audit Vault Server.
3. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/config/` directory, locate the `mysql_spa_user_setup.sql` script and open it for editing.
4. Modify the script to provide the same values for username, hostname, and password that you used in step 1.
5. Execute the `mysql_spa_user_setup.sql` script.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Register the host computers where you will deploy the Audit Vault Agent
- Deploy and activate the Audit Vault Agent on the registered hosts
- Create user accounts on your secured targets for Oracle AVDF
- Register the secured targets with the agent in the Audit Vault Server
- Configure audit trails for the secured targets
- Configure stored procedure auditing

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 5

- 5-1: Registering the Host
- 5-2: Deploying the Audit Vault Agent on the Host
- 5-3: Activating the Audit Vault Agent
- 5-4: Creating User Accounts on the Secured Target
- 5-5: Registering the Secured Target
- 5-6: Configuring an Audit Trail for the Secured Target
- 5-7: Configuring Stored Procedure Auditing

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

6

Networking and Oracle AVDF

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Describe the OSI seven-layer networking model
- Describe IPv4 addressing and routing
- Explain Oracle AVDF deployment models

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Seven-Layer Network Model: Overview

Open System Interconnect (OSI) provides a network model.

- Seven layers each defined by function.
  - Goal: Each layer is independent.
  - Method: Each layer encapsulates its data.
  - Actual: Certain protocol layers will only work with certain other protocol layers, neither Goal or Method is completely achieved.
- Other models have different number of layers.
  - TCP/IP has a four-layer model.
  - Other models map to the OSI model

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The OSI model is a conceptual or logical model of a communication system used today primarily as an educational tool. Actual protocol suites with implementation centered around OSI concepts can combine several layers into a single protocol. The implementations seldom have clear delineation of the layers or a pure application of the model. The OSI model has seven logical layers, numbered from one to seven. Layer one is the lowest layer. Each layer handles a specific function. The goal of this model is that the various layers are independent, so that one or more layers could be changed without changing the others. For example, Oracle Network Services provides a stack from layers five to seven that use transparent network services (TNS) to provide network services to the database. TNS works with a wide variety of popular network solutions. Layers one to four are typically provided by the OS and hardware vendors.

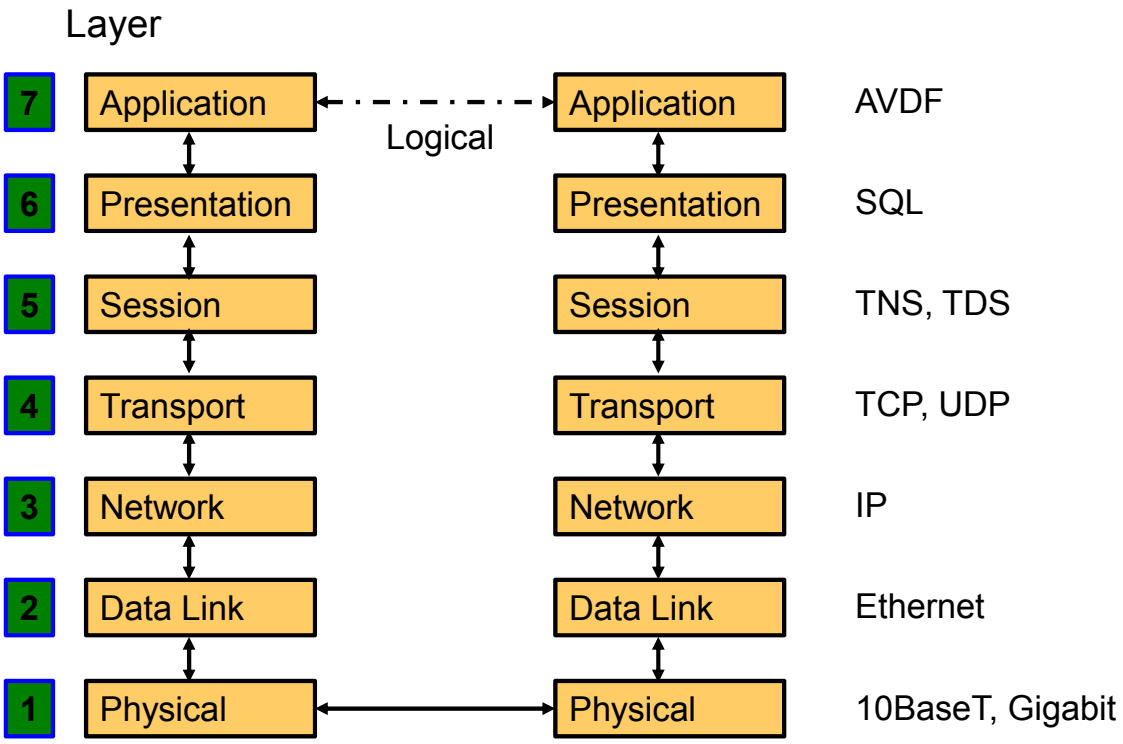
To reduce the interdependence, each layer encapsulates its data before passing it down the stack. A general principle is that each layer encapsulates its data and passes it to the next layer going down the stack until it is transmitted over the network. Upon receipt of the data from the network, each layer strips the encapsulation and formats the data for the layer above. These principles for isolating the functions of the layer are not applied uniformly.

Knowing the OSI model exists is very helpful in troubleshooting, and understanding the functioning and capabilities of the Oracle Database Firewall appliance.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Layer Processing



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Each layer “talks” to the same layer on a connected machine. Using Oracle Database and client communication as an example. The Oracle process uses the Oracle net services stack at layer seven. The client sends the SQL statement to layer six where it is transformed into bits, possibly a character set transformation, and encryption applied. Layer six passes the data payload to layer five, the session layer. A TNS session “talks” to a layer five TNS-enabled session on another machine. Layer five wraps data payload with the TNS protocol information and passes it to layer four. At layer four, the protocol layer creates packets from the data payload and wraps each packet with the Transmission Control Protocol (TCP) format. In TCP, the wrapper includes the source and destination information, sequence, flags, and options. Layer four passes the packets to layer three, which manages connections between different networks (implemented by routers) and encapsulates the packets into datagrams with IP addressing information and options. Then, at layer two connections between machines on the same network are managed. Layer two transforms the IP datagrams into Ethernet frames encapsulating them with Ethernet addressing information. Then to layer one, which handles the actual transmission.

When the frame is received the process is reversed, passing the payload up the stack to the appropriate application.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model
Physical Layer

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Manages physical connections
Electrical specification: pin arrangement, signal levels, wiring
Radio transmission: frequencies

Examples: 10Base-T, 1000Base-T, 802.11ac WiFi

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In the OSI model, layer one, the physical layer, handles the physical connection, that is the electrical or radio transmission of the data bits from one location to another. This includes the pin arrangement, cabling, and signal processing. Each layer provides a specific set of services to the layer above.

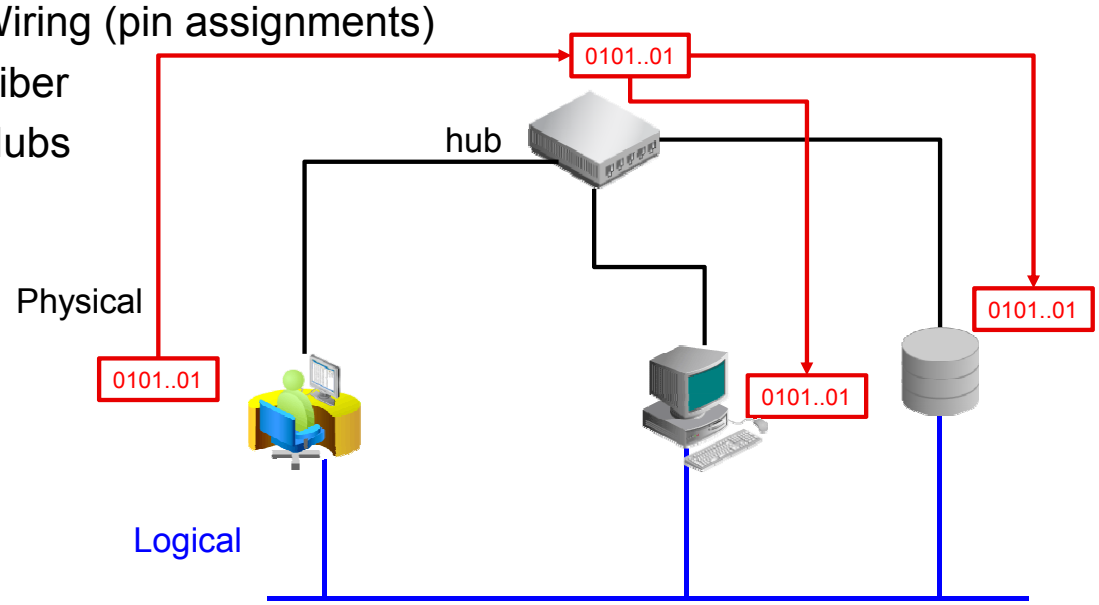
A layer one transmitter does the actual physical transmission of the Ethernet frames to a layer one receiver.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Physical Layer

- Electrical specifications
- Wiring (pin assignments)
- Fiber
- Hubs



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The OSI physical, layer one, and link, layer two, are closely related and in the case of Ethernet (IEEE 802.3) are implemented in hardware. The Ethernet interface card that you buy for your computer already has both layers built in. The physical layer will determine the type of cable, connectors, or fiber that you use. Ethernet is implemented in layer two of the OSI model. Ethernet is a family of standards that allow for an increasing number of physical implementations from the early coaxial cable, to the current cable specifications (including cat6, and fiber optic specifications).

An example of a network device that is only concerned with the physical layer is a hub. The purpose of the hub (repeater) is to receive a signal (frame) and echo the signal on all the connected ports (cables). The hub has no need to know addresses, routing information, or even that the signal is a frame. The signal is just a wave form that the hub faithfully reproduces. In network connected by hubs all the data frames are received by all the end point devices. In practical terms most wiring works best in a star configuration so the first physical implementations were implemented with a hub.

The logical model is a data bus. In this model, there has to be collision detection and resolution, every device has to be listening even while it is sending, and must have a way to resend when there is a collision (multiple devices sending at the same time). Additional collision resolution is provided by the link layer.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model
Data Link Layer

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Manages network segment connections
Manages connection between endpoints in one network segment. Implemented by switches, bridges.
In Ethernet, manages Ethernet frames, MAC address routing, and VLAN segmentation

Examples: Ethernet, FDDI

Addressing: MAC addresses, a8:bb:cf:14:ef:ea

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Data Link layer, two, or link, manages network segment connections in an Ethernet (IEEE 802.3) implementation by using media access control (MAC) addresses. The link layer wraps the network layer 3 datagram with the Ethernet frame information that includes the source and destination MAC address. The Ethernet (MAC) address works at this layer and each physical device in a Ethernet network has a unique MAC address.

Layer two is often closely related to layer one, as only certain data link specifications will work with particular physical specifications. For example: Fiber Distributed Data Interface (FDDI) software will not work with the 10BaseT cabling.

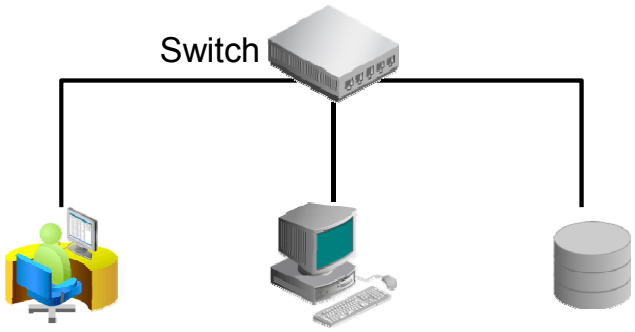
The link and physical layers are most often implemented in hardware together. Physical connections are seldom made directly between computer hosts, but have an intermediate device called a switch, or a hub. These devices receive and transmit Ethernet frames. A switch looks into the frame, finds the MAC address, and forwards the frame to the ports that are connected to the addressed endpoint. At power on, the switch acts like a hub, broadcasting the frames to all connected ports, but the switch learns the ports and connected MAC addresses. So after a short time the switch sends frames only to the ports with the attached MAC addresses.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Link Layer

- Provides basic network infrastructure
- Is composed of switches
- AVDF supports only Ethernet link-layer protocol
- AVDF NICs compatibility list exactly matches that of Oracle Linux 5.10



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The link layer of the OSI provides the hardware-level addressing and collision processing algorithms. This layer is aware of the MAC addresses of neighboring devices and handles packet collision and resolution. The early data bus model was not scalable. As the number of devices on the network grew the collisions grew exponentially.

The switch allows a much more scalable solution. A traditional switch operates at layer two, data link. The great advantage of a switch over a hub is that each port of the switch has to deal with only the collisions generated on that physical connection. If there is only one device, that device can take advantage of the full bandwidth and not share the bandwidth with all the other devices as with using the hub.

Note: Some modern switches include layer three (IP) functions implemented in hardware, with some packet examination to discover IP addresses and routing information.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Media Access Control (MAC) Addresses

- Identify physical end-point in a network segment
- Are globally (that is, world-wide) unique
- Are represented by six groups of two hexadecimal digits separated by hyphens (-) or colons (:) (for example, ‘a8-bb-cf-14-ef-ea’ or ‘a8:bb:cf:14:ef:ea’)
- Are used in Ethernet (OSI Link Layer) protocol

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

MAC addresses are the hardware endpoint identifiers used in the Ethernet protocol. The MAC addresses are assigned by manufacturers. The intent was that network devices could be plugged in, connected, and they would just work. The first 24 bits (three groups of hexadecimal digits) is the Organizational Unique Identifier that identifies the manufacturer. The following 24 bits (three groups) make up the device identifier. Although intended to be a permanent and globally unique identification, it is possible to change the MAC address on most modern hardware. Changing MAC addresses may be necessary in network virtualization.

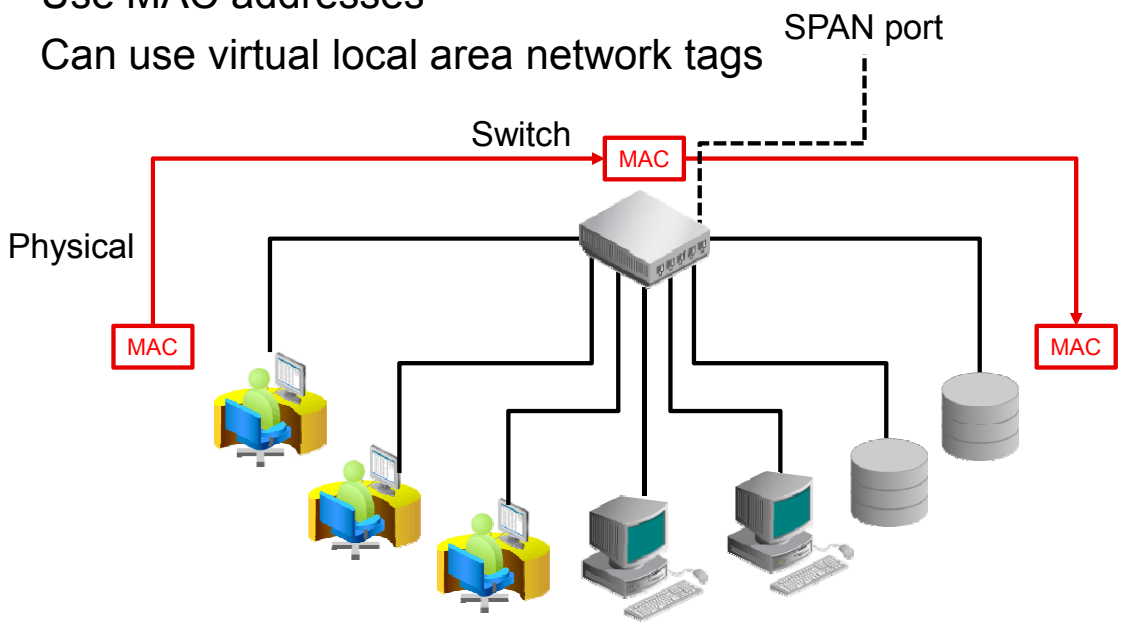
A host cannot determine from the MAC address of another host whether that host is on the same network segment as the sending host, or on a network segment bridged to that network segment. The network or subnet information is in the network layer (layer three) included with the IP address.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Switches

- Are layer 2 devices
- Use MAC addresses
- Can use virtual local area network tags



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

All Ethernet switches provide link layer MAC address routing, the Ethernet frame is examined, the destination MAC address is discovered, and the frame is sent to the port where that MAC address is known to be.

If the frame is a broadcast frame, the frame is repeated on all the ports.

A Switched Port Analyzer (SPAN) port or mirror port is a special port on a switch or a router that has specified traffic sent to it for analysis. This can be all the traffic or the traffic on specified ports. A SPAN port is normally configured to transmit only copies of traffic. The purpose is to allow a monitoring device to “see” all the interesting traffic.

Most switches can be configured to use virtual local area network (VLAN) tags. These tags are added at the first switch that is configured, and stripped off at the last switch ahead of the end point device.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Virtual Local Area Networks (VLANs)

- VLAN allows creation of multiple distinct logical Ethernet networks over one physical network.
- VLAN tags (numbers 0-4096) in Ethernet frames identify which logical network they belong to.
- VLAN tagging is used by switches to route traffic between themselves. Switches forward VLAN-tagged packets onto the corresponding VLAN-dedicated ports.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

VLAN is a layer 2 construct that allows the creation and separation of subnets without incurring the cost of a router. The concept is that a group of end point devices should be a part of a common broadcast group, and should be able to talk to each other without going through a router. This also implies a one-to-one relationship between the subnet IP address of the end points and the VLAN.

By default all ports connected by switches and bridges are in the same broadcast domain. That is, when a broadcast message is sent, every port of the switch receives the frame. Ordinary frames are routed to only the port where they are addressed by MAC address.

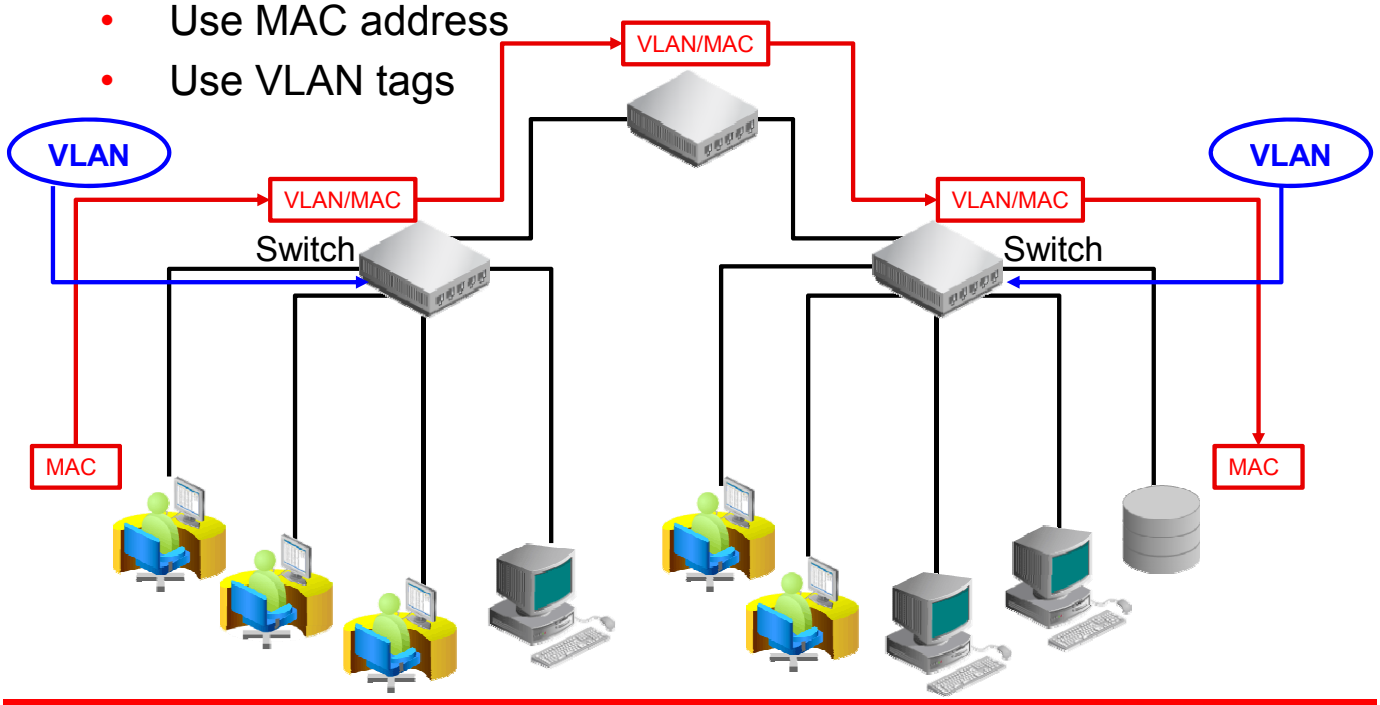
A VLAN is a software-controlled assignment of ports to a group. This group, a VLAN, segregates the ports of the group as if they were on a separate switch. In addition, a VLAN tag is added to the frame so that other switches can participate in the same VLAN. The benefit is an end point device can be in the same subnet but on a different, and possible geographically distant switch without having to use a router, and incur the overhead of examining layer 3 (IP) information in the frames. The danger is that there is no physical indication on the switch which ports are part of a VLAN, so a simple mistake in the wiring can stop the communication.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Switches with VLAN Tags

- Are layer 2 devices
- Use MAC address
- Use VLAN tags



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

With VLANs, ports on the switch are assigned to a VLAN. Each VLAN gets a tag. The tag is added to the Ethernet frame at the switch and stripped at the last switch in the path.

If the frame is a broadcast frame, the frame is repeated on all the ports belonging to the same VLAN.

This allows fast subnet switching without having to use routers. Only one VLAN is shown in the diagram.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

The set of bits sent as a message at layer 2 is called:

a. A datagram
b. A frame
c. A packet
d. A payload
e. A message

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model
Network Layer

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Manages network connections
Manages connection between hosts in different networks
Implemented by routers
Maintains IP routing tables
Provides address resolution
Sends and receives datagrams

Examples: IP, Ipsec, Appletalk

Addressing: IP address, 192.0.2.12

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The network layer, layer three, manages connections at the network level. Routers maintain the rules for routing packets between various networks at this level. In a TCP/IP stack, layer three turns packets into datagrams by wrapping the packet with IP address information to pass to layer two and layer three strips the IP information from the datagram to pass to layer four.

In the network layer, the datagrams are atomic and each datagram stands or fails on its own. Success or failure does not depend on previous or subsequent datagrams. The transport layer, four, is responsible for handling packets to handle acknowledgement, and resend failed transmissions.

Even though multiple protocols exist and are deployed, because IP is the most widespread protocol in use, IP will be the only protocol covered in this course. Internet Protocol version 4 (IPv4) is a standard that defines network addresses and is most widely used. This course concentrates on IPv4. A successor protocol, Internet Protocol version 6 (IPv6), has been defined and is in various stages of deployment.

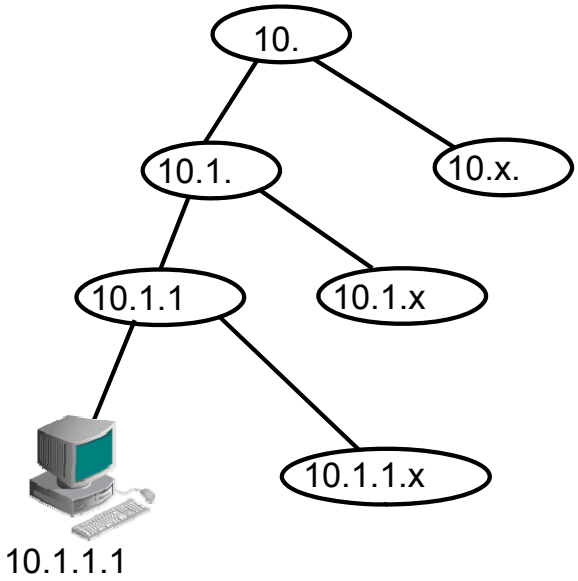
Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Layer 3 (Network)

Functions:

- Addressing
- Routing



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

OSI layer three is the network layer. The services provided at this layer are host addressing and routing. Routing is an important issue and any protocol that is successful must solve the problems of routing. IP is the most widely used protocol today. IP handles routing as a tree structure. The diagram in the slide shows a possible arrangement of subnets with a variety of prefix lengths. At the top, 10.xxx.xxx.xxx defines the entire network. At the next level, you could define 255 subnets, the first could be 10.1.xxx.xxx. At the next level, another 255 subnets. Then, at the bottom 253, individual network devices. The leading bits of the IP address provide the information needed to route the data packet to the proper subnet with the fewest number of hops. If the host at 10.1.1.1. wanted to connect to the host at 10.1.43.2, the packet would have to be sent up the tree (through routers) until a router or switch could send the packet down the 10.1.xxx.xxx branch, and again down the 10.1.42.xxx branch. The IP network specification is much more flexible than is shown in this simple diagram.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

IPv4 Addresses

- IP address identifies a network host.
- IPv4 address is usually represented by four sets of digits separated by dots (for example, 192.0.2.12).
  - The smallest number is 0 (leading zeros usually omitted).
  - The largest number is 255.
- IP address must be unique within a subnet.
- Oracle Audit Vault and Database Firewall (Oracle AVDF) uses only IPv4 addressing throughout.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

These protocols specify the addressing of networks and network hosts. The IPv4 address is 32 bits, and is usually represented by the “quad-dot” notation—four sets of digits separated by dots (for example, 192.0.2.12). The digits can range from 0 to 255 in each set. Leading zeros are allowed, but usually omitted. Addresses with the last set of bits set to all 1s (255) or 0s (0) are reserved for broadcast messages and subnet identifiers, respectively.

In IPv4, a subnet can be defined on a per subnet basis, using a specified number of the leading bits as a network identifier. The IP address for a network device must be unique within a subnet. Private networks (no connection to the internet) may use any IP address they want. There are address ranges reserved for private networks. These ranges are not routable, so they cannot conflict with other private networks. Internet-connected networks must apply for IP addresses. The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities.

Note: IPv4 addresses are exhausted, all new address assignments must IPv6. Many corporate sites use private IP address ranges, and then network address translation (NAT) for those services that must access the internet to extend the use of IPv4.

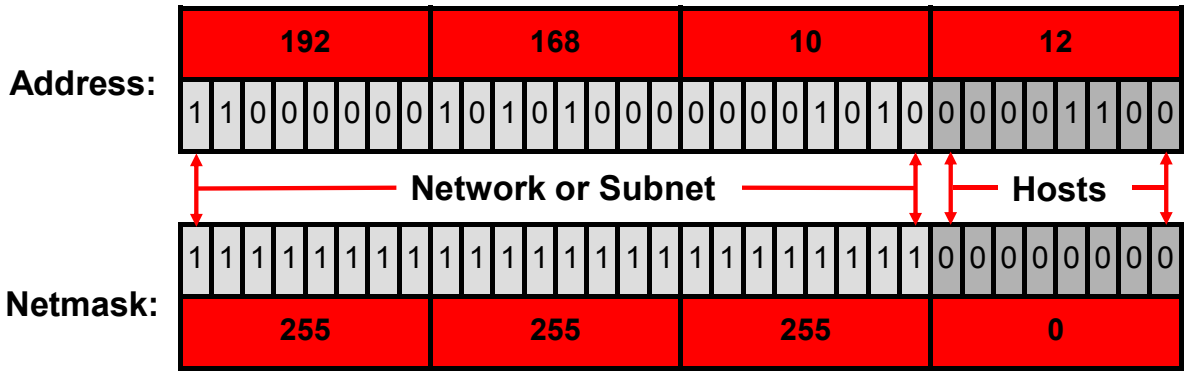
Oracle Audit Vault Database Firewall (AVDF) uses only IPv4 addressing throughout.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

IPv4 Subnets

- Each IP address identifies a network ID and a host ID.
- Subnets define sets of hosts, which can directly communicate with each other (within a subnet).
- A subnet is a range of IP addresses.
- Host configuration commonly requires “network mask” to identify which subnet the host belongs to.



ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To communicate on an IPv4 network without a router, the two network devices must have a physical or electrical connection, fiber, cable, or radio, and be assigned to the same subnet. A subnet is a range of IP addresses, identified by specified number of leading bits in the IP address.

To communicate with a different subnet a “gateway” node (IP address) must be specified that addresses a router or a bridge that connects to a path that includes the destination end point device.

In Linux when a device is initialized, usually the IP address and netmask are assigned. The netmask determines which bits are used for the network or subnet address, and which bits are used for the host ID on that network or subnet. For example, the network address 192.168.10.12 is on the 192.168.10.0 network when the netmask 255.255.255.0 is applied.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

IPv4 Subnets

- Subnets define sets of hosts, which can directly communicate with each other (within a subnet).
- A subnet is a range of IP addresses.
- Host configurations require a “network mask” to identify the subnet of the host.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To communicate on an IPv4 network without a router, the two network devices must have a physical or electrical connection, fiber, cable, or radio, and be assigned to the same subnet. A subnet is a range of IP addresses, identified by specified number of leading bits in the IP address. In what is known as a class C network, the first 24 bits determine the subnet. But in practice any number of leading bits can determine the subnet. A Class C network uses a netmask of 255.255.255.0 that indicates the first 24 bits are the subnet identifier, and the rest is the host identifier. In the Classless Inter Domain Routing (CIDR) notation, the same Class C address is specified by the lowest possible number in the subnet followed by ‘/’ and the number of bits in the subnet identifier (for example, 192.168.20.0/24 is a Class C subnet with 192.168.20 as the subnet identifier). The maximum number of bits in the subnet is 30, allowing only 2 bits, or 4 host addresses, 2^2. The minimum subnet identifier has 8 bits, and allows 2^24, or 16,777,214 host addresses.

To communicate with a different subnet a “gateway” node (IP address) must be specified that addresses a router or a bridge that connects to a path that includes the destination end point device.

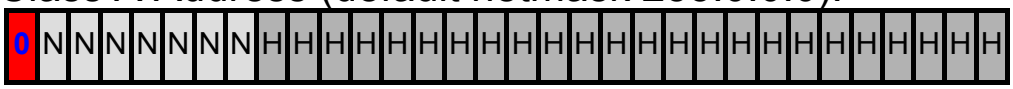
In Linux, when a device is initialized, the IP address and netmask are assigned.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

IPv4 Historical Class-Based Addressing

- Class A Address (default netmask 255.0.0.0):



  - 1 bit to identify class, 7 network ID bits, 24 host ID bits
  - Network IDs: $2^7 – 2 = 126$; Host IDs: $2^{24} – 2 = 16,277,214$
- Class B Address (default netmask 255.255.0.0):

  - 2 bits to identify class, 14 network ID bits, 16 host ID bits
  - Network IDs: $2^{14} = 16,384$; Host IDs: $2^{16} - 2 = 65,534$
- Class C Address (default netmask 255.255.255.0):

  - 3 bits to identify class, 21 network ID bits, 8 host ID bits
  - Network IDs: $2^{21} = 2,097,152$; Host IDs: $2^8 - 2 = 254$

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Historically, the IPv4 address space was divided into distinct classes of addresses. These classes used some the most significant bits to determine the class name: A, B, or C. Class A addresses required the first bit to be '0', followed by 7 bits to identify the network, and then followed by 24 bits to determine the host on the network. In Class A addresses, the network IDs consisting of all zeros and a zero followed by all ones were not allowed. This resulted in 126 valid network identifiers instead of 128. Class B addresses required the first two bits to be '10', followed by 14 bits to identify the network, and then followed by 16 bits to determine the host on the network. Class C addresses required the first three bits to be '110', followed by 21 bits to identify the network, and then followed by 8 bits to determine the host on the network. In all three classes, the available host ID space is reduced by two addresses. The host ID of all zeros does not identify a host and is reserved to identify the network itself. The host ID of all ones is reserved to be the broadcast address and refers to all hosts on the network.

The historical class based address space allowed for 2,113,662 total network addresses (126 + 16,384 + 2,097,152). The number of networks could be extended through custom subnet mask patterns. For example, if a company was assigned a Class B address and only had 4000 host devices to address, they could convert some of their most significant host ID bits into an extended network ID. This would convert the one network address assigned to the company into multiple network addresses with fewer hosts on each network.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Classless Inter-Domain Routing (CIDR)

Classless Inter-domain Routing (CIDR) deprecates the Class A/B/C network address assignment system.

- Assigns the network ID bits in a 32 bit IPv4 address explicitly
- Uses historical class-based notation followed by a slash '/' and the number of bits to use to identify the network ID segment (for example, 10.192.112.18/20)
- Allows assignment where Class B is too big (65,534 hosts) and Class C is to small (254 hosts)
- Maps device network address 10.192.182.18/20 into network ID 10.192.176.0 with netmask 255.255.240.0 and a broadcast address of 10.192.191.255

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Classless Inter-domain Routing (CIDR) replaces the class-based network address assignment system by removing the restrictions that the most significant bits be assigned specific patterns and allowing for any number of bits to be used for the network ID portion of the IPv4 address.

On many host systems, it is implemented by using custom netmask patterns. This can often result in the network address having a different prefix than the device's network address. It can also result in the broadcast address having a different prefix than the network address.

For example, consider the following network address by using CIDR notation:

(10.192.182.18/20)	Network Address CIDR notation
(00001010.11000000.10110110.00010010)	Bit format of 10.192.182.18
(**11111111.11111111.1111**0000.00000000)	Netmask for 20 bit network ID (/20)
(255.255.240.0)	Netmask decimal form
(00001010.11000000.1011**0000.00000000**)	Bit format network ID—host bits all zero
(10.192.176.0)	Decimal network ID format
(00001010.11000000.1011**1111.11111111**)	Broadcast Address—host bits all ones
(10.192.191.255)	Broadcast Address decimal format

Note: There are subnet calculators available on the internet to perform the calculations to identify the network address and broadcast address for a give IPv4 address and netmask.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

IP Version 6

Designed to replace IPv4

Not interoperable with IPv4

Requires a different network stack

Larger address space

- Address is 128 bits represented as eight groups of four hexadecimal digits
- Example: 4061:3db8:86a3:1253:605f:9a2e:0730:9234
- 64 bits for Network ID
- 64 bits for Host ID

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

IP version 6 (IPv6) is designed as replacement for IPv4, with a larger address space, a simpler routing algorithm, a different packet format, and simplified renumbering of networks. IPv6 is not designed to be interoperable with IPv4, and uses a different packet format to reduce amount of processing by routers. Most operating systems have both IPv4 and IPv6 network stacks available. The implementation of IPv6 is inevitable, but is progressing slowly.

IPv6 addresses are 128 bits, represented as eight groups of four hexadecimal digits separated by colons (for example, 4061:3db8:86a3:1253:605f:9a2e:0730:9234). Several methods of abbreviation of this full notation exist. Because many of the fields of an IPv6 address are currently zeroes, leading zeroes can be dropped, and consecutive all zero groups can be represented by a double colon (for example, 3098:0000:0000:0043:009a:0007:000f:0006 becomes 3098::43:9a:7:f:6). A double colon may be used only once in the address.

The major benefit of IPv6 is the much larger address space. IPv6 has 2^64 host addresses available in a single subnet, more than all of the IPv4 address space of 2^32 possible not counting the reserved numbers.

Note: AVDF has not implemented IPv6.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model
Layer 4

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Manages connections between processes on different hosts
Provides multiplexing by means of ports
Sends and receives packets

Examples: TCP, UDP

Addressing: IP:port e.g 1521

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Layer 4 is where port addresses are applied. Ports allow several applications to use a single IP address. Processes establish connections, or listen on different ports. Ports are assigned and must be unique, two processes cannot use the same port.

In these connections, the inbound and outbound connections often use different ports. In the case of an Oracle network session, a request for a session will contact the listener port, typically 1521, and a separate database server process will start using an available port in a assigned range. This port will be used for communication between the client and server until the session is ended (by actions in layer 5), and then released. This port is called an ephemeral port.

Note: Each IP address has a separate set of ports from 1 to 65535.

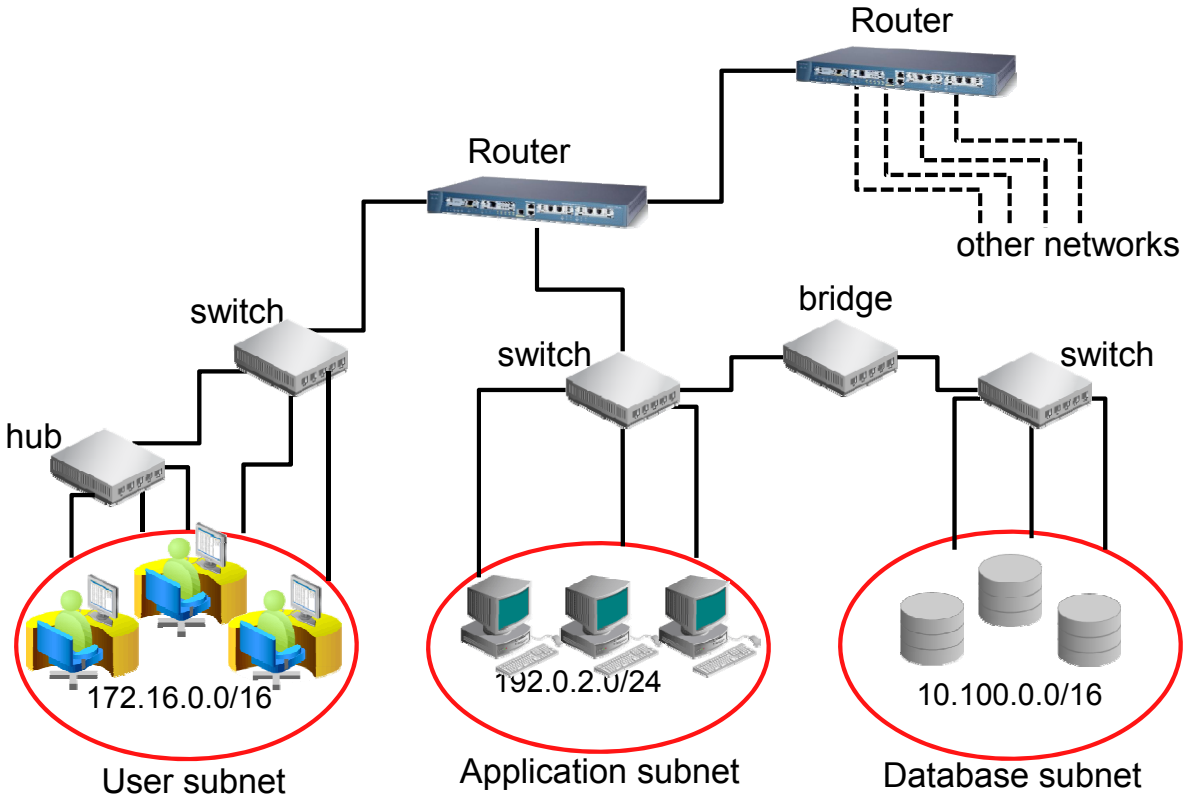
At layer 4, a session is opened, maintained, closed, and possibly reopened between the source and destination. The payloads are split into packets, packets are ordered, and packets are combined to reassemble the payloads. Each TCP packet gets a sequence number so that the receiving session can detect missing packets. Receipt of packets are acknowledged, and resend of packets can be requested. If one of the source or destination is much faster than the other, flow control can be employed to prevent overflowing input buffers.

Note: UDP protocol does not maintain ordering, or acknowledgement, so it is typically faster, but datagrams can be lost.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network Connections



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

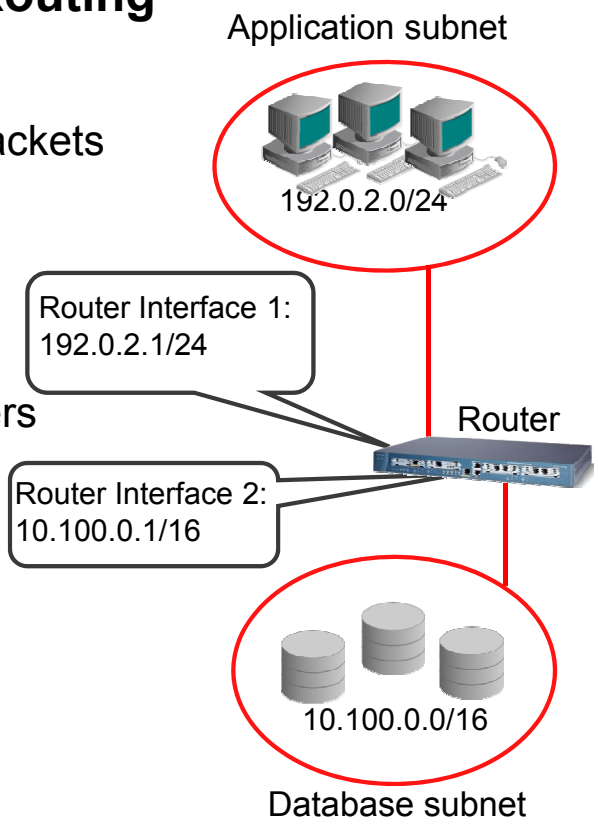
The physical connections in a network are designed to go through network devices that can transfer or route the signals to and from the source and destination: hubs, switches, bridges, and routers. The slide shows that packets originating in the user subnet must come through the application subnet to get to the database subnet. In a corporate environment, where all users connect to application servers to access the databases, this is a reasonable topology.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network Routing

- Hosts send “out-of-subnet” packets toward the gateway.
- Routers transfer packets between “gateway” interfaces for different subnets.
- There are often multiple routers between two TCP/IP session end points.
- End devices “know” only their own gateway.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

A host addresses a packet with the IP source and destination. If the destination is in the same subnet, the packet is sent through a port that connects to the subnet; that is, the port has the same subnet identifier as the destination. If the packet is going to a destination that is not on the same subnet, the packet is sent to a gateway. The gateway may be a router that has connections to both the source and destination networks.

The router may not have a direct connection to the destination, but it does have its own gateway node. Each router, including the gateway node, understands the network addressing hierarchy above and below itself. The route a packet takes to and from a destination can go through a large number of gateways.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Hostname Resolution

- IP protocol operates in terms of numeric addresses.
- IP addresses sometimes need to be changed.
- Datacenters use hostnames to identify IP-enabled “nodes” to avoid manual re-configurations.
- DNS servers provide centralized automatic look-up and maintenance of names-to-address mapping.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Host name resolution is the process that network protocols use to translate a hostname into an IP address. The hostname has not been mentioned with regard to the network stack because the hostname is not used to route the packets. TCP/IP protocol uses the numeric IP address.

IP addresses are not easy use to remember, so hostnames are used. The association between the hostname and IP address allows a two-way translation.

The simplest form of this translation is a file-based method where each machine on the subnet has a list of all the hostnames and IP addresses of the machines it will attempt communication. This can be very cumbersome to modify if any IP address on the network needs to change, is completely impractical for large networks, and impossible for internet access. A name resolution service known as Domain Name Service (DNS) is the standard method to find the mapping of hostname and IP address. A distributed repository of mapping files, managed by the DNS servers, provides the translation information. A local service at the end point queries a DNS server for the IP address for a hostname, or the hostname attached to an IP address. The IP hostname association is entered in one location and the DNS servers propagate this information as needed. Usually, each host has a list of one to three DNS servers that it can query for the IP information. By using DNS, the host only needs to know its own address, the default gateway, and the DNS server address.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Layer 4, the transport layer in the TCP protocol, provides which of the following services?

a. TCP packet ordering
b. Packet acknowledgement and re-transmission
c. Packet transformation into datagram
d. Packet assembly for layer 5 (session layer)
e. TCP address resolution into hostname

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a, b, and d

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model
Layer 5

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Manages sessions
Provides session functions open, close, restart, and link specifications

Examples: TCP,TNS, TDS variants

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Layer 5, the session layer, handles the opening, closing, and maintaining sessions. This layer in a TCP stack keeps the session state information.

ADVF has necessary libraries to understand Transparent Network Substrate (TNS) the Oracle proprietary networking protocol, Tabular Data Stream (TDS) the protocol used by Sybase and SQL Server, and TCP sessions.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model
Layer 6

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Transforms data between bits and application data format

Examples: SQL, XML, encryption

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Layer 6 handles transforming the bits in the payload, to and from the format the application layer understands. This is the layer that handles encryption, SQL, XML, and other data formats.

Note: You generally deploy Database Firewall between the database tier and application tier. The Database Firewall can decrypt traffic to and from an Oracle Database. For non-Oracle databases, if SQL traffic between the database tier and application tier is encrypted, the Database Firewall cannot understand or enforce protection policies on this SQL traffic.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

OSI Networking Model
Layer 7

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Application
Generates and consumes data transmitted to and from another host

Examples: AVDF, DNS, WWW

Addressing: Hostname, URL

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In the OSI model, layer 7 is the application layer, this is the layer where Oracle AVDF operates and other applications such as DNS, Browsers, NFS, and other network-based programs.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network Requirements

Universal Connectivity requires:

- Gateways and bridges
- Address resolution
  - Hostname to IP address
  - IP address to MAC address

High availability implies redundancy

- Fail pass network devices
- Multiple paths to each end point
- Routing must work with multiple paths

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Networks that we use and take for granted have some requirements that go beyond the original designs of the TCP/IP protocol. The possibility of a world-wide internet requires a connectivity between a multitude of subnets, and a reliability.

Connectivity, flexibility, and availability imply redundancy. Reliability requires multiple paths to subnets and end points, or a way to pass frames through a failed switch, or bridge.

A fail pass device, also called a by-pass network interface, will allow frames to “pass through” when the device is powered off. This configuration favors availability over security, because any policies implemented in the device will not be applied while it is powered down, and any network separation is negated.

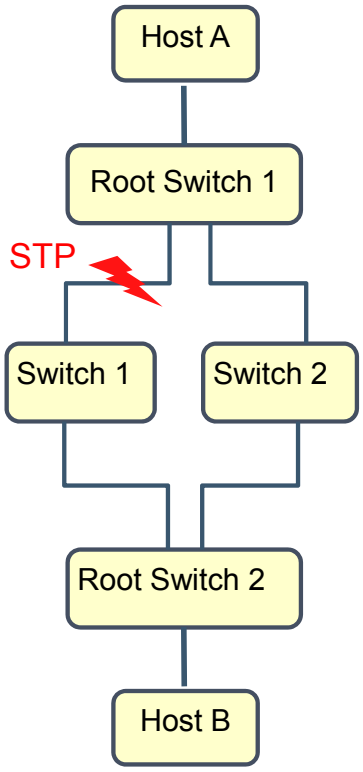
Multiple paths to an end point provides redundancy as long as the routing algorithms can find a single route. Multiple routes can create loops that are not allowed in TCP/IP networks.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Spanning Tree Protocol

- In complex networks with multiple paths to a destination, basic Layer 2 routing can fail with “broadcast storm.”
- Spanning Tree Protocol (STP) deals with this problem by shutting down all but one of the paths.
- If the primary path fails, a disabled path will be activated.



ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In larger networks, it is common to have multiple routes to a destination. This situation can arise by mistake, or intentionally, to provide redundancy. In either case, the layer 2 routing can fail or slow to unacceptable levels due to a “broadcast storm.” In a network without Spanning Tree Protocol (STP) enabled, as in the diagram, a broadcast packet transmitted by either root switch will be repeated on every port on switches 1 and 2, except on the incoming port. When the root switches see the same packet from a different source, they repeat it.

STP uses a special packet to discover all the possible paths to each destination in the network and a cost algorithm to choose a lowest cost path. STP then blocks or “disables” other paths so that there is a single path to each destination. Because there a several inputs to the cost algorithm there is no guarantee that the chosen path is the shortest or the fastest. The Network Administrator can manual adjust the costs.

The STP algorithm also continues to check the paths periodically so if the primary path fails one blocked path will be reactivated. This feature provides high availability.

STP operates at layer 2 by using MAC routing tables. Most switches include some version of STP.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

By-Pass Network Cards

- Allow traffic to traverse two physical ports when the appliance is powered down
- Are used to prioritize availability over security
- Are effective when single network path is used
- Do not work with STP
- AVDF supports Niagara by-pass network cards.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Conceptually, a by-pass network card will allow a network device to continue to pass signals through when it is powered down. This usually means that availability is more important than security for this device. The terms used to describe the network by-pass device are confusing: fail-open and fail-closed are both used to describe the behavior of the device.

A network by-pass device can be effective when there is a single network path and down-time is not acceptable. The security of subnet or database protected by this device may be compromised when the device is powered down.

When a bypass device is powered down, the bypass device maintains the path. Because the path to the MAC address is still intact, STP will not detect a different path is needed.

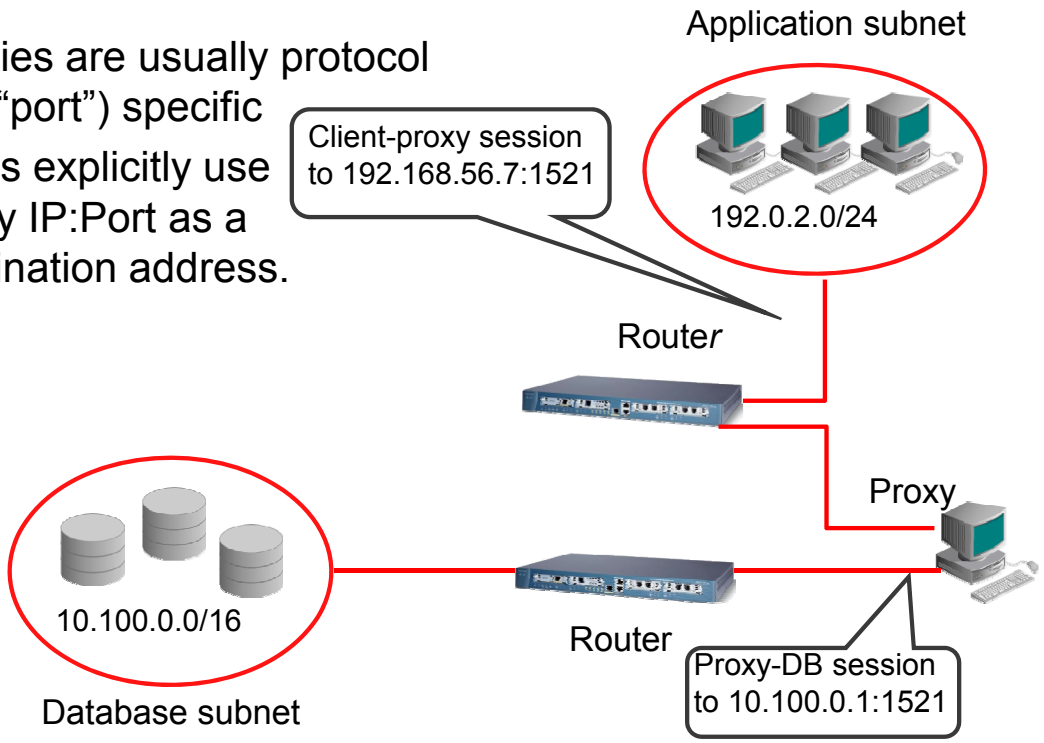
Note: Niagara by-pass network cards are supported by the Oracle Database Firewall appliance.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network Proxy

- Proxies are usually protocol (i.e. “port”) specific
- Hosts explicitly use proxy IP:Port as a destination address.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

A network proxy replaces a direct connection to a data source. A protected target address is replaced with a proxy address at the client. All network traffic to and from the protected target is routed through the proxy. The users are given the proxy address rather than the address of the protected target. A proxy is often used with multiple routers, the routers ensure all traffic to and from the target goes through the proxy.

A proxy is designed to allow only a particular application’s traffic and examines the application packets. Packets that are not related to the application are not passed through.

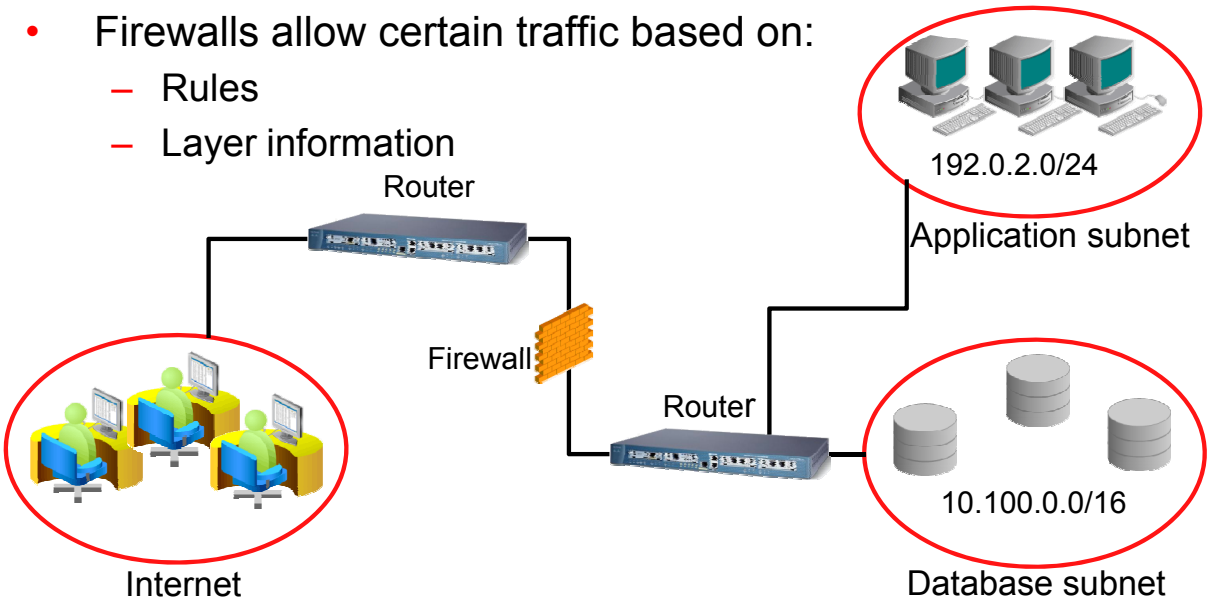
In the example shown, if there were a path from the application subnet to the database subnet without going through the proxy, the proxy protections could be defeated. The application proxies for mail, http, and database operate at the application layer 7.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network Firewall

- Routers are designed to allow traffic.
- Firewalls are designed to block traffic.
- Firewalls allow certain traffic based on:
  - Rules
  - Layer information



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

A firewall is a router that has been given a set of rules to control packet routing. A typical router allows all traffic originating from “inside” and denying all traffic originating from outside. A common router rule is that packets coming from a source that was previously a destination for a packet originating from the “inside” will be allowed from the “outside.” A firewall is placed inline so that all packets going to a protected destination must pass through the firewall. By default, a firewall denies all traffic. Rules must be added to allow traffic on specific ports or to and from specific IP addresses. Routers usually work at an IP address level layer 3, but application firewalls work at higher layers. Depending on the rules, and the layer at which the firewall is working, packets are analyzed, forwarded, dropped, or denied. Network firewalls typically apply the rules based on source and destination IP addresses blocking or allowing all traffic matching the rules.

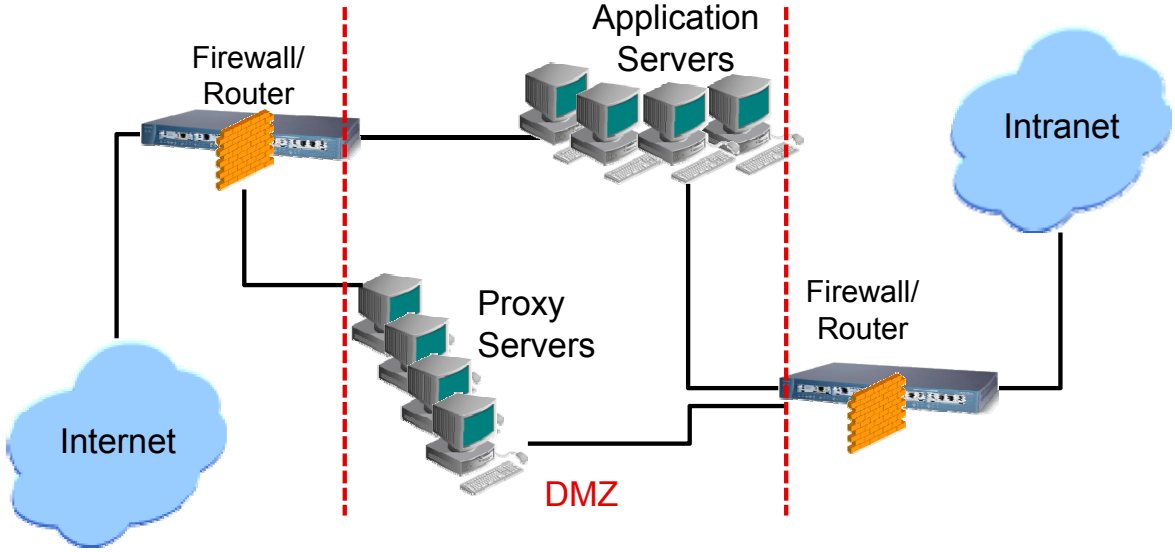
Application firewalls vary, some examining layer 5 application port information or higher layer information. The AVDF Database Firewall does deep packet analysis, looking at the payload SQL, which is application layer 7. The Oracle Database Firewall appliance analyzes the SQL payload inside the packets, but low level packets such as those generated by ping are ignored and passed.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network Protection Techniques

- Demilitarized Zone (DMZ)
- Firewall
- Proxies



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Three basic network protection techniques are the use of a demilitarized zone (DMZ), firewalls, and proxies. A DMZ is an area in a network that is typically placed between the internet and the intranet. It is assumed that there is no control over the activities on the internet. Any traffic that originates on the internet is suspected. The intranet is considered secure and traffic originating on the intranet is trusted. No traffic is allowed directly between the internet and the intranet. All traffic that moves between the two must pass through a proxy server. For applications, internet clients may access the application servers, but only the application servers may access the intranet. The rules in the firewalls enforce this access. In general, firewalls allow nothing, the firewall administrators have to create the rules allowing specific traffic.

The DMZ concept is frequently applied to the perimeter of a corporate network, to secure department networks, and to subnets with sensitive information.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Assume a DMZ for a corporate intranet with both application proxies and application servers. What are some reasonable rules to be implemented?

a. Pass packets originating in the intranet to internet.
b. Drop packets from internet responding the packets originating in the intranet.
c. Pass packets originating in the intranet to proxies, or application servers.
d. Pass packets from proxies going directly to the internet.
e. Pass packets from proxies going directly to the intranet.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b, d, e

A is false. Even though the intranet is trusted, applications (users) running in the intranet can inadvertently request hazardous pages from the internet.

C is false. While the intranet should communicate with proxies, there should be no reason intranet users need to use the application servers in the DMZ. These should be reserved for users coming in from the internet.

Note: A denied or blocked packet returns an error, a dropped packet produces no response and provides no information to the originator.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

AVDF Supported Protocols

Layer	Name	
7	Application	Oracle, MS SQL Server DB2 LUW , Sybase, MySQL
6	Presentation	SQL
5	Session	TNS (Oracle), TNS variants (MS SQL Server, Sybase, MySQL), DB2 LUW
4	Transport	TCP
3	Network	IPv4
2	Data Link	Ethernet
1	Physical	Copper wire, fiber, hubs, repeaters, span ports

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Inside the Oracle Database Firewall the network messages have to be processed through layer 6 for the SQL payload to be available. The various SQL variants are supported at layer 7.

The application or user data, “payload,” goes through processing sequentially. The Oracle Database Firewall processes the messages: layer 1 through layer 7 on the way “in,” the payload is examined, the policy applied, and then layer 7 through layer 1 on the way “out.”

Each payload is encapsulated by layer control information.

AVDF monitors and records relevant OSI layer control information alongside the payload in its audit repository.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle AVDF Deployment Models

The Oracle Database Firewall appliance may be deployed in three different configurations.

- Inline
- Out-of-band
- Proxy

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Database Firewall appliance has three configurations: Inline using an internal bridge to monitor and block SQL, Out-of-band using a single network interface for each SPAN port to monitor the SQL traffic, and Proxy using a single network interface and port for each protected target to monitor and block SQL.

Note: The Oracle Database Firewall appliance must have one network interface for use as the management interface. This interface should be different from the other network interfaces.

The inline configuration and proxy configuration can block or monitor SQL based on the policy. The Out-of-band configuration is limited to monitoring.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database Firewall Operational Modes

Operational Mode	Description
Database activity monitoring (DAM) (also known as monitoring mode)	The system detects and logs unusual activity. It produces warnings, but does not block potential threats. It can be implemented inline or out-of line.
Database policy enforcement (DPE) (also known as blocking mode)	The system detects and logs unusual activity. It produces warnings and blocks potential attacks. It must be inline.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

There are two operational modes for Oracle Database Firewall: Database activity monitoring (DAM) and Database policy enforcement (DPE).

DAM mode only monitors the SQL activity and does not block any SQL statements. In DAM mode, the Database Firewall makes a copy of the SQL statement and then applies the policy. Potential attack warnings can be generated in DAM mode. You will use the audit vault console as an auditor to develop a policy that specifies which statements to allow. Any statement that does not match the policy will generate a warning, but will be passed through to the database. When a new policy is put in place, it is recommended that the policy be used in DAM mode for a while to be sure that all normal SQL activity will be allowed and then change the operational mode to enforce the policy. This mode is also used to monitor for compliance.

Oracle University and Error : You are not a Valid Partner use only

DPE mode monitors the SQL activity and the Database Firewall will block SQL statements as specified in the policy. In DPE mode, the Database Firewall examines each SQL statement coming through the Database Firewall, applies the policy, and then forwards it to the database. Potential attack blocking can be enforced by developing a policy and setting the operational mode to database policy enforcement (DPE). In this mode, SQL statements will be blocked. Using the Firewall Analyzer to create the policy, you can categorize the statements into groups, and then assign actions to these groups. The actions specify which groups of statements should be passed through and which should be blocked.

For both modes, the level of logging is specified as part of the policy.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

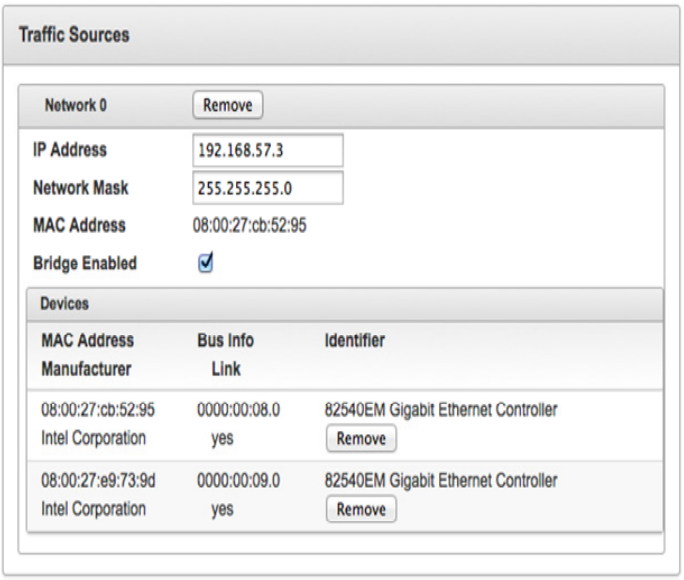
Database Firewall Bridge Configuration Basics

Inline deployment:

- Assign an IP address to the bridge.
- Do not assign IP addresses to the Ethernet interfaces.

Out-of-band deployment:

- IP address is not needed for bridge.
- IP address is not assigned to the Ethernet interface.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

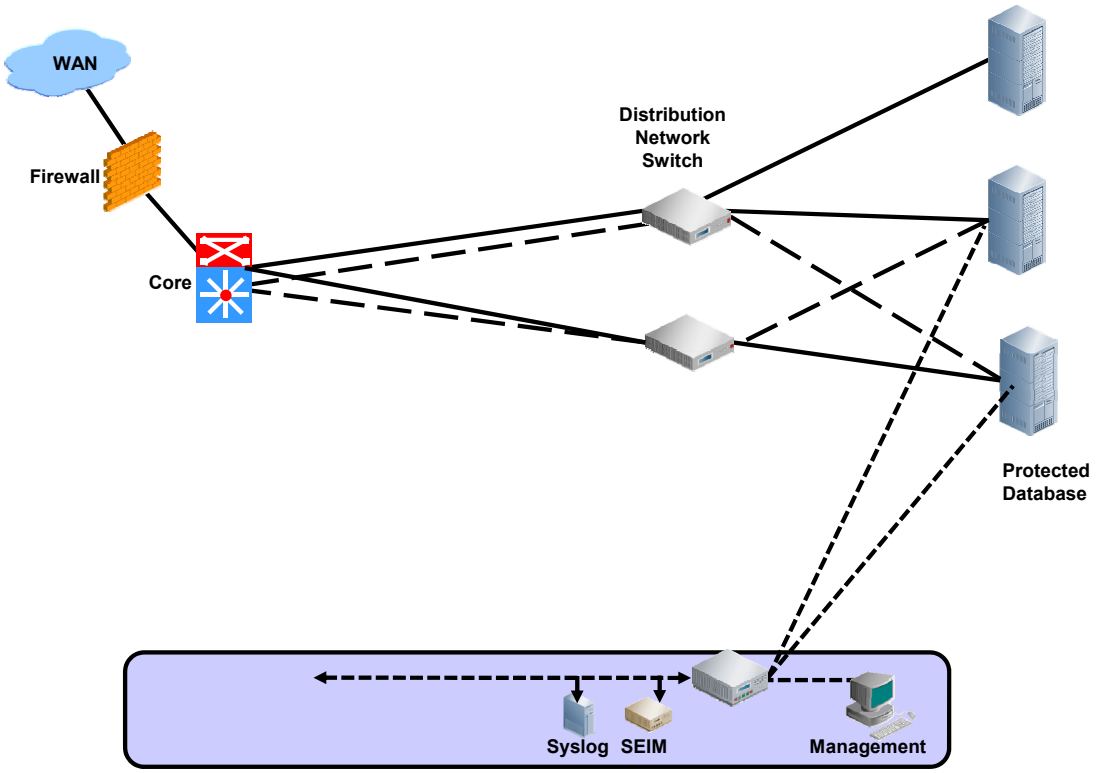
When the DBFW is deployed inline, each bridge requires an IP address and two Ethernet interfaces per bridge. The slide shows a configuration with a bridge and two devices assigned to the bridge. This configuration will place the DBFW between the protected database and sources of any SQL traffic in either DPE (monitoring and blocking) or DAM (monitoring only) mode. The bridge must be enabled before any traffic will be passed through the bridge.

In an Out-of-band deployment, the DBFW Ethernet interface is connected to a SPAN or mirror port on one or more routers/switches. The DBFW appliance monitors (DAM mode) all the traffic. The bridge may have an IP address assigned but it is not used. The bridge is not enabled, and only one Ethernet interface is required per SPAN port.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Basic Data Center Environment



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

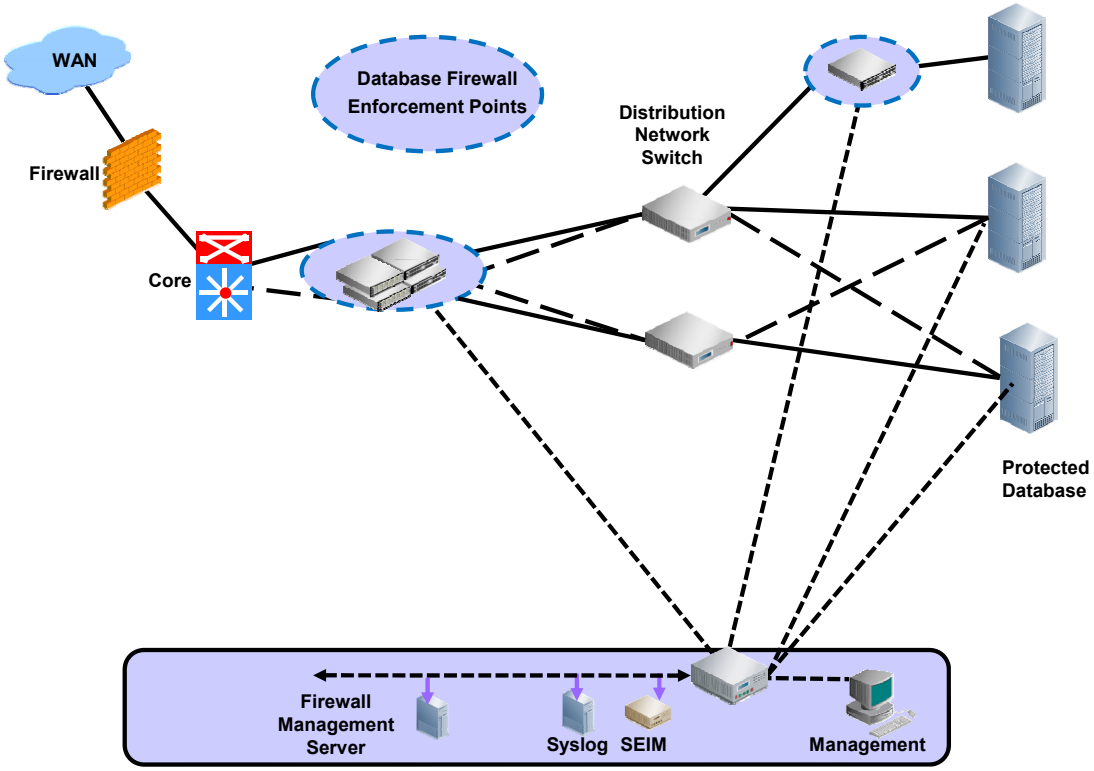
The diagram in the slide is a very simplified version of the data center showing an external firewall separating the internet from the intranet, a set of core network switches or routers, a set of distribution network switches, and a set of databases.

As is common in Data Centers, there are redundant paths to the protected databases. The management network includes syslog server and management nodes.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database Firewall Inline Deployment



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In this configuration, Oracle Database Firewall (DBFW) is deployed inline to protect all databases from traffic entering the data center. DBFW has one or more bridges. With an inline deployment, the SQL traffic is examined by the Oracle Database Firewall and inspected before it is forwarded to the database or blocked. This configuration is required for protecting the database from SQL injection and similar attacks using malicious SQL code.

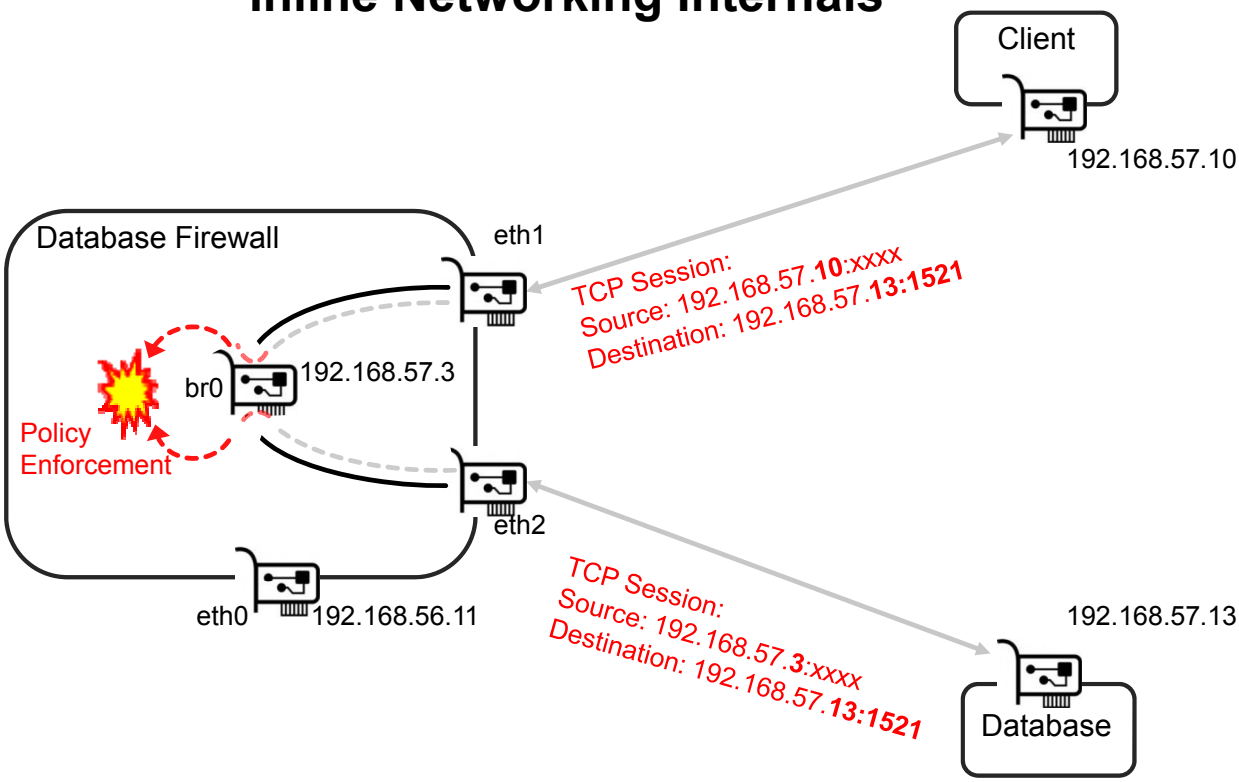
There are two possible placements for the Database Firewall shown in this diagram. You would choose one. The first places the Database Firewall between the core network switches and the distribution switches. This configuration may require multiple Database Firewall installations to allow enough network interfaces and enforcement points. The second configuration places the Database Firewall between the distribution network switch and each of the protected databases.

In both cases, the IP address of the bridge in the Database Firewall is the same as the subnet of the protected target. The number of bridges depend on the number of network segments to be protected, with two interfaces for each bridge. The number of Database Firewalls needed will depend on the number of interfaces and the total number of statements per second relative to the memory and processing power available.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Inline Networking Internals



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

With an inline configuration, the Ethernet devices are not assigned IP addresses, the bridge is assigned an IP address on the same subnet as the protected target.

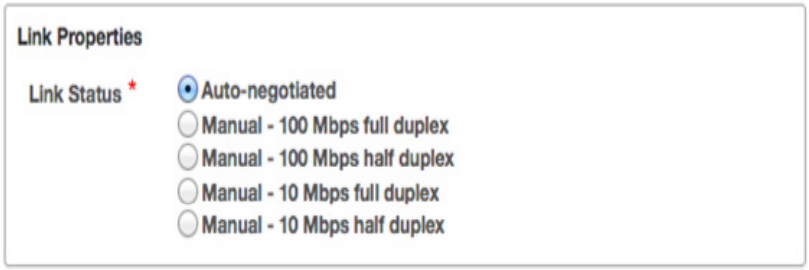
The DBFW appliance may be configured either for DAM mode or DPE mode. In DAM mode, the policy enforcement is limited to monitoring and alerting. When DPE mode is enabled, the traffic is examined and the policy is enforced, monitoring and blocking SQL statements. If the policy is “pass-all,” the result is the same as enabling DAM mode.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Audit Vault Server and Database Firewall Link Layer Settings

- Vast majority of networks use auto-negotiation. For these, the default auto-negotiated settings for Ethernet properties is the right one.
- Set manually only when auto-negotiation fails.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

With switches segmenting the traffic, almost all networks can run in full duplex mode at the full bandwidth of the network. Almost all Ethernet cards, switches and routers are capable of auto negotiation. The negotiated settings are the right ones to use.

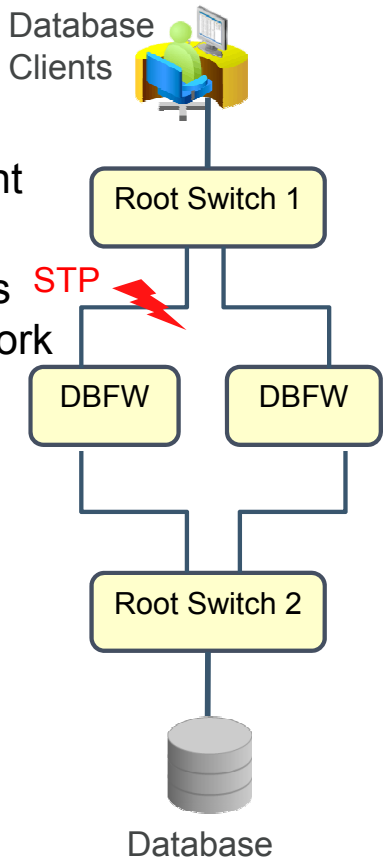
In the infrequent case that auto-negotiation fails, use the manual settings.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

AVDF Bridging

- Most real world networks provide redundant paths to Databases.
- Database Firewall "inline" deployment uses bridging to forward traffic between its network cards.
- Database Firewall works with STP and should be deployed in each path.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle DBFW firewall works with the redundant network paths in a data center. STP detects the redundant paths and disables all but one of them. If the enabled path ceases to function, STP will enable an alternate path. For the newly enabled path to maintain protection level, a DBFW appliance must be configured in that path.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Audit Vault and Database Firewall and VLANs

- In DAM mode, Database Firewall ignores VLAN tags and uses SQL payload as the basis of monitoring decisions.
- In DPE mode and inline configuration in a VLAN-enabled network, Database Firewall should be positioned at the last LAN segment “in front” of the database to avoid VLAN tags.

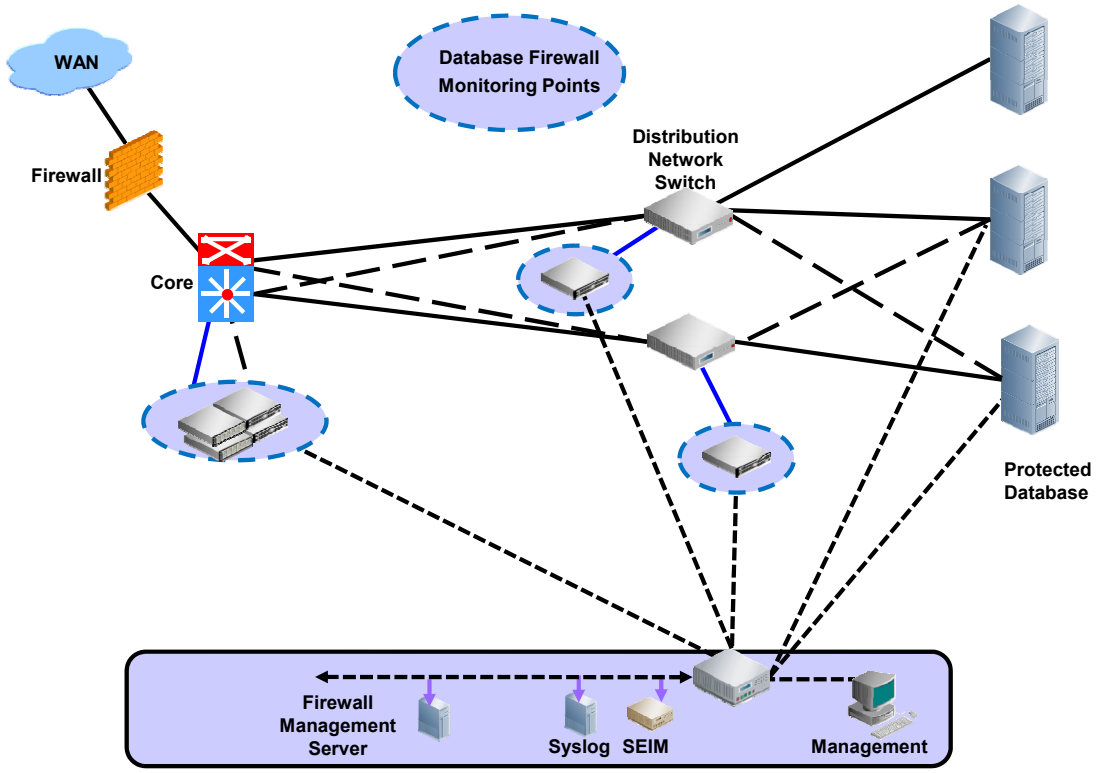
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The VLAN tags are stripped from the Ethernet frame in the last switch. If DBFW appliance is positioned between the last switch and the protected target, VLAN information will not appear in the frame.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database Firewall Out-of-Band Monitoring



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In this configuration, Oracle Database Firewall is deployed out-of-band to provide real-time monitoring, alerting, and reporting. With an out-of-band deployment, the SQL traffic is copied to Oracle Database Firewall usually by means of a SPAN port, while at the same time the SQL is sent directly to the database. Auditing can be provided for all traffic within the data center with this configuration. This configuration allows you to monitor SQL traffic for compliance. The Database Firewall can warn and alert for out-of-policy SQL statements, but cannot block SQL traffic in an out-of-band configuration.

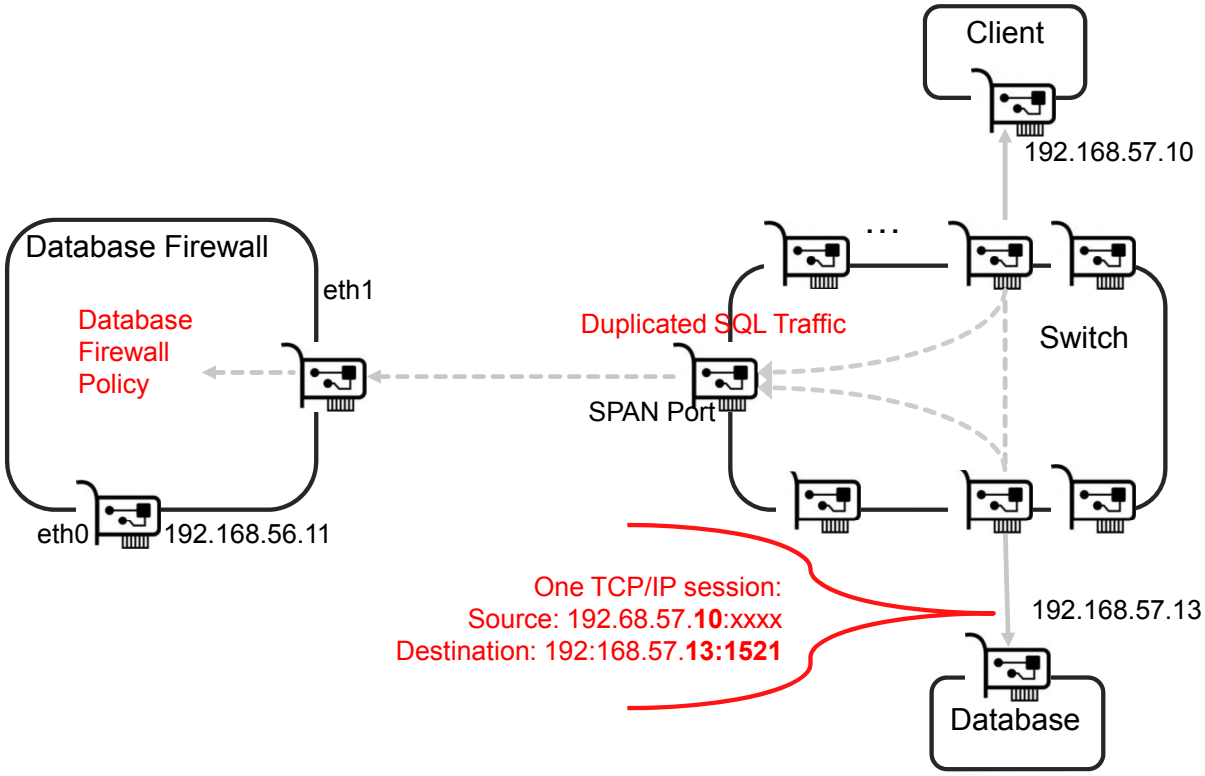
There are two placements for the Database Firewall shown in this diagram. Typically, you would choose one. The first places the Database Firewall on a bridged or SPAN port on the core network switches. This configuration may require multiple Database Firewall installations to allow enough network interfaces and enforcement points. The second configuration places the Database Firewall on a SPAN or bridged port of the distribution network switch for each of the protected databases.

Note: In the diagram, two DBFW appliances are shown attached to the two network switches. If practical, a single DBFW appliance with multiple Ethernet interfaces (one per switch) could monitor the traffic for both switches. But then the DBFW appliance becomes a single point of failure. If the appliance fails, the traffic monitoring for both switches would be lost.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Out-of-Band Networking Internals



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

When DBFW is deployed out-of-band, DAM mode is the only mode possible. The SQL traffic is sent directly to the database, and copies of the SQL traffic are sent to the DBFW appliance by way of a SPAN port.

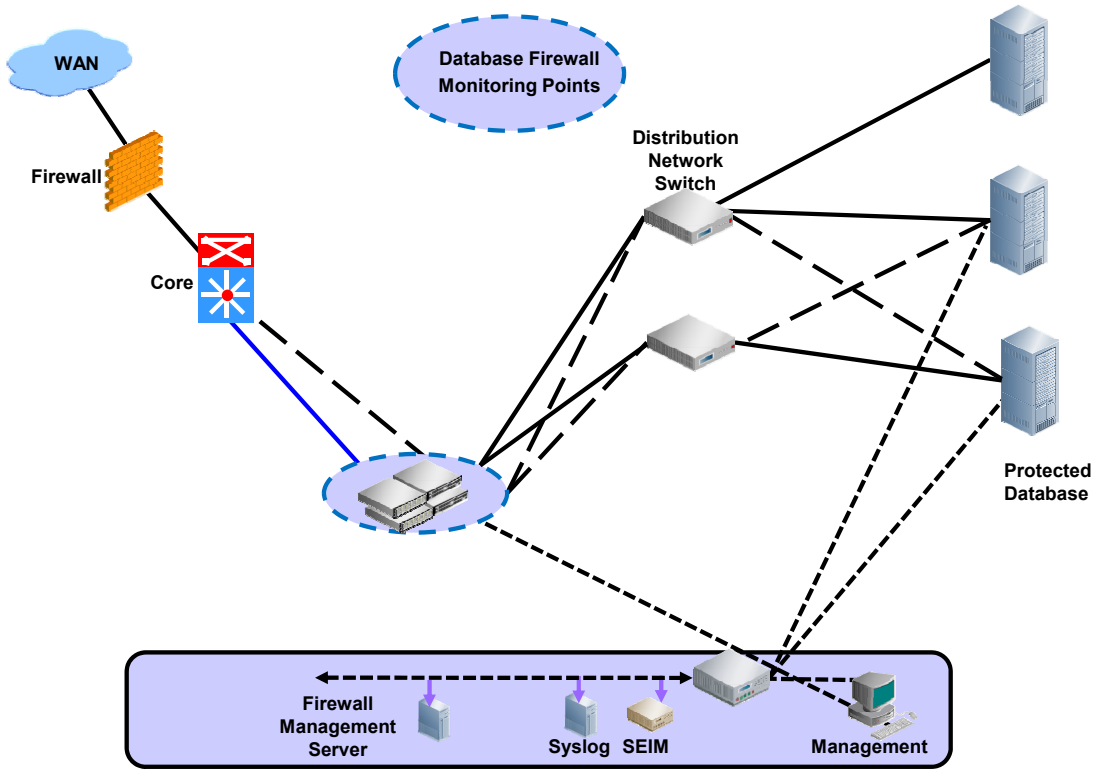
Note: The Ethernet port on the DBFW appliance does not have an IP address assigned.

The SPAN port is normally configured as an egress only port. The traffic goes out to the DBFW appliance and the DBFW never sends messages to the SPAN port.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database Firewall Proxy



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In this configuration, Oracle Database Firewall (DBFW) is deployed as proxies to protect all databases from traffic entering and leaving the data center. Multiple proxies can be configured in each DBFW. With a proxy deployment, DBFW is in DPE mode.

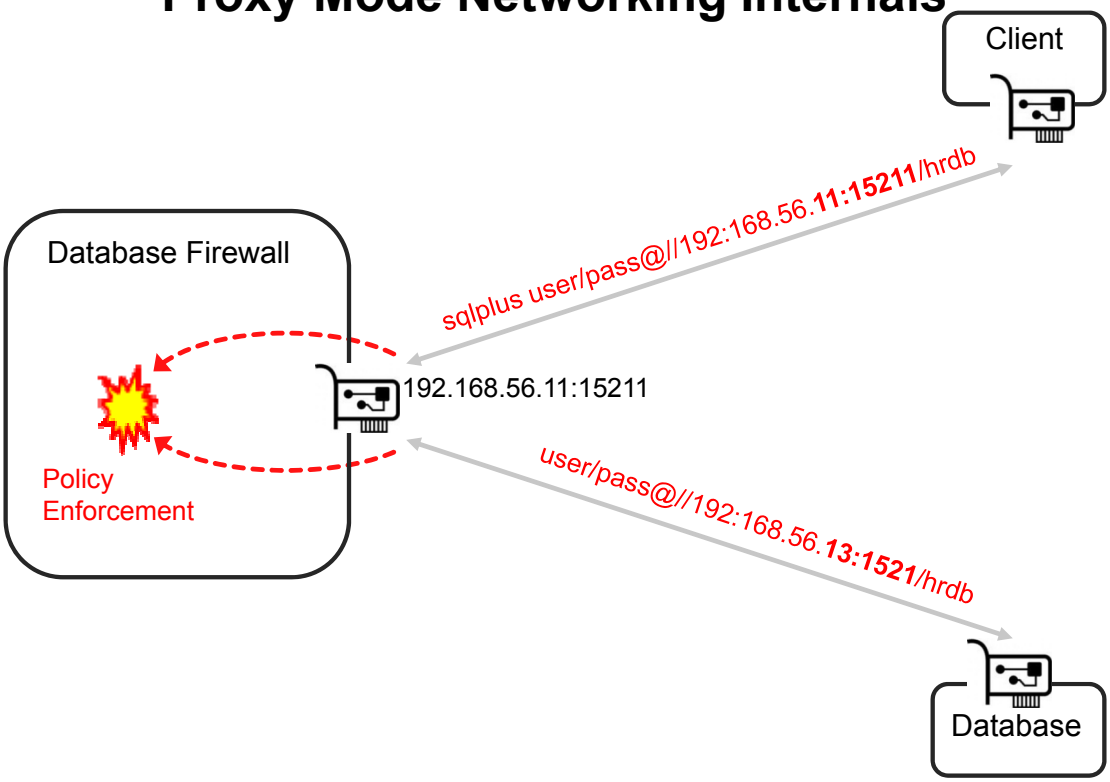
A possible placement for the Database Firewall is shown in the diagram in the slide. In a proxy configuration, the DBFW appliance is the end point for the clients, the enforcement point configuration forwards SQL that meets the policy rules to the protected target.

IP address of the proxy Database Firewall is different from the protected target, possibly a different subnet. The number of proxies configured in a single appliance depend on the number of targets to be protected. Each target requires a separate port number. Each Ethernet interface can support multiple enforcement points. The number of Database Firewalls is dependent on the total number of statements per second relative to the memory and processing power available.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Proxy Mode Networking Internals



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In proxy configuration, the DFBW must be in DPE mode. The client will be given the proxy IP address and port, but not the actual database IP and port. The enforcement point configures the DBFW proxy associating the proxy address and port with the protected database IP address and port.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Network Firewalls and Audit Vault and Database Firewall Deployment

- Corporate networks are usually sectioned by network firewalls only allowing specific traffic between zones.
- Audit Vault and Database Firewall components interact with each other and third-party enterprise systems.
- Open ports are required for Audit Vault and Database Firewall to communicate.
- Open ports are required for Audit Vault agent on secure targets to communicate with the Audit Vault server.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Best practice in corporate networks is to section the network into zones by function and access requirements and then allow specific traffic between zones.

The Audit Vault must be able to communicate with the management interface on the Database Firewall, and with the agent on the various secured targets. It is unlikely the secured target will be on the same segment, so ports have to be opened through the firewalls to allow communication between the various components.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

The Oracle Database Firewall may be deployed Inline, Out-of-band, or as a Proxy. What modes could you use with each?

a. Out-of-band with DPE, inline with DAM, and proxy with DPE
b. Out-of-band with DAM, inline with DPE, and proxy with DPE
c. Out-of-band with DAM, inline with DAM, and proxy with DAM
d. Out-of-band with DPE, inline with DPE, and proxy with DPE
e. Out-of -and with DAM, inline with DPE, and proxy with DPE

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b,e

- Out-of-band can only be deployed in DAM mode.
- Proxy can only be deployed in DPE mode
- Inline configurations may be deployed in either DPE or DAM mode.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

After completing this lesson, you should be able to:

- Describe the OSI seven-level networking model
- Describe IPv4 addressing and routing
- Explain Oracle AVDF deployment models

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 6

- 6-1: Configuring Database Firewall
- 6-2: Using Network Diagnostic Tools

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

7 Installing a Database Firewall

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- List installation requirements (hardware, software, and privileges)
- Describe network configuration requirements, including network interface cards (NICs)
- Install a Database Firewall and perform Database Firewall post-installation tasks

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Installation Requirements: Hardware

- Each Database Firewall requires an x86 64-bit server with:
  - 2 GB of RAM
  - Minimum 125 GB of disk space
- Hardware must support Oracle Linux, Release 5 Update 10.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Each Database Firewall is installed on its own dedicated x86 64-bit server. Your hardware must be compatible with Oracle Linux, Release 5 Update 10.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

NIC Requirements

- Before installation, ensure that the AV Server host can communicate with the Database Firewall hosts.
- Oracle recommends the following number of NICs for each x86 64-bit server on which you install the specified components:
  - At least one NIC for a Database Firewall operating as a proxy
  - At least two NICs for a Database Firewall in Database Activity Monitoring (DAM) mode (monitoring only)
  - At least three NICs for a Database Firewall in Database Policy Enforcement (DPE) mode (monitoring and blocking)

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Database Firewall must have one NIC for a management interface to the Audit Vault Server. This interface may also be used when the Database Firewall is configured as a proxy. An additional NIC is required for each stream that is monitored when the Database Firewall is configured in DAM mode. A stream corresponds to a span port that is being monitored. When the Database Firewall is configured in DPE mode, each stream requires two NICs. A stream corresponds to a secured target host. There may be multiple secured target databases on the same host using a single stream for communication.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Client Software Requirements

The following requirements pertain to the client machines, which will be used for the Database Firewall Console:

- Java SE version 6 or later for:
  - AVCLI command-line utility
  - AVPACK utility
- AVDF Administrator and Auditor GUIs support the following browsers:
  - Mozilla Firefox 14 or later
  - Microsoft Internet Explorer 8.0 or later
  - Google Chrome 21 or later
  - Apple Safari 5.0 or later
- Latest version of Adobe Flash plug-in to view charts and interactive reports

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The software requirements listed in the slide are applicable for the client machines, which will be used for management of the Oracle Audit Vault and Database Firewall components.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Ports for Services Provided by a Database Firewall

Port Number	Protocol Family	Protocol	Description
22	TCP	SSH	Command-line access (disabled by default)
161	UDP	SNMP	SNMP access (disabled by default)
443	TCP	HTTPS	Administration Console
2050-5100	TCP	AVDF internal protocol	Incoming traffic captured from Host Monitor
2050-5100	TCP	Syslog	Incoming WAF (F5 BIGIP) connection

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The table in the slide lists the ports that are used for general services provided by a Database Firewall.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Ports for External Network Access by a Database Firewall

Port Number	Protocol Family	Protocol	Description
53	UDP	DNS	Domain name service
123	UDP/TCP*	NTP	Time synchronization with external time servers
514	UDP/TCP*	Syslog	System and WAF (F5 BIGIP) alerts sent to syslog

*** TCP port is configurable through the Audit Vault Server console.**

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

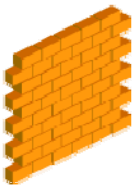
The table in the slide lists the ports for external services that may be used by a Database Firewall.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Installing a Database Firewall

- Reminder: A Database Firewall must be installed on its own dedicated server.
- Provide the following information during the installation:
  - An installation passphrase to be used again during post-installation tasks
  - The network interface to be used as the management interface
  - The IP address of the management interface
  - The network mask for the management interface
  - The gateway IP address for the management interface



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Database Firewall is an appliance. You must install it on its own dedicated server.

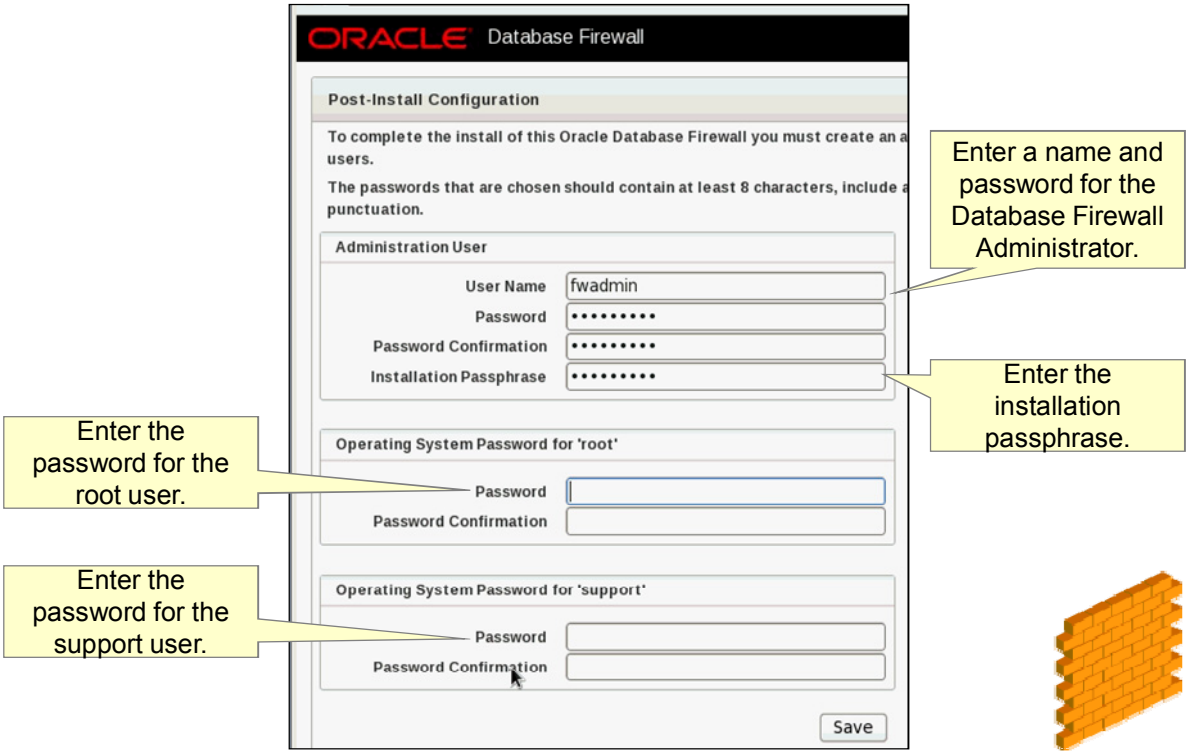
When you install the Database Firewall, you create an installation passphrase. You will use the installation passphrase for the post-installation configuration tasks. The installation passphrase protects the Database Firewall until you have completed configuration.

During installation, you supply information for the management interface.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Performing Database Firewall Post-Installation Tasks



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

After you install the Database Firewall, you must set the passwords of the administration user, root, and support user. The administration user is the web GUI user. Root and support users are the Linux system operating system user accounts on the Audit Vault Server machine.

Perform the post-installation tasks as follows:

1. Access the Database Firewall Console and enter the installation passphrase.
2. On the Post-Install Configuration page:
   - Enter a name and password for the Database Firewall Administrator
   - Enter passwords for the root and support users

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Each Database Firewall must be installed on a separate, dedicated x86 64-bit server.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

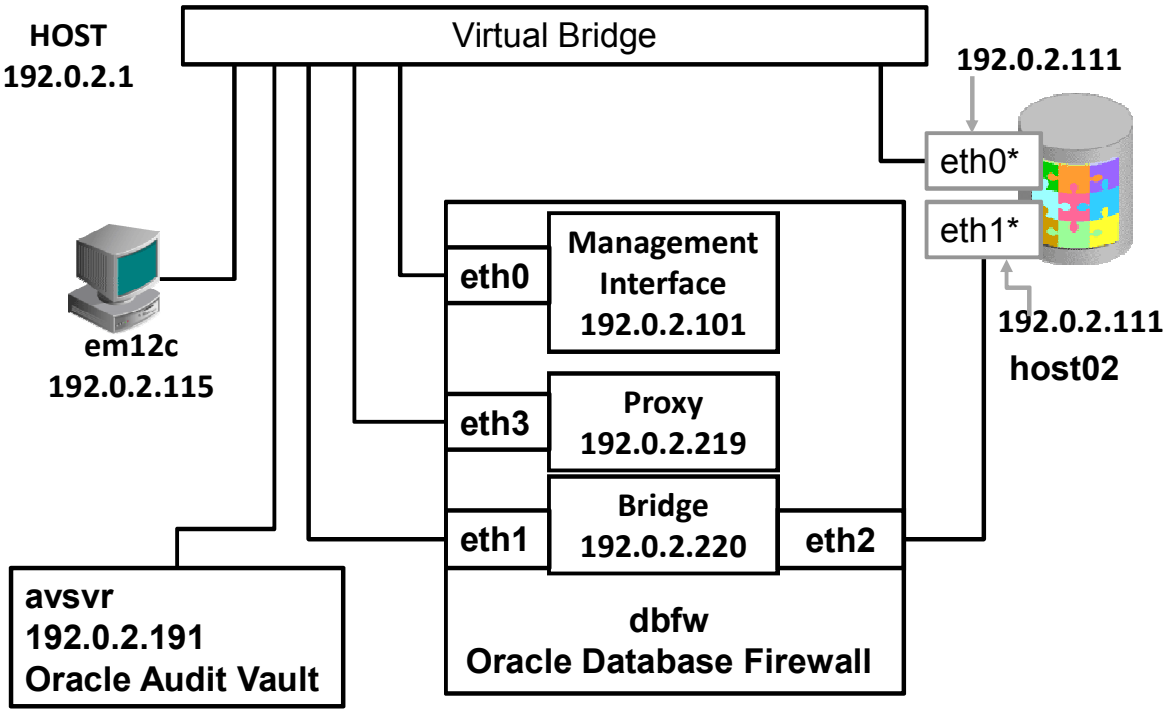
- List installation requirements (hardware, software, and privileges)
- Describe network configuration requirements, including network interface cards (NICs)
- Install a Database Firewall and perform Database Firewall post-installation tasks

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Understanding the Classroom Configuration



* **Note:** Only one of these interfaces may be active at any given time.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

There are four virtual machines in the classroom environment:

- em12c: The client machine
- host02: The database machine containing an Oracle Database 12*c* database
- avsvr: The Audit Vault Server appliance
- dbfw: The Database Firewall appliance

The host machine is the machine that contains the student desktop. You will connect to the virtual machines in your environment from here.

The database VM, `host02`, has two network devices that will use the same IP address. Only one can be active at any given time. The `eth0` device can connect to all the other VMs and will be used to demonstrate the traffic proxy configuration. The `eth1` device is connected to the Database Firewall `eth2` device and can communicate only with the `dbfw` VM.

The Database Firewall management link is set in the network configuration as part of the installation process. This is shown in the lesson titled "Deploying Oracle Database Firewall."

The bridge IP address is set to a default and is disabled by default on install. The IP address will be changed and enabled when you configure traffic sources in the Database Firewall Network Settings. Later, when the enforcement point is created, the connection between the `dbfw eth2` and `host02 eth1` will be specified in the Administration Console as shown in the practice titled "Configuring Enforcement Points."

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 7

- 7-1: Performing Database Firewall Post-Installation Tasks

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

8

Configuring Oracle AVDF and Deploying Database Firewall

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Configure the Database Firewall basic settings
- Associate each Database Firewall with the Audit Vault Server
- Configure the firewall on your network
- Register the secured targets with the Database Firewall in the Audit Vault Server
- Configure enforcement points for the secured targets
- Describe how to configure database interrogation
- Configure database response monitoring

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Basic Database Firewall Configuration

Basic Database Firewall configuration consists of four steps:

1. Configuring the Database Firewall's network and services settings
2. Setting the date and time in the Database Firewall
3. Specifying the Audit Vault Server certificate and IP address
4. Configuring Database Firewalls on your network

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To configure a Database Firewall, you will perform the steps listed in the slide.

Based on your overall plan for deployment of Oracle Audit Vault and Database Firewall (Oracle AVDF), you will make configuration choices for each Database Firewall's system and network settings.

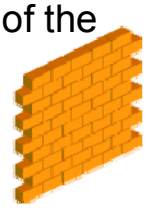
You must identify the Audit Vault Server that will manage each Database Firewall.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Basic Settings for Database Firewall

- Change or configure a Database Firewall's network settings: IP address, network mask, gateway, name
- Change or configure a Database Firewall's network services:
  - IP address of at least one DNS server on the network if you require translation of host names
  - IP addresses of computers that have web access to the Database Firewall administration console
  - IP addresses of computers that have secure shell access to the Database Firewall
  - IP addresses for access to the network configuration of the Database Firewall through SNMP



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Although the installer configures initial network settings for the Database Firewall during installation, you can change the network settings after installation.

You can also configure Database Firewall network services, which determine how users can access the Database Firewall.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring a Database Firewall on Your Network

Perform the following tasks as required to implement your planned network configuration:

- Configure traffic sources.
- Configure a bridge in the Database Firewall.
- Configure a Database Firewall as a traffic proxy.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

As part of planning the network configuration, you should determine whether to place Database Firewalls inline with traffic to your secured target databases, or out of band. You may also decide to use a Database Firewall as a traffic proxy. The network configuration is impacted based on whether the Database Firewall will operate in Database Activity Monitoring (DAM) or Database Policy Enforcement (DPE) mode.

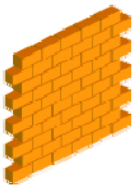
Additional information on each of these tasks follows in this lesson.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Traffic Sources

- *Traffic sources* specify the IP address and network interface details for the traffic going through a Database Firewall.
- Traffic sources are automatically configured during installation.
- You can change the following traffic source configuration information:
  - IP address
  - Network mask
  - Bridge
  - Network interface (network card)



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

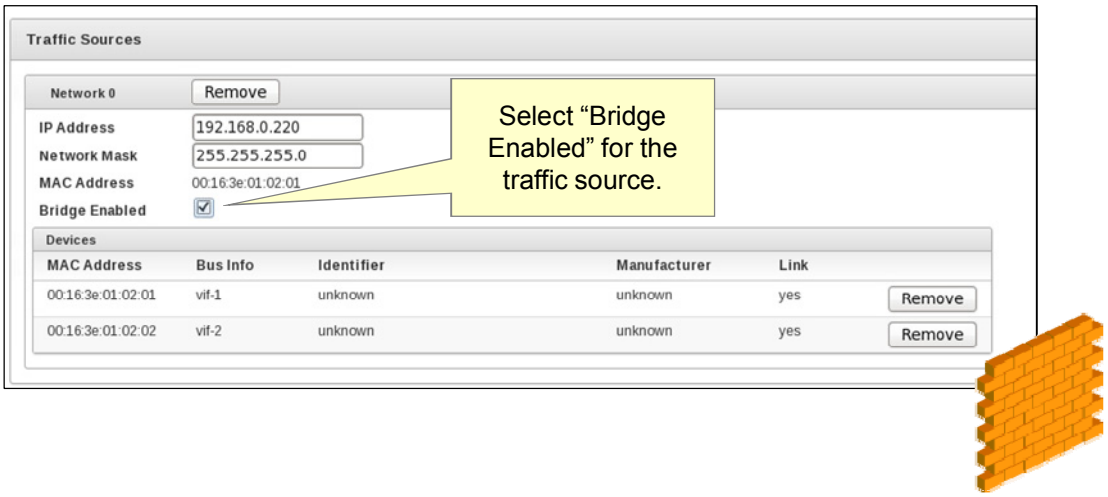
Traffic sources specify the IP address and network interface details for the traffic going through a Database Firewall. Traffic sources are automatically configured during the installation process. However, you can change their configuration details later. You can also add new traffic sources and remove existing traffic sources through the Database Firewall Console.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring a Bridge in the Database Firewall

- Bridge IP address is used to redirect traffic within the Database Firewall.
- A traffic source must have two network interfaces to be configured as a bridge.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Database Firewall can be deployed as a transparent network bridge. It is simply inserted into the network in a segment that lies between database clients/application servers and the databases being protected. This inline bridge architecture requires no configuration changes to database clients, applications, or the database itself, and provides the flexibility for both active and passive monitoring.

To enable a traffic source as a bridge, the traffic source must have two network interfaces. These network interface ports must connect the Database Firewall in-line between the database and its clients, regardless of whether DPE or DAM mode is used.

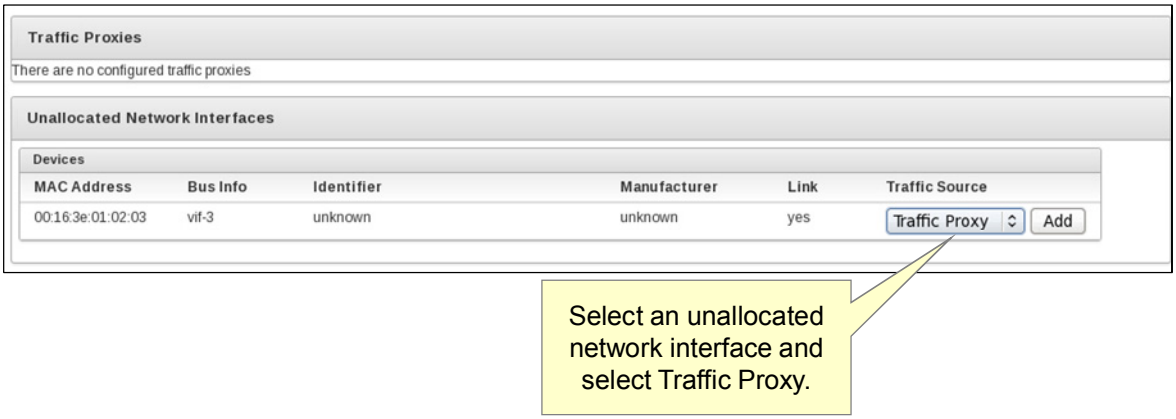
Note: The IP address of the bridge must be on the same subnet as all protected databases deployed in DPE mode on that bridge. This restriction does not apply to protected databases deployed in DAM mode.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring a Database Firewall as a Traffic Proxy

- The IP address of the proxy interface must be on the same subnet as the secured target.
- In the Unallocated Network Interfaces section of the Network page, find an available network interface, and select Traffic Proxy in the Traffic Source drop-down list.



Select an unallocated network interface and select Traffic Proxy.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

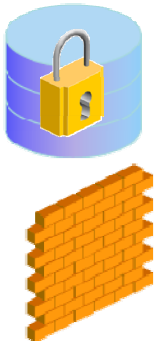
In scenarios where it is difficult to add a network bridge, or when the database servers are in remote locations, Database Firewall can also be configured as a proxy so that all traffic to the database server is routed through the Database Firewall. To configure a traffic proxy, the database server IP address/port on the database client or application must be changed to the IP address/port for the Database Firewall proxy and the database listener must be configured to reject direct connections. Most enterprise network switches and traditional firewalls can also be used to redirect database traffic to an Oracle Database Firewall proxy port, allowing SQL traffic to be protected without requiring any changes to database clients or applications. A specific Database Firewall can operate as a transparent bridge for some databases and a proxy for others.

After you configure the Database Firewall as a traffic proxy, your database clients connect to the database by using the Database Firewall proxy IP and port.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Associating the Database Firewall with an Audit Vault Server



- On the Certificate page of the Audit Vault Server console, copy the certificate.
- On the Audit Vault Server page of the Database Firewall administration console:
  - Enter IP address of the Audit Vault Server
  - Paste the certificate

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To enable the Audit Vault Server to manage the Database Firewall, you must associate each Database Firewall with an Audit Vault Server by specifying the server's certificate and IP address in the Database Firewall Console. If you are using a resilient pair of Audit Vault Servers for high availability, you must associate the Database Firewall to each Audit Vault Server.

Note: You must specify the Audit Vault Server certificate and IP address in the Database Firewall Console before you register the Database Firewall in the Audit Vault Server.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Registering the Database Firewall with the Audit Vault Server

- Register the Database Firewall with the Audit Vault Server by specifying:
  - The name of the Database Firewall
  - The IP address of the Database Firewall

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must register the Database Firewalls in the Audit Vault Server to enable communication between them.

Database Firewalls must be registered in the Audit Vault Server before you can pair them for high availability.

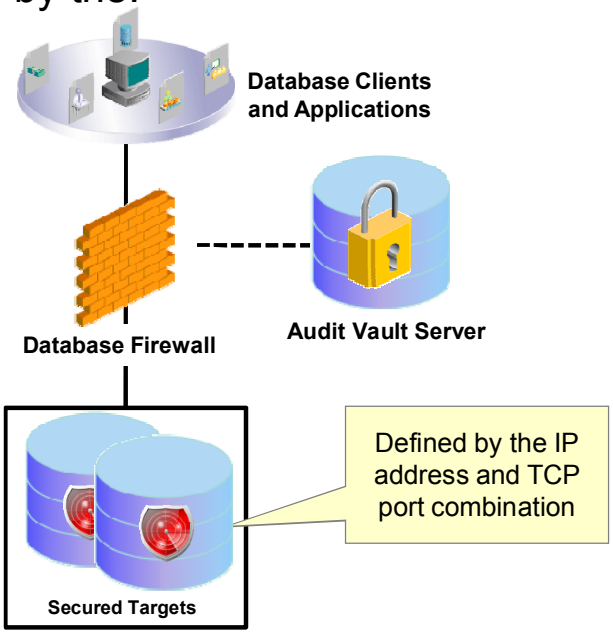
Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Secured Targets

A *secured target* is defined by the:

- IP address
- TCP port number



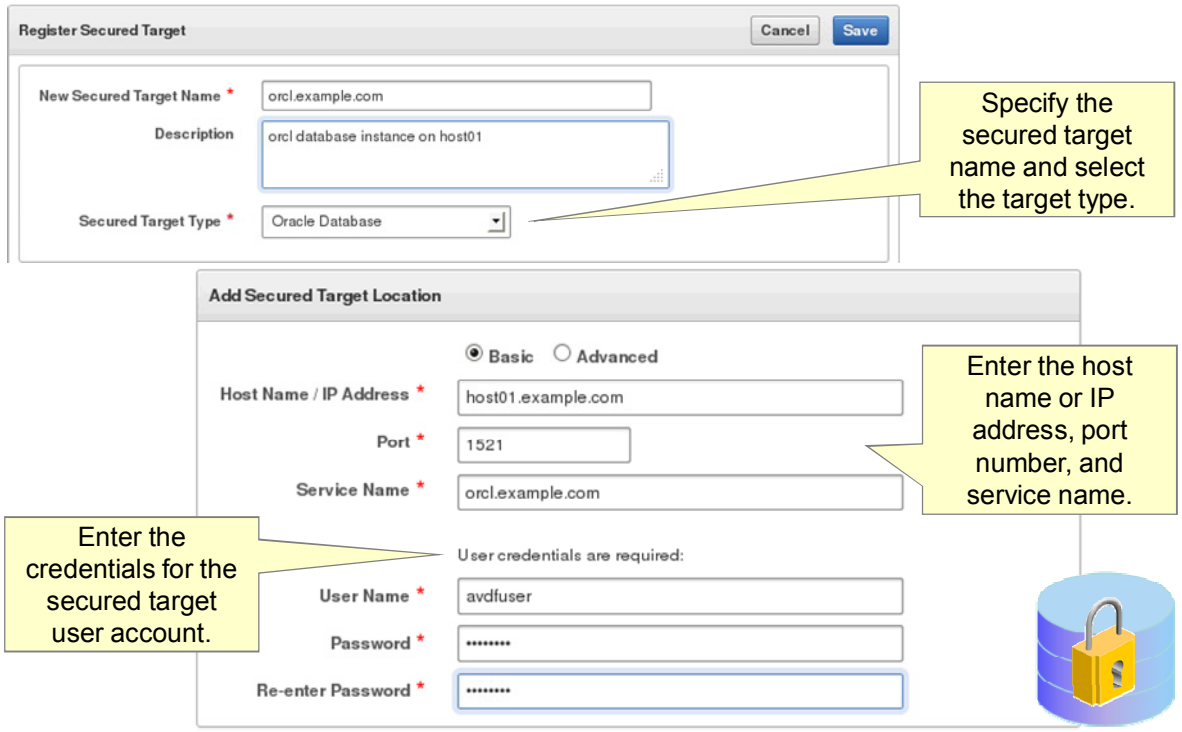
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

A *secured target* is defined by the combination of IP address and port number.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Registering Secured Targets



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

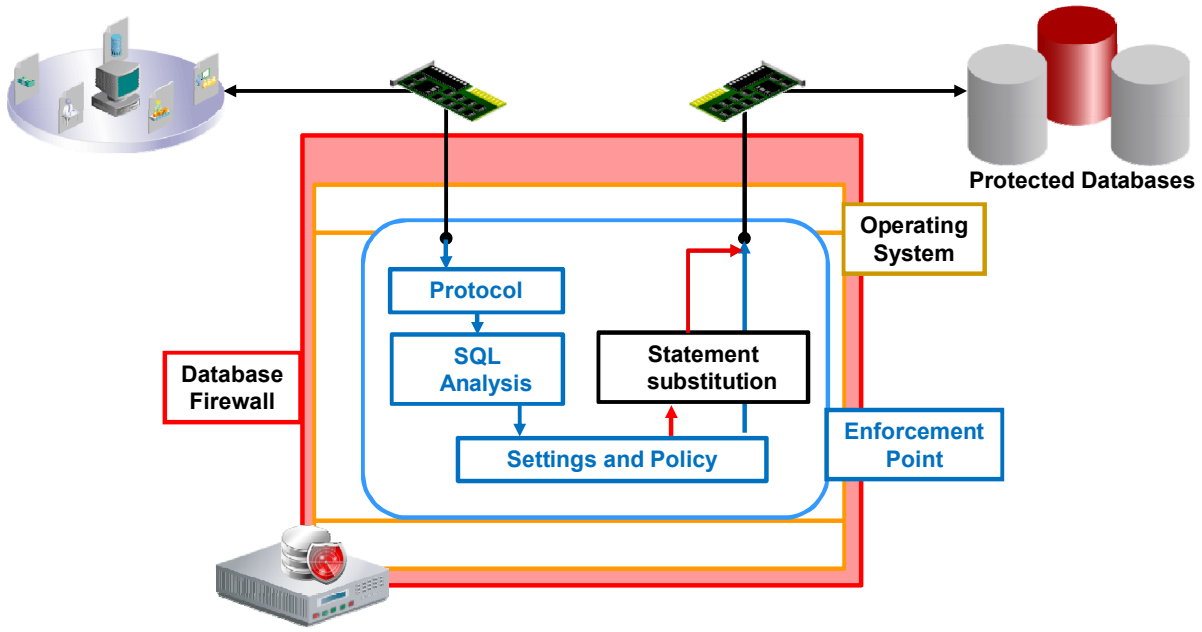
You must register all secured targets in the Audit Vault Server, regardless of whether you are deploying the Audit Vault Agent, the Database Firewall, or both.

In Oracle Database 12*c*, if you are using a multitenant container database (CDB), you must register a secured target for the CDB, as well as each pluggable database (PDB).

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Enforcement Point Architecture



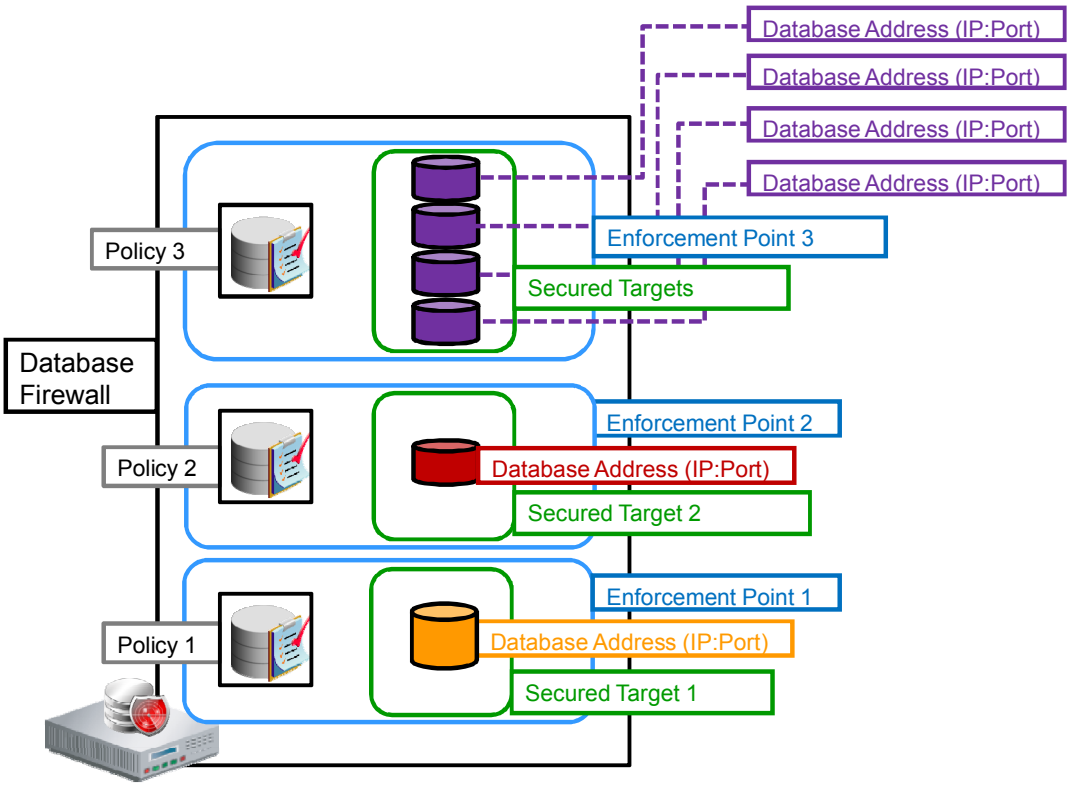
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

An *enforcement point* is a Database Firewall container that stores the settings that enforce the Database Firewall policies that you create. The enforcement point takes the SQL statements collected from the network traffic and decides how to handle them. In effect, the enforcement point defines the relationship between the database and the policy.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Enforcement Point Architecture



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

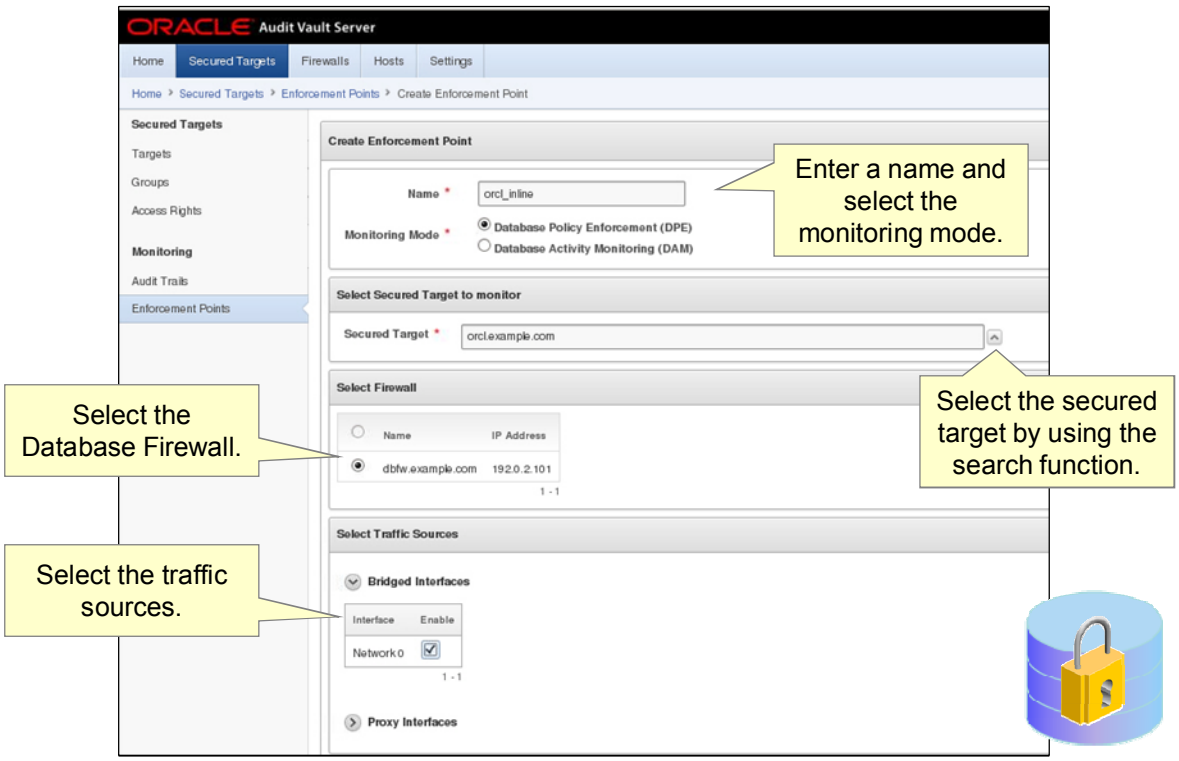
Each Database Firewall can have multiple enforcement points. Each enforcement point will apply to one or more databases. You can configure multiple databases to use one enforcement point. All the databases protected by the same enforcement point must be of the same database server type.

Note: A protected database is defined by the combination of IP address and port number. The term *database* in the context of this page is used in the way that it is defined for Microsoft SQL Server and Sybase. With Microsoft SQL Server and Sybase, there is one database engine instance per enforcement point because there can be multiple databases per instance. With Oracle Database, there is only one database per enforcement point because there is only one database per database engine instance. But if multiple Oracle instances are using one listener, all on the same port, the Database Firewall cannot distinguish to which instance the traffic is being sent.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Enforcement Points



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must configure one enforcement point for every secured target database that you want to monitor with the Database Firewall. When you configure the enforcement point, you specify the following:

- The firewall monitoring mode (monitoring only or blocking)
- The secured target database being monitored
- The network traffic sources to that database
- The Database Firewall used for the enforcement point

Before configuring enforcement points, configure network traffic sources as described earlier in the lesson.

If you configured a resilient pair of Audit Vault Servers, configure the enforcement points on the primary server. After defining the enforcement point you must start it.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

You must associate each Database Firewall with an Audit Vault Server by specifying the server's certificate and IP address in the Database Firewall Console before registering the Database Firewall in the Audit Vault Server.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring and Using Database Interrogation

Configure and use database interrogation by:

1. Configuring database interrogation for:
   - SQL Server and SQL Anywhere databases
   - Oracle Databases with Network Encryption
2. Enabling database interrogation in an enforcement point

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The database interrogation feature enables the Database Firewall to interrogate supported database secured targets for specific information. The information collected depends on the database type.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Database Interrogation for Oracle Databases

To configure database interrogation for Oracle databases, perform the following steps:

1. For databases prior to Oracle Database 12*c*, apply the 13051081 patch.
2. Execute the **`advanced_security_integration.sql`** script.
3. Modify the **`sqlnet.ora`** file of the Oracle Database to include the Database Firewall public key and to require Oracle Advanced Security native traffic encryption.
4. Enable database interrogation in the enforcement point that monitors the secured target by entering information on the Enforcement Point page.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

If you are using a release prior to Oracle Database 12*c*, you must apply the patch for bug number 13051081.

To configure database interrogation for Oracle databases, you need to execute the `advanced_security_integration.sql` script. Locate the script as follows:

1. Extract the database directory from the Oracle AVDF utilities file named `avdf-utility.zip`. This file was downloaded with your Oracle AVDF software.
2. Change to the `database/ddi` directory and uncompress one of the two Oracle compressed files (both contain the same content), preferably into a directory called `oracle`.
3. This directory now contains the uncompressed file named `advanced_security_integration.sql`.

To decrypt database traffic by using database interrogation, you must provide the Database Firewall public key to the Oracle Database that is using Oracle Advanced Security.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Database Interrogation for SQL Server Databases

To configure database interrogation for SQL Server databases, perform the following steps:

1. Execute the **`ddi_add_user.sql`** script to grant privileges to an existing user account in the secured target.
2. Enable database interrogation in the enforcement point that monitors the secured target by entering the database address and port of the secured target, database name, user name, and password on the Enforcement Point page.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To configure database interrogation for SQL Server databases, you need to execute the `ddi_add_user.sql` script to grant privileges. Locate the `ddi_add_user.sql` script as follows:

1. Extract the database directory from the Oracle AVDF utilities file named `avdf-utility.zip`. This file was downloaded with your Oracle AVDF software.
2. Copy the database directory to the server where you plan to execute the `ddi_add_user.sql` script.
3. On this server, change to the `database/ddi` directory and uncompress the `sqlserver` compressed file, preferably into a directory called `sqlserver`.
4. In this directory, you will find the uncompressed file named `ddi_add_user.sql`.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Database Interrogation for SQL Anywhere Databases

To configure database interrogation for SQL Anywhere databases, perform the following steps:

1. Execute the **`ddi_add_user.sql`** script to grant privileges to an existing user account in the secured target.
2. Enable database interrogation in the enforcement point that monitors the secured target by entering the database address and port of the secured target, database name, user name, and password on the Enforcement Point page.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Note: Before you can use Sybase SQL Anywhere, you must download and install the SQL Anywhere ODBC driver for Linux.

To configure database interrogation for Sybase SQL Anywhere databases, you need to execute the `ddi_add_user.sql` script to grant privileges. Locate the `ddi_add_user.sql` script as follows:

1. Extract the database directory from the Oracle AVDF utilities file named `avdf-utility.zip`. This file was downloaded with your Oracle AVDF software.
2. Copy the database directory to the server where you plan to execute the `ddi_add_user.sql` script.
3. On this server, change to the `database/ddi` directory and uncompress the `sqlanywhere` compressed file, preferably into a directory called `sqlanywhere`.
4. In this directory you will find the uncompressed file named `ddi_add_user.sql`.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring and Using Database Response Monitoring

To configure database response monitoring, perform the following steps:

1. Enable database response monitoring by selecting the "Enable Database Response" option on the Enforcement Points page.
2. Configure login and logout policies on the Firewall Policies page.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Database Response Monitoring feature enables the Database Firewall to record responses that the secured target database makes to login requests, logout requests, and SQL statements sent from database clients.

The recorded information includes the response interpreted by Oracle AVDF (such as "statement fail"), the detailed status information from the database, and the database response text, which may be displayed at the database client.

The Oracle AVDF auditor can view database responses in audit reports.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Configure the Database Firewall basic settings
- Associate each Database Firewall with the Audit Vault Server
- Configure the firewall on your network
- Register the secured targets with the Database Firewall in the Audit Vault Server
- Configure enforcement points for the secured targets
- Describe how to configure database interrogation
- Configure database response monitoring

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 8

- 8-1: Verifying the Database Firewall's Network Settings
- 8-2: Verifying the Database Firewall's Network Services
- 8-3: Verifying the Traffic Source Configuration
- 8-4: Configuring a Bridge in the Database Firewall
- 8-5: Configuring a Database Firewall as a Traffic Proxy
- 8-6: Specifying the Audit Vault Server Certificate and IP Address
- 8-7: Registering the Database Firewall
- 8-8: Registering the Secured Targets in the Audit Vault Server (OPTIONAL)
- 8-9: Creating and Configuring Enforcement Points
- 8-10: Configuring Database Response Monitoring

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Practice 8-8: Registering the Secured Targets in the Audit Vault Server (OPTIONAL): In this practice, you register the Oracle Database 12*c* secured target with the Audit Vault Server. You need to perform this practice only if you did not complete this task in an earlier practice.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

9 Using Host Monitoring

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

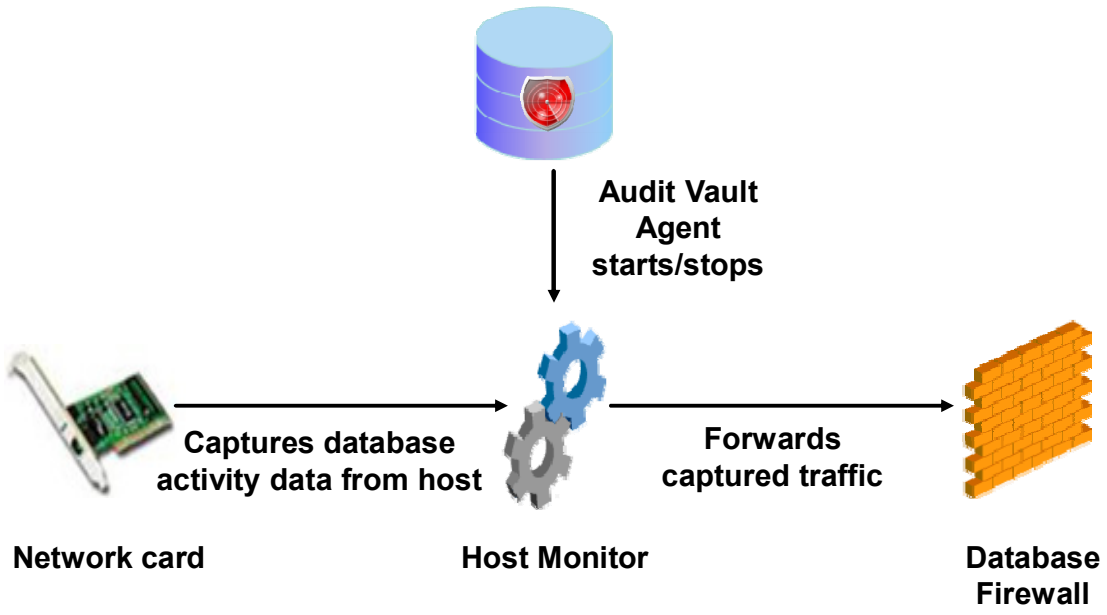
- Describe host monitoring and when it should be used
- Install and enable host monitoring
- Check the status of the host monitor
- Stop the host monitor

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Host Monitoring: Overview



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Audit Vault and Database Firewall (Oracle AVDF) supports a local server-side, monitor-only agent to ensure flexibility in the choice of the point at which the traffic is monitored. Host Monitor, part of the Audit Agent, captures SQL traffic reaching the database server and securely forwards it to the Database Firewall. It can be used to remotely monitor database servers running on Linux and Windows platforms.

The host monitor captures the SQL traffic from the network card and sends it to a Database Firewall. This SQL data is then available for use in reports generated by Oracle AVDF. Host monitoring is used only for monitoring SQL traffic and cannot be used to block or substitute SQL statements.

Deploy the Audit Vault Agent on the host machine that you want to deploy the host monitor on, usually the same machine as the database. For larger databases, the SQL traffic captured by a host monitor will increase network traffic. In this case, you can install the host monitoring software on a different server and use a spanning port to connect the database server to the server used for the host monitor.

You can use one Database Firewall to monitor multiple secured target databases using host monitoring by creating an enforcement point for each secured target.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Operating System Prerequisites

The host monitor host machine must have the following:

- OpenSSL
  - For Linux: OpenSSL 0.9.8*i* or higher
  - For Windows: OpenSSL 1.0.1*c* or higher
- For Linux hosts: The libpcap library, version 0.9.4 or higher
- For Windows hosts: The wincap library, version 4.1.2 or higher

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The machine that you will deploy the host monitor on must meet the requirements detailed in the slide. The host monitor must be deployed on Linux and Windows x86-64 platforms. The host monitor is not supported on 32-bit platforms.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Installing and Enabling Host Monitoring

Complete the following steps to install and enable host monitoring:

1. Register the computer that will run the host monitor.
2. Deploy the Audit Vault Agent and install the host monitor.
3. Create a secured target for the host-monitored database.
4. Create an enforcement point.
5. Configure a NETWORK audit trail.
6. Start the audit trail.

ORACLE

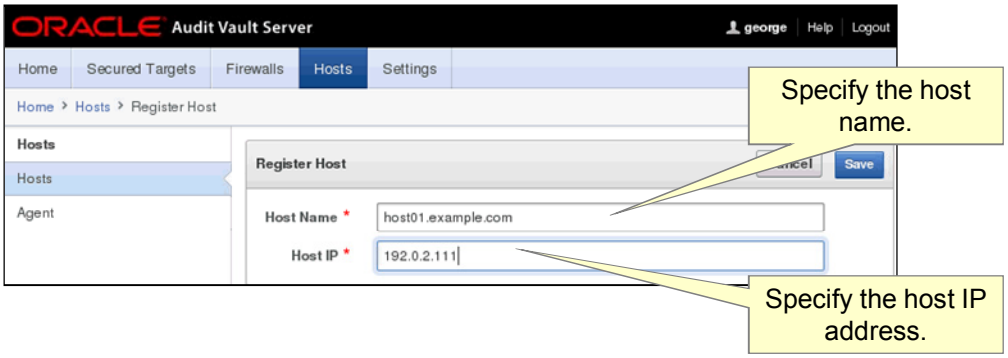
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Perform the steps listed in the slide to install and enable host monitoring. More details on each follows in this lesson.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Registering Hosts in the Audit Vault Server



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must configure a connection between the Audit Vault Server and the secured target host machine to enable audit data collection.

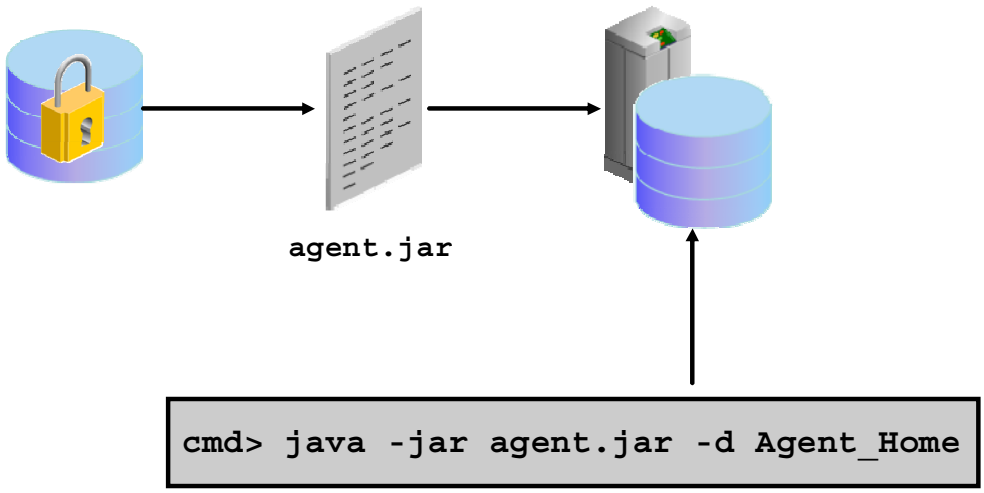
To register a host, log in to the Audit Vault Server console as an administrator and click the Hosts tab. Click register and enter the host name and host IP address.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Deploying the Audit Vault Agent on the Host Computer

Copy the `agent.jar` file from the Audit Vault Server and deploy this file on the host machine.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Before installing the Host Monitor, you must deploy the Audit Vault Agent. If you have not already done so, perform the following steps to deploy the Audit Vault Agent on the host computer:

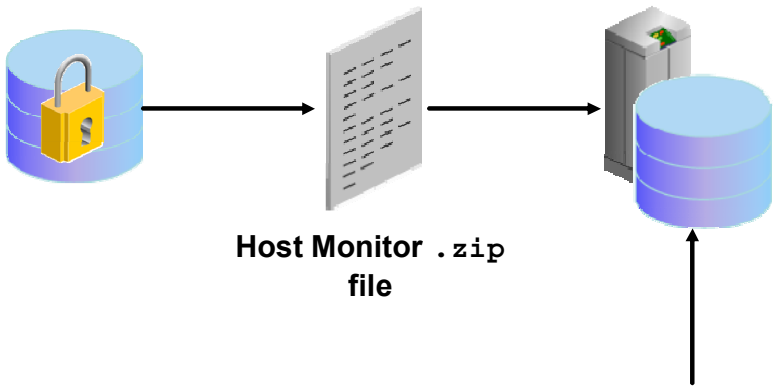
1. Log in to the Audit Vault Server console as an administrator.
2. Click the Hosts tab. Click Agent in the Hosts menu.
3. Click Download next to the Agent file. Save the `agent.jar` file to a location of your choice.
4. Using an operating system account, copy the `agent.jar` file to the secured target's host computer.
5. On the host machine, set `JAVA_HOME` to the installation directory of the jdk1.6 (or higher version), and make sure the Java executable corresponds to this `JAVA_HOME` setting.
6. Extract the agent by using the following command: `java -jar agent.jar -d Agent_Home`

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Installing the Host Monitor

Click the Download button next to Host Monitor, and then save the `.zip` file to a root-owned directory on the local hard disk.




```
HM_Home/hostmonsetup install agenthome=Agent_Home
   agentuser=Agent_Username agentgroup=Agent_Group
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To install the Host Monitor, perform the following steps:

1. Log in as root and identify a root-owned directory on the local hard disk, such as `/usr/local`, where you will install the host monitor. **Note:** The entire directory hierarchy must be root-owned, and must not contain any directories with write permission for other users or group.
2. Log in to the Audit Vault Server console as an administrator.
3. Click the Hosts tab and then click Agent.
4. Click the Download button next to Host Monitor (Linux x86-64), and then save the `.zip` file to the root-owned directory (on the local hard disk) you identified in step 1.
5. As root user, unzip the host monitor file. A directory named `hm` is created. This is your `HM_Home` directory.
6. Verify that the `hostmonsetup` file permissions include execute.
7. Execute the following command:

   ```
   HM_Home/hostmonsetup install agenthome=Agent_Home
   agentuser=Agent_Username agentgroup=Agent_Group
   ```

Oracle University and Error : You are not a Valid Partner use only

Providing parameter values as follows:

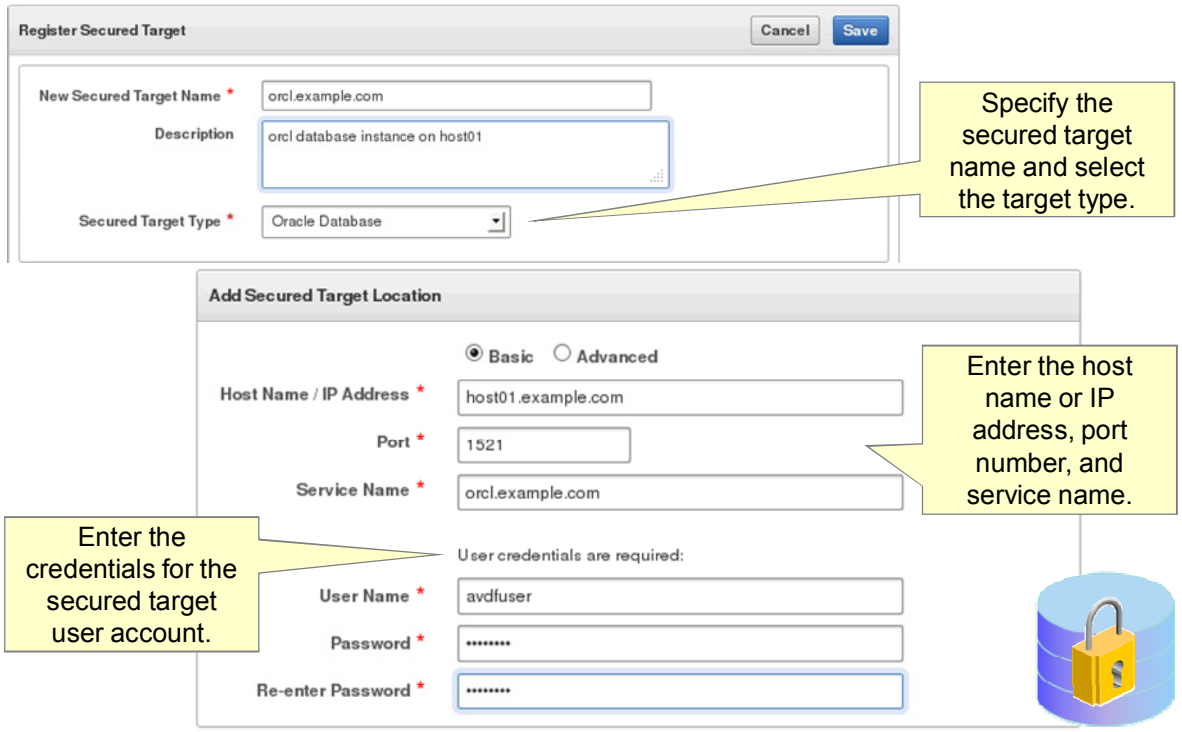
- `Agent_Home`: Audit Vault Agent installation directory
- `Agent_Username`: Username of the user who installed the Audit Vault Agent (the user who executed the `java -jar agent.jar` command)
- `Agent_Group`: Group to which `Agent_Username` belongs

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Registering Secured Targets



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

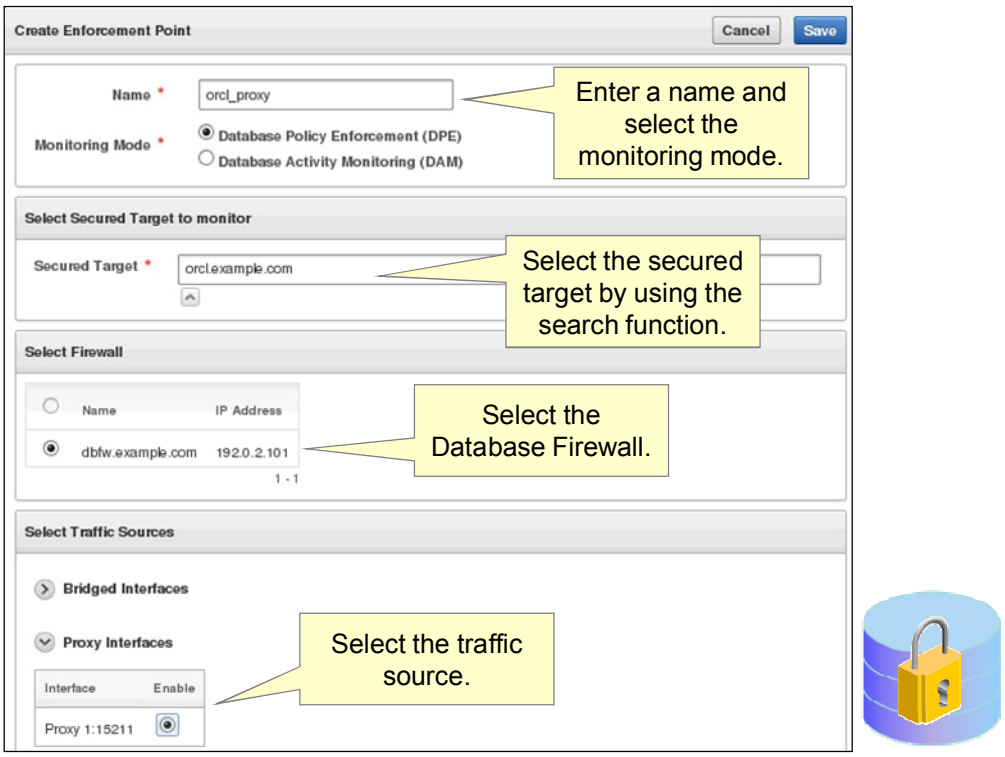
You must register all secured targets in the Audit Vault Server, regardless of whether you are deploying the Audit Vault Agent, the Database Firewall, or both.

In Oracle Database 12*c*, if you are using a multitenant container database (CDB), you must register a secured target for the CDB, as well as each pluggable database (PDB).

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Enforcement Points



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You must configure one enforcement point for every secured target database that you want to monitor with the Database Firewall. When you configure the enforcement point, you specify the following:

- The firewall monitoring mode (monitoring only or blocking)
- The secured target database being monitored
- The network traffic sources to that database
- The Database Firewall used for the enforcement point

Before configuring enforcement points, configure network traffic sources.

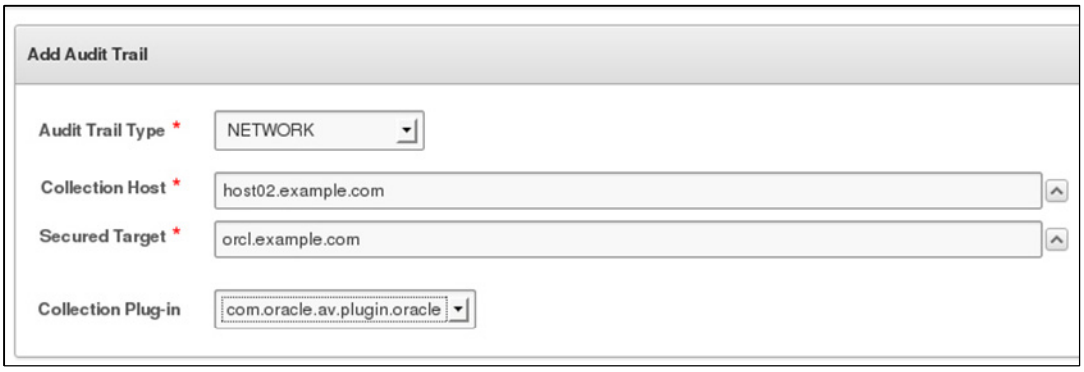
If you configured a resilient pair of Audit Vault Servers, configure the enforcement points on the primary server. After defining the enforcement point you must start it.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring an Audit Trail for Host Monitoring

- Create an audit trail with a type of NETWORK.
- Start the host monitor by starting the NETWORK audit trail on the Audit Trails page.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

For host monitoring, you must create an audit trail with a type of NETWORK. To start the host monitor, start the NETWORK audit trail on the host you are monitoring.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Checking the Status of the Host Monitor

To check the status of a host monitor:

1. Log in to the Audit Vault Server console.
2. Click the Secured Targets tab.
3. In the Monitoring menu, click Audit Trails. The collection status of a host monitor audit trail is listed in the Audit Trails page. You can search or sort the list to find the host monitor.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Stopping the Host Monitor

To stop a host monitor, stop the audit trail you created for the secured target that is being monitored.

To stop audit trail collection for a secured target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the Secured Targets tab.
3. Click Audit Trails.
4. Select the audit trail(s) you want to stop, and then click Stop.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Uninstalling the Host Monitor

To uninstall a host monitor, perform the following steps:

1. Log in to the host computer as `root`.
2. Change to the `HM_Home` directory where you installed the host monitor.
3. Execute the following command:

```
hostmonsetup uninstall
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Prior to installing the host monitor, you must install the Audit Vault Agent on the same machine.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Describe host monitoring and when it should be used
- Install and enable host monitoring
- Check the status of the host monitor
- Stop the host monitor

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 9

- 9-1: Reviewing Sample Configurations for Host Monitoring Implementation
- 9-2: Installing the Host Monitor
- 9-3: Configuring an Audit Trail for Host Monitoring
- 9-4: Starting the Host Monitor

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In Practice 9-1, a pen-and-paper practice, you review sample configurations and determine whether host monitoring is an appropriate choice.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

10

Configuring High Availability

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Describe Oracle AVDF high availability configurations
- Describe how to configure a resilient pair of Audit Vault Servers
- Describe how to configure a resilient pair of Database Firewalls

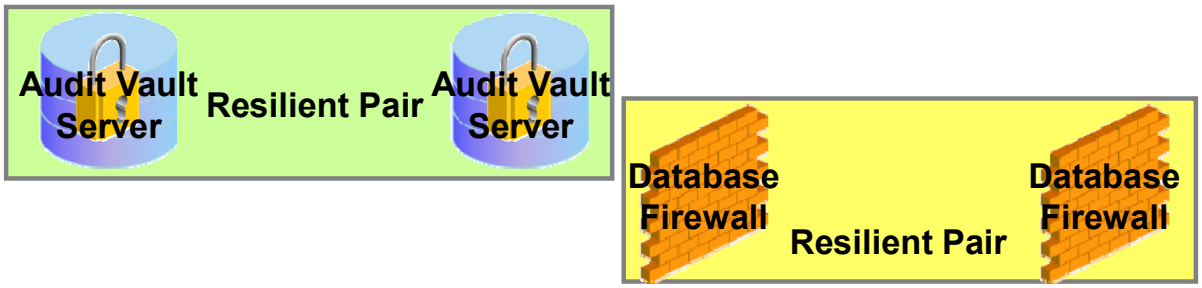
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle AVDF
High Availability Architecture: Overview

- Configure pairs of Database Firewalls or pairs of Audit Vault Servers, or both, to provide a high-availability system architecture.
- Database Firewall resilient pair configuration applies to Database Activity Monitoring (DAM) mode only.
- Primary device carries out all normal operations.
- Secondary device monitors traffic and gives alerts only if the primary device fails.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

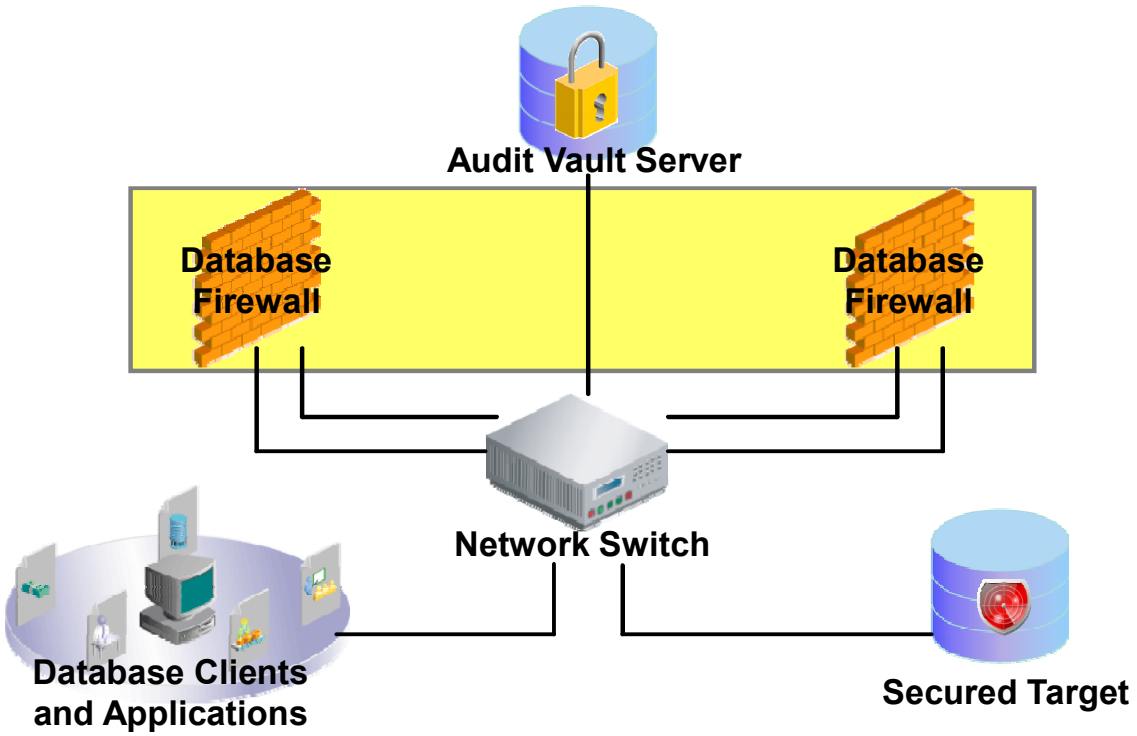
You can configure pairs of Database Firewalls or pairs of Audit Vault Servers, or both, to provide a high-availability system architecture. The pairs of Audit Vault Servers and Database Firewalls are referred to as “resilient pairs.” For Database Firewall, the resilient pair configuration described in this lesson applies to Database Activity Monitoring (DAM) mode only.

In a resilient pair, you specify one device as the primary device and the other as the secondary device. The primary device carries out all normal operations while the secondary device monitors traffic. The secondary device sends alerts only if the primary device fails.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

A High Availability Pair of Database Firewalls Protecting a Single Secured Target



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In a resilient pair configuration of Database Firewalls, only the primary Database Firewall sends out real-time alerts. Both primary and secondary Database Firewalls:

- Receive the same span traffic
- Have the same configuration, which is synchronized by the Audit Vault Server
- Create log files according to the policy applied

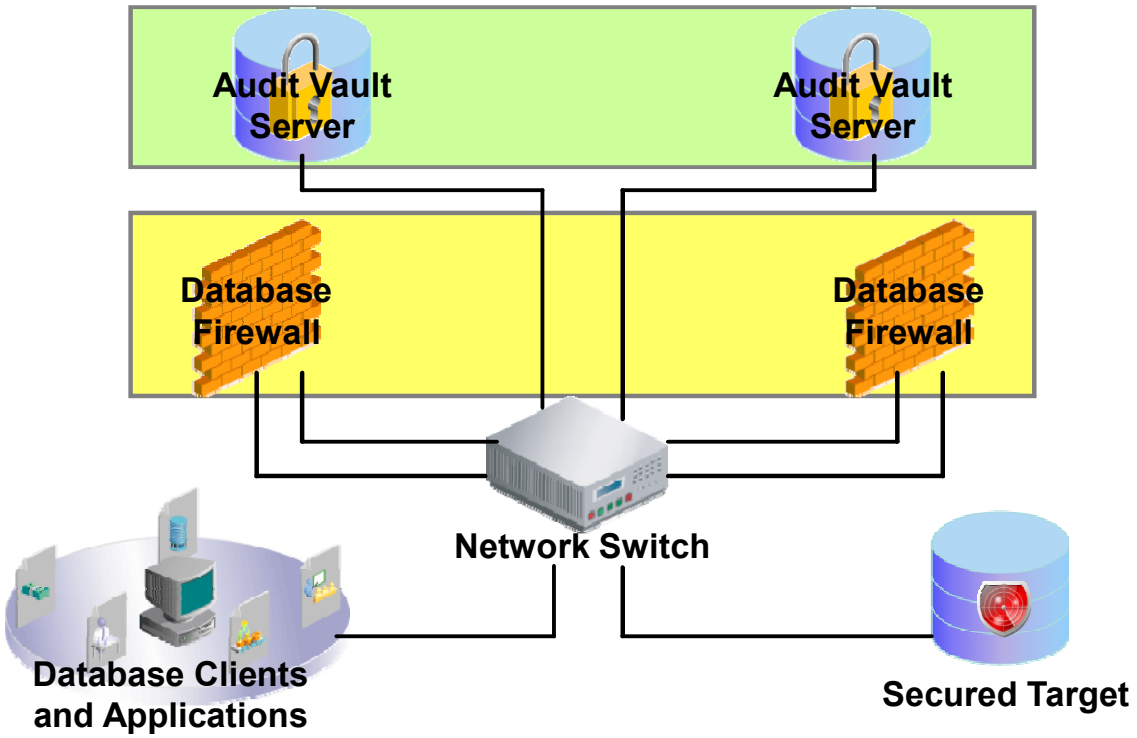
The Audit Vault Server collects logs from the primary Database Firewall, and deletes the log files from both Database Firewalls.

If the primary Database Firewall is not available or cannot be contacted by the Audit Vault Server, it collects the log files from the secondary Database Firewall and promotes the secondary Database Firewall to be the primary. Then the new primary Database Firewall will start sending out real-time alerts.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Pairs of Audit Vault Servers and Database Firewalls in High Availability Mode



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In a resilient pair configuration of Audit Vault Servers, the primary Audit Vault Server performs all server functions. The secondary Audit Vault Server copies all data and configuration information from the primary server. The console UI is not available in the secondary Audit Vault Server.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Recommended Configuration Sequence

Configure High Availability as follows:

1. Configure initial settings on both Audit Vault Servers.
2. Pair Audit Vault Servers before performing additional configuration tasks.
3. Deploy and activate Audit Vault Agents.
4. Attach Database Firewalls to Audit Vault Server.
5. Configure Database Firewalls for high availability.
6. Configure secured targets, enforcement points, and audit trails.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The recommended configuration sequence for resilient pairs of Audit Vault Servers and Database Firewalls is listed in the slide.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring a Resilient Pair of Audit Vault Servers

Perform the following steps to configure a resilient pair of Audit Vault Servers:

1. Configure the secondary Audit Vault Server by copying the server certificate from the primary server to the secondary server and entering the IP address of the primary server.
2. Configure the primary Audit Vault Server by copying the server certificate from the secondary server to the primary server and entering the IP address of the secondary server.
3. Start high availability pairing of the Audit Vault Servers at the primary server.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

When you pair two Audit Vault Servers, you designate one as the primary and the other as the secondary server. All data and configuration in the primary server is automatically copied to the secondary server. Going forward it is automatically kept in sync.

After configuring the resilient pair of Audit Vault Servers, perform any additional configuration tasks for your AVDF implementation on the primary server only.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring a Resilient Pair of Database Firewalls

- It is applicable to a Database Firewall in DAM mode only.
- Ensure there are no enforcement points configured on either of the Database Firewalls that you plan to pair.
- Select the primary and secondary firewalls you want to pair on the Resilient Pairs page of the Audit Vault Server console.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The procedure described here applies to a Database Firewall in DAM mode only.

Ensure that there are no enforcement points configured on either of the Database Firewalls before you pair them. If either Database Firewall has enforcement points, you must delete the enforcement points before creating a resilient pair.

If you also configured a resilient pair of Audit Vault Servers, you must provide each Audit Vault Server's IP address and certificate to each Database Firewall.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

Order the following steps in the recommended configuration sequence:

a. Configure initial settings on both Audit Vault Servers.
b. Deploy and activate Audit Vault Agents.
c. Configure resilient pairs of Database Firewalls.
d. Attach Database Firewalls to Audit Vault Servers.
e. Configure resilient pairs of Audit Vault Servers.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a, e, b, d, c

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Describe Oracle AVDF high availability configurations
- Describe how to configure a resilient pair of Audit Vault Servers
- Describe how to configure a resilient pair of Database Firewalls

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 10

- 10-1: Listing the Steps to Configure a Resilient Pair of Audit Vault Servers
- 10-2: Listing the Steps to Configure a Resilient Pair of Database Firewalls

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

11

Creating Custom Collection Plug-ins

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Describe when a custom collection plug-in would be needed
- List the requirements for a database table collection plug-in
- List the requirements for an XML file collection plug-in
- List the steps performed to create and package a custom collection plug-in

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Custom Collection Plug-ins: Overview

- Write a custom collector or customize a collector template.
- Custom collection plug-ins:
  - Collect audit information written to database tables, XML files, or other locations.
  - Collect audit data from secured targets such as relational databases, operating systems, mid-tier systems, or enterprise applications.
- Types of custom collection plug-ins:
  - Database table
  - XML File
  - Java-based

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You can write a new collector or customize one of the collector templates that is provided with the Audit Vault Server. Templates can be modified to collect from any DB table or XML file-based audit trail. If the collector must collect from other audit trails, a new collector must be written.

Exception: If the audit trail can be transformed into a DB table or XML file, a template can be used to create the collector.

Custom Collectors

You can build custom collection plug-ins to collect audit data from a new secured target type or support new audit trails written by a secured target type that has been previously defined to AVDF.

You can write custom collection plug-ins to collect audit trails stored in database tables and XML files. There is also a Java-based type of collection plug-in, which uses a Java API.

Custom collection plugs-ins can access data in secured targets such as relational databases, operating systems, mid-tier systems, or enterprise applications.

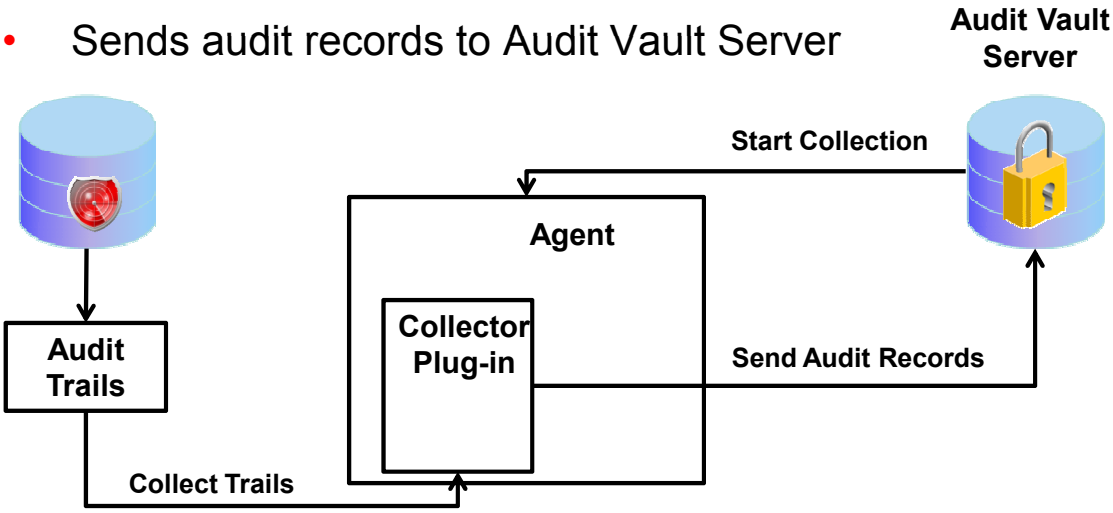
A custom collection plug-in uses an XML file, called a mapper file, to describe the audit data being collected. Audit Vault Server uses this file to access and interpret the audit records being collected.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Collector Plug-in

- Collects audit records from a secured target
- Uses the collector framework
- Translates or reformats audit records
- Sends audit records to Audit Vault Server



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Audit Vault Server will start the collection using the console or AVCLI.

The collector plug-in runs as a thread in the agent on the secured target host. The collector reads the audit trails produced by the secured target. These audit trails may be database tables, XML files, or other sources. Source audit record fields are reformatted if necessary and mapped from the source audit trail to the Audit Vault Server fields. The specification of this mapping is included in a mapper file.

The collector plug-in sends the reformatted audit records to the Audit Vault Server.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Deploying the Collector Plug-in

1. Develop the plug-in in an appropriate environment.
2. Use AVPACK to package the plug-in files with into a zip file.
3. Use the AVCLI `DEPLOY PLUGIN` command to include the plug-in into the agent source on the Audit Vault Server.
4. Redeploy the agent to the secured target.
5. Start collections.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This is a brief overview of a collector plug-in deployment. More details of the development requirements follow in this lesson.

The best practice recommendation is to develop your plug-in in a test environment. This environment will have an Audit Vault Server appliance and a development version of the secured target. The actual development can be done on any machine that has network connectivity to an Audit Vault Server and the audit trail of interest. The development machine must have a JDK installed. It is possible to do the development in the production environment, but it is not recommended.

When the development files have been created in the required directory structure, use the `AVPACK` tool to package the plug-in files into a zip file.

Use the AVCLI `DEPLOY PLUGIN` command to include the plug-in into the agent source on the Audit Vault Server. This plugin is now available to download with the agent.

Re-deploy the agent to the secured target. Now, the plug-in is available to collect the audit trail on that target.

Use the Audit Vault Server console or AVCLI to start the agent collections.

When the collector plug-in is working as expected, move the zip file to the Audit Vault Server in the production environment, and perform steps 3-5 for the production environment.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Database Table Collection Plug-in Requirements

Requirement	Notes
Audit table must be accessible via a JDBC driver.	
One-step user/password authentication must be used.	The username/password is provided from the trail specification on the AV Server.
Audit record must be stored in a single table.	

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The table in the slide lists the requirements for database table collection plug-ins.

The connection information (connect string, username, password, and so forth) is sent from the server to the collector during start of the audit trail. These are not specified during the collector design. These are run-time parameters that are defined when an audit trail is defined in the Audit Vault Server. When the trail is started, the information is sent from the server to the agent, which then uses this information to connect to the source.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

XML File Collection Plug-in Requirements

Requirement	Notes
XML audit log files are valid and complete XML documents.	
XML audit log files are stored in a single directory conforming to a *.xml pattern.	The trail location is specified in the Audit Trail specification as a directory mask (path).
The third-party auditing system only writes into one “active” file at a time.	Once the file has been written to and it is complete (closed and a new one opened), it is never reopened by the auditing system.
The agent has read/write access to the directory where the custom XML audit log files reside.	

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The table in the slide lists the requirements for XML file collection plug-ins.

The XML file being collected must be a well formed XML file. These XML files must be in a single directory.

The location and name of the XML file to be collected is specified when you add the audit trail in the Audit Vault Server. See the specifications of the templated collectors in *Appendix B Plugin Reference* of the *Oracle Audit Vault and Database Firewall Administrator's Guide*.

To maintain valid audit logs on the AV Server, the audit files that are being collected must be written to one “active” file at a time.

When the file is complete, it is closed and never reopened by the writer. Instead, a new file is opened.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Template-Based Customizable Collection

- Supports database table and XML file trail types
- No need to write code
- Package configuration files with the AVPACK utility
- Required information:
  - Secured target type, version, timezone offset
  - Connection and/or location information of audit trail
  - Field or group of field in the original trail to use as unique record marker
  - Mapping from custom fields to Audit Vault fields
  - Value transformation for field values

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

If the audit trail you want to collect is in a database table or an XML file on the secured target, you can use the available set of generalized collector plug-ins. These templates eliminate the need to write code. They can be customized by providing a mapper file and a manifest.

The list of available plug-in templates is in *Appendix B 'Plugin Reference' of the Oracle Audit Vault and Database Firewall Administrator's Guide Release 12.1.2.*

The required information listed here is placed in the mapper file.

Note: All plug-ins require a mapper file and a manifest file.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

General Procedure for Creating Custom Collection Plug-ins

The general procedure for creating custom collection plug-ins is as follows:

1. Determine whether you need to add a new secured target type or a new audit trail for an existing secured target type.
2. Verify that a pre-packaged plug-in to suit your purpose is not included with AVDF.
3. Determine the events and fields that are written by your secured target type.
4. Determine which type of plug-in you need to write.
5. Determine which platforms your plug-in will support.
6. Determine how to connect to the secured target and interrogate it to obtain the required data.
7. Decide whether your plug-in will support audit trail cleanup.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The general procedure for creating custom collection plug-ins is listed on this page and the next page. Additional information follows in the lesson.

Use appropriate existing events and fields when you write your custom collection plug-in. Refer to Appendix A, “Audit Vault Server Fields” in the *Oracle Audit Vault and Database Firewall Developer's Guide* for examples of existing events and fields. If the events or fields you need are not available, you can use extension fields as described in Appendix A.

The information in step 3 is captured in the mapper file.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

General Procedure for Creating Custom Collection Plug-ins

The general procedure for writing audit collection plug-ins is:

8. Set up your development environment.
9. Set up the collection plug-in parameters.
10. Create a plug-in manifest file to describe the collection plug-in.
11. Run the `avpack` utility to package the plug-in.
12. Test the plug-in in the staging environment.
13. Deploy the plug-in in the production environment.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

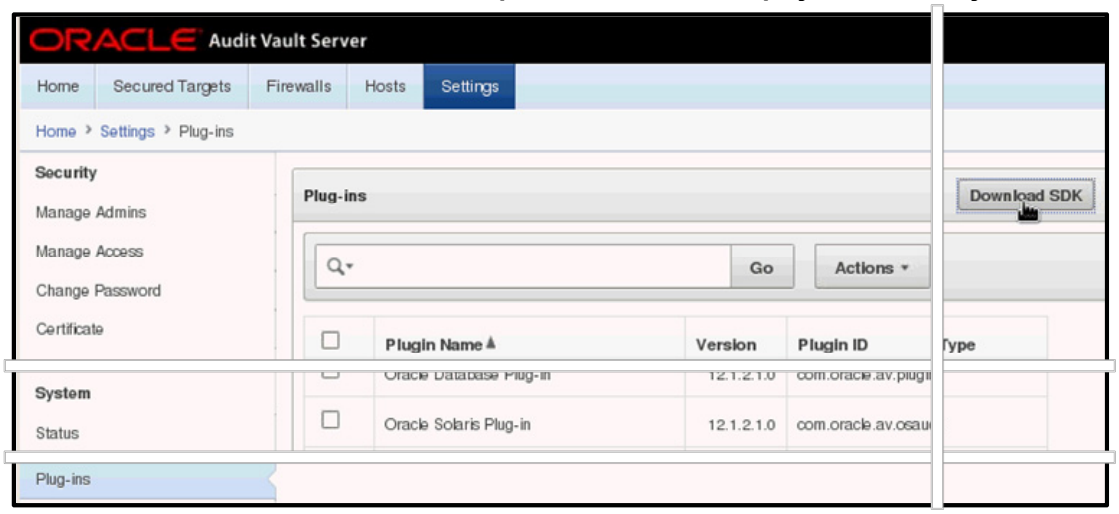
Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Setting Up Your Development Environment

Perform the following steps to set up your development environment:

1. Download the Oracle AVDF SDK from the Audit Vault Server console and unzip it into an empty directory.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To develop custom collection plug-ins, you must first set up the development environment. This setup provides a consistent environment for developing and testing the collection plug-ins. The development environment must have network or direct access to the audit target files or tables, and network access to the Audit Vault Server. The development environment must have JDK for Java Version 6 or later installed.

First download the SDK. Unzip it to an empty directory. This directory will be `AV_SDK_HOME`.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Setting Up Your Development Environment

Perform the following steps to set up your development environment:

2. Set the `AV_SDK_HOME` variable to the directory you extracted the SDK into.
3. Set the `PATH` environment variable to the bin directory of the `AV_SDK_HOME`.
4. Set the `CLASSPATH` environment variable to include the relevant jars for your collection plug-in project.
5. If you are using Java, ensure that the `PATH` and `JAVA_HOME` variables are set to the appropriate JDK.
6. Create any required directories.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

2. In this example: `AV_SDK_HOME` is set to `/home/oracle/SDK`.
3. Set the PATH environment variable as follows: `export PATH=$AV_SDK_HOME/bin:$PATH` /* syntax is for a bash shell */
4. Set the `CLASSPATH` variable (for example, `export CLASSPATH=$AV_SDK_HOME/av/jlib`).
5. If you are building Java-based plug-ins, use the appropriate version of Java Development Kit (JDK). Oracle Audit Vault Server 12.1.2.x uses Java 6 or later.
6. The directory structure varies depending on whether you are building the collector or modifying a template. It also varies based on the platform. See *Chapter 2 Setting Up Your Development Environment* of the *Oracle Audit Vault and Database Firewall Developer's Guide Release 12.1.2* for more details. The top level of this directory is called `STAGE_DIR_ROOT` in the documentation.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating Custom Collection Plug-ins

Perform the following steps to create custom collection plug-ins for database tables or XML files from a template:

1. Create a plug-in manifest file.
2. Create an XML mapper file.
3. Package the XML mapper file and manifest file.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

All plug-ins require manifest and mapper files. However, if you are customizing a template collector, the manifest and mapper files must be created but no code needs to written. Perform the following steps to create custom collection plug-ins for database tables or XML files:

1. Create a plug-in manifest file for this secured target type. Place the manifest file in the `STAGE_DIR_ROOT` directory of the directory structure you created for the development of this collector.
2. Create an XML Mapper file for a secured target audit trail. The mapper file is created in the `STAGE_DIR_ROOT/templates` directory.
3. Create the collection plug-in by packaging the mapper file and plug-in manifest file by using the `avpack` tool.

Additional information on these three steps follows in this lesson.

After completing these steps, you can deploy the collection plug-in at the Audit Vault Server and start collecting audit data.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating a Plug-in Manifest File

- `plugin-manifest.xml` is a core XML file that describes the collection plug-in and defines its attributes.
- Stage the `plugin-manifest.xml` file directly under the `STAGE_DIR_ROOT` directory.
- Perform the following steps:
  1. Create a directory structure.
  2. Create a `plugin-manifest.xml` file.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The `plugin-manifest.xml` file is a core XML file that describes the collection plug-in and defines its attributes. It provides the Audit Vault Collection Framework with information to instantiate and run the collection plug-in. The manifest file includes version information about the plug-in and the version of the target, the files included in the `STAGE_DIR_ROOT` directory, the location of the mapper file, and the target extension type.

Note: The only type supported at this time is `securedTargetType`.

Perform the following steps to create a `plugin-manifest.xml` file:

1. Create a directory structure. You must stage the `plugin-manifest.xml` file directly under the `STAGE_DIR_ROOT` directory.
2. Create a `plugin-manifest.xml` file.

   Start with a copy of an existing manifest file from the documentation examples, or a working collector, and modify. The fields of the manifest file are described in Section *4.4 Description of Plug-in Manifest File* of the *Oracle Audit Vault and Database Firewall Developer's Guide Release 12.1.2*.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating an XML Mapper File

- *Mapper files*: XML files, which contain information about which secured target fields must be collected from an audit trail and how these fields map to Audit Vault Server fields
- The mapper file is packaged as part of the collection plug-in.
- Place mapper files in the `templates` folder during the plug-in packaging process.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Mapper files are XML files that mainly contain information about the secured target fields that must be collected from the audit trail and how these secured target fields map to Audit Vault Server fields. Mapper files are specific to a secured target type and contain secured target information such as `securedTargetType` and `securedTargetVersion`.

Mapper files include the following information:

- The supported secure target name and secured target version
- Mapping information from secured target fields to Audit Vault Server fields
- Secured target fields for constructing markers, which uniquely identify each audit record
- Audit table and data source class names when the audit trail type is data
- Event time (timestamp format) when the audit trail type is an XML file

Package the mapper files as part of the collection plug-in. Place mapper files in the `templates` folder during the plug-in packaging process.

Refer to section 3.3.3 Creating a Database Table Mapper File in the *Developer's Guide* for a detailed example of a mapper file for a database table collection plug-in.

Refer to section 3.4.3 Creating the XML File Audit Collection Mapper File in the *Developer's Guide* for a detailed example of a mapper file for an XML file collection plug-in.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating the Collection Plug-in Package

After creating the `plugin-manifest.xml` file, perform the following steps:

1. Package the collection plug-in files, the `plugin-manifest.xml` file, and any additional jars that collection plug-in depends on at run-time.
2. Run the `avpack` tool to generate a `.zip` package that represents a collection plug-in package.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Perform the following steps to create the collection plug-in package:

1. Package the collection plug-in files, the `plugin-manifest.xml` file, and any additional jars that collection plug-in depends on at run-time.
2. Execute the `avpack` tool to validate and generate a `.zip` package that represents a collection plug-in package. The `avpack` tool runs a number of validity checks (such as whether the directory structure is correctly populated, the manifest file is well-formed, and is without errors, and so on) and then generates the collection plug-in package, in the form of a zip file, for deployment.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Deploying a Custom Collection Plug-in

- Use the AVCLI `DEPLOY PLUGIN` command.
- Specify the plug-in archive, which is the `.zip` file created by the `avpack` utility.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

After packaging the plug-in with the `avpack` utility on the development machine, transfer the `.zip` file to the Audit Vault Server.

The AVCLI `DEPLOY PLUGIN` command is used to deploy a plug-in into the Audit Vault Server home from a given archive file.

The syntax for the command is: `DEPLOY PLUGIN <plugin archive>`.

`plugin archive` is the plug-in archive created by the `avpack` utility.

The `DEPLOY PLUGIN` command updates the agent archive with the contents of this plug-in for future Agent deployments.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Setting Secured Target Collection Attributes

- Set secured target collection attributes after you have deployed the collection plug-in in the Audit Vault Server and registered the secured target, but before the plug-in starts collecting data from the audit trail.
- Use the `ALTER SECURED TARGET` AVCLI command to specify the following attributes:
  - `av.collector.securedtargetversion`
  - `av.collector.atcintervaltime`
  - `av.collector.timezoneoffset`

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

For database table and XML file collection plug-ins, you need to set secured target collection attributes after you have deployed the collection plug-in in the Audit Vault Server and registered the secured target, but before the plug-in starts collection from the audit trail.

You define collection attributes by using the `ALTER SECURED TARGET` AVCLI command.

The syntax is:

```
ALTER SECURED TARGET secured_target_name SET attribute=value;
```

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Best Practices Checklist

- Separate individual secured target trails.
- Make sure that XML trail files are standard-conformant.
- Correctly identify marker tag.
- Check file system and database permissions.
- Verify time stamp functions properly.
- Use multiple trails (separate directory, tables) for increased performance.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You are allowed to have multiple audit trails for a secured target and each trail can be stopped and started individually. Multiple directory and table trail types are allowed, so specify a trail name for each.

The XML files accessed by the `DIRECTORY` trail type must be well-formed XML.

The marker field is an unique field, often a concatenated set of fields used to identify a record, and used to checkpoint the audit trail. The marker field is used to ensure collections start at the correct point without duplication or omissions.

The event time stamp is a required field. If the time stamp is `NULL`, the collector stops.

Each trail gets a separate thread in the agent. On multiple processor machines this can make the collections perform better.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

You only need to write a custom collection plug-in if there is no pre-packaged collection plug-in for the type of audit data you want to collect.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Note: If the audit data can be transformed into a database table or an XML file, a pre-packaged collection plug-in can be used.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Describe when a custom collection plug-in would be needed
- List the requirements for a database table collection plug-in
- List the requirements for an XML file collection plug-in
- List the steps performed to create and package a custom collection plug-in

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 11

- 11-1: Identifying the Need for a Custom Collection Plug-in
- 11-2: Identifying Database Table Collection Plug-in Requirements
- 11-3: Identifying XML File Collection Plug-in Requirements
- 11-4: Listing the Steps to Create a Custom Collection Plug-in

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

11-1: In this pen-and-paper practice, you identify whether a given source is applicable for a custom collection plug-in.

11-2: In this pen-and-paper practice, you review a description and determine whether the system meets the requirements for a database table collection plug-in.

11-3: In this pen-and-paper practice, you review a description and determine whether the system meets the requirements for an XML file collection plug-in.

11-4: In this pen-and-paper practice, you list the steps you need to perform to create and package a custom collection plug-in.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

12

Managing the Audit Vault Server

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

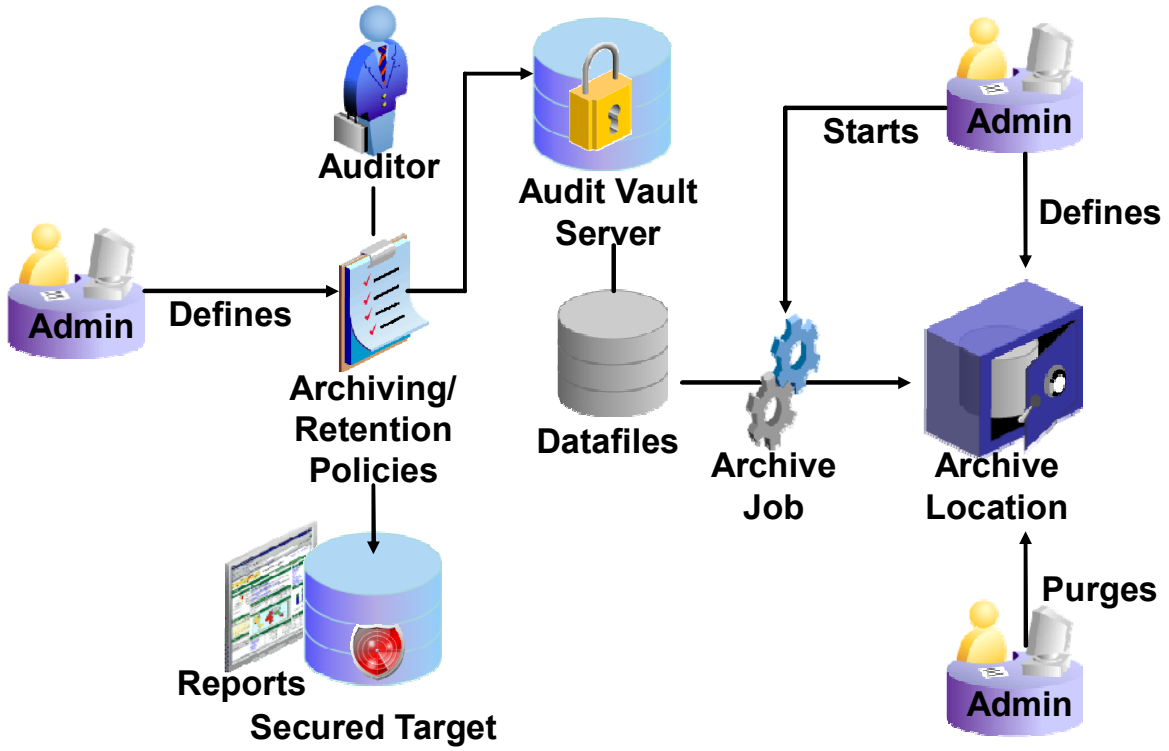
- Start an archive job
- Restore audit data that was archived
- Monitor jobs
- Manage the Audit Vault Agent
- Back up the Audit Vault Server

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Managing Audit Data Retention



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You can archive data files in Oracle Audit Vault and Database Firewall (Oracle AVDF) as part of your information life cycle strategy. Once data files meet the requirements of the archiving policy, the data is no longer visible in reports. The data is physically removed from the Audit Vault Server when it is archived. Data in the archive location can be restored to the Audit Vault Server if necessary.

The tasks are as follows:

- Create archiving (or retention) policies specifying:
  - The number of months to retain audit data online in Oracle AVDF
  - How many months to retain data in the archives before purging
- Configure archive locations to which data will be transferred according to the policies. You can create different data file archives for each secured target.
- Specify a retention policy for each secured target, as well as for scheduled reports. If the auditor does not select a retention policy for a secured target or scheduled report, the default retention policy of 12 months online and 12 months in archives before purging applies.
- Start archive jobs by selecting data files from those that are ready for archiving according to specified retention policies.
- Manually purge data from the archive locations according to the retention policy.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle AVDF Administrator's Role in Audit Data Management

- Create archiving (or retention) policies specifying:
  - The number of months to retain audit data online in Oracle AVDF
  - How many months to retain data in the archives before purging (purging is not automatic)
- Configure archive locations to which data will be transferred according to the policies (archiving is not automatic).
- Start archive jobs by selecting data files from those that are ready for archiving according to the retention policies.
- Manually purge data from the archive locations according to the retention policy.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The AVDF administrator performs the tasks listed in the slide with respect to managing audit data in the Audit Vault Server.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle AVDF Auditor's Role in Audit Data Management

- Select a specific retention policy for:
  - Each secured target
  - Scheduled reports

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The AVDF auditor performs the tasks listed in the slide with respect to managing audit data in the Audit Vault Server.

When an Oracle AVDF auditor selects a retention policy for a secured target, audit data for that secured target will be available for archive jobs based on the value specified for "months online" in the retention policy. After the months online period has expired, the data is available for archiving. In addition, after the months online period has expired the data is no longer visible in reports.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Starting an Archive Job

Enter the following information on the Archive page:

- Job Name: Name for the archive job
- Archive Location: Selected location for the archive
- Select data files from those that are ready for archiving according to specified retention policies.

ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

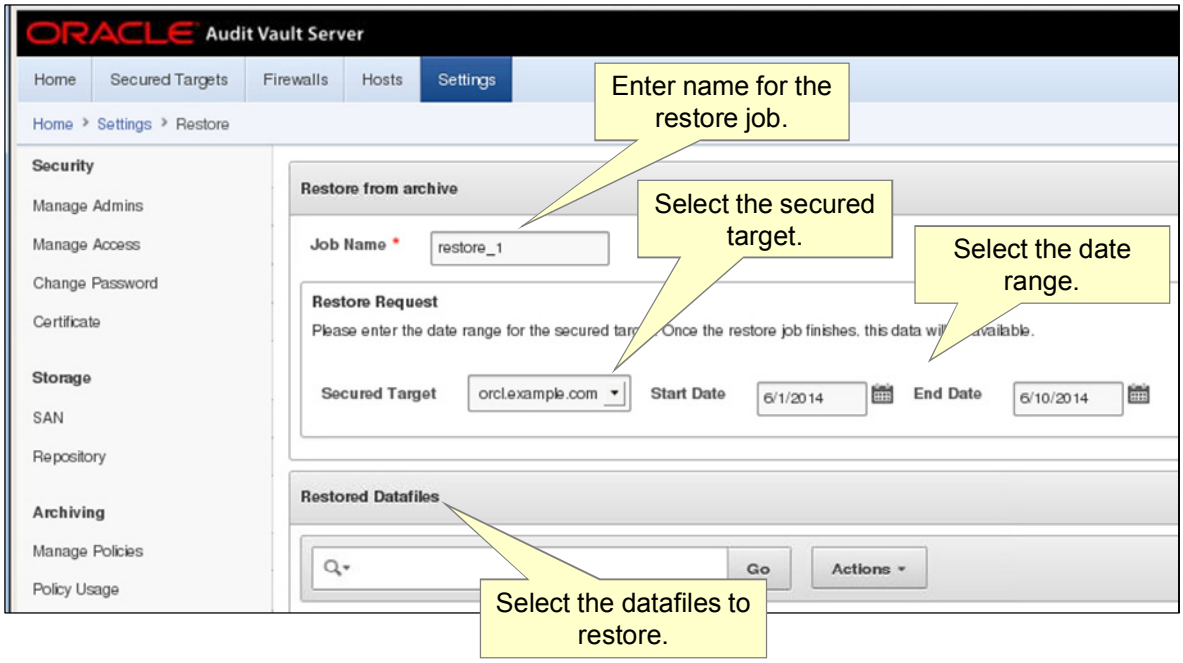
To start an archive job, select data files from those that are ready for archiving according to specified retention policies.

You must configure at least one archive location before you can start an archive job.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Restoring Audit Data



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

If data has been archived and is needed again for reporting, it can be restored.

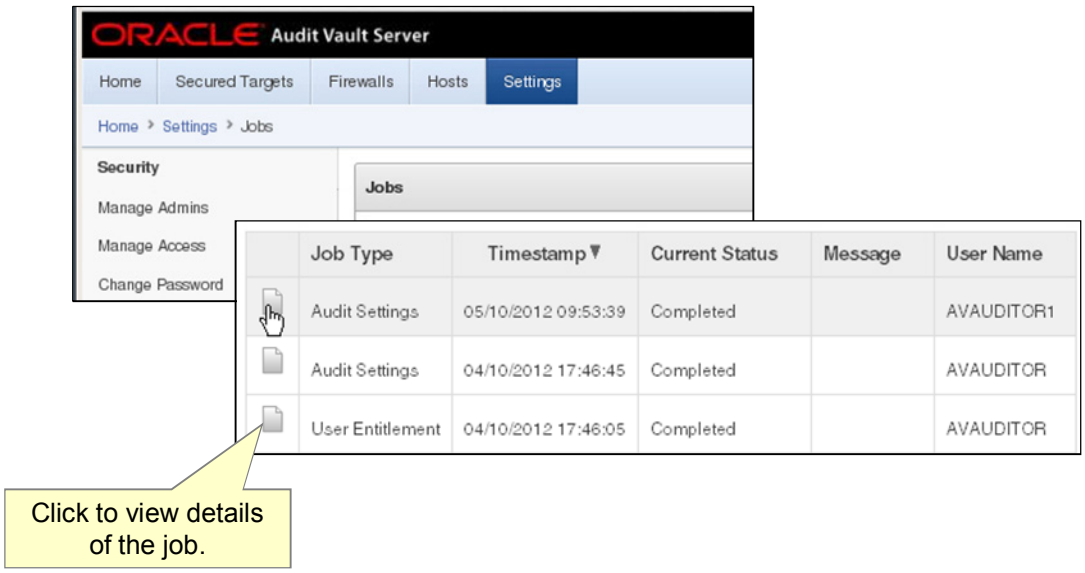
You can restore data files for a specific secured target and time range. The Months Archived value in the retention policy determines how long the data is available for restoring to the Audit Vault Server. When the Months Archived period expires, the data is no longer available to restore.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Monitoring Jobs

You can monitor jobs by accessing the Jobs page in the Audit Vault Server console.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You can see the status of Audit Vault Server jobs by performing the following steps:

1. Log in to the Audit Vault Server as an Administrator.
2. Click the Settings tab.
3. In the System menu, click Jobs. A list of jobs is displayed, showing the job type, ID, timestamp, status, and associated username.
4. To see details for an individual job, click the icon to the left of the job.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Managing the Audit Vault Agent

- Check the status of the Audit Vault Agent.

```
$ ./agentctl status
Agent is running.
```

- Start the Audit Vault Agent.

```
$ ./agentctl start
Agent started successfully.
```

- Stop the Audit Vault Agent.

```
$ ./agentctl stop
Stopping Agent...
```

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You can check the status of the Audit Vault Agent by executing the `agentctl status` command on the host computer.

You can start the Audit Vault Agent by executing the `agentctl start` command on the host computer. You may need to execute this command if the host computer has been rebooted.

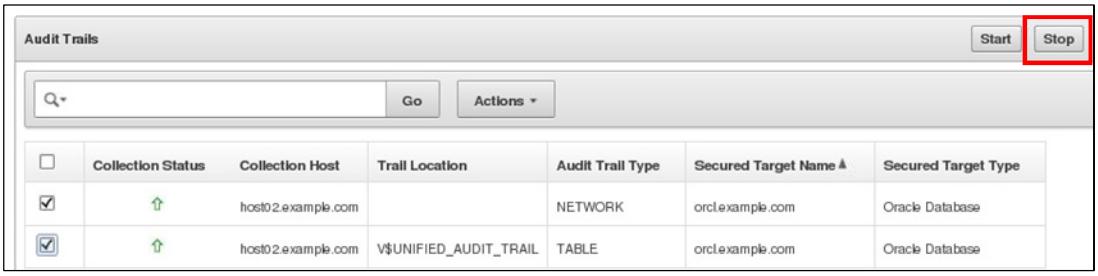
If there is a problem with the Audit Vault Agent, you may need to stop it by executing the `agentctl stop` command on the host computer.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Deactivating and Removing the Audit Vault Agent

- Stop all audit trails being collected by the Audit Vault Agent



- Stop the Audit Vault Agent

```
$ ./agentctl stop
```

- Deactivate the Audit Vault Agent on the host computer

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Perform the following steps to deactivate and remove the Audit Vault Agent:

1. Stop all audit trails being collected by the Audit Vault Agent by accessing the Audit Trails page in the Audit Vault Server console, selecting the audit trails, and clicking Stop.
2. Stop the Audit Vault Agent by executing the `agentctl stop` command on the host computer.
3. Deactivate the Audit Vault Agent on the host computer by accessing the Hosts page in the Audit Vault Server console, selecting the host, and clicking Deactivate.
4. Delete the Audit Vault Agent home directory on the host computer.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Backing Up and Restoring the Audit Vault Server

Create a manual backup of the Audit Vault Server installation and restore that backup by following the instructions in article 556200.1 on My Oracle Support:

- Download the `12.1.2.0.0.tar.gz` file attached to the note to obtain the Bash shell scripts for this procedure.
- To create a backup, configure and execute the `backup_restore.sh` script.
- To restore a backup, perform the following steps:
  1. Install the same Audit Vault Server version on the replacement hardware.
  2. Set the date and time of the replacement Audit Vault Server.
  3. Put the backup directory at the same absolute path location.
  4. Configure and execute the `backup_restore.sh` script.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The information in the slide is a high-level overview of the procedure outlined in article number 1556200.1 on the My Oracle Support web site.

All scripts must be run by the root user.

When a backup is taken, the Audit Vault Server's configurations and database data are copied to the backup directory.

The disk space needed by the backup directory is determined by the size of the Audit Vault Server's internal database. To find the database size, execute the following command in SQL*Plus: `select sum (bytes)/1024/1024/1024||' GB' from dba_data_files`

To create a backup, configure and execute the `backup_restore.sh` script. The user-configurable portion of this script is above the line "STOP! No user customization variables below this line."

The restored Audit Vault Server uses all the configurations of the original server; therefore, it is not recommended to have both the restored and original Audit Vault Servers online at the same time in a single network due to IP address and database name conflicts.

During execution of the scripts, logs are written to the location specified by the TMP_DIR variable.

Note: Always review article number 1556200.1 on My Oracle Support before performing this procedure to obtain the most current set of detailed instructions and scripts.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

An archiving job is started automatically based on the retention policy.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Start an archive job
- Restore audit data that was archived
- Monitor jobs
- Manage the Audit Vault Agent
- Back up the Audit Vault Server

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 12

- 12-1: Verifying an Archived Location Definition
- 12-2: Starting an Archive Job
- 12-3: Restoring Archived Data Files

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

13

Managing the Database Firewall

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- View and capture network traffic in a Database Firewall
- View diagnostics for the Database Firewall
- Describe how to remove a Database Firewall from the Audit Vault Server

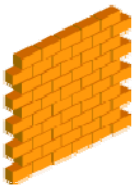
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Viewing and Capturing Network Traffic in a Database Firewall

- View and capture network traffic for debugging purposes:
  - View live network traffic going through a firewall
  - Capture the traffic to a file that you can download and review
- Level of detail:
  - Summary
  - Packet
- Enable in the Database Firewall console by selecting File Capture under Network Traffic.



ORACLE

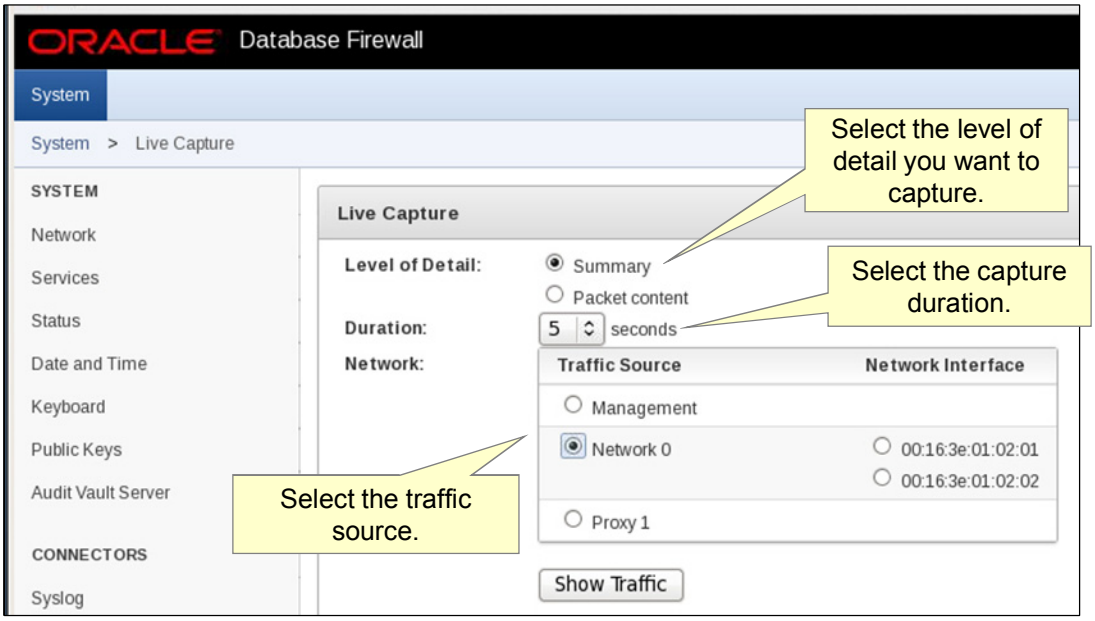
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You can view live network traffic going through a firewall, or capture the traffic to a file that you can download and analyze.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Viewing Live Network Traffic



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

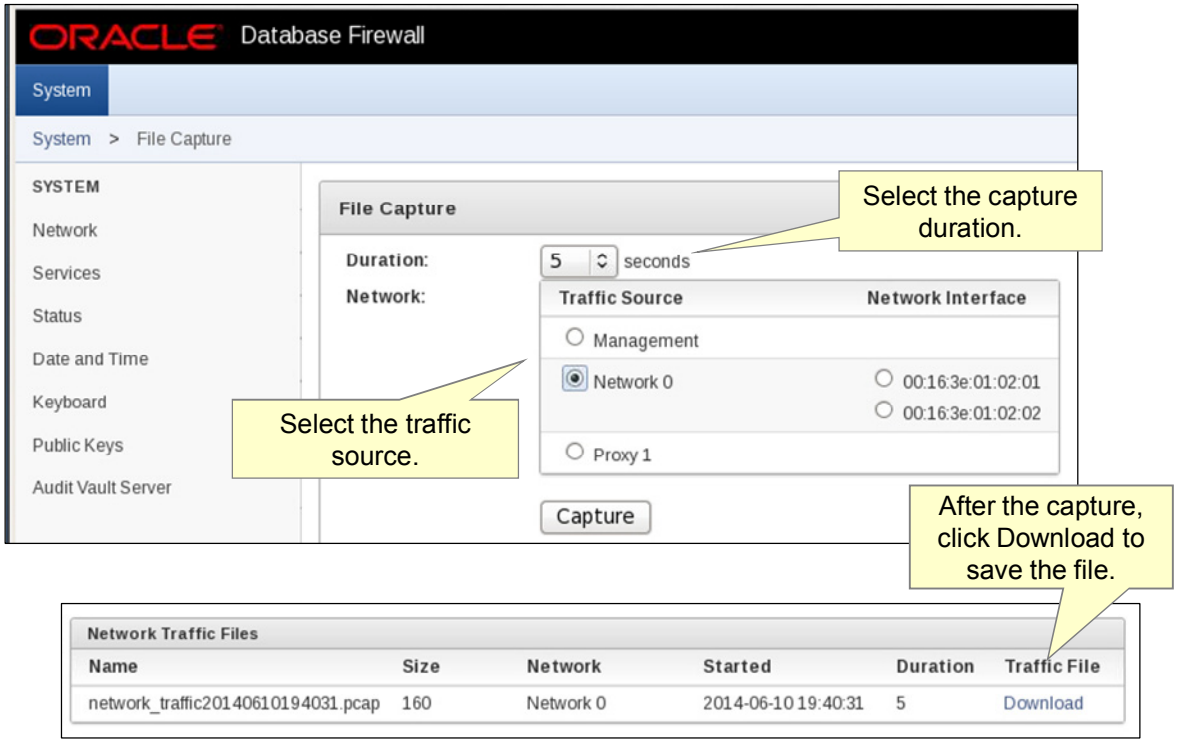
To view live network traffic in a Database Firewall, perform the following steps:

1. Log in to the Database Firewall console.
2. Under Network Traffic, click Live Capture.
3. In the Level of Detail field, select Summary or Packet Content.
4. In the Duration field, select the number of seconds to capture live traffic.
5. In the Network field, select the network traffic source for which to capture traffic.
6. Click Show Traffic.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Capturing Network Traffic to a File



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To capture network traffic to a file, perform the following steps:

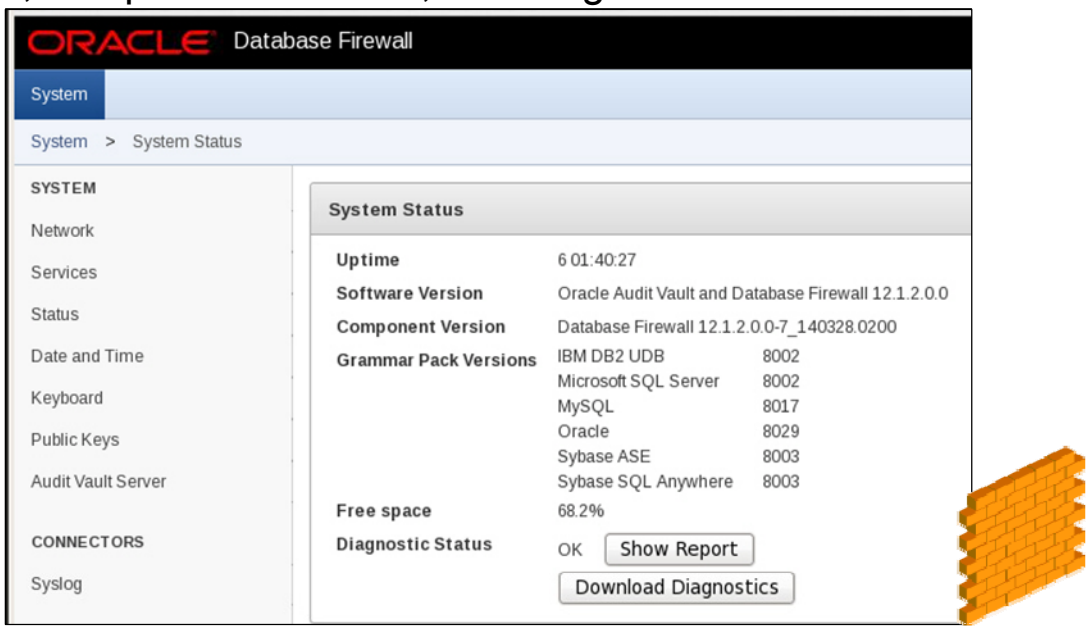
1. Log in to the Database Firewall console.
2. Under Network Traffic, click File Capture.
3. In the Duration field, select the number of seconds to capture traffic.
4. In the Network field, select the network traffic source for which to capture traffic.
5. Click Capture.
   The traffic file (`.pcap` format) is displayed in the Network Traffic Files list.
6. Click Download for the file you want to download.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Viewing the Status and Diagnostics Report for a Database Firewall

Status page in the Database Firewall console displays system status, component versions, and diagnostic status.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To view the status and/or diagnostic report for a Database Firewall, perform the following steps:

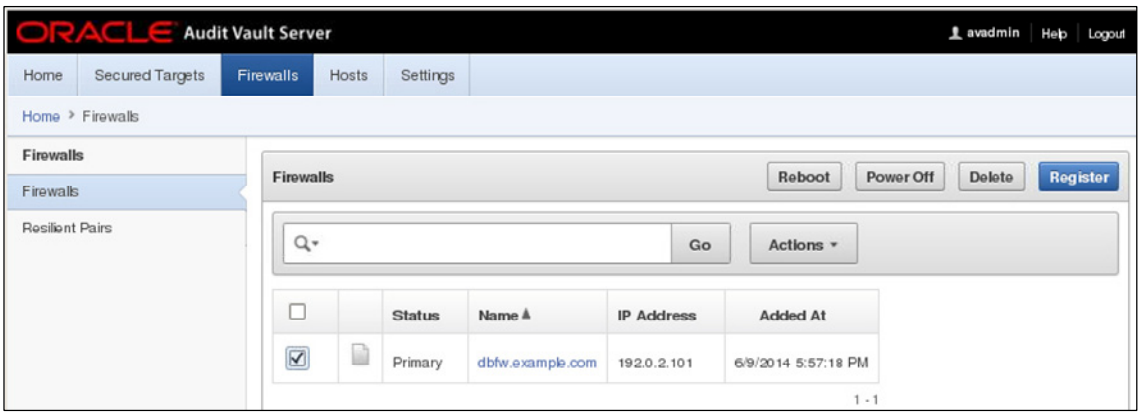
1. Log in to the Database Firewall console. The Status page is displayed by default.
2. If necessary, in the System menu, click Status. The Status page displays system status, component versions, and diagnostic status. The text next to Diagnostic Status indicates OK or Error.
3. To view the diagnostics report, click Show Report next to the Diagnostic Status field.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Removing a Database Firewall from the Audit Vault Server

Select the Database Firewall you want to remove and click Delete.



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To remove a Database Firewall from the Audit Vault Server:

1. Log in to the Audit Vault Server as an administrator.
2. Click the Firewalls tab, and then select the firewall(s) you want to remove.
3. Click the Delete button.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

When you remove a Database Firewall from the Audit Vault Server, the Database Firewall software is removed from the machine.

a. True
b. False

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- View and capture network traffic in a Database Firewall
- View diagnostics for the Database Firewall
- Describe how to remove a Database Firewall from the Audit Vault Server

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 13

- 13-1: Viewing Live Network Traffic
- 13-2: Capturing Network Traffic
- 13-3: Viewing the Database Firewall Status Report
- 13-4: Viewing a Database Firewall Diagnostic Report

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

14

Overview of the Auditing and Reporting Features

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Objectives

After completing this lesson, you should be able to:

- Describe Database Firewall policies
- Describe audit policies for Oracle Database
- Describe reports and report schedules
- Describe entitlement auditing for Oracle Database
- Describe stored procedure auditing
- Describe alerts and email notifications

ORACLE

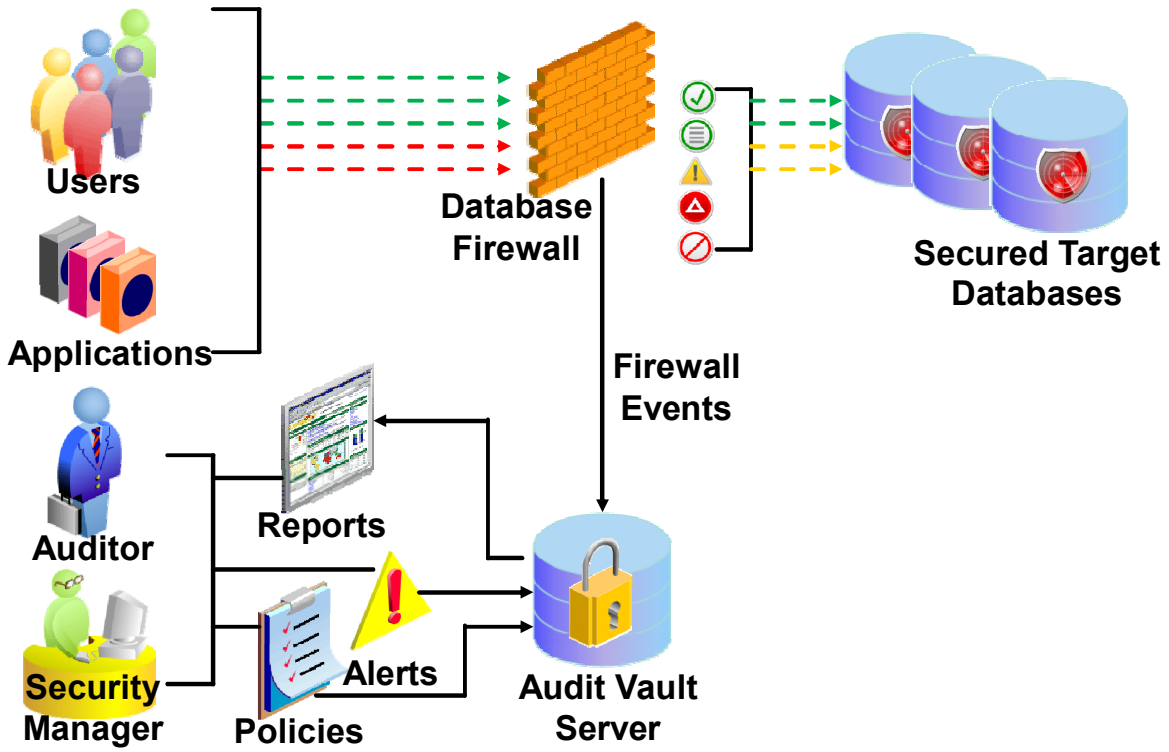
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This lesson provides an introduction to the tasks typically performed by an AVDF auditor. Detailed information on these tasks is provided in the course titled *Oracle Audit Vault and Database Firewall: Policies and Reports*.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Database Firewall Policies: Overview



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

A Database Firewall monitors SQL traffic to the database, logs activity, sends alerts, and can block specific types of SQL statements and replace them with substitute statements.

A Database Firewall policy specifies how the Database Firewall will handle SQL traffic to the secured target database.

Oracle Audit Vault and Database Firewall (Oracle AVDF) includes preconfigured Database Firewall policies, including policies that log all SQL statements, or log only unique SQL statements. The Database Firewall policy editor enables the AVDF auditor to design policies quickly and efficiently. The AVDF auditor can create the policy by analyzing current SQL statement traffic or providing a file of SQL statements, and then configuring settings in the firewall policy based on these statements. Policy rules can depend on any combination of the SQL statement type, name of the database user, IP address of the database client, operating system username, client program name, or any exceptions you specify.

After the AVDF auditor creates the policy, he or she can upload it to a secured target. A different policy can be assigned to each secured target.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Database Firewall Policy Enforcement

Database Firewall policy enforcement architecture provides:

- Performance and scalability: Millions of statements can be simplified into a small number of SQL characteristics or "clusters"
- High level of accuracy: SQL grammar–based analysis to enforce "normal" activity
- Flexible enforcement:
  - Statements can be blocked.
  - Statements can be passed and an alert generated.
  - Another SQL statement can be substituted for the statement.
  - Statements can be logged only.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

A Database Firewall *cluster* is a set of semantically similar SQL statements that is created when the Oracle AVDF reads logged SQL statements, either to create a model or when testing against new logged SQL data. Oracle AVDF uses its built-in knowledge of the SQL syntax to categorize the SQL statements into semantic clusters.

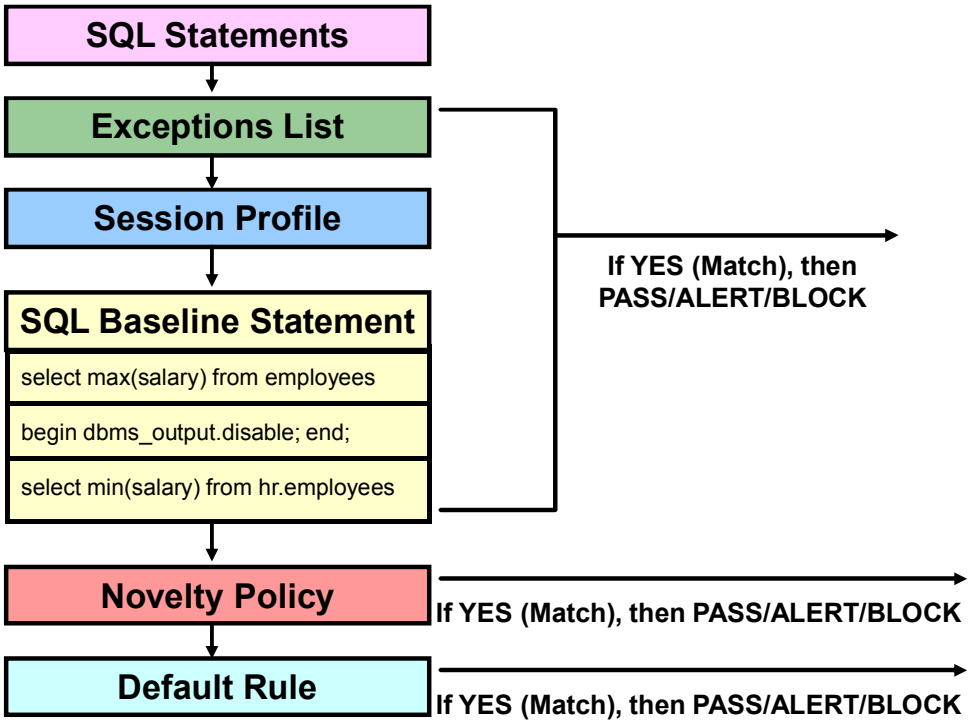
SQL statements are processed by using a powerful grammar-based analysis engine that decomposes and categorizes the SQL. In addition to looking at the SQL statement, policies can evaluate factors such as IP address, time, and program name.

Oracle AVDF monitors data access, enforces access policies, highlights anomalies, and helps protect against network-based attacks originating from outside or inside.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Database Firewall Policy Enforcement Flow



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Policy enforcement flow is key to understanding which statements will be matched and which will not. If a statement is matched, an action can be taken. If it is not matched, default rules determine the action taken by the Database Firewall.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Configuring Policies

Policies are easily configured by using:

- White list for positive security enforcement:
  - Can be automatically generated for any application
  - "Allowed" behavior can be defined for any user or application
  - Transactions that do not match the policy are rejected
- Black list for negative security enforcement:
  - Stop unwanted transactions, users, or schema access
  - Prevent privilege or role escalation and illegal access to sensitive data by using factors
  - Selectively block any part of transaction in context to your business and security goals

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle AVDF supports white list–based and black list–based policies.

A white list is a set of approved SQL statements. SQL traffic is compared with the white list. Based upon the policy, Database Firewall alerts, blocks, or substitutes a statement for the SQL statement.

A black list is used to block specific SQL statements.

Note: There is nothing in the Oracle AVDF product that refers to "white list" or "black list." Whether it is a white list or a black list depends upon how the policy is configured.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database Firewall Preconfigured Policies

Policy	Description
logall	Log all statements for offline analysis
logall-nomask	Log all statements for offline analysis without masking data
logsample	Log a sample of statements for offline analysis
passall	Pass all statements and log none
unique	Log examples of statements for offline analysis covering each distinct source of traffic
unique-nomask	Log examples of statements for offline analysis covering each distinct source of traffic in the statements

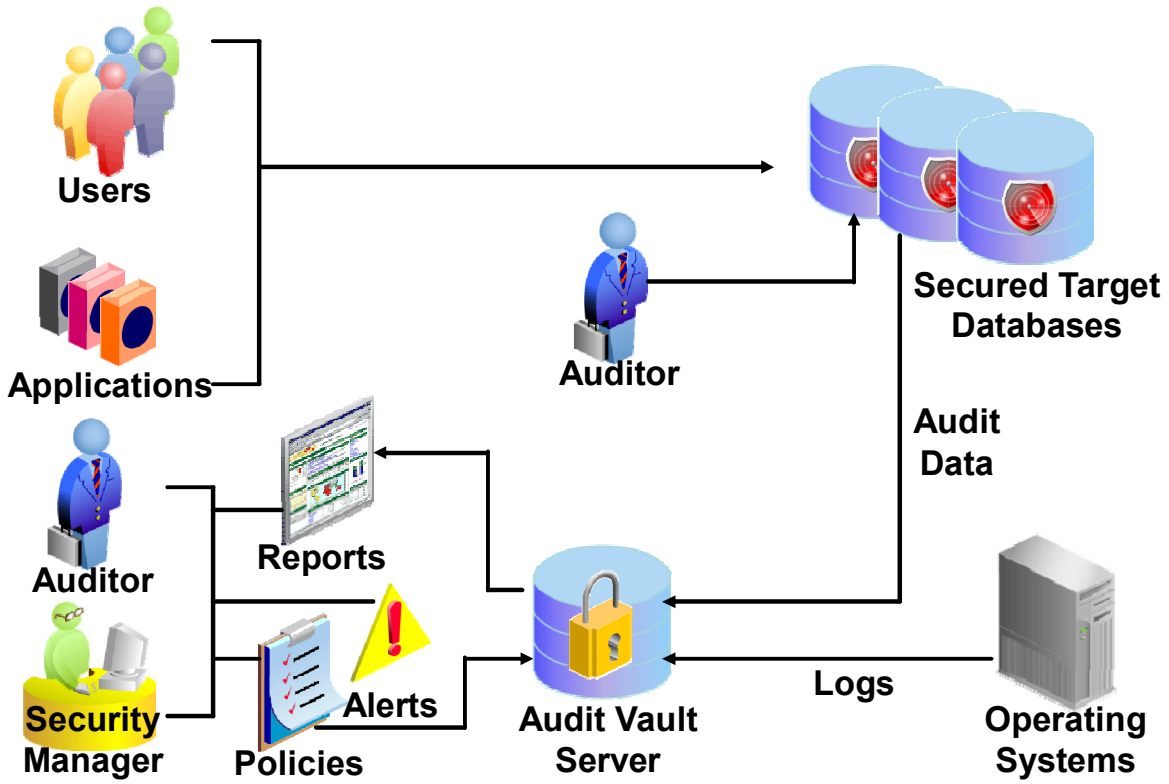
ORACLE
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Database Firewall includes the policies listed in the slide as part of the product installation. The preconfigured firewall policies can be viewed on the Firewall Policies page in the Audit Vault Server console.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Audit Policies: Overview



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle AVDF auditor can retrieve audit data from secured targets and generate various reports.

If the secured target is an Oracle Database, the AVDF auditor can configure and provision audit policies for the database by using the Audit Vault Server console. The AVDF auditor can retrieve the current audit settings from an Oracle Database and modify them, as well as add new audit policies, for the following:

- SQL statements
- Database objects
- Fine-grained auditing
- Capture rules for redo log activity

After the AVDF auditor configures the audit policies for an Oracle Database, the policies can be provisioned to the database. Through the Audit Vault Server console the AVDF auditor will be able to determine whether the policies are changed by a database administrator.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Reports and Report Schedules: Overview

- Reports include information on audit data, entitlements, and stored procedures.
- Oracle AVDF auditor can:
  - Schedule, print, and/or email the reports to others in PDF or XLS format
  - Browse and customize report data interactively
  - Generate compliance reports to comply with regulations associated with credit card, financial, data protection, and health care–related data

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

An Oracle AVDF auditor can generate various audit reports for the secured targets to which he or she has access. The Oracle AVDF auditor can schedule, print, and/or email the reports to others in PDF or XLS format. Reports include information on audit data, entitlements, and stored procedures. Compliance reports to comply with regulations associated with credit card, financial, data protection, and health care–related data can also be generated.

The Oracle AVDF auditor can also browse and customize report data interactively, and upload custom reports created with third-party tools.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database Entitlement Auditing: Overview

- *User entitlement*: Range of access to the database system
- To generate data for entitlement reports:
  - Retrieve entitlement audit data to create a snapshot
  - Optionally, organize the snapshots into a group and assign a label

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

User entitlement refers to the range of access that a user has to a database. User entitlement in an Oracle database includes system and other SQL privileges, object privileges, role privileges, and user profiles that enable users to access the database system.

Entitlement audit data must be retrieved from the source database. The retrieved entitlement data is referred to as a *snapshot*. The snapshot name includes the time stamp of when the entitlement data was retrieved from the source database. Snapshots can be grouped by assigning the snapshots to a *label*.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database Entitlement Auditing Reports

Entitlement Reports

User Accounts	Details of all existing user accounts
User Accounts by Secured Target	User accounts by Secured Target report
User Privileges	Details of audited failed user logins for a specified period of time
User Privileges by Secured Target	User privileges by Secured Target report
User Profiles	Digest of all existing user profiles
User Profiles by Secured Target	User profiles by Secured Target report
Database Roles	Digest of all existing database roles and application roles
Database Roles by Secured Target	Database roles by Secured Target report
System Privileges	Details of all existing system privileges and their allocation to users
System Privileges by Secured Target	System privileges by Secured Target report
Object Privileges	Details of all existing object privileges and their allocation to users
Object Privileges by Secured Target	Object privileges by Secured Target report
Privileged Users	Details of all existing privileged users
Privileged Users by Secured Target	Privileged users by Secured Target report

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle AVDF includes a set of default entitlement reports. An AVDF auditor can filter a report to show the data from an earlier snapshot or label, or compare the entitlement data from two snapshots or two labels.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle Database
Stored Procedure Auditing: Overview

- Audit changes to stored procedures in a secured target
- Stored procedure auditing for the secured target enabled
- Reports

Stored Procedure Audit Reports

Stored Procedure Activity Overview	Digest of all audited operations on stored procedures for a specified period of time
Stored Procedure Modification History	Details of audited stored procedure modifications for a specified period of time
Created Stored Procedures	Stored procedures created within a specified period of time
Deleted Stored Procedures	Stored procedures deleted within a specified period of time
New Stored Procedures	Latest state of stored procedures created within a specified period of time

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Stored procedure auditing enables Oracle AVDF auditors to audit changes to stored procedures on secured target databases.

Stored procedure auditing must be enabled for the secured target. Refer to the lesson titled “Configuring Oracle AVDF and Deploying the Audit Vault Agent” for details on configuring stored procedure auditing.

Stored procedure audit reports provide information on all stored procedure operations, deleted and created procedures, as well as modification history.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Alerts and Email Notifications: Overview

- Define rule-based alerts on audit records.
- Alerts can be created and configured on events for secured targets and for third-party plug-ins.
- Specify notification actions for the alerts:
  - Email message can be automatically sent to a user or to a distribution list.
- Configure templates to be used for email alert notification.
- Monitor and respond to alerts from the Audit Vault Server console and from alert reports.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The AVDF auditor can define rule-based alerts on audit records and specify notification actions for those alerts. Whenever an audit event meets the rule or condition defined in the alert definition, an alert is raised and a notification is sent as specified.

The AVDF auditor can monitor and respond to alerts from the Audit Vault Server console and from alert reports.

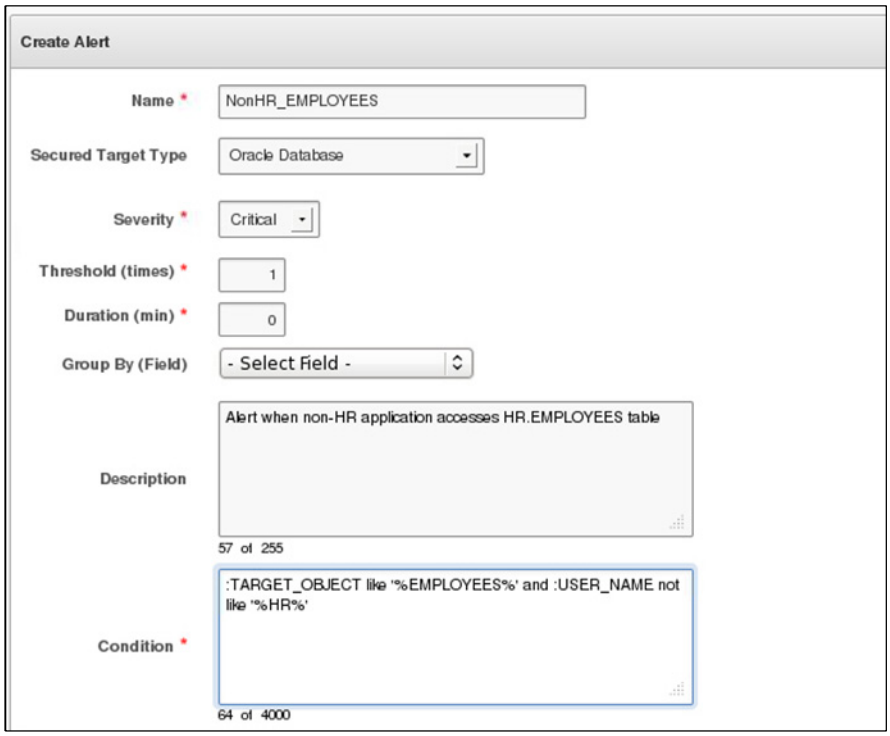
Alerts can be created and configured on events for secured targets, and for third-party plug-ins that have been developed by using the Oracle AVDF SDK. These events may be collected by the Audit Vault Agent or the Database Firewall. Alerts are independent of audit policies or firewall policies.

When the AVDF auditor configures an alert, he or she can set it up so that an email message is automatically sent to a user, such as a security officer, or to a distribution list. The AVDF auditor can also configure templates to be used for email alert notification.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Creating an Alert



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You can define alerts by type of secured target, the number of times an event occurs, and by using available fields in audit records to define a Boolean condition that must be met. You can also configure email templates to be used for alert notifications.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Quiz

The AVDF auditor can use the Audit Vault Server console to perform which of the following reporting activities?

a. Filter report data
b. Create a PDF file of a report
c. Schedule the creation of a PDF file of a report
d. Store a report in the source database

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a, b, c

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Summary

In this lesson, you should have learned how to:

- Describe Database Firewall policies
- Describe audit policies for Oracle Database
- Describe reports and report schedules
- Describe entitlement auditing for Oracle Database
- Describe stored procedure auditing
- Describe alerts and email notifications

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Practice 14

- 14-1: Identifying Steps to Create an Audit Policy
- 14-2: Viewing the Auditor's Dashboard
- 14-3: Determining Whether Built-in Reports Satisfy Requirements

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle University and Error : You are not a Valid Partner use only

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED

Oracle University and Error : You are not a Valid Partner use only