Oracle® Audit Vault and Database Firewall

Concepts Guide

Release 12.2
E49916-15
March 2021

Oracle Audit Vault and Database Firewall Concepts Guide, Release 12.2

E49916-15

Primary Authors: Karthik Shetty, Gigi Hanna

Contributing Authors: Andrey Brozhko

Contributors: Sunil Channapatna Ravindrachar, Marek Dulko, Paul Hackett, Ravi Handyal, Anita Hegde, William Howard-Jones, Sachin Deshmanya, Shirley Kumamoto, Ravi Kumar, Paul Laws, Harm Joris Napel, Eric Paapanen, Scott Rotondo, Vipin Samar, Sreekumar Seshadri

Contents

List of Figures

List of Tables

Preface

Oracle Audit Vault and Database Firewall Concepts Guide introduces the concepts and terminology used in Oracle Audit Vault and Database Firewall (also referred to as Oracle AVDF). This document provides an overview of the main features used by Database Auditors, Database Administrators, and developers.

Audience

This document is intended for security managers, audit managers, and database administrators (DBAs) who are involved in the configuration of Oracle Audit Vault and Database Firewall.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Downloading the Latest Version of this Manual

You can download the latest version of this manual, as well as the entire Oracle Audit Vault and Database Firewall online library, from the following website:

`http://www.oracle.com/pls/topic/lookup?ctx=avdf122`

You can find documentation for other Oracle products at the following website:

`http://docs.oracle.com`

Where to Find More Information

Oracle Audit Vault and Database Firewall collects audit data from databases and operating systems. It secures the critical components of the IT infrastructure. It monitors the activity and blocks SQL statements on the network.

For detailed instructions about configuring and using Oracle Audit Vault and Database Firewall, refer to these documents:

- *Oracle Audit Vault and Database Firewall Administrator's Guide*: This guide provides the following instructions:
  - Configuring and administering Oracle Audit Vault and Database Firewall
  - Deploying the Audit Vault server, Database Firewall, and Audit Vault Agent
  - Backing up and restoring data
  - Configuring high availability
  - Archiving data
  - Setting up external storage
- *Oracle Audit Vault and Database Firewall Auditor's Guide*: This guide provides the following instructions:
  - Creating audit policies and firewall policies
  - Generating reports
  - Creating alerts on audit and firewall data
  - Creating alert notification templates
- *Oracle Audit Vault and Database Firewall Developer's Guide*: This guide provides instructions for creating, packaging, and testing custom audit collection plug-ins.

Related Documents

For more information, see the following documents in the documentation set:

- *Oracle Audit Vault and Database Firewall Release Notes*
- *Oracle Audit Vault and Database Firewall Installation Guide*
- *Oracle Audit Vault and Database Firewall Administrator's Guide*
- *Oracle Audit Vault and Database Firewall Auditor's Guide*
- *Oracle Audit Vault and Database Firewall Developer's Guide*
- *Oracle Audit Vault and Database Firewall Licensing Information*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Changes In This Document

This section lists the updates and correction to the document in Oracle Audit Vault and Database Firewall (AVDF) release 12.2.

Revision History

The following are the updates and correction in this document.

E49916-13 (September 2019)

- Updates and correction to Database Firewall deployment types. See Introduction to Oracle Database Firewall Deployment (page 4-1) for complete information.
- Updates and correction to the entire document.

E49916-12 (June 2019)

Included information on Database Firewall deployment types:

- In-line (bridge) (page 4-2)
- Proxy (page 4-4)
- Out-of-Band (page 4-6)
- Host Monitor (page 4-7)

E49916-11 (October 2018)

- Minor update to section Introduction to Oracle Database Firewall Deployment (page 4-1).
- **F5 BIG-IP ASM** integration is deprecated in release `12.2.0.7.0`, and will be desupported in `19.1.0.0.0`. This functionality is only supported on **F5 BIG-IP ASM** version `10.2.1`.
- **Micro Focus Security ArcSight SIEM** is deprecated in `12.2.0.8.0` and is desupported in `12.2.0.9.0`. Use the `syslog` integration feature instead.
- See About Oracle Audit Vault Information Lifecycle Management (page 1-11).
- See the following sections regarding change in supported systems and components:
  - Integrating Oracle AVDF with F5 BIG-IP ASM (page 1-17)
  - Integrating Syslog With a SIEM System (page 1-18)

E49916-10 (June 2018)

- Added important information relating to Available Built-in Reports (page 5-3).
- **Micro Focus Security ArcSight SIEM** (previously known as **HP ArcSight SIEM**) is deprecated in `12.2.0.8.0`, and will be desupported in `12.2.0.9.0`.

It is advisable to use the `syslog` integration feature instead. Updated section Integrating Syslog With a SIEM System (page 1-18).

- In-line bridge mode is deprecated in `12.2.0.8.0`, and will be desupported in `19.1.0.0.0`. It is advisable to use proxy mode as an alternative.
- See the following sections regarding change in supported systems and components:
  - Introduction to Oracle Database Firewall Deployment (page 4-1)
  - Planning and Rolling Out the Database Firewall (page 4-15)
  - Integrating Oracle AVDF with F5 BIG-IP ASM (page 1-17)
  - Integrating Syslog With a SIEM System (page 1-18)
- Added an important note on assigning roles to the source user for running the REDO collector with Database Vault. See section Available Built-in Reports (page 5-3) for more information.
- Added important information regarding in-line bridge mode and proxy mode in section Introduction to Oracle Database Firewall Deployment (page 4-1).

E49916-09 (February 2018)

F5 is deprecated in release `12.2.0.7.0`, and will be desupported in `19.1.0.0.0`.

E49916-08 (December 2017)

Minor cosmetic changes to the document.

E49916-07 (August 2017)

- Included important instruction in Introduction to Oracle Audit Vault Agent Deployment (page 3-1).
- The **Data Modification Before-After Values Report** displays both before and after values in the main report. See Available Built-in Reports (page 5-3) for complete information.
  - Filter on **Column Name** can be added in before and after values report.
  - Information Lifecycle Management is extended for before and after values data.

E49916-06 (June 2017)

Included important note. See How Oracle Audit Vault and Database Firewall Fits into the Oracle Security Architecture (page 1-6) for more information.

E49916-05 (December 2016)

Introducing support for retrieval of data from multiple targets. Updated section Planning and Rolling Out the Audit Vault Server (page 2-1).

1

Overview of Oracle Audit Vault and Database Firewall

Topics

1.1 Introduction to Database Security

Topics:

1.1.1 What Is Auditing?

Auditing is the main tool in the "trust but verify" approach to security, as well as a tool for forensic analysis, that is, finding who performed certain actions and when they performed these actions.

Maintaining an audit trail of activity is an essential component of any defense-in-depth strategy for securing a system. Even when access controls are properly configured and privilege grants are minimized, two important risks still remain. The first is that users who need significant privileges to perform their jobs may misuse those privileges. The second is that a user may gain unexpected access through access controls or privilege grants that are unintentionally configured to be more generous than necessary. Auditing is the primary tool for detecting the actions that these users perform so that they can be corrected.

Effective auditing requires audit policies that are selective in capturing the important details about significant events while minimizing the noise from routine activity. Some of the most important events to audit in databases are failed logins, events requiring access by privileged users, and data definition (DDL) types of activities such as `CREATE`, `DROP`, `ALTER`, `RENAME`, or `TRUNCATE`. Besides databases, other systems such as operating systems, file systems, and directory services, also have audit data that can be collected. Auditing provides a history of who did what and when, and enables organizations to meet stringent controls and reporting requirements.

In addition, many customers must audit systems to comply with SOX, HIPAA, PCI DSS, GLB, FISMA, and other international standards. Internal governance, local security policies, and forensic reporting also drive the need to audit.

Auditing requires secure storage and controlled access for the audit data so that it cannot be manipulated to hide suspicious activities. Auditing also requires convenient ways to search through the collected audit data to find specific information or detect unusual activity.

You may be using Oracle Database's robust auditing features as well as auditing features of other database products. Regardless of whether you are using Oracle Database, auditing and auditing features of other database products are important to make sure that your systems are provisioned with sufficient storage capacity to sustain the amount of audit data collected. Oracle Database's native auditing has low overhead and does not degrade performance when done correctly. When using other database products, refer to their documentation libraries as necessary.

Related Topics

- Understanding Audit Data Collection and Audit Policies (page 3-3)
  Learn about audit data collection and audit policies.
- What to Audit (page 3-3)
- Predefined Unified Audit Policies for Oracle Database (page 3-6)
  If you use Oracle Database 12c or later, and have migrated to unified auditing, then you can take advantage of six predefined unified audit policies.

1.1.2 What Is Database Activity Monitoring?

With effective monitoring of SQL input to the database, you can block or raise alerts for attempted policy violations and provide comprehensive reports about database activity for compliance purposes.

Most applications today operate using a single user account for communicating with the database, and many do not validate their input sufficiently. This application architecture, combined with the increasing number of attacks on databases via SQL injection or insiders with access to privileged accounts, has made database activity monitoring an important component of the overall security architecture.

SQL injection is perhaps the most common attack approach to databases. SQL injection exploits flaws in application code—the application that sends SQL statements to a database. Given that much of that application code is written without analyzing possible SQL injection issues, many applications are exposed to vulnerabilities.

Whereas auditing captures events that already happened at the database, the Database Firewall monitors, and optionally blocks, malicious SQL before it reaches the database. Database Firewall not only monitors the connection to the database, but it monitors any connection to the database whether coming from an application server or a user connecting to the database directly. This monitoring reduces both insider threats, as well as the ability of an outsider to launch a successful SQL injection attack.

Database Firewall policies can be used to monitor, alert, block, and/or substitute SQL based on user session information, such as IP address or user name, or based on the SQL grammar itself. In this way, you can use a firewall to both allow approved SQL and disallow specific SQL statements.

Related Topics

- Introduction to Oracle Database Firewall Deployment (page 4-1)
  Depending on your requirements, you can choose from one of three types of deployments available for Oracle Database Firewall.
- Understanding Oracle Database Firewall Policies (page 4-9)

1.1.3 Why Auditing and Monitoring?

Auditing and monitoring provides security against data breaches.

In today's global enterprise environments, security must be considered as important as high availability and scalability. Studies indicate that the most prevalent data breaches involve access by privileged users and SQL injection attacks. A DBA, or someone using a DBA user account privileged access rights, can walk out of the office with enormous amounts of sensitive data. Similarly, a remote intruder can gain access to sensitive data, and exploit a SQL injection vulnerability.

The recommended approach to securing data against breaches due to access rights is to "trust but verify." You can trust your privileged users, but you need tools to verify that neither they, nor others who have gained access to their privileges, have accessed data, or violated your security policies. Similarly, applications that access your databases are often vulnerable to SQL injection attacks if they are not programmed with the correct security considerations.

The Oracle solution to these problems is Oracle Audit Vault and Database Firewall. Oracle Audit Vault and Database Firewall can collect audit data from many different types of systems that produce audit trails. It also can monitor network activity to databases, analyze all SQL statements, and take appropriate action before this SQL reaches your database. This capability is called **monitoring and blocking mode**.

Oracle Audit Vault and Database Firewall provides support for Oracle Database, third-party databases, and operating systems. It provides the ability to capture and analyze audit data from Oracle Database, other databases, and operating system logs.

Related Topics

- How Oracle Audit Vault and Database Firewall Fits into the Oracle Security Architecture (page 1-6)
  Oracle Audit Vault and Database Firewall is the key component of the Oracle security architecture.

1.2 What Is Oracle Audit Vault and Database Firewall?

Topics:

1.2.1 Introduction to Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall provides a comprehensive way to deal with a large amount of audit data, the risk from SQL injection, application bypass attacks over the network, and problems of unauthorized access.

Deploying Oracle Database or third-party databases can produce a large amount of audit data to consolidate. In addition to audit data from databases, operating systems, file systems and other such systems produce audit trails that can be used to analyze events relevant to security.

Standard security practices require that you transmit and manage audit data on a remote centralized location, where it is secure from tampering by the individuals whose activities you want to audit.

With large amount of audit data, it is important to have a mechanism to efficiently monitor the ongoing stream of data, to find the specific events with security implications, and to identify problems that need immediate attention.

In addition to managing a stream of audit data from heterogeneous systems, it is important to protect against SQL injection attacks, and to monitor traffic going into the database.

A Comprehensive Solution

Oracle Audit Vault and Database Firewall:

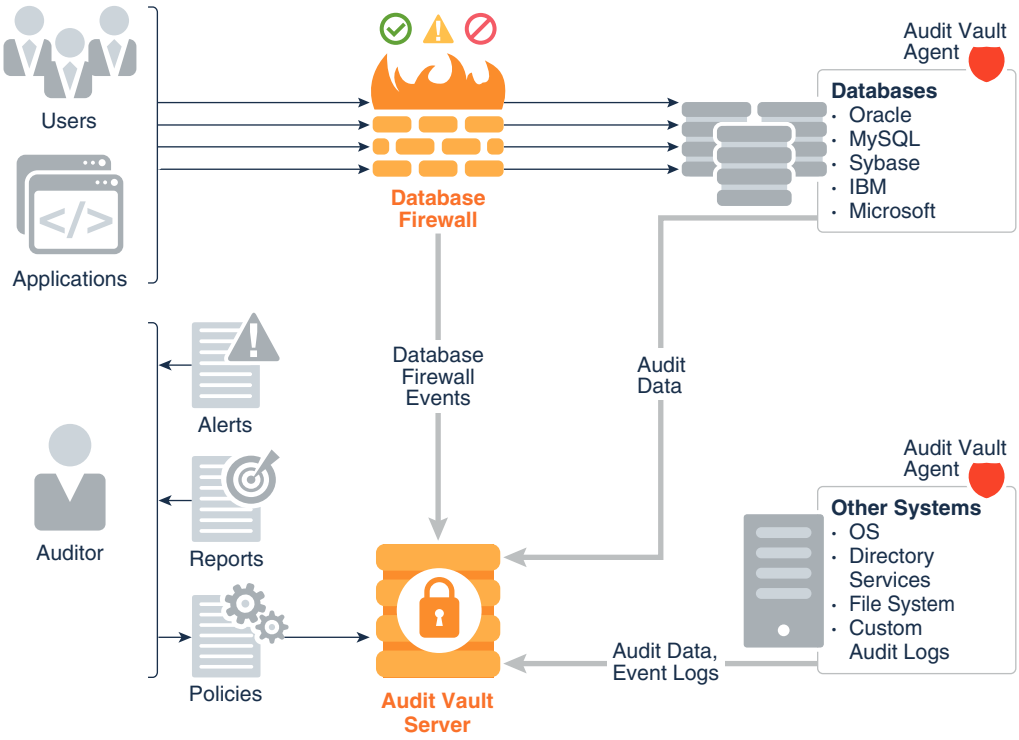
- Collects audit data from Oracle Database and third-party databases
- Supports audit collection from operating systems, file systems, and directory services
- Is delivered as a software appliance
- Secures targets from SQL attacks
- Is easy to provision, and to use with predefined policies and reports
- Is easy to consolidate, and has a unified approach
- Collects audit data from database trails and firewalls

Oracle Audit Vault and Database Firewall solves these problems by collecting and consolidating audit data, monitoring network traffic, blocking and substituting of SQL, logging, policy management, raising alerts, and providing comprehensive reports for forensic and compliance purposes.

Oracle Audit Vault and Database Firewall has three components:

- **Audit Vault Server**, which stores audit data from various types of sources, enables you to manage Oracle Database audit policies, and manages Database Firewall policies to protect secured targets. A secured target refers to the audited or protected systems with their databases, operating systems, and file systems.
- **Audit Vault Agent**, which retrieves audit trails from the secured targets and sends audit data to Audit Vault Server. An audit trail is a set of audit records collected from a sequence of activities or events on a specified target. There can be more than one audit trail for a target depending on the activities being captured.
- A **database firewall**

Figure 1-1 Audit Vault and Database Firewall Architecture



You can choose to deploy Audit Vault Server with either the Audit Vault Agent component, or with the database firewall component, or with both components. You can use Oracle Audit Vault and Database Firewall to protect both Oracle Database, and third-party databases, and to protect both databases and non-databases such as operating systems, file systems, and directory services.

Related Topics

- Oracle Audit Vault and Database Firewall Components (page 1-8)

1.2.2 Audit Data Consolidation Functions

Using Oracle Audit Vault Server and Audit Vault Agents, you can consolidate audit data from multiple sources, manage Oracle Database audit policies, and monitor user entitlements.

For example:

- Consolidate audit data from multiple sources:
  - Database audit trails including Oracle Database, Microsoft SQL Server, SAP Sybase, IBM DB2 for LUW, and MySQL. These audit trails can be audit tables, audit files, or Oracle Database REDO records.
  - Stored procedure auditing (SPA), which enables you to audit changes to stored procedures on monitored databases
  - User role auditing (URA), which enables you to audit and approve changes to user roles in the databases on a specified database server

  - Operating system audit trails (Linux, IBM AIX, Oracle Solaris, Microsoft Windows)
  - Directory services, such as Microsoft Active Directory
  - File systems such as Oracle ACFS
  - Custom audit data in either database tables or XML files
- Manage Oracle Database audit policies
- Monitor Oracle Database user entitlements or activities

1.2.3 Oracle Database Firewall Functions

Oracle Database Firewall specifically protects databases from SQL attacks over the network, and monitors database activity on the network with alerts and warnings.

Using the combination of Oracle Audit Vault Server and Oracle Database Firewall, you can monitor SQL transactions to your databases. You can then decide whether a SQL statement should be permitted, blocked, or substituted before it reaches the database server.

Oracle Database Firewall sends database activity events to Oracle Audit Vault Server, which then provides specialized database firewall reports. Oracle Audit Vault Server consolidates both database firewall event logs, as well as audit events from other sources where you may have also deployed Audit Vault Agents to collect audit data.

1.2.4 How Oracle Audit Vault and Database Firewall Fits into the Oracle Security Architecture

Oracle Audit Vault and Database Firewall is the key component of the Oracle security architecture.

Oracle's security architecture provides both preventative and detective pillars of protection against threats. Oracle Audit Vault and Database Firewall is the key component of the detection pillar.

The following products form the prevention pillar:

- Oracle Advanced Security - This feature includes:
  - Transparent Data Encryption (TDE) - Automatically encrypts data before it is written on disk, and decrypts it when reading from the disk.
  - Oracle Data Redaction - Controls the display of sensitive data within applications.
- Oracle Key Vault - Securely manages database encryption keys.
- Oracle Database Vault - Controls access by privileged users.
- Oracle Data Masking and Subsetting - Masks sensitive data before exporting it from the database.
- Oracle Label Security - Simplifies the process of assigning labels to data and users and enforcing access control based on those labels

Related Topics

- Considerations for Deploying Network-Based Solutions

1.3 Oracle Audit Vault and Database Firewall Architecture, Components, and Roles

This section contains:

1.3.1 Oracle Audit Vault and Database Firewall Terminology

Use this Oracle Audit Vault and Database Firewall terminology when describing the system and its functions.

The following terms describe the Oracle Audit Vault and Database Firewall system and its functions:

- **Secured Targets**: the systems that you want to monitor and protect

  A secured target is any supported database or non-database system that you monitor with Oracle Audit Vault and Database Firewall. A secured target can be an Oracle Database, or a third party product. Secured targets can be monitored by the Oracle Audit Vault and Database Firewall Audit Vault Agent component, the database Firewall component (if the secured target is a database), or both components. All secured targets are registered in Audit Vault Server.

  Oracle Audit Vault and Database Firewall supports various secured target types out-of-the-box. These include various databases, operating systems, file systems, and directory services. To capture audit trails from more secured target types, you can also create custom **collection plug-ins** for Oracle Audit Vault and Database Firewall by using the Oracle Audit Vault and Database Firewall software development kit (SDK).

- **Audit Trails**: how you specify the location of the audit data to collect.

  An audit trail specifies the location and type of repository where the audit data is collected. To collect audit data from a secured target, you add one or more audit trails in Oracle Audit Vault and Database Firewall for each secured target from which you want to collect the data. Defining the audit trail in Oracle Audit Vault and Database Firewall specifies the type of audit trail you are collecting, and the location of the audit data on the secured target. For example, a database can have multiple audit trails, with a different audit trail for each location where audit data is written. You can specify audit trails for a table or a transaction log. Other systems have specific locations where audit data is written. For example, in a Linux operating system, the audit trail is located in the `audit.log` file.

- **Collection Plug-ins**: Agent components that collect audit data from specific secured target types.

  The Audit Vault Agent component contains a set of collection plug-ins. There is one collection plug-in for each type of secured target that is supported out of the box. For example, there is a plug-in for Oracle Database, another plug-in for the Linux operating system, and so on. Each plug-in collects data from a specific type

of audit trail, and maps the specific events from that audit trail to the audit record format in Oracle Audit Vault and Database Firewall.

You can also develop custom collection plug-ins to collect audit data from other audit trails that are not supported out of the box.

- **Hosts**: the systems where you install the Audit Vault Agent component to collect audit data

  If you want to collect audit data from a secured target, then you deploy Audit Vault Agent on a host computer (usually the same computer where the secured target is located). Before you deploy the agent on this host, you specify how to connect to it by registering the host in Audit Vault Server.

- **Enforcement Points**: How you set up a Database Firewall to protect a database

  If you are deploying one or more instances of the database firewall component to protect databases, then you configure one database firewall monitoring point (or enforcement point) for each database. Configuring an enforcement point in Oracle Audit Vault and Database Firewall lets you select the specific instance of a database firewall used for monitoring, identify the database being monitored, and identify the network traffic sources to that database. In the enforcement point configuration, you also specify whether you want the database firewall only to monitor and raise alerts on the SQL traffic to the database, or also to block SQL traffic that is out of policy.

1.3.2 Oracle Audit Vault and Database Firewall Components

This section contains:

1.3.2.1 Introduction to Oracle Audit Vault and Database Firewall Components

The components of Oracle Audit Vault and Database Firewall are Oracle Audit Vault Server, Audit Vault Agent, and Database Firewall.

Oracle Audit Vault Server is required and at least one of the other two components. You have the flexibility to deploy Oracle Audit Vault Server with either the Audit Vault Agent component, with the database firewall component, or with both. The Audit Vault Agent component enables you to consolidate and manage audit data from heterogeneous sources. The database firewall component secures your databases from SQL attacks over the network. Depending on your needs, you can decide which of the components to deploy.

1.3.2.2 About Oracle Audit Vault Server

Oracle Audit Vault Server stores audit data from various types of sources (secured targets), and the event data from the firewall of Oracle Audit Vault and Database Firewall.

Event data refers to the data gathered when an Oracle Audit Vault and Database Firewall policy is applied on an incoming SQL statement. Specifically, an incoming SQL statement and session data are compared to those defined in the policy. An action is then performed, such as logging, blocking, or substituting data. Oracle Audit Vault Server enables you to manage Oracle Database audit policies, and manages firewall policies of Oracle Audit Vault and Database Firewall to protect databases. Oracle Audit Vault Server is a dedicated server that also contains the tools necessary to configure Audit Vault Agent and the firewall of Oracle Audit Vault and Database Firewall.

Oracle Audit Vault Server has a central repository of audit and event data (from both Audit Vault Agents and firewalls). This repository is contained in an embedded Oracle Database, which includes features such as compression, partitioning, encryption, and privileged user controls.

The Oracle Audit Vault Server Web interface provides administrators with the tools to perform the following tasks:

- Creating the essential definitions necessary to monitor secured targets and configure the system
- Configuring Audit Vault Agent host connections
- Configuring (that is, adding, editing, and deleting) secured targets, audit trails, and enforcement points
- Setting up data retention (archive) policies and archive locations
- Configuring external storage
- Setting up connections to external systems, for example, for email notifications and syslog destinations
- Configuring high availability
- Controlling access by administrators and auditors

Some highlights of the Oracle Audit Vault Server Web console are illustrated in the following figures.

Figure 1-2 Audit Vault Server Dashboard

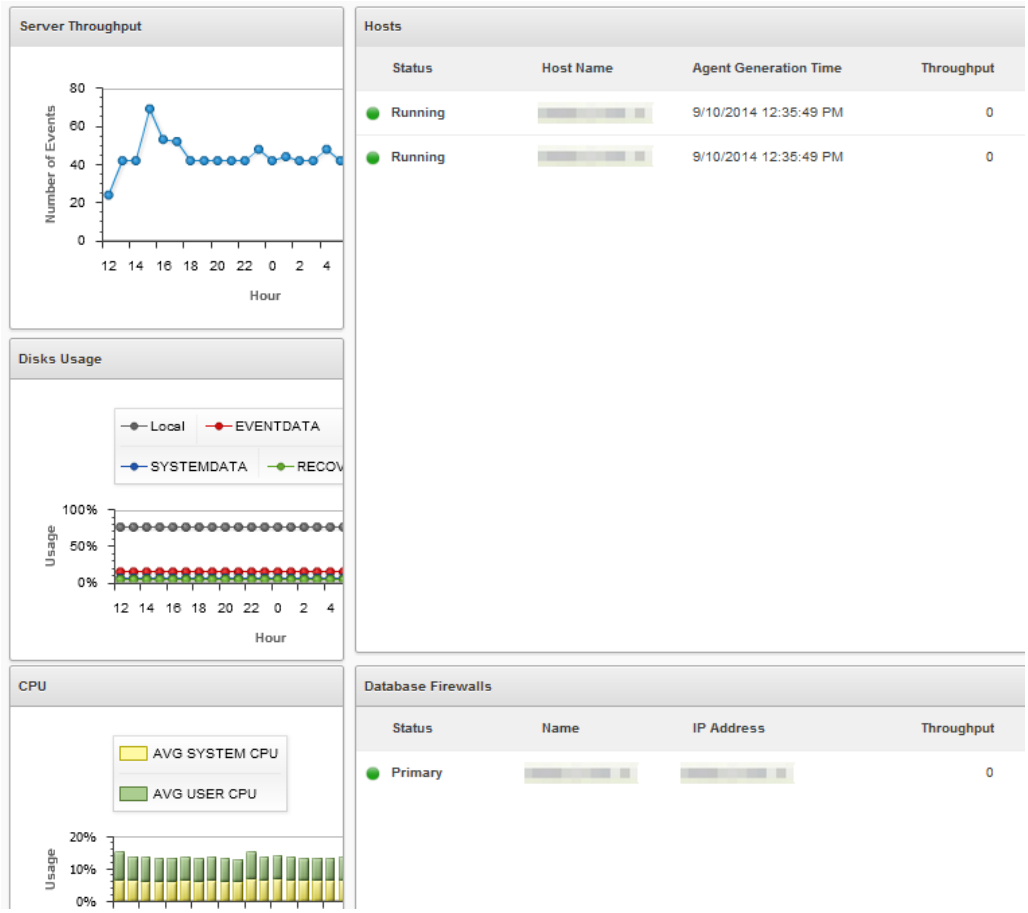


Figure 1-3 Audit Vault Server - Secured Targets

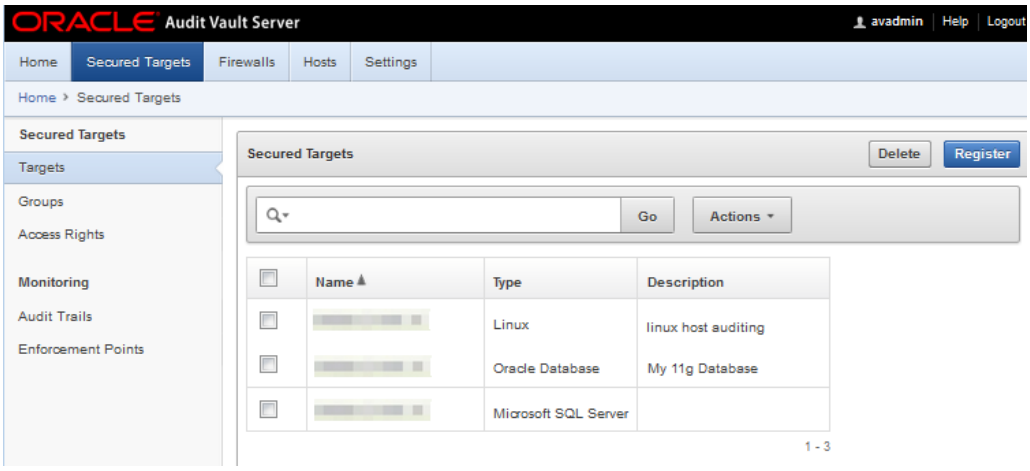
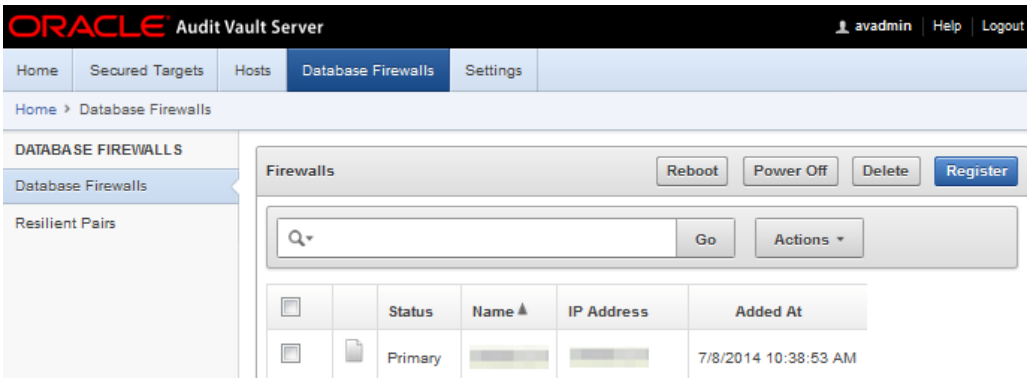


Figure 1-4 Audit Vault Server - Database Firewalls



1.3.2.3 About Oracle Audit Vault Information Lifecycle Management

The Information Lifecycle Management (ILM) component of the Oracle Audit Vault and Database Firewall handles audit data retention management.

The discovery task involves identifying hosts, deploying, and adding them as secured targets. Discovery manages audit data collected from all the secured targets.

Compliance Management involves evaluating compliance of targets and systems for security and storage. It performs many other tasks that maintain stability of the system.

Compliance Management enforces retention policy and expired event data. Retention policy management involves all of the tablespaces that are managed by the appliance. A new tablespace is created when a record from a target with the policy arrives into Oracle Audit Vault Server.

The audit data collected from secured targets is moved into new tablespaces based on the retention policy defined for a specific secured target. The new tablespace name is based on the retention policy. After the online retention period expires, the data is offline. The data remains in the system, and you can archive it. The data is offline, and kept local in the system until you manually archive it, either to a network file storage (NFS) or to NFS or a secure copy (SCP) location. Before triggering an archive job, you must define one or more archive locations.

You can schedule an archive job, and view the status. The tablespaces that contain audit data are automatically deleted after their retention period expires. The retention period is determined from the retention policy for a specific secured target. There is no manual intervention required.

After the tablespaces are moved to an archived location, you must not move them, or delete them manually. Any manual intervention hampers the back-end metadata, and leaves it in an inconsistent state. An inconsistent state can result in an unstable Oracle Audit Vault Server. If you want to run reports, or use tables for any other activity in the database, you can restore the tablespaces.

The appliance (Oracle Audit Vault and Database Firewall) manages expired event data. Management involves all the tasks from creating, archiving, and deleting the tablespaces, based on the retention policy defined. However, you must manually archive the data.

The ILM component has a built in health check package. To check the current status of the component, execute the following command:

```
SQL> exec avsys.ilmcheck.run('check_all')
```

A log file with a name `ilmcheck.log` is generated under the file path `$ORACLE_HOME/av/log`.

To check more options with this health check component, run the following command:

```
SQL> set serveroutput on; exec avsys.ilmcheck.run('help');
```

Related Topics

- Defining Archive Locations

1.3.2.4 About Audit Vault Agent

Audit Vault Agent retrieves audit trails from various types of secured targets and sends the audit data to Oracle Audit Vault Server.

Secured targets can be either an Oracle Database, or other databases, operating systems, file systems, directory services, or custom audit data in either database tables or XML files.

Audit Vault Agent is deployed on a host. Usually the host is the same host running the audit data source (secured target), such as a database, or an operating system. However, you can also deploy the agent on a remote host. Hosts are registered in the Oracle Audit Vault Server. Each audit data source has an associated secured target, and one or more audit trails defined in Oracle Audit Vault Server for the secured target.

Related Topics

- Planning the Audit Vault Agent Deployment (page 3-1)

1.3.2.5 About Oracle Database Firewall

The Oracle Database Firewall component of Oracle Audit Vault and Database Firewall monitors databases, access activity events, and acts as a first line of defense on the network.

You can deploy Oracle Database Firewall using two different methods:

1. Monitoring only
2. Monitoring and blocking

Oracle Database Firewall monitors databases, and provides a complete event repository of significant database access activity events, as defined by an Oracle Audit Vault and Database Firewall policy. Oracle Database Firewall also acts as a first line of defense on the network by enforcing expected database access behavior, thereby helping to prevent SQL injection, application bypass, and other malicious activity from reaching the database.

Oracle Database Firewall uses a highly accurate SQL grammar-based engine to monitor all SQL traffic, and to block unauthorized SQL traffic. By parsing the SQL, Oracle Audit Vault and Database Firewall can recognize the multiple number of ways

to express the different equivalent SQL statements, so that you can properly decide whether to allow these statements. In contrast, naive filtering that is based on regular expressions usually recognizes only a subset of equivalent statements.

Unlike solutions that leverage regular expressions, Oracle Database Firewall parses the SQL itself to achieve the level of accuracy required for enterprise database monitoring. Oracle Database Firewall collects SQL requests from the network. SQL statements are then associated with as much session information as possible (for example, database user name, client program name, or client IP address). This information is then combined with further analysis of SQL statements, including SQL category, such as `SELECT` statements, Oracle Definition Language (DDL) and Data Manipulation Language (DML) writes, Tool Command Language (TCL), and so on.

Oracle Database Firewall analyzes the SQL statements in accordance with the firewall policy. Oracle Database Firewall groups SQL statements into **clusters**, which are SQL statements with the same grammatical structure. This enables the distillation of hundreds of millions of SQL statements down to just a few hundred. Oracle Audit Vault and Database Firewall lets you define firewall policies that include both allowed SQL (allowlist), and disallowed SQL (blocklist). In this way, Oracle Database Firewall distinguishes normal transactions from abnormal transactions.

To ensure flexibility in the choice of the network point at which the traffic is monitored, Oracle Database Firewall also supports a monitor-only agent that is local to the database server. Host Monitor, which is part of the Audit Vault Agent, captures SQL traffic reaching the database server, and securely forwards it to Oracle Database Firewall. You can use Host Monitor to remotely monitor database servers running on Linux, Oracle Solaris, and Microsoft Windows platforms. To use Oracle Database Firewall Host Monitor, deploy the Audit Vault Agent. Note that Host Monitor does not perform the blocking.

Related Topics

- Understanding Oracle Database Firewall Policies (page 4-9)
- Database Firewall Deployment (page 4-1)

1.3.2.6 Oracle Audit Vault and Database Firewall Components Working Together

Oracle Audit Vault and Database Firewall components work together to protect a secured target, and collect the appropriate audit trail from that secured target.

The Oracle Audit Vault and Database Firewall architecture provides a high-level overview of how the Oracle Audit Vault and Database Firewall components work together. Though this diagram shows both a database firewall and Audit Vault Agents, you can deploy Oracle Audit Vault Server with both components, or only the Audit Vault Agent component, or only the database firewall component.

Oracle Audit Vault and Database Firewall components work together in this way:

- An Audit Vault Server is deployed for every Oracle Audit Vault and Database Firewall installation. You can configure multiple secured targets. such as a heterogeneous set of databases, operating systems, file systems, or custom audit logs. For each secured target, you must deploy the Audit Vault Agent component. If the secured target is a database, then the database firewall can also be placed in the network, and configured to protect that secured target. If you want to collect

audit data from the secured target, then you must deploy the Audit Vault Agent on the host.

- If the Audit Vault Agent is deployed, Oracle Audit Vault and Database Firewall is configured to collect the appropriate audit trail from the secured target. If the Database Firewall is deployed to protect a database, a firewall policy is applied for that database secured target by configuring an enforcement point. An enforcement point is a connection point between a secured target and the Database Firewall. Enforcement point can be used for monitoring the database activity and take action on the incoming SQL in some configuration types.
- The Audit Vault Agent component retrieves the audit data from secured targets and sends this data to Audit Vault Server.
- The database firewall component monitors SQL traffic to database secured targets, creates traffic logs, and takes actions according to a firewall policy. You can design the firewall policy to monitor and raise warnings only, or to block SQL traffic, and optionally substitute harmless statements in place of the blocked ones. The database firewall sends traffic logs to the Audit Vault Server component.
- Audit Vault Server stores the Oracle Audit Vault and Database Firewall configuration data, the collected audit data, and Database Firewall event data in its internal repository. An auditor can then generate and customize reports, as well as configure email notifications and system audit log (syslog) messages on Audit Vault Server.

Related Topics

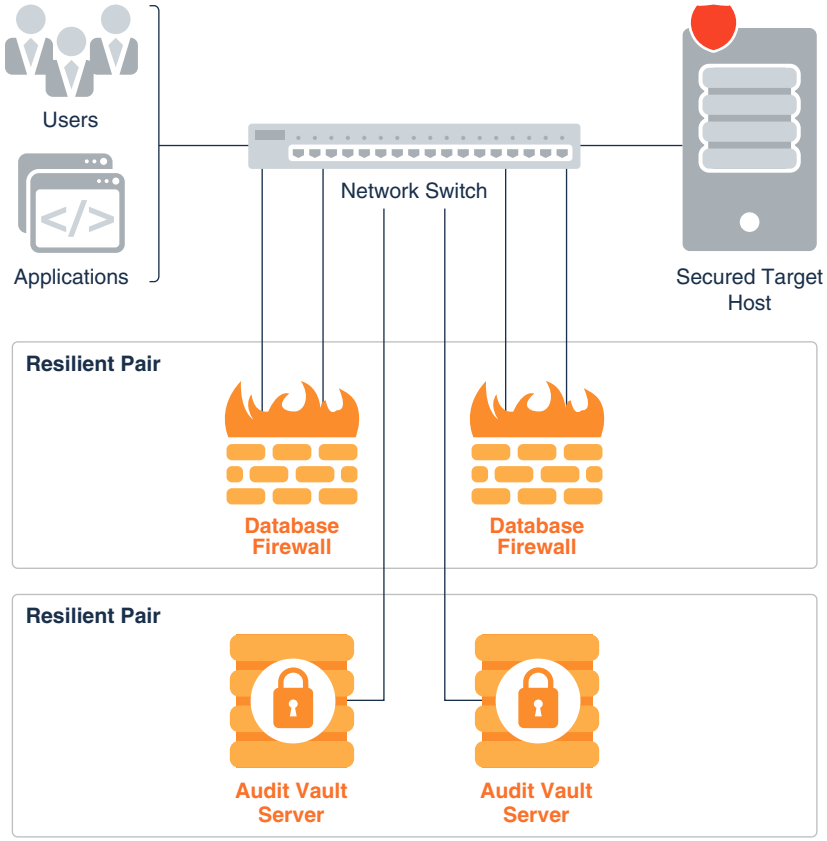
- Introduction to Oracle Audit Vault and Database Firewall (page 1-4)
  Oracle Audit Vault and Database Firewall provides a comprehensive way to deal with a large amount of audit data, the risk from SQL injection, application bypass attacks over the network, and problems of unauthorized access.

1.3.2.7 Oracle Audit Vault and Database Firewall Network Topology

The Oracle Audit Vault and Database Firewall network topology differs depending on the size of your deployment, your high availability configuration, and optional integration with other systems.

The following illustration is a simplified illustration of Audit Vault Server with both database firewall and Audit Vault Agent components deployed. There are several ways to deploy the database firewall component on the network.

Figure 1-5 Illustration of Oracle Audit Vault and Database Firewall on the Network (Simplified)



In this illustration, to obtain high availability, two Audit Vault Servers and two database firewalls are deployed. You can pair database firewalls, pair Audit Vault Servers, or pair both database firewalls and Audit Vault Servers.

Related Topics

- Introduction to Oracle Database Firewall Deployment (page 4-1)
  Depending on your requirements, you can choose from one of three types of deployments available for Oracle Database Firewall.
- High Availability in Oracle Audit Vault and Database Firewall (page 2-2)
  Planning for high availability is an important part of deployment planning.

1.3.3 Roles and User Accounts in Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall offers multiple roles as part of the separation of duties.

The following table shows the user accounts in Oracle Audit Vault and Database Firewall.

Table 1-1 Oracle Audit Vault and Database Firewall User Accounts

Account	Description
Super Administrator	Super administrators configure and maintain the Oracle Audit Vault and Database Firewall system, including Audit Vault Server settings such as network settings, high availability, data retention policies, etc. The super administrator can create other administrators or super administrators, and has access to all secured targets. The super administrator can also grant access to specific secured targets to other administrators.
Administrator	The administrator can perform a subset of the system configuration tasks that a super administrator can, such as registering hosts and secured targets, running archive jobs, etc. Administrators can also manage secured targets for which they have been granted access by a super administrator. An administrator cannot create another administrator. This can be performed by a super administrator only.
Database Firewall Administrator	The Database Firewall Administrator user can access the administrative interface on the Database Firewall Appliance. This user can configure the Database Firewall component's system and network settings, traffic sources, and view diagnostics information.
Super Auditor	The Super Auditor user can create firewall policies, provision audit policies for Oracle Database secured targets, and specify settings for secured targets. For example, the Super Auditor user can create a policy that determines whether to enable stored procedure auditing. Super Auditor users also generate reports, and create alerts and notifications. Super Auditor users can access all secured targets, create auditor or super auditor users, and grant access to specific secured targets to those users.
Auditor	Auditor users can perform all the functions of Super Auditor users, but only for the secured targets to which they have access.
root	Operating system Super User (root) account. Only use this account as instructed in the documentation, or under the guidance of Oracle Support. This account is typically used for upgrades and patching.
Support	The Support user account should only be used under the guidance of Oracle Support. This account is typically used to log in, using SSH.

> **Note:**
>
> - To provide greater security, the Oracle Audit Vault and Database Firewall **Administrator** and **Auditor** roles have different user interfaces, and different user accounts. This separation of roles ensures that there is a separation of duties between these two roles.
> - In addition to the Oracle Audit Vault and Database Firewall administrative role user accounts, set up user accounts on your secured targets as necessary for Oracle Audit Vault and Database Firewall to access these targets for collecting audit data. Oracle Audit Vault and Database Firewall provides scripts to set up these user accounts on database secured targets, as well as guidance for other types of secured targets.

1.3.4 Integrating Other Systems with Oracle AVDF

Topics:

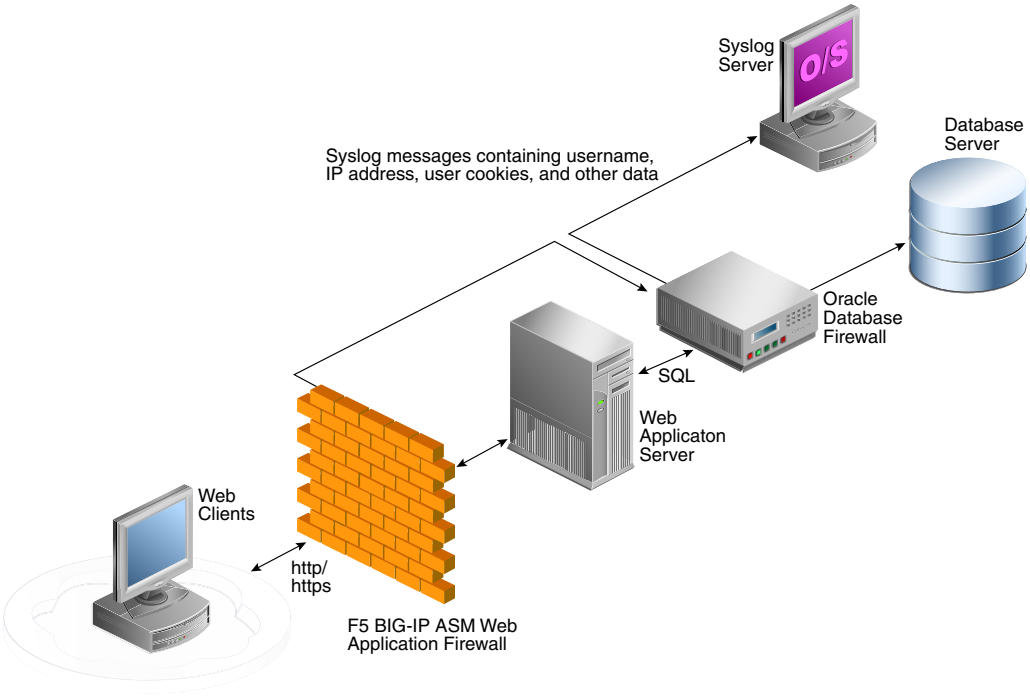
1.3.4.1 Integrating Oracle AVDF with F5 BIG-IP ASM

Oracle Audit Vault and Database Firewall (Oracle AVDF) supports integrating BIG-IP Application Security Manager (ASM).

> **Note:**
>
> - This functionality is only supported on F5 BIG-IP ASM version `10.2.1`.
> - F5 BIG-IP ASM integration is deprecated in release `12.2.0.7.0`, and can be desupported in a future release.

BIG-IP Application Security Manager (ASM), from F5 Networks, Inc., is a web application firewall (WAF) that provides protection against web-based attacks. BIG-IP ASM is deployed between web clients and the web application server. It analyzes each HTTP and HTTPS request, and blocks potential attacks before they reach the Web application server. Refer to the following figure for details:

Figure 1-6 Oracle AVDF with F5 BIG-IP ASM Data Flow Unit



Oracle Database Firewall is deployed between the web application server and the database. It provides protection against attacks originating from inside or outside the network. It works by analyzing the intent of the SQL statements sent to the database.

A deployment that includes both BIG-IP ASM and Oracle Database Firewall provides the functionality of both products, and enables the two systems to work in partnership.

A key benefit of the integration is that it allows BIG-IP ASM to pass to Oracle Database Firewall additional information about the SQL statements sent to the database, including the web user name, and the IP address of the web user who originated them. This information is not usually available from the SQL statements generated by the web application server.

1.3.4.2 Integrating Syslog With a SIEM System

Learn how to integrate Oracle Audit Vault and Database Firewall System Logging Protocol logs (`syslog`) with a Security Information and Event Management (SIEM) system.

You can configure `syslog` message destinations in Oracle Audit Vault Server. If you use a SIEM system, then you can configure it to receive the required information from `syslog`. The `syslog` messages that you can integrate with a SEIM system are:

- **Alert** - alert messages raised by Oracle Database Firewall policies, and user-configured alerts
- **System** - `syslog` messages from subcomponents of the Oracle Audit Vault Server and Oracle Database Firewall
- **Info** - specific change logging from Oracle Database Firewall

- **Debug** - a category that should only be used under the direction of Oracle Support

Oracle Audit Vault and Database Firewall has an integration with HP ArcSight SIEM. You can configure this integration in Oracle Audit Vault Server to send these types of `syslog` messages for Oracle Database Firewall events directly to HP ArcSight.

> **Note:**
>
> Micro Focus ArcSight SIEM (previously known as HP ArcSight SIEM) is deprecated in `12.2.0.8.0`, and is desupported in `12.2.0.9.0`. Use the `syslog` integration feature instead.

1.4 Understanding the Software Appliance Model

With the software appliance model, your hardware is dedicated to Oracle Audit Vault Server or to the Oracle Audit Vault and Database Firewall software firewall (the Database Firewall).

Both Oracle Audit Vault Server and the Database Firewall are software appliances. Unlike a hardware appliance, a software appliance uses your own industry-standard hardware. The software appliance includes the operating system, repository, and application. This system is preconfigured for you, and hardened to meet the requirements of Oracle Audit Vault and Database Firewall. Therefore, you do not need to change these settings, because the entire appliance is highly tuned. With this software appliance model, your hardware is dedicated to Oracle Audit Vault Server or to the Database Firewall software, both of which include an Oracle Linux operating system, Oracle Database, and the Oracle Audit Vault and Database Firewall software.

In addition to the benefits that Oracle Audit Vault and Database Firewall software provides, the appliance model provides these additional benefits:

- Time (cost) saving on the configuration of components, the appliance comes with an operating system, database, and middleware pre-configured for optimal operation of Oracle Audit Vault and Database Firewall application software
- Implicit upgrading and patching. With the appliance deployment, there is no need for separate patching of the operating system, database or application. All component updates are delivered as bundle patches that are installed in a single, simple procedure.
- Improved reliability and support responsiveness due to restricting scenarios to particular combination of the operating system, database, and application.

In contrast to a hardware appliance model, the software appliance model provides the flexibility to choose hardware sizing to accommodate your needs.

This software model also provides easy patching and upgrading, which includes all components. Therefore, you do not need to install or patch components such as the operating system or repository separately.

You must not make any changes to the Linux operating system, or Oracle Audit Vault Server repository through the command line on these servers, unless you are following official Oracle documentation, or are under guidance from Oracle Support.

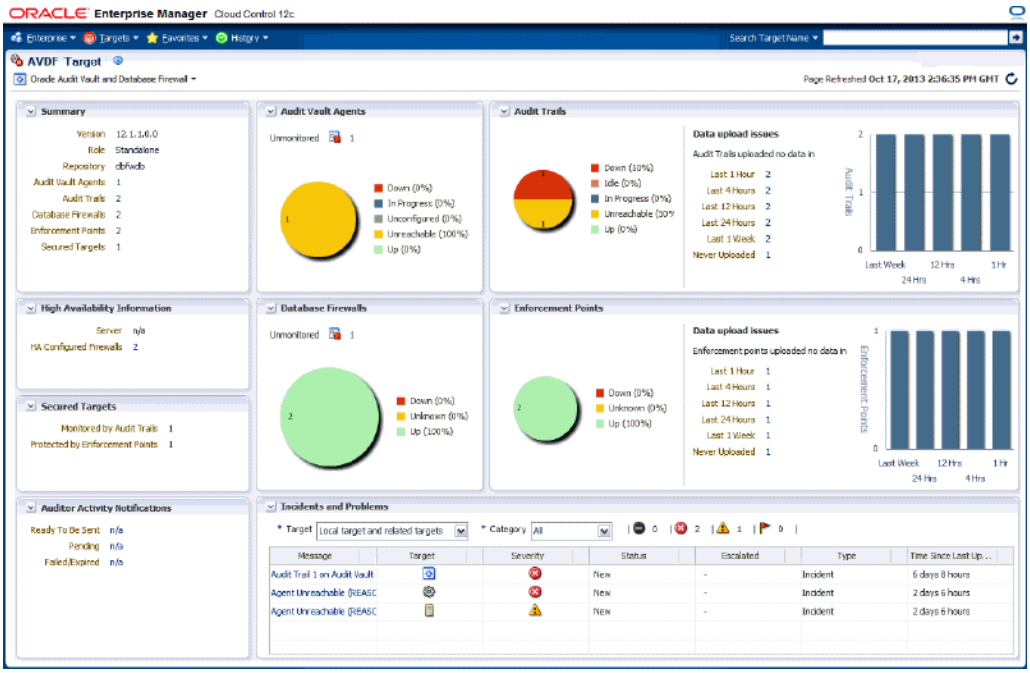
> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Installation Guide* for information on specific hardware required.

1.5 Oracle Audit Vault and Database Firewall and Oracle Enterprise Manager

You can monitor the components of Oracle Audit Vault and Database Firewall using a plug-in to Enterprise Manager.

If you have Oracle Enterprise Manager Cloud Control 12c Release 2 (12.1.0.3.0) or higher, you can install the Oracle Audit Vault and Database Firewall plug-in to the Enterprise Manager (EM) to monitor Oracle Audit Vault and Database Firewall through the EM. This plug-in provides an interface within Enterprise Manager Cloud Control for administrators to manage and monitor Oracle Audit Vault and Database Firewall components.

Figure 1-7 Oracle Audit Vault and Database Firewall Plug-in for Oracle Enterprise Manager Cloud Control



The Oracle Audit Vault and Database Firewall plug-in gives you a summary view, and lets you monitor:

- Audit Vault Agents
- Database Firewalls

- Targets
- Audit trails
- Enforcement points
- High availability information
- Auditor activity notifications
- Incidents and problems

1.6 Planning an Oracle Audit Vault and Database Firewall Deployment

To deploy Oracle Audit Vault and Database Firewall, you must prepare the server, plan the Oracle Audit Vault Server deployment, and plan the Oracle Database Firewall deployment.

Planning your Oracle Audit Vault and Database Firewall deployment includes planning Oracle Audit Vault Server deployment and deciding whether you will deploy the Audit Vault Agent, Oracle Database Firewall, or both. In addition, depending on which components you are deploying, you must gather some key information.

1.7 Support Policy When Third Party Software is Installed on Oracle AVDF

Oracle Audit Vault and Database Firewall (Oracle AVDF) is shipped as an appliance, and no third-party software should be installed on the Audit Vault Server. Oracle does not test or certify any third party software on Oracle AVDF. If third party software is installed, and results in problems with the Audit Vault Server and/or Database Firewall, then Oracle may not be able to help you recover the system. In cases where we believe the third party software has contributed to an issue, we may ask you to reproduce the issue on an Oracle AVDF system that does not include the third-party software.

During patching or upgrade of Oracle AVDF, you may find that the presence of third party software contributes to difficulties in completing the operation. You may also find that the process of patching/upgrading Oracle AVDF causes third party software to malfunction or cease to work altogether. Oracle AVDF upgrades also update the underlying operating system and may remove any custom libraries added by third party software.

Audit data is particularly sensitive, and loss of an audit data may result in inability to support compliance reporting and forensic investigations. In the event that you choose to install third party software on Oracle AVDF, then Oracle recommends you take additional appropriate precautions such as more frequent backups that may reduce the damage in the event the third-party software causes system instability or corruption.

2

Planning the Audit Vault Server Deployment

Topics

2.1 Introduction to Oracle Audit Vault Server Deployment

You must deploy Oracle Audit Vault Server before you can deploy the other components: the Audit Vault Agent component to collect audit data, and Oracle Database Firewall to protect databases.

Oracle Audit Vault Server performs these primary functions:

- Consolidating the following data:
  - Audit data from Oracle Database and third-party databases, operating systems, directories, and other custom sources
  - Event logs from Oracle Database Firewall
- Managing audit policies for Oracle Database
- Managing database firewall component policies for any supported database
- Alerting
- Reporting and distribution of unplanned or scheduled reports
- Managing the system configuration including settings for Oracle Audit Vault Server itself, networking, firewalls and enforcement points, agents and agent hosts, secured targets, audit trails, high availability, storage area network (SAN) storage, archiving policies, and locations

2.2 Planning and Rolling Out the Audit Vault Server

When planning the Audit Vault Server deployment, it is important to consider the questions below. Several of these questions impact the sizing of Audit Vault Server. See the Oracle Audit Vault and Database Firewall Sizing Advice (MOS Doc ID 2223771.1) for help in estimating the amount of storage required. Work with Oracle Support team to obtain the sizing guide.

- How many databases do I need to protect with Database Firewall?
- How many systems (for example, databases, operating systems, file systems) am I going to need to collect audit data from? How many audit events do I expect to collect each day? Typically, if you mainly audit privileged user access or direct connections to a database, then the audit data is likely minimal up to a few

hundred records every day. If you want to perform a fine-grained audit, you must first look at how much data is actually created.

The amount of data you will collect, and how long you retain it, will determine whether you upgrade to a higher capacity disk, or possibly configure SAN storage for Audit Vault Server data. Work with Oracle Support for help in estimating the amount of storage required.

- How long do I need to retain data in Audit Vault Server?

  Audit Vault Server lets you set data retention policies, and configure archive locations. You must determine how long you want data to be available online in Audit Vault Server before it is archived, and how long you want to retain the data in the archives before it is purged.

  Retaining data online in Audit Vault Server lets you view reports based on that data. Once data is moved from Audit Vault Server into archive locations, the data is no longer visible in reports, but can be retrieved to Audit Vault Server if necessary. Once its specified archive period has ended, the archived data is deleted so the data can no longer be retrieved to Audit Vault Sever.

  Before you start collecting audit data, you should define your data retention policies in Audit Vault Server, and select a retention policy for each secured target as required. Once data is collected, the selected retention policy will be applied to that data and cannot change. Changing the retention policy for a secured target applies that policy to new data from that point forward.

- Do I need to configure high availability, and if so, will I have paired Audit Vault Servers, paired Database Firewalls, or both?

  Remember that your network must also be resilient in order to achieve high availability for the Oracle AVDF system.

- How often will I back up Audit Vault Server data and configuration?

- Does my hardware support hardware acceleration, such as encryption using hardware security modules for Transparent Data Encryption (TDE)?

  This is important for sizing Audit Vault Server. More CPUs are required if the CPUs do not support hardware acceleration.

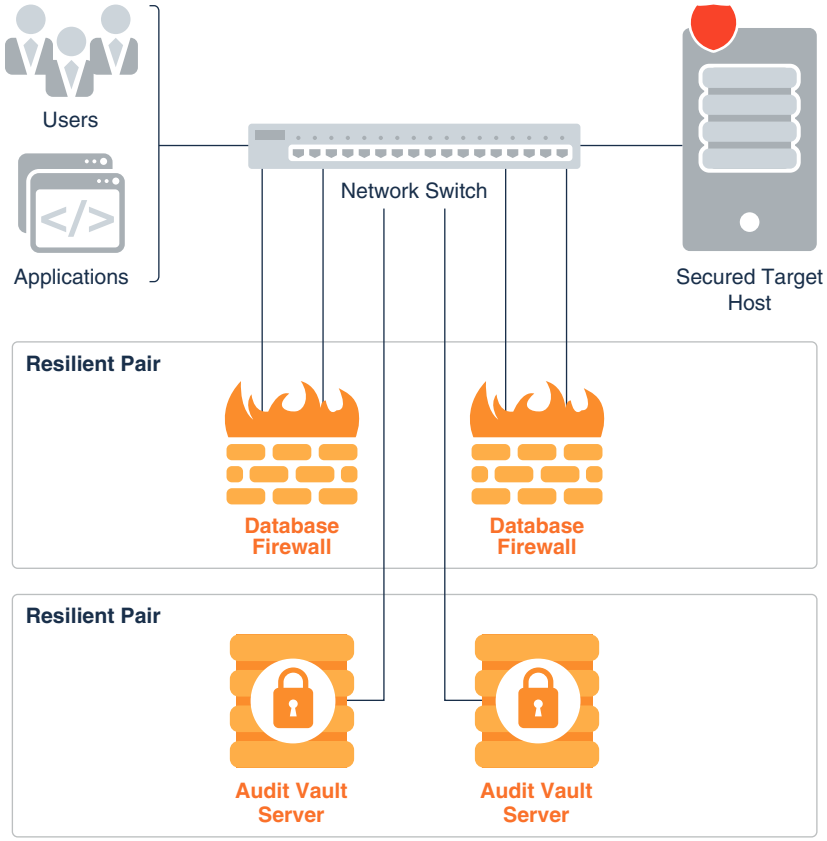
2.3 High Availability in Oracle Audit Vault and Database Firewall

Planning for high availability is an important part of deployment planning.

Within the Oracle Audit Vault and Database Firewall system, the term **high availability** is focused on ensuring no audit data is missed or lost. This is accomplished by configuring pairs of either Oracle Audit Vault Servers, Oracle Database Firewalls, or both. It is important to note that you must also ensure that high availability is built into the network itself.

The following figure shows a simplified illustration of an Oracle Audit Vault and Database Firewall deployment, where there are both Oracle Audit Vault Servers and database firewalls configured for high availability.

Figure 2-1 Pairs of Oracle Audit Vault Servers and Database Firewalls in High Availability Mode



With Oracle Audit Vault Server in high availability mode, during normal operation the system periodically checks the availability of the primary Oracle Audit Vault Server in the resilient pair. If the primary Oracle Audit Vault Server becomes unavailable, then the system automatically fails over to the secondary Oracle Audit Vault Server. The secondary Oracle Audit Vault Server continues to collect audit data, without loss, if the primary fails. After the former primary Oracle Audit Vault Server is repaired, it can then become the new secondary server.

With Oracle Database Firewall in high availability mode, both primary and secondary database firewalls:

- Have the same configuration (which Oracle Audit Vault Server synchronizes). This is the configuration of secured targets, enforcement points, policies, and other monitoring settings.
- Monitor the same traffic.
- Create log files according to the policy applied.
- Send out alerts to Oracle Audit Vault Server. Oracle Audit Vault Server then sends only the alerts from the primary Oracle Database Firewall.

After the data is stored in the database, Oracle Audit Vault Server deletes all the traffic log files from both the database firewall instances.

Oracle Audit Vault Server controls the state of the resilient pair of database firewalls. There is no communication between the database firewalls in a resilient pair. If Oracle Audit Vault Server is unable to contact the primary database firewall for an extended period of time, then Oracle Audit Vault Server collects the log files from the secondary database firewall, and promotes the secondary database firewall to be the primary.

See Also:

Oracle Audit Vault and Database Firewall Administrator's Guide for detailed instructions for configuring high availability.

3
Planning the Audit Vault Agent Deployment

Topics

3.1 Introduction to Oracle Audit Vault Agent Deployment

Collect and consolidate audit data from various systems (secured targets) by deploying one or more Audit Vault Agents.

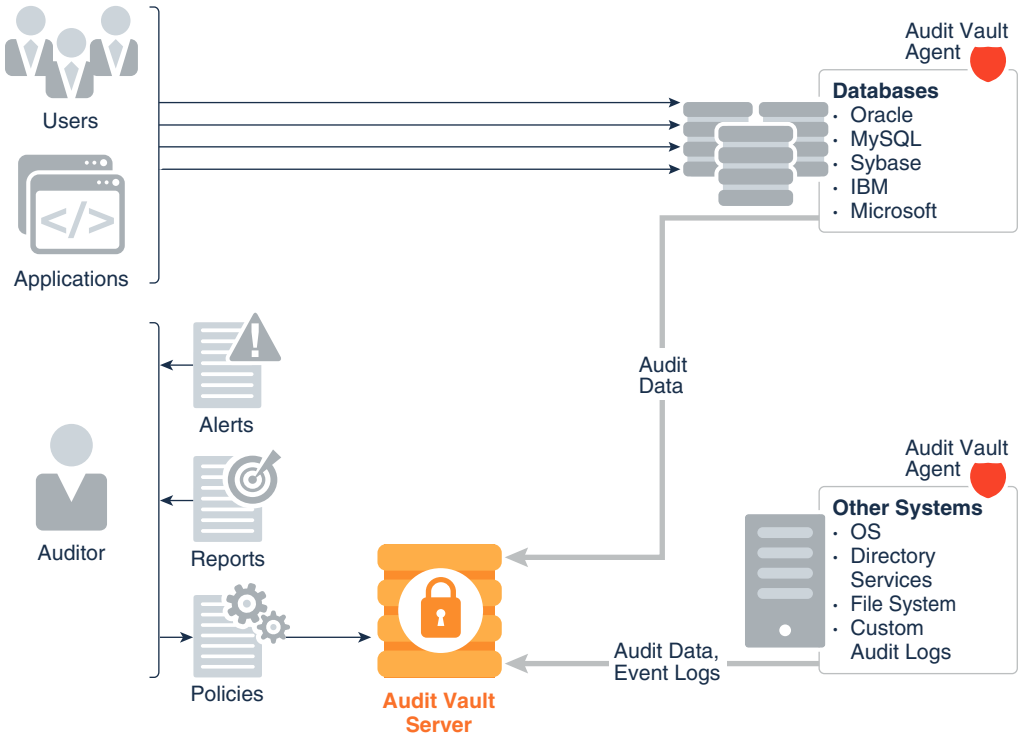
Typically, you deploy the Audit Vault Agent on the same host as a secured target, but you can deploy it on a different host as well, depending on the host location. Secured targets can be databases or other systems that Oracle Audit Vault and Database Firewall supports.

The Audit Vault Agent contains collection plug-ins that collect audit data from specific secured targets. Each supported secured target has a corresponding collection plug-in in the Audit Vault Agent. You can also develop custom plug-ins that collect audit data from a source that is not already supported out-of-the-box using the Oracle Audit Vault and Database Firewall SDK.

The following figure shows Oracle Audit Vault Server with Audit Vault Agents deployed on both database and non-database systems. The agents are collecting audit data from these systems, and sending this data to Oracle Audit Vault Server.

With the data collected, Oracle Audit Vault and Database Firewall auditors can generate numerous pre-configured, customizable reports that consolidate this data, and can also configure rule-based alerts and notifications that are triggered when certain conditions are met.

Figure 3-1 Oracle Audit Vault Server with Audit Vault Agents Deployed



Only one Audit Vault Agent can be installed on a host for a single Oracle Audit Vault Server. Multiple audit trail collections can be started using a single Audit Vault Agent.

One Audit Vault Agent can collect audit data from multiple secured targets, if the audit logs are accessible from the agent. For example, the database can be accessed using a database connection string, and the files (file path) can be accessed from that host. So in some cases secured target may not be on the same host. Even if there are multiple databases on the same host, the agent can collect from multiple secured targets. For each secured target, you configure one or more audit trails in Oracle Audit Vault and Database Firewall. For example, an agent can be collecting audit data from a database and an operating system. This agent is deployed on a host, and there may be three audit trails configured. For example, two audit trails can be configured to collect data from two different audit data sources on the database (for instance, from `REDO` logs and from the `SYS.AUD$` dictionary table), and one audit trail can be configured for the operating system (for instance, from the `audit.log` file on a Linux system).

Related Topics

- Oracle Audit Vault and Database Firewall Reports and Alerts (page 5-1)

See Also:

- *Oracle Audit Vault and Database Firewall Installation Guide* for supported secured targets.
- *Oracle Audit Vault and Database Firewall Developer's Guide* for detailed instructions on how to develop custom plug-ins.

3.2 Understanding Audit Data Collection and Audit Policies

Learn about audit data collection and audit policies.

3.2.1 Introduction to Audit Data Collection and Audit Policies

You can apply the philosophy of "trust but verify" by understanding the specific auditing capabilities of your system, and setting its auditing features accordingly.

Whether you are auditing Oracle Database, or another type of database, keep in mind that privileged users are often targeted to infiltrate systems. Understanding the auditing capabilities of your system, you can then deploy Oracle Audit Vault and Database Firewall to collect and consolidate audit information from the various systems you are monitoring.

In addition to consolidating audit data from these heterogeneous systems, Oracle Audit Vault and Database Firewall supports retrieving Oracle Database audit policies, modifying them directly from Oracle Audit Vault Server, and then provisioning the updated policies to Oracle Database.

If you use Oracle Database 12c or later, then you can take advantage of the predefined unified audit policies mentioned for Oracle Database 12c and later releases.

3.2.2 What to Audit

Topics

3.2.2.1 Auditing Relevant Activities

Although auditing is relatively inexpensive, you should limit the number of audited events to those required for your needs.

This minimizes the performance impact on the execution of audited statements and the size of the audit trail, making it easier to analyze and understand. The big impact is on the storage requirements on the Audit Vault Server, especially if the archival period is large.

Follow these guidelines when devising an auditing strategy:

1. Evaluate your reason for auditing and focus on specific activities. After you have a clear understanding of the reasons for auditing, you can devise an appropriate auditing strategy and avoid unnecessary auditing.

   For example, an important reason for auditing is to monitor the activity of privileged users. If you are auditing database activity, we recommend you audit the activity of any user who has direct access to the database, especially administrative users such as the DBA.

   In the case of a DBA, audit all of their activities. For other users, you can narrow your focus to specific types of suspicious activity. One auditing strategy might be to audit unauthorized deletions from arbitrary tables in the database. This narrows the type of action being audited and the type of object being affected by the suspicious activity.

2. Use the audit functionality efficiently. Audit the minimum number of statements, users, or objects required to get the targeted information. This prevents clutter from unnecessary audit information from obscuring the meaningful information. Balance your need to gather sufficient security information with your ability to store and process it.

Related Topics

- Guidance on Auditing for Database Activity (page 3-4)
  When you first configure auditing for a database, we recommend starting with the database's default audit settings.

3.2.2.2 Guidance on Auditing for Database Activity

When you first configure auditing for a database, we recommend starting with the database's default audit settings.

Beyond that, you can use these guidelines:

1. Audit common suspicious activities.

   Auditing these common activities below can help you spot suspicious activity:

   - Activity of privileged users such as `SYS`, users who have been granted the `SYSOPER` or `SYSDBA` administrative privileges, or users who have been granted the `DBA` role

     For example, for an Oracle Database that has not yet migrated to unified auditing, set the `AUDIT_SYS_OPERATIONS` initialization parameter to `TRUE`.

   - Users who access the database directly. This can reveal activity such as:
     - Users who access the database during unusual hours
     - Multiple failed login attempts
     - Login attempts by non-existent users, which can happen if an intruder is attempting to gain access
   - Attempts to access critical business information in tables or columns. For example, if you see the same username coming from different IP addresses, it could be an hint that multiple people are sharing the same account.

   In addition, monitor users who share accounts or multiple users who are logging in from the same IP address. For example, if you are auditing to gather information about database activity, then determine exactly what types of activities you want to track, audit only the activities of interest, and audit only for the amount of time

necessary to gather the information that you want. As another example, do not audit objects (such as tables or views) if you are only interested in logical I/O information for each session.

2. Audit only relevant actions.

   At a minimum, audit user access and the use of system privileges. Also audit changes to the database schema structure. These include DDL changes such as the Oracle Database `CREATE TABLE` or `DROP TABLE` SQL statements. To avoid cluttering meaningful information with irrelevant audit records and reduce the amount of audit trail administration, only audit the targeted database activities.

   Remember also that auditing too much can affect database performance. For example, auditing DML changes to all tables in a database produces far too many audit trail records and can slow down database performance. However, auditing all DDL changes, or selected tables with sensitive columns, is highly recommended.

3. Be careful when auditing sensitive information.

   Be aware that sensitive data, such as credit card numbers, can appear in the audit trail columns, such as SQL text when used in the SQL query. If you have sensitive data that is being audited, do not enable the collection of SQL text in the audit trail.

4. Remember your organization's privacy considerations.

   Privacy regulations often lead to additional business privacy policies. Most privacy laws require businesses to monitor access to personally identifiable information (PII), and monitoring is implemented by auditing. A business-level privacy policy should address all relevant aspects of data access and user accountability, including technical, legal, and company policy concerns.

5. Check your database log files for additional information that can be useful for auditing purposes

   The log files generated by a database may contain useful information that you can use when auditing the database. For example, in Oracle Database, you can audit `REDO` logs to see before and after values for a particular database object. By enabling the `REDO` logs in Oracle Database, then creating an audit trail in Oracle Audit Vault and Database Firewall to collect events from `redo` logs, you will be able to see this information in an Oracle Audit Vault and Database Firewall report (the Data Modification Before-After Values report).

6. Archive audit records and purge the audit trail.

   After you collect the required information, archive the audit records of interest and then purge the audit trail of this information. Consult the documentation for your database for specific instructions.

See Also:

- *Oracle Database Security Guide* to hide sensitive information for Oracle Database 12*c*.
- *Oracle Database Security Guide* to hide sensitive information for Oracle Database 11*g*.
- *Oracle Database Security Guide* for information about purging audit trail records.
- *Oracle Database Administrator's Guide* for more information about redo logs.

3.2.3 Predefined Unified Audit Policies for Oracle Database

If you use Oracle Database 12c or later, and have migrated to unified auditing, then you can take advantage of six predefined unified audit policies.

You can enable six predefined audit policies that apply to the Oracle Database 12c and later release unified audit trails. These audit trails capture audit data from several audited components, and place the data in a single location, and in a single format.

These predefined unified audit policies cover commonly used security-relevant audit settings:

- **Logon Failures** - Tracks failed log ons
- **Secure Options** - Provides all the secure configuration audit options, such as audits to `ANY` privileges (for example, `CREATE ANY JOB`) and audits to actions that can have a wide impact such as altering users, creating roles, or dropping profiles.
- **Oracle Database Parameter Changes** - Audits changes to the Oracle Database parameter settings: `ALTER DATABASE`, `ALTER SYSTEM`, and `CREATE SPFILE`.
- **User Account and Privilege Management** - Audits commonly used user account and privilege settings, such as `CREATE USER`, `ALTER ROLE`, `GRANT`, `REVOKE`.
- **Center for Internet Security Recommendations** - Performs audits that are recommended by the Center for Internet Security (CIS)
- **Oracle Database Vault** - Audits all actions that are performed on the Oracle Database Vault `DVSYS` and `DVF` schema objects, and the Oracle Label Security `LBACSYS` schema objects

You can enable multiple policies in one database. If you do not have unified auditing enabled, or if your version of Oracle Database is earlier than Release 12c, then you may want to create policies that model these policies. You can find the unified audit policy creation statements for these policies in *Oracle Database Security Guide*.

See Also:

Oracle Database Security Guide for more information about policies.

3.3 Managing Oracle Database Audit Policies Using Oracle Audit Vault and Database Firewall

With the Audit Vault Agent deployed, if a secured target is Oracle Database 11g, 10g, or 12c, in addition to collecting audit data from it, you can also retrieve, modify, and provision audit policies for the database.

You can modify audit settings, as well as add new audit policies, for the following:

- SQL statements
- Database schema objects
- User management
- Fine-grained auditing
- Capture rules for redo log activity

> **See Also:**
>
> *Oracle Database Security Guide* for information on Oracle Database 11g auditing.

3.4 Monitoring Oracle Database Entitlements

An Oracle Database **entitlement** is a role, permission, or group membership that permits a user account to perform a specific task in Oracle Database.

The set of entitlements in Oracle Database releases can change over time, so it is important for an auditor to be able to track these changes to make sure no unauthorized entitlements have been granted. For example, an auditor may want to check grants of the DBA role or new user accounts and privileges.

With the Audit Vault Agent deployed, Oracle Audit Vault and Database Firewall lets you take snapshots in time of Oracle Database entitlements, and then compare snapshots in a number of reports, as well as see overall Oracle Database entitlement information.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed information.

3.5 Planning and Rolling Out Audit Vault Agent

Learn how to plan and roll out the Audit Vault Agent component of Oracle Audit Vault and Database Firewall.

Before deploying the Audit Vault Agent, you will need to think about the following questions:

- From which systems do I need to collect audit data?

  For each of the systems from which you want to collect audit data, you must up a secured target in Oracle Audit Vault Server.

- How many Audit Vault Agents do I need, and where will they be deployed?

  Identify the hosts on which you will deploy the Audit Vault Agents (usually the secured target host), and get their host names , IP addresses, or both, so that you can register them in Oracle Audit Vault Server.

- What types of audit trails, audit logs, and redo logs do I need to collect, and where are they located?

  Different types of secured targets produce different types of audit data, and place this data in various locations. For example, for a Microsoft SQL Server database you may want to collect audit data from C2 audit logs, server-side trace logs, and `sqlaudit` log files. You may also want to collect Oracle Database audit records from `syslog` files on a Linux platform. Finally, you may also want to collect data from Microsoft Windows event logs for these two databases, as well as from a Microsoft Windows operating system, and a Microsoft Active Directory.

- What audit settings do I need on my secured target?

  It is important to know the auditing features for your types of secured targets, and to have an auditing strategy for each of them. Consult the documentation for the specific secured targets you have (for example Oracle Database, or Microsoft SQL Server).

- How many audit trails will be collected by one Agent?

  Estimating the number of audit trails associated to a particular Agent will help you make performance optimizations.

See Also:

Oracle Audit Vault and Database Firewall Administrator's Guide

4
Database Firewall Deployment

Topics

4.1 Planning the Protection Level for Your Databases

To meet your protection level requirements, you can deploy Oracle Database Firewall in monitoring only mode, or monitoring and blocking mode.

Depending on your operational needs you can deploy Oracle Database Firewall in one of two modes:

- Monitoring only: In this mode, Oracle Database Firewall only monitors SQL traffic to the target database, and cannot block any SQL statements.
- Monitoring and blocking: In this mode, Oracle Database Firewall both monitors SQL traffic to the target database, and can block any SQL statements, based on the defined policy. In this mode, Oracle Database Firewall is inline with the traffic reaching the target database.

Related Topics

- *Oracle Audit Vault and Database Firewall Auditor's Guide*

4.2 Overview of Oracle Database Firewall Deployment

Learn about the types of deployments available for Oracle Database Firewall.

4.2.1 Introduction to Oracle Database Firewall Deployment

Depending on your requirements, you can choose from one of three types of deployments available for Oracle Database Firewall.

To monitor SQL traffic and restrict SQL statements reaching the target databases:

- Place the database firewall inline with your database traffic on the network (between the database and its clients)
- Configure the database firewall
- Create and deploy a policy that includes blocking, and optionally substituting SQL statements

Table 4-1 Oracle Database Firewall Deployment Types

Deployment Type	Supported Modes	Minimum Number of Network Interface Cards (NICs)
Proxy	DPE	3 (for deployment with network separation) 1 (for deployment without network separation)
Out-of-Band	DAM	2
Host Monitor	DAM	1

The same database firewall can monitor traffic from multiple Host Monitors, and at the same time be a proxy for some databases, and out-of-band (span) for some databases.

Note:

- A single network interface card (NIC) is required in case the client and database are on the same sub-network. There is no network separation.
- You can require additional NICs in case the client and databases are on different sub-networks.

4.2.2 In-line (bridge)

Learn about features of the in-line (bridge) mode of Oracle Database Firewall.

Note:

In-line bridge mode is deprecated in release 12.2.0.8.0, and can be desupported in a future release. Oracle recommends that you use Proxy mode instead. Proxy mode provides equivalent network security deployment features.

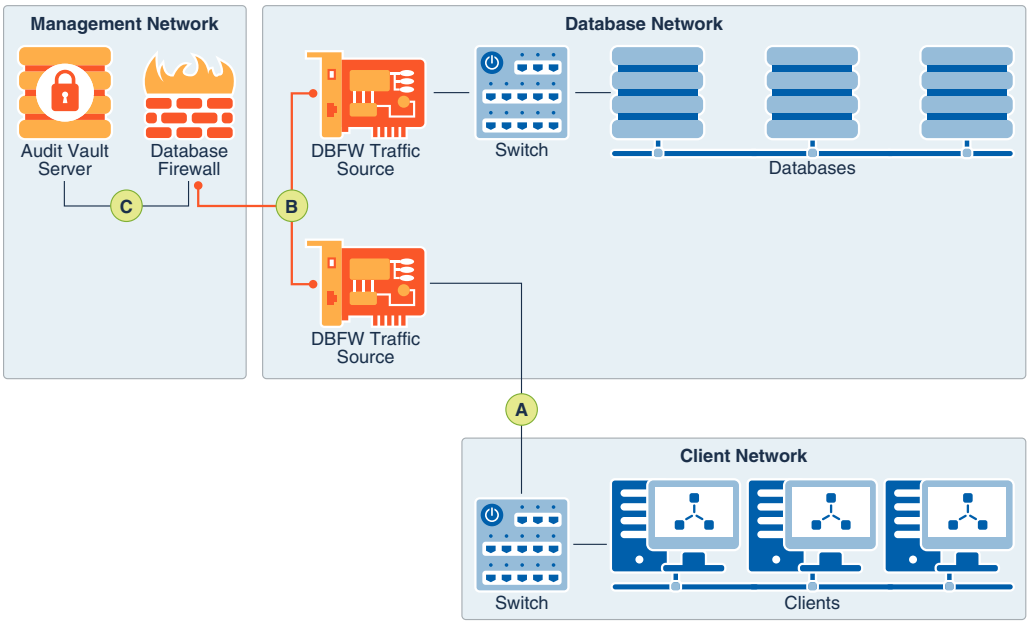
In this mode, Oracle Database Firewall:

- Is placed in-line with the traffic traveling between the client and the target database
- Can monitor, block SQL statements, and optionally substitute SQL statements

- Is deployed as a network bridge, which is inserted into the network in a segment between database clients and the databases that are secured
- Intercepts the traffic destined for the IP addresses and ports of the configured targets
- Intercepts traffic, analyzes the same, makes an explicit outbound connection to the database server, and forwards all the received data
- Is identified as the as the client by the database server

This **in-line** bridge architecture requires no configuration changes to database clients, applications, or to the database itself. It can require a configuration change of the network topology.

Figure 4-1 In-line Bridge



The image illustrates deployment under In-line Bridge mode for Oracle Database Firewall, which is indicated by DBFW in the illustration. The callouts in the image indicate the following:

- A: The clients connect to the database firewall component through the switch. The clients are not aware of the database firewall deployed on the network. It appears that they are connected to the database. However, they are actually connected to the database firewall. The traffic from the database servers travels back over the bridge to the switch and later directed into the wider network. The database firewall makes an explicit outbound connection to the target database. The database firewall may require static routing to be applied to the bridge so that it can route back the client connection.
- B: The bridge physically separates the network segments between the database firewall traffic source and the switch.
- C: The extracted SQL data from the client traffic is analyzed and sent to Oracle Audit Vault Server based on the database firewall policy.

4.2.3 Proxy

Learn about how to configure Oracle Database Firewall in Proxy mode.

In proxy mode, Oracle Database Firewall can both monitor and block SQL, as well as optionally substitute SQL statements. In scenarios where it is difficult to add a network bridge, or if the database servers are in remote places, Oracle Database Firewall is configured as a proxy, so that all the traffic to the database server is routed through the database firewall .

Database clients connect to the database firewall proxy that in turn connects to the database server, forwarding all data received from the database client. In all cases, the database server identifies the database firewall as the client.

The clients must be reconfigured to connect to the database firewall instead of the database. Oracle recommends that you configure the database to reject all connections that do not come from the database firewall.

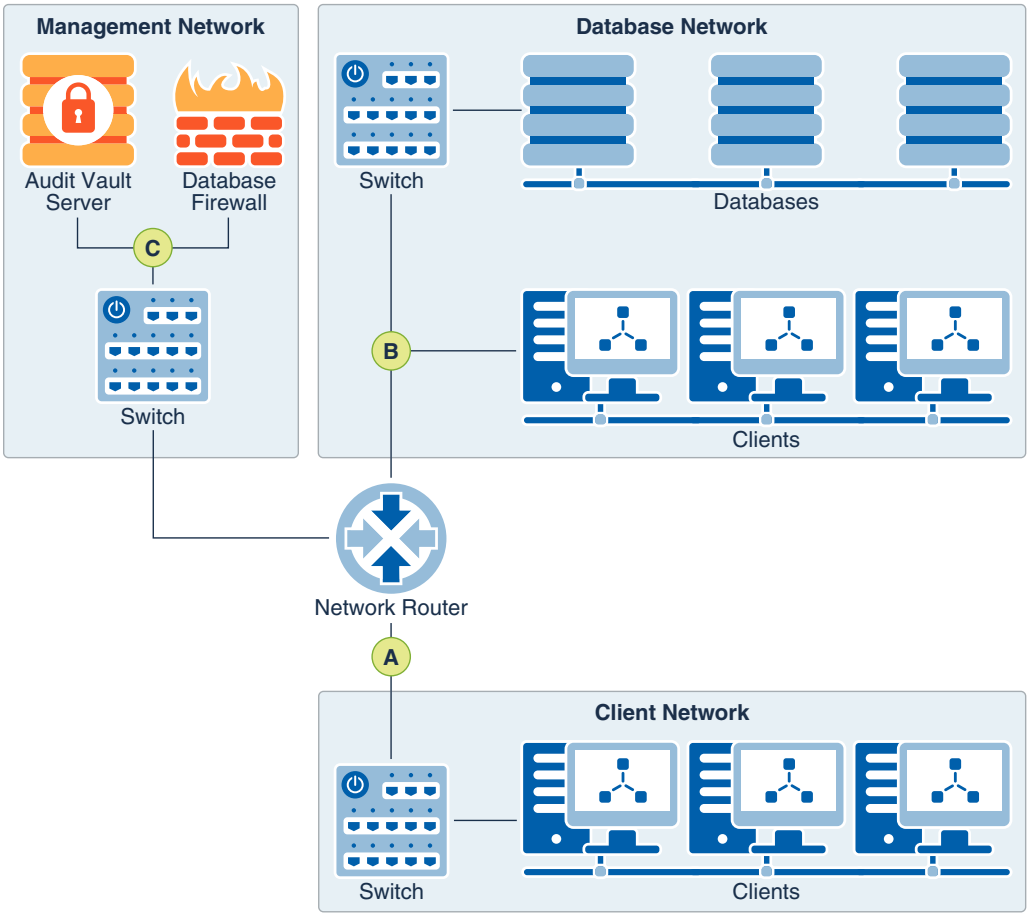
> **Note:**
>
> To simplify the modification required for applications to connect to the database firewall deployments through proxy, configure local domain name servers (DNS) in a way that the target fully qualified domain name (FQDN) resolves to the IP address of the database firewall.

You can deploy the proxy mode in the following two ways:

1. Without network separation (Proxy Without Network Separation mode)
2. With network separation (Proxy With Network Separation mode)

The Proxy Without Network Separation mode has the client and database on the same sub-network. In this mode, Oracle Database Firewall allows clients to connect through the database firewall. It also allows the clients to connect to the database directly, without a single point of failure.

Figure 4-2 Proxy Without Network Separation

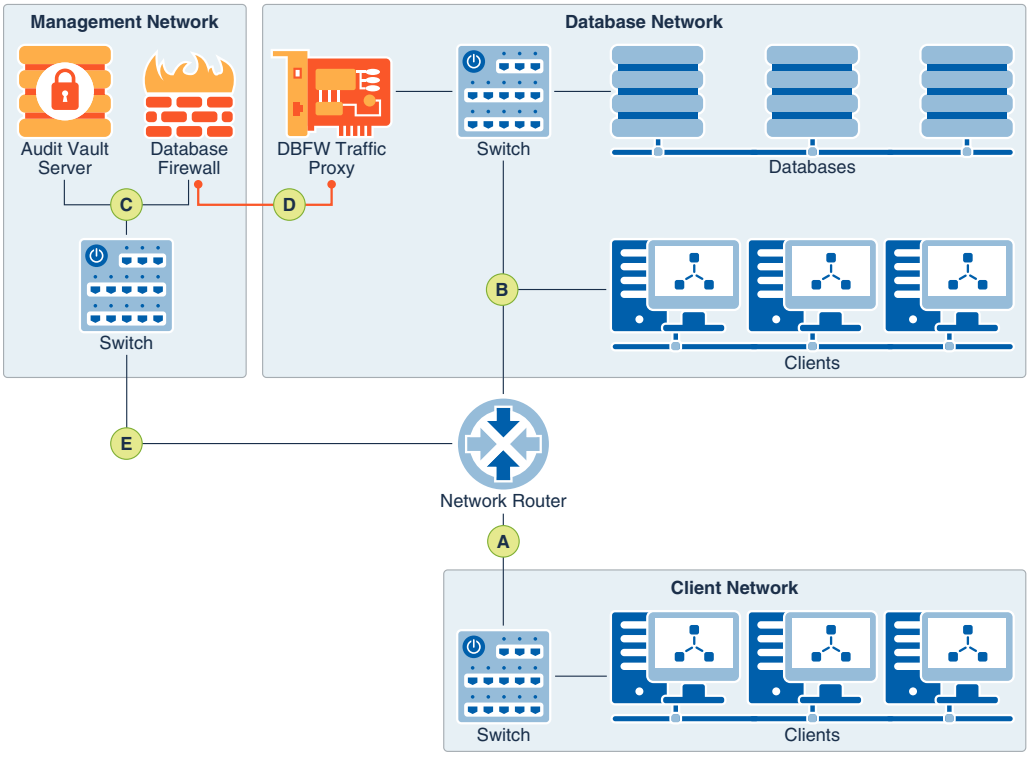


The image illustrates Oracle Database Firewall deployment in proxy mode without network separation. The callouts or pointers in the image indicate the following:

- A: The clients in the Client Network make an explicit connection to the database firewall directly.
- B: The clients in the Database Network also connect to the database firewall directly.
- C: The extracted SQL data from the client traffic is analyzed and sent to Oracle Audit Vault Server, based on the database firewall policy.

With the Proxy With Network Separation mode, the client and database are on different subnets. Additional network interface cards (NICs) are required for every additional subnet deployed.

Figure 4-3 Proxy With Network Separation



The image illustrates Oracle Database Firewall deployment in proxy mode with network separation. The callouts or pointers in the image indicate the following:

- A: The clients connect to the database firewall traffic proxy through the network router.
- B: The clients in the database network also connect to the database firewall directly.
- C: The extracted SQL data from the client traffic is analyzed and sent to Oracle Audit Vault Server, based on the database firewall policy.
- D: The traffic is forwarded to the target database by the database firewall. The response from target database reaches the originator through the network router. The response from the database is returned to the database firewall.
- E: The management network is separate from the client and database networks.

4.2.4 Out-of-Band

Learn about how to configure Oracle Database Firewall in the Out-of-Band mode.

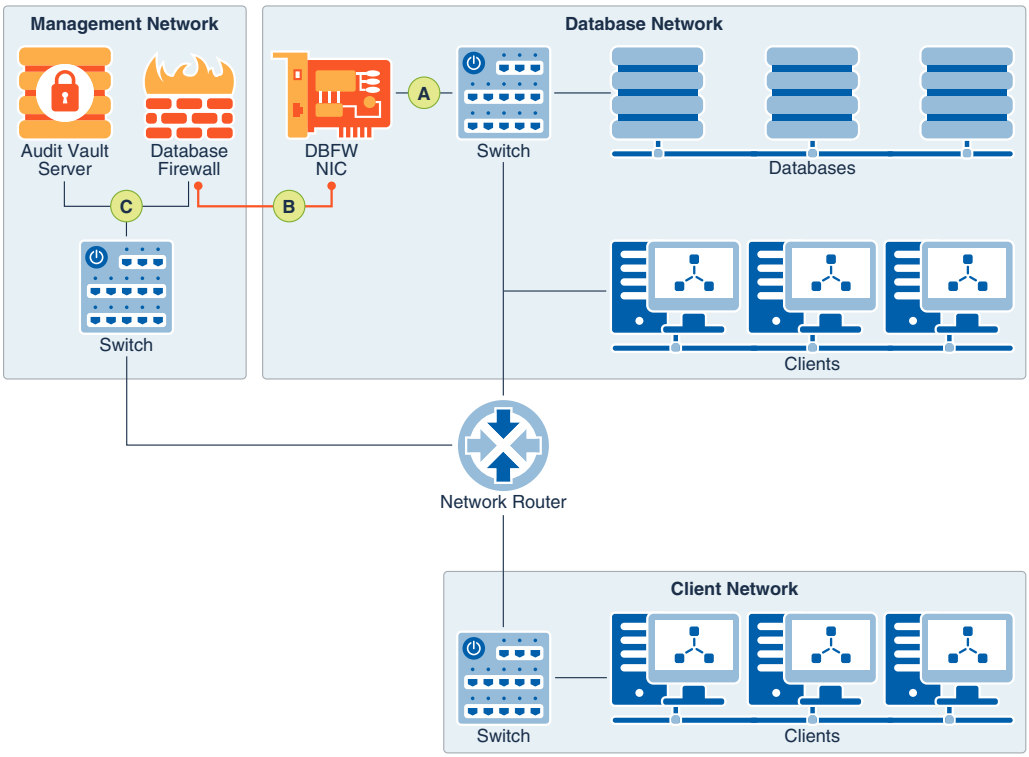
When you configure database activity monitoring in Out-of-Band mode, the database firewall intercepts the network traffic, including client requests to the database and the response from the database.

The database activity is monitored as per the defined policy. There are several technologies that can be used to copy database traffic to the database firewall. These technologies include (but are not limited to) spanning ports, network taps, and using packet replicators.

In this mode, Oracle Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.

The Out-of Band mode is the simplest deployment mode overall for a non-blocking policy requirement. There is no additional load on the database or the clients. There is no latency or single point of failure introduced by the database firewall. Oracle Audit Vault and Database Firewall supports high availability in this deployment mode.

Figure 4-4 Out-of-Band Mode



The image illustrates deployment of the database firewall component in Out-of-Band mode. The callouts in the image indicate the following:

- A: The Oracle Database Firewall interface is plugged into a span port on the switch.
- B: Oracle Database Firewall monitors the SQL traffic received.
- C: The extracted SQL data from the client traffic is analyzed and sent to Oracle Audit Vault Server, based on database firewall policy.

Related Topics

- *Oracle Audit Vault and Database Firewall Audit Vault and Database Firewall Administrator's Guide*

4.2.5 Host Monitor

Learn about how to configure the Host Monitor mode of Oracle Audit Vault Agent with Oracle Database Firewall.

To use the Host Monitor deployment mode with Oracle Database Firewall, an Oracle Audit Vault Agent must be placed on the host server, and configured to monitor network traffic to and from the database, as this traffic comes across the network interface card. Host Monitor then securely forwards the network traffic to the database firewall.

Oracle Database Firewall supports an Oracle Audit Vault Agent that only monitors and is deployed by the Oracle Audit Vault Server. This deployment option provides more flexibility in terms of monitoring at the network point. Using the Host Monitor mode is helpful in situations where it is not easy to use any of the previously described Oracle Audit Vault and Database Firewall networking options.

Caution:

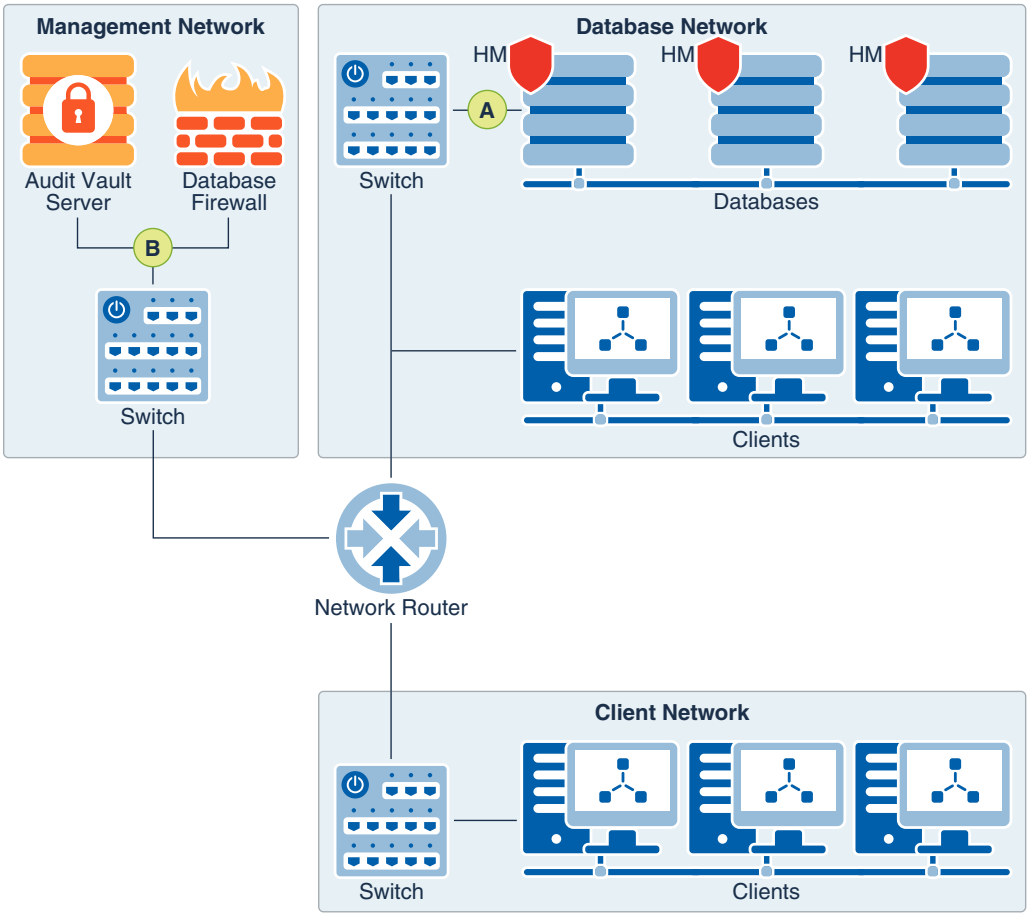
Host Monitor on Microsoft Windows platforms is not certified in release 12.2.0.11.0. Upgrade or use 12.2.0.11.0 only when you are sure that network trail monitoring functionality on Microsoft Windows platform is not required. This functionality can be certified in a future release. If your installation is pertaining to any of the older releases before 12.2.0.11.0, then Host Monitor functionality on Microsoft Windows platform is certified.

Host Monitor mode performs the following actions:

- Captures the SQL traffic of the target database
- Leaves unmonitored the traffic from local clients on the same host
- Forwards the data securely to Database Firewall

In this deployment mode, Oracle Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.

Figure 4-5 Host Monitor Mode



The image illustrates deployment of Oracle Database Firewall in Host Monitor mode. The callouts or pointers in the image indicate the following:

- A: The Host Monitor agent records the traffic in between the client and the database over a network interface. The data is then forwarded securely to the database firewall for monitoring.
- B: The extracted SQL data from the client traffic is analyzed and sent to Oracle Audit Vault Server, based on the database firewall policy.

4.3 Understanding Oracle Database Firewall Policies

4.3.1 Introduction to Oracle Database Firewall Policies

Learn how to define the parts of the Oracle Database Firewall policy for Oracle Audit Vault and Database Firewall.

To understand configuring the database firewall policies for Oracle Database Firewall, it is helpful to understand the terms **allowlist** and **blocklist**. Though you will not see the terms allowlist or blocklist in the Oracle Audit Vault and Database Firewall user interface when you are creating Oracle Database Firewall policy, these concepts are useful as you define the parts of Oracle Database Firewall policy.

A blocklist policy specifies a set of harmful statements that are disallowed. It also provides information about the various parameters and properties attached to the statements such as the incoming IP address, user name, and so on. Most monitoring solutions on the market today rely on regular expressions within their policies to determine which SQL statements should be blocked from reaching the database. The challenge with these first-generation solutions is that regular expressions do not match the expressive power of the SQL language. Because there are many different ways to write a SQL statement that will have some harmful effect, it is nearly impossible to write a regular expression rule that will detect all such statements. You can benefit from a blocklist by using it to define policies that disallow certain SQL statements based on the type of statement, the database object it acts upon, or session information such as IP addresses, user names, or client application names.

Because the set of harmful statements does not remain constant, instead of blocking a fixed set of “bad" statements, it is much more effective to allow only “good" statements, which are based on the normal activity of the applications, and the users that connect to the database. This set of good statements is a allowlist. To set up a allowlist policy, create a policy that monitors “normal" user behavior.

Oracle Database Firewall policies focus on the positive enforcement model of allowlists. However, a firewall policy can also support blocklists in the sense that you can use various elements of a firewall policy to disallow specific SQL statements.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed information on creating Database Firewall policies.

4.3.2 Components of an Oracle Database Firewall Policy

4.3.2.1 Exception Rules

Exception rules (also called preconditions) within a firewall policy evaluate various factors before analyzing SQL statements.

Exceptions evaluate these session factors:

- Database or operating system users
- Application IP addresses
- Application program names

For example, you can use an exception to block a set of client applications from accessing the database, except if the request is from a specific set of users. You can also use an exception to enable a specific remote administrator, coming from a predetermined IP address, to diagnose a particular application performance issue. without being bound by the rules for "normal" SQL set in the firewall policy.

As these examples show, exceptions can be seen either in terms of a allowlist or a blocklist, depending on how you define the exceptions. For blocklists, you also can disallow clusters, based on the user, or on the IP address.

4.3.2.2 Analyzed SQL

Learn about how to apply policies on clusters of analyzed SQL using Oracle Database Firewall.

Oracle Database Firewall automatically analyzes the SQL traffic to a database, and groups the SQL into similar statements, known as **clusters**. With these clusters of analyzed SQL, you can then use a simple policy manager user interface to quickly set up allowlists of normal behavior for the same type of SQL interaction. To set up these normal behavior allowlists, you set an appropriate action for each cluster. For example, in the Analyzed SQL part of a firewall policy, you can set the actions **Warn** or **Block**. In this way, you build a set of rules for different kinds of SQL statements in your firewall policy.

You can also use a blocklist policy for analyzed SQL by disallowing specific clusters of SQL in your policy.

4.3.2.3 Session Profiles

As with exceptions, session profiles in firewall policies evaluate session information before analyzing SQL statements.

You can define session profiles using the following information:

- Application IP addresses
- Application program names
- Database or operating system users

Session profiles differ from exceptions:

- An exception lets you bypass all the rules for analyzed SQL in your normal policy.
- A profile lets you define rules for any cluster of SQL in the analyzed SQL, based on the session factors.

For example: You can have different rules for the same SQL cluster if the cluster originates from a specific set of users, or specific IP addresses.

You can define several session profiles within a single firewall policy. By evaluating session information first, the policy lets you define different rules for the same analyzed SQL, depending on the session information. Session information includes client IP addresses, database user names, operating system user names, or database client names.

As with exceptions, you can define session profiles either in terms of a allowlist or a blocklist, depending on how you decide to define your rules.

4.3.2.4 Novelty Policies

To prevent or allow specific types of SQL statements acting on specific database tables, you can set novelty policies within a firewall policy.

\Novelty rules are often used for controlling behavior of DBAs over the network where it might be necessary to stop them from accessing specific application tables.

A novelty rule can be specified to act on the following categories of SQL:

- Data Manipulation: Statements such as `INSERT`, `UPDATE`, `DELETE`, `SELECT INTO`, and so on
- Data Manipulation Read-Only: `SELECT`
- Procedural: Stored procedures, or remote procedure call (RPC) commands
- Data Definition: Statements such as `CREATE`, `DROP`, `ALTER`, and so on
- Data Control Language: Statements such as `GRANT`, `REVOKE`, and so on
- Composite: commands that are executed in a transaction
- Transaction Control Language (TCL): `COMMIT`, `ROLLBACK`, and so on
- Composite with Transaction: a data manipulation language (DML) statement with a transaction control language (TCL) command, and so on

By combining SQL categories with specific tables, novelty rules enable you to define policy behavior for the entire classes of tables.

The database dictionary tables are not related to the application, and are not part of these rules.

As with other parts of a firewall policy, you can define novelty policies either in terms of a allowlist or a blocklist, depending on how you define the rules for the policies.

4.3.2.5 Default Rule

Learn about the default rule that Oracle Database Firewall can apply in a firewall policy.

The default rule in a firewall policy covers any remaining SQL that does not match any of the other policy rules that you define for a policy, such as rules for SQL statements, database objects, and so on. The default rule specifies the action that the database firewall applies for SQL that is not addressed in the allowlist or blocklist rules that you specify in your policy.

4.3.3 Flow of SQL Through a Database Firewall Policy

There are four categories of SQL analysis that Oracle Audit Vault and Database Firewall performs using the firewall policy.

SQL statements are evaluated in logical groups through Oracle Database Firewall instances using the following rules, in order of their application:

- Exceptions

  Exceptions to the policy are evaluated first. For example, if an exception says "apply the rules for analyzed SQL, except if the request is from this administrator," that rule is considered first.

- Session Profiles

  Session profiles are considered next. Depending on the session information (for example, the request is coming from a specific set of IP addresses), the policy applies the set of rules for analyzed SQL for that session profile.

- Clusters

  Clusters of SQL statements are identified, and matched with the rules defined for Analyzed SQL clusters.

- Novelty Policies

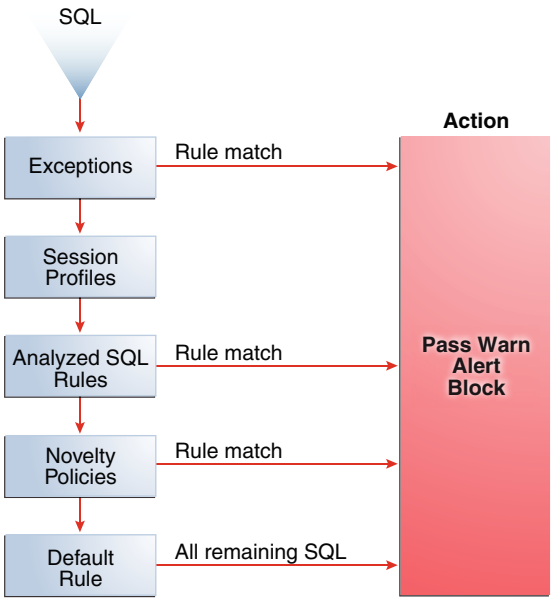
  The rules that you define for database objects are considered next for a possible rule match. These policies look at which database tables are accessed, and what type of SQL statement is used to access them.

- Default Rule

  The default rule is applied to any remaining SQL that does not match any of the above rules, so that you can set a standard policy for SQL.

The diagram below shows the order in which SQL statements are evaluated using the firewall policy. You can configure all rules or a subset of the rules.

Figure 4-6 Flow of SQL Through a Firewall Policy



Oracle Database Firewall monitors incoming SQL to the database, and applies the firewall policy assigned to the database in the descending order shown in the illustration. When SQL matches a rule in the firewall policy, Oracle Database Firewall takes the action defined in the policy.

4.3.4 How Oracle Database Firewall Handles Unauthorized SQL

You can configure four types of responses when Oracle Database Firewall identifies unauthorized SQL.

When Oracle Database Firewall finds an unauthorized statement, it can handle the statement in one or more of the following ways, based on the firewall policy that you define:

- Alert

  Raise an alert on all out-of-policy SQL statements.

- Block

  Block the SQL statement. When you define a block policy for a SQL statement, this specific statement is stopped from reaching the database server. When a statement is blocked, you can set the following actions in the firewall policy:

  – Do nothing after blocking the statement.

    When you set no response after the block, the client connection appears to hang, and the client has to terminate the session and reconnect to the database to execute more SQL.

  – Substitute (preferred)

    When you set a substitute policy, you provide a substitute statement for the blocked SQL statement: You replace the blocked statement with a new statement that does not return any data. Providing a substitute results in the

best end-user experience, and ensures that applications can keep running. The client session is maintained, and the client can execute more SQL if needed without having to reconnect.

– Drop the Connection

  When you set this response, the blocked SQL statement results in a drop of the client connection to the database. This response blocks all traffic from that specific connection to the database. This response is the most aggressive action. If the application is using connection pooling, then this response affects all of the users using the pool. Because an attacker can reestablish the connection, Oracle recommends that this action is always logged, and that appropriate users are alerted.

4.4 Planning and Rolling Out the Database Firewall

Before you deploy and configure database firewalls with Oracle Audit Vault and Database Firewall, you must review and make decisions about the Database Firewalls that you require, the level of protection you need, and other factors affecting configuration.

To deploy and configure database firewalls using Oracle Audit Vault and Database Firewall (the Database Firewalls), you must consider the following questions as part of your firewall planning:

- Which databases do I need to protect? In which networks are they located?

  Each of the databases that you want to protect will be added as secured targets in Oracle Audit Vault Server. The database location on the network affects how you can place the database firewall to achieve the type of monitoring that you need.

- Do I need to both monitor and block or substitute SQL traffic to my databases, or only monitor and alert?

  The answers you have to these questions can differ, depending on the database that you want to protect. Remember that to block and substitute SQL statements, a database firewall must be in-line between the database and its client applications, or configured as a proxy.

- How many Database Firewalls do I need, and where will they be on the network? Which ones will be in-line (bridge), out-of-band (for example, using a span port), or configured as proxies?

  In-line bridge mode is deprecated in 12.2.0.8.0, and can be desupported in a later release. Oracle recommends that you use proxy mode as an alternative.

  Based on your answer to this question, as well as the previous question, you can have a matrix showing the database secured targets, level of protection, and network mode. For example:

Table 4-2 Database Secured Target Matrix

Secured Target	Monitor Only or Block?	Network Mode	Oracle Audit Vault Agent?
Database 1	Monitor	Out-of-band	Optional
Database 2	Block	Proxy	Optional
Database 3	Block	In-line	Optional

Table 4-2 (Cont.) Database Secured Target Matrix

Secured Target	Monitor Only or Block?	Network Mode	Oracle Audit Vault Agent?
Database 3	Monitor	Host Monitor	Required

- How many enforcement points do I need for my Database Firewall?

  For each database secured target, you must configure one enforcement point in Oracle Audit Vault Server The enforcement point provides the following information to Oracle Audit Vault Server:

  – Which Database Firewall is protecting this database secured target
  – What protection level to use: activity monitoring (DAM) or policy enforcement/ blocking (DPE)
  – What are the network traffic sources to this database secured target?

  When configuring your enforcement points, consider compiling a list containing this information so that it is available to you during configuration.

- Do I need to configure database firewalls for high availability?

  To ensure that Oracle Audit Vault and Database Firewall can access security objects in the event of a failure, Oracle recommends that you configure Oracle Audit Vault and Database Firewall for a high availability environment.

5

Oracle Audit Vault and Database Firewall Reports and Alerts

Topics

5.1 Introduction to Oracle Audit Vault and Database Firewall Reports

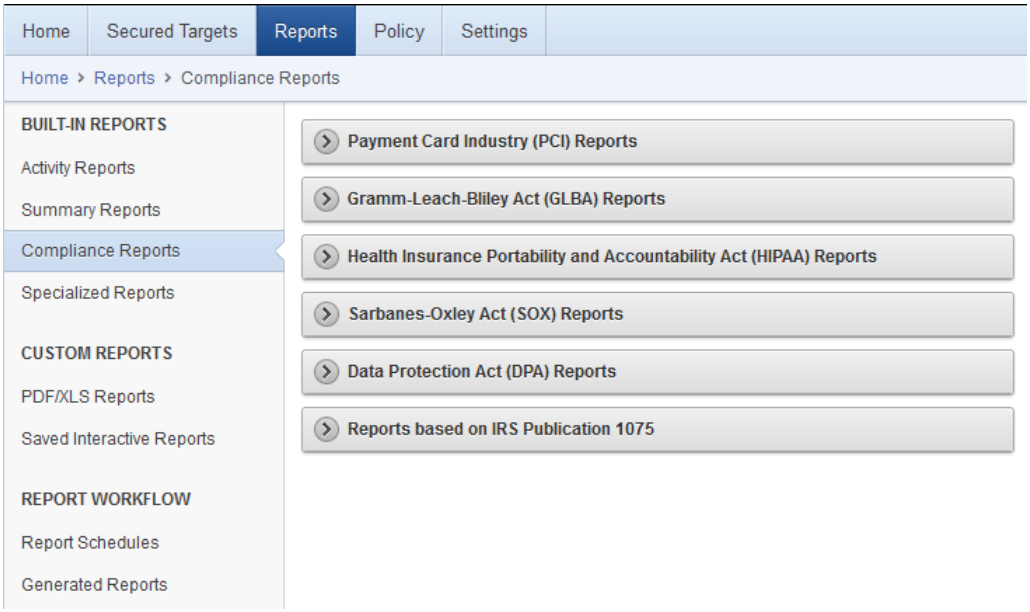
As an Oracle AVDF auditor, you can generate built-in audit reports that capture a wide range of audit data.

Oracle AVDF reports allow you to examine audit data in a consolidated fashion, that is, they show audit data collected from various secured targets, as well as data from Database Firewalls you have deployed. You can use the reports to monitor activities of interest, to meet regulatory requirements, and as a basis for setting up additional alerts to meet your needs.

The built-in reports are organized into various categories, such as activity reports and compliance reports. An alerts report allows you to view and respond to alerts. To meet regulatory requirements, you can produce reports such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Data Protection Act (DPA), Gramm-Leach-Bliley Act (GLBA), and Health Insurance Portability and Accountability Act (HIPAA) reports (shown in Figure 5-1 (page 5-2)).

You can save or schedule reports in either PDF or Excel format. You can also view reports online and interactively adjust the online report view by filtering, grouping, and highlighting data, and selecting the report columns to display. You can save these interactive views to see them online later. You can also send a report to other auditors for attestation.

Figure 5-1 Oracle AVDF Built-in Reports - Compliance Reports Section



5.2 Built-in Reports

Topics

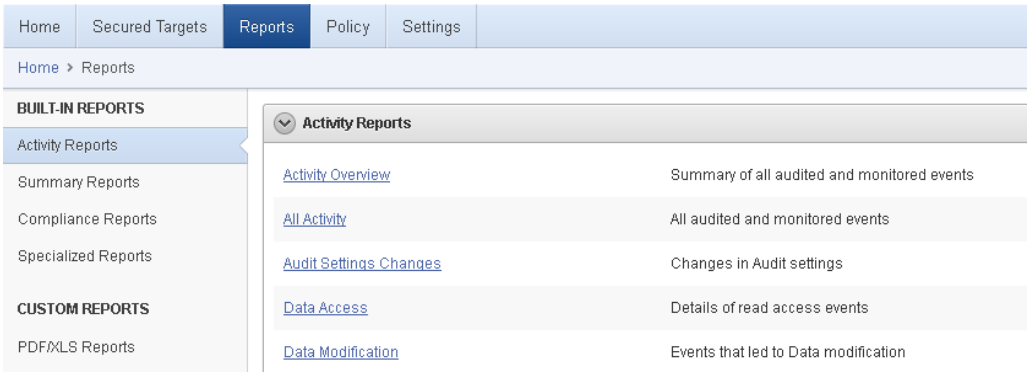
5.2.1 How to Use the Built-in Reports

You can run the built-in report immediately, or you can create a schedule to run the report at a later time. You can specify a list of users who receive notifications of the report, or who need to attest to the report.

While browsing reports online, you can download them in HTML or CSV format. You can also schedule reports and download them in PDF or XLS format, or send them to other users. When you specify report notifications, you can use your own notification templates to send emails to other users with either a link to a report, or an attached PDF version of the report.

Figure 5-2 (page 5-3) shows a few of the built-in audit reports.

Figure 5-2 Browsing, Scheduling, or Viewing Previously Generated Reports



5.2.2 Available Built-in Reports

There are many built-in reports that you can use to monitor your systems with Oracle Audit Vault and Database Firewall.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Auditor's Guide* for a complete list of the built-in reports.

The following table summarizes the different types of reports available.

Table 5-1 Available Types of Built-in Reports in Oracle Audit Vault and Database Firewall

Types of Reports	Description
Activity	A set of reports that track general database access activities such as audited SQL statements, application access activities, and user login activities. Some typical reports are: • Activity Overview: Displays information about all monitored and audited events • Data Modification: Displays the details of audited data modifications for a specified period of time • Data Modification Before-After Values: Displays the details of modified data and lists the values before and after modification. This report can be filtered. Note: – The transaction log collector uses Oracle Streams to collect the audit trail. When the transaction log trail is added, it creates the capture process on the secured target. When the capture process begins, it creates a log miner dictionary in an archive log. From then onwards, only the Before and After records from the archive logs are captured. It is not possible to acquire the Before and After values before the creation of the log miner dictionary. So transaction log trails cannot capture the old data. – While setting up a REDO collector, no role should be granted to the source user other than `DV_STREAMS_ADMIN`. To set up `DVSYS.AUDIT_TRAIL$` table trail, first set up the REDO collector with the role `DV_STREAMS_ADMIN` role granted to the source user. Once REDO collector is up and running, grant the role `DV_SECANALYST` to the source user. • Database Schema Changes: Displays details of audited DDL activity for a specified period of time • Login Failures: Displays details of audited failed user logins for a specified period of time
Alert	Alert reports track critical and warning alerts, and also let you respond online to alerts and notify others about them.
Stored Procedure Audit	A set of reports that help you keep track the changes made to the stored procedures, for example: • Stored Procedure Modification History: Displays details of audited stored procedure modifications for a specified period of time • Created Stored Procedures: Displays information about stored procedures created within a specified period of time • Deleted Stored Procedures: Displays information about deleted stored procedures deleted within a specified period of time
Compliance	A set of reports that track possible violations that are defined by the following compliance areas: • Payment Card Industry (PCI) • Gramm-Leach-Bliley Act (GLBA) • Health Insurance Portability and Accountability Act (HIPAA) • Sarbanes-Oxley Act (SOX) • Data Protection Act (DPA) • IRS Publication 1075

Table 5-1 (Cont.) Available Types of Built-in Reports in Oracle Audit Vault and Database Firewall

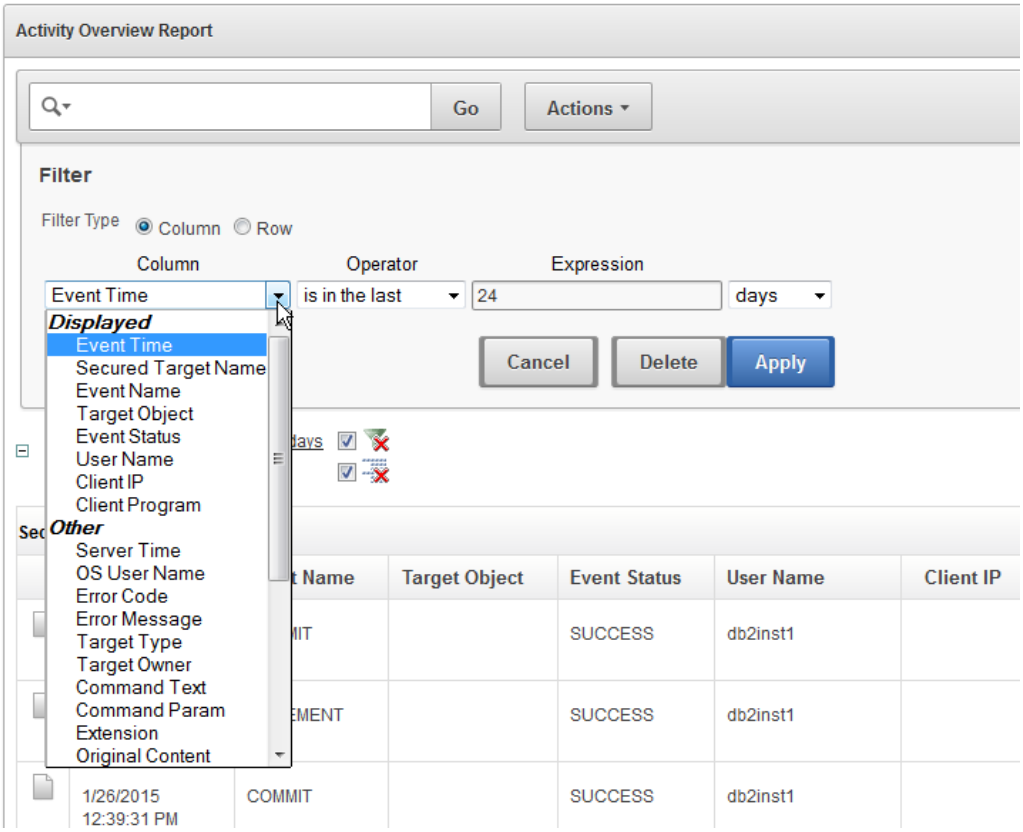
Types of Reports	Description
Database Firewall	For database secured targets that you are monitoring with the database firewall, this set of reports gives detailed event information about SQL traffic to these databases. Much of the information is dependent on the firewall policy you have assigned to a database. For example, you can see details of statements that had warnings, or were blocked, according to the policy. You can also see general information about SQL traffic to these databases, for example, statement type (data definition, data manipulation, etc.). Some example reports are: • Database Traffic Analysis by Client IP: Displays audit details for statements by the protected database and client IP address • Database Traffic Analysis by OS User: Displays audit details for statements grouped by protected database and OS user • Database Traffic Analysis by User Blocked Statements: Displays audit details for blocked statements grouped by protected database and OS use
User Entitlements	A set of reports that describe user access and privileges for Oracle Database secured targets, for example: • User Accounts: Displays information such as the secured target in which the user account was created or the user account name, and whether this account is locked or expired • User Privileges: Displays information such as the secured target in which the privilege was created, user name, and privilege • Object Privileges: Displays information such as the secured target in which the object was created, users granted the object privilege, and the schema owner • Privileged Users: Displays information such as the secured target in which the privileged user account was created, user name, and privileges granted to the user
User Correlation	For Oracle Database secured targets running on Linux, these reports let you correlate events on the database with the original Linux OS user. This is useful in cases where this user runs a shell or executes a command on the database as another user by using `su` or `sudo`.
Database Vault Activity	If your Oracle Database secured targets have Database Vault enabled, the Database Vault Activity report shows Database Vault events, which capture policy or rule violations, unauthorized access attempts, etc.

5.2.3 Customizing Built-in Reports

You can create customized reports based on the built-in reports and then save the new report formats to view them online. Oracle AVDF provides tools to filter, group, and highlight data, and define columns displayed in the reports.

Figure 5-3 (page 5-6) shows an example of filters that you can use to customize built-in reports.

Figure 5-3 Interactively Customizing a Built-In Report



The next topic shows some examples of customizing built-in reports.

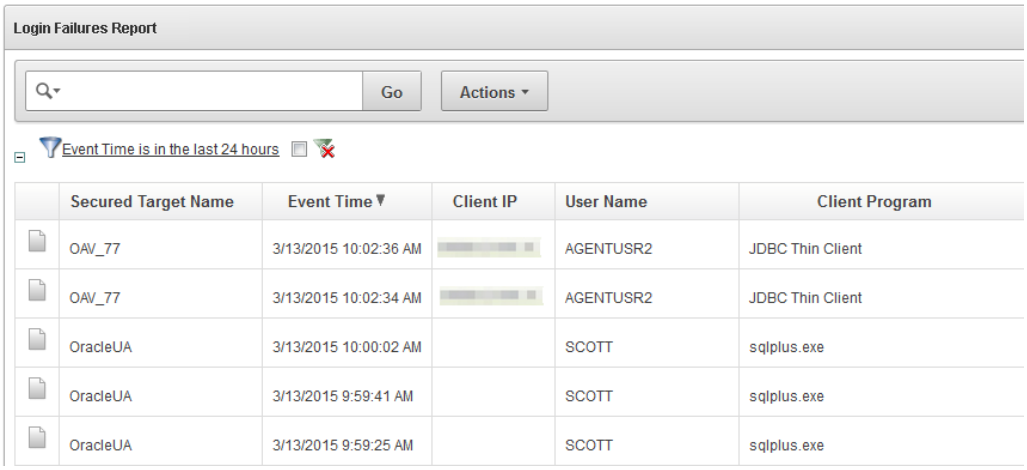
5.2.4 Examples of Customizing Built-in Reports

Topics

5.2.4.1 Login Failures Report

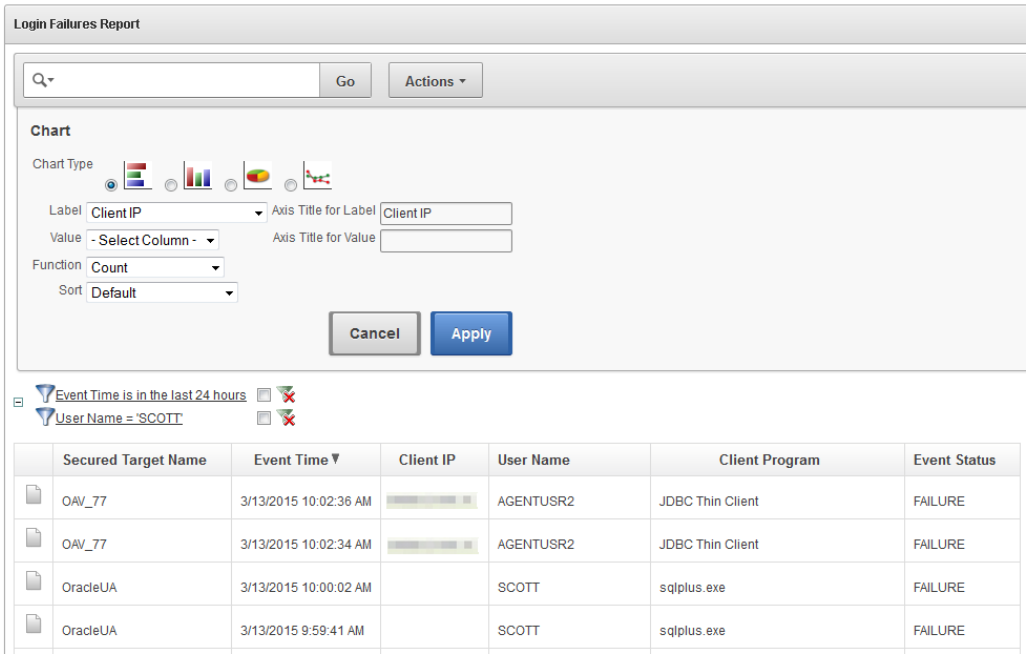
You may want to examine the Login Failures report to see if there are an unusual number of failed attempts to access a database, as well as which users or IP addresses originated those attempts. Figure 5-2 (page 5-3) shows the Failed Logins report.

Figure 5-4 Login Failures Report



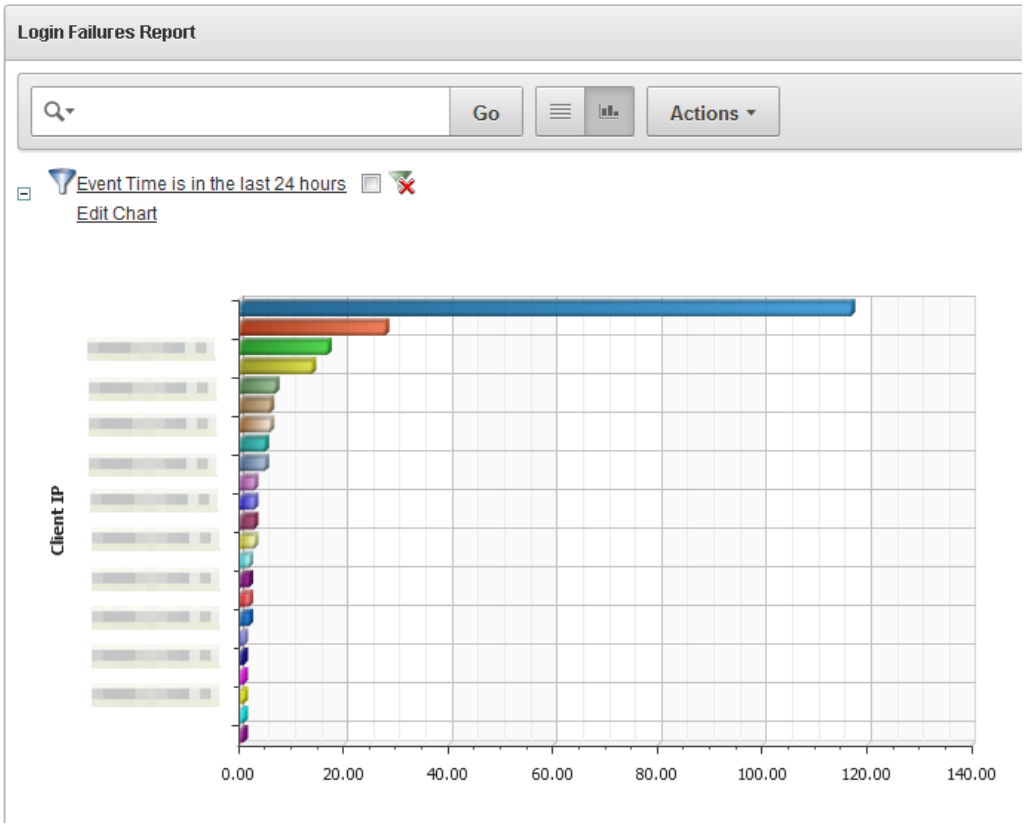
Suppose you want to see a visual breakdown of failed logins by client IP address. You can use the formatting tools to create a chart type of your choice, as shown in Figure 5-5 (page 5-7).

Figure 5-5 Customizing the Failed Logins Report into a Chart Format by Client IP



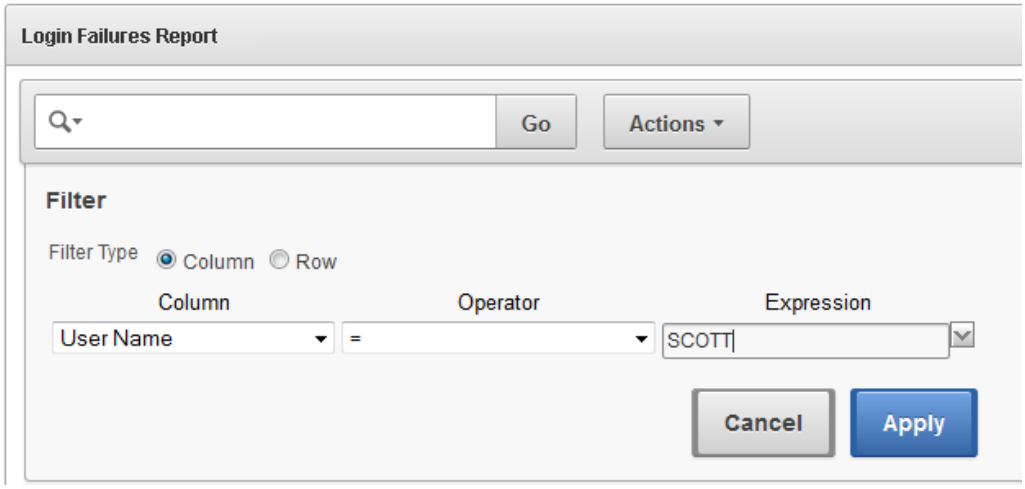
In the preceding illustration, we have chosen a horizontal bar chart with each bar representing a different client IP address. We have chosen a simple count to show the number of failed login attempts. The resulting chart, shown in Figure 5-6 (page 5-8), clearly shows a large number of failed logins from one IP address.

Figure 5-6 Failed Logins Shown in a Bar Chart by Client IP Address



Similarly, you may want to see failed logins originated by a particular user, using the formatting tools to filter the report as shown in Figure 5-7 (page 5-8).

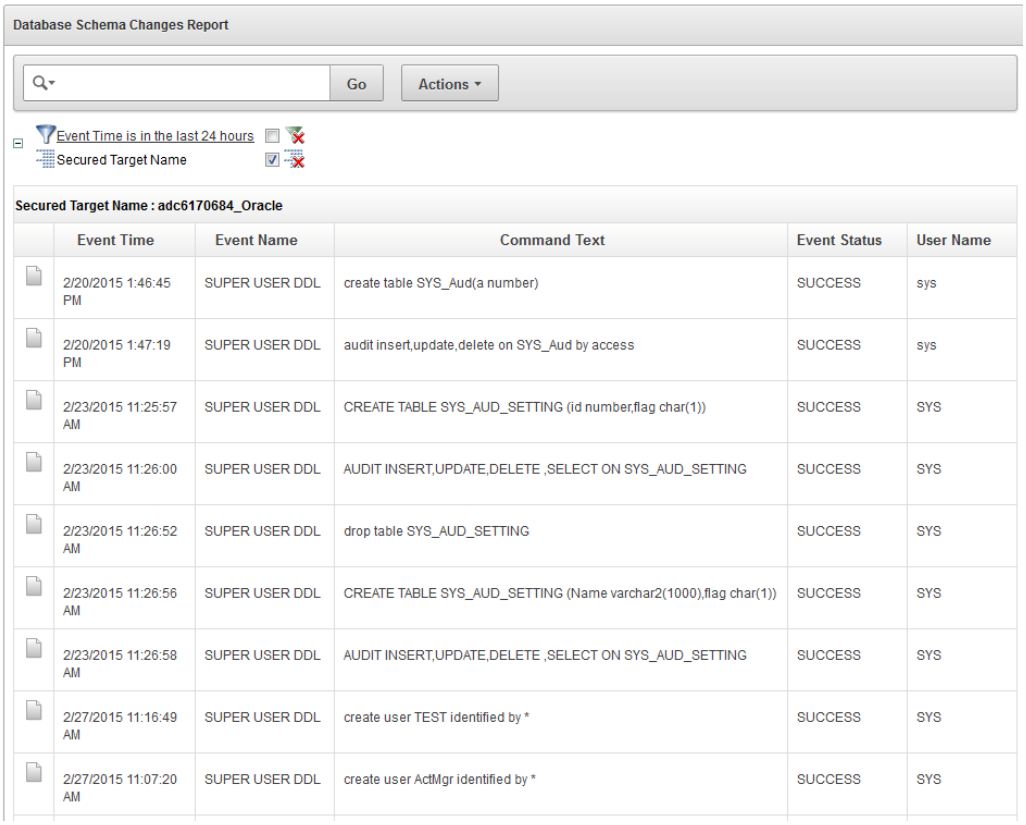
Figure 5-7 Filter the Failed Logins Report for a Specific User



5.2.4.2 Database Schema Changes

The Database Schema Changes report shows audited DDL activities, for example, `DROP TABLE` or `CREATE PROCEDURE`. This is useful for finding unauthorized changes and when you want to investigate changes to the database schema. For example, you may want to maintain strict standards for changes to the database, where multiple users may implement these changes. Or, an application may stop working, requiring you to investigate if a change to the database may be the cause. Figure 5-8 (page 5-9) shows the Database Schema Changes report.

Figure 5-8 Database Schema Changes Report



Using the same techniques used for the Failed Logins report, you can sort and group the report in various ways to get the information you want. You can add or remove columns, filter by user name, client program name or IP address, and many other fields.

For example, suppose you are interested in investigating `SUPER USER DDL` commands for the user `SYS`. You can filter the report data for that event name and that user. Figure 5-9 (page 5-10) shows an example of adding the event name filter, and Figure 5-10 (page 5-10) shows the resulting report filtered by both this event name and the user name `SYS`.

Figure 5-9 Filtering a Report by Event Name

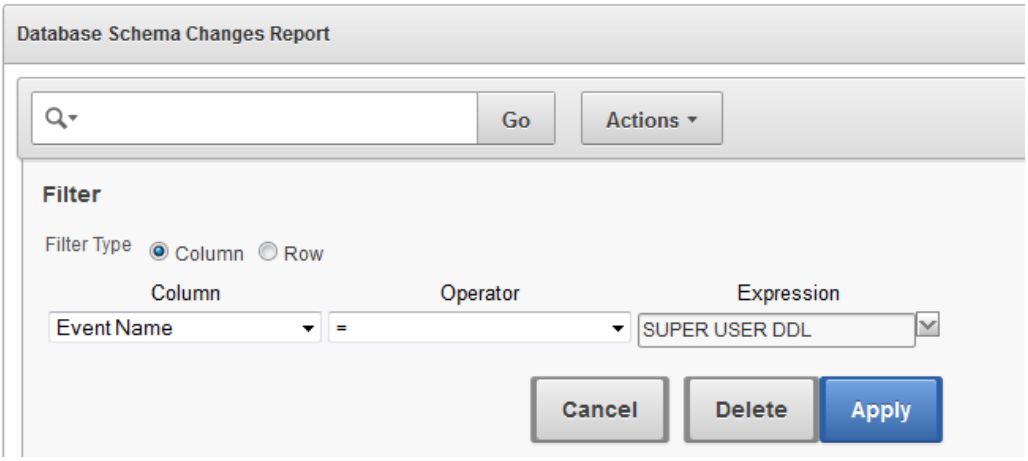
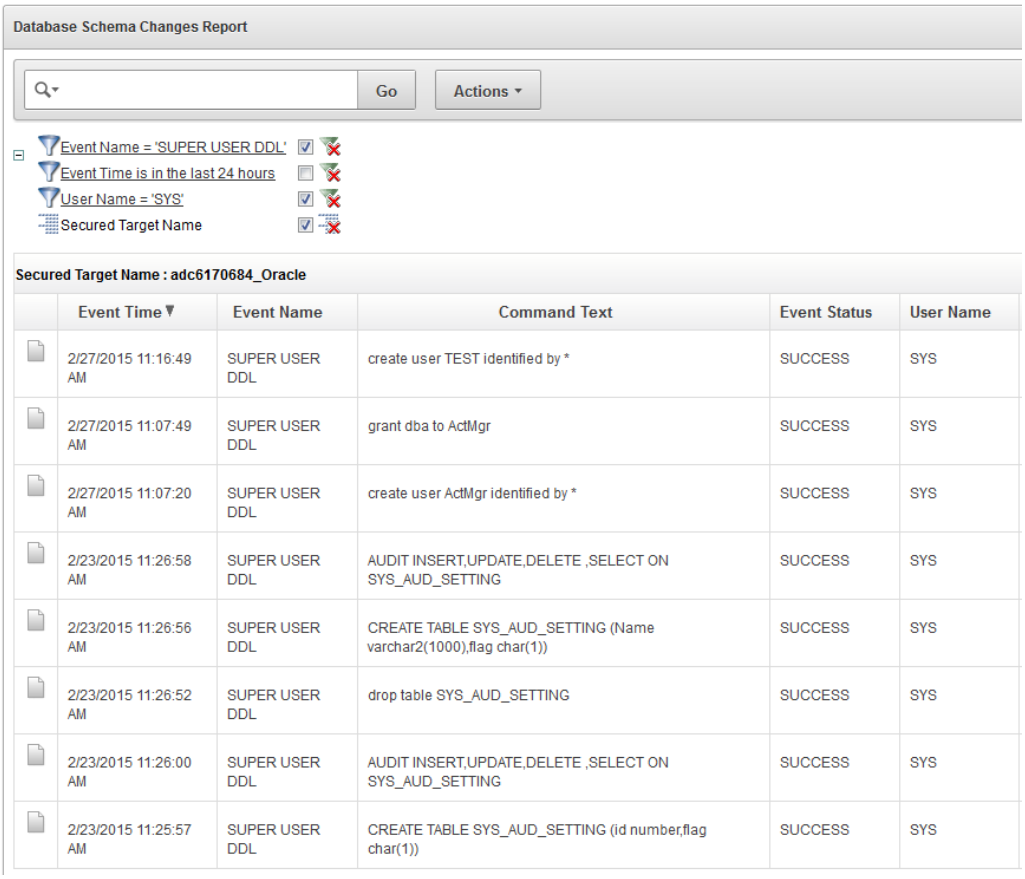
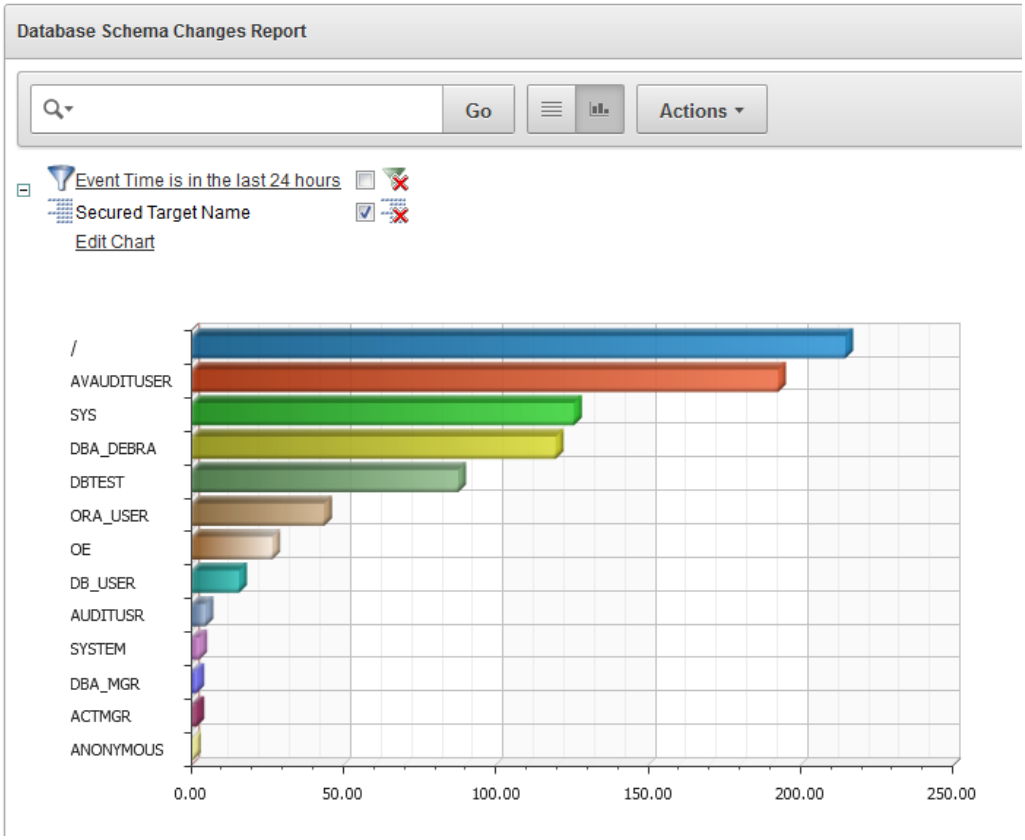


Figure 5-10 Database Schema Changes Filtered for a Specific Event Name and User



As another example of customizing this report, in Figure 5-11 (page 5-11), we have chosen to show schema changes by user name, displayed in a bar chart.

Figure 5-11 Database Schema Changes Shown in a Bar Chart by User Name



This chart shows you the breakdown of how many DDL changes were done by each user.

5.3 Custom Reports

Topics

5.3.1 Introduction to Custom Reports

This topic describes how to create customized reports for Oracle Audit Vault and Database Firewall.

There are two ways of creating custom reports with Oracle Audit Vault and Database Firewall. One way is to interactively customize the built-in reports by filtering data, and then save these interactive views so you can view them again online later.

> **See Also:**
>
> Examples of Customizing Built-in Reports (page 5-6)

The second way is to create your own reports by making simple customizations based on built-in report templates, or by using a software package (such as Oracle BI Publisher). You can then upload your own custom reports into Oracle Audit Vault and Database Firewall. This second method is discussed below.

5.3.2 Tools for Creating Your Own Custom Reports for Oracle AVDF

You can upload your own custom reports to Oracle Audit Vault and Database Firewall (Oracle ADVF) by using Oracle BI Publisher, or another report authoring tool from a third party.

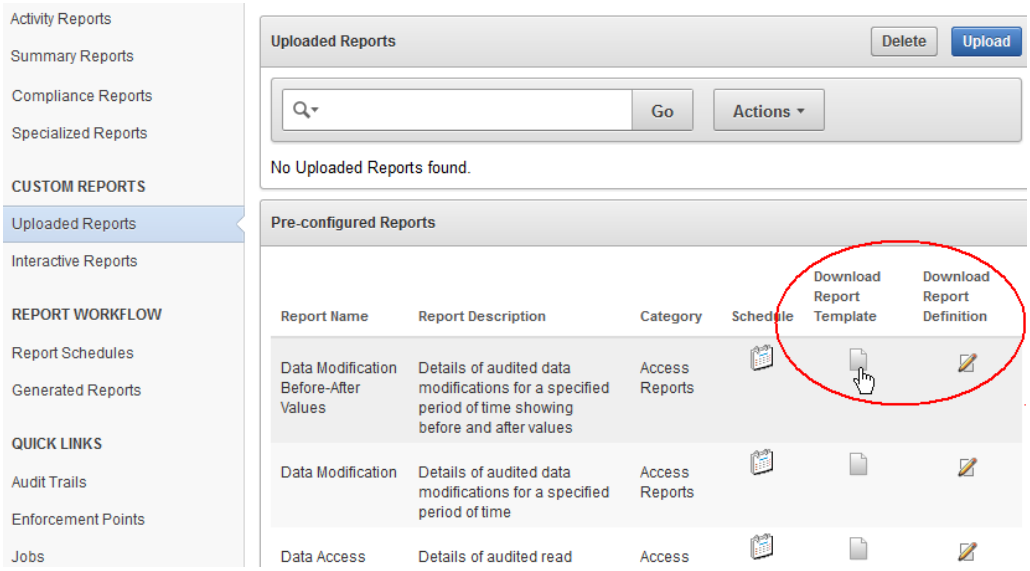
For simple changes to the built-in report formats, you can also do some customizations without using a report authoring tool.

Oracle Audit Vault and Database Firewall provides two types of files to help you get started creating custom reports. The first type of file is a report template in rich text format (RTF), which you can open in a tool such as Microsoft Word. The template determines the display of the report, so for example, you can easily add your own custom logo on the report. The second type of file is a report definition in XML format, which you can open in a text or XML editor. The report definition file specifies the data in the report.

You can download report definition and template files corresponding to any of the built-in reports, and then you can use these files as a starting point for creating your own custom report. Oracle AVDF documentation also provides several appendices on event data collected from different types of secured targets that will help you in creating your own reports.

The following illustration shows how an auditor can download various types of report definition and template files with which to start creating a custom report.

Figure 5-12 Downloading Report Template and Definition Files



5.4 Alerts and Notifications

Oracle Audit Vault and Database Firewall lets you define rule-based alerts on audit records, whether these records come from the Audit Vault Agent or the Database Firewall.

You can also specify notifications for rule-based alerts. For example, you can set up an email to be automatically sent to a user, such as a security officer, or to a distribution list. Alerts can also be forwarded to `syslog`. This is useful if you want to integrate them with another system.

Alerts you define are independent of audit policies or firewall policies. For example, in firewall policies, you can specify that certain SQL statements types (clusters) should raise an alert when encountered by the Database Firewall. But you may also want to define a special condition that raises an alert based on factors other than those specified in a firewall policy. This can be a quick way to notify a specific person or group when that condition is met. Or you may want to be alerted whenever this condition is met for all secured targets, whereas the firewall policy may have been assigned to only one secured target.

Because alerts are rule-based, if the rule definition is matched (for example, User A fails to log in to Database B after three tries), then an alert is raised. The rule is called a **condition** in Oracle Audit Vault and Database Firewall. The condition is a Boolean statement, similar to a `WHERE` clause in a `SELECT` statement. For example:

Note he `WHERE` clause in this `SELECT` statement:

```
SELECT user_name, event_status, event_name from avsys.event_log
   WHERE event_status='FAILURE' and upper(event_name)='LOGON';
```

The `WHERE` clause can be translated into this alert condition:

```
:event_status='FAILURE' and upper(:event_name)='LOGON'
```

Alert conditions are flexible and can include more than one event, and the events can come from different secured targets. For example, an alert can be applied to four Oracle Databases. The alert condition can also be a complex statement. For example: User A failed to log in to secured target X, and User A also failed to log in to secured target Y.

A good way to define an alert condition is to first look at the Oracle Audit Vault and Database Firewall All Activity Report, which displays details of all captured audit events. From this report you can see possible events that may be of interest to you. This can be the starting point for your alert condition.

Index

M

N

O

P

R

S

T