Oracle® Audit Vault and Database Firewall

Administrator's Guide

Release 12.1.2

E27776-24

December 2016

ORACLE®

Oracle Audit Vault and Database Firewall Administrator's Guide, Release 12.1.2

E27776-24

Primary Author: Karthik Shetty

Contributing Authors: Janis Greenberg, Gigi Hanna, Pat Huey, Sheila Moore.

Contents

2 General Security Guidelines

3 Configuring the Audit Vault Server

4 Configuring the Database Firewall

5 Registering Hosts and Deploying the Agent

6 Configuring Secured Targets, Audit Trails, and Enforcement Points

7 Enabling and Using Host Monitoring

8 Configuring High Availability

9 Configuring Integration with BIG-IP ASM

10 Configuring Integration with ArcSight SIEM

Part II General Administration Tasks

11 Managing User Accounts and Access

12 Managing the Audit Vault Server and Database Firewalls

13 Configuring a SAN Repository (AVDF 12.1.2)

Part III General Reference

A AVCLI Commands Reference

B Plug-in Reference

List of Figures

List of Tables

Preface

Oracle Audit Vault and Database Firewall Administrator's Guide explains how to configure an Audit Vault and Database Firewall installation.

Topics

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.

Related Documents

For more information, see the following documents:

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

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 Release

This preface describes new features in the most recent, as well as prior, releases of Oracle Audit Vault and Database Firewall (AVDF).

Topics

Oracle AVDF Release 12.1.2 Changes

The following are new features in this release:

- You can configure the Audit Vault Server to use an external iSCSI SAN server to store the audit event repository and system data.
- The Audit Vault Agent is updated automatically when the Audit Vault Server is upgraded or a patch is applied.
- You can store archive data in a Network File Share (NFS) location.
- Entitlement reports include data specific to Oracle Database 12*c*.
- Database Vault is automatically enabled and configured in the Oracle Database embedded in the Audit Vault Server. This further strengthens security by restricting privileged access to the Oracle Database for all users including those with administrative access.
- Password hashing has been upgraded to a more secure standard. Change your passwords after upgrade to take advantage of the more secure hash.
- The Audit Vault Agent deployment procedure has been simplified. Registering a host in the Audit Vault Server automatically generates an Agent activation key, and therefore, the step requesting Agent activation is no longer required.
- Adding and updating a secured target location has been simplified in the Audit Vault Server administrator console UI.
- You can set alerts to be forwarded to syslog.
- You can download diagnostics log files from the Audit Vault Server UI.
- The Audit Vault Agent is supported on 32-bit Linux and Windows platforms.
- Oracle Database 9*i* is supported for Database Firewall.
- MySQL 5.6 is supported on the Database Firewall.
- Updated the Audit Vault error messages.

Oracle AVDF Release 12.1.1 Changes

The following are new features in this release:

- Audit data collection and Database Firewall protection is now supported for the following secured targets:
  - Oracle Database 12*c* Release 1 (12.1)
  - Microsoft SQL Server 2012
- Audit data collection is now supported for the following secured targets:
  - Linux OS
  - MySQL
  - Oracle ACFS
- Audit Vault Agent is now supported on HP-UX Itanium platforms
- Host monitoring is now supported on the following host platforms:
  - Solaris
  - Windows
- Simpler installation and upgrade process

  The installation procedure has been simplified to use only one disc for installing the Audit Vault Server, and one disc to install the Database Firewall, and requires less user intervention.

  The same discs used to install the Audit Vault Server or Database Firewall are used to upgrade these components to release 12.1.1. Once the user selects to upgrade the system, no further intervention is required.

Quick Reference for Common Tasks

Topics

About this Quick Reference

This chapter is intended for users familiar with Oracle Audit Vault and Database Firewall (AVDF), and who want to quickly locate step-by-step instructions for common tasks. If you are new to AVDF, we recommend you read the introductory material to get an understanding of the system and to plan your configuration.

See "Summary of Configuration Steps" on page 1-9 to understand the suggested workflows for configuring Oracle AVDF.

Audit Vault Server

System Settings

"Specifying the Server Date, Time, and Keyboard Settings" on page 3-2

"Setting or Changing the Audit Vault Server Network Configuration" on page 3-3

"Configuring or Changing the Audit Vault Server Services" on page 3-4

"Configuring the Audit Vault Server Syslog Destinations" on page 3-5

"Configuring the Email Notification Service" on page 3-7

Archiving and Restoring

High Availability Pairing of Audit Vault Servers

AVCLI (Command Line Interface)

Other Operations

Database Firewall

Firewall System Settings

Host Monitor

Host Monitor Installation

Host Monitor Operations

Updating

Host Monitor Security

Secured Targets

Registering and Managing

Auditing

Preparing for Auditing

Audit Trails

Monitoring with Database Firewall

Enforcement Points

Database Interrogation and Response Monitoring

See also: "Database Firewall" on page 4-xxii

BIG-IP ASM Integration

Arcsight Integration

Other Administrator Tasks

Reference Information

Plug-ins

Other Reference Information

Part I

Getting Started

Part I guides you through the process of a basic configuration of the Audit Vault and Database Firewall system. It takes you from the point of a new installation through the process of configuring the Audit Vault and Database Firewall components to connect with one another.

This part contains the following chapters:

1

Introducing Oracle Audit Vault and Database Firewall

Topics

Downloading the Latest Version of This Manual

You can download the latest version of this manual from the following website:

`http://www.oracle.com/pls/topic/lookup?ctx=avdf121`

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

`http://docs.oracle.com`

Supported Platforms

See *Oracle Audit Vault and Database Firewall Installation Guide* for detailed platform support for the current release.

In addition, you can find platform information for prior releases in **Article 1536380.1** at the following website:

`https://support.oracle.com`

Understanding System Features and Concepts

Topics

About Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (AVDF) secures databases and other critical components of IT infrastructure (such as operating systems) in these key ways:

- Provides a database firewall that can monitor activity and/or block SQL statements on the network based on a firewall policy.
- Collects audit data, and makes it available in audit reports.
- Provides dozens of built-in, customizable activity and compliance reports, and lets you proactively configure alerts and notifications.

This section provides a brief overview of the administrative and auditing features of Oracle AVDF.

Oracle AVDF auditing features are described in detail in *Oracle Audit Vault and Database Firewall Auditor's Guide*.

System Requirements

For complete hardware and software requirements, refer to the AVDF pre-installation requirements in *Oracle Audit Vault and Database Firewall Installation Guide*.

Supported Secured Targets

A secured target is a database or nondatabase product that you secure using either the Audit Vault Agent, the Database Firewall, or both. If the secured target is a database, you can monitor or block its incoming SQL traffic with the Database Firewall. If the secured target, whether or not it is a database, is supported by the Audit Vault Agent, you can deploy the agent on that target's host computer and collect audit data from the internal audit trail tables and operating system audit trail files.

Oracle AVDF supports various secured target products out of the box in the form of built-in plug-ins. See the following for information about plug-ins and currently supported secured target versions:

- "About Plug-ins" on page 5-9
- Appendix B, "Plug-in Reference" on page B-1 for detailed information on each plug-in.
- Table B–1 on page B-2 for supported secured target products and versions.
- Table B–13 on page B-11 for the data collected and platforms supported for each audit trail type.

You can also create custom plug-ins to capture audit trails from more secured target types using the Oracle AVDF SDK. For information about the SDK, see *Oracle Audit Vault and Database Firewall Developer's Guide*.

Oracle AVDF also supports Oracle Big Data Appliance as a secured target. For details, see *Oracle Big Data Appliance Owner's Guide*.

Administrative Features

Oracle AVDF administrative features allow an administrator to configure and manage the following:

- Secured Targets and their host computers
- Database Firewalls
- High Availability
- Third party integrations
- Audit Vault Agent deployment
- Audit trail collection
- Audit data lifecycle, archiving, and purging

Auditing Features

Oracle AVDF auditing features allow an auditor to configure and manage the following:

- Firewall policies
- Audit policies for Oracle Database
- Reports and report schedules
- Entitlement auditing for Oracle Database
- Stored procedure auditing
- Alerts and email notifications

See *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed information on these auditing features.

Integrations With Third-Party Products

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

- **BIG-IP Application Security Manager (ASM):** This product from F5 Networks, Inc. is an advanced Web Application Firewall (WAF) that provides comprehensive edge-of-network protection against a wide range of Web-based attacks. It analyzes each HTTP and HTTPS request, and blocks potential attacks before they reach the Web application server. For more information, see Chapter 9, "Configuring Integration with BIG-IP ASM."
- **ArcSight Security Information Event Management (SIEM):** This product is a centralized system for logging, analyzing, and managing syslog messages from different sources. For more information, see Chapter 10, "Configuring Integration with ArcSight SIEM."

Overview of the Oracle AVDF Component Architecture

Topics

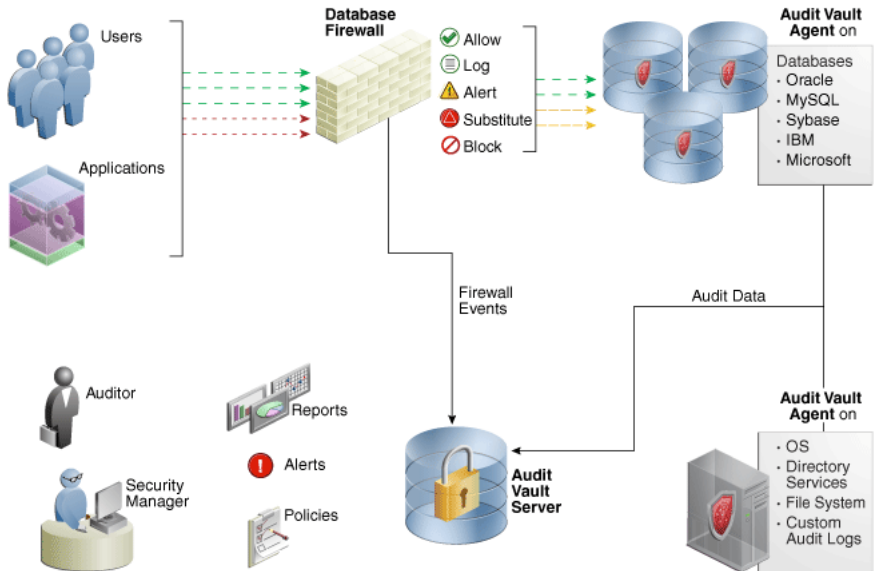
Components of Oracle AVDF

Topics

How Oracle AVDF Components Work Together

Oracle AVDF includes the Audit Vault Server, the Database Firewall, and the Audit Vault Agent. Figure 1–1 provides a high-level overview of how these components work together.

Figure 1–1 Audit Vault and Database Firewall Architecture



The process flow for the Audit Vault and Database Firewall components is as follows:

1. For each secured target, the Audit Vault Agent is deployed, and/or the Database Firewall is placed in the network and configured to protect that target.

   If the agent is deployed, Oracle AVDF is configured to collect the appropriate audit trail from the secured target. If the Database Firewall is protecting the target, a firewall policy is applied for that target.

   You can configure multiple secured targets from different database product families, as well as nondatabase products, using the same Audit Vault Server.

2. The Audit Vault Agent retrieves the audit data from secured targets and sends this data to the Audit Vault Server.

   The Database Firewall monitors SQL traffic to database secured targets and sends data to the Audit Vault Server according to a firewall policy. The firewall can be configured to monitor and raise alerts only, or to block SQL traffic and optionally substitute statements according to a policy.

3. The Audit Vault Server stores the Oracle AVDF configuration data, and the collected audit data, in its internal data warehouse.

4. Once the audit data is in the data warehouse, an auditor can generate and customize reports, as well as configure email notifications, on the Audit Vault Server.

The Audit Vault Server

The Audit Vault Server contains the tools necessary to configure Audit Vault and Database Firewall components, and to collect audit data from, and apply firewall policies to, your secured targets. Any settings that you, the administrator, create, such as security settings, are contained in this server.

The Audit Vault Server also contains an Oracle database, and makes it available to reporting tools through a data warehouse.

This embedded Oracle Database has Database Vault automatically enabled and configured. Database Vault provides greater security by restricting access to sensitive areas of the Oracle Database for any user, including those with administrative access.

> **Note:** You should not attempt to administer or set password policies for the Oracle Database embedded in the Audit Vault Server.

The Audit Vault Server provides the following services:

- Audit data collection and lifecycle management
- Audit Vault Agent management
- Database Firewall management
- Audit and firewall policy management
- Alerting and notification management
- User entitlement auditing
- Stored procedure auditing (SPA)
- Reporting
- Archiving data
- High availability mode
- Published data warehouse schema that can be used with reporting tools such as Oracle Business Intelligence Publisher to create customized reports
- User access management
- Third party integrations

The Database Firewall

The Database Firewall is a dedicated server that runs the Database Firewall software. Each Database Firewall monitors SQL traffic on the network from database clients to secured target databases. The Database Firewall then sends SQL data, according to a defined firewall policy, to the Audit Vault Server to be analyzed and presented in reports.

An Oracle AVDF auditor can create firewall policies that define rules for how the Database Firewall handles SQL traffic to the database secured target. The firewall policy specifies the types of alerts to be raised in response to specific types of SQL statements, and when to log specific statements. The policy also specifies when to block potentially harmful statements, and optionally substitute harmless SQL statements for blocked statements. To do this, the Database Firewall can operate in one of two monitoring modes:

- **DPE Mode:** Database Policy Enforcement. When in this mode, the Database Firewall applies rules in a firewall policy to monitor SQL traffic to your secured target database and raise alerts, block traffic, and/or substitute benign SQL statements for potentially destructive ones.
- **DAM Mode:** Database Activity Monitoring. When in this mode, the Database Firewall applies rules in a firewall policy to monitor and raise alerts about potentially harmful SQL traffic to your secured target database, but it does not block or substitute SQL statements.

In order to control how the Database Firewall protects a database secured target, you configure enforcement points for each secured target. The enforcement point specifies whether the firewall operates in DPE or DAM mode, which firewall policy to apply to the secured target, and other settings. For more information, see "Configuring Enforcement Points" on page 6-13.

The Database Firewall can be placed in your network in various ways: inline, out of band, or configured as a proxy. For more information, see:

- "Configuring Database Firewalls on Your Network" on page 4-5
- "Configuring a Database Firewall as a Traffic Proxy" on page 4-6

The Audit Vault Agent

The Audit Vault Agent retrieves the audit trail data from a secured target database and sends it to the Audit Vault Server. If the Audit Vault Agent is stopped, then the secured target database will still create an audit trail (assuming auditing is enabled). The next time you restart the Audit Vault Agent, the audit data that had been accumulating since the Audit Vault Agent was stopped is retrieved.

You configure one Audit Vault Agent for each host and one or more audit trails for each individual secured target database. For example, if a host contains four databases, then you would configure one Audit Vault Agent for that host and one or more audit trails for each of the four databases. The number and type of audit trails that you configure depends on the secured target database type and the audit trails that you want to collect from it. See Table B–13 on page B-11 for information on the types of audit trails that can be configured for each secured target type.

You can create the Audit Vault Agent on one computer and manage multiple audit trails from there. For example, suppose you have 2 secured target databases on 2 servers. You must configure an audit trail for each of these secured target databases, but you do not need to configure an Audit Vault Agent on each of the 2 servers. Instead, just create one Audit Vault Agent to manage the 2 audit trails. Be aware, however, that for Oracle Databases, you cannot use a remote Audit Vault Agent to

collect audit data from users who have logged in with the SYSDBA or SYSOPER privilege because an audit trail is on to the local file system, and therefore you need file system access.

The Audit Vault Agent also contains Host Monitor capability, which enables AVDF to directly monitor SQL traffic in a database. This can be useful for monitoring many small databases centrally. See "Enabling and Using Host Monitoring" on page 7-1 for detailed information.

For information on deploying the Audit Vault Agent, see "Deploying and Activating the Audit Vault Agent on Host Computers" on page 5-2.

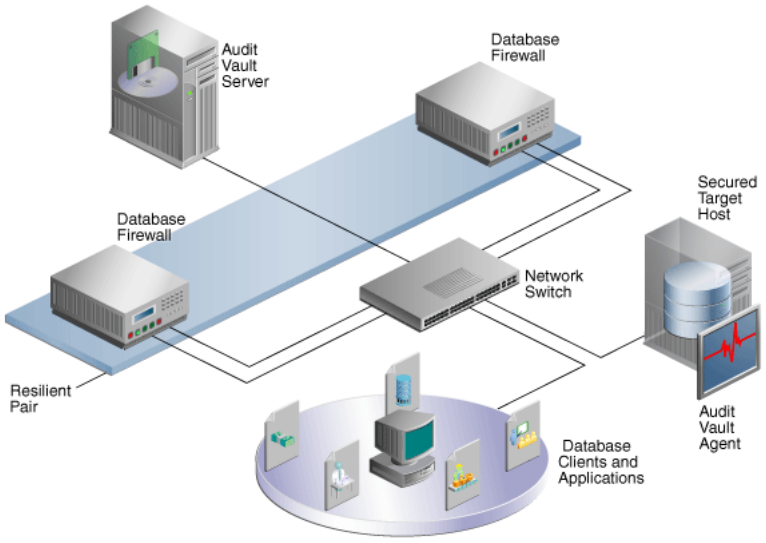
> **Note:** The Audit Vault Agent is supported on x86-64, x86-32, x64, and HP-UX Itanium platforms, and requires Java SE 6 or 7 on the host computer. See *Oracle Audit Vault and Database Firewall Installation Guide* for platform support details for the current release. For supported platforms in prior releases, see **Article 1536380.1** at the Oracle Support website: https://support.oracle.com

Placing Oracle AVDF Within Your Enterprise Architecture

When you deploy Oracle AVDF you set up the Audit Vault Server, then you can choose to deploy the Audit Vault Agent only, the Database Firewall only, or both.

Figure 1–2 shows Audit Vault and Database Firewall in an enterprise environment. This figure shows only one secured target for simplicity. A typical architecture will have many secured targets such as databases or nondatabase secured targets.

Figure 1–2 Oracle AVDF in the Enterprise Architecture



An Audit Vault Agent is deployed on the host computer of the secured target, which in this case, is a database that is also protected by the Database Firewall. The Database Firewall has two connections, one for management and one for monitoring database traffic. They are treated the same way in the switch.

Database Firewalls use different network ports (network devices, and therefore, network paths) to connect to the Audit Vault Server. The Network Switch in this diagram shows two port connections for each of the Database Firewalls.

The Database Firewall can connect to the database network in one of three ways:

- **Through a hub, tap or network switch configured with a "spanning port":** A spanning port is also known as a "mirror port" on some switches. This method sends a copy of all database traffic to the Database Firewall. This configuration enables a Database Firewall to operate as an out-of-band audit and monitoring system, and produce warnings of potential attacks, but it cannot block potentially harmful traffic.

  For more information about connecting hubs, taps or switches, see the following Web site:

  `http://www.sans.org/security-resources/idfaq/switched.php`

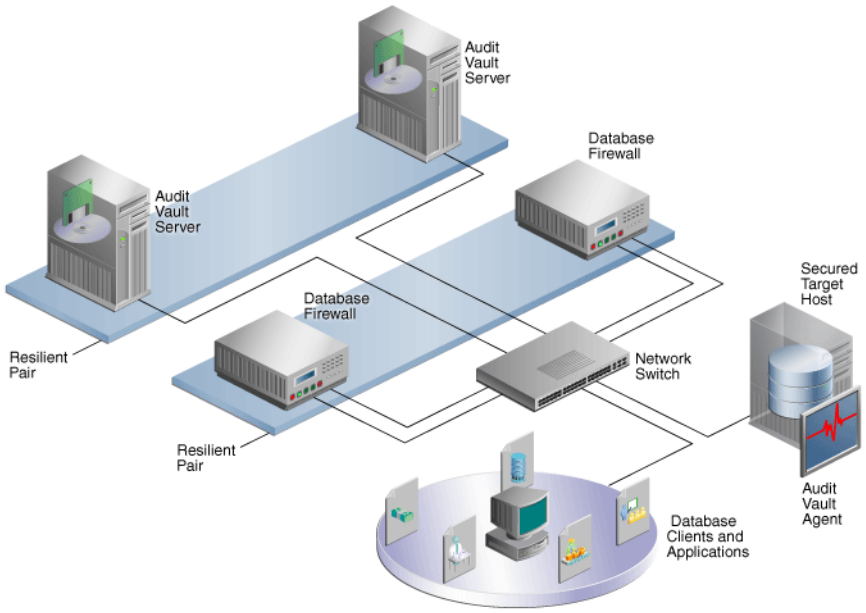
- **Inline between the database clients and database:** This method enables Database Firewall to both block potential attacks and/or operating as an audit or monitoring system.
- **As a proxy:** Using this method, the Database Firewall acts as a traffic proxy, and the database client applications connect to the database using the Database Firewall's proxy IP and port address.

High-Availability Modes

You can configure pairs of Database Firewalls or pairs of Audit Vault Servers, or both, to provide a high-availability system architecture. These pairs are known as **resilient pairs**. The resilient pair configuration works in Database Activity Monitoring (DAM) mode only. See "The Database Firewall" on page 1-6 for information on DAM mode.

Figure 1–3 shows a pair of Database Firewalls and a pair of Audit Vault Servers being used to protect a single database.

Figure 1–3 Audit Vault and Database Firewall High Availability



For details on configuring resilient pairs, see "Configuring High Availability" on page 8-1.

Understanding the Administrator's Role

Oracle AVDF Administrator Tasks

As an administrator, you configure Audit Vault and Database Firewall. The administrator's tasks include the following:

- Configuring system settings on the Audit Vault Server
- Configuring connections to the host computers where the Audit Vault Agent is deployed (usually the same computer as the secured targets)
- Creating secured targets in the Audit Vault Server for each database or operating system you are monitoring
- Deploying and activating the Audit Vault Agent on the secured target host computers
- Configuring audit trails for secured targets that are monitored by the Audit Vault Agent
- Configuring Database Firewalls on your network
- Creating enforcement points for secured targets that are monitored by a Database Firewall.
- Backing up and archiving audit and configuration data
- Creating administrator users and managing access (super administrator only)

Administrator Roles in Oracle AVDF

There are two administrator roles in Oracle AVDF, with different levels of access to secured targets:

- **Super Administrator** - This role can create other administrators or super administrators, has access to all secured targets, and grants access to specific secured targets and groups to an administrator.
- **Administrator** - Administrators can only see data for secured targets to which they have been granted access by a super administrator.

Summary of Configuration Steps

With Oracle AVDF, you can deploy the Audit Vault Agent, the Database Firewall or both. This section provides suggested high-level steps for configuring the Oracle AVDF system when you are:

- Configuring Oracle AVDF and Deploying the Audit Vault Agent
- Configuring Oracle AVDF and Deploying the Database Firewall

Configuring Oracle AVDF and Deploying the Audit Vault Agent

This is a general workflow for configuring Oracle AVDF and deploying the Audit Vault Agent:

1. Configure the Audit Vault Server. See "Configuring the Audit Vault Server" on page 3-1.
2. Register the host computers where you will deploy the Audit Vault Agent. Then deploy and activate the Audit Vault Agent on those hosts. See "Registering Hosts and Deploying the Agent" on page 5-1.

3. Create user accounts on your secured targets for Oracle AVDF to use. See "Scripts for Oracle AVDF Account Privileges on Secured Targets" on page B-12.
4. Register the secured targets you are monitoring with the agent in the Audit Vault Server, and configure audit trails for these secured targets. See "Configuring Secured Targets, Audit Trails, and Enforcement Points" on page 6-1.

After you have configured the system as an administrator, the Oracle AVDF auditor creates and provisions audit policies for Oracle Database secured targets, and generates various reports for other types of secured targets.

Configuring Oracle AVDF and Deploying the Database Firewall

This is a general workflow for configuring Oracle AVDF and deploying the Database Firewall:

1. Configure the Audit Vault Server, and associate each Database Firewall with this server. See "Configuring the Audit Vault Server" on page 3-1.
2. Configure the Database Firewall basic settings, and associate the firewall with the Audit Vault Server. Then configure the firewall on your network. See "Configuring the Database Firewall" on page 4-1.
3. Register the secured targets you are monitoring with the Database Firewall in the Audit Vault Server. Then configure enforcement points for these secured targets. Optionally, if you want to also monitor database response to SQL traffic, use the scripts and configuration steps to do so. See "Configuring Secured Targets, Audit Trails, and Enforcement Points" on page 6-1.

After you have configured the system as an administrator, the Oracle AVDF auditor creates firewall policies and assigns them to the secured targets. The auditor's role and tasks are described in *Oracle Audit Vault and Database Firewall Auditor's Guide*.

Planning the System Configuration

Topics

Questions to Help You Plan the Oracle AVDF Configuration

When planning the Oracle AVDF system configuration, you will need to think about the following questions:

- What types of targets do I need to secure? Your secured targets may be databases, operating systems, or other types of targets.

- To secure the types of targets I have, will I deploy the Audit Vault Agent, use Database Firewalls, or both?
- If I deploy the Audit Vault Agent, what types of audit trails do I need to collect? What audit settings do I need on my secured target?
- If I use Database Firewalls, how many do I need and where will they be on the network? Will they be inline, out of band (for example, using a span port), or configured as proxies?
- Do I need to configure the system for high availability?
- Who are the super administrators and administrators? For which secured targets should they have access?

The steps in this section provide information for your planning process.

Step 1: Plan the Audit Vault Server Configuration

In this step, plan whether to configure a resilient pair of servers, whether to change the network configuration settings made during the installation, and optional services configuration.

Starting in AVDF 12.1.2, due to additional space requirements for certain archive data transfer methods, configure archiving as part of the initial configuration of the Audit Vault Server.

For information on the Audit Vault Server configuration settings, see "Configuring the Audit Vault Server" on page 3-1.

For information on setting up resilient pairs of Audit Vault Servers, see "Configuring High Availability" on page 8-1.

Step 2: Plan the Database Firewall Configuration

If you are using Database Firewalls, plan how many you will need, which secured target databases they will protect, where to place them in the network, whether they will be in DAM (monitoring only) or DPE (monitoring and blocking) mode, and whether to configure a resilient pair of firewalls. Also plan whether to change the Database Firewall network configuration specified during installation.

For information on the Database Firewall configuration settings, see "Configuring the Database Firewall" on page 4-1.

For information on setting up resilient pairs of firewalls, see "Configuring High Availability" on page 8-1.

Step 3: Plan the Audit Vault Agent Deployments

If you are deploying the Audit Vault Agent(s), determine the secured targets for which you want to collect audit data, and identify their host computers. You will register these hosts with Oracle AVDF and deploy the Audit Vault Agent on each of them. Then you will register each secured target in the Audit Vault Server.

For more information, see:

- "Registering Hosts and Deploying the Agent" on page 5-1
- "Registering Secured Targets and Creating Groups" on page 6-2

Step 4: Plan the Audit Trail Configurations

If you are deploying the Audit Vault Agent to collect audit data, you will need to configure audit trails. This section provides guidelines for planning the audit trail configuration for the secured targets from which you want to extract audit data. The type of audit trail that you select depends on the secured target type, and in the case of an Oracle Database secured target, the type of auditing that you have enabled in the Oracle Database.

To plan the secured target audit trail configuration:

1. Ensure that auditing is enabled on the secured target.

   For an Oracle Database secured target, find the type of auditing that the Oracle Database uses. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for more information about the Oracle Database requirements.

2. Ensure that the agent is installed on the same computer as the secured target.

   For a Sybase ASE secured target, ensure that the Audit Vault Agent is installed on a computer in which SQL*Net can communicate with the Sybase ASE database.

   For more information, see "Deploying and Activating the Audit Vault Agent on Host Computers" on page 5-2.

3. Determine what type of audit trail to collect.

   Table B–13 on page B-11 lists the types of audit trails that can be configured for each secured target type and supported platforms.

4. Familiarize yourself with the procedures to register a secured target and configure an audit trail. See the following topics for details:

   - "Registering Secured Targets and Creating Groups" on page 6-2
   - "Configuring and Managing Audit Trail Collection" on page 6-7

5. If you are collecting audit data from MySQL or IBM DB2 secured targets, there are additional steps you need to take. See the following topics:

   - "(Required for MySQL) Running the XML Transformation Utility" on page 6-10
   - "(Required for IBM DB2) Converting Binary DB2 Audit Files to ASCII Format" on page 6-11

Step 5: Plan Integration Options

Oracle AVDF can be integrated with the following third party products:

- **BIG-IP Application Security Manager (ASM), from F5 Networks, Inc.** See "Configuring Integration with BIG-IP ASM" on page 9-1 for information on implementing this integration.
- **ArcSight Security Information Event Management (SIEM).** See "Configuring Integration with ArcSight SIEM" on page 10-1 for information on implementing this integration.

Step 6: Plan for High Availability

In this step, consider the high availability options outlined in "Configuring High Availability" on page 8-1.

Step 7: Plan User Accounts and Access Rights

As a super administrator, you can create other super administrators and administrators. Super administrators will be able to see and modify any secured target. Administrators will have access to the secured targets you allow them to access. In this planning step, determine how many super administrators and administrators you will create accounts for, and to which secured targets the administrators will have access.

For more information, see "Managing User Accounts and Access" on page 11-1.

Logging in to the Audit Vault Server Console UI

Topics

Logging in to the Audit Vault Server Console

When you first log in after installing the Audit Vault Server, you are required to set up a password. See *Oracle Audit Vault and Database Firewall Installation Guide* for information on post-installation tasks.

To log in to the Audit Vault Server console:

1. From a browser, enter the following URL:

   `https://host/`

   where *host* is the server where you installed Audit Vault Server.

   For example:

   `https://192.0.2.1/`

   If you see a message saying that there is a problem with the Web site security certificate, this could be due to a self-signed certificate. Click the **Continue to this website** (or similar) link.

2. In the Login page, enter your user name and password, and then click **Login**.

   The Dashboard page appears.

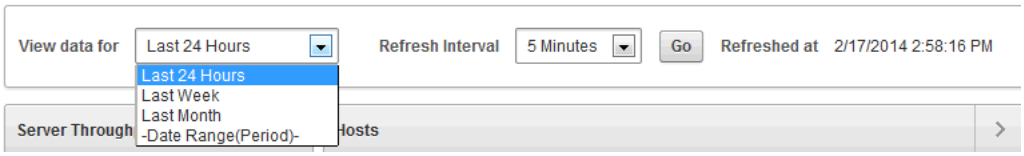
Understanding the Tabs and Menus in the Audit Vault Server Console

The Audit Vault Server console UI includes the following five tabs:

- **Home** - Displays a dashboard showing high level information and status for:
  - Server Throughput
  - Disks Usage
  - CPU
  - RAM
  - Hosts
  - Database Firewalls

At the top of the page, you can select the time range for the data displayed and the refresh interval, as shown in Figure 1–4.

Figure 1–4 Selecting the Time Range for the Dashboard in the Home Tab



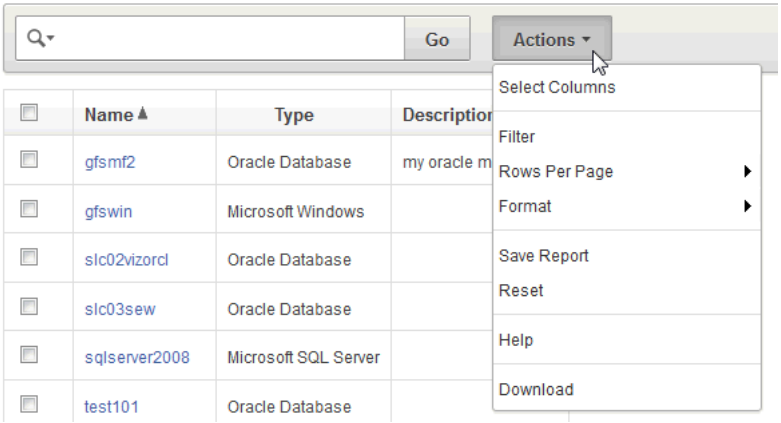
- **Secured Targets** - Provides menus for registering secured targets, managing secured target groups, managing access rights, and monitoring audit trails and enforcement points.
- **Firewalls** - Provides menus for registering Database Firewalls in the Audit Vault Server, and creating resilient pairs of firewalls for high availability.
- **Hosts** - Provides menus for registering and managing host computers (where the agent is deployed), and downloading and activating the Audit Vault Agent on those hosts.
- **Settings** - Provides menus for managing security, archiving, and system settings. From here, you can also download the AVCLI command line utility.

Working with Lists of Objects in the UI

Throughout the Audit Vault Server UI, you will see lists of objects such as users, secured targets, audit trails, enforcement points, etc. You can filter and customize any of these lists of objects in the same way as you can for Oracle AVDF reports. This section provides a summary of how you can create custom views of lists of objects. For more detailed information, see the Reports chapter of *Oracle Audit Vault and Database Firewall Auditor's Guide*.

To filter and control the display of lists of objects in the Audit Vault Server UI:

1. For any list (or report) in the UI, there is a search box and **Actions** menu:



2. To find an item in the list, enter its name in the search box, and then click **Go**.
3. To customize the list, from the **Actions** menu, select any of the following:
   - **Select Columns:** Select which columns to display.
   - **Filter:** Filter the list by column or by row using regular expressions with the available operators. When done, click **Apply**.

- **Rows Per Page: -** Select the number of rows to display per page.
- **Format:** Format the list by selecting from the following options:
  - **Sort**
  - **Control Break**
  - **Highlight**
  - **Compute**
  - **Aggregate**
  - **Chart**
  - **Group By**

  Fill in the criteria for each option as needed and click **Apply**.
- **Save Report:** Save the current view of the list. Enter a name and description and click **Apply**.
- **Reset:** Reset the list to the default view.
- **Help:** Display the online help.
- **Download:** Download the list. Select the download format (CSV or HTML) and click **Apply**.

Logging in to the Database Firewall Console UI

Topics

Logging in to the Database Firewall Console UI

When you first log in after installing the Database Firewall, you are required to set up a password. See *Oracle Audit Vault and Database Firewall Installation Guide* for information on post-installation tasks.

To log in to the Database Firewall Console UI:

1. From a browser, enter the following URL:

   `https://host/`

   where *host* is the server where you installed the Database Firewall.

   For example:

   `https://192.0.2.2/`

   If you see a message saying that there is a problem with the Web site security certificate, this could be due to a self-signed certificate. Click the **Continue to this website** (or similar) link.

2. In the Login page, enter your user name and password, and then click **Login**.

   The Dashboard page appears.

Using the Database Firewall UI

An administrator uses the Database Firewall UI to configure network, services, and system settings on the Database Firewall server, identify the Audit Vault Server that will be managing each firewall, and configure network traffic sources so that the firewall can monitor or block threats to your secured target databases.

See "Configuring the Database Firewall" on page 4-1 for detailed information on configuring the Database Firewall using the Database Firewall console UI.

Using the AVCLI Command Line Interface

You can download the AVCLI command line utility and use it, as an alternative to the Audit Vault Server console GUI, for configuring and managing Oracle AVDF.

For information on downloading and using AVCLI, see "Downloading and Using the AVCLI Command Line Interface" on page 12-7.

For details of available commands and syntax, see "AVCLI Commands Reference" on page A-1.

Using the AVDF Enterprise Manager Plug-in

If you have Oracle Enterprise Manager Cloud Control installed, you can install an Oracle AVDF plug-in to manage and monitor Oracle AVDF through the Enterprise Manager.

For more information see *Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Audit Vault and Database Firewall*.

2

General Security Guidelines

Topics

Installing Securely and Protecting Your Data

Topics

Installing Securely

The Audit Vault Server installs in a secure state by default. Therefore, it is important to be careful if changing default settings, as this may result in a less secure state. For details of the installation, see the *Oracle Audit Vault and Database Firewall Installation Guide*.

Protecting Your Data

Consider the following guidelines to protect your data:

- **Account Names and Passwords:** Use secure passwords for the Audit Vault Server console UI, `root`, `support`, and `sys` accounts and keep these passwords safe.
- **Administrator Accounts:** Oracle AVDF Administrator accounts should never be shared. This allows better auditing of administrator activity.
- **Strong Password Policies:** Create password policies to force users to use strong passwords.
- **Installed Accounts:** Oracle AVDF is installed with terminal (shell) access and embedded database accounts. You should avoid adding new accounts of this type or unlocking the existing ones, since these accounts can be used to tamper with the data or operation of the Oracle AVDF system.
- **Secure Archiving:** Since archive data is transferred over the network, ensure that the archive destination and network infrastructure are secure.

- **Remote Access:** Oracle AVDF allows you to set remote access permissions in the Services page of the Audit Vault Server console (**Settings** tab). Remote access can be granted for Web access to the console, shell (ssh), and SNMP. Follow these guidelines when granting remote access:
  - Grant access only if you need it for a specific task, and then revoke access when that task is completed.
  - Restrict access by IP address. Do this immediately after installing the system.
  - Grant terminal (shell) access only when doing a patch update, or when requested to do so in documentation or by Oracle support.

General Security Recommendations

Oracle recommends that you follow these security recommendations:

- If you are using the Database Firewall to block unwanted traffic, ensure that all data flowing from the database clients to the database and back, passes through the Database Firewall. This includes both requests and responses.
- Use the appropriate security measures for your site to control access to the computer that contains the Audit Vault Server and the Database Firewall appliances. Give access only to specific users.
- Ensure that passwords conform to best practice.
- Separate the duties of administrators and auditors by assigning these roles to different people.
- Assign users of the Audit Vault Server the appropriate administrator, super administrator, auditor, and super auditor roles.

Considerations for Deploying Network-Based Solutions

Topics

Handling Network Encryption

This section is relevant to the Database Firewall.

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

You can use SSL termination solutions to terminate the SQL traffic just before it reaches the Database Firewall.

Handling Server-Side SQL and Context Configurations

This section is relevant to the Database Firewall.

The Database Firewall policy enforcement relies on capturing and understanding SQL traffic between the database client and server. Because the Database Firewall only analyzes network traffic between the application tier and the database server, be aware

that it cannot see SQL that is directly invoked from the database server itself. Some of the common types of SQL statements that the Database Firewall cannot see are system-provided and user-defined SQL executed from stored procedures and callouts, SQL executed from background jobs such as those that were created by the `DBMS_JOB` or `DBMS_SCHEDULER` PL/SQL packages in Oracle databases, or SQL that is indirectly executed from DDLs or other SQL statements. You can use the auditing features in Oracle AVDF to capture these types of SQL statements.

The Database Firewall builds its execution context entirely from the information that it captures from the network traffic. However, enforcement may depend on context information on the server. The lack of this context affects how an identifier used in novelty policies is resolved.

How Oracle AVDF Works with Various Database Access Paths

Be aware of how Oracle AVDF works with the following types of database access paths:

- **Non-SQL protocol access**. Database platforms support different network protocols beyond the database SQL-based protocols. For example, Oracle Database supports HTTP, FTP, Advanced Queuing, Direct Path, and NFS access to the data stored in the database. The Database Firewall provides policy enforcement only for SQL-based access to the database. The protocols that the Database Firewall understands are Oracle TTC/Net and Tabular Data Stream (TDS) for Microsoft SQL Server, Sybase ASE, and IBM Distributed Relational Database Architecture (DRDA)
- **IPv6 Connections**. Oracle AVDF does not support IPv6 deployments. The Database Firewall automatically blocks all traffic coming from an IPv6 connection.
- **Non-TCP-based Connections**. The Database Firewall only supports TCP-based network connections to database servers. It cannot monitor connections made to database servers using non-TCP protocols such as Systems Network Architecture (SNA), Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

Security Considerations for Special Configurations

Topics

Handling an Oracle Shared Server Configuration and Dispatchers

This section is relevant to the Database Firewall.

A shared server architecture enables a database server to permit many user processes to share few server processes. The dispatcher process directs multiple incoming network session requests to a common queue, and then redirects these session requests to the next available process of the shared server. By default, Oracle Database creates one dispatcher service for the TCP protocol. In the `init.ora` file, this setting is controlled by the `DISPATCHERS` parameter, as follows:

```
dispatchers="(PROTOCOL=tcp)"
```

In the default configuration, a dynamic port listens to the incoming connection using the TCP protocol. With a shared server configuration, many user processes connect to a dispatcher on this dynamic port. If the Database Firewall is not configured to monitor the connections on this port, then the policy cannot be enforced on these connections. To facilitate the Database Firewall connection configuration, you should explicitly include the port number in the DISPATCHERS parameter. For example:

```
dispatchers="(PROTOCOL=tcp)(PORT=nnnn)"
```

Choose a value for *nnnn*, and configure the Database Firewall to protect that address, alongside the usual listener address.

See also *Oracle Database Administrator's Guide* for more information about managing shared servers. For more information about the `DISPATCHERS` parameter, see *Oracle Database Reference*.

How TCP Invited Nodes Are Affected by Client IP Addresses

When the Database Firewall is in Database Policy Enforcement (DPE) mode, the secured target database only recognizes the Database Firewall's IP address, which is the IP address assigned to the Database Firewall bridge (as described in "Configuring a Bridge in the Database Firewall" on page 4-6). It will no longer recognize the IP addresses of the protected database's clients, and as a result, users will be unable to connect to this database.

You can remedy this problem by including the Database Firewall Bridge IP address in the TTC/Net parameter `TCP.INVITED_NODES` setting in the `sqlnet.ora` file. The `TCP.INVITED_NODES` parameter specifies the nodes from which clients are allowed access to the database. When you deploy the Database Firewall, you should use the policy profiles feature to implement network access restrictions similar to those provided by `TCP.INVITED_NODES`. The policy profiles feature in the Database Firewall supports additional factors such as IP address sets, time of day, users, and so on. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for more information about profiles.

As described in this section, the client IP address seen by the database server is the address assigned to the bridge in the Database Firewall. This feature can affect functionality on the database server that depends on the original client IP address. Some of this functionality that can depend on the client IP address includes logon triggers, analysis of audit data, and Oracle Database Vault factors.

Additional Behavior to be Aware Of

- **Client-side context**. Database Firewall policies can be configured to use client-side context information such as client program name, client OS username, etc. After the client transmits this information to the database server, the Database Firewall captures it from the network. The Database Firewall does not control or enforce the integrity of the client side or network; the integrity of this information must be considered before using it to define a security policy.
- **Multiple databases and services on a shared listener**. The Database Firewall supports policies based on Oracle Database service names. For non-Oracle databases, the Database Firewall enforces policies that are based on the IP address and port number. In a configuration where a single listener endpoint (*`IP_address:port`*) is shared among multiple databases, the Database Firewall cannot differentiate traffic directed to each individual database.

3

Configuring the Audit Vault Server

Topics

About Configuring the Audit Vault Server

This chapter explains how to do the initial configuration of an Audit Vault Server.

> **CAUTION:** The Audit Vault Server and the Database Firewall server are software appliances. You must not make any changes to the Linux operating system through the command line on these servers unless following official Oracle documentation or under guidance from Oracle Support.

There are four main steps involved in the configuration process:

1. Perform the initial configuration tasks at the Audit Vault Server, for example, confirm system services and network settings, and set the date and time.
2. (Optional) Define resilient pairs of servers for high availability.
3. (Optional) Add each Database Firewall at the Audit Vault Server.
4. Check that the system is functioning correctly.

Each of these steps is described next.

To understand the high-level workflow for configuring the Oracle AVDF system, see "Summary of Configuration Steps" on page 1-9.

Note: If you plan to configure a resilient pair of Audit Vault Servers for a high availability configuration, do the initial configuration described in this chapter for both Audit Vault Servers in the pair.

See "Configuring a Resilient Pair of Audit Vault Servers" on page 8-3 for more information.

Logging In to the Audit Vault Server

For login instructions, see "Logging in to the Audit Vault Server Console UI" on page 1-13.

Specifying Initial System Settings and Options (Required)

Topics

Specifying the Server Date, Time, and Keyboard Settings

Super administrators can change the date, time, and keyboard settings in the Audit Vault Server. It is important to ensure that the date and time set for the Audit Vault Server are correct because events performed by the Server are logged with the date and time at which they occur. In addition, archiving occurs at specified intervals based on the Server time settings.

About Time Stamps

Audit Vault Server stores all data in UTC. Time stamps are displayed as follows:

- If you are accessing data interactively, for example using the Audit Vault Server UI or AVCLI command line, all time stamps are in your time zone. In the UI, the time zone is derived from the browser time zone. If using AVCLI, the time zone is derived from the "shell" time zone (usually set by the TZ environment variable).
- If you log in to the Audit Vault Server as `root` or `support`, time stamps are displayed in UTC, unless you change the TZ environment variable for that session.
- If you are looking at a PDF or XLS report or email generated by the system, time stamps displayed reflect the **Time Zone Offset** setting in the Audit Vault Server **Manage** page (see procedure below).

WARNING: Do not change the Audit Vault Server's database time zone or change the time zone through any configuration files. Doing so will cause serious problems in the Audit Vault Server.

- If you are looking at the Database Firewall UI, all time zones are displayed in UTC. See "Setting the Date and Time in the Database Firewall" on page 4-3 for more information.

To set the server date, time, and keyboard settings:

1. Log in to the Audit Vault Server console as a super administrator.

2. Click the **Settings** tab.
3. From the **System** menu, click **Manage**.
4. From the **Timezone Offset** drop-down list, select your local time in relation to Coordinated Universal Time (UTC).

   For example, **-5:00** is five hours behind UTC. You must select the correct setting to ensure that the time is set accurately during synchronization.
5. From the **Keyboard** drop-down list, select the keyboard setting.
6. In the **System Time** field, select **Manually Set** or **NTP Synchronization**.

   Selecting NTP Synchronization keeps the time synchronized with the average of the time recovered from the time servers specified in the **Server 1/2/3** fields.
7. If you selected **NTP Synchronization**, select **Enable NTP Time Synchronization** in order to start using the NTP Server time.

   If you do not enable time synchronization in this step, you can still enter NTP Server information in the steps below, and enable NTP synchronization later.
8. (Optional) Select **Synchronize Time After Save** if you want the time to be synchronized when you click **Save**.
9. In the **Server 1**, **Server 2**, and **Server 3** sections, use the default server addresses, or enter the IP addresses or names of your preferred time servers.

   If you specify a name, the DNS server specified in the System Services page is used for name resolution.

   Click **Test Server** to display the time from the server,

   Click **Apply Server** to update the Audit Vault Server time from this NTP server. The update will not take effect until you click **Save**.
10. Click **Save**.

To enable time synchronization, you may also need to specify the IP address of the default gateway and a DNS server, as described in "Setting or Changing the Audit Vault Server Network Configuration" on page 3-3, and "Configuring or Changing the Audit Vault Server Services" on page 3-4.

Specifying the Audit Vault Server System Settings

Topics

Setting or Changing the Audit Vault Server Network Configuration

The Oracle AVDF installer configures initial network settings for the Audit Vault Server during installation. You can change the network settings after installation.

For a list of default Audit Vault Server port numbers, see "Ports Used by Audit Vault and Database Firewall" on page D-1.

Note: If you change the Audit Vault Server network configuration, you must also do the following:

- Restart all audit trails.
- If you have configured a resilient pair of Database Firewalls, reconfigure the pair. See "Configuring a Resilient Pair of Database Firewalls" on page 8-6.
- If you change the Audit Vault Server's IP address, update this information in the Database Firewall. See "Specifying the Audit Vault Server Certificate and IP Address" on page 4-4.

To configure the Audit Vault Server network settings:

1. Log in to the Audit Vault Server console as an administrator or super administrator.
2. Click the **Settings** tab.
3. In the **System** menu, click **Network**.
4. Edit the following fields as necessary, then click **Save**.
   - **IP Address:** The IP address of the Audit Vault Server. An IP address was set during the installation of the Audit Vault Server; if you want to use a different address, you can change it now. The IP address is static and must be obtained from the network administrator. **Note:** Changing the IP address requires a reboot.

     The specified IP Address may need to be added to routing tables to enable traffic to go between the Audit Vault Server and Database Firewalls.
   - **Network Mask:** (Super Administrator Only) The subnet mask of the Audit Vault Server.
   - **Gateway:** (Super Administrator Only) The IP address of the default gateway (for example, to access the management interface from another subnet). The default gateway must be on the same subnet as the Audit Vault Server.
   - **Host Name:** Enter the host name for the Audit Vault Server. The host name must start with a letter, can contain a maximum number of 24 characters, and cannot contain spaces in the name.

     Note: Changing the host name requires a reboot. After you click **Save**, the system asks you to confirm if you want to reboot, or cancel. If you confirm, the system will reboot and the Audit Vault Server will be unavailable for a few minutes.
   - **Link properties:** Do not change the default setting unless your network has been configured not to use auto negotiation.

Configuring or Changing the Audit Vault Server Services

To configure the Audit Vault Server services:

1. Log in to the Audit Vault Server console as a super administrator.
2. In the **System** tab, from the **System** menu, click **Services**.
3. Complete the following fields as necessary, then click **Save**.

Caution: When allowing access to Oracle AVDF you must be careful to take proper precautions to maintain security. See "Protecting Your Data" on page 2-1 for a list of recommendations before completing this step.

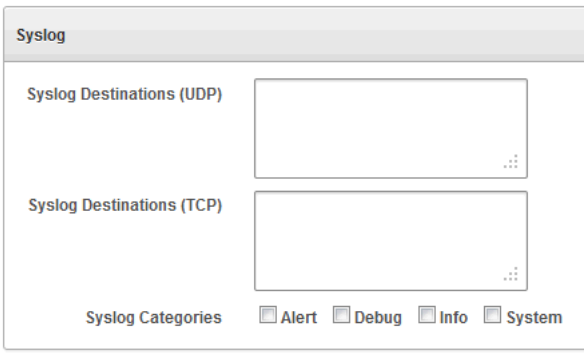
- **DNS Servers 1, 2, 3:** (Optional) Select **IP Address(es)** and enter the IP address(es) of up to three DNS servers on the network. These IP addresses are used to resolve any host names that may be used by Audit Vault Server. Keep the fields disabled if there is no DNS server, otherwise system performance may be impaired.
- **Web Access:** If you want to allow only selected computers to access the Audit Vault Server console, select **IP Address(es)** and enter specific IP addresses in the box, separated by spaces. Using the default of **All** allows access from any computer in your site.
- **SSH Access:** You can specify a list of IP addresses that are allowed to access Audit Vault Server from a remote console by selecting **IP Address(es)** and entering them in this field, separated by spaces. Using a value of **All** allows access from any computer in your site. Using a value of **Disabled** prevents console access from any computer.
- **SNMP Access:** You can specify a list of IP addresses that are allowed to access the network configuration of Audit Vault Server through SNMP by selecting **IP Address(es)** and entering them in this field, separated by spaces. Selecting **All** allows access from any computer. Selecting the default value of **Disabled** prevents SNMP access. The SNMP community string is `gT8@fq+E`.

Configuring the Audit Vault Server Syslog Destinations

Use the following procedure to configure the types of syslog messages to send from the Audit Vault Server. The message categories are Debug, Info, or System. Starting in Oracle AVDF 12.1.2, you can also forward Alert messages.

Caution: Ensure that the IP addresses you provide for Syslog destinations are on a different host than the Audit Vault Server.

1. Log in to the Audit Vault Server console as an administrator, and click the **Settings** tab.
2. From the **System** menu, click **Connectors**. and scroll down to the **Syslog** section.



3. Complete the fields, as necessary:

- **Syslog Destinations (UDP):** Use this box if you are using User Datagram Protocol (UDP) to communicate syslog messages from the Audit Vault Server. Enter the IP address of each machine that is permitted to receive the syslog messages, separated by spaces.
- **Syslog Destinations (TCP):** Use this box if you are using Transmission Control Protocol (TCP) to communicate syslog messages from the Audit Vault Server. Enter the IP address and port combinations of each server that is permitted to receive the syslog messages, separated by spaces.
- **Syslog Categories:** You can select the types of syslog messages to generate as follows:
  - **Alert:** (AVDF 12.1.2 Only) Alerts based on alert conditions that an AVDF auditor specifies.

    To forward AVDF alerts to syslog, in addition to this setting, the AVDF auditor must configure alert forwarding. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed instructions and AVDF syslog alert format.
  - **Debug:** Engineering debug messages (for Oracle support use only).
  - **Info:** General Oracle AVDF messages and property changes (Oracle AVDF syslog message IDs 1, 4 and 8).
  - **System:** System messages generated by Oracle AVDF or other software that have a syslog priority level of at least "INFO".

4. Click **Save**.

If you are using two Audit Vault Servers as a resilient pair, repeat "Specifying Initial System Settings and Options (Required)" on page 3-2 for the second Audit Vault Server.

Configuring the Email Notification Service

Topics

About Email Notifications in Oracle AVDF

An auditor can configure Oracle AVDF to send users email notifications when alerts or reports are generated. An administrator must configure an SMTP server in order to enable email notifications. The email notifications can be sent in text format to mobile devices, or routed through an SMS gateway if you already have one.

Note the following:

- You can configure one SMTP (or ESMTP) server for each Oracle AVDF installation.
- You can configure Oracle AVDF to work with both unsecured SMTP servers as well as secured and authenticated SMTP servers.

See *Oracle Audit Vault and Database Firewall Auditor's Guide* for information on configuring alerts and generating reports.

Configuring the Email Notification Service

To configure the email notification service:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and in the **System** menu, click **Connectors**.
3. In the **SMTP Server Address** field, enter the IP address of the SMTP server.
4. In the **SMTP Port** field, enter the SMTP server port.
5. In the **From Username** field, enter the user name used as the sender of the email.
6. In the **From Address** field, enter the sender's address that appears in the email notifications.
7. If this SMTP server requires it, select **Require Credentials**, then supply a **Username**, **Password**, and **Re-enter Password**.
8. If this SMTP server requires authentication, select **Require Secure Connection**, and then select the authentication protocol (SSL or TLS).

Configuring Archive Locations and Retention Policies

Topics

About Archiving and Restoring Data in Oracle AVDF

You can archive data files in Oracle AVDF as part of your information life cycle strategy. To do so, you must create archiving (or retention) policies, and configure archive locations to which data will be transferred according to the policies. We recommend that you archive regularly in accordance with your corporate policy. If required, you can create different data file archives for each secured target.

Note: As of Oracle AVDF 12.1.2, there are additional space requirements for archiving if you use Secure Copy (scp) or Windows File Sharing (SMB) transfer methods. Therefore, configure archiving as part of the initial Audit Vault Server configuration if you use these methods to transfer data to archive locations.

You can create many data archiving policies, each specifying the number of months to retain audit data online in Oracle AVDF, and how many months to retain data in the archives before purging. The Oracle AVDF auditor can then select a specific retention policy for each secured target, as well as for scheduled reports. If the auditor does not select a retention policy for a secured target or scheduled report, the default retention policy will be used (12 months retention online and 12 months in archives before purging).

You start archive jobs by selecting data files from those that are ready for archiving according to specified retention policies. Retention times are based on the time that the audit events occurred in the secured target.

Once data files become ready for archiving, the data is no longer visible in reports. When the administrator archives these data files, the data is physically removed from the Audit Vault Server. Data in the archive location can be restored to the Audit Vault Server if necessary, and this data then becomes visible in reports. It is up to the

administrator to manually purge data from the archive locations according to the retention policy.

You can restore data for a specific secured target and time range. For archive and restore procedures, see "Archiving and Restoring Audit Data" on page 12-3.

Defining Archiving Locations

You must define one or more locations as destinations for archive files before you can start an archive job. An archiving destination specifies the archive storage locations and other settings.

Oracle recommends that you use NFS to transfer data to an archive location. If you use Secure Copy (SCP) or Windows File Sharing (SMB) to transfer data to an archive location, then your data files are first copied to a staging area in the Audit Vault Server. Therefore, you must ensure that there is additional space in the file system. Otherwise the data file copying may fail. Be aware that transferring large files using SCP or SMB may take a long time.

To create an archive location:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and under **Archiving**, click **Manage Archive Locations**.

   A list of existing archive locations is displayed.
3. Click the **Create** button, and complete the following fields:
   - **Transfer Method:** The method used to transfer data from the Audit Vault Server to the machine that archives the data:
     - **Secure Copy (scp):** Select if the data is archived by a Linux machine.
     - **Windows File Sharing (SMB):** Select if the data is archived by a Windows machine
     - **Network File Storage (NFS)**: (AVDF 12.1.2 Only) Select if using a network file share or NAS.
   - **Location Name:** The name of the archiving destination. This name is used to select the archiving destination when starting an archive.
   - **Remote Filesystem:** (AVDF 12.1.2 Only) If you use the Network File System (NFS) transfer method, you can select an existing filesystem, or one will be created automatically based on the details of this archive location.

     You can register a remote filesystem using the `AVCLI` utility, so that the filesystem can be selected here. See "REGISTER REMOTE FILESYSTEM" on page A-42 for details.
   - **Address:** The name or IP address of the machine that archives the data. If **Windows File Sharing** is the transfer method, specify an IP address.
   - **Export Directory:** (AVDF 12.1.2 Only) If you use the Network File System (NFS) transfer method, enter the NFS server's export directory, for example, `/export_dir`.
   - **Path:** The path to the archive storage location. Enter a path to a directory (not a file), noting the following for these transfer methods:
     - **Secure Copy (scp):** If there is no leading slash character, the path is relative to the user's home directory. If there is a leading slash, the path is relative to the `root` directory.

  - **Windows File Sharing (SMB):** Enter the sharename, followed by a forward slash and the name of the folder (for example, `/sharename/myfolder`).
  - **Network File System (NFS):** (AVDF 12.1.2 Only) Enter the path relative to the export directory. For example if the export directory is `/export_dir`, and the full path to the directory you want to designate as an archive location is `/export_dir/dir1/dir2`, then enter `/dir1/dir2` in the **Path** field. If you want to put archives directly in the NFS server's export directory, then enter `/` (forward slash) for the **Path**.

    You can click the **Test** button to validate the NFS location when done.

- **Port:** This is the port number used by the secure copy or Windows fileshare service on the machine that archives the data. You can normally use the default port number.

  If you selected **Windows File Sharing** as the Transfer Method, it is recommended you use port 445.
- **Username:** The account name on the machine to which the archive data will be transferred.
- **Authentication Method:** If Secure Copy (scp) is the transfer method, you can select **Password** and enter the login password. If a Linux machine is used, you can select **Key Authentication**.

  If using Key Authentication, the administrator of the remote machine must ensure that the file that contains the RSA key (~/.ssh/authorized_keys) has permissions set to 664.
- **Password and Confirm Password:** If you use Windows file sharing, or you selected Password as the authentication method, this is the password to log into the machine that archives the data.
- **Public Key:** This field appears if you selected Key Authentication. Copy this public key and add it to the public keys file on the machine that archives the data. For example, add the key in `~/.ssh/authorized_keys`.

4. Click **Save**.

Creating or Deleting Archiving Policies

Topics

Creating Archiving (Retention) Policies

After you create a retention policy, an Oracle AVDF auditor can apply it to secured targets. For detailed instructions, see *Oracle Audit Vault and Database Firewall Auditor's Guide*.

To create an archiving (retention) policy:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. Under **Archiving**, select **Manage Policies**, and then click the **Create** button.
4. Enter a **Name** for this policy.

5. In the **Months Online** field, enter the number of months to retain audit data in the Audit Vault Server before it is marked for archiving. The default value is 1.

   For example, if you enter 2, then audit data for secured targets that use this retention policy will be available for archive jobs after two months online in the Audit Vault Server. After the months online period has expired, the data is no longer visible in reports.

6. In the **Months Archived** field, enter the number of months to retain audit data in the archive location. The default value is 6.

   This value determines how long data is available to restore to the Audit Vault Server, but does not cause the data to be purged from the archive location. For example if you enter 4, data can be restored from archives for a period of four months after it has been archived.

Deleting Archiving Policies

You can only delete a user-defined archiving policy.

To delete an archiving (retention) policy:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. Under **Archiving**, click **Manage Policies**.
4. Select the user-defined policy you want to delete, and then click **Delete**.

Defining Resilient Pairs for High Availability

You can define resilient pairs of Audit Vault Servers, Database Firewalls, or both. For these procedures, see "Configuring High Availability" on page 8-1.

When you define a resilient pair of Audit Vault Servers, you do all configuration tasks, such as adding Database Firewalls to the server and registering secured targets, on the primary Audit Vault Server.

Registering a Database Firewall in the Audit Vault Server

If you are deploying Database Firewalls, you must register each one in the Audit Vault Server in order to enable communication between the two. We suggest you first configure the Database Firewall using the instructions in "Configuring the Database Firewall" on page 4-1.

Database Firewalls must be registered in the Audit Vault Server before you can pair them for high availability. See "Configuring a Resilient Pair of Database Firewalls" on page 8-6 for more information.

To register a Database Firewall in the Audit Vault Server:

1. If you have not done so, provide the Audit Vault Server's certificate and IP address to the Database Firewall you are registering. See "Specifying the Audit Vault Server Certificate and IP Address" on page 4-4.
2. Log in to the Audit Vault Server as an administrator.

   If there is a resilient pair of Audit Vault Servers, log in to the primary server.
3. Click the **Firewalls** tab.

   The Firewalls page displays the currently registered firewalls and their status.

4. Click **Register**.
5. Enter a **Name** for the Database Firewall, and its **IP Address**.
6. Click **Save**.

   If there is a message that indicates that there is a problem with the certificate, check that the date and time are set consistently across both the Database Firewall and the Audit Vault Server.

Testing the Audit Vault Server System Operation

You should verify that the system is fully operational before commencing normal day-to-day operations.

To test the system operation:

1. Log in to the Audit Vault Server as an administrator.
2. Check the date and time of the Audit Vault Server
3. Click the **Settings** tab.
4. In the **System** menu, click **Status**.
5. Click the **Test Diagnostics** button to run a series of diagnostic tests and see the results.

   These diagnostics include testing:

   - Existence and access permissions of configuration files
   - File system sanity
   - Network configuration
   - Status of various process that are required to run on the system, for example, database server process(es), event collection process, Java framework process, HTTP server process, etc.
6. Click the **Home** tab, and check the status of **Database Firewalls** and **Hosts**.

4

Configuring the Database Firewall

This chapter explains how to configure the Database Firewall on the network and how to configure traffic sources, bridges, and proxies.

Topics

About Configuring the Database Firewall

Configuring each Database Firewall's system and network settings depends on your overall plan for deploying Oracle Audit Vault and Database Firewall. See "Planning the System Configuration" on page 1-10 for an overview of the planning steps.

When you configure each firewall, you identify the Audit Vault Server that will manage that firewall. Depending on your plan for the overall Oracle AVDF system configuration, you also configure the firewall's traffic sources, and determine whether it will be inline or out of band with network traffic, and whether you will use it as a proxy.

> **CAUTION:** The Audit Vault Server and the Database Firewall server are software appliances. You must not make any changes to the Linux operating system through the command line on these servers unless following official Oracle documentation or under guidance from Oracle Support.

Basic firewall configuration consists of these four steps:

1. Configuring the Database Firewall's Network and Services Configuration
2. Setting the Date and Time in the Database Firewall
3. Specifying the Audit Vault Server Certificate and IP Address
4. Configuring Database Firewalls on Your Network

After you have configured the Database Firewalls, you configure enforcement points for each database secured target that the firewall is protecting. See "Configuring Enforcement Points" on page 6-13 for details on these procedures.

You can optionally set up resilient pairs of Database Firewalls for a high availability environment. See "Configuring High Availability" on page 8-1 for details.

To understand the high-level workflow for configuring the Oracle AVDF system, see "Summary of Configuration Steps" on page 1-9.

Logging in to the Database Firewall

For information on how to log in, see "Logging in to the Database Firewall Console UI" on page 1-15. When you first log in, you are required to set up a password.

Configuring the Database Firewall's Network and Services Configuration

Topics

Configuring a Database Firewall's Network Settings

The installer configures initial network settings for the Database Firewall during installation. You can change the network settings after installation.

To change the Database Firewall network settings:

1. Log in to the Database Firewall administration console.
2. In the **System** menu, select **Network**.
3. In the Network Configuration page, click the **Change** button.
4. In the Management Interface section, complete the following fields as necessary, then click **Save**.
   - **IP Address:** The IP address of the currently accessed Database Firewall. An IP address was set during installation. If you want to use a different address, then you can change it here. The IP address is static and must be obtained from the network administrator.
   - **Network Mask:** The subnet mask of the Database Firewall.
   - **Gateway:** The IP address of the default gateway (for example, for internet access). The default gateway must be on the same subnet as the host.
   - **Name:** Enter a descriptive name for this Database Firewall. The name must be alphanumeric with no spaces.
   - **Link properties:** Do not change the default setting unless your network has been configured not to use auto negotiation.

Configuring a Database Firewall's Network Services

The network services configuration determines how users can access the Database Firewall. See the guidelines in "Protecting Your Data" on page 2-1 to ensure that you take the appropriate security measures when configuring network services.

To configure a Database Firewall's network services:

1. Log in to the Database Firewall administration console.
2. In the **System** menu, select **Services**.
3. Click the **Change** button, and in the Configure Network Services page, edit the following as necessary:
   - **DNS Servers 1, 2, and 3:** If you require hostnames to be translated, you must enter the IP address of at least one DNS server on the network. You can enter IP addresses for up to three DNS servers. Keep the fields blank if there is no DNS server, otherwise system performance may be impaired.
   - **Web Access:** If you want to allow selected computers to have Web access to the Database Firewall administration console, enter their IP addresses separated by spaces. Entering **all** allows access from any computer in your site.
   - **SSH Access:** If you want to allow selected computers to have secure shell access to the Database Firewall, enter their IP addresses separated by spaces. Enter **disabled** to block all SSH access. Enter **all** to allow unrestricted access.
   - **SNMP Access:** If you want to allow access to the network configuration of the Database Firewall through SNMP, enter a list of IP addresses that are allowed to do so, separated by spaces. Enter **disabled** to restrict all SNMP access. Enter **all** to allow unrestricted access. The SNMP community string is `gT8@fq+E`.
4. Click **Save**.

Setting the Date and Time in the Database Firewall

To set the Database Firewall date and time:

1. Log in to the Database Firewall administration console.
2. Click **Date and Time** from the **System** menu on the left, and then scroll down and click the **Change** button.
3. Enter the correct date and time in Coordinated Universal Time (UTC).
4. (Optional) Select **Enable NTP Synchronization**.

   Selecting Enable NTP Synchronization keeps the time synchronized with the average of the time recovered from the time servers specified in the **Server 1**, **Server 2**, and **Server 3** fields, which can contain an IP address or name. If a name is specified, the DNS server specified in the System Settings page is used for name resolution.

   To enable time synchronization, you also must specify the IP address of the default gateway and a DNS server, as described in "Configuring the Database Firewall's Network and Services Configuration" on page 4-2.
5. (Optional) Use the default NTP server addresses in the three **Server** fields, or enter the addresses of your preferred time servers.

   Note: If using host names instead of IP addresses, you must have DNS already configured, otherwise name resolution will not work. See "Configuring a Database Firewall's Network Services" on page 4-2.

   Test Server displays the time from the server, but does not update the time.

Selecting **Synchronize Time After Save** causes the time to be synchronized with the time servers when you click **Save**.

> **WARNING:** **In DPE (blocking) mode, Synchronize Time After Save causes all enforcement points to restart, thereby dropping existing connections to protected databases. This would cause a temporary traffic disruption.**

6. Click **Save**.

Specifying the Audit Vault Server Certificate and IP Address

You must associate each Database Firewall with an Audit Vault Server by specifying the server's certificate and IP address, so that the Audit Vault Server can manage the firewall. If you are using a resilient pair of Audit Vault Servers for high availability, you must associate the firewall to both servers.

Note: You must specify the Audit Vault Server certificate and IP address to the Database Firewall (by following the procedure below) before you register the firewall in the Audit Vault Server.

To specify the Audit Vault Server certificate and IP address:

1. Log in to the Audit Vault Server as an administrator, and then click the **Settings** tab.
2. In the **Security** menu, click **Certificate**.

   The server's certificate is displayed.
3. Copy the server's certificate.
4. Log in to the Database Firewall administration console.
5. In the **System** menu, click **Audit Vault Server**.
6. Enter the **IP Address** of the Audit Vault Server.
7. Paste the Audit Vault Server's **Certificate** in the next field.
8. If you are using a resilient pair of Audit Vault Servers, select the **Add Second Audit Vault Server** check box, and enter the IP address and certificate of the secondary Audit Vault Server.

   > **Tip:** The secondary Audit Vault Server does not have a console UI. However, you can get the secondary server's certificate from the primary server: click the **Settings** tab, then **High Availability** from the **System** menu. The secondary server's certificate is in the **Peer System Certificate** field.

9. Click **Apply**.

> **Important:** To complete the association of the Database Firewall to the Audit Vault Server, you must register each firewall in the Audit Vault Server console. See "Registering a Database Firewall in the Audit Vault Server" on page 3-10.

Configuring Database Firewalls on Your Network

Topics

About Configuring the Database Firewalls on Your Network

During your planning of the network configuration, you decide whether to place Database Firewalls inline with traffic to your secured target databases, or out of band (for example, using a spanning or mirror port). You may also decide to use a firewall as a traffic proxy. The network configuration is impacted by whether the Database Firewall will operate in DAM (monitoring only) or DPE (blocking) mode. See "The Database Firewall" on page 1-6 for information on these modes.

Using the Database Firewall administration console, you configure each firewall's traffic sources, specifying whether the sources are inline with network traffic, and whether the firewall can act as a proxy.

You will use a firewall's traffic and proxy sources to configure enforcement points for each secured target database you are monitoring with that firewall. See "Configuring Enforcement Points" on page 6-13 for details.

Configuring Traffic Sources

Traffic sources specify the IP address and network interface details for the traffic going through a Database Firewall. Traffic sources are automatically configured during the installation process, and you can change their configuration details later.

To change the configuration of traffic sources:

1. Log in to the Database Firewall administration console.
2. In the **System** menu, click **Network**.

   Current network settings are displayed including the Database Firewall's network settings, proxy ports, traffic sources, network interfaces, and any enabled bridges.
3. Click the **Change** button.
4. Scroll to the **Traffic Sources** section and change the following as necessary:
   - To remove the traffic source, click the **Remove** button next to the traffic source name.
   - Edit the **IP address** or **Network Mask** fields as necessary.
   - To enable or disable a bridge, check or uncheck the **Bridge Enabled** box. You can only enable a bridge if the traffic source has two network interfaces in the Devices area. See "Configuring a Bridge in the Database Firewall" on page 4-6.
   - To remove a network interface (i.e., network card) from the traffic source, in the Devices area, click the **Remove** button for a device.
   - To add a network interface to a traffic source, scroll to the **Unallocated Network Devices** section, and from the **Traffic Source** drop-down list, select the name of the traffic source to which you want to add this device.

5. Click **Save**.

Configuring a Bridge in the Database Firewall

The Database Firewall must be inline with network traffic (or configured as a proxy) if used in blocking (DPE) mode to block potential SQL attacks. If the Database Firewall is not in proxy mode, then you must allocate an additional IP address that is unique to the database network, to enable a bridge. The bridge IP address is used to redirect traffic within the Database Firewall. When the Database Firewall is used as a proxy, you do not need to allocate this additional IP address. See "Configuring a Database Firewall as a Traffic Proxy" on page 4-6 for details.

To enable a traffic source as a bridge, that traffic source must have two network interfaces. These network interface ports must connect the Database Firewall in-line between the database and its clients (whether Database Policy Enforcement or Database Activity Monitoring mode is used).

Note:

- The IP address of the bridge must be on the same subnet as all protected databases deployed in DPE mode on that bridge. This restriction does not apply to protected databases deployed in DAM mode.
- If the Database Firewall's management interface (specified in the console's **Network** page) and the bridge are connected to physically separate networks that are on the same subnet, the Database Firewall may route responses out of the wrong interface. If physically separate networks are required, use different subnets.

To configure the Database Firewall bridge IP address:

1. Log in to the Database Firewall administration console.
2. In the **System** menu, click **Network**, and then click the **Change** button.
3. In the Traffic Sources section, find the traffic source that you want to configure as a bridge.

   This traffic source must have two network interfaces. You can add an interface if necessary from the Unallocated Network Interfaces section of the page. See "Configuring Traffic Sources" on page 4-5.
4. Select **Bridge Enabled** for this traffic source.
5. If necessary, edit the **IP address** or **Network Mask**.

   The bridge IP address is used to redirect traffic within the Database Firewall.
6. Click **Save**.

Configuring a Database Firewall as a Traffic Proxy

Depending on your network configuration, you may prefer to configure a traffic proxy in the Database Firewall instead of a bridge inline with network traffic. You can then associate the proxy with an enforcement point. You can also specify multiple ports for a proxy in order to use them for different enforcement points. See "Configuring Enforcement Points" on page 6-13 for more information.

Once you set up the Database Firewall as a traffic proxy, your database clients connect to the database using the Database Firewall proxy IP and port.

To configure a traffic proxy:

1. Ensure that the IP address of the proxy interface is on the same subnet as the secured target.
2. Log in to the administration console of the Database Firewall that is acting as a proxy.
3. In the **System** menu, click **Network**, then click the **Change** button.
4. In the Unallocated Network Interfaces section of the page, find an available network interface, and select **Traffic Proxy** in Traffic Source drop-down list.

   To free up additional network interfaces, you can remove them from an existing traffic source or traffic proxy by clicking the **Remove** button for the network interface(s) you want to free up.
5. Click **Add**.

   The new traffic proxy appears under the Traffic Proxies area of the page.
6. Under the new proxy, select **Enabled**.
7. In the Proxy Ports section for the new proxy, enter a **Port** number, and then click **Add**.

   You can specify more than one port per proxy by entering another port number and clicking **Add**.
8. Check **Enabled** next to the port number(s).
9. Click **Save**.

   The traffic proxy is now available to use in an Enforcement Point. See "Configuring Enforcement Points" on page 6-13.

Viewing the Status and Diagnostics Report for a Database Firewall

To view the status and/or diagnostic report for a Database Firewall:

1. Log in to the Database Firewall administration console.

   The Status page is displayed by default.
2. If necessary, in the **System** menu, click **Status**.

   The Status page displays system status, component versions, grammar pack versions, free space, and diagnostic status.

   Text next to **Diagnostic Status** indicates `OK` or `Errors`.
3. Next to the **Diagnostic Status** field, you can click:
   - **Show Report** to see an overview of diagnostic status.
   - **Download Diagnostics** to download all diagnostics files.

5

Registering Hosts and Deploying the Agent

Topics

Registering Hosts in the Audit Vault Server

Topics

About Registering Hosts

If you want to collect audit data from a secured target, you must configure a connection between the Audit Vault Server and the host machine where the Audit Vault Agent resides for that secured target (usually the same computer as the secured target).

After registering a host, you must then deploy and activate the Audit Vault Agent on that host. See "Deploying and Activating the Audit Vault Agent on Host Computers" on page 5-2.

This chapter assumes the Audit Vault Agent is deployed on the secured target host, and describes the procedures for registering hosts using the Audit Vault Server console UI. For information on using the command line interface, see "Using the AVCLI Command Line Interface" on page 1-16.

After you register hosts and deploy the Audit Vault Agent on them, in order to start audit trail collections you must also register the secured targets, configure audit trails, and start audit trail collections manually. These procedures are described in:

- "Registering Secured Targets" on page 6-2
- "Configuring and Managing Audit Trail Collection" on page 6-7

To understand the high-level workflow for configuring the Oracle AVDF system, see "Summary of Configuration Steps" on page 1-9.

Registering Hosts in the Audit Vault Server

Sections in this chapter give information on configuring hosts that is specific to each secured target type. However, the procedure for registering any host machine in the Audit Vault Server is the same.

To register a host machine in the Audit Vault Server:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Hosts** tab.

   A list of the registered hosts, if present, appears in the Hosts page. To control the view of this list see "Working with Lists of Objects in the UI" on page 1-14.
3. Click **Register**.
4. Enter the **Host Name** and **Host IP** address.
5. Click **Save**.

   If you are using Oracle AVDF version 12.1.2, an Agent Activation Key is automatically generated when you register the host.

   See Also: "REGISTER HOST" on page A-2 for the command line syntax to register a host

Changing Host Names

Changing the name of a registered host can take up to 10 minutes because the system automatically reboots after you change the name.

Caution: Do not manually reboot the system after changing a host name as this may put the system in an inconsistent state. Wait up to 10 minutes for the system to automatically reboot.

To change the name of a registered host:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Hosts** tab.
3. Click the name of the host you want to change.
4. In the Modify Host page, change the **Host Name** field, and then click **Save**.
5. Wait for the system to automatically reboot.

   This may take up to 10 minutes. Do not manually reboot the system.

Deploying and Activating the Audit Vault Agent on Host Computers

Topics

About Deploying the Audit Vault Agent

In order to collect audit trails from secured targets, you must deploy the Audit Vault Agent on a host computer, usually the same computer where the secured target resides. The Audit Vault Agent includes plug-ins for each secured target type, as well as host monitoring functionality.

In addition to deploying the Audit Vault Agent, in order to start audit trail collections you must also register each host, register secured targets, configure audit trails, and start audit trail collections manually. For these procedures, see:

- "Registering Hosts in the Audit Vault Server" on page 5-1
- "Registering Secured Targets and Creating Groups" on page 6-2
- "Configuring and Managing Audit Trail Collection" on page 6-7

To understand the high-level workflow for configuring the Oracle AVDF system, see "Summary of Configuration Steps" on page 1-9.

Steps Required to Deploy and Activate the Audit Vault Agent

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

1. Registering the Host
2. Deploying the Audit Vault Agent on the Host Computer.
3. (Oracle AVDF 12.1.1 Only) Requesting Agent Activation
4. Activating and Starting the Audit Vault Agent.

Registering the Host

To register the host on which you deployed the Audit Vault Agent, follow the procedure in "Registering Hosts in the Audit Vault Server" on page 5-1.(

Deploying the Audit Vault Agent on the Host Computer

You must use an OS user account to deploy the Audit Vault Agent. In this step, you copy the `agent.jar` file from the Audit Vault Server and deploy this file on the host machine.

> **Note:** The Audit Vault Agent is supported on Unix, Windows, and HP-UX Itanium platforms, and requires Java SE 6 or 7 on the host computer. See *Oracle Audit Vault and Database Firewall Installation Guide* for platform support details for the current release. For supported platforms in prior releases, see **Article 1536380.1** at the Oracle Support website: `https://support.oracle.com`

To copy and deploy the Audit Vault Agent to the host machine:

1. Log in to the Audit Vault Server console as an administrator.

2. Click the **Hosts** tab, and then from the **Hosts** menu, click **Agent**.

   The Agent and host monitor files are listed.

3. Click the **Download** button next to the Agent file, and then save the `agent.jar` file to a location of your choice.

4. Using an OS user account, copy the `agent.jar` file to the secured target's host computer.

5. On the host machine, set `JAVA_HOME` to the installation directory of the `jdk1.6` (or higher version), and make sure the `java` executable corresponds to this `JAVA_HOME` setting.

   Note: For a Sybase ASE secured target, ensure that the Audit Vault Agent is installed on a computer in which SQL*Net can communicate with the Sybase ASE database.

6. Start a command prompt with **Run as Administrator**.

7. In the directory where you placed the `agent.jar` file, extract it by running:

   ```
   java -jar agent.jar -d Agent_Home
   ```

   This creates a directory by the name you enter for *Agent_Home*, and installs the Audit Vault Agent in that directory.

   On a Windows system, this command automatically registers a windows service named `OracleAVAgent`.

   Caution: After deploying the Audit Vault Agent, do not delete the *Agent_Home* directory unless directed to do so by Oracle Support. If you are updating an existing Audit Vault Agent, do not delete the existing *Agent_Home* directory.

(Oracle AVDF 12.1.1 Only) Requesting Agent Activation

This step is not required for Oracle AVDF 12.1.2.

Prerequisite: Follow the procedure in "Registering Hosts in the Audit Vault Server" on page 5-2 for this host computer.

To request activation of the Audit Vault Agent in version 12.1.1:

1. On the host computer, go to the following directory:

   Agent_Home`/bin`

   Agent_Home is the directory created in the step 7 above.

2. Run the following command:

   ```
   agentctl activate
   ```

   This sends an activation request to the Audit Vault Server.

Activating and Starting the Audit Vault Agent

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

Prerequisites:

- Follow the procedure in "Registering Hosts in the Audit Vault Server" on page 5-1.

- (Oracle AVDF 12.1.1 Only) Follow the procedure in "(Oracle AVDF 12.1.1 Only) Requesting Agent Activation" on page 5-4.

To activate and start the agent:

1. Log in to the Audit Vault Server console as an administrator, and click the **Hosts** tab.
2. **Oracle AVDF 12.1.1 Only:** Select the host you want to activate, and then click **Activate**.

   This will generate an activation key under the Agent Activation Key column.

   In AVDF version 12.1.1, you can only activate a host if you have completed the procedure in "(Oracle AVDF 12.1.1 Only) Requesting Agent Activation" on page 5-4. Otherwise the Agent Activation Status for that host will be `No Request`.
3. On the **Hosts** tab, make a note of the Agent Activation Key for this host.
4. On the host machine, change directory as follows:

   `cd` *`Agent_Home`*`/bin`

   `Agent_Home` is the directory created in the step 7 on page 5-4 above.
5. Run one of the following commands and provide the Agent Activation Key:
   - **In Oracle AVDF 12.1.2:**

     ```
     agentctl start -k
     Enter Activation Key:
     ```

     Enter the activation key when prompted. This key will not be displayed as you type it.
   - **In Oracle AVDF 12.1.1:**

     `agentctl start -k` *`activation_key`*

   Note: the `-k` argument is not needed after the initial `agentctl start` command.

   See Also: If the agent is deployed on a Microsoft Windows host computer, you can start or stop the agent Windows service through the Windows Services applet in the Windows Control Panel. See "Registering or Unregistering the Audit Vault Agent as a Windows Service" on page 5-5.

   See Also: "ACTIVATE HOST" on page A-5 for the command line syntax to activate the agent

Registering or Unregistering the Audit Vault Agent as a Windows Service

Topics

About the Audit Vault Agent Windows Service

When the Audit Vault Agent is deployed on a Microsoft Windows host computer, during agent deployment ("Deploying the Audit Vault Agent on the Host Computer"

on page 5-3), a Windows service named `OracleAVAgent` is automatically registered. Additionally, you can register and unregister the agent service using the `agentctl` command as shown below.

When the Audit Vault Agent is registered as a Windows service, you can start or stop the service through the Windows Services applet in the Windows Control Panel.

Registering the Audit Vault Agent as a Windows Service

Note: Deploying the Audit Vault Agent on a Windows host automatically registers a Windows service named `agentctl`. Use this procedure if you need to register the Windows service again.

To register the Audit Vault Agent as a Windows Service:

On the host machine, run the following command from the *`Agent_Home`*`\bin` directory:

```
agentctl registersvc
```

This adds the Oracle Audit Vault Agent service in the Windows services registry.

> **Important:** Be sure to set the Audit Vault Agent service to use the credentials of the Windows OS user account that was used to deploy the agent using the `java -jar` command. Do this in the service Properties dialogue.
>
> Note that in the service Properties dialogue, local user name entries in the **This account** field should be formatted as in the following example: user name `jdoe` should be entered as `.\jdoe`. Refer to Microsoft Windows documentation for procedures to do so.

Unregistering the Audit Vault Agent as a Windows Service

To unregister the Audit Vault Agent as a Windows Service, use one of the following methods:

- **Method 1 (Recommended)**

  On the host machine, run the command following command from the `Agent_Home\bin` directory:

  ```
  agentctl unregistersvc
  ```

  This removes the Oracle Audit Vault Agent service from the Windows services registry.

- **Method 2**

  If Method 1 fails, then execute the following from the Windows command prompt (Run as Administrator):

  ```
  cmd> sc delete OracleAVAgent
  ```

  You can verify that the Audit Vault Agent has been deleted by executing the following query from the Windows command prompt (Run as Administrator):

  ```
  cmd> sc queryex OracleAVAgent
  ```

Stopping, Starting, and Other Agent Operations

Topics

Stopping and Starting the Audit Vault Agent

Topics

Stopping and Starting the Agent on Unix Hosts

To stop or start the Audit Vault Agent after initial activation and start, run one of the following commands from the *Agent_Home*/bin directory on the host machine:

```
agentctl stop
```

```
agentctl start
```

Stopping and Starting the Agent on Windows Hosts

The Audit Vault Agent is automatically registered as a Windows service when you deploy the Agent on a Windows host. We recommend that you run the Agent as Windows service so that it can keep running after the user logs out.

See also "Registering or Unregistering the Audit Vault Agent as a Windows Service" on page 5-5.

To stop or start the Agent Windows service:

Use one of the methods below:

- In the Windows GUI (**Control Panel**, **Administrative Tools**, **Services**), find the Oracle Audit Vault Agent service, and then right-click it to select **Start** or **Stop**.
- Run one of these commands from the Agent_Home\bin directory on the host machine:

  ```
  agentctl stopsvc
  ```

  ```
  agentctl startsvc
  ```

To check that the Windows service is stopped:

Run this command:

```
cmd> sc queryex OracleAVAgent
```

You should see the agent Windows service in a STOPPED state.

To stop or start the Agent in console mode:

```
start /b agentctl stop
```

```
start /b agentctl start
```

Changing the Logging Level for the Audit Vault Agent

The logging level you set affects the amount of information written to the log files. You may need to take this into account for disc space limitations.

Log files are located in the *Agent_Home*`/av/log` directory.

The following logging levels are listed in the order of amount of information written to log files, with **debug** providing the most information:

- **error** - Writes only error messages
- **warning** - (Default) Writes warning and error messages
- **info** - Writes informational, warning, and error messages
- **debug** - Writes detailed messages for debugging purposes

To change the logging level for an Audit Vault Agent:

1. Ensure that you are logged into `AVCLI` on the Audit Vault Server.
2. Run the `ALTER HOST` command.

   The syntax is as follows:

   `ALTER HOST` *host_name* `SET LOGLEVEL=av.agent:`*log_level*

   In this specification:

   - *host_name*: The name of the host where the Audit Vault Agent is deployed.
   - *log_level*: Enter a value of `info`, `warn`, `debug`, or `error`.

Deactivating and Removing the Audit Vault Agent

If you have registered the Audit Vault Agent as a Windows service, see "Registering or Unregistering the Audit Vault Agent as a Windows Service" on page 5-5 to unregister the service.

Otherwise, to deactivate and remove the Audit Vault Agent:

1. Stop all audit trails being collected by the Audit Vault Agent.
   a. In the Audit Vault Server console, click the **Hosts** tab, then click **Audit Trails**.
   b. Select the audit trails being collected by this Audit Vault Agent, and then click **Stop**.
2. Stop the Audit Vault Agent by running the following command on the host computer:

   ```
   agentctl stop
   ```

3. Deactivate the Audit Vault Agent on the host computer:
   a. In the Audit Vault Server console, click the **Hosts** tab.
   b. Select the host name, and then click **Deactivate**.
   c. Optionally, drop the host by selecting it, and then clicking **Delete**.
4. Delete the Audit Vault Agent home directory on the host computer.

Updating the Audit Vault Agent

As of Oracle AVDF 12.1.1 BP2, when you update the Audit Vault Server to a future release, the Audit Vault Agent is automatically updated.

If your current release is prior to 12.1.1 BP2, refer to the README included with upgrade software or patch updates for instructions on how to update the Audit Vault Agent.

Information on downloading upgrade software is detailed in *Oracle Audit Vault and Database Firewall Installation Guide*.

Deploying Plug-ins and Registering Plug-in Hosts

Topics

About Plug-ins

Each type of secured target has a corresponding software plug-in in the Audit Vault Server, which enables the Audit Vault Agent to collect audit data. You can deploy more plug-ins, in addition to those shipped with Oracle AVDF, in order to collect audit data from more secured target types. New plug-ins are available from Oracle Technology Network or third parties. The plug-in deployment process updates the `agent.jar` file in the Audit Vault Server.

A plug-in supports only one secured target type. However, you may deploy more than one plug-in for the same secured target type if, for example, you acquired each plug-in from a different developer, or each plug-in supports a specific type of audit trail for the same secured target type. You can select the specific plug-in to use when you configure audit trail collections.

To start collecting audit data from the secured target type associated with a plug-in, you must also add the secured target in the Audit Vault Server, then configure and manually start audit trail collection. See "Configuring Secured Targets, Audit Trails, and Enforcement Points" on page 6-1.

Deploying a plug-in consists of three steps:

1. Ensuring that Auditing is Enabled in the Secured Target
2. Registering the Plug-in Host in Audit Vault Server
3. Deploying and Activating the Plug-in

Ensuring that Auditing is Enabled in the Secured Target

Ensure that auditing has been enabled in the secured target. See the secured target's product documentation for more information. For plug-ins for Oracle Database, see "Ensuring that Auditing is Enabled on Oracle Database Secured Targets" on page 6-6.

Registering the Plug-in Host in Audit Vault Server

To register a host in the Audit Vault Server, see "Registering Hosts in the Audit Vault Server" on page 5-2.

Deploying and Activating the Plug-in

To deploy and activate a plug-in:

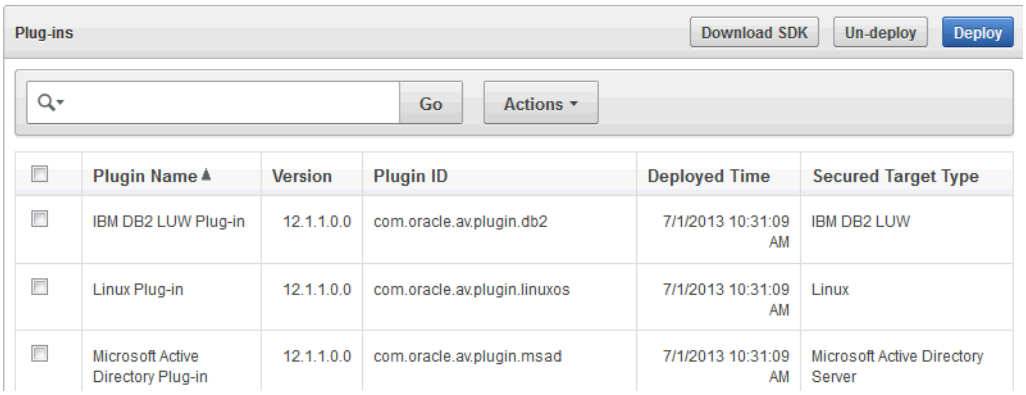
1. Copy the plug-in archive to the Audit Vault Server, and make a note of the location of the file.

   Plug-in archives are available from Oracle Technology Network or a third party.

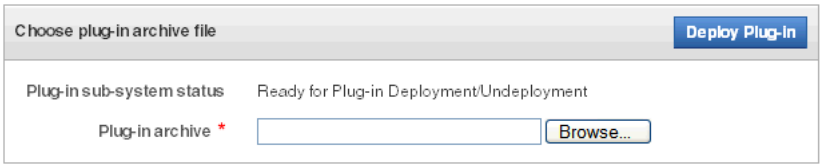
2. Log in to the Audit Vault Server console as an administrator.

3. Click the **Settings** tab, and from the **System** menu, click **Plug-ins**.

   The Plug-ins page lists the currently deployed plug-ins:



4. Click **Deploy**, and in the **Plug-in Archive** field, enter or browse for the name of the plug-in archive.



5. Click **Deploy Plug-in**.

   The new plug-in is listed in the **Hosts** tab, Agent page, under **Plug-ins**. The updated `agent.jar` file has a new Agent Generation Time shown in the Agent page.

   The Hosts page displays an Agent Generation Time column for each registered host, indicating the version of the `agent.jar` on that host.

6. Copy the updated `agent.jar` file to each registered host machine.

   If you have not registered a host machine, see "Registering Hosts in the Audit Vault Server" on page 5-2.

7. On the host machine, extract the agent:

   ```
   java -jar agent.jar
   ```

Note: You cannot download the agent during the same login session in which you deploy a plug-in, since the `agent.jar` is being updated. However, users in other sessions will be able to download the most current version of `agent.jar` until the plug-in deployment process is complete and a new version is available.

Un-Deploying Plug-ins

To un-deploy a plug-in:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab, and from the **System** menu, click **Plug-ins**.
3. Select the plug-in you want, and then click **Un-deploy**.

Deleting Hosts from the Audit Vault Server

When you delete a host, if you want to register it again to collect audit data, you must reinstall the Audit Vault Agent on this host.

To delete hosts:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Hosts** tab.

   A list of the registered hosts, if present, appears in the Hosts page. To control the view of this list see "Working with Lists of Objects in the UI" on page 1-14.
3. Select the host(s) you want to delete, and then click **Delete**.

6

Configuring Secured Targets, Audit Trails, and Enforcement Points

Topics

About Configuring Secured Targets

Secured targets can be supported databases or operating systems that Audit Vault and Database Firewall monitors. You must register all secured targets in the Audit Vault Server, regardless of whether you are deploying the Audit Vault Agent, the Database Firewall, or both.

If you want to collect audit trails from your secured targets, you must configure an audit trail for each target and start collection manually.

If you want to monitor a secured target with the Database Firewall, you must create an enforcement point for that secured target.

For some database secured targets that you monitor with the Database Firewall, you can configure Oracle AVDF to interrogate the database to collect certain data. To do so, you must run scripts on the secured target computers to configure the necessary privileges for database interrogation.

If you are using the Database Firewall, you can also monitor the secured target database's responses to incoming SQL traffic.

This section describes the above configurations in detail.

To understand the high-level workflow for configuring the Oracle AVDF system, see:

- "Configuring Oracle AVDF and Deploying the Audit Vault Agent" on page 1-9
- "Configuring Oracle AVDF and Deploying the Database Firewall" on page 1-10

Registering Secured Targets and Creating Groups

Topics

Registering or Removing Secured Targets in the Audit Vault Server

Topics

Registering Secured Targets

An Oracle AVDF super administrator can create secured targets and grant access to them to other administrators. An Oracle AVDF administrator can also create secured targets, but they are only accessible to that administrator and the super administrator.

Registering Oracle Database 12*c* Release 1 Secured Targets

In Oracle Database 12*c*, if you are not using a multitenant container database (CDB), then register a secured target for your database as you would for previous versions of Oracle Database. If you use a CDB, then you must register a secured target for the CDB, as well as each pluggable database (PDB).

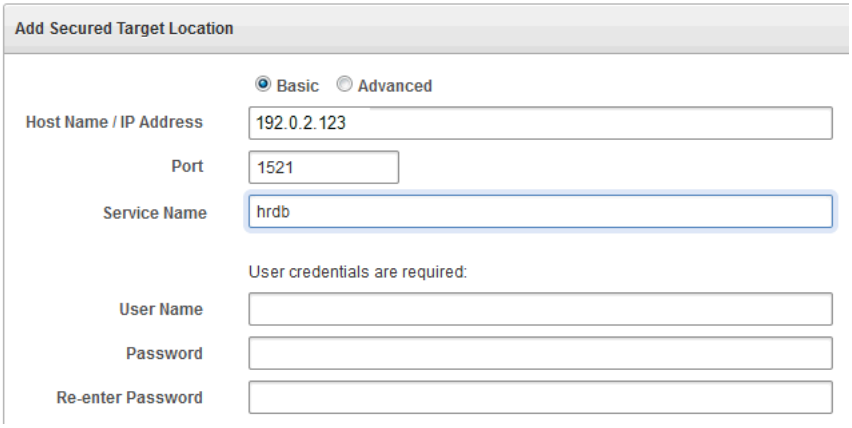
To register a secured target in the Audit Vault Server:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.

   The Secured Targets page lists the configured secured targets to which you have access. You can sort or filter the list of targets. See "Working with Lists of Objects in the UI" on page 1-14.
3. Click **Register**, and in the Register Secured Target page, enter a **New Secured Target Name** and optional **Description** for the new target.
4. In the **Secured Target Type** field, select the secured target type, for example, `Oracle Database`.
5. (Optional) Enter the **Secured Target Location**. This is not required for a Database Firewall-only deployment.

   This section looks slightly different depending on your Oracle AVDF version:

   - **In AVDF version 12.1.2:**

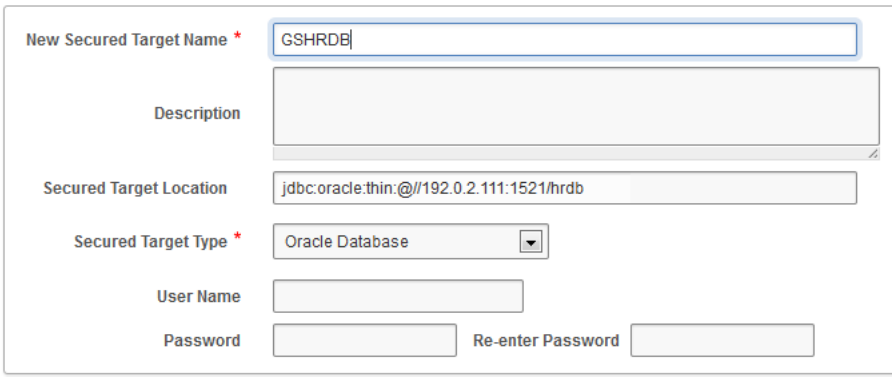


In the Add Secured Target Location section, enter the **Host Name** or **IP Address, Port**, and for Oracle Databases, the **Service Name** (or SID).

If you know the exact connect string, you can click the **Advanced** radio button instead, and enter the string there. See "Secured Target Locations (Connect Strings)" on page B-24.

Note: For an Oracle RAC secured target, enter the SCAN host name.

- **In AVDF version 12.1.1:**



Enter the connect string for the secured target. See "Secured Target Locations (Connect Strings)" on page B-24 for the connect string format for a specific secured target type. For example, for Oracle Database, the string might look like the following:

```
jdbc:oracle:thin:@//203.0.113.0:1521/hrdb
```

Note: For an Oracle RAC secured target, enter the SCAN host name.

6. If required by this type of secured target, in the **User Name**, **Password**, and **Re-enter Password** fields, enter the credentials for the secured target user account you created for Oracle AVDF.

   See "Setting User Account Privileges on Secured Targets" on page 6-7 for more information.

7. If you will monitor this secured target with a Database Firewall, in the **Add Secured Target Addresses** area, for each available connection of this database enter the following information, and then click **Add**.

   - **IP Address** (or Host Name)

- **Port Number**
- **Service Name** (Optional, for Oracle Database only)

  You can also use an **SID** in this field. To enter multiple service names and/or SIDs, enter a new line here for each of them, and then click **Add**.

  Important: If you specify service names and/or SIDs, the Database Firewall only captures traffic to the service names and/or SIDs listed. In this case, if a database client connects using a different Service Name or SID than those listed, that traffic is not monitored by the Database Firewall. If you want to enforce different Database Firewall policies for different service names or SIDs on the same database, you must create a separate secured target for each service name or SID.

8. If required, enter values for **Attribute Name** and **Attribute Value** at the bottom of the page, and click **Add**.

   Collection attributes may be required by the Audit Vault Agent depending on the secured target type. See "Collection Attributes" on page B-24 to look up requirements for a specific secured target type.

9. If you will monitor this secured target with a Database Firewall, you can increase the processing resource for this secured target by adding the following Collection Attribute:

   Attribute Name: `MAXIMUM_ENFORCEMENT_POINT_THREADS`

   Attribute Value: A number between 1 - 16 (default is 1)

   This defines the maximum number of Database Firewall processes (1 - 16) that may be used for the enforcement point associated with this secured target. You should consider defining this if the number of secured targets you are monitoring is less than the number of processing cores available on the system running the Database Firewall. Setting a value when it is not appropriate wastes resources.

10. Click **Save**.

Modifying Secured Targets

To modify a secured target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.

   The Secured Targets page lists the configured secured targets to which you have access. You can sort or filter the list of targets. See "Working with Lists of Objects in the UI" on page 1-14.

3. Click the name of the secured target you want to modify.
4. In the Modify Secured Target page, make your changes, and then click **Save**.

   Refer to "Registering Secured Targets" on page 6-2 for a description of the fields.

Note: If you change the name of a secured target, the new name does not appear in Oracle AVDF reports until you restart the Audit Vault Agent.

Removing Secured Targets

If you no longer need to have a secured target registered with Oracle AVDF, you can use either the console or the command-line utility to remove the secured target. After you have removed the secured target from Oracle AVDF, its audit data still resides in the data warehouse within its retention period (archiving policy). For information on archiving (retention) policies, see "Creating or Deleting Archiving Policies" on page 3-9.

After you have removed a secured target, its identity data remains in Oracle AVDF so that there will be a record of secured targets that have been dropped. Remove the secured target only if you no longer want to collect its data or if it has moved to a new host computer.

To remove a secured target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the Secured Targets tab, and then select the secured target(s) you want to remove.
3. Click **Delete**.

Creating or Modifying Secured Target Groups

As a super administrator you can create secured target groups in order to grant other administrators access to secured targets as a group rather than individually.

To create a secured target group:

1. Log into the Oracle Audit Vault and Database Firewall console as a super administrator, and click the **Secured Targets** tab.
2. From the **Groups** menu on the left.

   Preconfigured groups are listed in the top pane, and user defined groups are listed in the bottom pane.

   You can adjust the appearance of the list in the bottom pane from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-14.
3. Click **Create**, and enter a name and optional description for the group.
4. To add secured targets to the group, select the secured targets, and click **Add Members**.
5. Click **Save**.

   The new group appears in the bottom pane of the groups page.

To modify a secured target group:

1. Log into the Oracle Audit Vault and Database Firewall console as a super administrator, and click the **Secured Targets** tab.
2. From the **Groups** menu on the left.

   Preconfigured groups are listed in the top pane, and user defined groups are listed in the bottom pane.

   You can adjust the appearance of the list in the bottom pane from the **Actions** menu. See "Working with Lists of Objects in the UI" on page 1-14.
3. Click the group name.

4. In the Modify Secured Target page, select secured targets you want to add or remove, and then click **Add Members** or **Drop Members**.
5. Optionally, you can change the name or description of the group.
6. Click **Save**.

Controlling Access to Secured Targets and Target Groups

Oracle AVDF super administrators can control which administrators have access to secured targets or secured target groups. You can control access for an individual user, or for an individual secured target or group. For instructions, see "Managing User Access to Secured Targets or Groups" on page 11-3.

Preparing Secured Targets for Audit Data Collection

Topics

Using an NTP Service to set Time on Secured Targets

It is recommended that you also use an NTP service on both your secured targets and the Audit Vault Server. This will help to avoid confusion on timestamps on the alerts raised by the Audit Vault Server.

For instructions on using an NTP server to set time for the Audit Vault Server, see "Specifying the Server Date, Time, and Keyboard Settings" on page 3-2.

Ensuring that Auditing is Enabled on the Secured Target

In order to collect audit data from a secured target, you must ensure that auditing is enabled on that secured target, and where applicable, note the type of auditing that the secured target is using. Check the product documentation for your secured target type for details.

Ensuring that Auditing is Enabled on Oracle Database Secured Targets

To check if auditing is enabled on an Oracle Database secured target:

1. Log in to the Oracle database as a user with administrative privileges. For example:

```
sqlplus trbokuksa
Enter password: password
Connected.
```

2. Run the following command:

```
SHOW PARAMETER AUDIT_TRAIL

NAME                                 TYPE        VALUE
------------------------------------ ----------- -------
audit_trail                          string      DB
```

3. If the output of the `SHOW PARAMETER` command is `NONE` or if it is an auditing value that you want to change, then you can change the setting as follows.

   For example, if you want to change to `XML`, and if you are using a server parameter file, you would enter the following:

```
CONNECT SYS/AS SYSDBA
Enter password: password

ALTER SYSTEM SET AUDIT_TRAIL=XML SCOPE=SPFILE;
System altered.

SHUTDOWN
Database closed.
Database dismounted.
ORACLE instance shut down.

STARTUP
ORACLE instance started.
```

4. Make a note of the audit trail setting.

   You will need this information when you configure the audit trail in Oracle AVDF.

Setting User Account Privileges on Secured Targets

Some secured target types require credentials in order for Oracle AVDF to access them. If you plan to collect audit data from a secured target, do stored procedure auditing (SPA), entitlements auditing, or enable database interrogation, you must create a user account on the secured target with the appropriate privileges to allow Oracle AVDF to access the required data.

Setup scripts for database secured targets: Oracle AVDF provides scripts to configure user account privileges for database secured target types. See "Scripts for Oracle AVDF Account Privileges on Secured Targets" on page B-12.

Non-database secured targets: You must create a user that has the appropriate privileges to access the audit trail required. For example, for a Windows secured target, this user must have administrative permissions in order to read the security log.

> **Note:** Oracle AVDF does not accept user names with quotation marks. For example, "JSmith" would not be a valid user name for an Audit Vault and Database Firewall user account on secured targets.

Scheduling Audit Trail Cleanup

Oracle AVDF supports audit trail cleanup for Oracle Database, Microsoft SQL Server, and MySQL. For instructions, see "Audit Trail Cleanup" on page B-21.

Configuring and Managing Audit Trail Collection

Topics

- (Required for MySQL) Running the XML Transformation Utility
- (Required for IBM DB2) Converting Binary DB2 Audit Files to ASCII Format

Adding an Audit Trail in the Audit Vault Server

In order to start collecting audit data, you must configure an audit trail for each secured target in the Audit Vault Server, and then start the audit trail collection manually.

This procedure assumes that the Audit Vault Agent is installed on the same host computer as the secured target.

Prerequisites

Before configuring an audit trail for any secured target, you must:

- Add the secured target in the Audit Vault Server. See "Registering or Removing Secured Targets in the Audit Vault Server" on page 6-2 for details.
- Register the host machine. This is usually the machine where both the secured target resides and the Audit Vault Agent is deployed. See "Registering Hosts and Deploying the Agent" on page 5-1.
- Deploy and activate the Audit Vault Agent on the host machine. See "Deploying and Activating the Audit Vault Agent on Host Computers" on page 5-2.
- For MySQL secured targets, run the XML transformation utility. See "(Required for MySQL) Running the XML Transformation Utility" on page 6-10.
- For IBM DB2 secured targets, ensure that the binary audit file has been converted to ASCII format before starting an audit trail. See "(Required for IBM DB2) Converting Binary DB2 Audit Files to ASCII Format" on page 6-11.

To configure an audit trail for a secured target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.
3. Under **Monitoring**, click **Audit Trails**.

   The Audit Trails page appears, listing the configured audit trails and their status.
4. In the Audit Trails page, click **Add**.
5. In the **Collection Host** field, click the up-arrow icon to display a search box, and then find and select the host computer where the Audit Vault Agent is deployed.
6. In the **Secured Target Name** field, click the up-arrow icon to display a search box, and then find and select the secured target.
7. From the **Audit Trail Type** drop-down list, select one of the following:
   - CUSTOM
   - DIRECTORY
   - EVENT LOG
   - NETWORK
   - SYSLOG
   - TABLE
   - TRANSACTION LOG

For this audit trail type, ensure that the secured target database has a fully qualified database name. See the `GLOBAL_NAMES` setting in Table C–1.

See Table B–13 on page B-11 for details on which type(s) of audit trails can be collected for a specific secured target type, and "Summary of Data Collected for Each Audit Trail Type" on page B-10 for descriptions of data collected.

8. In the **Trail Location** field, enter the location of the audit trail on the secured target computer, for example, `sys.aud$`.

   The trail location depends on the type of secured target. See "Audit Trail Locations" on page B-28 for supported trail locations.

   Note: If you selected DIRECTORY for Audit Trail Type, the Trail Location must be a directory mask.

9. If you have deployed plug-ins for this type of secured target, select the plug-in in the **Collection Plug-in** drop-down list.

   For more information on plug-ins, see "About Plug-ins" on page 5-9.

10. Click **Save**.

    The audit trail is added to the list on the Audit Trails page. The collection status displays a red down-arrow (stopped) initially. The audit trail starts automatically shortly after it is added.

Stopping and Starting Audit Trails in the Audit Vault Server

An audit trail starts automatically shortly after you add it. In order to start an audit trail, the Audit Vault Agent must be running on a host computer. See "Deploying and Activating the Audit Vault Agent on Host Computers" on page 5-2 for details.

To start or stop audit trail collection for a secured target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.
3. Click **Audit Trails**.
4. Select the audit trail(s) you want to start or stop, and then click **Stop** or **Start**.

   You cannot start an audit trail while the Audit Vault Agent is updating. See "Updating the Audit Vault Agent" on page 5-8.

Note: If your environment has a large number of audit files to collect, for example 1 million or more, the audit trail may take a few minutes to start.

Checking the Status of Audit Trails in the Audit Vault Server

To check the status of audit trails:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.
3. Click **Audit Trails**.

   The Audit Trails page lists audit trails and their status in the **Collection Status** column. A green up-arrow indicates that collection is working. A red down-arrow

indicates that collection is down. You can see the following specific status values by pointing your mouse to the up or down arrow icons:

- **Idle** - Trail is up and running, no new audit data to collect. In this state, the trail is waiting for the Secured Target to generate new audit data.
- **Collecting** - Trail is currently actively collecting audit data.
- **Stopped** - Trail is currently stopped.
- **Recovering** - Trail has collected a batch of audit data and is setting a checkpoint on the Audit Vault Server. This can take a while depending on the server load.
- **Unreachable** - A heartbeat timeout has occurred, indicating that a heartbeat message has not been received from the trail in the last two minutes. This status is temporary unless the trail has crashed.

You can sort and filter the audit trail list. See "Working with Lists of Objects in the UI" on page 1-14.

Deleting an Audit Trail

You can delete an audit trail only if it does not have previously collected audit data associated with it.

To delete an audit trail:

1. Log in to the Audit Vault Server console as an administrator.
2. Make sure the audit trail is stopped. See "Stopping and Starting Audit Trails in the Audit Vault Server" on page 6-9.
3. Click the **Secured Targets** tab.
4. Click **Audit Trails**.
5. Select the audit trail(s) you want to delete, and then click **Delete**.

(Required for MySQL) Running the XML Transformation Utility

For MySQL secured targets, Oracle AVDF provides a utility to transform the MySQL XML audit log file into a required format for audit data collection. You must run this utility on the MySQL host machine before adding an audit trail.

Prerequisites

- Register the MySql secured target in the Audit Vault Server. See "Registering or Removing Secured Targets in the Audit Vault Server" on page 6-2.
- Deploy the Audit Vault Agent on the MySql host machine. See "Deploying the Audit Vault Agent on the Host Computer" on page 5-3.

To run the XML Transformation Utility:

1. On the MySQL host computer, go to the directory `AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/bin/`
2. Run the following command:

```
MySQLTransformationUtility.bat inputPath=path_to_log_folder
outputPath=path_to_converted_xml agentHome=path_to_AGENT_HOME
interval=interval_in_minutes xslPath=XSL_file_path
securedTargetName=registered_secured_target_name
```

The above command contains the following variables:

- *path_to_log_folder* - The path to the MySQL log folder listed in `my.ini`
- *path_to_converted_xml* - The path to the folder where the converted XML files will reside. You will use this path as the **Trail Location** when creating the audit trail for this MySQL secured target in the Audit Vault Server, or when starting audit trail collection using the `AVCLI` command line.
- *path_to_AGENT_HOME* - The path to the installation directory of the Audit Vault Agent
- *interval_in_minutes* - (Optional) The waiting time, in minutes, between two transformation operations. If not specified, the default it is 60 minutes. To run the transformation utility once, specify `-ve` for this argument.
- *XSL_file_path* - (Optional) The path to the XSL file to use for the transformation.
- *registered_secured_target_name* - The name of the MySQL secured target registered in the Audit Vault Server.

Example:

```
MySQLTransformationUtility.bat inputPath=D:\MySQLLog
outputPath=D:\ConvertedXML agentHome=E:\MySQLCollector interval=1
securedTargetName=MYSQL_DEV
```

(Required for IBM DB2) Converting Binary DB2 Audit Files to ASCII Format

IBM DB2 creates its audit log files in a binary file format that is separate from the DB2 database. For IBM DB2 secured targets, you must convert the binary file to an ASCII file before each time you collect audit data (start an audit trail) for a DB2 database, using the script instructions in this section.

Ideally, schedule the script to run periodically. If the script finds older text files that have already been collected by the DB2 audit trail, then the script deletes them. It creates a new, timestamped ASCII text file each time you run it. Optionally, you can set the script to purge the output audit files.

> **Note:** It is recommended that you extract audit log files for each database and each instance in a separate directory. You must configure separate audit trails for each database and each instance in Oracle AVDF.

To convert the binary DB2 Audit File to an ASCII file:

1. Identify a user who has privileges to run the `db2audit` command.

   This user will extract the binary files to the text files.

2. Grant the user you identified in Step 1 execute privileges to run the conversion script from the Oracle AVDF directory. The script name is:

   - **DB2 release 8.2 databases:** `DB282ExtractionUtil` (for Microsoft Windows, this file is called `DB282ExtractionUtil.bat`.)
   - **DB2 9.5 release databases:** `DB295ExtractionUtil` (for Microsoft Windows, this file is called `DB295ExtractionUtil.bat`.)

3. Grant the user you identified in Step 1 read permission for the `$AGENT_HOME/av/atc` directory and its contents.
4. In the server where you installed the IBM DB2 database, open a shell as the `SYSADM` DB2 user.
5. Set the following variables:
   - `AGENT_HOME` (this is the Audit Vault Agent installation directory)
   - `DB2AUDIT_HOME` (this directory points to the main directory that contains the `db2audit` command)
6. Ensure that the Oracle AVDF owner of the agent process has read permissions for the audit text files that will be generated by the extraction utility.
7. Log in as the DB2 user that you identified in "IBM DB2 for LUW Setup Scripts" on page B-19.
8. Run one of the following scripts, depending on the version of DB2 that you have installed:
   - **For DB2 release 8.2 databases:**

     ```
     DB282ExtractionUtil -extractionpath default_DB2_audit_directory
     -audittrailcleanup yes/no
     ```

     – *default_DB2_audit_directory*: Enter the full directory path to the location of the DB2 audit directory. Typically, this directory is in the following locations:

       UNIX: *DB2_HOME*`/sqlib/security/auditdata`

       Microsoft Windows: *DB2HOME*`\instance\security\auditdata`

     – *yes/no*: Enter `yes` or `no`, to enable or disable the audit trail cleanup. Entering `yes` deletes the IBM DB2 audit file up to the latest audit record which has been collected by the Oracle AVDF DB2 audit trail. If you omit this value, then the default is `no`.

     For example, to extract audit files and enable the audit trail cleanup:

     ```
     DB282ExtractionUtil -extractionpath /home/extract_dir -audittrailcleanup
     yes
     ```

     This script creates the ASCII text file in the `auditdata` directory, using the following format, which indicates the time the file was created:

     ```
     db2audit.instance.log.0.YYYYDDMMHHMMSS.out
     ```

   - **For DB2 release 9.5 databases:**

     ```
     DB295ExtractionUtil -archivepath archive_path -extractionpath extraction_
     path -audittrailcleanup yes/no -databasename database_name
     ```

     In this specification:

     – *archive_path*: This is DB2 archive path configured using the `db2audit` utility.

     – *extraction_path*: This is the directory where the DB2 extraction utility places the converted ASCII text file. This file is created in either the `db2audit.instance.log.0.YYYYDDMMHHMMSS.out` or `db2audit.db.`*database_name*`.log.0.20111104015353.out` format.

- *yes/no*: Enter `yes` or `no`, to enable or disable the audit trail cleanup. Entering `yes` deletes the archived IBM DB2 audit files that were collected by the Oracle AVDF DB2 audit trail. If you omit this value, then the default is `no`.
- *database_name*: (Optional) This is the name, or names separated by spaces, of the database(s) that contain the audit records.

  The utility creates a separate ASCII file for each database named in the command. If this parameter is omitted, then the utility converts the instance binary to an ASCII file. This parameter enables you to collect categories of audit records such as object maintenance (`objmaint`) records, which capture the creation and dropping of tables.

  Important: If you enter more than one database name in this command, be sure to put the ASCII file for each database in a separate directory after you run the command.

Example 1: The following command creates an ASCII file for the `TOOLSDB` database, puts the file in the `/home/extract_dir` directory, and deletes archive files after you have collected audit data:

```
DB295ExtractionUtil -archivepath /home/archive_dir -extractionpath
/home/extract_dir -audittrailcleanup yes -databasename TOOLSDB
```

Example 2: The following command creates an ASCII file for the database instance, puts the file in the `/home/extract_dir` directory, and deletes archive files after you have collected audit data:

```
DB295ExtractionUtil -archivepath /home/archive_dir -extractionpath
/home/extract_dir -audittrailcleanup yes
```

To schedule the script to run automatically, follow these guidelines:

- **UNIX**: Use the `crontab` UNIX utility. Provide the same information that you would provide using the parameters described previously when you normally run the script.
- **Microsoft Windows:** Use the Windows Scheduler. Provide the archive directory path (for release 9.5 databases only), extraction path, and secured target database name in the scheduled task.

Configuring Enforcement Points

Topics

About Configuring Enforcement Points for Secured Targets

If you are monitoring databases with a Database Firewall, you must configure one enforcement point for every secured target database that you want to monitor with the

firewall. The enforcement point configuration lets you specify the firewall monitoring mode (monitoring only or blocking), identify the secured target database being monitored, the network traffic sources to that database, and the Database Firewall used for the enforcement point.

Before configuring enforcement points, configure network traffic sources as part of database firewall configuration. See "Configuring Database Firewalls on Your Network" on page 4-5 for details.

Creating and Configuring an Enforcement Point

Configure each enforcement point at the Audit Vault Server console. If you have configured a resilient pair of Audit Vault Servers, configure the enforcement points on the primary server.

See "Configuring High Availability" on page 8-1 for details on configuring a resilient pair of servers.

To configure an enforcement point:

1. Ensure that you have configured traffic sources on the Database Firewall you plan to use for this enforcement point.

   See "Configuring Database Firewalls on Your Network" on page 4-5.

2. Log in to the Audit Vault Server console as an administrator.
3. Click the **Secured Targets** tab, and from the **Monitoring** menu, click **Enforcement Points**.

   The Enforcement Points page displays a list of configured enforcement points and their status.

4. Click **Create**.
5. Enter a **Name** for this enforcement point.
6. Select a **Monitoring Mode**:

   - **Database Policy Enforcement (DPE)** - to block or substitute SQL statements.
   - **Database Activity Monitoring (DAM)** - to log SQL statements and raise alerts only

   See "The Database Firewall" on page 1-6 for more information on these modes.

7. In the **Select Secured Target to monitor** section, select a secured target.

   Secured targets are listed here with their specified firewall policy. If the policy specified contains SQL blocking rules, but you select the DAM mode (monitoring only), SQL statements will not be blocked. Therefore, if you want to block SQL statements according to policy rules, you should have both a "blocking" policy for the secured target, and DPE monitoring mode for the enforcement point.

8. In the **Select Firewall** section, select the Database Firewall that will handle this enforcement point.

   The **Select Traffic Sources** section appears below the **Select Firewall** section.

9. Select traffic sources in either the **Bridged Interfaces** or the **Proxy Interfaces** area.

   See these topics for more information on traffic sources:

   - "Configuring Traffic Sources" on page 4-5
   - "Configuring a Bridge in the Database Firewall" on page 4-6

- "Configuring a Database Firewall as a Traffic Proxy" on page 4-6

Note: If you select a proxy traffic source, you cannot select any other traffic sources. Also, selecting a proxy forces the Monitoring Mode to DPE. See "Configuring a Database Firewall as a Traffic Proxy" on page 4-6.

10. Click **Save**.

    The new enforcement point appears in the Enforcement Points list and starts automatically.

11. To stop or restart the enforcement point, select it from the Enforcement Points list and click **Stop** or **Start**.

Note: When you use a Database Firewall in DPE mode, you must configure any external devices that use IP or MAC address spoofing detection rules such that they ignore database IP or MAC address changes made by the Database Firewall.

Modifying an Enforcement Point

After you create an enforcement point, you can modify it to change its settings, or to enable database response monitoring, database interrogation, and/or host monitoring.

Advanced settings in the enforcement point let you configure Oracle AVDF to work with BIG-IP Application Security Manager (ASM). See "Configuring Oracle AVDF to Work with F5" on page 9-4 for details.

To modify an enforcement point:

1. Log in to the Audit Vault Server console as an administrator, and click the **Secured Targets** tab.
2. From the **Monitoring** menu, click **Enforcement Points**, and then click the name of the enforcement point you want to modify.
3. In the Modify Enforcement Point page, you can change the following settings:
   - **Secured Target** - Select a different secured target to monitor
   - **Monitoring Mode** - Select the alternate monitoring mode.

     Note: If switching from DAM to DPE mode, select whether or not to **Maintain Existing Connections** from clients to your secured target database. If you select this option, existing connections will not be disrupted, but will need to reconnect to the secured target database before they can be monitored in DPE mode.
   - **Traffic Sources** - Enable different traffic sources.
   - **Database Response** - Select to enable database response monitoring. See "Configuring and Using Database Response Monitoring" on page 6-22.
   - **Database Interrogation** - Select to enable database interrogation. See "Configuring and Using Database Interrogation" on page 6-17.
4. Click **Save**.

Starting, Stopping, or Deleting Enforcement Points

To manage enforcement points:

1. Log in to the Audit Vault Server console as an administrator.

2. Click the **Secured Targets** tab, and under **Monitoring**, click **Enforcement Points**.
3. Select the enforcement points you want, and click one of the following buttons:
   - **Start** to start the enforcement point
   - **Stop** to stop the enforcement point
   - **Delete** to delete the enforcement point

Viewing the Status of Enforcement Points

To view the status of enforcement points:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab, and under **Monitoring**, click **Enforcement Points**.

   A list of enforcement points and their status is displayed. Possible status values are:
   - **Up** - The enforcement point is up and running, and there are no errors.
   - **Suspended** - The user has stopped the enforcement point, and there are no errors.
   - **Down** - The enforcement point is not working, probably due to errors.
   - **Unreachable** - There are communications errors between the Database Firewall and the Audit Vault Server.

Finding the Port Number Used by an Enforcement Point

To find the port number used by an enforcement Point:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab, and under **Monitoring**, click **Enforcement Points**.
3. Select the enforcement points you want, and in the Modify Enforcement Point page click **Advanced**.

   The port number is shown next to **DBFW TCP Port**.

Configuring Stored Procedure Auditing (SPA)

Stored procedure auditing (SPA) enables Oracle AVDF auditors to audit changes to stored procedures on secured target databases. Oracle AVDF connects to the database server at scheduled intervals and discovers any changes or additions that have been made to stored procedures. SPA is supported for all database secured targets supported by Oracle AVDF. See "Supported Secured Targets" on page 1-2.

To enable SPA, you simply configure the user account privileges necessary for Oracle AVDF to do stored procedure auditing on a secured target. Oracle AVDF provides scripts for setting up these privileges. For script instructions, see "Scripts for Oracle AVDF Account Privileges on Secured Targets" on page B-12, and run the script specific for the secured target type.

An Oracle AVDF auditor can view changes to stored procedures in reports if the auditor enables Stored Procedure Auditing in the Secured Target configuration. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for details.

Configuring and Using Database Interrogation

Topics

About Database Interrogation

Database interrogation allows the Database Firewall to interrogate supported database secured targets for specific information. The information collected depends on the database type. This section describes two ways to use database interrogation:

- Using Database Interrogation for SQL Server and SQL Anywhere Databases
- Using Database Interrogation for Oracle Databases with Network Encryption

Using Database Interrogation for SQL Server and SQL Anywhere Databases

You can use database interrogation to interrogate a monitored Microsoft SQL Server and Sybase SQL Anywhere database to obtain the name of the database user, operating system, and client program that originated a SQL statement, if this information is not available from the network traffic. This information then is made available in the Audit Vault and Database Firewall reports.

To configure database interrogation for these two databases you must:

- Create a user account for AVDF database interrogation on the database, then grant specific privileges to that user account. See "Configuring Database Interrogation for SQL Server and SQL Anywhere" on page 6-18.
- In AVDF, enable database interrogation in the enforcement point that monitors the secured target database. See "Enabling Database Interrogation" on page 6-21.

Using Database Interrogation for Oracle Databases with Network Encryption

If you are using the Database Firewall to monitor an Oracle Database secured target that uses Network Encryption, you must use Database Interrogation in order to decrypt statements sent to, and responses received from, that database so they can be analyzed.

For detailed configuration steps, see "Configuring Database Interrogation for Databases Using Network Encryption" on page 6-18.

Limitations on Decryption of Oracle Database Statements

Configuring Audit Vault and Database Firewall to decrypt traffic with Network Encryption has the following limitations:

- The supported Oracle Database versions are: 10.x, 11.1, 11.2, 12*c*
- There is no statement substitution in Audit Vault and Database Firewall when Network Encryption checksum is used.
- There is no support for Network Encryption RC4 cipher.

Configuring Database Interrogation for SQL Server and SQL Anywhere

Topics

Setting Database Interrogation Permissions in a Microsoft SQL Server Database

To set up the user account for a Microsoft SQL Server (versions 2005, 2008, or 2012) database:

1. Create a user account for AVDF database interrogation on the database that you want to interrogate. (This database should be a secured target in AVDF.)

   Make a note of the user name and password for this account.

2. Grant the following permissions to the user account you created in Step 1:
   - `VIEW ANY DEFINITION` and `VIEW SERVER STATE` for SQL Server 2005 and later
   - `SELECT` on the `master.dbo.sysdatabases` table

3. Enable database interrogation in the enforcement point that monitors this secured target database, using the credentials you created in Step 1.

   See "Enabling Database Interrogation" on page 6-21.

Setting Database Interrogation Permissions in a Sybase SQL Anywhere Database

Note: Before you can use Sybase SQL Anywhere, you must download and install the SQL Anywhere ODBC driver for Linux.

To set user permissions for database interrogation in a Sybase SQL Anywhere database:

1. Create a user account for AVDF database interrogation on the database that you want to interrogate. (This database should be a secured target in AVDF.)

   Make a note of the user name and password for this account.

2. Grant the following permissions to the user account you created in Step 1:
   - `CONNECT`
   - `SELECT` on these system tables:

     ```
     sys.sysuser
     sys.sysuserauthority
     sys.sysremoteuser
     sys.sysloginmap
     sys.sysgroup
     ```

3. Enable database interrogation in the enforcement point that monitors this secured target database, using the credentials you created in Step 1.

   See "Enabling Database Interrogation" on page 6-21.

Configuring Database Interrogation for Databases Using Network Encryption

To configure Database Interrogation for an Oracle Database that uses Network Encryption, follow steps in this section:

Step 1: Apply the Specified Patch to the Oracle Database

Important: This step is not required for Oracle Database versions 11.2.0.4, or 12*c*. Do not perform this step if you have these versions.

For all other supported Oracle Database versions, you must apply the patch specified in this section to the Oracle Database that is using Network Encryption.

To apply the patch:

1. Shut down the Oracle Database.
2. Get the patch identified by the bug number `13051081`.

   The patch file will be in the format: `p13051081_`*`OracleVersion_Platform`*`.zip`. For example: `p13051081_112030_Linux-x86-64.zip`
3. Unzip the patch `.zip` file in a directory, identified here as *`Patch_Directory`*.
4. Go to the directory Patch_Directory`/13051081`.
5. Execute the command:

   ```
   $ opatch apply
   ```
6. Start the Oracle Database.

Step 2: Run the Oracle Advance Security Integration Script

To run the Network Encryption integration script:

1. From the Oracle AVDF utilities file `avdf-utility.zip` (downloaded with your Oracle AVDF software), copy the `database` directory to a location from which you can connect to the Oracle Database being patched.
2. In this location, go to the `database/ddi` directory and uncompress one of the two `oracle` compressed files (both contain the same content), preferably into a directory called `oracle`.

   This directory now contains the uncompressed file: `advanced_security_integration.sql`.
3. Execute the following command as a user that has privileges to create users and grant privileges:

   `sqlplus / as sysdba @advanced_security_integration` *`schema password`*

   For *`schema`*, use the name of an existing schema or choose a name for a new schema. We do not recommend using `SYSTEM` or `SYS` as the target schema. If the schema does not exist, this procedure will create a user and a schema.

   This command grants the `create session` and `resource` privileges to the schema user.

   The password for the schema is set to *`password`*.

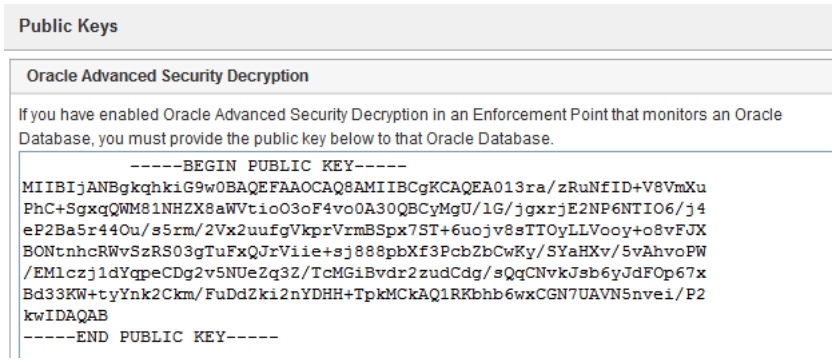
   A package supporting Network Encryption integration is installed into *`schema`*.

Step 3: Provide the Database Firewall Public Key to the Oracle Database

In order for to decrypt database traffic using database interrogation, you must provide the Database Firewall public key to the Oracle Database that is using Network Encryption.

To provide the public key to the Oracle Database:

1. In the Administration console of the Database Firewall that will be monitoring this Oracle Database, in the **System** menu, click **Public Keys** .



2. Copy the public key under Oracle Advanced Security Decryption and paste it into a text file, for example, `dbfw_public_key.txt`.

   Each Database Firewall has its own public key. In a case where you have Database Firewall high availability or enforcement point resiliency, when you have more than one Database Firewall monitoring this secured target, each Database Firewall public key must be copied and appended to the `dbfw_public_key.txt` file.

   Note: For security purposes the `dbfw_public_key.txt` file must have the same access permissions as the `sqlnet.ora` file on the Oracle Database server.

3. Modify the `sqlnet.ora` file in the Oracle Database to include the public key and to require Network Encryption native traffic encryption:

   a. Put the file you created in Step 2 on the Oracle Database server, preferably in the same directory as the `sqlnet.ora` file.

   b. Open the `sqlnet.ora` file and append the following parameters (in this example the public key file is `dbfw_public_key.txt`):

   ```
   SQLNET.ENCRYPTION_TYPES_SERVER=AES256
   SQLNET.DBFW_PUBLIC_KEY="/path_to_file/dbfw_public_key.txt"
   SQLNET.EXCRYPTION_SERVER=REQUIRED
   ```

   Note: If the `sqlntet.ora` file contains the optional parameter `SQLNET.ENCRYPTION_CLIENT`, its value must not be `REJECTED`. Otherwise, an error will occur.

   c. Save and close the `sqlnet.ora` file.

   For more information on network encryption, see *Oracle Database Security Guide*.

Step 4: Enable Database Interrogation for the Oracle Database

Follow the procedure in "Enabling Database Interrogation" on page 6-21 to complete the Database Interrogation setup for an Oracle Database that uses Network Encryption.

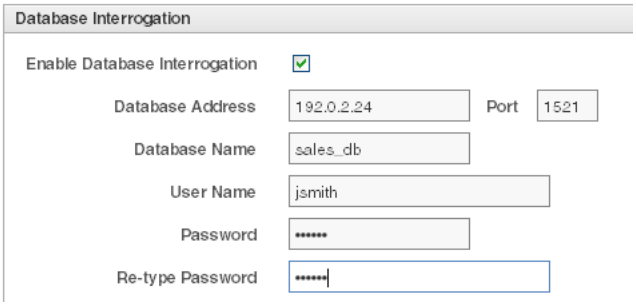
Enabling Database Interrogation

To enable database interrogation in an enforcement point:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Enforcement Points**.
3. Find the enforcement point that monitors the secured target that will be interrogated, and then click the name of that enforcement point.

   The Modify Enforcement Point page appears.
4. In the Database Interrogation section of the page, click the **Enable Database Interrogation** check box.

   Additional input fields appear:



5. Enter values for the following:
   - **Database Address** and **Port** - Enter the IP address and port number of the secured target database that will be interrogated.
   - **Database Name** - Enter the name of the database or database instance.
   - **User Name** - Enter the database interrogation user name that was set up for this secured target. (See "Configuring Database Interrogation for SQL Server and SQL Anywhere" on page 6-18.)
   - **Password** and **Re-type Password** - Enter the password for the database interrogation user name.
6. Click **Save**.

Disabling Database Interrogation

You can temporarily disable database interrogation. Audit Vault and Database Firewall saves the configuration information that you have created for the next time that you want to enable it.

To disable database interrogation:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Enforcement Points**.

   The Enforcement Points page appears, listing enforcement points and their status. You can sort or filter the list. See "Working with Lists of Objects in the UI" on page 1-14.

3. Find the enforcement point for which you want to disable database interrogation, and then click the name of that enforcement point.

   The Modify Enforcement Point page appears.

4. In the Database Interrogation section of the page, clear the **Enable Database Interrogation** check box.

5. Click **Save**.

Configuring and Using Database Response Monitoring

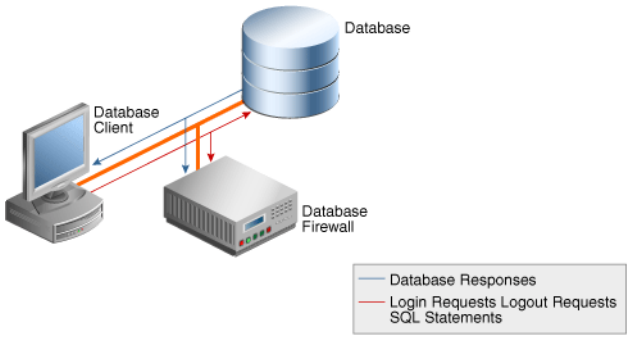
Topics

About Database Response Monitoring

Enabling the Database Response Monitoring feature allows the Database Firewall to record responses that the secured target database makes to login requests, logout requests and SQL statements sent from database clients, as shown in Figure 6–1. This feature allows you to determine whether the database executed logins, logouts and statements successfully, and can provide useful information for audit and forensic purposes.

Figure 6–1 illustrates the process flow of database response monitoring.

Figure 6–1 Database Response Monitoring



The Oracle AVDF auditor can view database responses in audit reports.

Database Response Monitoring records database responses for all SQL statements, logins, and logouts that are logged the Database Firewall policy

The information recorded includes the response interpreted by Oracle AVDF (such as "statement fail"), the detailed status information from the database, and the database response text (which may be displayed at the database client).

Configuring Database Response Monitoring

Topics

Enabling Database Response Monitoring

To enable database response monitoring for a secured target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Enforcement Points**.

   The Enforcement Points page appears, listing enforcement points and their status. You can sort or filter the list. See "Working with Lists of Objects in the UI" on page 1-14.
3. Find the enforcement point the monitors the secured target, and then click the name of that enforcement point.

   The Modify Enforcement Point page appears.
4. In the Database Response section of the page, select the **Enable Database Response** check box.

   If you also select **Full error message annotation**, any detailed error message text generated by the database is logged along with the error code.
5. Click **Save**.

Setting Up Login/Logout Policies in the Firewall Policy

The login and logout policies are stored in the Audit Vault and Database Firewall and must be configured in the firewall policy. See the *Oracle Audit Vault and Database Firewall Auditor's Guide* for details.

7

Enabling and Using Host Monitoring

Topics

About Host Monitoring

Ho st monitoring is designed for situations in which you have many small databases in a distributed environment, and you want Oracle AVDF to monitor SQL traffic to all of these databases centrally with one Database Firewall. This allows flexibility in the choice of the network point at which the traffic is monitored. For example, this is helpful in situations where it is not easy to route the traffic through a bridge or to get it from a mirror port.

The host monitor captures the SQL traffic from the network card and sends it over the network to a Database Firewall. This SQL data is then available for reports generated by Oracle AVDF. Host monitoring is used only for monitoring SQL traffic (DAM mode) and cannot be used to block or substitute SQL statements.

To use host monitoring, you deploy the Audit Vault Agent on the host machine that you want to deploy the host monitor on, usually the same machine as the database. For larger databases, the SQL traffic captured by a host monitor will increase network traffic. In this case, you can install the host monitoring software onto a server that is different from the database server. Then you must use a spanning port to connect this database server to the server used for the host monitor.

You can use one Database Firewall to monitor multiple secured target databases on the same host using one host monitor installation. To do this, you create an enforcement point in DAM mode, and a `NETWORK` audit trail, for each secured target.

To monitor all network traffic for a secured target, the Oracle AVDF auditor must select a firewall policy that will log events, for example, **Log Unique**. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for instructions.

Host monitoring is supported on Linux and Windows platforms, and can monitor any database supported by the Database Firewall. See Table B–1 on page B-2 for supported databases.

Installing and Enabling Host Monitoring

Topics

Prerequisites for Host Monitoring

The host monitor runs on Linux and Windows x86-64 platforms. The host monitor is not supported on 32-bit platforms. For additional details and the latest supported platform matrix, see **Article 1536380.1** at the Oracle Support website: `https://support.oracle.com`

The host machine on which the host monitor will run must have the following (these may be in any of the system default directories such as `/usr/lib`, `/lib`, or `/lib64` on a linux system):

- OpenSSL - Full version (not "Light"). See `http://www.openssl.org/`.
  - For Windows: OpenSSL 1.0.1c or higher
  - For Linux: OpenSSL 0.9.8i or higher
- **For Linux hosts:** The `libpcap` library, version 0.9.4 or higher. See `http://www.tcpdump.org/`. Install the following packages on the host computer:
  - `libpcap`
  - `libpcap-devel`

  For example, on an Oracle Linux system execute the following command as `root`:

  ```
  yum -y install libpcap libpcap-devel
  ```
- **For Windows hosts:** The `wincap` library, version 4.1.2 or higher. See `http://www.winpcap.org/`.

Step 1: Register the Computer that will Run the Host Monitor

To register a host in the Audit Vault Server, see "Registering Hosts in the Audit Vault Server" on page 5-1.

Step 2: Deploy the Audit Vault Agent and Install the Host Monitor

Topics

Deploying the Agent and Host Monitor on Windows Hosts

For Windows hosts, the host monitor is automatically installed when the Audit Vault Agent is deployed. See "Deploying the Audit Vault Agent on the Host Computer" on page 5-3.

See also: "Registering or Unregistering the Audit Vault Agent as a Windows Service" on page 5-5.

Deploying the Agent and Host Monitor on Linux Hosts

Follow one of the procedures below depending on which version of Oracle AVDF you have installed:

- Installing a Host Monitor in Oracle AVDF 12.1.2 on Linux Hosts
- Installing a Host Monitor in Oracle AVDF 12.1.1 on Linux Hosts

Installing a Host Monitor in Oracle AVDF 12.1.2 on Linux Hosts

To install the Host Monitor:

1. If you have not already done so, deploy the Audit Vault Agent. See "Deploying the Audit Vault Agent on the Host Computer" on page 5-3.
2. Log in as `root` and identify a `root`-owned directory on the local hard disk, such as `/usr/local`, where you will install the host monitor.

   Note: The entire directory hierarchy must be `root`-owned, and must not contain any directories with write permission for other users or group.
3. Log in to the Audit Vault Server console as an administrator, click the **Hosts** tab, and then click **Agent**.
4. Click the **Download** button next to `Host Monitor (Linux x86-64)`, and then save the `.zip` file to the `root`-owned directory (on the local hard disk) you identified in Step 2, for example `/usr/local`.
5. As `root` user, unzip the host monitor file.

   This creates a directory named `hm`. This is your *`HM_Home`* directory, which in this example is `/usr/local/hm`.
6. Ensure that the `hostmonsetup` file (in the `hm` directory) has **execute** permission.
7. Run the following command:

   `HM_Home``/hostmonsetup install agenthome=`*`Agent_Home`* `agentuser=`*`Agent_Username`* `agentgroup=`*`Agent_Group`*

   - *`HM_Home`* - The directory created in Step 5.
   - *`Agent_Home`* - Enter the Audit Vault Agent installation directory.
   - *`Agent_Username`* - Enter the username of the user who installed the Audit Vault Agent (the user who executed the `java -jar agent.jar` command).
   - *`Agent_Group`* - Enter the group to which the *`Agent_Username`* belongs.

Installing a Host Monitor in Oracle AVDF 12.1.1 on Linux Hosts

To install the Host Monitor:

1. If you have not already done so, deploy the Audit Vault Agent. See "Deploying and Activating the Audit Vault Agent on Host Computers" on page 5-2.

2. Log in as `root` and identify a `root`-owned directory on the local hard disk, such as `/usr/local`, where you will install the host monitor.
3. Copy the two host monitor `.zip` files from the *`Agent_Home`*`/stage/plugins` directory, for example:

   ```
   agent-linux-x86-64-deps.zip
   agent-linux-x86-64-hmon.zip
   ```

   The file names should match your supported Linux platform.
4. Place the copied files in the `root`-owned directory (on the local hard disk) that you identified in Step 2, and unzip them.

   This creates a directory named `hm`. This is your *`HM_Home`* directory, which in this example is `/usr/local/hm`.
5. Ensure that the `hostmonsetup` file permissions include **execute**.
6. Run the following command:

   `HM_Home``/hostmonsetup install agenthome=`*`Agent_Home`*

Step 3: Create a Secured Target for the Host-Monitored Database

To create a secured target, see "Registering or Removing Secured Targets in the Audit Vault Server" on page 6-2.

Step 4: Create an Enforcement Point in DAM Mode

You must create an enforcement point in the Audit Vault Server for each database that you will monitor remotely with a host monitor. This enforcement point must use **Database Activity Monitoring (DAM)** as the **Monitoring Mode**. See "Configuring Enforcement Points" on page 6-13.

Step 5: Create a NETWORK Audit Trail

Create an audit trail for each secured target you are monitoring with a host monitor, specifying the following:

- For **Audit Trail Type**, select `NETWORK`.
- (AVDF 12.1.1 only) For **Trail Location**, enter `NETWORK`.

For instructions for adding audit trails see "Adding an Audit Trail in the Audit Vault Server" on page 6-8.

Starting, Stopping, and Other Host Monitor Operations

Topics

Starting the Host Monitor

Starting the host monitor consists of starting collection for the NETWORK audit trail on the host you are monitoring.

To start the host monitor from the Audit Vault Server console:

1. Log in to the Audit Vault Server console as an administrator.
2. Start the audit trail(s) you created for host monitoring in "Step 5: Create a NETWORK Audit Trail" on page 7-4.

   See "Stopping and Starting Audit Trails in the Audit Vault Server" on page 6-9.

Stopping the Host Monitor

To stop the host monitor, stop the audit trail you created for the secured target that is being monitored. See "Stopping and Starting Audit Trails in the Audit Vault Server" on page 6-9.

Changing the Logging Level for a Host Monitor

See "Changing the Logging Level for the Audit Vault Agent" on page 5-8.

Checking the Status of a Host Monitor Audit Trail

To check the status of a host monitor:

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Audit Trails**.

   The collection status of a host monitor audit trail is listed in the Audit Trails page. A host monitor audit trail has `NETWORK` in the **Audit Trail Type** column.

Uninstalling the Host Monitor (Linux Hosts Only)

This procedure applies to Linux hosts only. There is no install or uninstall for Windows hosts.

Uninstalling Host Monitor Versions 12.1.1 BP2 and Later

To uninstall a host monitor:

1. Log in to the host computer as `root`.
2. From the *`HM_Home`* directory (where you installed the host monitor in Step 7 on page 7-3) run the following command:

   ```
   hostmonsetup uninstall
   ```

Uninstalling Host Monitor Versions 12.1.1 BP1 and Earlier

To uninstall a host monitor:

1. Log in to the host computer as `root`.
2. From the *`Agent_Home`*`/bin/` directory run the following command:

   ```
   hostmonsetup uninstall
   ```

Updating the Host Monitor (Linux Hosts Only)

As of Oracle AVDF 12.1.2, when you update the Audit Vault Server to a future release, the host monitor is automatically updated.

If your current release is prior to 12.1.2, refer to the README included with upgrade software or patch updates for instructions on how to update the host monitor.

Information on downloading upgrade software is detailed in *Oracle Audit Vault and Database Firewall Installation Guide*.

Using Certificate-based Authentication for the Host Monitor

By default, the Database Firewall allows the host monitor connection based on verifying the host's (originating) IP address.

If you want the additional security of using certificate-based authentication for the host monitor, follow these procedures after the host monitor is installed:

- Requiring a Signed Certificate for Host Monitor Connections to the Firewall
- Getting a Signed Certificate from the Audit Vault Server

Requiring a Signed Certificate for Host Monitor Connections to the Firewall

To require a signed certificate for host monitor connections:

1. Stop the host monitor if it is running.

   See "Stopping the Host Monitor" on page 7-5.

2. At the Database Firewall, log in as `root`, and run the following commands:

   ```
   cp /usr/local/dbfw/etc/controller.crt /usr/local/dbfw/etc/fw_ca.crt
   chown dbfw:dbfw /usr/local/dbfw/etc/fw_ca.crt
   chmod 400 /usr/local/dbfw/etc/fw_ca.crt
   ```

3. Run the following command to restart the monitor process:

   ```
   /etc/init.d/monitor restart
   ```

Getting a Signed Certificate from the Audit Vault Server

Follow this procedure for each host running host monitor. The host monitor should already be installed.

To get a signed certificate from the Audit Vault Server:

1. Log in to the Audit Vault Server as `root`.
2. Go to the directory `/usr/local/dbfw/etc`.
3. Run the following two commands:

   ```
   openssl genrsa -out hmprivkey.perm 2048
   openssl req -new -key hmprivkey.perm -out hmcsr.csr -subj "/CN=Hostmonior_Cert_
   hostname/"
   ```

   The *hostname* is the name of the host machine where the Audit Vault Agent is installed.

4. To generate one signed certificate, run the following command:

   ```
   /usr/local/dbfw/bin/generate_casigned_hmcert.sh
   ```

The signed certificate file `hmcert.crt` is generated in the directory `/usr/local/dbfw/etc`.

5. Copy the following files from the Audit Vault Server to the *Agent_Home*`/hm` directory on the host machine where the Audit Vault Agent is installed:

   ```
   /usr/local/dbfw/etc/hmcert.crt
   /usr/local/dbfw/etc/hmprivkey.perm
   ```

6. (Linux Hosts Only) As `root`, run the following commands:

   ```
   chown root:root Agent_Home/hm/hmcert.crt Agent_Home/hm/hmprivkey.perm
   chmod 400 Agent_Home/hm/hmcert.crt Agent_Home/hm/hmprivkey.perm
   ```

7. (Windows Hosts Only) Ensure that the files `hmcert.crt` and `hmprivkey.perm` have Agent user ownership and appropriate permissions to prevent unwanted user access.
8. Start the host monitor to capture network traffic. See "Starting the Host Monitor" on page 7-5.
9. Repeat this procedure for every host running host monitor.

8

Configuring High Availability

Topics

About High Availability Configurations in Oracle AVDF

You can configure pairs of Database Firewalls or pairs of Audit Vault Servers, or both, to provide a high-availability system architecture. These are known as **resilient pairs**. For the Database Firewall, the resilient pair configuration described in this chapter applies to Database Activity Monitoring (DAM) mode only. See "The Database Firewall" on page 1-6 for more information on DAM and DPE (Database Policy Enforcement) modes.

In a resilient pair of Audit Vault Servers, the primary Audit Vault Server performs all server functions. Audit and configuration data are copied from the primary to the secondary Audit Vault Server. The UI is not available on the secondary Audit Vault Server, so if you attempt to access the UI on the secondary server, you will be redirected to the UI on the primary server.

In a resilient pair of Database Firewalls, both primary and secondary Database Firewalls:

- Receive the same span traffic
- Have the same configuration (which the Audit Vault Server synchronizes). This is the configuration of secured targets, enforcement points, policies, and other monitoring settings, not the Database Firewall's system configuration (which is set on the system page of the Database Firewall console, and is not synchronized).
- Create log files according to the policy applied
- Send out alerts to the Audit Vault Server. The Audit Vault Server then sends only the alerts from the primary Database Firewall.

The Audit Vault Server collects traffic logs from the primary Database Firewall. If there is a time gap in the audit data from the primary Database Firewall, possibly due to a reboot of this Database Firewall, then the Audit Vault Server collects traffic log files from the secondary Database Firewall. The Audit Vault Server then deletes all the traffic log files from both Database Firewalls.

The Audit Vault Server controls the state of the resilient pair of Database Firewalls. There is no communication between Database Firewalls in a resilient pair. If the Audit Vault Server is unable to contact the primary Database Firewall for an extended period

of time, the Audit Vault Server collects the log files from the secondary Database Firewall and promotes the secondary Database Firewall to be the primary (so the new primary firewall starts sending out real-time alerts).

Figure 8–1 shows a pair of Database Firewalls being used to protect a single database.

Figure 8–1 A High Availability Pair of Database Firewalls Protecting a Single Secured Target

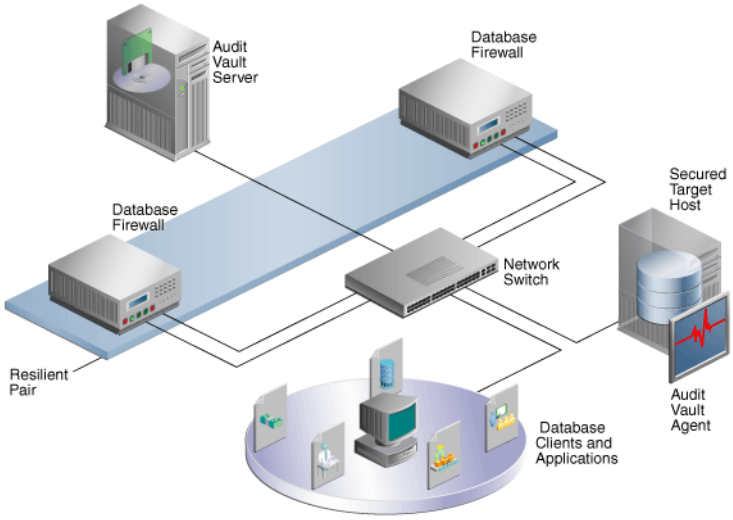
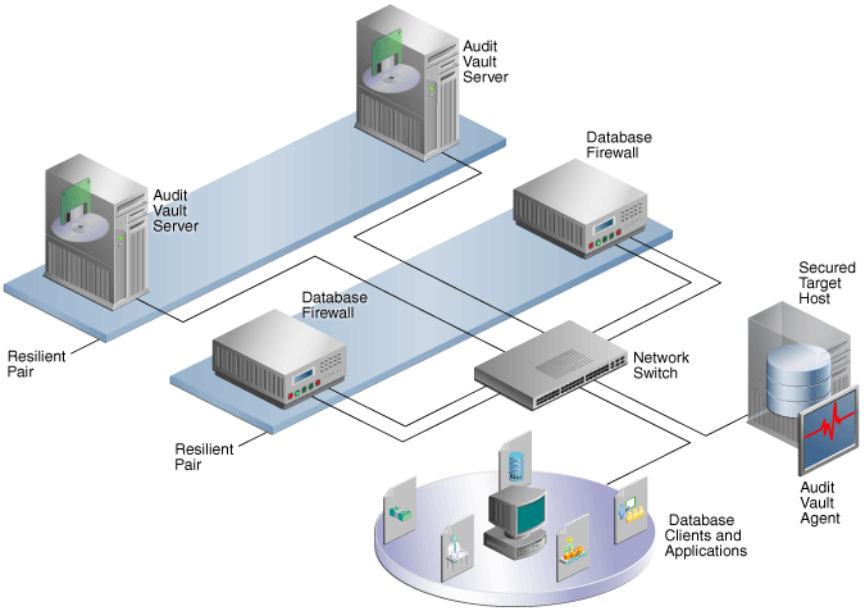


Figure 8–2 shows a pair of Audit Vault Servers and a pair of Database Firewalls in high availability mode.

Figure 8–2 Pairs of Audit Vault Servers and Database Firewalls in High Availability Mode



Configuring a Resilient Pair of Audit Vault Servers

Topics

About Pairing Audit Vault Servers

When you pair two Audit Vault Servers, designating one as the primary and the other as the secondary server, all data and configuration in the primary server (with the exception of network settings) is automatically copied to, and thereafter synchronized with, the secondary server.

After configuring the resilient pair of Audit Vault Servers, do all configuration tasks on the primary server only. This includes tasks such as deploying the Audit Vault Agent, setting up secured targets and hosts, and adding Database Firewalls and enforcement points.

Remember that if you are deploying Database Firewalls, and you configure a resilient pair of Audit Vault Servers, you must provide the server certificate and IP address of both the primary and secondary Audit Vault Server to each Database Firewall. See "Specifying the Audit Vault Server Certificate and IP Address" on page 4-4 for instructions.

If you have deployed Audit Vault Agents before pairing Audit Vault Servers, you should manually update those agents after pairing. See "Updating Audit Vault Agents After Pairing Audit Vault Servers" on page 8-5.

See also: "Handling a Failover of the Audit Vault Server Pair" on page 8-6.

Prerequisites for Configuring a Resilient Pair of Audit Vault Servers

The following are prerequisites for configuring a pair of Audit Vault Servers:

- Ensure that both the primary and secondary Audit Vault Servers have the same amount of disk space.
- Do the initial system configuration tasks for both primary and secondary Audit Vault Servers. See "Specifying Initial System Settings and Options (Required)" on page 3-2.

Step 1: Configure the Secondary Audit Vault Server

In this procedure, the secondary or standby server is called Server2, and the primary server is called Server1.

To configure Server2, the secondary server:

1. Copy the server certificate from Server1 (the primary):

a. Log in to Server1 as an administrator.

b. In the **Settings** tab of Server1, from the **Security** menu, click **Certificate**.

c. Copy the certificate.

2. In another browser window, log in to Server2 as a super administrator.
3. In the Server2 console, click the **Settings** tab.
4. From the **System** menu, select **High Availability**.
5. In the **Peer System IP Address** field, enter the IP address of Server1.
6. In the **Peer System Certificate** field, paste the certificate of Server1.
7. Click **Save**.

Step 2: Configure the Primary Audit Vault Server

In this procedure, the primary server is called Server1, and the secondary or standby server is called Server2.

To configure Server1, the primary server:

1. Copy the server certificate from Server2 (the secondary):

   a. Log in to Server2 as an administrator.

   b. In the **Settings** tab of Server1, from the **Security** menu, click **Certificate**.

   c. Copy the certificate.

2. In another browser window, log in to Server1 as a super administrator.
3. In the Server1 console, click the **Settings** tab.
4. From the **System** menu, select **High Availability**.
5. Select the checkbox **Configure this system as the Primary server**.
6. In the **Peer System IP Address** field, enter the IP address of Server2.
7. In the **Peer System Certificate** field, paste the certificate of Server2.
8. Click **Save**.

   When you are ready to start the pairing of Server1 and Server2, go to "Step 3: Start High Availability Pairing of the Audit Vault Servers" on page 8-4.

Step 3: Start High Availability Pairing of the Audit Vault Servers

You initiate high availability pairing at the primary server (Server1). This will take a few minutes, and once it is complete, the secondary server will no longer have a console UI.

Note: After completing this procedure, do all configuration tasks on the primary server only. This includes tasks such as deploying the Audit Vault Agent, setting up secured targets and hosts, and adding Database Firewalls and enforcement points. The console UI of Server2 (the standby) will be unavailable and you will be redirected to Server1.

To initiate high availability pairing at the primary server (Server1):

1. Log in to Server1 as a super administrator.
2. In the Server1 console, click the **Settings** tab.

3. From the **System** menu, click **High Availability**.
4. Be sure the checkbox **Configure this system as the Primary server** is selected.
5. Click **Save**.
6. Click **Make Primary**.

   The embedded Oracle Database is restarted and the console UI is temporarily unavailable. After this process is complete, this Audit Vault Server becomes the primary server.
7. If you deployed Audit Vault Agents before doing this procedure, manually update those agents. See "Updating Audit Vault Agents After Pairing Audit Vault Servers" on page 8-5.

   This step is necessary in order for those Audit Vault Agents to be recognized in the event of a failover.

Checking the High Availability Status of an Audit Vault Server

To check the high availability status of an Audit Vault Server:

1. In the Audit Vault Server console, click the **Settings** tab.
2. From the **System** menu, click **Status**.

   Check the **High Availability Status**. The values are:

   - **Standalone** - This server has no partner server.
   - **Primary** - This server is currently the primary server.
   - **Role Conflict** - This primary server has failed over and can no longer be used to collect data.

   To see the IP address and certificate of the other (peer) server in a paired system, in the **System** menu, click **High Availability**.

Updating Audit Vault Agents After Pairing Audit Vault Servers

In a high availability pair of Audit Vault Servers, the secondary server becomes the primary in the event of a failover. If you deployed Audit Vault Agents before you did the high availability pairing of the Audit Vault Servers, after a failover, the agent status in the new primary server is `UNREACHABLE`. To avoid this scenario, manually update previously deployed Audit Vault Agents after pairing Audit Vault Servers.

To manually update an Audit Vault Agent after pairing Audit Vault Servers:

1. On the host machine, kill the agent process:

   ```
   kill -9 agent_process_id
   ```
2. Remove the file `agent.lck` in the directory *`Agent_Home`*`/av/conf`.
3. Download the new `agent.jar` from the new primary Audit Vault Server, and copy it to the *`Agent_Home`* directory on the host machine.
4. In the *`Agent_Home`* directory run:

   ```
   java-jar agent.jar
   ```
5. Restart your audit trails.

Handling a Failover of the Audit Vault Server Pair

During normal operation, the system periodically checks the availability of the primary Audit Vault Server in the resilient pair. If the primary Audit Vault Server becomes unavailable, the system automatically fails over to the secondary Audit Vault Server after a 10 minute delay. The delay prevents a failover due to a reboot of the primary server.

In the event of a failover, the secondary server becomes a standalone Audit Vault Server. You must do the following to configure this standalone serve, and repeat the high availability pairing:

1. On the standalone server, configure the network and services settings (for example DNS settings). See "Specifying the Audit Vault Server System Settings" on page 3-3.
2. On the standalone server, manually mount any remote filesystems (NFS shares) defined as archive locations, using this AVCLI command:

   ```
   ALTER REMOTE FILESYSTEM filesystem_name MOUNT
   ```

   See "ALTER REMOTE FILESYSTEM" on page A-43 for details.
3. Disconnect the failed server and replace it. The replacement server can now be configured as the new secondary server.
4. Follow the configuration steps again to pair the two Audit Vault Servers. See "Configuring a Resilient Pair of Audit Vault Servers" on page 8-3.

Configuring a Resilient Pair of Database Firewalls

Topics

About Configuring a Resilient Pair of Database Firewalls

The procedure described here applies to a Database Firewall in DAM mode only.

Prerequisites

- Before you designate two Database Firewalls as a resilient pair, do the initial configuration tasks for each of them. See "Configuring the Database Firewall" on page 4-1.
- There must be no enforcement points configured on either of the Database Firewalls that you plan to pair. Be sure to delete all enforcement points on both Database Firewalls before creating a resilient pair.

If You Configure a Resilient Pair of Audit Vault Servers

If you have also configured a resilient pair of Audit Vault Servers, remember you must provide each Audit Vault Server's IP address and certificate to each Database Firewall in your system. See "Specifying the Audit Vault Server Certificate and IP Address" on page 4-4.

Configuring a Resilient Pair of Database Firewalls

To configure a resilient pair of Database Firewalls:

1. Log in to the Audit Vault Server console as an administrator.

   If you have defined a resilient pair of Audit Vault Servers, use the primary server's console.

2. Select the **Firewalls** tab.
3. In the **Firewalls** menu, select **Resilient Pair**.
4. In the **Primary** and **Secondary** fields, select the primary and secondary firewalls you want to use in this pair.

Swapping Roles in a Resilient Pair of Database Firewalls

Follow this procedure if you need to switch the roles of the primary and secondary Database Firewalls in a resilient pair.

To swap the roles of a resilient pair of Database Firewalls:

1. Log in to the Audit Vault Server console as an administrator.

   If you have defined a resilient pair of Audit Vault Servers, use the primary server's console.

2. Select the **Firewalls** tab.
3. In the **Firewalls** menu, select **Resilient Pair**.
4. Select the resilient pair you want, and then click **Swap**.

Breaking (Un-pairing) a Resilient Pair of Database Firewalls

Use this procedure if you need to break (or un-pair) a resilient pair of Database Firewalls.

To break a resilient pair of Database Firewalls:

1. Log in to the Audit Vault Server console as an administrator.

   If you have defined a resilient pair of Audit Vault Servers, use the primary server's console.

2. Select the **Firewalls** tab.
3. In the **Firewalls** menu, select **Resilient Pair**.
4. Select the resilient pair you want, and then click **Break**.

9

Configuring Integration with BIG-IP ASM

Topics

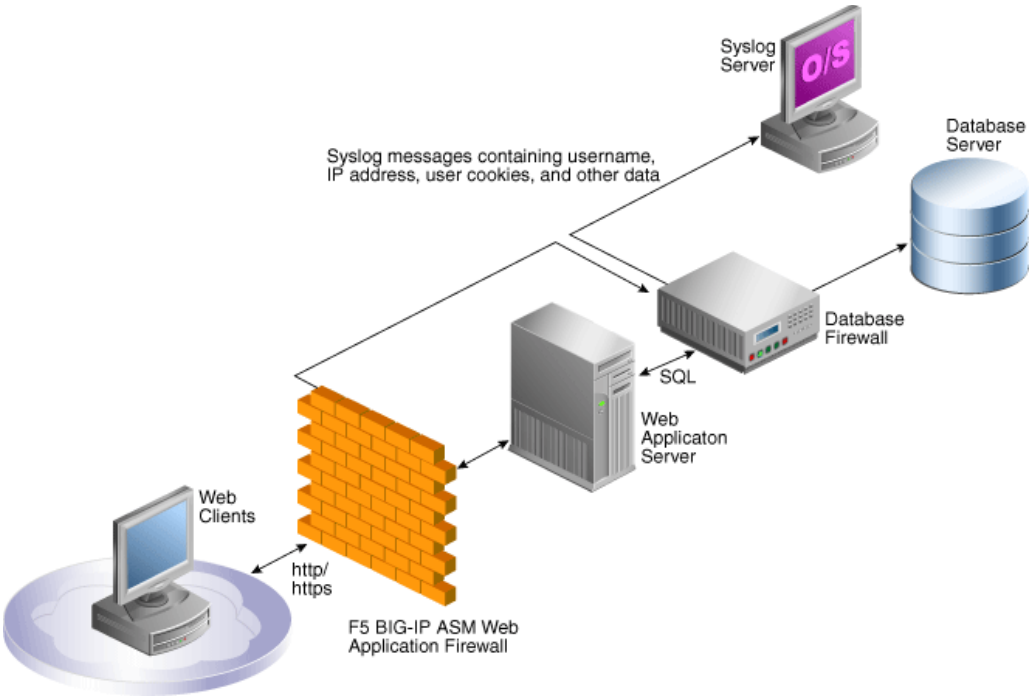
About the Integration of Oracle AVDF with BIG-IP ASM

This chapter discusses integration of Audit Vault and Database Firewall (Oracle AVDF), BIG-IP Application Security Manager (ASM), Web clients, and the Web application server, how the integration works, and its key benefits.

BIG-IP Application Security Manager (ASM), from F5 Networks, Inc., is an advanced Web Application Firewall (WAF) that provides comprehensive edge-of-network protection against a wide range of Web-based attacks.

BIG-IP ASM is deployed between the Web clients and the Web application server, see Figure 9–1. It analyzes each HTTP and HTTPS request, and blocks potential attacks before they reach the Web application server. BIG-IP ASM can be installed on a wide range of BIG-IP platforms, see "Deploying the Oracle AVDF and BIG-IP ASM Integration" on page 9-3.

Figure 9–1 Oracle AVDF with F5 BIG-IP ASM Data Flow Unit



The Database Firewall is deployed between the Web application server and database. It provides protection against attacks originating from inside or outside the network and works by analyzing the intent of the SQL statements sent to the database. It is not dependent on recognizing the syntax of known security threats, and can therefore block previously unseen attacks, including those targeted against an organization.

A deployment that includes both BIG-IP ASM and the Database Firewall provides all the security benefits of both products and enables the two systems to work in partnership to reach unparalleled levels of data security.

A key benefit of the integration is that it allows BIG-IP ASM to pass to the Database Firewall additional information about the SQL statements sent to the database, including the Web user name and 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.

The information obtained from BIG-IP ASM, and from the Database Firewall system itself, is logged by the Database Firewall as attributes of the appropriate statements. Once the data has been logged, it can be retrieved in views of the traffic logs to give complete visibility into the source and nature of any attacks.

Summary of Key Benefits

The key benefits of this integration are:

- Improves security through a partnership of the two systems.
- Allows Oracle AVDF to provide detailed information about the origin and context of the SQL statements from the Web application layer.
- Enables Oracle AVDF to act as a log store for data generated by BIG-IP ASM.
- Provides layered security at the edge of the network, and close to the database.

How the Integration Works

The integration works by using a syslog messaging system to deliver alerts from BIG-IP ASM. Standard BIG-IP ASM syslog messages enabled through the ASM logging profile provide details of each alert, such as the secured target client's IP address and other attributes of the session.

A BIG-IP ASM iRule™ is set up, which generates a syslog message during a user login to provide the Web username. Oracle AVDF provides a sample iRule, which must be customized to match the specific login procedures of the Web application. See "Developing a BIG-IP ASM iRule" on page 9-6.

During the deployment procedure, BIG-IP ASM is set up to route all its syslog messages to Oracle AVDF. Oracle AVDF attempts to match each relevant BIG-IP ASM syslog message with the appropriate SQL statements generated by the Web application server. If a match is found, it extracts the information contained in the BIG-IP ASM syslog message, and stores that information as attributes of the logged SQL statements. If a match is not found, a separate record is added to the traffic log, containing the attributes from the syslog message.

The software uses cookies to match SQL statements with Web users. When the user logs in, BIG-IP ASM assigns a unique cookie to that user (normally the cookie's name starts with "TS"). The cookie and the name of the user is sent to Oracle AVDF by a syslog message generated by the iRule on the ASM. If the user's actions cause an alert or other event, BIG-IP ASM generates an additional syslog message containing the same identifying cookie, which enables the software to match the syslog message with the specific user. Since the Oracle AVDF system is also able to match syslog messages with SQL statements, this enables individual SQL statements relating to potential threats to be attributed to specific Web users.

Oracle AVDF can automatically relay all syslog messages received from BIG-IP ASM to an external syslog server, up to a maximum size of 2KB each. If required, syslog messages generated by Oracle AVDF itself can be routed to the same destination. Oracle AVDF does not alter the BIG-IP ASM syslog traffic in any way.

Oracle AVDF monitors the status of the connection to BIG-IP ASM, and generates syslog messages every two minutes if the connection is not present or has been lost.

Deploying the Oracle AVDF and BIG-IP ASM Integration

Topics

About the Deployment

Deploying BIG-IP ASM with Oracle AVDF requires the configuration of a few straightforward settings in both systems, and the customization of an iRule so that it matches the Web application's configuration.

System Requirements

The integration requires:

- Oracle AVDF
- F5 BIG-IP ASM versions 9.4.5, 10, or 11. Other F5 products, such as FirePass®, BIG-IP LTM™, BIG-IP GTM™, WebAccelerator™ or WANJet® are not currently supported.

Visit the F5 Web site for the latest information on BIG-IP ASM: `http://www.f5.com/`

Configuring Oracle AVDF to Work with F5

You can configure Oracle AVDF to operate with F5 BIG-IP ASM only after you have configured the enforcement point for the secured target.

To configure Oracle AVDF to operate with F5 BIG-IP ASM for a secured target:

1. Ensure that an enforcement point has been defined for this secured target.

   See "Configuring Enforcement Points" on page 6-13.

2. Log in to the Audit Vault Server console as an administrator.
3. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Enforcement Points**.
4. Click the name of the enforcement point that monitors this secured target.
5. Click **Advanced**.
6. Complete the options:
   - **System Address:** This read-only information shows the IP address of the Database Firewall associated with this enforcement point. BIG-IP ASM must send syslog messages to this address and port.
   - **WAF Addresses:** Delete the word `DISABLED`, and enter the IP address of each BIG-IP ASM system that generates syslog messages to send to the Database Firewall. Separate each IP address with a space character.
   - **Disable WAF Alert Forwarding:** Select this check box to stop the Database Firewall from forwarding syslog messages. The current status of alert forwarding is displayed below this option.
   - **Destination Host** and **Dest Port:** Specify the IP address and port number of the syslog server that is to receive the BIG-IP ASM syslog messages forwarded by the Database Firewall. The Database Firewall relays these messages unmodified.

     The IP address does not need to be the same as the syslog destination used for syslog messages generated by the Database Firewall itself.
   - **Enhance reports with WAF logging data:** Select this check box to enable the Database Firewall to record BIG-IP ASM attributes obtained from the syslog messages, such as the IP address and name of the Web application user. If this box is not checked, the Database Firewall will not attempt to match F5 and Database Firewall SQL messages.
   - **Cookie Prefixes:** F5 adds cookies, with a standard prefix, to the pages it serves up. If necessary change the prefix of these cookies in this field. The Database Firewall searches for cookies with this prefix.

- **Session Idle Timeout:** The user's cookie is stored only for the length of time specified in this field. This enables the same cookie to be used by different users, providing the time period specified here has elapsed.
- **Exclude Addresses:** You can specify a list of IP addresses of Web application servers or other SQL-generating sources to ignore for reporting purposes. For example, you may want to add the IP address of an internal Web application server.

Configuring BIG-IP ASM

This section describes how to create the logging profile and write policy settings:

- Logging Profile
- Policy Settings

Logging Profile

Configure the Web application's logging profile to send BIG-IP ASM syslog messages to Oracle AVDF. Use Server IP and Server Port, for example 5514, to specify the IP address of the Database Firewall (this is the same IP address used to connect to the firewall's Administration console). Select TCP for the Protocol.

The Selected Items box must include the following attributes:

- `violations`
- `unit_hostname`
- `management_ip_address`
- `policy_name`
- `policy_apply_date`
- `x_forwarded_for_header_value`
- `support_id`
- `request_blocked` for F5 v9, or `request_status` for F5 v10 and v11
- `response_code`
- `method`
- `protocol`
- `uri`
- `query_string`
- `ip` for F5 v9, or `ip_client` for F5 v10 and v11
- `web_application_name` (`http_class_name` for F5 v11.2)
- `request`

> **Note:** The attributes must appear in the Selected Items box in the order shown here.

Policy Settings

In the policy settings, enable the required events to send through the syslog (refer to the ASM help if you are not sure how to do this).

Oracle AVDF recognizes the following events:

- Evasion technique detected
- Request length exceeds defined buffer size
- Illegal dynamic parameter value
- Illegal meta character in header
- Illegal meta character in parameter value
- Illegal parameter data type
- Illegal parameter numeric value
- Illegal parameter value length
- Illegal query string or POST data
- Illegal static parameter value
- Parameter value does not comply with regular expression
- Attack signature detected
- Illegal HTTP status in response

Developing a BIG-IP ASM iRule

Optionally, an iRule can be used to monitor the login page and generate a syslog message each time a user logs into the Web application. The syslog message contains the username of the Web application user, and the cookies associated with that user. The message is routed to the Database Firewall, which logs the username against SQL statements generated by the Web application server.

The sample iRule provided with Oracle AVDF contains the required format of the syslog message, but must be customized to handle the specific login requirements of your Web application.

```
# F5 BIG-IP example iRule
# Description: Capture username and cookies from user login to web application
#
# Global variable definitions and other initialisation logic goes here
when RULE_INIT {
        ### Customise this to suit your application
        # The page that user logins from
        set ::login_page "/login.asp"
        # The name of the field holding the user name
        set ::login_parameter_name "Uname"
        # The method of authentiaction which will be sent to  Oracle Database
Firewall
        set ::auth_method "webforms"
        # HTTP protocol methods that is used by the login form
        set ::login_method "POST"
        ### Don't change these
        # Limit the length of the HTTP request for safety
        set ::max_header_content_length 5242880
        # Log iRule trace messages to /var/log/ltm? 1=yes, 0=no
        # Must be set to 0 for production systems
        set ::payload_debug 0
}
# HTTP request received, check if it's a login request and start assembling the
# data
when HTTP_REQUEST {
```

```
        # Log the debug message if trace is enabled
        if {$::payload_debug}{log local3. "[IP::client_addr]:[TCP::client_port]:
                New HTTP
        [HTTP::method] request to [HTTP::host][HTTP::uri]"}
        # Reset cookies to empty, later used as an indicator of the fact that
        # login HTTP
        request has been received
        set cookie_all ""
        # If the request is to the login page populate cookie_all variable with
        # all the cookies received
        if {[HTTP::path] starts_with $::login_page and [HTTP::method] eq
                $::login_method}
        {
                set cookie_name [HTTP::cookie names]
        for {set c 0}{$c < [HTTP::cookie count]}{incr c}{
                set cookie_string [split [lindex $cookie_name $c] " "]
                set cookie_list $cookie_string=[HTTP::cookie [lindex
                $cookie_string 0]]
                append cookie_all "," $cookie_list
        }
        # Log the debug message if trace is enabled
        if {$::payload_debug}{log local3. "[IP::client_addr]:[TCP::client_port]:

        Matched path and method check"}
        # Validate the Content-Length value and set the content_length variable
        if {[HTTP::header value Content-Length] > $::max_header_content_length }
            {set content_length $::max_header_content_length
        } else {
        set content_length [HTTP::header value Content-Length]
        }
        # Get the payload data
        if {$content_length > 0}{
        HTTP::collect $content_length
        # Log the debug message if trace is enabled
        if {$::payload_debug}{log local3.
        "[IP::client_addr]:[TCP::client_port]: Collecting $content_length
        bytes"}
}
       }
}
# Got the data, parse them and generate the syslog message
when HTTP_REQUEST_DATA {
        # If cookies are present this is a login request, get the user name
        if {$cookie_all != "" } {
                # Log the debug message if trace is enabled
                if {$::payload_debug}{log local3. "[IP::client_addr]:
                        [TCP::client_port]:
        Collected request data: [HTTP::payload]"}
        # Reset the error flag to 0
        set uname_logged 0
        # Find the $::login_parameter_name among the parameters in the request and
        extrat its value
        set param_value_pairs [split [HTTP::payload] "&"]
        for {set i 0} {$i < [llength $param_value_pairs]} {incr i} {
                set params [split [lindex $param_value_pairs $i] "="]
                if { [lindex $params 0] equals $::login_parameter_name } {
                        # User name was found, generate the syslog message
                        # which includes IP, port, all the cookies, user name and
                        # the auth_method string
                        set username [lindex $params 1]
```

```
                        log local3. "DBFIREWALL:CLIENT=[IP::client_
                             addr]:[TCP::client_port]$cookie_all,
                             USERNAME=$username,AUTHMETHOD=$::auth_method"
                        # Set the flag so not to trigger the error reporting log
                        message below
                        set uname_logged 1
                        break
                }
        }
        # If user name has not been found in parameters log an error
        if {$uname_logged == 0 } {
                log local0. "ERROR: iRule failed to extract user name from
                page $login_page with parameter $login_parameter_name"
       }
}
}
```

Required Syslog Message Format

The required format of the syslog message to be generated by the custom iRule is as follows:

```
Rule [iRuleName] HTTP_REQUEST_DATA:
DBFIREWALL:CLIENT=[ClientIPAddress]:[ClientPort],[Cookies],
USERNAME=[Name],AUTHMETHOD=[AuthMethod]
```

In this specification:

- [*iRuleName*] is the name of the `iRule`.
- [*ClientIPAddress*] is the secured target IP address of the Web client.
- [*ClientPort*] is the secured target port number of the Web client.
- [*Cookies*] is a list of cookies available from the BIG-IP ASM HTTP object.
- [*Name*] is the user name.
- [*AuthMethod*] is the method of authentication used between the F5 Web server and its Web clients, as set up in BIG-IP ASM. Oracle AVDF does not use this information, other than to report the authentication method used.

  For example:

  ```
  Rule capture_login_rule HTTP_REQUEST_DATA:
  DBFIREWALL:CLIENT=192.0.2.1:443,ASPSESSIONIDSASSBSCD=1234,TS10da7b=23545,
    USERNAME=FredBloggs,AUTHMETHOD=webforms
  ```

Configuring syslog-ng.conf

To enable the iRule syslog messages to be transmitted to Oracle AVDF, it is necessary to log in to the BIG-IP hardware platform and execute the BIG-IP ASM commands listed below for the version you are using. Doing so modifies `/etc/syslog-ng/syslog-ng.conf` (do not modify the file directly, because changes will not persist after you restart the system).

For BIG-IP ASM Version 11

To configure `syslog-ng.conf`:

1. Run this command:

   ```
   modify sys syslog remote-servers add {dbfw_server_name {host dbfw_IP_address
   remote-port dbfw_port}}
   ```

Where *dbfw_server_name* is the name of your Database Firewall server, and *dbfw_IP_address* and *dbfw_port* are the IP address and port number of the Database Firewall. For example:

```
modify sys syslog remote-servers add { d_dbfw {host 192.0.2.181 remote-port
5514}}
```

2. Save the system configuration:

```
save sys config
```

For All Other Supported BIG-IP ASM Versions

To configure `syslog-ng.conf`, run this command:

```
bigpipe syslog include "destination d_dbfw { tcp(\"dbfw_ip_address\" port(dbfw_
port));};log { source(local); filter(f_local3); destination(d_dbfw);};"
```

Where *dbfw_ip_address* and *dbfw_port* are the IP address and port number of the Database Firewall (the value entered for **System Address** in Step 6 on page 9-4).

For example (the IP address and port will be different for each enforcement point):

```
bigpipe syslog include "destination d_dbfw { tcp(\"192.0.2.181\" port(5514));};log
{ source(local); filter(f_local3); destination(d_dbfw);};"
```

The two instances of the syslog destination name (`d_dbfw`) need to be changed only in the unlikely event that the destination name is already in use.

Viewing F5 Data in Oracle AVDF Reports

You can generate several reports from the Audit Vault Server console. These reports are listed in the Database Firewall F5 Reports table in the *Oracle Audit Vault and Database Firewall Auditor's Guide*.

10

Configuring Integration with ArcSight SIEM

Topics

How Oracle AVDF Integrates with HP ArcSight SIEM

The HP ArcSight Security Information Event Management (SIEM) system is a centralized system for logging, analyzing, and managing messages from different sources. The Audit Vault Server forwards messages to ArcSight SIEM from both the Audit Vault Server and Database Firewall components of Oracle AVDF.

You do not need to install additional software if you want to integrate ArcSight SIEM with Oracle AVDF. You configure the integration by using the Audit Vault Server console.

Messages sent to the ArcSight SIEM Server are independent of any other messages that may be sent from Oracle AVDF. This means you can send standard syslog messages to a different destination.

Oracle AVDF categorizes the messages that can be sent to ArcSight SIEM. There are three categories:

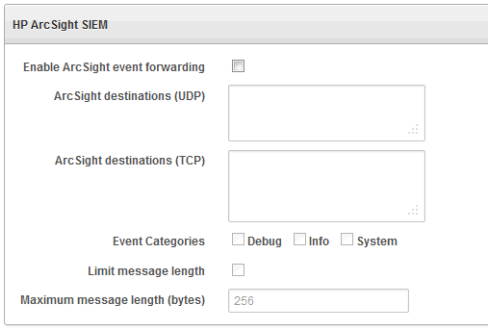
- **System** - syslog messages from subcomponents of the Audit Vault Server and Database Firewall components of Oracle AVDF
- **Info** - specific change logging from the Database Firewall component of Oracle AVDF
- **Debug** - a category that should only be used under the direction of Oracle Support

Enabling the HP ArcSight SIEM Integration

When you enable the ArcSight SIEM integration, the settings take effect immediately. You do not need to restart the Audit Vault Server.

To enable ArcSight SIEM integration:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. From the **System** menu, click **Connectors**, and scroll down to the **HP ArcSight SIEM** section.



4. Specify the following:
   - **Enable ArcSight event forwarding:** Select this check box to enable ArcSight SIEM integration.
   - **ArcSight destinations:** Depending on the communications protocol you are using, enter the IP address or host name of the ArcSight server in the **UDP** field, or its IP address, host name, and port in the **TCP** field. This setting enables the syslog log output to be sent to this ArcSight server in Common Event Format (CEF).
   - **Event categories:** Select any combination of message categories depending on which type of messages that are needed in the ArcSight server.
   - **Limit message length:** You can choose to limit the message to a specified number of bytes.
   - **Maximum message length (bytes):** If you selected **Limit message length**, enter the maximum length that you want. The range allowed is 1024 to 1048576 characters.
5. Click **Save**.

Part II

General Administration Tasks

Part II assumes that you have completed the steps in Part I to configure your Audit Vault and Database Firewall system. This part covers general administrative tasks.

This part contains the following chapters:

11

Managing User Accounts and Access

Topics

About Oracle AVDF Administrative Accounts

When administrators log in to Oracle Audit Vault and Database Firewall, they have access only to administrative functions, whereas auditors have access only to the auditing functions.

Oracle AVDF has three types of administrative user accounts:

- **Audit Vault Server Super Administrator:**
  - Manages system-wide settings
  - Creates user accounts for super administrators and administrators
  - Has access to all secured targets and secured target groups
  - Grants access to secured targets or secured target groups to administrators
- **Audit Vault Server Administrator:** Has access to specific secured targets or secured target groups granted by a super administrator. Administrators cannot manage system-wide settings.
- **Database Firewall Administrator:** Has access to the Database Firewall administrative interface.

After installing Oracle AVDF, a post-installation configuration page lets you create and specify passwords for one super administrator account and one super auditor account for the Audit Vault Server, and one administrator account for the Database Firewall.

Thereafter, the Audit Vault Server super administrator can create other administrative users, and the super auditor can create other auditor users, for the server.

The Database Firewall has only one administrator. See *Oracle Audit Vault and Database Firewall Installation Guide* for information on post-installation configuration.

This chapter describes managing user accounts and passwords for the Oracle AVDF administrator user interfaces. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for information on managing auditor accounts.

Configuring Administrative Accounts for the Audit Vault Server

Topics

Guidelines for Securing the Oracle AVDF User Accounts

As a best practice, you should use the installed Audit Vault and Database Firewall user accounts only as back-up accounts. Add new user accounts, with unique user names and passwords, for the users who are responsible for the day-to-day Oracle AVDF operations.

Note: Audit Vault and Database Firewall does not accept user names with quotation marks. For example, "jsmith" would not be a valid user name for an Oracle AVDF user account, or an account created on a secured target for use by Oracle AVDF.

Creating Administrative Accounts for the Audit Vault Server

Audit Vault Server super administrators can create both super administrator and administrator user accounts.

To create an administrative account in the Audit Vault Server:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.

   The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.
3. Click **Create**.
4. Enter the **User Name** and **Password**, and re-type the password in the appropriate fields.

   Note that Oracle AVDF does not accept user names with quotation marks, such as "jsmith".
5. In the **Type** drop-down list, select **Admin** or **Super Admin**.

   See "About Oracle AVDF Administrative Accounts" on page 11-1 for an explanation of these roles.
6. Click **Save**.

   The new user is listed in the Manage Admins page.

Changing a User Account Type for the Audit Vault Server

You can change an administrative account type from administrator to super administrator, or vice versa.

Note that if you change a user's account type from administrator to super administrator, that user will have access to all secured targets and secured target groups.

To change a user account type in Oracle AVDF:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.

   The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.
3. Click the name of the user account you want to change.
4. In the Modify Admin page, in the **Type** section, click **Change**.
5. In the **Type** drop-down list, select the new administrator type.
6. If you changed the type from **Super Admin** to **Admin**, grant or revoke access to any secured targets or groups as necessary for this user:
   a. Select the secured targets or groups to which you want to grant or revoke access.
   b. Click **Grant Access** or **Revoke Access**.

      A check mark indicates access granted. An X indicates access revoked.
   c. Repeat steps a and b if necessary.
7. Click **Save**.

Deleting an Audit Vault Server Administrator Account

To delete an Audit Vault Server administrator user account:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.

   The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.
3. Select the users you want to delete, and then click **Delete**.

Managing User Access to Secured Targets or Groups

Topics

About Managing User Access

Super administrators have access to all secured targets and secured target groups, and can grant access to specific targets and groups to administrators.

You can control access to secured targets or groups in two ways:

- Modify a secured target or group to grant or revoke access for one or more users.

- Modify a user account to grant or revoke access to one or more secured targets or groups.

Controlling Access by User

To control which secured targets or groups are accessible by a user:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.

   The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.
3. Click the name of the user account you want to modify.

   The Modify Admin page appears.
4. In the Targets and Groups section, select the secured targets or secured target groups to which you want to grant or revoke access for this user.
5. Click **Grant Access** or **Revoke Access**.

   A check mark indicates access granted. An "x" indicates access revoked.
6. If necessary, repeat steps 4 and 5.
7. Click **Save**.

Controlling Access by Secured Target or Group

To control which users have access to a secured target or group:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **Manage Access**.
3. Click the name of the secured target or secured target group for which you want to define access rights.

   The Modify Access for... page appears, listing user access rights to this secured target or group. Super administrators have access by default.
4. In the Modify Access page, select the users for which you want to grant or revoke access to this secured target or group.
5. Click **Grant Access** or **Revoke Access**.

   A check mark indicates access granted. An "x" indicates access revoked.
6. If necessary, repeat steps 4 and 5.
7. Click **Save**.

Changing User Passwords in Oracle AVDF

Topics

Recommended Password Guidelines

You should have a policy in place for changing passwords for the Audit Vault and Database Firewall user accounts. For example, you may require that users change their passwords on a regular basis, such as every 120 days, and that they create passwords that are not easily guessed.

Passwords need not be unique; however, Oracle recommends that passwords:

- Have at least one uppercase alphabetic, one alphabetic, one numeric, and one special character (plus sign, comma, period, or underscore).
- Be between 8 and 30 characters long.
- Be composed of the following characters:
  - Lowercase letters: a-z.
  - Uppercase letters: A-Z.
  - Digits: 0-9.
  - Punctuation marks: comma (,), period (.), plus sign (+), colon(:), and underscore (_).
- Not be the same as the user name.
- Not be an Oracle reserved word.
- Not be an obvious word (such as welcome, account, database, and user).
- Not contain any repeating characters.

Changing the Audit Vault Server Administrator User Password

To change your Audit Vault Server user password:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and then click **Change Password**.
3. Type your **Current Password**, **New Password**, and then re-type the new password in the appropriate fields.

   Check the "Recommended Password Guidelines" on page 11-5.
4. Click **Save**.

Changing the Database Firewall Administrator Password

To change the Database Firewall administrator Password:

1. Log in to the Database Firewall.

   See "Logging in to the Database Firewall Console UI" on page 1-15.
2. In the **Users** menu, click **List**.
3. In the Users List, click the user name whose password you want to change.
4. Enter and confirm your new password in the **Password** and **Password Confirmation** fields.
5. In the **User Password** field, enter your old password (the one you are changing).
6. Click **Save**.

12

Managing the Audit Vault Server and Database Firewalls

This section describes managing day-to-day Audit Vault Server and Database Firewall operations once the initial configuration is completed.

Topics

Managing Audit Vault Server Settings, Status, and Maintenance Operations

Topics

Checking Server Status and System Operation

To check the Audit Vault Server status:

1. Log in to the Audit Vault Server as an Administrator.
2. Click the **Settings** tab.
3. In the **System** menu, click **Status**.

   Server statistics, processes, and network services and connections are displayed.
4. Optionally, click the **Test Diagnostics** button to perform a series of diagnostic checks.

   These diagnostics include testing:

   - Existence and access permissions of configuration files
   - File system sanity
   - Network configuration
   - Status of various process that are required to run on the system, for example, database server process(es), event collection process, Java framework process, HTTP server process, etc.

   After the system completes the diagnostic tests, it displays a report listing the results of each test.

Accessing the Audit Vault Server Certificate and Public Key

Topics

Accessing the Server Certificate

If you have deployed Database Firewalls, you must provide the Audit Vault Server certificate and IP address to each Database Firewall.

To access the server certificate:

1. Log in to the Audit Vault Server console as an Administrator.
2. Click the **Settings** tab.
3. In the **Security** menu, click **Certificate**.

   The server's certificate is displayed. You can copy the certificate and provide it to each Database Firewall. See "Specifying the Audit Vault Server Certificate and IP Address" on page 4-4.

Accessing the Server Public Key

You must provide the server's public key to another system in order to upload archive files from the Audit Vault Server to that system. This public key must be added to the `authorized_keys` file for that system. For a typical linux installation, this file is in the user's home directory under `.ssh`, and its permissions must be set to 0700.

To access the server public key:

1. Log in to the Audit Vault Server console as an Administrator.
2. Click the **Settings** tab.

3. In the **Archiving** menu, click **Manage Archive Locations**, and then click **Create**.

   The **Public Key** field contains the public key. You can copy the key and paste it into the appropriate file on another system.

Rebooting or Powering Off the Audit Vault Server

To reboot or power off the Audit Vault Server:

1. Log in to the Audit Vault Server as super Administrator.
2. Click the **Settings** tab, and in the **System** menu, click **Manage**.
3. Click **Reboot** or **Power Off**.

Changing the Keyboard Layout

To change the keyboard layout used in the Audit Vault Server:

1. Log in to the Audit Vault Server console as a super Administrator.
2. Click the **Settings** tab, and in the **System** menu, click **Manage**.
3. From the **Keyboard** drop-down list, select the keyboard you want.
4. Click **Save**.

Downloading Diagnostics for the Audit Vault Server (AVDF 12.1.2)

This procedure lets you download diagnostics for the Audit Vault Server. If you want to see diagnostics for a database firewall, see "Viewing the Status and Diagnostics Report for a Database Firewall" on page 4-7.

You can adjust the amount of diagnostics information gathered by setting the `LOGLEVEL` for different server components using the `ALTER SYSTEM` command. See "ALTER SYSTEM SET" on page A-45 for details.

To download a log file for Audit Vault Server diagnostics:

1. Log in to the Audit Vault Server console as a super Administrator.
2. Click the **Settings** tab, and in the **System** menu, click **Status**.
3. Click the **Download Diagnostics** button, select a file location, and then click **Save**.

   A diagnostics log file (`.zip`) is downloaded to the location you selected.

See also: "Viewing the Status and Diagnostics Report for a Database Firewall" on page 4-7.

Archiving and Restoring Audit Data

Topics

Starting an Archive Job

When an Oracle AVDF auditor selects a retention (archiving) policy for a secured target, audit data for that secured targets will be available for archive jobs according to

the **Months Online** specified in the retention policy. After the months online period has expired, the data is available for archiving, and is no longer visible in reports.

To start an archive job, you must have configured at least one archive location. See "Defining Archiving Locations" on page 3-8.

For more information, see "About Archiving and Restoring Data in Oracle AVDF" on page 3-7.

To start an archive job:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and from the **Archiving** menu, click **Archive**.
3. Complete the following fields:
   - **Job Name:** Enter a name for the archive job.
   - **Archive Location:** Select the archive location.

     If you have not created archiving locations, see "Defining Archiving Locations" on page 3-8.
4. Select the files you want to archive.

   The files listed are those for which the Months Online period has expired according to the secured target's retention policy.
5. Click the **Archive** button.

You can view the progress of an archive job from the **Jobs** page (from the **System** menu in the **Settings** tab). See "Monitoring Jobs" on page 12-5.

Restoring Oracle AVDF Audit Data

You can restore data files for a specific secured target and time range. The **Months Archived** value in a secured targets retention (archiving) policy determines how long the secured target's data is available to restore to the Audit Vault Server. When the Months Archived period expires, the data is no longer available to restore, however, it continues to reside in the archive location.

For more information, see "Creating Archiving (Retention) Policies" on page 3-9, and "About Archiving and Restoring Data in Oracle AVDF" on page 3-7.

To restore data files from an archive:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and from the **Archiving** menu, click **Restore**.
3. In the **Job Name** field, enter a name for this restore job.
4. Select the **Secured Target** whose data you want to restore, and a **Start Date** and **End Date** for the data to be restored.

   The start and end dates are associated with the event time (the time the event occurred).
5. Click the **Restore** button.

   You can check the status of the restore job in the **Jobs** page (from the **System** menu in the **Settings** tab). When the restored data files are available, they are listed in the Restored Datafiles section of the Restore From Archive page, and the data will be visible in reports.

6. To purge restored files when no longer needed, from the Restored Datafiles section of the page, select the files you want to unload from the system, and then click the **Release** button.

   Once the release is successful, the data is not visible in reports.

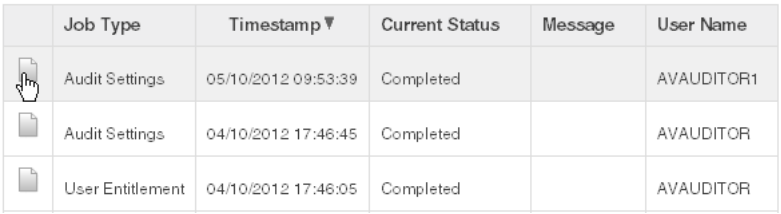
Monitoring Jobs

You can see the status of various jobs that run on the Audit Vault Server, such as report generation, and user entitlement or audit policy retrieval from secured targets.

To see the status of jobs on the Audit Vault Server:

1. Log in to the Audit Vault Server as an Administrator.
2. Click the **Settings** tab.
3. In the **System** menu, click **Jobs**.

   A list of jobs is displayed, showing the job type, ID, timestamp, status, and associated user name.
4. To see details for an individual job, click the icon to the left of that job.



	Job Type	Timestamp ▼	Current Status	Message	User Name
	Audit Settings	05/10/2012 09:53:39	Completed		AVAUDITOR1
	Audit Settings	04/10/2012 17:46:45	Completed		AVAUDITOR
	User Entitlement	04/10/2012 17:46:05	Completed		AVAUDITOR

Changing the Audit Vault Server's Network or Services Configuration

To set or change the network or services configuration, follow the relevant procedure below:

- "Setting or Changing the Audit Vault Server Network Configuration" on page 3-3
- "Configuring or Changing the Audit Vault Server Services" on page 3-4

Managing Server Connectors for Email, Syslog, and Arcsight SIEM

To set or change connector information, follow the relevant procedure below:

- "Configuring the Email Notification Service" on page 3-6
- "Configuring the Audit Vault Server Syslog Destinations" on page 3-5
- "Enabling the HP ArcSight SIEM Integration" on page 10-1

Managing Plug-ins

You can deploy additional plug-ins to support more types of secured targets, or un-deploy plug-ins that are no longer needed. See "Deploying Plug-ins and Registering Plug-in Hosts" on page 5-9 for details.

Monitoring the Server Tablespace Space Usage

The Audit Vault Server database contains the SYSAUX tablespace, which by default has one data file. The SYSAUX tablespace is a locally managed tablespace with automatic segment space management.

You should monitor the space usage for the SYSAUX tablespace and create additional data files for storage as needed.

See *Oracle Database Administrator's Guide* for more information about the ALTER TABLESPACE SQL statement, which you can use to add more storage data files. For information about optimizing a tablespace, see *Oracle Database Performance Tuning Guide*.

Monitoring the Server Archive Log Disk Space Usage

By default, ARCHIVELOG mode is enabled in the Audit Vault Server database. The ARCHIVELOG mode copies filled online redo logs to disk. This enables you to back up the database while it is open and being accessed by users, and to recover the database to any desired point in time. You should monitor the disk space usage for the redo logs.

See *Oracle Database Administrator's Guide* for more information about changing the LOG_ARCHIVE_DEST_*n* location to relocate these archive log files to larger disks. For information about backing up the archive logs, see *Oracle Database Backup and Recovery Advanced User's Guide*.

Monitoring the Server Flash Recovery Area

By default, the Audit Vault Server database has the following initialization parameter settings:

- The DB_RECOVERY_FILE_DEST_SIZE initialization parameter is set to 2 GB.
- The DB_RECOVERY_FILE_DEST initialization parameter is set to the default flash recovery area, typically the *ORACLE_HOME/flash_recovery_area* directory.

Ensure that the size of the flash recovery area is large enough to hold a copy of all data files, all incremental backups, online redo logs, archived redo logs not yet backed up on tape, control files, and control file auto backups. This space can fill up quickly, depending on the number of audit trails configured, the scope of the audit record collection being administered, and the backup and archive plans that you have in place.

You can use Oracle Enterprise Manager Database Control to monitor the available space in the flash recovery area. Monitor the percent space that is usable in the Usable Flash Recovery Area field under the High Availability section on the Home page. Check the alert log in the Database Console for messages. When the used space in the flash recovery area reaches 85 percent, a warning message is sent to the alert log. When the used space in the flash recovery area reaches 97 percent, a critical warning message is sent to the alert log.

You can manage space in the flash recovery area by adjusting the retention policy for data files to keep fewer copies or reduce the number of days these files stay in the recovery window. Alternatively, increase the value of the DB_RECOVERY_FILE_DEST_SIZE initialization parameter to accommodate these files and to set the DB_RECOVERY_FILE_DEST initialization parameter to a value where more disk space is available. See *Oracle Database Administrator's Guide* and *Oracle Database Backup and Recovery Basics* for more information.

Downloading and Using the AVCLI Command Line Interface

Topics

About the AVCLI Command Line Interface

As an alternative to using the Audit Vault Server console (Web) UI, you can use the AVCLI command line interface to manage Oracle AVDF, including registering and configuring secured targets and their connections to the Audit Vault Server.

You can run AVCLI from the Audit Vault Server, or download the AVCLI utility from the Audit Vault Server and install and run the utility on another computer.

The syntax used for AVCLI is similar to SQL*Plus. For example, from within AVCLI, you can use the `CONNECT` command to log in as another user. In addition, the AVCLI commands are not case sensitive. In this manual, the commands are entered in upper case.

See "AVCLI Commands Reference" on page A-1 for details of the available AVCLI commands.

Downloading the AVCLI Command Line Utility and Setting JAVA_HOME

The AVCLI utility is already installed on the Audit Vault Server. If you want to run AVCLI on a different computer, then you must download it from the Audit Vault Server console and install it on the other computer.

To download the AVCLI command line utility:

1. Log in to the Audit Vault Server console as an Administrator.
2. Click the **Settings** tab, and in the **System** menu, click **Manage**.
3. Click the **Download Command Line Utility** button, and save the `avcli.jar` file.
4. Copy the `avcli.jar` file to the computer from which you want to run AVCLI, and then run this command:

   ```
   java -jar avcli.jar
   ```

   The AVCLI utility is installed in the current directory with the necessary permissions. To install in a different directory, use the command:

   ```
   java -jar avcli.jar -d directory_name
   ```

5. Set the `JAVA_HOME` environment variable to point to the JDK 1.6 or 1.7 installation directory.

Starting AVCLI

You can invoke AVCLI interactively (that is, you must provide a password) with or without a user name.

Note: You must set the JAVA_HOME environment variable to point to the JDK 1.6 or 1.7 installation directory.

Starting AVCLI Interactively

Follow one of the methods below to invoke AVCLI interactively. Except for a few commands where it is optional, all AVCLI commands must end in a semi-colon (;). For simplicity, in this guide we use a semi-colon for all AVCLI commands.

Using Interactive Mode with a User Name

The command syntax for invoking AVCLI with a user name is:

```
avcli -u username
Enter password: password
```

For example:

```
avcli -u psmith
AVCLI : Release 12.1.0.0.0 - Production on timestamp
Copyright (c) 1996, 2012 Oracle.  All Rights Reserved.
Enter password for 'psmith': password

Connected to:
Oracle Audit Vault Server 12.1.0.0.0

AVCLI>
```

Using Interactive Mode Without a User Name

If you invoke AVCLI without a user name, you must connect to the Audit Vault Server as a valid user who has been granted the AV_ADMIN role. The command syntax for invoking AVCLI with a user name is:

```
avcli
AVCLI> CONNECT username;
```

For example:

```
avcli

AVCLI : Release 12.1.2.0.0 - Production on timestamp
Copyright (c) 1996, 2014 Oracle.  All Rights Reserved.

AVCLI> CONNECT psmith
Enter password: password;
Connected.
```

Running AVCLI Scripts

An AVCLI script contains a series of AVCLI commands. You can run an AVCLI script from the shell. Valid AVCLI script names have a .av extension.

Here is an example AVCLI script:

```
#Here is an AVCLI command
start collection for secured target sample_target1 using host sample_host1 from
table SYS.AUD$;
#More AVCLI commands
#Quit command
quit;
```

To run an AVCLI script from the shell, use the following syntax:

```
avcli -u username -f scriptname.av
```

For example:

```
avcli -u psmith -f myscript.av
AVCLI : Release 12.1.0.0.0 - Production on timestamp
Copyright (c) 1996, 2012 Oracle.  All Rights Reserved.
Enter password for 'psmith': password

Connected to:
Oracle Audit Vault Server 12.1.0.0.0

AVCLI> the script myscript.av executes
```

Specifying Log Levels for AVCLI

When you invoke AVCLI, you can specify the following log levels. Oracle AVDF writes the logs to the Audit Vault Server `$ORACLE_HOME/av/log` directory.

- `info`: Logs informational and error messages
- `warning`: Logs both warning and error messages
- `error`: Logs only error messages (default)
- `debug`: Logs debug, error, warning, and informational messages

To specify a log level, enter the `L` option. For example, to invoke AVCLI as user `psmith` with the log level set to `warning`:

```
avcli -l warning -u psmith
AVCLI : Release 12.1.0.0.0 - Production on timestamp
Copyright (c) 1996, 2012 Oracle.  All Rights Reserved.
Enter password for 'psmith': password

Connected to:
Oracle Audit Vault Server 12.1.0.0.0

AVCLI>
```

To invoke AVCLI using a script and with the `debug` warning level:

```
avcli -l debug -f myscript.av

AVCLI : Release 12.1.0.0.0 - Production on timestamp
Copyright (c) 1996, 2012 Oracle.  All Rights Reserved.

AVCLI> Connected.

AVCLI> the script myscript.av executes
```

Note: You must be connected as a valid user who has been granted the `AV_ADMIN` role. You can do so using the `CONNECT username/password` directive.

Displaying Help and the Version Number of AVCLI

To display the `AVCLI` help information and version number:

```
avcli -h
```

If you only want to find the version number, then use the `V` argument:

```
avcli -v
```

Downloading the Oracle AVDF SDK

An SDK is available for developing custom Oracle AVDF plug-ins. For more information, see "About Plug-ins" on page 5-9. For developer information, see *Oracle Audit Vault and Database Firewall Installation Guide*.

To download the SDK:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab, and then click **Plug-ins** (under the System subsection).
3. Click **Download SDK**.

Backing up and Restoring the Audit Vault Server

A knowledge base article is available for backing up and restoring the Audit Vault Server. Search for document number **1556200.1** at the following website:

`https://support.oracle.com`

Managing Database Firewalls

Topics

Changing the Database Firewall's Network or Services Configuration

See one of the topics below if you need to change a Database Firewall's network, traffic sources, or services configuration:

- "Configuring a Database Firewall's Network Settings" on page 4-2
- "Configuring a Database Firewall's Network Services" on page 4-2
- "Configuring Traffic Sources" on page 4-5
- "Configuring a Bridge in the Database Firewall" on page 4-6
- "Configuring a Database Firewall as a Traffic Proxy" on page 4-6

Viewing and Capturing Network Traffic in a Database Firewall

You may wish to view network traffic for debugging purposes. You can view live network traffic going through a firewall, or capture the traffic to a file (`.pcap` file type) that you can download and analyze.

To view live network traffic in a Database Firewall:

1. Log in to the Database Firewall administration console.

   See "Logging in to the Database Firewall Console UI" on page 1-15.
2. Under **Network Traffic**, click **Live Capture**.
3. In the **Level of Detail** field, select Summary or Packet Content.
4. In the **Duration** field, select the number of seconds to capture live traffic.
5. In the **Network** field, select the network traffic source for which to capture traffic.
6. Click the **Show Traffic** button.

   The live traffic is displayed for the selected duration.

To capture network traffic to a file:

1. Log in to the Database Firewall administration console.

   See "Logging in to the Database Firewall Console UI" on page 1-15.
2. Under **Network Traffic**, click **File Capture**.
3. In the **Duration** field, select the number of seconds to capture traffic.
4. In the **Network** field, select the network traffic source for which to capture traffic.
5. Click the **Capture** button.

   The traffic file (`.pcap` format) is displayed in the Network Traffic Files list.
6. Click **Download** for the file you want to download.

Rebooting or Powering Off Database Firewall

To reboot or power off a Database Firewall:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Firewalls** tab, and then select the firewall(s) you want to reboot or power off.
3. Click the **Reboot** or **Power Off** button.

Removing a Database Firewall from the Audit Vault Server

To remove a Database Firewall from the Audit Vault Server:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Firewalls** tab, and then select the firewall(s) you want to remove.
3. Click the **Delete** button.

Fetching an Updated Certificate from a Database Firewall

Starting with AVDF 12.1.2, you can update the Database Firewall certificate stored in the Audit Vault Server using the Audit Vault Server console UI. You must update this

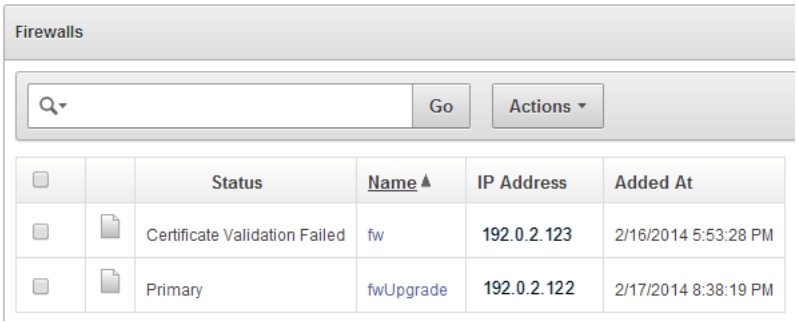
certificate when you upgrade the Database Firewall to maintain communication between the firewall and the Audit Vault Server.

If you have an earlier AVDF release, you must manually copy the Audit Vault Server certificate to the upgraded Database Firewall. See "Specifying the Audit Vault Server Certificate and IP Address" on page 4-4.

To update the Database Firewall certificate stored in the Audit Vault Server:

1. After upgrading the Database Firewall, log in to the Audit Vault Server console as an administrator.
2. Click the **Firewalls** tab.

   A list of firewalls appears.



3. Click the name of a firewall with the status Certificate Validation Failed.
4. In the Modify Firewall page, click **Update Certificate**.

Viewing Diagnostics for a Database Firewall

See this procedure for viewing Database Firewall diagnostics: "Viewing the Status and Diagnostics Report for a Database Firewall" on page 4-7.

13

Configuring a SAN Repository (AVDF 12.1.2)

Topics

About Configuring a SAN Repository

Starting in Oracle AVDF 12.1.2 you can optionally configure a SAN storage repository for these data types:

- **Event Data** - Data that is kept online in the Audit Vault Server for a specified duration according to archiving policies. After the online duration expires, this data is then archived.
- **System Data** - Data specific to the Oracle AVDF system
- **Recovery** - Recovery data for the Audit Vault Server repository

During the Audit Vault Server installation process, your server will be partitioned to store **Event**, **System**, and **Recovery** data in a way that works with the number of disk partitions you have set up on the server. Optionally, you can register SAN servers and configure your storage repository to use additional disks to store this data. See *Oracle Audit Vault and Database Firewall Installation Guide* for installation information.

About Configuring a SAN Repository in High Availability Environments

In a high availability environment, you can configure the storage repository on the secondary Audit Vault Server from the primary Audit Vault Server, using either the console UI or AVCLI commands. The primary and secondary Audit Vault Servers must not share (read or write to) the same SAN disks, and you must ensure that the secondary server has at least the same amount of space in each disk group as the primary server.

Configuring a SAN Server to Communicate with Oracle AVDF

Oracle AVDF uses Linux Open-iSCSI to communicate with SAN servers. You must ensure that the iSCSI service is enabled on the SAN server you want to use for storing AVDF data, and provide the Audit Vault Server's iSCSI initiator name to your storage administrator to use in configuring the SAN server. The SAN server must allow iSCSI

targets and LUNs (logical unit numbers) to communicate with this iSCSI initiator name. We recommend that the LUN numbers assigned to a disk should be fixed.

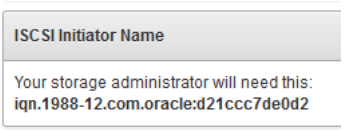
Important: Ensure that you do not have more than one target mapped to the same disk on the SAN storage server.

Some SAN servers may also require the Audit Vault Server's IP address.

To find the Audit Vault Server's iSCSI initiator name and IP address:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.

   The SAN Servers page is displayed with the ISCSI initiator name at the bottom.



   In a high availability environment, you will see two ISCSI initiator names, one for the primary Audit Vault Server and one for the secondary.
3. To find the Audit Vault Server's IP address, click the **Settings** tab, then click **Network**. The IP address is at the top of this page.

Important: Do not restart the iSCSI service on either the Audit Vault Server or the SAN server that is servicing the Audit Vault Server. If there is a need to restart either of these services, contact Oracle support.

Registering or Dropping SAN Servers in the Audit Vault Server

Topics

Registering a SAN Server

This procedure registers a SAN server in the Audit Vault Server. In a high availability environment, you can use this procedure to register a SAN server to the primary or the secondary Audit Vault Server. Note that while you can register the same SAN server to both the primary and secondary Audit Vault Servers, they must not share (read or write to) the same SAN disks.

To register a SAN server in the Audit Vault Server:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.
3. Click **Register**, and provide the following information:
   - **Register to** - (High Availability Only) Select the Primary or Secondary Audit Vault Server.

- **Storage Name** - Name for this SAN server
- **IP Address** - SAN Server IP address
- **Port** - SAN Server port
- **Method** - The data transfer method
- **Authentication** - If sendTargets is the transfer method, this specifies no authentication, or CHAP (one way). Using CHAP (one way), the Audit Vault Server is authenticated by the SAN server.

4. Click **Submit**.

Dropping a SAN Server

You can drop a SAN server if none of its disks are in use for storage in the Audit Vault Server repository. Otherwise, you must first drop the disks from any disk groups that use this SAN server. See "Dropping SAN Disks from the Audit Vault Server Repository" on page 13-6.

To drop a SAN server from the Audit Vault Server:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.
3. Select the SAN server(s) you want to drop, and then click **Drop**.

Discovering Targets on a SAN Server

Topics

About SAN Targets and Disks

Once you have registered SAN servers in the Audit Vault Server, in order to make SAN disks available for storing Audit Vault Server data, you must discover and log in to the available target(s) on the SAN server.

When you log in to a target on the SAN server, a number of storage disks are made available to the Audit Vault Server, corresponding to the number of LUNs available on the SAN server for that target.

Discovering Targets on a SAN Server and Making Disks Available

You can discover targets on a SAN server that is registered with the Audit Vault Server. See "Registering a SAN Server" on page 13-2.

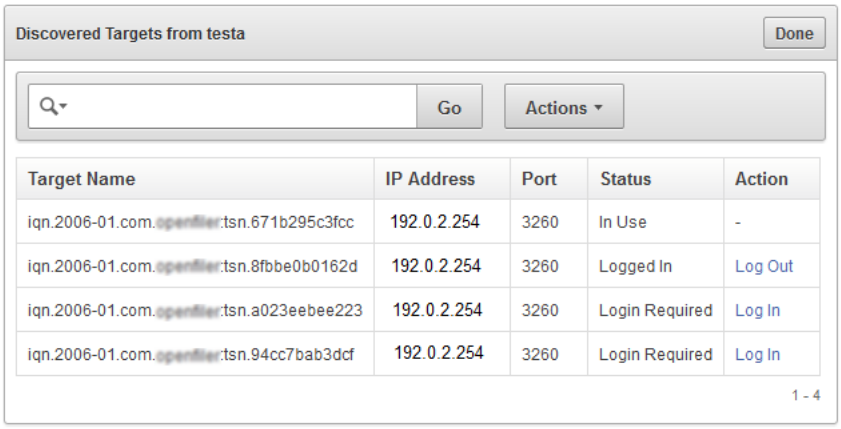
To make SAN server disks available for storing Audit Vault Server data, you must log in to a target on the SAN server, and provide login credentials if required.

To discover targets on a SAN server:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.

3. Find the SAN server you want, and then click the corresponding **Discover** link.

   A list of targets appears, showing the status of each target.



4. Click **Log In** to log in to a target on this SAN server and make its disks available for storage.

   If the SAN server is configured so that the target does not require credentials, you can leave those fields empty and click **Log in**.

Logging out of Targets on a SAN Server

You can log out of a target if none of its disk are in use for storing Audit Vault Server data. If a disk from a target is in use, you must first drop the disk(s), then log out of the target. See "Dropping SAN Disks from the Audit Vault Server Repository" on page 13-6 for instructions.

To log out of a target on a SAN server:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.
3. Find the SAN server you want, and then click the corresponding **Discover** link.

   A list of targets appears, showing the status of each target.
4. Find the target you want, and then click the corresponding **Log Out** link in the Action column.

   If there is a dash character in the Action column for the target, then disks from this target are in use.

Adding or Dropping SAN Disks in the Audit Vault Server Repository

Topics

About Disk Groups in the Audit Vault Server Repository

There are three disk groups used for storing Audit Vault Server data, corresponding to three data types:

- EVENTDATA
- SYSTEMDATA
- RECOVERY

If desired, you can add disks from a registered SAN server to the EVENTDATA, SYSTEMDATA, and RECOVERY disk groups to increase the storage capacity for those types of data. Otherwise, these data types are stored in disk partitions on the Audit Vault Server.

Adding SAN disks to these disk groups is optional. See "About Configuring a SAN Repository" on page 13-1 for more information.

In a high availability environment: You must ensure that the secondary server has at least the same amount of space in each disk group as the primary server.

Figure 13–1 shows the **Settings** > **Repository** page. In the repository shown here:

- The EVENTDATA disk group uses a SAN disk for extra storage.
- The SYSTEM DATA and RECOVERY disk groups use only the Audit Vault Server disk partitions for storage.
- For the EVENTDATA, SYSTEMDATA, and RECOVERY disk groups, the amount of free space available on the local Audit Vault Server partitions is also shown.

Figure 13–1 The Repository Page

The Repository Page in a High Availability Environment

In a high availability environment, you would see the above disk groups for the Primary Audit Vault Server, followed by the same disk groups for the Secondary Audit Vault Server. You must ensure that the secondary server has at least the same amount of space in each disk group as the primary server.

Adding SAN Disks to the Audit Vault Server Repository

You can add SAN disks that are not already in use to any of the disk groups in the repository.

To add disks to a disk group in the repository:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **Repository**.
3. Click the **Add Disk** button corresponding the disk group you want.

   Details for available disks are displayed, including disk capacity and free space.
4. Select the disk(s) you want to add to this disk group, and then click **Use Disk(s)**.
5. Click **OK** to confirm.

   The selected disk(s) are displayed under the specified disk group.

Dropping SAN Disks from the Audit Vault Server Repository

Before dropping a SAN disk, be sure that there is enough space on the remaining disks in the disk group to relocate the data from the disk you want to drop.

To drop a SAN disk from a disk group in the repository:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **Repository**.
3. Find the disk you want to drop under one of the disk groups, select the disk, and then click **Drop Disk**.
4. Click **OK** to confirm.

Part III

General Reference

Part III provides general reference information for administering the Audit Vault and Database Firewall system.

This part contains the following appendixes:

- Appendix A, "AVCLI Commands Reference"
- Appendix B, "Plug-in Reference"
- Appendix C, "REDO Logs Audit Data Collection Reference"
- Appendix D, "Ports Used by Audit Vault and Database Firewall"
- Appendix E, "Troubleshooting Oracle Audit Vault and Database Firewall"
- Appendix F, "Audit Vault Error Messages"

A

AVCLI Commands Reference

Topics

About the AVCLI Commands

You can use the `AVCLI` commands to configure host connections from the command line. You must be granted the `AV_ADMIN` role before you can run these commands. This appendix does not list all of the `AVCLI` commands, however. It only covers the commands that an Audit Vault and Database Firewall administrator needs to configure secured target connections.

All AVCLI commands must end in a semi-colon (;).

> **See:** "Using the AVCLI Command Line Interface" on page 1-16 for general usage information about using the `AVCLI` command line interface

Setting the JAVA_HOME Environment Variable

In the Audit Vault Server, you must set the `JAVA_HOME` environment variable to point to the JDK 1.6 or 1.7 installation directory.

Agent Host AVCLI Commands

The AVCLI host commands enable you to configure the host computer on which the Audit Vault Agent will reside.

Table A–1 lists the AVCLI agent host commands.

Table A–1 AVCLI Agent Host Commands

Command	Description
REGISTER HOST	Adds the host to Audit Vault Server and identifies it as a host on which an agent can be deployed
ALTER HOST	Alters a host registered with the Audit Vault Server
LIST HOST	Lists the names of the currently registered agent host computers
DROP HOST	Drops the specified agent host from Audit Vault Server
ACTIVATE HOST	Activates the host on Audit Vault Server
DEACTIVATE HOST	Deactivates the specified host

REGISTER HOST

The REGISTER HOST command adds the host to Audit Vault Server and identifies it as a host on which an agent can be deployed.

Syntax

```
REGISTER HOST host_name [WITH IP ip_address]
```

Arguments

Argument	Description
host_name	The name of the host computer that you want to register. To find the names of currently registered hosts, see "LIST HOST" on page A-4. See also "LIST ATTRIBUTE FOR SECURED TARGET" on page A-19.
ip_address	Optional. The IP ADDRESS associated with the host

Usage Notes

To change the IP address associated with a host, use the "ALTER HOST" on page A-2 command.

Examples

```
avcli> REGISTER HOST sample_host.example.com;
```

Registers the host, sample_host.example.com, to run the agent process with the Audit Vault Server.

```
avcli> REGISTER HOST sample_host.example.net with ip 192.0.2.1;
```

Registers the host, sample_host.example.net, and associates it with the IP address 192.0.2.1.

ALTER HOST

The ALTER HOST command alters a host registered with the Audit Vault Server.

Syntax

```
ALTER HOST hostname SET {key=value [,key=value...]}

ALTER HOST hostname SET {key=value [,LOGLEVEL=component_name:loglevel_value...]}
```

Arguments

Argument	Description
hostname	The name of the host.
key	The attribute being changed. See Table A–2 for supported *key* values.

Usage Notes

This command alters the attributes associated with the named host using key/value pairs. To modify multiple attributes in a single command invocation, specify comma-separated key/value pairs.

The following host name attributes are supported:

Table A–2 Host Attributes (key values)

Parameter	Description
NAME	The new host name that replaces the existing one.
IP	The new IP address that replaces the existing IP address.
LOGLEVEL	The log level of various code components running on this host. This option can dynamically change the log levels of various Audit Vault Server code components. The LOGLEVEL attribute takes a two part value, separated by a colon, as follows: *component_name*:*loglevel_value* where *component_name* can be av.agent, av.common, av.server: See Table A–3 for descriptions of LOGLEVEL component names, and Table A–4 for LOGLEVEL values. Multiple components log levels can be changed by delimiting them using the | symbol.

The following are valid values for the LOGLEVEL attribute:

Table A–3 LOGLEVEL Component Names

Parameter	Description
av.agent	agent *component_name* of LOGLEVEL value
av.server	Audit Vault Server *component_name* of LOGLEVEL value
av.common	shared Server and Agent *component_name* of LOGLEVEL value

Table A–4 LOGLEVEL Values

Loglevel Value	Description
INFO	INFO level, loglevel_value of LOGLEVEL value
WARNING	WARNING level, loglevel_value of LOGLEVEL value

Table A–4 (Cont.) LOGLEVEL Values

Loglevel Value	Description
ERROR	ERROR level, loglevel_value of LOGLEVEL value
DEBUG	DEBUG level, loglevel_value of LOGLEVEL value

Examples

```
avcli> ALTER HOST sample_host.example.com SET ip=192.0.2.1;
```

Alters the host, sample_host.example.com, and changes the associated IP address to 192.0.2.1.

```
avcli> ALTER HOST sample_host.example.com SET name=new_sample_host.example.com;
```

Alters the host, sample_host.example.com, to new_sample_host.example.com. Additionally, it updates the IP address by doing a lookup against new_sample_host.example.com.

```
avcli> ALTER HOST sample_host.example.com SET
loglevel=av.agent:info|av.common:debug;
```

Alters the log levels of the av.agent and av.common code components embedded in the agent process running on the host, sample_host.example.com.

LIST HOST

The LIST HOST command lists the names of the currently registered agent host computers.

Syntax

```
LIST HOST
```

Example

```
avcli> LIST HOST;
```

The various active hosts registered with the Audit Vault Server are listed.

DROP HOST

The DROP HOST command drops the host specified by the *host_name* from the Audit Vault Server and removes any associated metadata.

After dropping a host, if you want to register it again to collect audit data, you must reinstall the Audit Vault Agent on this host.

Syntax

```
DROP HOST hostname
```

Arguments

Argument	Description
hostname	The name of the host computer being dropped. To find the names of currently registered hosts, see "LIST HOST" on page A-4. See also "LIST ATTRIBUTE FOR SECURED TARGET" on page A-19.

Usage Notes

Ensure that the agent process on this host is in the stopped state before dropping the host. The `DROP HOST` command will fail otherwise.

Example

```
avcli> DROP HOST sample_host;
```

The host, `sample_host`, and any associated metadata is dropped.

ACTIVATE HOST

The `ACTIVATE HOST` command activates the host specified by *`hostname`*.

Syntax

`ACTIVATE HOST` *`hostname`*

Arguments

Argument	Description
hostname	The host name.

Usage Notes

Once an host is activated, an activation key appears, which must be entered when an agent process is started to complete activation process.

Example

```
avcli> ACTIVATE HOST sample_host.example.com
```

Activates the host, `sample_host.example.com`, and displays the activation key for this host.

DEACTIVATE HOST

The `DEACTIVATE HOST` command deactivates the host specified by *`hostname`*.

Syntax:

`DEACTIVATE HOST` *`hostname`*

Arguments

Argument	Description
hostname	The host name.

Usage Notes

Once a host is deactivated, it may not be able to connect to the Audit Vault Server.

Example

```
avcli> DEACTIVATE HOST sample_host.example.com;
```

Deactivates the host, `sample_host.example.com`. The agent process on this host may not be able to connect to the Audit Vault Server.

Database Firewall AVCLI Commands

The `AVCLI` Database Firewall commands enable you to configure the Database Firewall.

Table A–5 lists the `AVCLI` Database Firewall commands.

Table A–5 Database Firewall Commands

Command	Description
REGISTER FIREWALL	Registers the Database Firewall that has the specified IP address with the Audit Vault Server
DROP FIREWALL	Drops an already registered Database Firewall from the Audit Vault Server.
LIST FIREWALL	Lists all the Database Firewalls registered with the Audit Vault Server
REBOOT FIREWALL	Reboots a named Database Firewall that is already registered with the Audit Vault Server
POWEROFF FIREWALL	Powers off a named Database Firewall that is already registered with the Audit Vault Server
CREATE RESILIENT PAIR	Creates a resilient pair with two Database Firewalls for high availability
SWAP RESILIENT PAIR	Swaps Database Firewalls in a resilient pair that includes the named Database Firewall
DROP RESILIENT PAIR	Drops the resilient pair that contains the specified Database Firewall
ALTER FIREWALL	Alters the Database Firewall attributes
SHOW STATUS FOR FIREWALL	Displays the status for a particular Database Firewall

REGISTER FIREWALL

The `REGISTER FIREWALL` command registers the Database Firewall that has the specified IP address with the Audit Vault Server.

Syntax

```
REGISTER FIREWALL firewall_name WITH IP ip_address
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.
ip_address	The IP address of the Database Firewall.

Usage Notes

The Database Firewall must be installed at the given IP address location.

To specify a firewall name with white space, enclose the entire string in quotes.

Example

```
avcli> REGISTER FIREWALL sample_fw WITH IP 192.0.2.14;
```

Database Firewall `sample_fw` is installed at IP address `192.0.2.14`.

DROP FIREWALL

The `DROP FIREWALL` command drops an already registered Database Firewall from the Audit Vault Server.

Syntax

```
DROP FIREWALL firewall_name
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.

Example

```
avcli> DROP FIREWALL sample_fw;
```

The Database Firewall `sample_fw` is dropped.

LIST FIREWALL

The `LIST FIREWALL` command lists all the Database Firewalls registered with the Audit Vault Server.

Syntax

```
LIST FIREWALL
```

Example

```
avcli> LIST FIREWALL;
```

A list of the Database Firewalls registered with Audit Vault Server appears.

REBOOT FIREWALL

The `REBOOT FIREWALL` command reboots a named Database Firewall that is already registered with the Audit Vault Server.

Syntax

```
REBOOT FIREWALL firewall_name
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.

Example

```
avcli> REBOOT FIREWALL sample_fw;
```

The Database Firewall `sample_fw` reboots.

POWEROFF FIREWALL

The `POWEROFF FIREWALL` command powers off a named Database Firewall that is already registered with the Audit Vault Server.

Syntax

```
POWEROFF FIREWALL firewall_name
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.

Example

```
avcli> POWEROFF FIREWALL sample_fw;
```

The Database Firewall `sample_fw` switches off.

CREATE RESILIENT PAIR

The `CREATE RESILIENT PAIR` command creates a resilient pair with two Database Firewalls for high availability.

Syntax

```
CREATE RESILIENT PAIR FOR FIREWALL PRIMARY primary_firewall
  SECONDARY secondary_firewall
```

Arguments

Argument	Descriptions
primary_firewall	The name of the primary Database Firewall. Only this Firewall can generate syslog alerts
secondary_firewall	The name of the secondary Database Firewall.

Example

```
avcli> CREATE RESILIENT PAIR FOR FIREWALL PRIMARY sample_fw1 SECONDARY sample_fw2;
```

A resilient pair is created with primary Database Firewall `sample_fw1` and secondary Database Firewall `sample_fw2`.

SWAP RESILIENT PAIR

The `SWAP RESILIENT PAIR` command swaps Database Firewalls in a resilient pair that includes the named Database Firewall.

Syntax

```
SWAP RESILIENT PAIR HAVING FIREWALL firewall_name
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.

Example

```
avcli> SWAP RESILIENT PAIR HAVING FIREWALL sample_fw1;
```

In the existing resilient pair, Database Firewall `sample_fw1`, the primary firewall is swapped with the secondary firewall, or the reverse.

DROP RESILIENT PAIR

The `DROP RESILIENT PAIR` command drops the resilient pair that contains the specified Database Firewall.

Syntax

```
DROP RESILIENT PAIR HAVING FIREWALL firewall_name
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.

Example

```
avcli> DROP RESILIENT PAIR HAVING FIREWALL sample_fw1;
```

The existing resilient pair that includes Database Firewall `sample_fw1` is broken.

ALTER FIREWALL

The `ALTER FIREWALL` command alters the Database Firewall attributes.

Syntax

```
ALTER FIREWALL firewall_name SET attribute=value [, attribute=value]
```

Arguments

Argument	Description
firewall_name	The name of the Database Firewall.
attribute	The pair (attribute and new value) for the Database Firewall. Separate multiple pairs by a space on the command line. See Table A–6 for a list of attributes.

Usage Notes

Table A–6 lists Database Firewall attributes that you can specify for the attribute=value argument.

Table A–6 Oracle Database Firewall Attributes

Parameter	Description
`NAME`	The new name of the Database Firewall.
`IP`	The IP address of the Database Firewall.

Example

```
avcli> ALTER FIREWALL sample_fw1 SET NAME=sample_newfw1;
```

Database Firewall name changes from `sample_fw1` to `sample_newfw1`.

```
avcli> ALTER FIREWALL sample_fw1 SET IP=192.0.2.169;
```

Database Firewall IP address is set to 192.0.2.169.

SHOW STATUS FOR FIREWALL

The `SHOW STATUS` command displays the status for a particular Database Firewall.

Syntax

```
SHOW STATUS FOR FIREWALL firewall_name
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.

Example

```
avcli> SHOW STATUS FOR FIREWALL sample_fw1;
```

The running information for Database Firewall `sample_fw1` appears.

Enforcement Point AVCLI Commands

The AVCLI Enforcement Point commands enable you to configure the Database Firewall.

Table A–7 lists the AVCLI Enforcement Point commands.

Table A–7 Enforcement Point Commands

Command	Description
CREATE ENFORCEMENT POINT	Creates an enforcement point with the specified name and protects the Database Firewall using either mode DAM or DPE
DROP ENFORCEMENT POINT	Drops the enforcement point
LIST ENFORCEMENT POINT	Lists all the enforcements points associated with the Database Firewall or secured target
START ENFORCEMENT POINT	Starts an enforcement point that was previously suspended
STOP ENFORCEMENT POINT	Stops the enforcement point monitoring the secured target
ALTER ENFORCEMENT POINT	Alters the enforcement point and attributes

CREATE ENFORCEMENT POINT

The CREATE ENFORCEMENT POINT command creates an enforcement point with the specified name and protects the Database Firewall using either mode DAM or DPE.

Syntax

```
CREATE ENFORCEMENT POINT enforcement_point_name
  FOR SECURED TARGET secured_target_name
  USING FIREWALL firewall_name
  TRAFFIC SOURCE traffic_source_name
  WITH MODE DPE|DAM
```

Arguments

Argument	Descriptions
enforcement_point_name	The name of the enforcement point.
secured_target_name	The name of the secured target.
firewall_name	The name of the Database Firewall.
traffic_source_name	The name of the traffic source

Example

```
avcli> CREATE ENFORCEMENT POINT sample_ep FOR SECURED TARGET sample_source USING
  FIREWALL sample_fw TRAFFIC SOURCE sample_trafficsource WITH MODE DPE;
```

An enforcement point named sample_ep is created on Database Firewall sample_fw, using DPE mode to protect the secured target sample_source, and using the traffic source sample_trafficsource.

DROP ENFORCEMENT POINT

The DROP ENFORCEMENT POINT command drops the enforcement point.

Syntax

```
DROP ENFORCEMENT POINT enforcement_point_name
```

Arguments

Argument	Descriptions
enforcement_point_name	The name of the enforcement point.

Example

```
avcli> DROP ENFORCEMENT POINT sample_ep;
```

The enforcement point named sample_ep is dropped from the Database Firewall.

LIST ENFORCEMENT POINT

The LIST ENFORCEMENT POINT command lists all the enforcements points associated with either the Database Firewall or the secured target.

Syntax

```
LIST ENFORCEMENT POINT FOR FIREWALL firewall_name

LIST ENFORCEMENT POINT FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Descriptions
firewall_name	The name of the Database Firewall.
secured_target_name	The name of the secured target.

Example

```
avcli> LIST ENFORCEMENT POINT FOR FIREWALL sample_fw;
```

A list of all the enforcement points associated with Database Firewall sample_fw appears.

```
avcli> LIST ENFORCEMENT POINT FOR SECURED TARGET sample_source;
```

A list all the enforcement points associated with secured target sample_source appears.

START ENFORCEMENT POINT

The START ENFORCEMENT POINT command starts an enforcement point that was previously suspended.

Syntax

```
START ENFORCEMENT POINT enforcement_point_name
```

Arguments

Argument	Descriptions
enforcement_point_name	The name of the enforcement point.

Example

```
avcli> START ENFORCEMENT POINT sample_ep;
```

The enforcement point named `sample_ep` starts.

STOP ENFORCEMENT POINT

The `STOP ENFORCEMENT POINT` command stops the enforcement point monitoring the secured target.

Syntax

```
STOP ENFORCEMENT POINT enforcement_point_name
```

Arguments

Argument	Descriptions
enforcement_point_name	The name of the enforcement point.

Example

```
avcli> STOP ENFORCEMENT POINT sample_ep;
```

The enforcement point named `sample_ep` stops.

ALTER ENFORCEMENT POINT

The `ALTER ENFORCEMENT POINT` command alters the enforcement point and attributes.

Syntax

```
ALTER ENFORCEMENT POINT enforcement_point_name SET attribute=value
   [, attribute=value]
```

Arguments

Argument	Description
enforcement_point_name	The name of the enforcement point.
attribute	The pair (attribute and new value) for the enforcement point being altered. Separate multiple pairs by a space on the command line. See Table A–8 on page A-14 for enforcement point attributes.

Usage Notes

Attributes are specified by a comma-separated list of key=value/pairs. The following key values are supported:

Table A–8 Enforcement Point Attributes

Parameter	Description
TARGET	The new secured target name, which should be registered already in the Audit Vault Server, including the address.
MODE	The mode which monitors the enforcement point. Valid modes are: DAM or DPE.
PRESERVE_CONNECTION	True or False where True indicates that when the database firewall starts operating in DPE mode (either because it had been changed from DAM, or because it has restarted), any existing connections passing through the firewall are allowed to continue. This favors availability over security, because the firewall cannot enforce policy on these connections. False indicates that any preexisting connections are broken. The database firewall can then enforce the policy when clients reconnect. This is the default behavior.
TRAFFIC_SOURCE	New valid traffic sources for enforcement point.
DATABASE_RESPONSE	True or False indicates whether or not to activate database response monitoring function for enforcement point.
FULL_ERROR_MESSAGE	True or False enables this option. This starts logging the error message associated with the error code.
DATABASE_INTERROGATION	True or False enables this option. This starts the database interrogation feature for enforcement point.
HOST_MONITOR	True or False enables this option. This specifies whether or not the remote agent needs to be enabled.
HOST_MONITOR_ADDRESS	The new IP Address for Remote agent.

Examples

```
avcli> ALTER ENFORCEMENT POINT ep1 SET TARGET=newsource;
```

The enforcement point to monitor new secured target is altered.

```
avcli> ALTER ENFORCEMENT POINT ep1 SET MODE=dam;
```

The enforcement point monitoring is altered to DAM mode.

```
avcli> ALTER ENFORCEMENT POINT ep1 SET database_response=true,
  Full_error_message=true;
```

The enforcement point is altered to activate database response and log error messages associated with error codes.

```
avcli> ALTER ENFORCEMENT POINT ep1 SET database_interrogation=true;
```

The enforcement point is altered to activate direct database interrogation.

Secured Target AVCLI Commands

The AVCLI secured target commands enable you to configure both database and nondatabase secured targets for Audit Vault Server.

Table A–9 lists the AVCLI secured target commands.

Table A–9 AVCLI Secured Target Commands

Command	Description
REGISTER SECURED TARGET	Registers a secured target to be monitored by Audit Server
ALTER SECURED TARGET	Modifies the attributes of a secured target
LIST ADDRESS FOR SECURED TARGET	Lists all the addresses registered with the secured target
LIST SECURED TARGET	Lists the various active secured targets registered with the Audit Vault Server
LIST SECURED TARGET TYPE	Lists the secured target types currently registered with Audit Vault Server
LIST ATTRIBUTE FOR SECURED TARGET	Lists the attributes of a given secured target
LIST METRICS	Lists the metrics of a given secured target, such as the various trails
DROP SECURED TARGET	Removes the registration of the specified secured target from Audit Vault Server

REGISTER SECURED TARGET

The `REGISTER SECURED TARGET` command registers a secured target to be monitored by Audit Vault Server.

Syntax

```
REGISTER SECURED TARGET secured_target_name OF SECURED TARGET TYPE
   "secured_target_type" [AT location] [AUTHENTICATED BY username/password]
```

Arguments

Argument	Description
secured_target_name	Name of secured target. Must be unique.
secured_target_type	A valid secured target type, for example `"Oracle"`. To find a list of supported secured target types, see "LIST SECURED TARGET TYPE" on page A-19.
location	The secured target database connection information. Optional in Oracle AVDF 12.1.2, and can be added later using the command ALTER SECURED TARGET. The location is an opaque string that specifies how to connect to the secured target, typically a JDBC connect string. The syntax that you use depends on the secured target type. See the database-specific Usage Notes below. If location is not provided, certain features such as entitlement retrieval, audit settings management, SPA retrieval, and audit trail collection are disabled if applicable to this secured target type.

Argument	Description
user_name/*password*	Optional. Credentials to connect to the secured target. After you enter this argument and run the REGISTER SECURED TARGET command, Audit Vault Server prompts you for the user name and password of the secured target user account. For secured target databases, this account must exist on the secured target database. Optional. See the database-specific Usage Notes in the following sections.

General Examples

```
avcli> HELP REGISTER SECURED TARGET;
```

Displays detailed help for the REGISTER SECURED TARGET command.

Oracle Database Usage Notes and Examples

- For the *location* argument, enter the host name, port number, and service ID (SID), separated by a colon. Use the following syntax:

  ```
  AT host:port:service
  ```

  For example:

  ```
  Oracle Database: jdbc:oracle:thin:@//host:port/service
  ```

  If you are unsure of this connection information, then run the `lsnrctl status listener_name` command on the computer where you installed the secured target database.

- The AUTHENTICATED BY command prompts for the secured target user name and password. This user account must exist in the secured target database.

  To find this user, query the SESSION_PRIVS and SESSION_ROLES data dictionary views.

Oracle Database Examples:

```
avcli> REGISTER SECURED TARGET sample_source OF SECURED TARGET TYPE "Oracle
Database"
   AT jdbc:oracle:thin:@//anymachinename:1521/example.com
   AUTHENTICATED BY system/welcome_1;
```

Registers a Oracle secured target, sample_source, of secured target type Oracle Database, reachable using connect string jdbc:oracle:thin:@//anymachinename:1521/example.com using credentials system/welcome_1.

SQL Server Example

```
avcli> REGISTER SECURED TARGET sample_mssqldb OF SECURED TARGET TYPE "Microsoft
SQL Server" AT jdbc:av:sqlserver://hostname:port;
```

IBM DB2 Example

```
avcli> REGISTER SECURED TARGET sample_db2db OF SECURED TARGET TYPE "IBM DB2 LUW"
AT
   jdbc:av:db2://host:port;
```

Registers a DB2 secured target, `sample_db2db`, of secured target type `"IBM DB2 LUW"`, reachable using connect string `jdbc:av:db2://host:port` using credentials *sa/welcome_1*.

ALTER SECURED TARGET

The `ALTER SECURED TARGET` command modifies the attributes of a secured target.

Syntax

```
ALTER SECURED TARGET secured_target_name
   SET attribute=value [, attribute=value]

ALTER SECURED TARGET secured target name ADD ADDRESS ip:port:[service]

ALTER SECURED TARGET secured target name DROP ADDRESS ip:port:[service]
```

Arguments

Argument	Description
secured_target_name	The name of the secured target database to be modified. The name is case-sensitive. To find a list of existing secured targets, see "LIST SECURED TARGET" on page A-19.
attribute=value	The key/value pair for the secured target attributes of the secured target to be modified. You can modify one or more secured target attributes at a time using a space on the command line. See Table A–10 for secured target attributes. Some types of secured targets also require collection attributes. See "Collection Attributes" on page B-24. To find a list of attribute values for a secured target, see "LIST ATTRIBUTE FOR SECURED TARGET" on page A-19.
ip	The IP address
port	The port number
service	**REQUIRED FOR ORACLE DATABASE ONLY:** The service name or SID

Table A–10 lists secured target attributes that you can specify,

Table A–10 Secured Target Attributes

Attribute	Description
`NAME`	The name for this secured target database instance. This must not be defined already in the Audit Vault Server for another secured target.
`LOCATION`	The location of the secured target
`CREDENTIALS`	The new set of username and password pair used to connect to the secured target. This is a two part value separated by a slash (/).
`DESCRIPTION`	The description for this secured target database instance
`MAXIMUM_ ENFORCEMENT_ POINT_THREADS`	The maximum number of enforcement point threads for the secured target. The valid range is between 1 and 16 (inclusive). The default value is 1.

General Usage Examples:

```
avcli> ALTER SECURED TARGET sample_source SET name=sample_source2;
```

The secured target name of sample_source changed to sample_source2.

```
avcli> ALTER SECURED TARGET sample_source SET credentials=scott/leopard;
```

The credentials used to connect to the secured target, sample_source, are changed.

```
avcli> ALTER SECURED TARGET sample_source SET description='This is a new
description';
```

Number of enforcement point threads is set for secured target, sample_source.

```
avcli> ALTER SECURED TARGET sample_source SET maximum_enforcement_point_
threads=14;
```

The description for the secured target, sample_source, is changed.

```
avcli> ALTER SECURED TARGET sample_source ADD address 192.0.2.2:1234:srcdb;
```

New secured target address is registered with secured target sample_source.

```
avcli> ALTER SECURED TARGET sample_source DROP address 192.0.2.2:1234:srcdb;
```

Secured target address registered before with secured target, sample_source, is dropped.

```
avcli> ALTER SECURED TARGET sample_source set maximum_enforcement_point_threads =
10;
```

Sets the maximum number of enforcement point threads for secured target sample_source to 10.

Oracle Example:

```
avcli> ALTER SECURED TARGET secured target sample_source set
 location=jdbc:oracle:thin:@//new_sample_host:1521:sample_db;
```

The location of the secured target, sample_source, changes.

LIST ADDRESS FOR SECURED TARGET

The LIST ADDRESS FOR SECURED TARGET command lists all the addresses registered with the secured target.

Syntax

```
LIST ADDRESS FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Descriptions
secured_target_name	The name of the secured target.

Example

```
avcli> LIST ADDRESS FOR SECURED TARGET sample_source;
```

All the addresses for secured target, sample_source, appear.

LIST SECURED TARGET

The `LIST SECURED TARGET` command lists the active secured targets registered with the Audit Vault Server.

Syntax

```
LIST SECURED TARGET;
```

Lists the active secure targets registered with the Audit Vault Server.

LIST SECURED TARGET TYPE

The `LIST SECURED TARGET TYPE` command lists the secured target types currently supported in the Audit Vault Server.

Syntax

```
LIST SECURED TARGET TYPE
```

Examples

```
avcli> LIST SECURED TARGET TYPE;
```

Lists the secured target types currently supported in the Audit Vault Server.

LIST ATTRIBUTE FOR SECURED TARGET

The `LIST ATTRIBUTE FOR SECURED TARGET` command lists the attributes of a given secured target.

Syntax

```
LIST ATTRIBUTE FOR SECURED TARGET secured target name;
```

Arguments

Argument	Description
secured target name	The name of the secured target. To find all registered secured targets, see "LIST SECURED TARGET" on page A-19.

LIST METRICS

The `LIST METRICS` command lists the metrics of a given secured target, such as various trails.

Syntax

```
LIST METRICS FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Description
secured_target_name	The name of the secured target To find all registered secured targets, see "LIST SECURED TARGET" on page A-19.

Usage Notes

The `LIST METRICS` command has the same usage for all secured target types.

Examples

```
avcli> LIST METRICS FOR SECURED TARGET sample_source;
```

Metrics available for the secured target, `sample_source`, are listed.

DROP SECURED TARGET

The `DROP SECURED TARGET` command removes the registration of the specified secured target from Audit Vault Server.

Syntax

```
DROP SECURED TARGET secured_target_name
```

Arguments

Argument	Description
secured_target_name	The name of the secured target. To find all registered secured targets, see "LIST SECURED TARGET" on page A-19.

Usage Notes

Ensure that all trails associated with this secured target are in stopped state before dropping the secured target. Otherwise, the `DROP SECURED TARGET` command fails. See `HELP STOP COLLECTION` for an explanation of how to stop active trails.

Dropping a secured target stops the Audit Vault Server from monitoring it. Any audit data collected earlier continues to be available in the Audit Vault Server repository.

Examples

```
avcli> DROP SECURED TARGET sample_source;
```

Drops the `sample_source` secured target.

Audit Trail Collection AVCLI Commands

The `AVCLI` secured target audit trial collection commands enable you to manage the audit trail collections for the secured targets.

Table A–11 lists the `AVCLI` secured target connection commands.

Table A–11 AVCLI Secured Target Connection Commands

Command	Description
START COLLECTION FOR SECURED TARGET	Starts the collection of specified audit trail data from a given secured target
STOP COLLECTION FOR SECURED TARGET	Stops the audit trail collection
LIST TRAIL FOR SECURED TARGET	Lists the available audit trails that have been started with the `START COLLECTION` command or stopped with the `STOP COLLECTION` command

Table A–11 (Cont.) AVCLI Secured Target Connection Commands

Command	Description
DROP TRAIL FOR SECURED TARGET	Drops an audit trail

START COLLECTION FOR SECURED TARGET

The `START COLLECTION FOR SECURED TARGET` command starts the collection of specified audit trail data from a given secured target, optionally using the specified collection plug-in.

Syntax

```
START COLLECTION FOR SECURED TARGET secured_target_name USING HOST host FROM
location
   [USING PLUGIN plugin id]
```

Arguments

Argument	Description
secured_target_name	The name of the secured target whose audit trail collection you want to begin. To find all registered secured targets, see "LIST SECURED TARGET" on page A-19.
host	The name of the host where the secured target agent resides. To find a list of configured agent hosts, see "LIST HOST" on page A-4. For detailed information about a secured target, see "LIST ATTRIBUTE FOR SECURED TARGET" on page A-19.
location	The *location* is one of following: ■ DIRECTORY *directory name* / *mask* ■ TABLE *tablename* ■ SYSLOG DEFAULT | *filename* / *file mask* ■ NETWORK ■ EVENT LOG *eventlog_name* ■ TRANSACTION LOG ■ CUSTOM *name*
plugin id	The collection plug-in id being used. Required if there is more than one possible plug-in. Optional if there is only one plug-in. To find a list of existing plug-ins for the type, see "LIST PLUGIN FOR SECURED TARGET TYPE" on page A-48.

General Usage Notes

To start the trail, the agent process which manages the trail should also be in running state. If the collection process connects to the secured target, the secured target must up and running. When multiple plug-ins can process audit data from a secured target, use the optional `USING PLUGIN` directive to disambiguate the collection process.

A trail starts in the START_REQUESTED state and transitions to a starting state, followed by a running state. If there is no outstanding audit data to process from the given trail, the collection process switches to an idle state. The current state can be viewed using the LIST TRAIL command.

If a trail must be authenticated, the Audit Vault Server uses the credentials provided in the AUTHENTICATED BY argument of the REGISTER SECURED TARGET command. (See "REGISTER SECURED TARGET" on page A-15.)

After you run the START COLLECTION command, the Audit Vault Server begins to collect audit data from the configured secured targets. If you want to stop the collection, then run the STOP COLLECTION command, described in "STOP COLLECTION FOR SECURED TARGET" on page A-24.

Windows Systems Usage Notes

On Windows systems, enter directory and file name locations in either double-quoted strings or as a nonquoted string using forward slashes. For example:

```
... FROM DIRECTORY "c:\app\oracle\product\11.1\av";

... FROM DIRECTORY c:/app/oracle/product/11.1/av;
```

General Examples

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM
   directory/opt/audit_trail;
```

Audit data collection from trail /opt/audit_trail for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM TABLE
sys.aud$;
```

Audit data collection from table trail sys.aud$ for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM
syslog
   /usr/syslog/syslog*;
```

Collecting syslog trail /usr/syslog/syslog* for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM event
  log application;
```

Collecting application event log trail for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo
  FROM transaction log;
```

Collecting transaction log trails for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo
  FROM TABLE sys.aud$ USING PLUGIN com.sample_plugin;
```

Audit data collection from table trail sys.aud$ for the secured target sample_source, using the com.sample_plugin, plug-in starts.

Oracle Database Secured Target Usage Notes

Audit Trail Settings

For the operating system type of audit trail, use the following settings:

Type of Audit Trail	trail_type Setting	audit_trail Setting
Operating system directory	DIRECTORY	*directory_location*
Syslog file	SYSLOG	*file_name*
Windows event log	EVENTLOG	n/a

SQL Server Secured Target Usage Notes

Audit Trail Settings

You can write the SQL Server audit trail to the Windows event log, C2 trace files, or server side trace files. The FROM *trail_type audit_trail* arguments are as follows:

Type of Audit Trail	trail_type Setting	audit_trail Setting
Windows event log	EVENTLOG	n/a
C2 trace file	DIRECTORY	*file_wildcard*
Server-side trace files	DIRECTORY	*file_wildcard*
SQLAUDIT files	DIRECTORY	*file_wildcard*

Sybase ASE Secured Target Usage Notes and Examples

For the Sybase ASE audit trail, set the *trail_type audit_trail* setting to TABLE SYSAUDITS.

Sybase ASE Example

```
avcli> START COLLECTION FOR SECURED TARGET hr_syb_db USING HOST sybserver
FROM TABLE SYSAUDITS;
```

MySQL Usage Notes

The trail *location* is the path to the directory where converted XML files are created by running the MySQL XML transformation utility. See "(Required for MySQL) Running the XML Transformation Utility" on page 6-10.

IBM DB2 Usage Notes and Examples

For the IBM DB2 audit trail, set the *trail_type audit_trail* setting to DIRECTORY *directory_location*.

IBM DB2 Example

```
avcli> START COLLECTION FOR SECURED TARGET hr_db2_db USING HOST db2server
FROM DIRECTORY "d:\temp\trace";
```

Oracle Solaris Secured Target Usage Notes

For an Oracle Solaris secured target, the trail *location* used in this command must be in the format:

hostname:*path_to_trail*

where *hostname* matches the hostname in the audit log names, which look like this:

```
timestamp1.timestamp2.hostname
```

Windows Secured Target Usage Notes

For a Windows secured target, the event log audit trail type collects data from the Windows Security Event Log. The trail *location* used in this command must be `security`.

STOP COLLECTION FOR SECURED TARGET

The `STOP COLLECTION FOR SECURED TARGET` command stops the audit trail collection.

Syntax

```
STOP COLLECTION FOR SECURED TARGET secured_target_name USING HOST hostname FROM
location
 [USING PLUGIN plugin_id]]
```

Arguments

Argument	Description
secured_target_name	The name of the secured target for the trail collection you want to stop. To find a list of all registered secured targets, see "LIST SECURED TARGET" on page A-19.
hostname	The name of the host where the secured target agent resides. To find a list of configured agent hosts, see "LIST HOST" on page A-4. For detailed information about a secured target, see "LIST ATTRIBUTE FOR SECURED TARGET" on page A-19.
location	The *location* is one of following: ■ `DIRECTORY` *directory name* / *mask* ■ `TABLE` *tablename* ■ `SYSLOGDEFAULT` | *filename* / *file mask* ■ `NETWORK` ■ `EVENT LOG` *eventlog name* ■ `TRANSACTION LOG` ■ `CUSTOM` *name*
plugin_id	The collection plug-in id being used. Required if there is more than one possible plug-in. Optional if there is only one plug-in. To find a list of existing plug-ins for the type, see "LIST PLUGIN FOR SECURED TARGET TYPE" on page A-48.

General Usage Notes

Since the command is sent to the trail directly, the agent process does not need to be in running state. When multiple plug-ins process audit data from a secured target, use the optional `USING PLUGIN` directive to disambiguate the process.

A trail will be in a `STOP_REQUESTED` state when stopped and transitions to a stopping state, followed by a stopped state. The current state can be viewed using the "LIST TRAIL FOR SECURED TARGET" on page A-27.

Windows Systems Usage Notes

On Windows systems, enter directory and file name locations in either double-quoted strings or as a nonquoted string using forward slashes. For example:

```
... FROM DIRECTORY "c:\app\oracle\product\11.1\av";

... FROM DIRECTORY c:/app/oracle/product/11.1/av;
```

General Examples

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host
FROM directory /opt/audit_trail;
```

Audit data collection from trail `/opt/audit_trail` for secured target `sample_source` stops.

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host
FROM TABLE sys.aud$;
```

Audit data collection from table trail `sys.aud$` for secured target `sample_source` stops.

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host
FROM syslog
  /usr/syslog/syslog*;
```

Collecting syslog trail `/usr/syslog/syslog*` for secured target `sample_source` stops.

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host
FROM event log application;
```

Collecting application event log trail for secured target `sample_source` stops

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host
FROM transaction log;
```

Collecting transaction log trail for secured target `sample_source` stops

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host
FROM TABLE sys.aud$ USING PLUGIN com.sample_plugin;
```

Audit data collection from table `sys.aud$` for the secured target, `sample_source`, using the `com.sample_plugin`, plug-in stops

Oracle Database Usage Notes and Examples

Audit Trail Settings

For the operating system type of audit trail, use the following settings:

Oracle Database Examples

Operating system directory example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com
FROM DIRECTORY $ORACLE_HOME/logs;
```

Operating system syslog file example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com
FROM SYSLOG /etc/syslog.conf;
```

Operating system Windows event log example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com
FROM EVENTLOG;
```

Database audit trail example:

```
avcli> START COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com
FROM TABLE sys.aud$;
```

REDO log example:

```
avcli> START COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com
FROM TRANSACTIONLOOG;
```

SQL Server Usage Notes and Example

The SQL Server audit trail can be in the Windows event log, C2 trace files, or server side trace files. The `FROM` *`trail_type audit_trail`* arguments are as follows:

Type of Audit Trail	trail_type Setting	audit_trail Setting
Windows event log	`EVENTLOG`	n/a
C2 trace file	`C2TRACE`	*`file_wildcard`*
Server-side trace files	`SERVERSIDETRACE`	*`file_wildcard`*

SQL Server Examples

Windows event log example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST mssqlserver
FROM EVENTLOG;
```

C2 trace example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST mssqlserver
FROM DIRECTORY "c:\SQLAuditFile*.trc";
```

Server-side trace example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST mssqlserver
FROM DIRECTORY "c:\SQLAuditFile*.trc";
```

Sybase ASE Usage Notes and Example

For the Sybase ASE audit trail, set the *`trail_type audit_trail`* setting to `TABLE SYSAUDITS`.

Sybase ASE Example

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_syb_db USING HOST sybserver
FROM TABLE SYSAUDITS;
```

MySQL Usage Notes

The trail *`location`* is the path to the directory where converted XML files are created by running the MySQL XML transformation utility. See "(Required for MySQL) Running the XML Transformation Utility" on page 6-10.

IBM DB2 Usage Notes and Example

For the IBM DB2 audit trail, set the *`trail_type audit_trail`* setting to `DIRECTORY` *`directory_location`*.

IBM DB2 Example

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_db2_db USING HOST db2server
FROM DIRECTORY "d:\temp\trace";
```

Oracle Solaris Usage Notes

For Oracle Solaris, the trail location must be in the format:

hostname:*path_to_trail*

where *hostname* matches the hostname in the audit log names, which look like this:

timestamp1.timestamp2.hostname

Windows Secured Target Usage Notes

For a Windows secured target, the event log audit trail type collects data from the Windows Security Event Log. The trail *location* used in this command must be security.

LIST TRAIL FOR SECURED TARGET

The LIST TRAIL FOR SECURED TARGET command lists the available audit trails that have been started with the START COLLECTION command or stopped with the STOP COLLECTION command.

Syntax

LIST TRAIL FOR SECURED TARGET *secured_target_name*

Arguments

Argument	Description
secured_target_name	The name of the secured target. To find a list of existing secured targets, see "LIST SECURED TARGET" on page A-19.

Usage Notes

LIST TRAIL FOR SECURED TARGET does not list audit trails have been created but not yet started or stopped.

Examples

```
avcli> LIST TRAIL FOR SECURED TARGET sample_source;
```

The trails available for the secured target sample_souce are listed.

DROP TRAIL FOR SECURED TARGET

The DROP TRAIL FOR SECURED TARGET drops a trail that no longer needs to be monitored.

> **Note:** An audit trail must be in a STOPPED state in order for it to be dropped. A trail that has previously collected audit data associated with it cannot be dropped.

Syntax

DROP TRAIL FOR SECURED TARGET *secured_target_name* USING HOST *hostname* FROM

location

Arguments

Argument	Description
secured_target_name	The name of the secured target whose audit trail you want to drop. To find all registered secured targets, see "LIST SECURED TARGET" on page A-19.
hostname	The name of the host where the secured target agent resides. To find a list of configured agent hosts, see "LIST HOST" on page A-4. For detailed information about a secured target, see "LIST ATTRIBUTE FOR SECURED TARGET" on page A-19.
location	The *location* is one of following: ■ DIRECTORY *directory name* / *mask* ■ TABLE *tablename* ■ SYSLOG DEFAULT | *filename* / *file mask* ■ NETWORK ■ EVENT LOG *eventlog name* ■ TRANSACTION LOG ■ CUSTOM *name*

Examples

```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo FROM
   DIRECTORY /opt/audit_trail;
```

The audit trail from the directory `/opt/audit_trail` for secured target `sample_source` is dropped.

```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo FROM TABLE
sys.aud$;
```

The audit trail from table trail `sys.aud$` for secured target `sample_source` is dropped.

```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo FROM SYSLOG
DEFAULT
   /usr/syslog/syslog*;
```

Syslog trail `/usr/syslog/syslog*` for secured target `sample_source` is dropped.

```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo
   FROM TRANSACTION LOG;
```

The transaction log trail for secured target `sample_source` is dropped.

SMTP Connection AVCLI Commands

The `AVCLI` SMTP commands enable you to manage SMTP email notifications for Audit Vault Server reports and alert.

Table A–12 lists the SMTP-specific `AVCLI` commands.

Table A–12 AVCLI SMTP Commands

Command	Description
REGISTER SMTP SERVER	Registers the SMTP server configuration with the Audit Vault Server
ALTER SMTP SERVER	Modifies the SMTP server configuration and state
ALTER SMTP SERVER ENABLE	Enables SMTP server configurations for servers registered with the `REGISTER SMTP SERVER` command or modified with the `ALTER SMTP SERVER` command
ALTER SMTP SERVER DISABLE	Disables the SMTP server configuration
ALTER SMTP SERVER SECURE MODE ON	Enables the SMTP server configuration and specifies the secure protocol mode used
ALTER SMTP SERVER SECURE MODE OFF	Disables secure mode in an existing secure SMTP server
TEST SMTP SERVER	Tests SMTP integration with the Audit Vault Server by sending a test email
LIST ATTRIBUTE OF SMTP SERVER	Displays the current SMTP configuration details used by Audit Vault Server
DROP SMTP SERVER	Unregisters the SMTP Server registered with the Audit Vault Server and removes any associated configuration metadata

REGISTER SMTP SERVER

The `REGISTER SMTP SERVER` command registers the SMTP server configuration with the Audit Vault Server.

Syntax

```
REGISTER SMTP SERVER AT host:[port] SENDER ID sender_id SENDER EMAIL sender_email
[AUTHENTICATED BY username/password]
```

Arguments

Argument	Description
host:[port]	The name, and optionally, the outgoing port number of the SMTP server. The *port* defaults to 25, if unspecified.
sender_id	The user ID of the person responsible for sending the email (that is, the email address that appears after `From`).
sender_email	The email address of the person whose ID you entered for the `SENDER ID`, in Request For Comments (RFC) 822 format.
username/password	Optional. The authentication credentials for the recipient user. If the SMTP server runs in authenticated mode and needs a valid *username/password* to connect to send emails, use the `AUTHENTICATED BY` clause to specify those credentials.

Usage Notes

- Right after you create the SMTP server configuration, it is enabled and ready to use.

- If the SMTP server is a secure server, then run the `ALTER SYSTEM SMTP SECURE MODE ON` command ("ALTER SMTP SERVER SECURE MODE ON" on page A-32) after you run `REGISTER SMTP SERVER`.
- To test the configuration, run the `TEST SMTP SERVER` command ("TEST SMTP SERVER" on page A-33).
- This command associates the *sender id* and *sender email* with this configuration data so that all generated emails are sent with this *sender id* and *sender email*.

Examples

```
avcli> REGISTER SMTP SERVER AT sample_mail.example.com sender id "do-not-reply";
```

For an SMTP server running in non-authentication mode at `sample_mail.example.com`, all email is generated and sent from the address: `do-not-reply<donotreply@example.com>`.

```
avcli> REGISTER SMTP SERVER AT sample_mail.example.com:455 SENDER ID av-alerts
SENDER
  EMAIL avalerts@example.com AUTHENTICATED BY smtpuser/smtppass;
```

For an SMTP server running in authentication mode at `sample_mail.example.com`, port `455`; all email is generated and sent from the address: `av-alerts<avalerts@example.com>`. The credentials `smtpuser/smtppass` connect to this server to send emails.

ALTER SMTP SERVER

The `ALTER SMTP SERVER` command modifies the SMTP server configuration and state.

Syntax

```
ALTER_SMTP SERVER AT host:[port] [SENDER ID sender_id]|
  [SENDER EMAIL sender_email] | [AUTHENTICATED BY username/password]
```

Arguments

Argument	Description
host:[port]	The name, and optionally, the outgoing port number of the SMTP server. The *port* defaults to 25.
sender_id	The user ID of the person responsible for sending the email (that is, the email address that appears after `From`).
sender_email	The email address of the person whose ID you entered for the `SENDER ID`, in Request For Comments (RFC) 822 format.
username/password	Optional. The authentication credentials for the recipient user. If the SMTP server runs in authenticated mode and needs a valid *username/password* to connect to send emails, use the `AUTHENTICATED BY` clause to specify those credentials.

Usage Notes

- After you complete the SMTP server configuration, it is enabled and ready to use.

- If the SMTP server is a secure server, then run the `ALTER SYSTEM SMTP SECURE MODE ON` command ("ALTER SMTP SERVER SECURE MODE ON" on page A-32) after you run `REGISTER SMTP SERVER`.
- To test the configuration, run the `TEST SMTP SERVER` command ("TEST SMTP SERVER" on page A-33).
- If you omit an argument, then Audit Vault Server uses the previously configured setting.

Example

```
avcli> ALTER SMTP SERVER AT new_sample_host:465;
```

The host and port configuration information of the SMTP server is changed.

```
avcli> ALTER SMTP SERVER SENDER ID new-do-not-reply;
```

The sender ID configuration information of the SMTP server is changed.

```
avcli> ALTER SMTP SERVER AT new_sample_host:465 sender id new-do-not-reply;
```

The host and port as well as the sender ID of the SMTP server is changed.

ALTER SMTP SERVER ENABLE

The `ALTER SMTP SERVER ENABLE` command enables SMTP server configurations for servers registered with the `REGISTER SMTP SERVER` command or modified with the `ALTER SMTP SERVER` command.

Syntax

```
ALTER SMTP SERVER ENABLE
```

Usage Notes

- When you enable the configuration, Audit Vault Server uses the configuration that was in place when you last disabled the SMTP configuration.
- To find details about the most recent service configuration, see "LIST ATTRIBUTE OF SMTP SERVER" on page A-34.

Example

```
avcli> ALTER SMTP SERVER ENABLE;

SMTP integration is enabled.
```

Enables the integration between the Audit Vault and SMTP server.

ALTER SMTP SERVER DISABLE

The `ALTER SMTP SERVER DISABLE` command disables the SMTP server configuration.

Syntax

```
ALTER SMTP SERVER DISABLE
```

Usage Notes

- After you disable the configuration, Audit Vault Server preserves the most recent configuration. So, when you re-enable the configuration, this configuration is made active again.

- To find details about the most recent service configuration, see "LIST ATTRIBUTE OF SMTP SERVER" on page A-34.
- This command may be useful when the SMTP Server is down for system maintenance.

Example

```
avcli> ALTER SMTP SERVER DISABLE;

SMTP integration is disabled.
```

Disables the integration between the Audit Vault and SMT Server.

ALTER SMTP SERVER SECURE MODE ON

The `ALTER SMTP SERVER SECURE MODE ON` command enables the SMTP server configuration and specifies the secure protocol mode used.

Syntax

```
ALTER SMTP SERVER SECURE MODE ON PROTOCOL [SSL | TLS ] [TRUSTSTORE location]
```

Arguments

Argument	Description
`PROTOCOL`	Optional: One of the following types of protocol: ■ `SSL`: Secure Sockets Layer (default) ■ `TLS`: Transport Layer Security
`location`	The path to the truststore file used to validate the server certificates. Optional.

Usage Notes

Run this command after you run either the `REGISTER SMTP SERVER` ("REGISTER SMTP SERVER" on page A-29) or `ALTER SMTP SERVER` ("ALTER SMTP SERVER" on page A-30) command.

Only run this command if the SMTP server that you are configuring is a secure server.

Examples

```
avcli> ALTER SMTP SERVER SECURE MODE ON PROTOCOL ssl TRUSTSTORE /sample_tstore;
```

This command acknowledges that the SMTP Server registered with Oracle Audit Vault Server is in secure mode, that is, supports SSL or TLS, and uses the file `/sample_tstore` to validate the certificate obtained from the SMTP Server during connects.

```
avcli> ALTER SMTP SERVER SECURE MODE ON PROTOCOL tls TRUSTSTORE /sample_tstore;
```

This example sets TLS protocol instead of SSL.

ALTER SMTP SERVER SECURE MODE OFF

The `ALTER SMTP SERVER SECURE MODE OFF` command disables secure mode in an existing secure SMTP server.

Syntax

```
ALTER SMTP SERVER SECURE MODE OFF
```

Usage Notes

Run this command after you run either the `REGISTER SMTP SERVER` ("REGISTER SMTP SERVER" on page A-29) or `ALTER SMTP SERVER` ("ALTER SMTP SERVER" on page A-30) command.

Example

```
avcli> ALTER SMTP SERVER SECURE MODE OFF;

Updated SMTP server configuration to not use secure protocol.
```

Sets the SMTP Server registered with Oracle Audit Server to non-secure mode.

TEST SMTP SERVER

The `TEST SMTP SERVER` command tests SMTP integration with the Audit Vault Server by sending a test email.

Syntax

```
TEST SMTP SERVER SEND EMAIL TO email_address
```

Arguments

Argument	Description
email_address	Recipient of the test email notification

Usage Notes

- If the test fails, then check the configuration by running the `LIST ATTRIBUTE OF SMTP SERVER` ("LIST ATTRIBUTE OF SMTP SERVER" on page A-34) command.
- You can recreate the configuration by running the `ALTER_SMTP SERVER` command ("ALTER SMTP SERVER" on page A-30).
- If there are no errors, a test email appears in the mail box of the user specified by the *e-mail address* argument.
- You can provide a list of comma-separated email addresses to this command.
- A SMTP Server must first be registered with the Audit Vault Server before this command can be used. See "REGISTER SMTP SERVER" on page A-29.

Example

```
avcli> TEST SMTP SERVER SEND EMAIL TO me@example.com
```

To test the SMTP integration, a test email is sent to the email address, `me@example.com`.

```
avcli> TEST SMTP SERVER SEND EMAIL TO abc@example1.com,xyz@example2.com
```

To test the SMTP integration, a test email is sent to the email address list, `abc@example1.com,xyz@example2.com`.

LIST ATTRIBUTE OF SMTP SERVER

The `LIST ATTRIBUTE OF SMTP SERVER` command displays the current SMTP configuration details used by Audit Vault Server.

Syntax

```
LIST ATTRIBUTE OF SMTP SERVER
```

Usage Notes

To reconfigure the SMTP service connection, run the `ALTER SMTP SERVER` ("ALTER SMTP SERVER" on page A-30) command.

Example

```
avcli> LIST ATTRIBUTE OF SMTP SERVER;
```

The configuration data/attributes for the SMTP server appear.

DROP SMTP SERVER

The `DROP SMTP SERVER` command unregisters the SMTP Server registered with the Audit Vault Server and removes any associated configuration metadata.

Syntax

```
DROP SMTP SERVER
```

Example

```
avcli> DROP SMTP SERVER;

SMTP server unregistered successfully.
```

The SMTP Server is unregistered and any associated configuration metadata is removed.

Security Management AVCLI Commands

The AVCLI security management command enable you to manage various administrator and super administrator privileges.

Table A–13 AVCLI Security Management Commands

Command	Description
GRANT SUPERADMIN	Grants super administrator privileges to the user specified by *username*
REVOKE SUPERADMIN	Revokes super administrator privileges from users specified by *username*
GRANT ACCESS	Grants access to secured target name or secured target group name to specified user
REVOKE ACCESS	Revokes access to secured target or secured target group name from specified user
GRANT ADMIN	Grants administrator privileges to specified user
REVOKE ADMIN	Revokes administrator privileges from specified user

GRANT SUPERADMIN

The GRANT SUPERADMIN command grants super administrator privileges to the user specified by *username*.

Syntax

```
GRANT SUPERADMIN TO username
```

Arguments

Argument	Description
username	The specified user.

Usage Notes

This user automatically receives regular administrator rights as well.

Example

```
avcli> GRANT SUPERADMIN TO scott;
```

Super administrator (and administrator) privileges granted to user scott.

REVOKE SUPERADMIN

The REVOKE SUPERADMIN command revokes super administrator privileges from users specified by *username*.

Syntax:

```
REVOKE SUPERADMIN FROM username
```

Arguments

Argument	Description
username	The specified user.

Usage Notes

The user continues to retain regular administrator rights.

Example:

```
avcli> REVOKE SUPERADMIN FROM scott;
```

Super administrator privileges are revoked from user scott.

GRANT ACCESS

The GRANT ACCESS command grants access to a secured target name or secured target group name to a specified user.

Syntax

```
GRANT ACCESS ON SECURED TARGET secured_target_name TO username

GRANT ACCESS ON SECURED TARGET GROUP secured_target_group name TO username
```

Arguments

Argument	Description
username	The specified user.
secured_target_name	The name of the secured target.
secured_target_group_name	The name of the secured target group.

Example

```
avcli> GRANT ACCESS ON SECURED TARGET sample_source TO scott;
```

User `scott` granted access to secured target `sample_source`.

```
avcli> GRANT ACCESS ON SECURED TARGET GROUP hr_db_group TO hr;
```

User `hr` granted access to group of secured targets specified by the group `hr_db_group`.

REVOKE ACCESS

The `REVOKE ACCESS` command revokes access to a secured target or secured target group name from a specified user.

Syntax

```
REVOKE ACCESS ON SECURED TARGET secured_target_name FROM username

REVOKE ACCESS ON SECURED TARGET GROUP secured_target_group_name FROM username
```

Arguments

Argument	Description
username	The specified user.
secured_target_name	The name of the secured target.
secured_target_group_name	The name of the secured target group.

Example

```
avcli> REVOKE ACCESS ON SECURED TARGET sample_source FROM scott;
```

Access to secured target `sample_source` revoked from user `scott`.

```
avcli> REVOKE ACCESS ON SECURED TARGET GROUP hr_db_group FROM hr;
```

Access to a group of secured targets specified by the group `hr_db_group` revoked from user `hr`.

GRANT ADMIN

The `GRANT ADMIN` command grants administrator privileges to specified user.

Syntax

```
GRANT ADMIN TO username
```

Arguments

Argument	Description
username	The specified user.

Example

```
avcli> GRANT ADMIN TO scott;
```

Administrator privileges granted to user `scott`.

REVOKE ADMIN

The `REVOKE ADMIN` command revokes administrator privileges from specified user.

Syntax:

```
REVOKE ADMIN FROM username
```

Arguments

Argument	Description
username	The specified user.

Example:

```
avcli> REVOKE ADMIN FROM scott;
```

Administrator privileges revoked from user `scott`.

SAN Storage AVCLI Commands (AVDF 12.1.2)

Table A–14 lists SAN storage AVCLI commands. These commands are available as of Oracle AVDF version 12.1.2.

Table A–14 AVCLI SAN Storage Commands

Command	Description
REGISTER SAN SERVER	Registers a SAN server of a specified storage type with the Audit Vault Server
ALTER SAN SERVER	Alters a SAN server registered with the Audit Vault Server by logging into or logging out of a target available on the SAN server
LIST TARGET FOR SAN SERVER	Displays the details of targets available on a specified SAN server
DROP SAN SERVER	Drops a SAN server registered with Audit Vault Server
LIST DISK	Displays details of disks available on the system
ALTER DISKGROUP	Alters a diskgroup by adding or dropping disks
LIST DISKGROUP	Displays details of all diskgroups in the system
LIST SAN SERVER	Displays details of SAN servers registered with the Audit Vault Server

Table A–14 (Cont.) AVCLI SAN Storage Commands

Command	Description
SHOW ISCSI INITIATOR DETAILS FOR SERVER	Displays iSCSI initiator details for the Audit Vault Server

REGISTER SAN SERVER

Note: This command is available as of Oracle AVDF version 12.1.2.

The `REGISTER SAN SERVER` command registers a SAN server with the Audit Vault Server.

Syntax:

```
REGISTER SAN SERVER SAN_server_name OF TYPE storage_type ADDRESS address [PORT
port] [METHOD discovery_method] [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Arguments

Argument	Description
SAN_server_name	Name of the SAN server. Must be unique.
storage_type	Storage type. Currently, only `iSCSI` is supported (case-insensitive).
address	IP address SAN server
port	Optional. Port number. Default is 3260.

discovery_method	Optional. Method used to discover targets. Possible values are:
	`SENDTARGETS [AUTHENTICATED BY username/password]`
	`ISNS`
	
	Default is `SENDTARGETS`.

Examples:

```
avcli> REGISTER SAN SERVER testServer1 OF TYPE iSCSI ADDRESS 192.0.2.1;
```

Registers a SAN server `testServer1` of storage type `iSCSI` at address `192.0.2.1`. The default port number `3260` and the default discovery method `sendtargets` will be used.

```
avcli> REGISTER SAN SERVER testServer2 Of Type iSCSI ADDRESS 192.0.2.1 METHOD
sendtargets AUTHENTICATED BY username2/password2;
```

Registers a SAN server `testServer2` of storage type `iSCSI` at address `192.0.2.1` using the discover method `sendtargets` with credentials `username2` and `password2`.

ALTER SAN SERVER

Note: This command is available as of Oracle AVDF version 12.1.2.

The `ALTER SAN SERVER` command alters a SAN server registered with the Audit Vault Server by logging in or logging out of a target available on the SAN server.

Syntax:

```
ALTER SAN SERVER server_name LOGIN target_name ADDRESS address
```

```
  [PORT port][AUTHENTICATED BY username/password] [ON SECONDARY]

ALTER SAN SERVER server_name LOGOUT target_name ADDRESS address
  [PORT port][AUTHENTICATED BY username/password] [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Arguments

Argument	Description
server_name	Name of the SAN server registered with the Audit Vault Server.
target_name	Name of the target on the SAN server. To get a list of targets, use the command "LIST TARGET FOR SAN SERVER" on page A-39.
address	IP address or hostname of the target on the SAN server
port	Optional. Default is 3260.
username/password	If needed, credential used to log in to the target.

Example:

```
avcli> ALTER SAN SERVER testServer1 LOGIN target1 ADDRESS sample_
target.example.com
  AUTHENTICATED BY username1/password1;
```

Alter the SAN server `testServer1` by logging into `target1` at address `sample_target.example.com` using credentials `username1` and `password1`. The default port number 3260 will be used.

```
avcli> ALTER SAN SERVER testServer2 LOGOUT target2 ADDRESS sample_
target.example.com
```

Alter the SAN server `testServer2` by logging out of `target2` at address `sample_target.example.com`.

LIST TARGET FOR SAN SERVER

Note: This command is available as of Oracle AVDF version 12.1.2.

The `LIST TARGET FOR SAN SERVER` command displays details of the targets available on a specified SAN server.

Syntax:

```
LIST TARGET FOR SAN SERVER server_name [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Arguments

Argument	Description
server_name	Name of the SAN server registered with the Audit Vault Server.

Example:

```
avcli> LIST TARGET FOR SAN SERVER testServer1;
```

Displays the details of targets available on SAN server `testServer1`.

DROP SAN SERVER

Note: This command is available as of Oracle AVDF version 12.1.2.

The `DROP SAN SERVER` command removes a SAN server registered with the Audit Vault Server.

Syntax:

```
DROP SAN SERVER server_name [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Arguments

Argument	Description
server_name	Name of the SAN server registered with the Audit Vault Server.

Example:

```
avcli> DROP SAN SERVER testServer1;
```

Removes SAN server `testServer1` from the Audit Vault Server.

LIST DISK

Note: This command is available as of Oracle AVDF version 12.1.2.

The `LIST DISK` command displays details of all disks available in the system, or disks in a specific disk group.

Syntax:

```
LIST DISK [FOR DISKGROUP SYSTEMDATA|EVENTDATA|RECOVERY] [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Examples:

```
avcli> LIST DISK;
```

Displays the details of all disks in the system.

```
avcli> LIST DISK FOR DISKGROUP SYSTEMDATA;
```

Displays the details of the `SYSTEMDATA` disk group.

ALTER DISKGROUP

Note: This command is available as of Oracle AVDF version 12.1.2.

The `ALTER DISKGROUP` command alters a disk group by adding or dropping disks from the group.

Syntax:

```
ALTER DISKGROUP SYSTEMDATA|EVENTDATA|RECOVERY ADD DISK disk_name
   [ON SECONDARY]

ALTER DISKGROUP SYSTEMDATA|EVENTDATA|RECOVERY DROP DISK disk_name
   [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Arguments

Argument	Description
disk_name	Name of the disk to add or drop. When adding a disk, the disk must be available in the system, and not previously added to a disk group. To display all disks available in the system, use the command "LIST DISK" on page A-40.

Examples:

```
avcli> ALTER DISKGROUP SYSTEMDATA ADD DISK disk1;
```

Adds `disk1` to the `SYSTEMDATA` disk group.

```
avcli> ALTER DISKGROUP RECOVERY DROP DISK disk2;
```

Drops `disk2` from the `RECOVERY` disk group.

LIST DISKGROUP

Note: This command is available as of Oracle AVDF version 12.1.2.

The `LIST DISKGROUP` command displays details of a disk group in the Audit Vault Server.

Syntax:

```
LIST DISKGROUP [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Example:

```
avcli> LIST DISKGROUP;
```

Displays details for all disk groups in the system, for example, name, total space, and free space. To see details of disk in a specific disk group, use the command "LIST DISK" on page A-40.

LIST SAN SERVER

Note: This command is available as of Oracle AVDF version 12.1.2.

The `LIST SAN SERVER` command displays details of SAN servers registered with the Audit Vault Server.

Syntax:

```
LIST SAN SERVER [ON SECONDARY]
```

Use the [ON SECONDARY] option in a high availability configuration to apply this command to secondary Audit Vault Server.

Example:

```
avcli> LIST SAN SERVER;
```

Displays details of SAN servers registered in the system, for example, storage name, storage type, etc.

SHOW ISCSI INITIATOR DETAILS FOR SERVER

Note: This command is available as of Oracle AVDF version 12.1.2.

The SHOW ISCSI INITIATOR DETAILS FOR SERVER command displays iSCSI initiator details for the Audit Vault Server. These initiator details are used in the SAN server configuration to allow it to connect to the Audit Vault Server.

Syntax:

```
SHOW ISCSI INITIATOR DETAILS FOR SERVER [ON SECONDARY]
```

Use the [ON SECONDARY] option in a high availability configuration to apply this command to secondary Audit Vault Server.

Example:

```
avcli> SHOW ISCSI INITIATOR DETAILS FOR SERVER;
```

Displays the iSCSI initiator details for the Audit Vault Server.

Remote Filesystem AVCLI Commands (AVDF 12.1.2)

Table A–15 lists the remote filesystem AVCLI commands. These commands are available as of Oracle AVDF 12.1.2. Currently they support registering and managing connections to NFS filesystems that are used as archive locations.

Table A–15 AVCLI Remote Filesystem Commands

Command	Description
REGISTER REMOTE FILESYSTEM	Registers a remote filesystem with the Audit Vault Server
ALTER REMOTE FILESYSTEM	Alters a remote filesystem registered with the Audit Vault Server
DROP REMOTE FILESYSTEM	Drops a remote filesystem registered with the Audit Vault Server
LIST EXPORT	Displays the list of exports available on an NFS server
LIST REMOTE FILESYSTEM	Lists all remote filesystems registered with the Audit Vault Server
SHOW STATUS OF REMOTE FILESYSTEM	Shows the status of a remote filesystem registered with the Audit Vault Server

REGISTER REMOTE FILESYSTEM

Note: This command is available as of Oracle AVDF version 12.1.2.

The REGISTER REMOTE FILESYSTEM command registers a remote filesystem with the Audit Vault Server. This command currently supports registering an NFS filesystem. After registering a remote filesystem, an administrator can select it when specifying an archive location.

Syntax:

```
REGISTER REMOTE FILESYSTEM filesystem_name OF TYPE NFS ON HOST NFS_server_address
USING EXPORT export [MOUNT]
```

Arguments

Argument	Description
filesystem_name	A unique name for the remote filesystem
NFS_server_address	Hostname or IP address of the NFS server
export	Name of the export directory on the NFS server. The export must be one of the exports available on the NFS server.

Examples:

```
avcli> REGISTER REMOTE FILESYSTEM sample_Filesystem OF TYPE NFS ON HOST example_
host.example.com USING EXPORT /export/home1;
```

Registers a remote NFS filesystem named sample_Filesystem on the host example_host.example.com using the export directory /export/home1. This will mount the registered remote filesystem.

```
avcli> REGISTER REMOTE FILESYSTEM sample_Filesystem OF TYPE NFS ON HOST example_
host.example.com USING EXPORT /export/home1 MOUNT;
```

Registers a remote NFS filesystem named sample_Filesystem on the host example_host.example.com using the export directory /export/home1. This will also mount the registered remote filesystem.

ALTER REMOTE FILESYSTEM

Note: This command is available as of Oracle AVDF version 12.1.2.

The ALTER REMOTE FILESYSTEM command alters a remote filesystem registered with the Audit Vault Server.

Syntax:

```
ALTER REMOTE FILESYSTEM filesystem_name SET {key=value [,key=value...]}

ALTER REMOTE FILESYSTEM filesystem_name MOUNT

ALTER REMOTE FILESYSTEM filesystem_name UNMOUNT [FORCE]
```

Arguments

Argument	Description
filesystem_name	Name of the remote filesystem
key	For an NFS remote filesystem, the *key* NAME is supported.

Examples:

```
avcli> ALTER REMOTE FILESYSTEM sample_filesystem SET NAME=newfilesystem;
```

Changes the name of the remote filesystem `sample_filesystem` to `newfilesystem`.

```
avcli> ALTER REMOTE FILESYSTEM sample_filesystem MOUNT;
```

Mounts the remote filesystem `sample_filesystem`.

```
avcli> ALTER REMOTE FILESYSTEM sample_filesystem UNMOUNT
```

Unmounts remote filesystem `sample_filesystem`.

```
avcli> ALTER REMOTE FILESYSTEM sample_filesystem UNMOUNT FORCE
```

Unmounts remote filesystem `sample_filesystem` and forces this operation.

DROP REMOTE FILESYSTEM

Note: This command is available as of Oracle AVDF version 12.1.2.

The `DROP REMOTE FILESYSTEM` command drops a remote filesystem registered with the Audit Vault Server.

Syntax:

```
DROP REMOTE FILESYSTEM file_system_name
```

Arguments

Argument	Description
filesystem_name	Name of the remote filesystem.

Examples:

```
avcli> DROP REMOTE FILESYSTEM filesystem1;
```

Drops the remote filesystem `filesystem1`.

LIST EXPORT

Note: This command is available as of Oracle AVDF version 12.1.2.

The `LIST EXPORT` command displays the list of exports available on a NFS server.

Syntax:

```
LIST EXPORT OF TYPE NFS ON HOST address
```

Arguments

Argument	Description
address	Hostname or IP address of the NFS server.

Example:

```
avcli> LIST EXPORT OF TYPE NFS ON HOST example_server.example.com;
```

Lists the exports available on the NFS server example_server.example.com.

LIST REMOTE FILESYSTEM

Note: This command is available as of Oracle AVDF version 12.1.2.

The `LIST REMOTE FILESYSTEM` command lists all remote filesystems registered with the Audit Vault Server.

Syntax:

```
LIST REMOTE FILESYSTEM
```

Example:

```
avcli> LIST REMOTE FILESYSTEM;
```

Lists all remote filesystems registered with the Audit Vault Server.

SHOW STATUS OF REMOTE FILESYSTEM

Note: This command is available as of Oracle AVDF version 12.1.2.

The `SHOW STATUS OF REMOTE FILESYSTEM` command shows the status of a specified remote filesystem.

Syntax:

```
SHOW STATUS OF REMOTE FILESYSTEM filesystem_name
```

Arguments

Argument	Description
filesystem_name	Name of the remote filesystem

Examples:

```
avcli> SHOW STATUS OF REMOTE FILESYSTEM filesystem1;
```

Shows the status of remote filesystem `filesystem1`.

Server Management AVCLI Commands

Table A–16 AVCLI Server Management Commands

Command	Description
ALTER SYSTEM SET	Modifies system configuration data
SHOW CERTIFICATE	Displays the certificate for the Audit Vault Server
DOWNLOAD LOG FILE	Downloads the Audit Vault Server log file for diagnostics

ALTER SYSTEM SET

The `ALTER SYSTEM` command modifies system configuration data.

Syntax:

```
ALTER SYSTEM SET {attribute=value [,attribute=value...]}
```

Arguments

Argument	Description
attribute	System attributes as key/value pairs. See Table A–17.

Usage Notes

Typically, system configuration data affects all components system-wide.

Multiple component log levels can be changed by delimiting them using the | symbol.

Modify system configuration data by altering the attributes associated with the data using key=value pairs and multiple attributes by specifying comma-separated pairs.

Log files are located in the *$Oracle_Home*/av/log directory in the Audit Vault Server.

The following *attributes* are supported:

Table A–17 System Attributes

Parameter	Description
LOGLEVEL	The log level of components running on this host. The LOGLEVEL attribute takes a two part value, separated by a colon, as follows: *component_name*:*loglevel_value* where *component_name* can be JfwkLog, PolicyLog, ReportLog, AlertLog, PfwkLog, and GUIlog See Table A–18 for descriptions of values for the LOGLEVEL attribute (a combination of component names and log level values). Multiple components' log levels can be changed by delimiting them using the | symbol.
SYS.HEARTBEAT_INTERVAL	Sets the system heartbeat interval to a numerical value in seconds.

Table A–18 shows valid values for *component_name* and *loglevel_value* for the LOGLEVEL attribute:

Table A–18 LOGLEVEL VALUES

Parameter	Description
JfwkLog	The JfwkLog *component_name* of the LOGLEVEL attribute
PolicyLog	The PolicyLog *component_name* of the LOGLEVEL attribute
ReportLog	The ReportLog *component_name* of the LOGLEVEL attribute
AlertLog	The AlertLog *component_name* of the LOGLEVEL attribute
PfwkLog	The PfwkLog *component_name* of the LOGLEVEL attribute
GUIlog	The GUIlog *component_name* of the LOGLEVEL attribute

Table A–18 (Cont.) LOGLEVEL VALUES

Parameter	Description
INFO	The INFO *loglevel_value* of the LOGLEVEL attribute
WARNING	The WARNING *loglevel_value* of the LOGLEVEL attribute (not supported for GUIlog)
ERROR	The ERROR *loglevel_value* of the LOGLEVEL attribute
DEBUG	The DEBUG *loglevel_value* of the LOGLEVEL attribute

Examples

```
avcli> ALTER SYSTEM SET SYS.HEARTBEAT_INTERVAL=10;
```

The SYS.HEARTBEAT_INTERVAL system configuration setting changes to 10 seconds.

```
avcli> ALTER SYSTEM SET loglevel=JfwkLog:DEBUG|PfwkLog:INFO;
```

SHOW CERTIFICATE

The SHOW CERTIFICATE command displays the certificate for the Audit Vault Server.

Syntax

```
SHOW CERTIFICATE FOR SERVER
```

Example

```
avcli> SHOW CERTIFICATE FOR SERVER;
```

The Audit Vault Server certificate appears.

DOWNLOAD LOG FILE

Note: This command is available as of Oracle AVDF version 12.1.2.

The DOWNLOAD LOG FILE command downloads the diagnostics log file (as a .zip file) from the Audit Vault Server and saves it in the following directory:

AVCLI_installation_path/av/log

Syntax

```
DOWNLOAD LOG FILE FROM SERVER
```

Example

```
avcli> DOWNLOAD LOG FILE FROM SERVER;
```

The Audit Vault Server log file is downloaded.

Collection Plug-In AVCLI Commands

The AVCLI collection plug-in commands enable you to manage the deployment of collection plug-ins.

Table A–12 lists the collection plug-in AVCLI commands.

Table A–19 AVCLI Collection Plug-In Commands

Command	Description
DEPLOY PLUGIN	Deploys a plug-in into Audit Vault Server home from a given archive file
LIST PLUGIN FOR SECURED TARGET TYPE	Lists all the plug-ins in an Audit Vault Server installation
UNDEPLOY PLUGIN	Undeploys a plug-in from an Audit Vault Server home

DEPLOY PLUGIN

The `DEPLOY PLUGIN` command deploys a plug-in into the Audit Vault Server home from a given archive file.

Syntax

```
DEPLOY PLUGIN plugin archive
```

Arguments

Argument	Description
plugin archive	The plug-in archive. Archive files have an `.zip` extension, specifying custom plug-ins that third-party vendors or partners develop to add functionality to Audit Vault Server.

Usage Notes

No action is required after this command.

The `DEPLOY PLUGIN` command updates the agent archive with the contents of this plug-in for future Agent deployments.

When a newer version of the plug-in is available, use the `DEPLOY PLUGIN` command to update the plug-in artifacts. Multiple plug-ins can support a single secured target type.

Example

```
avcli> DEPLOY PLUGIN /opt/avplugins/sample_plugin.zip;
```

Deploys the plug-in at `/opt/avplugins/sample_plugin.zip` into the Audit Vault Server and updates the agent archive by adding the plug-in to its contents.

LIST PLUGIN FOR SECURED TARGET TYPE

The `LIST PLUGIN FOR SECURED TARGET TYPE` command lists all the plug-ins that support a particular secured target type.

Syntax

```
LIST PLUGIN FOR SECURED TARGET TYPE secured target type name
```

Arguments

Argument	Description
secured target type name	The name of the secured target type

Usage Notes

To find a list of available secured target types, see "LIST SECURED TARGET TYPE" on page A-19.

Examples

```
avcli> LIST PLUGINS FOR SECURED TARGET TYPE "Oracle Database";
```

The plug-ins that support the secured target type "Oracle Database" are listed.

UNDEPLOY PLUGIN

The UNDEPLOY PLUGIN command deletes a plug-in from an Audit Vault Server home.

Syntax

```
UNDEPLOY PLUGIN plugin_id
```

Arguments

Argument	Description
plugin_id	The ID of the plug-in that you want to undeploy.

Usage Notes

UNDEPLOY PLUGIN attempts to identify dependent plug-ins or packages prior to deleting the plug-in.

This command undeploys a plug-in specified by the plug-in ID from the Audit Vault Server. It also updates the agent archive removing this plug-in, so that it is not deployed in future agent deployments.

Examples

```
avcli> UNDEPLOY PLUGIN com.abc.sample_plugin;
```

The plug-in, com.abc.sample_plugin, is undeployed from Oracle Audit Vault Server and the agent archive is updated by removing the plug-in.

General Usage AVCLI Commands

Table A–20 lists the general usage AVCLI commands.

Table A–20 AVCLI HELP and EXIT Commands

Command	Description
CONNECT	Connects the current user in AVCLI as a different user
HELP	Lists all AVCLI commands with their categories
-HELP	Displays help information for all of the commands in the AVCLI utility
-VERSION	Displays the version number for AVCLI
QUIT	Exits AVCLI

CONNECT

The CONNECT command enables you to connect as a different user in AVCLI.

Syntax

```
CONNECT username
```

Usage Notes

- If you have logged into to AVCLI without specifying a username and password, then you must use the CONNECT command to connect as a valid user.
- For additional ways to connect to AVCLI, see "Using the AVCLI Command Line Interface" on page 1-16.

Example

```
avcli> CONNECT psmith
Enter password: password

Connected.
```

HELP

The HELP command lists all available AVCLI commands and their categories.

Syntax

```
HELP
```

Example

```
avcli> HELP;
```

-HELP

The -HELP command displays version number and help information about the AVCLI commands. Run the -HELP command from outside of AVCLI.

Syntax

```
avcli -h
avcli -H
avcli -help
avcli -HELP
```

Example

```
avcli -help:

[oracle@slc02vjp ~]$ avcli -help


AVCLI : Release 12.1.2.0.0 - Production on Thu Nov 8 00:53:54 UTC 2012


Copyright (c) 1996, 2014 Oracle.  All Rights Reserved.


Usage 1: avcli -{h|H} | -{v|V}

    -{h|H}             Displays the AVCLI version and the usage help

    -{v|V}             Displays the AVCLI version.
```

```
Usage 2: avcli [ [<option>] [<logon>] [<start>] ]

   <option> is: [-{l|L} <log level>]

    -{l|L} <log level>   Sets the log level to the level specified.
                         Supported log levels: INFO, WARNING, ERROR, DEBUG

   <logon> is: -{u|U} <username>
     Specifies the database account username for the database
     connection

   <start> is: -{f|F} <filename>.<ext>
     Runs the specified AVCLI script from the local file system
     (filename.ext). Valid AVCLI script files should have
     their file extension as '.av' (e.g. sample_script.av)
```

-VERSION

The -VERSION command displays the version number for AVCLI. Run the -VERSION command from outside of AVCLI.

Syntax

```
avcli -v
avcli -V
avcli -version
avcli -VERSION
```

Example

```
avcli -v

AVCLI : Release 12.1.2.0.0 - Production on Tue Apr 26 14:25:31 PDT 2011

Copyright (c) 2014, Oracle.  All Rights Reserved.
```

QUIT

The QUIT; command exits AVCLI.

Syntax

```
QUIT
```

Example

```
avcli> QUIT;
```

B

Plug-in Reference

Topics

About Oracle AVDF Plug-ins

Oracle AVDF supports different types of secured targets by providing a plug-in for each secured target type. Oracle AVDF ships with a set of plug-ins out-of-the-box. These plug-ins are packaged and deployed with the Audit Vault Server.

You can also develop your own plug-ins, or get new available plug-ins, and add them to your Oracle AVDF installation. For more information on this topic, see "Deploying Plug-ins and Registering Plug-in Hosts" on page 5-9.

This appendix contains high-level data for each plug-in shipped with Oracle AVDF. The appendix also contains look-up information you will need to complete the procedures for registering secured targets and configuring audit trails. These procedures link directly to the relevant section of this appendix.

Note: Oracle AVDF also supports Oracle Big Data Appliance as a secured target. For details, see *Oracle Big Data Appliance Owner's Guide*.

Plug-ins Shipped with Oracle AVDF

This section describes each plug-in shipped with Oracle AVDF.

See *Oracle Audit Vault and Database Firewall Installation Guide* for the latest detailed platform support for the current release.

In addition, you can find platform information for prior releases in **Article 1536380.1** at this website: `https://support.oracle.com`

Topics

- Sybase ASE
- Sybase SQL Anywhere
- IBM DB2 for LUW
- MySQL
- Oracle Solaris
- Oracle Linux
- Microsoft Windows
- Microsoft Active Directory
- Oracle ACFS
- Summary of Data Collected for Each Audit Trail Type

Out-of-the Box Plug-ins at a Glance

Oracle AVDF out-of-the-box plug-ins support the secured target versions listed in Table B–1. Click the link for each secured target to get detailed information.

Table B–1 Out-of-the-Box Plug-ins and Features Supported in Oracle AVDF

Secured Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor	Database Interrogation
Oracle Database 9*i*					Yes		
Oracle Database 10*g*, 11*g*, 12*c*	Yes	Yes (except Unified Audit Policies)	Yes	Yes	Yes	Yes	Yes
Microsoft SQL Server 2000	Yes		Yes	Yes	Yes		
Microsoft SQL Server 2005	Yes		Yes	Yes	Yes	Yes (on Windows 2008)	Yes
Microsoft SQL Server 2008, 2008 R2	Yes		Yes	Yes	Yes	Yes (on Windows 2008, 2008 R2)	Yes
Microsoft SQL Server 2012	Yes			Yes	Yes	Yes	
Sybase ASE 12.5.4 to 15.7	Yes		Yes		Yes	Yes	
Sybase SQL Anywhere 10.0.1			Yes		Yes	Yes	Yes
IBM DB2 for LUW 9.x	Yes		Yes		Yes	Yes	

Table B–1 (Cont.) Out-of-the-Box Plug-ins and Features Supported in Oracle AVDF

Secured Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor	Database Interrogation
MySQL 5.0, 5.1			Yes		Yes	Yes	
MySQL 5.5, 5.6	Yes Versions 5.5.29 to 5.6.12		Yes	Yes	Yes	Yes	
Oracle Solaris Version 10 and 11, on SPARC64 and x86-64 platforms	Yes						
Oracle Solaris - other versions, see **Note** below.	Yes						
Oracle Linux - Version 5 Versions OL 5.8, with `auditd` package 1.8 (run `rpm -q audit` to get audit package version)	Yes						
Oracle Linux - Version 6 Version OL 6.0 with `auditd` package 2.0 (run `rpm -q audit` to get audit package version)	Yes						
Oracle Linux - Version 6 Versions OL 6.1 to OL 6.4 with `auditd` package 2.2.2 (run `rpm -q audit` to get audit package version)	Yes						
Microsoft Windows Microsoft Windows Server 2008, and 2008 R2, on x86-64	Yes						
Microsoft Active Directory Version 2008, and 2008 R2 on 64 bit	Yes						
Oracle ACFS 12*c* Release 1 (12.1)	Yes						

Note: Audit data can also be collected from Solaris version 2.3 or later (contact Oracle Support for guidance).

Oracle Database

Table B–2 lists features of the Oracle Database Plug-in.

Table B–2 Oracle Database Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.oracle
Secured Target Versions	Oracle 10*g*, 11*g*, 12*c* Release 1 (12.1)
Secured Target Platforms	Linux/x86-64 Solaris /x86-64 Solaris /SPARC64 AIX/Power64 Windows /86-64 HP-UX Itanium
Setup Script(s)	Yes. See "Oracle Database Setup Scripts" on page B-13 for instructions.
Secured Target Location (Connect String)	jdbc:oracle:thin:@//*hostname*:*port*/*service*
Collection Attribute(s)	ORCLCOLL.NLS_LANGUAGE ORCLCOLL.NLS_TERRITORY ORCLCOLL.NLS_TERRITORY ORCLCOLL.MAX_PROCESS_TIME ORCLCOLL.MAX_PROCESS_RECORDS ORCLCOLL.RAC_INSTANCE_ID ORCLCOLL.HEARTBEAT_INTERVAL ORCLCOLL.HEARTBEAT_INTERVAL See Table B–15 on page B-26 for details.
AVDF Audit Trail Types	TABLE DIRECTORY TRANSACTION LOG SYSLOG (Linux only) EVENT LOG (Windows only) NETWORK See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	For TABLE audit trails: sys.aud$, Sys.fga_log$, dvsys.audit_trail$, v$unified_audit_trail For DIRECTORY audit trails: Full path to directory containing AUD or XML files. For SYSLOG audit trails: Full path to directory containing the syslog file. For TRANSACTION LOG, EVENT LOG and NETWORK audit trails: no trail location required.
Audit Trail Cleanup Support	Yes. See "Oracle Database Audit Trail Cleanup" on page B-21 for instructions.

Microsoft SQL Server

Table B–3 lists the features of the Microsoft SQL Server plug-in.

Table B–3 Microsoft SQL Server Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.mssql

Table B–3 (Cont.) Microsoft SQL Server Plug-in

Plug-in Specification	Description
Secured Target Versions	2000, 2005, 2008, 2008 R2, 2012
Secured Target Platforms	Windows/x86-64
Setup Script(s)	Yes. "Microsoft SQL Server Setup Scripts" on page B-17 for instructions.
Secured Target Location (Connect String)	`jdbc:av:sqlserver://hostname:port`
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY EVENT LOG NETWORK See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	**For DIRECTORY audit trail:** `*.sqlaudit` files, or `*.trc` (trace) files. Examples: *`directory_path`*`\*.sqlaudit` *`directory_path`*`\`*`prefix`*`*.sqlaudit` *`directory_path`*`\`*`prefix`*`*.trc` For *`prefix`*, you can use any prefix for the `.trc` or `*.sqlaudit` files. `#C2_DYNAMIC` and `#TRACE_DYNAMIC` are only supported for SQL Server 2000, 2005, and 2008 versions. **For EVENT LOG audit trail:** ▪ `application` ▪ `security` (SQL Server 2008 and 2012 only)
Audit Trail Cleanup Support	Yes. See "SQL Server Audit Trail Cleanup" on page B-22 for instructions.

Sybase ASE

Table B–4 lists the features of the Sybase ASE plug-in.

Table B–4 Sybase ASE Plug-in

Plug-in Specification	Description
Plug-in directory	*`AGENT_HOME`*`/av/plugins/com.oracle.av.plugin.sybase`
Secured Target Versions	12.5.4 to 15.7
Secured Target Platforms	All platforms
Setup Script(s)	Yes. See "Sybase ASE Setup Scripts" on page B-14 for instructions.
Secured Target Location (Connect String)	`jdbc:av:sybase://hostname:port`
Collection Attribute(s)	None
AVDF Audit Trail Types	TABLE NETWORK See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	`SYSAUDITS`

Table B–4 (Cont.) Sybase ASE Plug-in

Plug-in Specification	Description
Audit Trail Cleanup Support	No

Sybase SQL Anywhere

Table B–5 lists the features of the Sybase SQL Anywhere plug-in.

Table B–5 Sybase SQL Anywhere Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.sqlanywhere
Secured Target Versions	10.0.1
Secured Target Platforms	All platforms
Setup Script(s)	Yes. See "Sybase SQL Anywhere Setup Scripts" on page B-16 for instructions.
Secured Target Location (Connect String)	jdbc:av:sybase://*hostname*:*port*
Collection Attributes	None
AVDF Audit Trail Types	NETWORK (used for host monitoring only) See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	Not required
Audit Trail Cleanup Support	No

IBM DB2 for LUW

Table B–6 lists the features of the IBM DB2 for LUW plug-in.

Table B–6 IBM DB2 for LUW Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.db2
Secured Target Versions	9.x
Secured Target Platforms	All platforms
Setup Script(s)	Yes. See "IBM DB2 for LUW Setup Scripts" on page B-19 for instructions.
Secured Target Location (Connect String)	jdbc:av:db2://*hostname*:*port*
Collection Attribute(s)	av.collector.databasename (case sensitive) - (Required) Specifies the IBM DB2 for LUW database name.
AVDF Audit Trail Types	DIRECTORY NETWORK See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	Path to a directory, for example: d:\temp\trace
Audit Trail Cleanup Support	No

MySQL

Table B–7 lists the features of the MySQL plug-in.

Table B–7 MySQL Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.mysql
Secured Target Versions	For Database Firewall: 5.0, 5.1, 5.5, 5.6. For audit data collection: 5.5.29 to 5.6.12
Secured Target Platforms	Linux/x86-64 Windows 2008, 2008 R2 64-bit
Setup Script(s)	Yes. See "MySQL Setup Scripts" on page B-20.
Secured Target Location (Connect String)	jdbc:av:mysql://*hostname*:*port*/mysql
Collection Attribute(s)	av.collector.securedTargetVersion - (Required) Specifies the MySQL version. av.collector.AtcTimeInterval - (Optional) Specifies the audit trail cleanup file update time interval in minutes. Default is 20.
AVDF Audit Trail Types	DIRECTORY NETWORK See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	The path to the directory where converted XML files are created when you run the MySQL XML transformation utility. See "(Required for MySQL) Running the XML Transformation Utility" on page 6-10.
Audit Trail Cleanup Support	Yes. See "MySQL Audit Trail Cleanup" on page B-23 for instructions.

Oracle Solaris

Table B–8 lists the features of the Oracle Solaris plug-in.

Table B–8 Oracle Solaris Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.solaris
Secured Target Versions	Version 10 update 6 or later, Version 11, on SPARC64 and x86-64 platforms
Secured Target Platforms	Solaris/x86-64 Solaris/SPARC64
Setup Script(s)	No
Secured Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY See Table B–13 on page B-11 for descriptions of audit trail types.

Table B–8 (Cont.) Oracle Solaris Plug-in

Plug-in Specification	Description
Audit Trail Location	*hostname:path_to_trail* The *hostname* matches the hostname in the audit log names, which look like this: *timestamp1.timestamp2.hostname*
Audit Trail Cleanup Support	No

Oracle Linux

Table B–9 lists the features of the Oracle Linux plug-in.

Table B–9 Oracle Linux Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.linux
Secured Target Versions	▪ OL 6.1 - 6.4 with `auditd` package 2.2.2 ▪ OL 6.0 with `auditd` package 2.0 ▪ OL 5.8 with `auditd` package 1.8 Run `rpm -q audit` to get the audit package version.
Secured Target Platforms	Linux/x86-64
Setup Script(s)	No. However, the following user/group access rights are needed to start Linux audit trail: If the agent process is started with `root` user, no changes to access rights are needed. If the agent process is started with a user other than `root`: 1. Assign the group name of the Agent user (the one who will start the Agent process) to the `log_group` parameter in the `/etc/audit/auditd.conf` file. 2. The Agent user and group must have **read** and **execute** permissions on the folder that contains the `audit.log` file (default folder is `/var/log/audit`). 3. Restart the Linux audit service after you make the above changes.
Secured Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	Default location of `audit.log` (`/var/log/audit/audit*.log`) or any custom location configured in the `/etc/audit/auditd.conf` file
Audit Trail Cleanup Support	No

Microsoft Windows

Table B–10 lists the features of the Microsoft Windows plug-in.

Table B–10 Microsoft Windows Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.winos
Secured Target Versions	Microsoft Windows Server 2008, and 2008 R2
Secured Target Platforms	Windows/x86-64
Setup Script(s)	No
Secured Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	EVENT LOG See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	security (case-sensitive)
Audit Trail Cleanup Support	No

Microsoft Active Directory

Table B–11 lists the features of the Microsoft Active Directory plug-in.

Table B–11 Microsoft Active Directory Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.msad
Secured Target Versions	2008, and 2008 R2 on 64 bit
Secured Target Platforms	Windows/x86-64
Setup Script(s)	No
Secured Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	EVENT LOG See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	directory service or security (case-sensitive)
Audit Trail Cleanup Support	No

Oracle ACFS

Table B–12 lists the features of the Oracle ACFS plug-in.

Table B–12 Oracle ACFS Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.acfs
Secured Target Versions	12*c* Release 1 (12.1)

Table B–12 (Cont.) Oracle ACFS Plug-in

Plug-in Specification	Description
Secured Target Platforms	Linux/x86-64 Solaris/x86-64 Solaris/SPARC64 Windows 2008, 2008 R2 64-bit
Setup Script(s)	No
Secured Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	`av.collector.securedtargetversion` - (Required) Specify the Oracle ACFS version.
AVDF Audit Trail Types	DIRECTORY See Table B–13 on page B-11 for descriptions of audit trail types.
Audit Trail Location	The path to the directory containing XML audit files. For example, for a file system mounted at *$MOUNT_POINT*, the audit trail location is: *$MOUNT_POINT*`/.Security/audit/`
Audit Trail Cleanup Support	No

Summary of Data Collected for Each Audit Trail Type

When you configure an audit trail for a secured target, you select the type of audit trail in the **Audit Trail Type** field. The audit trail type depends on your secured target type. Table B–13 describes the types of audit trails that can be configured for each secured target type.

Refer to the product documentation for your secured target type for details on its auditing features and functionality. Refer to the following documentation for Oracle products:

- Oracle Database 12*c* Release 1 (12.1): *Oracle Database Security Guide*
- Oracle Database 11*g* Release 2 (11.2): *Oracle Database Security Guide*
- Oracle Solaris 11.1: `http://docs.oracle.com/cd/E26502_01/html/E29015/auditm-1.html#scrolltoc`
- Oracle Solaris 10.6: `http://docs.oracle.com/cd/E26505_01/html/E27224/auditm-1.html#scrolltoc`
- Oracle ACFS 12c Release 1 (12.1): *Oracle Automatic Storage Management Administrator's Guide*

Table B–13 Summary of Audit Trail Types Supported for Each Secured Target Type

Secured Target Type	Trail Type	Description
Oracle Database	TABLE Releases 10.1.*x*, 10.2.*x*, 11.*x*, and 12c	Collects from the following audit trails: ■ Oracle Database audit trail, where standard audit events are written to the `SYS.AUD$` dictionary table ■ Oracle Database fine-grained audit trail, where audit events are written to the `SYS.FGA_LOG$` dictionary table ■ Oracle Database Vault audit trail, where audit events are written to the `DVSYS.AUDIT_TRAIL$` dictionary table ■ Oracle database 12*c* Unified Audit trail, where audit events are written to `v$unified_audit_trail`
Oracle Database	DIRECTORY Releases 10.1.*x*, 10.2.*x*, 11.*x*, and 12*c*	Collects data from the following audit trails: ■ **On Linux and UNIX platforms:** The Oracle database audit files written to the operating system (`.aud` and `.xml`) files ■ **On Windows platforms:** The operating system Windows Event Log and operating system logs (audit logs) XML (`.xml`) files
Oracle Database	TRANSACTION LOG Enterprise Edition Releases 10.2.0.3 and later, 11.1.0.6 and later 11.2 for REDO connection	Collects audit data from logical change records (LCRs) from the REDO logs. If you plan to use this audit trail type, you can define the data to audit by creating capture rules for the tables from which the Transaction Log trail type will capture audit information. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for more information. **Note:** For Oracle Database 12*c*, the Transaction Log audit trail is only supported when not using a PDB/CDB.
Oracle Database	SYSLOG	Collects Oracle audit records from `syslog` files on Linux and Unix platforms only
Oracle Database	EVENT LOG	Collects Oracle audit records from Microsoft Windows Event Log on Windows platforms only
Oracle Database	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Microsoft SQL Server	DIRECTORY	Collects audit data from C2 audit logs, server-side trace logs, and `sqlaudit` log files
Microsoft SQL Server	EVENT LOG	Collects audit data from Windows Event Logs. For Microsoft SQL Server 2008 and 2012, collection from the Security Event Log is also supported.
Microsoft SQL Server	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Sybase ASE	TABLE	Collects audit data from system audit tables (`sysaudits_01` through `sysaudits_08`) in the `sybsecurity` database
Sybase ASE	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Sybase SQL Anywhere	NETWORK	(For host monitoring only) Collects network traffic (all database operations using a TCP connection).
IBM DB2 for LUW	DIRECTORY	Collects audit data from ASCII text files extracted from the binary audit log (`db2audit.log`). These files are located in the `security` subdirectory of the DB2 database instance.
IBM DB2 for LUW	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
MySQL	DIRECTORY	Collects XML-based audit data from a specified location

Table B–13 (Cont.) Summary of Audit Trail Types Supported for Each Secured Target

Secured Target Type	Trail Type	Description
MySQL	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Oracle Solaris	DIRECTORY	Collects Solaris Audit records (version 2) generated by the `audit_binfile` plug-in of Solaris Audit
Linux	DIRECTORY	Collects audit data from `audit.log`
Windows OS	EVENT LOG	Collects audit data from Windows Security Event Log
Microsoft Active Directory	EVENT LOG	Collects audit data from Windows Directory Service, and Security Event Logs
Oracle ACFS	DIRECTORY	Collects audit data from ACFS encryption and ACFS security sources.

Scripts for Oracle AVDF Account Privileges on Secured Targets

Topics

About Scripts for Setting up Oracle AVDF Account Privileges

You must set up a user account with appropriate privileges on each secured target for Oracle AVDF to use in performing functions related to monitoring and collecting audit data. Oracle AVDF provides setup scripts for database secured targets. Depending on the type of secured target, the scripts set up user privileges that allow Oracle AVDF to do the following functions:

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

When you deploy the Audit Vault Agent on a host computer (usually the same computer as the secured target), the setup scripts for creating the user permissions for Oracle AVDF are located in the following directory (Linux example below):

`$AGENT_HOME/av/plugins/com.oracle.av.plugin.`*`secured_target_type`*`/config/`

Oracle Database Setup Scripts

The Oracle AVDF setup scripts for an Oracle Database secured target, `oracle_user_setup.sql` and `oracle_drop_db_permissions.sql`, are located in the following directory (Linux example below):

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

These scripts are used to set up or revoke user privileges on the Oracle Database in order for Oracle AVDF to do the following functions:

- Audit data collection
- Audit policy management
- Stored procedure auditing (SPA)
- User entitlement auditing

To set up or revoke Oracle AVDF user privileges on an Oracle Database secured target:

1. Create a user account for Oracle AVDF on the Oracle Database. For example:

   `SQL> CREATE USER` *`username`* `IDENTIFIED BY` *`password`*

   You will use this username and password when registering this Oracle Database as a secured target in the Audit Vault Server.

2. Connect as user `SYS` with the `SYSDBA` privilege. For example:

   ```
   SQL> CONNECT SYS / AS SYSDBA
   ```

3. To set up Oracle AVDF user privileges, run the setup script as follows:

   SQL> `@oracle_user_setup.sql` *`username mode`*

   - *`username`*: Enter the name of the user you created in Step 1.
   - *`mode`*: Enter one of the following:
     - `SETUP`: To set up privileges for managing the Oracle Database audit policy from Oracle AVDF, and for collecting data from any audit trail type except the REDO logs. For example, use this mode for a TABLE audit trail in Oracle AVDF.
     - `REDO_COLL`: To set up privileges for collecting audit data from the REDO logs. Use this mode only for a TRANSACTION LOG audit trail in Oracle AVDF.
     - `SPA`: To enable stored procedure auditing for this database
     - `ENTITLEMENT`: To enable user entitlement auditing for this database

4. If Database Vault is installed and enabled on the Oracle database, log in as a user who has been granted the `DV_OWNER` role do the following:

   a. Grant the Oracle AVDF user the `DV_SECANALYST` role on this Oracle Database. For example:

      `SQL> GRANT DV_SECANALYST TO` *`username`*`;`

      For *`username`*, enter the user name you created in Step 1.

      The `DV_SECANALYST` role enables Oracle AVDF to monitor and collect audit trail data for Oracle Database Vault, and run Oracle Database Vault reports.

b. For `REDO_COLL` mode (TRANSACTION LOG audit trail) only, execute one of these procedures depending on your Oracle Database version:

For Oracle Database 12c:

```
SQL> GRANT DV_STREAMS_ADMIN TO username;
```

For *username*, enter the user name you created in Step 1.

For all other supported Oracle Database versions:

```
SQL> EXEC DBMS_MACADM.ADD_AUTH_TO_REALM('Oracle Data Dictionary',
'username', null, dbms_macutl.g_realm_auth_participant);
SQL> COMMIT;
```

For *username*, enter the user name you created in Step 1.

5. To revoke Oracle AVDF user privileges, connect to this database as user `SYS` with the `SYSDBA` privilege, and run the following script:

SQL> `@oracle_drop_db_permissions.sql` *username mode*

- *username* - Enter the name of the user you created in Step 1.
- *mode* - Enter one of the following:
  - `SETUP`: To revoke privileges for managing the Oracle Database audit policy from Oracle AVDF, and for collecting data from any audit trail type except the REDO logs.
  - `REDO_COLL`: To revoke privileges for collecting audit data from the REDO logs.
  - `SPA`: To disable stored procedure auditing for this database
  - `ENTITLEMENT`: To disable user entitlement auditing for this database

Sybase ASE Setup Scripts

Topics

About the Sybase ASE Setup Scripts

The following scripts are provided for configuring necessary user privileges for Oracle AVDF in a Sybase ASE secured target:

```
sybase_auditcoll_user_setup.sql
sybase_auditcoll_drop_db_permissions.sql
sybase_spa_user_setup.sql
sybase_spa_drop_db_permissions.sql
```

The scripts are located in the following directory (Linux example below):

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

These scripts allow Oracle AVDF to perform the following functions for Sybase ASE:

- Audit data collection
- Stored procedure auditing (SPA)

Setting Up Audit Data Collection Privileges for a Sybase ASE Secured Target

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

1. Create a user account for Oracle AVDF in Sybase ASE with the user name `avdf_sybuser`. For example:

   ```
   sp_addlogin avdf_sybuser, password
   ```

   You will use the user name `av_sybuser` and password when registering this Sybase ASE database as a secured target in the Audit Vault Server.

2. Run the setup `sybase_auditcoll_user_setup.sql` script as follows:

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

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

3. When prompted for a password, enter the system administrator password.

4. To revoke the Oracle AVDF user privileges, run the `sybase_auditcoll_drop_db_permissions.sql` script as follows:

   ```
   isql -S server_name -U sa -i sybase_auditcoll_drop_db_permissions.sql
   ```

   - *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the -S *server_name* argument.
   - *sa*: Enter the system administrator user name.
   - When prompted for a password, enter the system administrator password.

Setting Up Stored Procedure Auditing Privileges for a Sybase ASE Secured Target

To set up or revoke stored procedure auditing privileges on a Sybase ASE secured target:

1. If you have not already done so, create a user account for Oracle AVDF in Sybase ASE with the user name `avdf_sybuser`. For example:

   ```
   sp_addlogin avdf_sybuser, password
   ```

   You will use the user name `av_sybuser` and password when registering this Sybase ASE database as a secured target in the Audit Vault Server.

2. Run the `sybase_spa_user_setup.sql` script as follows:

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

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

3. When prompted for a password, enter the system administrator password.

4. To revoke the SPA user privileges, run the `sybase_spa_drop_db_permissions.sql` script as follows:

   ```
   isql -S server_name -U sa -i sybase_spa_drop_db_permissions.sql
   ```

- *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the -S *server_name* argument.
- *sa*: Enter the system administrator user name.
- When prompted for a password, enter the system administrator password.

Sybase SQL Anywhere Setup Scripts

The Oracle AVDF setup scripts for a Sybase SQL Anywhere secured target, `sqlanywhere_spa_user_setup.sql` and `sqlanywhere_spa_drop_db_permissions.sql`, are located in the following directory (Linux example below):

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.sqlanywhere/config/
```

These scripts are used to set up or revoke user privileges on the SQL Anywhere database for Oracle AVDF to do stored procedure auditing (SPA).

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

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

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

   - *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the -S *server_name* argument.
   - *sa*: Enter the system administrator user name.
   - *username*: Enter the name of the user you want to create for Oracle AVDF to use for SPA. Enclose this user name in double quotation marks.
   - *password*: Enter a password for the Oracle AVDF SPA user you are creating. Enclose the password in double quotation marks.

   After running the script, the user is created with privileges for SPA.
3. When prompted for a password, enter the system administrator password.
4. To revoke these privileges and remove this user from the database, run the sqlanywhere_spa_drop_db_permissions.sql as follows:

   ```
   isql -S server_name -U sa -i sqlanywhere_spa_drop_db_permissions.sql -v
   username="username"
   ```

   - *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the -S *server_name* argument.
   - *sa*: Enter the system administrator user name.
   - *username*: Enter the name of the user you want to create for Oracle AVDF to use for SPA. Enclose this user name in double quotation marks.
   - When prompted for a password, enter the system administrator password.

Microsoft SQL Server Setup Scripts

Topics

About the SQL Server Setup Script

The Oracle AVDF setup scripts for a Microsoft SQL Server secured target, `mssql_user_setup.sql` and `mssql_drop_db_permissions.sql`, are located in the following directory:

AGENT_HOME`\av\plugins\com.oracle.av.plugin.mssql\config\`

The scripts set up or revoke user privileges for Oracle AVDF to perform the following functions for SQL Server:

- Audit data collection
- Stored procedure auditing (SPA)

Setting Up Audit Data Collection Privileges for a SQL Server Secured Target

To set up or revoke Oracle AVDF user privileges for audit data collection:

1. Create a user account for Oracle AVDF in SQL Server. For example:

   In SQL Server 2000:

   ```
   exec sp_addlogin 'username', 'password'
   ```

   In SQL Server 2005, 2008, 2012:

   ```
   exec sp_executesql N'create login username with password = ''password'',
   check_policy= off'

   exec sp_executesql N'create user username for login username'
   ```

   You will use this user name and password when registering this SQL Server database as a secured target in the Audit Vault Server.

2. Run the mssql_user_setup.sql script as follows:

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

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

3. When prompted for a password, enter the system administrator password.

4. To revoke audit data collection privileges run the `mssql_drop_db_permissions.sql` script as follows:

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

- *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the -S *server_name* argument.
- *sa*: Enter the system administrator user name.
- *username*: Enter the name of the user you created in Step 1.
- When prompted for a password, enter the system administrator password.

Setting Up Stored Procedure Auditing Privileges for a SQL Server Secured Target

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

1. If you have not already done so, create a user account for Oracle AVDF in SQL Server. For example:

   In SQL Server 2000:

   ```
   exec sp_addlogin 'username', 'password'
   ```

   In SQL Server 2005 and 2008:

   ```
   exec sp_executesql N'create login username with password = ''password'',
   check_policy= off'

   exec sp_executesql N'create user username for login username'
   ```

   You will use this user name and password when registering this SQL Server database as a secured target in the Audit Vault Server.

2. Run the mssql_user_setup.sql script as follows:

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

   - *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the -S *server_name* argument.
   - *sa*: Enter the system administrator user name.
   - *username*: Enter the name of the user you created in Step 1.
   - *Y/N*: Enter `Y` if all databases should be audited for stored procedures. Enter `N` to specify one database name in the `database` parameter.
   - *NA/database_name*: If you entered `Y` for `all_databases`, enter `NA`. If you entered `N` for `all_databases`, enter the database name that should be audited for stored procedures.

3. When prompted for a password, enter the system administrator password.

4. To revoke SPA privileges run the `mssql_drop_db_permissions.sql` script as follows:

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

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

- *sa_password*: Enter the system administrator password.
- *Y/N*: Enter Y if SPA privileges for all databases should be revoked. Enter N to specify one database name in the database parameter.
- *NA/database_name*: If you entered Y for all_databases, enter NA. If you entered N for all_databases, enter the database name for which SPA privileges should be revoked.
- When prompted for a password, enter the name of the user you created in Step 1.

IBM DB2 for LUW Setup Scripts

Topics

About the IBM DB2 for LUW Setup Scripts

The Oracle AVDF setup scripts for a DB2 secured target, db2_auditcoll_user_setup.sql and db2_spa_user_setup.sql, are located in the following directory (Linux example below):

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/
```

These scripts are used to set up or revoke user privileges on the DB2 database for Oracle AVDF to do the following functions:

- Audit data collection
- Stored procedure auditing (SPA)

Setting Up Audit Data Collection Privileges for IBM DB2 for LUW

To set up or revoke Oracle AVDF user privileges for audit data collection:

1. Create a new user account in DB2 to be used by Oracle AVDF for audit data collection.

   You will use this user name and password when registering this DB2 database as a secured target in the Audit Vault Server.

2. In the $AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/ directory, locate the db2_auditcoll_user_setup.sql script and open it for editing.
3. In the script, put the user name of the account from Step 1 in the grant statement, then save the modified script.
4. Execute the modified script as follows:

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

5. To revoke audit collection privileges:
   a. Modify the db2_auditcoll_drop_db_permissions.sql script as in Step 3 above.
   b. Run the script as follows:

      ```
      $> db2 -tvf db2_auditcoll_drop_db_permissions.sql
      ```

Setting Up SPA Privileges for an IBM DB2 for LUW Secured Target

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

1. Create a new user account in DB2 to be used by Oracle AVDF for stored procedure auditing.

   You will use this user name and password when registering this DB2 database as a secured target in the Audit Vault Server.

2. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/` directory, locate the `db2_spa_user_setup.sql` script and open it for editing.

3. In the script, put the user name of the account from Step 1 in the `grant` statement, then save the modified script.

4. Execute the modified script as follows:

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

5. To revoke SPA privileges:

   a. Modify the `db2_spa_drop_db_permissions.sql` script as in Step 3 above.

   b. Run the script as follows:

      ```
      $> db2 -tvf db2_spa_drop_db_permissions.sql
      ```

MySQL Setup Scripts

The Oracle AVDF setup scripts for a MySQL secured target, `mysql_spa_user_setup.sql` and `mysql_spa_drop_db_permissions.sql`, are located in the following directory (Linux example below):

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/config/
```

These scripts are used to set up or revoke user privileges on the MySql database for Oracle AVDF to do stored procedure auditing (SPA).

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

1. Log in to MySQL as a user who can create users and set user privileges.

2. Create a user for stored procedure auditing. For example:

   ```
   create user 'username'@'hostname' identified by 'password'
   ```

   You will use this user name and password when registering this MySQL database as a secured target in the Audit Vault Server.

3. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/config/` directory, locate the `mysql_spa_user_setup.sql` script and open it for editing.

4. Modify the script to provide the same values for *`username`*, *`hostname`*, and *`password`* that you used in Step 1.

5. Execute the `mysql_spa_user_setup.sql` script.

6. To revoke SPA privileges:

   a. Modify the `mysql_spa_drop_db_permissions.sql` script as in Step 4 above.

   b. Execute the `mysql_spa_drop_db_permissions.sql` script.

Audit Trail Cleanup

Some Oracle AVDF plug-ins support audit trail cleanup. This section describes the available audit trail cleanup (ATC) utilities:

- Oracle Database Audit Trail Cleanup
- SQL Server Audit Trail Cleanup
- MySQL Audit Trail Cleanup

Oracle Database Audit Trail Cleanup

Topics

- About Purging the Oracle Database Secured Target Audit Trail
- Scheduling an Automated Purge Job

About Purging the Oracle Database Secured Target Audit Trail

You can use the DBMS_AUDIT_MGMT PL/SQL package to purge the database audit trail.

The DBMS_AUDIT_MGMT package lets you perform audit trail cleanup tasks such as scheduling purge jobs, moving the audit trail to a different tablespace, setting archive timestamps in the audit trail, and so on. You must have the EXECUTE privilege for DBMS_AUDIT_MGMT before you can use it.

Oracle Database 11*g* Release 2 (11.2) or higher, includes the DBMS_AUDIT_MGMT package and its associated data dictionary views installed by default. If your secured target database does not have this package installed, then you can download the package and data dictionary views from My Oracle Support, from the following Web site:

https://support.oracle.com

Search for Article ID 731908.1.

For details about using the DBMS_AUDIT_MGMT PL/SQL package and views, refer to the following Oracle Database 11*g* Release 2 (11.2) documentation:

- The section "Purging Audit Trail Records" in *Oracle Database Security Guide* for conceptual and procedural information
- *Oracle Database PL/SQL Packages and Types Reference* for reference information about the DBMS_AUDIT_MGMT PL/SQL package
- *Oracle Database Reference* for information about the DBA_AUDIT_MGMT_* data dictionary views

Scheduling an Automated Purge Job

Oracle AVDF is integrated with the DBMS_AUDIT_MGMT package on an Oracle Database. This integration automates the purging of audit records from the AUD$ and FGA_LOG$ files, and from the operating system .aud and .xml files after they have been successfully inserted into the Audit Vault Server repository.

After the purge is completed, the Audit Vault Agent automatically sets a timestamp on audit data that has been collected. Therefore, you must set the USE_LAST_ARCH_TIMESTAMP property to TRUE to ensure that the right set of audit records are purged. You do not need to manually set a purge job interval.

To schedule an automated purge job for an Oracle Database secured target:

1. Log in to SQL*Plus on the secured target database as a user who has been granted the EXECUTE privilege for the DBMS_AUDIT_MGMT PL/SQL package.

   For example:

   ```
   sqlplus tjones
   Enter password: password
   ```

2. Initialize the audit trail cleanup operation.

   In the following example, the DEFAULT_CLEANUP_INTERVAL setting runs the job every two hours:

   ```
   BEGIN
    DBMS_AUDIT_MGMT.INIT_CLEANUP(
     AUDIT_TRAIL_TYPE            => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
     DEFAULT_CLEANUP_INTERVAL    => 2 );
   END;
   /
   ```

3. Verify that the audit trail is initialized for cleanup.

   For example:

   ```
   SET SERVEROUTPUT ON
   BEGIN
    IF
      DBMS_AUDIT_MGMT.IS_CLEANUP_INITIALIZED(DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL)
    THEN
      DBMS_OUTPUT.PUT_LINE('Database and OS audit are initialized for cleanup');
    ELSE
      DBMS_OUTPUT.PUT_LINE('Database and OS audit are not initialized for
   cleanup.');
    END IF;
   END;
   /
   ```

4. Use the DBMS_AUDIT_MGMT.CREATE_PURGE_JOB procedure to create and schedule the purge job.

   In this procedure, ensure that you set the USE_LAST_ARCH_TIMESTAMP property to TRUE, so all records older than the timestamp can be deleted.

   The following procedure creates a purge job called CLEANUP_OS_DB_AUDIT_RECORDS that will run every two hours to purge the audit records.

   ```
   BEGIN
     DBMS_AUDIT_MGMT.CREATE_PURGE_JOB (
      AUDIT_TRAIL_TYPE            => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
      AUDIT_TRAIL_PURGE_INTERVAL  => 2,
      AUDIT_TRAIL_PURGE_NAME      => 'CLEANUP_OS_DB_AUDIT_RECORDS',
      USE_LAST_ARCH_TIMESTAMP     => TRUE );
   END;
   /
   ```

SQL Server Audit Trail Cleanup

If the SQL Server audit trail has collected data from a trace or sqlaudit file and that file is inactive, then you can clean up this file. The SQL Server audit trail writes the names of the SQL Server audit text files to a plain text file with the .atc extension. The .atc file resides in the *AGENT_HOME*\av\atc directory on the computer on which the agent is installed.

To manually clean up files that Oracle AVDF has completed extracting audit records from:

1. Go to the *AGENT_HOME*\av\plugins\com.oracle.av.plugin.mssql\bin directory of the computer where the Audit Vault Agent is installed.

   Ensure that the *AGENT_HOME* environment variable is correctly set to the directory path where the agent.jar file is extracted.

2. Run the following utility:

   ```
   SQLServerCleanupHandler secured_target_name
   ```

   For example:

   ```
   SQLServerCleanupHandler mssqldb4
   ```

   If you do not set the *AGENT_HOME* environment variable, you can provide the agent home location in the command line using the following syntax:

   ```
   SQLServerCleanupHandler -securedtargetname secured_target_name agent_home_
   location
   ```

   For example:

   ```
   SQLServerCleanupHandler mssqldb4 c:\AV_agent_installation
   ```

   Important: If the name of the Audit Vault Agent installation directory contains spaces, enclose the name in double quotes, for example "C:\Agent Directory".

To automate the cleanup of SQL Server trace files, you can use the Windows Scheduler.

Note: If the SQL Server trace definition is redefined or reinitialized, then you must ensure that the file names of the trace files do not overlap with trace files that were created earlier.

For example, suppose you start SQL Server with a trace definition in which the trace files names use the following format:

```
c:\serversidetraces.trc
c:\serversidetraces_1.trc
c:\serversidetraces_2.trc
...
c:\serversidetraces_259.trc
```

Then you restart the SQL Server with a new trace definition. This new trace definition must use a different file name from the current trace files (for example, the current one named c:\serversidetraces.trc). If you do not, then when you purge the audit trail, the new trace files that have same names as the old ones will be deleted.

MySQL Audit Trail Cleanup

To run the MySQL audit trail cleanup utility:

1. On the host machine, go to the directory *AGENT_HOME*\av\plugins\com.oracle.av.plugin.mysql\bin

2. Run the following command:

   ```
   MySQLServerCleanupHandler.bat secured_target_name AGENT_HOME
   ```

The above command has the following variables:

- *secured_target_name* - the name of the MySQL secured target
- *AGENT_HOME* - the path to the directory where the Audit Vault Agent is deployed.

Procedure Look-ups: Connect Strings, Collection Attributes, Audit Trail Locations

This section contains reference information you will need to complete procedures in this manual for registering secured targets and configuring audit trails. The procedural steps include links to the topics in this section.

Topics

Secured Target Locations (Connect Strings)

When registering a secured target in the Audit Vault Server console, you enter a connect string in the **Secured Target Location** field (see "Registering or Removing Secured Targets in the Audit Vault Server" on page 6-2). Use a connect string format from Table B–14 depending on the secured target type.

Note: A connect string is not required for a Database Firewall-only deployment.

Table B–14 Secured Target Connect Strings (for Secured Target Location Field)

Secured Target Type	Connect String
Oracle Database	`jdbc:oracle:thin:@//`*`hostname:port/service`*
Sybase ASE	`jdbc:av:sybase://`*`hostname:port`*
Sybase SQL Anywhere	`jdbc:av:sybase://`*`hostname:port`*
Microsoft SQL Server	`jdbc:av:sqlserver://`*`hostname:port`*
IBM DB2 for LUW	`jdbc:av:db2://`*`hostname:port`*
MySQL	`jdbc:av:mysql://`*`hostname:port`*`/mysql`
Oracle Solaris	*hostname* (fully qualified machine name or IP address)
Oracle Linux	*hostname* (fully qualified machine name or IP address)
Microsoft Windows	*hostname* (fully qualified machine name or IP address)
Microsoft Active Directory Server	*hostname* (fully qualified machine name or IP address)
Oracle ACFS	*hostname* (fully qualified machine name or IP address)

Collection Attributes

Topics

About Collection Attributes

Some types of secured targets have optional or required audit trail collection attributes. You can specify collection attributes when registering or modifying a secured target in the **Collection Attributes** fields. See "Registering or Removing Secured Targets in the Audit Vault Server" on page 6-2.

The following secured target types do not require collection attributes:

- Microsoft SQL Server
- Sybase ASE
- Oracle Solaris
- Windows
- Linux
- Microsoft Active Directory Server

Oracle Database Collection Attributes

You can specify collection attributes for a DIRECTORY audit trail for Oracle Database. Table B–15 describes the collection attributes you can use if you select DIRECTORY as the **Audit Trail Type** when registering an Oracle Database secured target in Oracle AVDF.

Table B–15 Collection Attributes for DIRECTORY Audit Trail for Oracle Database

Attribute Name and Description	Required?	Default	Comments
ORCLCOLL.NLS_LANGUAGE The NLS language of the data source	**Yes:** If the started audit trail cannot establish a connection to the Oracle secured target (e.g., secured target is not running) **No:** If the started audit trail is able to connect to the Oracle secured target and get these parameter values from the secured target (e.g., the secured target is running when the trail is started)	NA	The value is not case sensitive.
ORCLCOLL.NLS_TERRITORY The NLS territory of the data source	**Yes:** If the started audit trail cannot establish a connection to the Oracle secured target (e.g., secured target is not running) **No:** If the started audit trail is able to connect to the Oracle secured target and get these parameter values from the secured target (e.g., the secured target is running when the trail is started)	NA	The value is not case sensitive.
ORCLCOLL.NLS_CHARSET The NLS character set of the data source	**Yes:** If the started audit trail cannot establish a connection to the Oracle secured target (e.g., secured target is not running) **No:** If the started audit trail is able to connect to the Oracle secured target and get these parameter values from the secured target (e.g., the secured target is running when the trail is started)	NA	The value is not case sensitive.
ORCLCOLL.MAX_PROCESS_TIME The maximum processing time, in centiseconds, for each call to process the audit trail	No	600	A valid value is an integer value from 10 to 10000. Cannot be reconfigured at run time. Indicates the maximum time for which the collection process records before sending a batch of records to the Audit Vault Server. If the value is too low it can affect performance. If the value is too high, it will take a longer time to stop the audit trail.

Table B–15 (Cont.) Collection Attributes for DIRECTORY Audit Trail for Oracle Database

Attribute Name and Description	Required?	Default	Comments
ORCLCOLL.MAX_PROCESS_RECORDS The maximum number of records to be processed during each call to process the audit trail	No	1000	A valid value is an integer value from 10 to 10000. Cannot be reconfigured at run time. Indicates the maximum number of records processed before sending a batch of records to the Audit Vault Server. If the value is too low it can affect performance. If the value is too high, it will take a longer time to stop the audit trail.
ORCLCOLL.RAC_INSTANCE_ID The instance ID in an Oracle RAC environment	No	1	
ORCLCOLL.HEARTBEAT_INTERVAL The interval, in seconds, to store the metric information	No	60	Cannot be reconfigured at run time. This interval determines how frequently metric information is updated. If the value is too low it creates overhead for sending metrics to the Audit Vault Server. If the value is too high it will skew the average metric information.
ORCLCOLL.NT_ORACLE_SID The Oracle SID name on a Microsoft Windows systems	No	No default	The value is not case sensitive. If no value is specified then the audit trail queries the value from the secured target.

IBM DB2 for LUW Collection Attribute

Table B–16 describes the collection attribute required when you register an IBM DB2 for LUW secured target in Oracle AVDF.

Table B–16 Collection Attribute for IBM DB2 for LUW Database

Attribute Name and Description	Required?	Default	Comments
av.collector.databasename The IBM DB2 for LUW database name	**Yes**	NA	This parameter is case sensitive.

MySQL Collection Attributes

Table B–17 describes the required and optional collection attributes when you register a MySQL secured target in Oracle AVDF.

Table B–17 Collection Attributes for MySQL Database

Attribute Name and Description	Required?	Default	Comments
`av.collector.securedTargetVersion` The MySQL database version	**Yes**	NA	
`av.collector.AtcTimeInterval` Specifies a time interval, in minutes, at which the audit trail cleanup time is updated	**No**	20	**Example:** If this value is 20, the audit trail cleanup time is updated every 20 minutes. Audit log files that have a time stamp before the audit trail cleanup time will be cleaned from the source folder when you run the audit trail cleanup utility. See also "MySQL Audit Trail Cleanup" on page B-23.

Oracle ACFS Collection Attributes

Table B–18 describes the collection attribute required when you register an Oracle ACFS secured target in Oracle AVDF.

Table B–18 Collection Attribute for Oracle ACFS

Attribute Name and Description	Required?	Default	Comments
`av.collector.securedtargetversion` The version number of Oracle ACFS	**Yes**	NA	Five integer values separated by dots, for example `12.1.0.0.0`.

Audit Trail Locations

When you configure an audit trail for a secured target in the Audit Vault Server, you must specify a **Trail Location** (see "Adding an Audit Trail in the Audit Vault Server" on page 6-8). The trail location depends on the type of secured target. Use the format below that corresponds to your secured target type.

Important: Trail locations are case sensitive. To avoid duplicate data collection, we recommend that you provide the entire trail location either in all capital letters or all small letters.

Note: If you selected DIRECTORY for Audit Trail Type, the Trail Location must be a directory mask.

Table B–19 Supported Trail Locations for Secured Targets

Secured Target Type	Supported Trail Locations
Oracle Database	For TABLE audit trails: `sys.aud$`, `Sys.fga_log$`, `dvsys.audit_trail$`, `v$unified_audit_trail` For DIRECTORY audit trails: Full path to directory containing `AUD` or `XML` files. For SYSLOG audit trails: Full path to directory containing the syslog file. For TRANSACTION LOG, EVENT LOG and NETWORK audit trails: no trail location required.

Table B–19 (Cont.) Supported Trail Locations for Secured Targets

Secured Target Type	Supported Trail Locations
Microsoft SQL Server	**For DIRECTORY audit trail:** `*.sqlaudit` files, or `*.trc` (trace) files. Examples: *directory_path*`\*.sqlaudit` *directory_path*`\`*prefix*`*`.sqlaudit *directory_path*`\`*prefix*`*.trc` For *prefix*, you can use any prefix for the `.trc` or `*.sqlaudit` files. `#C2_DYNAMIC` and `#TRACE_DYNAMIC` are only supported for SQL Server 2000, 2005, 2008, 2012. **For EVENT LOG audit trail:** ■ `application` ■ `security` (SQL Server 2008 and 2012 only)
Sybase ASE	`SYSAUDITS`
IBM DB2 for LUW	Path to a directory, for example: `d:\temp\trace`
MySQL	The path to the directory where converted XML files are created when you run the MySQL XML transformation utility. See "(Required for MySQL) Running the XML Transformation Utility" on page 6-10.
Oracle Solaris	*hostname:path_to_trail* The *hostname* matches the hostname in the audit log names, which look like this: *timestamp1.timestamp2.hostname*
Microsoft Windows	`security` (case-insensitive) You can use any case combination in the word `security`. However, once you start collecting a trail using a particular case case combination, you must use the same combination in subsequent collections, otherwise, a new audit trail will start collecting records from the start of the security event log.
Microsoft Active Directory Server	`directory service` or `security` (case-insensitive) You can use any case combination in the words `directory service` or `security`. However, once you start collecting a trail using a particular case combination, you must use the same combination in subsequent collections, otherwise, a new audit trail will start collecting records from the start of the security event log.
Oracle ACFS	The path to the directory containing XML audit files. For example, for a file system mounted at *$MOUNT_POINT*, the audit trail location is: *$MOUNT_POINT*`/.Security/audit/`
Linux	Default location of `audit.log` (`/var/log/audit/audit*.log`) or any custom location configured in the `/etc/audit/auditd.conf` file

C

REDO Logs Audit Data Collection Reference

Topics

About the Recommended Settings for Collection from REDO Logs

This chapter describes recommendations for setting initialization parameters if you plan to use the TRANSACTION LOG audit trail type to collect audit data from the REDO logs of an Oracle Database secured target. After you change the initialization parameters described in these sections, you must restart the secured target database before configuring the TRANSACTION LOG audit trail to collect audit data.

See Also:

- "Oracle Database Setup Scripts" on page B-13 for instructions on setting up privileges in the Oracle Database for collecting audit data from the REDO logs.
- *Oracle Audit Vault and Database Firewall Auditor's Guide* for instructions on creating a capture rule for redo log files

Oracle Database 11*g* Release 2 (11.2) and 12*c* Secured Target Audit Parameter Recommendations

For best results in a REDO collection environment, set the following initialization parameters at each participating database: `COMPATIBLE`, `GLOBAL_NAMES`, `_job_queue_interval`, `SGA_TARGET`, `STREAMS_POOL_SIZE`.

Note: Oracle AVDF does not support Oracle 12*c* pluggable databases (PDBs) or multitenant container databases (CDBs).

Table C–1 lists the initialization parameters that you must configure for each secured target database that will use the TRANSACTION LOG audit trail.

Table C–1 Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
COMPATIBLE	Mandatory	**Default:** 11.2.0 **Range:** 10.0.0 to default release **Modifiable?** No	This parameter specifies the release with which the Oracle server must maintain compatibility. Oracle servers with different compatibility levels can interoperate. To use the new Oracle Streams features introduced in Oracle Database 11*g* Release 2, this parameter must be set to 11.2.0 or higher.
GLOBAL_NAMES	Recommended	**Default:** false **Range:** true or false **Modifiable?** Yes	Specifies whether a database link is required to have the same name as the database to which it connects. Recommended value is TRUE. Ensure that the global name for the secured target database is a fully qualified name (for example, orcl.example.com). If you must change the global database, then run the following ALTER statement in SQL*Plus: ALTER DATABASE RENAME GLOBAL_NAME TO *new_name*; To use Oracle Streams to share information between databases, set this parameter to true at each database that is participating in your Oracle Streams environment.
LOG_ARCHIVE_CONFIG	Recommended	**Default:** 'SEND, RECEIVE, NODG_CONFIG' **Range**: Values: ■ SEND ■ NOSEND ■ RECEIVE ■ NORECEIVE ■ DG_CONFIG ■ NODG_CONFIG **Modifiable?** Yes	Enables or disables the sending of redo logs to remote destinations and the receipt of remote redo logs, and specifies the unique database names (DB_UNIQUE_NAME) for each database in the Data Guard configuration To use downstream capture and copy the redo data to the downstream database using redo transport services, specify the DB_UNIQUE_NAME of the secured target database and the downstream database using the DG_CONFIG attribute. This parameter must be set at both the secured target database and the downstream database.
LOG_ARCHIVE_DEST_*n*	Recommended	**Default:** None **Range**: None **Modifiable?** Yes	Defines up to 31 log archive destinations, where *n* is 1, 2, 3, ... 31. To use downstream capture and copy the redo data to the downstream database using redo transport services, at least one log archive destination must be set at the site running the downstream capture process.
LOG_ARCHIVE_DEST_STATE_*n*	Recommended	**Default:** enable **Range**: One of the following: ■ alternate ■ defer ■ enable **Modifiable?** Yes	Specifies the availability state of the corresponding destination. The parameter suffix (1 through 31) specifies one of the corresponding LOG_ARCHIVE_DEST_*n* destination parameters. To use downstream capture and copy the redo data to the downstream database using redo transport services, ensure that the destination that corresponds to the LOG_ARCHIVE_DEST_*n* destination for the downstream database is set to enable.
LOG_BUFFER	Recommended	**Default:** 5 MB to 32 MB depending on configuration **Range:** Operating system-dependent **Modifiable?** No	Specifies the amount of memory (in bytes) that Oracle uses when buffering redo entries to a redo log file. Redo log entries contain a record of the changes that have been made to the database block buffers. If an Oracle Streams capture process is running on the database, then set this parameter properly so that the capture process reads redo log records from the redo log buffer rather than from the hard disk.

Table C–1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
MEMORY_MAX_TARGET	Recommended	**Default:** 0 **Range:** 0 to the physical memory size available to Oracle Database **Modifiable?** No	Specifies the maximum systemwide usable memory for an Oracle database. If the MEMORY_TARGET parameter is set to a nonzero value, then set this parameter to a large nonzero value if you must specify the maximum memory usage of the Oracle database.
MEMORY_TARGET	Recommended	**Default:** 0 **Range:** 152 MB to MEMORY_MAX_TARGET setting **Modifiable?** Yes	Specifies the systemwide usable memory for an Oracle database. Oracle recommends enabling the autotuning of the memory usage of an Oracle database by setting MEMORY_TARGET to a large nonzero value (if this parameter is supported on your platform).
OPEN_LINKS	Recommended	**Default:** 4 **Range:** 0 to 255 **Modifiable?** No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, as well as external procedures and cartridges, each of which uses a separate process. In an Oracle Streams environment, ensure that this parameter is set to the default value of 4 or higher.
PROCESSES	Recommended	**Default:** 100 **Range:** 6 to operating system-dependent **Modifiable?** No	Specifies the maximum number of operating system user processes that can simultaneously connect to Oracle. Ensure that the value of this parameter allows for all background processes, such as locks and slave processes. In Oracle Streams, capture processes, apply processes, XStream inbound servers, and XStream outbound servers use background processes. Propagations use background processes in combined capture and apply configurations. Propagations use Oracle Scheduler slave processes in configurations that do not use combined capture and apply.
SESSIONS	Recommended	**Default:** Derived from: (1.1 * PROCESSES) + 5 **Range:** 1 to 2^{31} **Modifiable?** No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes, apply processes, XStream outbound servers, or XStream inbound servers in a database, you might need to increase the size of this parameter. Each background process in a database requires a session.
SGA_MAX_SIZE	Mandatory	**Default:** Initial size of SGA at startup **Range:** 0 to operating system-dependent **Modifiable?** No	Specifies the maximum size of System Global Area (SGA) for the lifetime of a database instance. If the SGA_TARGET parameter is set to a nonzero value, then set this parameter to a large nonzero value if you must specify the SGA size.
SGA_TARGET	Mandatory	**Default:** 0 (SGA autotuning is disabled) **Range:** 64 MB to operating system-dependent **Modifiable?** Yes	Specifies the total size of all System Global Area (SGA) components. If MEMORY_MAX_TARGET and MEMORY_TARGET are set to 0 (zero), then Oracle recommends enabling the autotuning of SGA memory by setting SGA_TARGET to a large nonzero value. If this parameter is set to a nonzero value, then the size of the Oracle Streams pool is managed by Automatic Shared Memory Management.

Table C–1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
SHARED_POOL_SIZE	Recommended	**Default:** When SGA_TARGET is set to a nonzero value: If the parameter is not specified, then the default is 0 (internally determined by Oracle Database). If the parameter is specified, then the user-specified value indicates a minimum value for the shared memory pool. When SGA_TARGET is not set (32-bit platforms): 64 MB, rounded up to the nearest granule size. When SGA_TARGET is not set (64-bit platforms): 128 MB, rounded up to the nearest granule size. **Range:** The granule size to operating system-dependent **Modifiable?** Yes	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. If the MEMORY_MAX_TARGET, MEMORY_TARGET, SGA_TARGET, and STREAMS_POOL_SIZE initialization parameters are set to zero, then Oracle Streams transfers an amount equal to 10% of the shared pool from the buffer cache to the Oracle Streams pool.

Table C–1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE	Mandatory	**Default:** 0 **Range:** 0 to operating system-dependent limit **Modifiable?** Yes	Specifies (in bytes) the size of the Oracle Streams pool. The Oracle Streams pool contains buffered queue messages. In addition, the Oracle Streams pool is used for internal communications during parallel capture and apply. If the MEMORY_TARGET or MEMORY_MAX_TARGET initialization parameter is set to a nonzero value, then the Oracle Streams pool size is set by Automatic Memory Management, and STREAMS_POOL_SIZE specifies the minimum size. If the SGA_TARGET initialization parameter is set to a nonzero value, then the Oracle Streams pool size is set by Automatic Shared Memory Management, and STREAMS_POOL_SIZE specifies the minimum size. This parameter is modifiable. If this parameter is reduced to zero when an instance is running, then Oracle Streams processes and jobs might not run. Ensure that there is enough memory to accommodate the Oracle Streams components. The following are the minimum requirements: ■ 15 MB for each capture process parallelism ■ 10 MB or more for each buffered queue. The buffered queue is where the buffered messages are stored. ■ 1 MB for each apply process parallelism ■ 1 MB for each XStream outbound server ■ 1 MB for each XStream inbound server parallelism For example, if parallelism is set to 3 for a capture process, then at least 45 MB is required for the capture process. If a database has two buffered queues, then at least 20 MB is required for the buffered queues. If parallelism is set to 4 for an apply process, then at least 4 MB is required for the apply process. You can use the V$STREAMS_POOL_ADVICE dynamic performance view to determine an appropriate setting for this parameter.
TIMED_STATISTICS	Recommended	**Default:** If STATISTICS_LEVEL is set to TYPICAL or ALL, then true If STATISTICS_LEVEL is set to BASIC, then false The default for STATISTICS_LEVEL is TYPICAL. **Range:** true or false **Modifiable?** Yes	Specifies whether statistics related to time are collected. To collect elapsed time statistics in the dynamic performance views related to Oracle Streams, set this parameter to true. The views that include elapsed time statistics include: V$STREAMS_CAPTURE, V$STREAMS_APPLY_COORDINATOR, V$STREAMS_APPLY_READER, V$STREAMS_APPLY_SERVER.
UNDO_RETENTION	Recommended	**Default:** 900 **Range:** 0 to 2^{32} - 1 **Modifiable?** Yes	Specifies (in seconds) the amount of committed undo information to retain in the database. For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period. If you run one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least 3600. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the UNDO_RETENTION setting.

Oracle Database 11*g* Release 1 (11.1) Secured Target Audit Parameter Recommendations

For best results in a REDO collection environment, set the following initialization parameters at each participating database: `compatible`, `GLOBAL_NAMES`, `_job_queue_interval`, `SGA_TARGET`, `STREAMS_POOL_SIZE`.

Table C–2 describes the hidden parameter that you must configure for each secured target database that will use the TRANSACTION LOG audit trail.

Table C–2 Hidden Initialization Parameters for aA Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
`_job_queue_interval=1`	Recommended	5	Scan rate interval (seconds) of job queue

Table C–3 lists the initialization parameters that you must configure for each secured target database that will use the TRANSACTION LOG audit trail. Enable autotuning of the various pools within the SGA, by setting `SGA_TARGET` to a large nonzero value. Leave the `STREAMS_POOL_SIZE` value set to 0. The combination of these to parameters enables autotuning of the SGA and the Streams Pool size will be automatically adjusted to meet the workload requirements.

Table C–3 Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
`COMPATIBLE= 11.1.0`	Mandatory	**Default:** `11.1.0` **Range:** `10.1.0` to Current Release Number **Modifiable?** No	This parameter specifies the release with which the Oracle server must maintain compatibility. Oracle servers with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10*g* release 1, this parameter must be set to `10.1.0` or higher. To use downstream capture, this parameter must be set to `10.1.0` or higher at both the secured target database and the downstream database. To use the new Streams features introduced in Oracle Database 10*g* release 2, this parameter must be set to `10.2.0` or higher. To use the new Streams features introduced in Oracle Database 11*g* release 1, this parameter must be set to `11.1.0` or higher.
`GLOBAL_NAMES=true`	Recommended	**Default:** false Range: true or false **Modifiable?** Yes	Specifies whether a database link is required to have the same name as the database to which it connects. To use Streams to share information between databases, set this parameter to `true` at each database that is participating in your Streams environment.
`JOB_QUEUE_PROCESSES=4`	Mandatory	**Default:** 0 **Range:** 0 to 1000 **Modifiable?** Yes	Specifies the number of J*nnn* job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by `DBMS_JOB`. This parameter must be set to at least 2 at each database that is propagating events in your Streams environment, and should be set to the same value as the maximum number of jobs that can run simultaneously plus two.

Table C–3 (Cont.) Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
LOG_ARCHIVE_DEST_n	Recommended	**Default:** None **Range:** None **Modifiable?** Yes	Defines up to ten log archive destinations, where n is 1, 2, 3, ... 10. To use downstream capture and copy the redo log files to the downstream database using log transport services, at least one log archive destination must be at the site running the downstream capture process. **See Also**: *Oracle Data Guard Concepts and Administration*
LOG_ARCHIVE_DEST_ STATE_n	Recommended	**Default**: enable **Range:** One of the following: alternate reset defer enable **Modifiable?** Yes	Specifies the availability state of the corresponding destination. The parameter suffix (1 through 10) specifies one of the ten corresponding LOG_ARCHIVE_DEST_n destination parameters. To use downstream capture and copy the redo log files to the downstream database using log transport services, ensure that the destination that corresponds to the LOG_ARCHIVE_DEST_n destination for the downstream database is set to enable.
OPEN_LINKS	Recommended	**Default:** 4 **Range:** 0 to 255 **Modifiable?** No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, as well as external procedures and cartridges, each of which uses a separate process. In a Streams environment, ensure that this parameter is set to the default value of 4 or higher.
PROCESSES	Recommended	**Default:** Derived from PARALLEL_ MAX_SERVERS **Range:** 6 to operating system dependent limit **Modifiable?** No	Specifies the maximum number of operating system user processes that can simultaneously connect to Oracle. Ensure that the value of this parameter allows for all background processes, such as locks, job queue processes, and parallel execution processes. In Streams, capture processes and apply processes use background processes and parallel execution processes, and propagation jobs use job queue processes.
SESSIONS	Recommended	**Default:** Derived from: (1.1 * PROCESSES) + 5 **Range:** 1 to 231 **Modifiable?** No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes or apply processes in a database, then you may need to increase the size of this parameter. Each background process in a database requires a session.
SGA_MAX_SIZE Increase by at least 200M	Mandatory	**Default:** Initial size of SGA at startup **Range:** 0 to operating system dependent limit **Modifiable?** No	Specifies the maximum size of SGA for the lifetime of a database instance. To run multiple capture processes on a single database, you may need to increase the size of this parameter. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
SGA_TARGET >0 Increase this parameter by at least 200M.	Mandatory	**Default:** 0 (SGA autotuning is disabled) **Range:** 64 to operating system-dependent **Modifiable?** Yes	Specifies the total size of all System Global Area (SGA) components. If this parameter is set to a nonzero value, then the size of the Streams pool is managed by Automatic Shared Memory Management. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.

Table C–3 (Cont.) Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SHARED_POOL_SIZE=0	Recommended	**Default:** 32-bit platforms: 32 MB, rounded up to the nearest granule size **64-bit platforms:** 84 MB, rounded up to the nearest granule size **Range:** Minimum: the granule size **Maximum:** operating system-dependent **Modifiable?** Yes	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. If the SGA_TARGET and STREAMS_POOL_SIZE initialization parameters are set to zero, then Streams transfers an amount equal to 10% of the shared pool from the buffer cache to the Streams pool. The STREAMS_POOL_SIZE initialization parameter should be set to 200 MB and, if necessary, increment the SGA_TARGET and SGA_MAX initialization parameters appropriately. For example, if the SGA_TARGET initialization parameter is already set to 2 GB, setting STREAMS_POOL_SIZE=200 MB would not require that the SGA_TARGET initialization parameter be increased. However, if the SGA_TARGET initialization parameter is set to 600 MB and the STREAMS_POOL_SIZE initialization parameter is increased to 200 MB, then it is recommended that the SGA_TARGET initialization parameter value be increased similarly.

Table C–3 (Cont.) Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_ SIZE=200	Mandatory	**Default:** 0 **Range:** Minimum: 0 **Maximum:** operating system-dependent **Modifiable?** Yes	Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, the Streams pool is used for internal communications during parallel capture and apply. If the SGA_TARGET initialization parameter is set to a nonzero value, then the Streams pool size is set by Automatic Shared memory management, and STREAMS_POOL_SIZE specifies the minimum size. This parameter is modifiable. If this parameter is reduced to zero when an instance is running, then Streams processes and jobs will not run. You should increase the size of the Streams pool for each of the following factors: 10 MB for each capture process parallelism 10 MB or more for each buffered queue. The buffered queue is where the Logical Change Records (LCRs) are stored. 1 MB for each apply process parallelism You can use the V$STREAMS_POOL_ADVICE dynamic performance view to determine an appropriate setting for this parameter. For example, if parallelism is set to 3 for a capture process, then increase the Streams pool by 30 MB. If parallelism is set to 5 for an apply process, then increase the Streams pool by 5 MB.
TIMED_STATISTICS	Recommended	**Default:** If STATISTICS_LEVEL is set to TYPICAL or ALL, then true If STATISTICS_ LEVEL is set to BASIC, then false The default for STATISTICS_LEVEL is TYPICAL. **Range:** true or false **Modifiable?** Yes	Specifies whether statistics related to time are collected. To collect elapsed time statistics in the data dictionary views related to Stream, set this parameter to true. The views that include elapsed time statistics include: V$STREAMS_CAPTURE V$STREAMS_APPLY_COORDINATOR V$STREAMS_APPLY_READER V$STREAMS_APPLY_SERVER
UNDO_RETENTION=3600	Recommended	**Default:** 900 **Range:** 0 to 2^32-1 (max value represented by 32 bits) **Modifiable?** Yes	Specifies (in seconds) the amount of committed undo information to retain in the database. For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period. If you are running one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least 3600. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the UNDO_RETENTION setting. **See Also**: *Oracle Database Administrator's Guide* for more information about the UNDO_RETENTION parameter

Oracle Database 10*g* Release 2 (10.2) Secured Target Audit Parameter Recommendations

For best results in a REDO collection environment, set the following initialization parameters at each participating database: COMPATIBLE, GLOBAL_NAMES, _job_queue_ interval, SGA_TARGET, STREAMS_POOL_SIZE.

Table C–4 describes the hidden parameter that you must configure for each secured target database that will use the TRANSACTION LOG audit trail.

Table C–4 Hidden Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
`_job_queue_interval=1`	Recommended	5	Scan rate interval (seconds) of job queue

Table C–5 lists the initialization parameters that you must configure for each secured target database. Enable autotuning of the various pools within the SGA, by setting `SGA_TARGET` to a large nonzero value. Leave the `STREAMS_POOL_SIZE` value set to 0. The combination of these to parameters enables autotuning of the SGA and the Streams Pool size will be automatically adjusted to meet the workload requirements.

Table C–5 Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
`COMPATIBLE= 10.2.0`	Mandatory	**Default:** `10.0.0` Range: `10.0.0` to Current Release Number Modifiable? No	This parameter specifies the release with which the Oracle database must maintain compatibility. Oracle databases with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10*g* release 1, set this parameter to `10.1.0` or higher. To use downstream capture, set this parameter `10.1.0` or higher for both the secured target database and the downstream database. To use the new Streams features introduced in Oracle Database 10*g* release 2, set this parameter to `10.2.0` or higher.
`GLOBAL_NAMES=true`	Recommended	**Default:** false Range: true or false Modifiable? Yes	Specifies whether a database link is required to have the same name as the database to which it connects. To use Streams to share information between databases, set this parameter to `true` for each database that participates in your Streams environment.
`JOB_QUEUE_ PROCESSES=4`	Mandatory	**Default:** 0 **Range:** 0 to 1000 **Modifiable?** Yes	Specifies the number of job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by the `DBMS_JOB` PL/SQL package. Set this parameter to at least `2` for each database that propagates events in your Streams environment, and then set it to the same value as the maximum number of jobs that can run simultaneously, plus `2`.
`LOG_ARCHIVE_DEST_n`	Recommended	**Default:** None **Range:** None **Modifiable?** Yes	Defines up to ten log archive destinations, where *n* is 1, 2, 3, ... 10. To use downstream capture and copy the redo log files to the downstream database using log transport services, at least one log archive destination must be at the site running the downstream capture process. **See Also**: *Oracle Data Guard Concepts and Administration*

`LOG_ARCHIVE_DEST_ STATE_n`	Recommended	**Default:** enable
		Range: One of the following:
		`alternate`
		`reset`
		`defer`
		`enable`
		Modifiable? Yes
			Specifies the availability state of the corresponding destination. The parameter suffix (1 through 10) specifies one of the ten corresponding `LOG_ARCHIVE_DEST_n` destination parameters.
			To use downstream capture and copy the redo log files to the downstream database using log transport services, ensure that the destination that corresponds to the `LOG_ARCHIVE_DEST_n` destination for the downstream database is set to `enable`.

Table C–5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
OPEN_LINKS	Recommended	**Default:** 4 **Range:** 0 to 255 **Modifiable?** No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, external procedures, and cartridges, each of which uses a separate process. In a Streams environment, set this parameter to the default value of 4 or higher.
PARALLEL_MAX_SERVERS Set this parameter to at least 20.	Mandatory	**Default:** Derived from the values of the following parameters: CPU_COUNT PARALLEL_ADAPTIVE_MULTI_USER PARALLEL_AUTOMATIC_TUNING **Range:** 0 to 3599 **Modifiable?** Yes	Specifies the maximum number of parallel execution processes and parallel recovery processes for an instance. As demand increases, Oracle Database increases the number of processes from the number created at instance startup up to this value. In a Streams environment, each capture process and apply process can use multiple parallel execution servers. Set this initialization parameter to an appropriate value to ensure that there are enough parallel execution servers.
PROCESSES	Recommended	**Default:** Derived from PARALLEL_MAX_SERVERS **Range:** 6 to operating system dependent limit **Modifiable?** No	Specifies the maximum number of operating system user processes that can simultaneously connect to an Oracle database. Ensure that the value of this parameter allows for all background processes, such as locks, job queue processes, and parallel execution processes. In Streams, capture processes and apply processes use background processes and parallel execution processes, and propagation jobs use job queue processes.
SESSIONS	Recommended	**Default:** Derived from: (1.1 * PROCESSES) + 5 **Range:** 1 to 231 **Modifiable?** No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes or apply processes in a database, then you may need to increase the size of this parameter. Each background process in a database requires a session.
SGA_MAX_SIZE Increase by at least 200M	Mandatory	**Default:** Initial size of SGA at startup **Range:** 0 to operating system dependent limit **Modifiable?** No	Specifies the maximum size of SGA for the lifetime of a database instance. To run multiple capture processes on a single database, you may need to increase the size of this parameter. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
SGA_TARGET >0 Increase this parameter by at least 200M.	Mandatory	**Default:** 0 (SGA autotuning is disabled) **Range:** 64 to operating system-dependent **Modifiable?** Yes	Specifies the total size of all System Global Area (SGA) components. If you set this parameter to a nonzero value, then the size of the Streams pool is managed by Automatic Shared Memory Management. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.

Table C–5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SHARED_POOL_SIZE=0	Recommended	**Default:** 32-bit platforms: 32 MB, rounded up to the nearest granule size **64-bit platforms:** 84 MB, rounded up to the nearest granule size **Range:** Minimum: the granule size **Maximum:** operating system-dependent **Modifiable?** Yes	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. If you set the SGA_TARGET and STREAMS_POOL_SIZE initialization parameters to zero, then Streams transfers an amount equal to 10 percent of the shared pool from the buffer cache to the Streams pool.

Table C–5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE=200	Mandatory	**Default:** 0 **Range:** Minimum: 0 Maximum: operating system-dependent **Modifiable?** Yes	Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, Oracle Database uses the Streams pool for internal communications during parallel capture and apply. If you set the SGA_TARGET initialization parameter to a nonzero value, then the Streams pool size is set by Automatic Shared memory management, and STREAMS_POOL_SIZE specifies the minimum size. You should set the STREAMS_POOL_SIZE initialization parameter to 200 MB and, if necessary, increment the SGA_TARGET and SGA_MAX initialization parameters appropriately. For example, if the SGA_TARGET initialization parameter is already set to 2 GB, setting STREAMS_POOL_SIZE=200 MB does not require you to increase the SGA_TARGET initialization parameter setting. However, if the SGA_TARGET initialization parameter is set to 600 MB and the STREAMS_POOL_SIZE initialization parameter is increased to 200 MB, then you should increase the SGA_TARGET initialization parameter value similarly. This parameter is modifiable. If you reduce this parameter setting to zero when an instance is running, then Streams processes and jobs cannot run. You should increase the size of the Streams pool for each of the following factors: ■ 10 MB for each capture process parallelism ■ 10 MB or more for each buffered queue. The buffered queue is where the Logical Change Records (LCRs) are stored. ■ 1 MB for each apply process parallelism You can use the V$STREAMS_POOL_ADVICE dynamic performance view to determine an appropriate setting for this parameter. For example, if you set parallelism to 3 for a capture process, then increase the Streams pool by 30 MB. If you set parallelism to 5 for an apply process, then increase the Streams pool by 5 MB.
TIMED_STATISTICS	Recommended	**Default:** If STATISTICS_LEVEL is set to TYPICAL or ALL, then true If STATISTICS_LEVEL is set to BASIC, then false The default for STATISTICS_LEVEL is TYPICAL. **Range:** true or false **Modifiable?** Yes	Specifies whether statistics related to time are collected. To collect elapsed time statistics in the data dictionary views related to Stream, set this parameter to true. The following views include elapsed time statistics: V$STREAMS_CAPTURE V$STREAMS_APPLY_COORDINATOR V$STREAMS_APPLY_READER V$STREAMS_APPLY_SERVER

Table C–5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
UNDO_RETENTION=3600	Recommended	**Default:** 900 **Range:** 0 to 2^32-1 (max value represented by 32 bits) **Modifiable?** Yes	Specifies (in seconds) the amount of committed undo information to retain in the database. For a database running one or more capture processes, set this parameter to specify an adequate undo retention period. If you are running one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least 3600. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the UNDO_RETENTION setting. **See Also:** *Oracle Database Administrator's Guide* for more information about the UNDO_RETENTION parameter

D

Ports Used by Audit Vault and Database Firewall

This appendix lists the TCP and UDP ports used by Oracle Audit Vault and Database Firewall.

Topics

Ports Required When Database Firewall is Deployed for Secured Targets

These following two classes of ports must be open in external network firewalls for these Database Firewall deployments:

- When a Database Firewall is configured to protect a Secured Target database, traffic directed to that database must be able to pass through external network firewalls to the Database Firewall. The ports required are configured in the Secured Target's page in the Audit Vault Server (see *Oracle Audit Vault and Database Firewall Administrator's Guide*).
- A Database Firewall can be configured to accept proxy connections, which are passed on to the database. The ports required for the proxy connection are configured in the Network Configuration page on the Database Firewall (see *Oracle Audit Vault and Database Firewall Administrator's Guide*).

We recommend that you do not change these ports.

Ports for Services Provided by the Audit Vault Server

Table D–1 lists ports for services provided by the Audit Vault Server. These services are used by outside users of the system, and access to most of them can be controlled within the AVDF system. If external network firewalls are used, these ports must be open to allow connections from the users (clients) of these services to the Audit Vault Server(s).

Table D–1 Ports for Services Provided by Audit Vault Server

Port	Protocol Family	Protocol	Purpose	Notes
22	TCP	SSH	Command line access to system	Disabled by default
161	UDP	SNMP	SNMP Access	Disabled by default
443	TCP	HTTPS	Administration Console (web interface)	
1521 1522	TCP	Oracle Database	Access for Audit Vault agents, and access to Oracle Database for reporting	

Ports for Services Provided by the Database Firewall

Table D–2 lists ports for general services provided by the Database Firewall. These services are used by outside users of the system, and access to all them can be controlled within the AVDF system. If external network firewalls are used, these ports must be open to allow connections from the users (clients) of these services to the Database Firewall(s) in the AVDF system.

Table D–2 Ports for Services Provided by Database Firewall

Port	Protocol Family	Protocol	Purpose	Notes
22	TCP	SSH	Command line access to system	Disabled by default
161	UDP	SNMP	SNMP Access	Disabled by default
443	TCP	HTTPS	Administration Console (web interface)	
2050 - 5100	TCP	AVDF Internal Protocol	Incoming traffic captured from Host Monitor	
2050 - 5100	TCP	Syslog	Incoming WAF (F5) violation alerts	The exact port number used by an enforcement point can be found in the **Advanced** settings page of the enforcement point. See *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Ports for External Network Access by the Audit Vault Server

Table D–3 lists ports for external services that may be used by the Audit Vault Server. If external network firewalls are used, the relevant ports must be open so that the Audit Vault Server can use these services as a client.

Table D–3 Ports for External Network Access by the Audit Vault Server

Port	Protocol Family	Protocol	Purpose	Notes
25	TCP	SMTP	Email delivery	
53	UDP	DNS	Domain name service	
123	UDP and TCP	NTP	Time Synchronization	

Table D–3 (Cont.) Ports for External Network Access by the Audit Vault Server

Port	Protocol Family	Protocol	Purpose	Notes
514	UDP, or configured as TCP	Syslog	Syslog alerts	For TCP-transport connections to syslog server(s) the port must be configured in the Audit Vault Server console. See *Oracle Audit Vault and Database Firewall Administrator's Guide*.
514	UDP, or configured as TCP	Proprietary ArcSight protocol over syslog transport	Alerts	For TCP-transport connections to ArcSight server(s) the port must be configured in the Audit Vault Server console. See *Oracle Audit Vault and Database Firewall Administrator's Guide*.
3260	TCP	Software ISCSI	SAN server communication	This port can be configured on Audit Vault Server console when registering a SAN server. See "Registering a SAN Server" on page 13-2.

Ports for External Network Access by the Database Firewall

Table D–4 lists ports for external services that may be used by the Database Firewall. If external network firewalls are used, the relevant ports must be open so that the Database Firewall can use these services as a client.

Table D–4 Ports for External Network Access by the Database Firewall

Port	Protocol Family	Protocol	Purpose	Notes
53	UDP	DNS	Domain name service	
123	UDP and TCP	NTP	Time Synchronization	
514	UDP, or configured as TCP	Syslog	Syslog alerts	For TCP-transport connections to syslog server(s) the port must be configured in the Audit Vault Server console. See *Oracle Audit Vault and Database Firewall Administrator's Guide*.
514	TCP	WAF (F5) alerts	WAF (F5) alerts	The port can be changed from the Audit Vault Server console. See *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Ports for AVDF Internal TCP Communication

Table D–5 lists ports for services that are used between the Database Firewall and the Audit Vault Server. If an external network firewall is placed between these systems, then the relevant ports must be opened.

Table D–5 Ports for AVDF Internal TCP Communication

Port	Protocol Family	Protocol	Direction	Notes
443	TCP	HTTPS	Database Firewall accepts connections from Audit Vault Server	Command interface
1514	TCP	SSL	Audit Vault Server accepts connections from Database Firewall	Event reporting and monitoring

E

Troubleshooting Oracle Audit Vault and Database Firewall

Topics

Troubleshooting Tips

Partial or No Traffic Seen for an Oracle Database Monitored by Database Firewall

Problem

I see no traffic, or only partial traffic, captured in reports for an Oracle Database monitored by the Database Firewall.

Solutions

Go through the following checks to find the trouble:

1. In the Audit Vault Server, check that the report filters are set correctly, including the time slot.
2. Check that the system time on the Database Firewall is synchronized with the time on the Audit Vault Server and the secured target system.

3. Check that the secured target's network traffic is visible to the Database Firewall using the Live Capture utility on the firewall. See "Viewing and Capturing Network Traffic in a Database Firewall" on page 12-11.
4. Check that the Oracle Database service name or SID is used correctly. If you specified an Oracle Database service name in the Enforcement Point settings for this secured target, you will only see traffic for that service name. To see all traffic, remove the service name from the Enforcement Point settings to see all traffic.

   If you have entered a service name in the Enforcement Point, and see no traffic, check to see that the service name is entered correctly in the Enforcement Point settings.

   For Enforcement Points set to use DAM mode, the Database Firewall may be monitoring traffic for existing client connections to the database. Since these connections were in place before you deployed the Database Firewall, it will not be able to detect the service name you specify in the Enforcement Point. In this case, restart the client connections to the database.

   For information on Enforcement Points, see "Configuring Enforcement Points" on page 6-13.
5. Check that the correct Database Firewall policy is deployed. For information on editing and deploying firewall policies, see *Oracle Audit Vault and Database Firewall Auditor's Guide*.

RPM Upgrade Failed

Problem

An RPM upgrade failed with the following error:

```
error: %post(dbfw-mgmtsvr-###) scriptlet failed, exit status 1
```

Solution

1. Check that there is at least 10MB of free `/tmp` space.
2. Remove the new RPM:

   ```
   rpm -e dbfw-mgmtsvr-###
   ```
3. Retry the upgrade.

Agent Activation Request Returns 'host is not registered' Error

Problem

I used the following two commands to register the Audit Vault Agent's host computer (where the agent is deployed), and to request Audit Vault Agent activation:

From the Audit Vault Server:

```
avcli> register host 'host_name'
```

From the host computer:

```
agentctl activate
```

But the `agentctl activate` command returns: `Agent host is not registered`

Solution

Your agent host may be multi-homed. In this case, the agent hostname to IP address resolution may resolve to the NIC/IP that is not used by the agent while connecting to the AV server. To resolve this issue, try to register the agent host using the `with ip` option and then try activating the agent again.

From the Audit Vault Server, use the following command:

```
avcli> register host 'host_name' with ip 'host_ip_address'
```

If you still have issues, try finding the IP address used in the database session when you connect to the Audit Vault server from the agent host, using these commands:

```
sqlplus username/password@"(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=Audit_
Vault_Server_IP)(PORT=1521))(CONNECT_DATA= (SERVICE_NAME=dbfwdb)))"
```

```
sqlplus> select  SYS_CONTEXT('USERENV','IP_ADDRESS') from dual;
```

Use the IP address from the above query to register your host.

Unable to Deploy Agent on the Secondary Audit Vault Server

Problem

When I try to deploy the Audit Vault Agent on the secondary Audit Vault Server in a high availability pair, I get an error that the host is not registered.

Cause

After you pair two Audit Vault Servers for high availability, you do all configuration on the primary server in the pair only, including Audit Vault Agent deployment. See "Step 3: Start High Availability Pairing of the Audit Vault Servers" on page 8-4.

Operation Fails When I Try to Build Host Monitor or Collect Oracle Database Trail

Problem

This problem may manifest with various symptoms:

- When I try to build a host monitor, the operation fails or cannot find the correct binaries.
- When I try to collect audit data from an Oracle Database secured target, the operation fails.
- The Audit Vault Agent cannot connect to the Audit Vault Server.
- Audit trail does not start.

Solution

1. Unset all environment variables except the following:
   - PATH
   - TERM
   - PS1
   - LANG
   - LC_*
   - JAVA_HOME

Then run the `java -jar agent.jar` command again on the host machine. For instructions, see "Deploying the Audit Vault Agent on the Host Computer" on page 5-3.

2. If you deployed the Audit Vault Agent in a Linux environment, ensure that the host machine name is present in the `/etc/hosts` file.

'java -jar agent.jar' Failed on Windows Machine

Problem

The command `java -jar agent.jar` failed on my Windows secured target machine, and I noticed in the log files that the Audit Vault Agent services installation/un-installation failed.

Solution

1. Follow the instructions for unregistering the agent in "Registering or Unregistering the Audit Vault Agent as a Windows Service" on page 5-5.

   If Method 1 fails, then try Method 2.

2. Run the `java -jar agent.jar` command again.

Unable to Un-install the Audit Vault Agent Windows Service

Follow the instructions for unregistering the agent in "Registering or Unregistering the Audit Vault Agent as a Windows Service" on page 5-5.

If Method 1 fails, then try Method 2.

Access Denied Error While Installing Agent as a Windows Service

Problem

I got an error during installation of the Audit Vault Agent on Windows, and I noticed the following error in the *AGENT_HOME*`\av\log\av.agent.prunsvr` log file:

```
[2013-05-02 11:55:53] [info] Commons Daemon procrun (1.0.6.0 32-bit) started
[2013-05-02 11:55:53] [error] Unable to open the Service Manager
[2013-05-02 11:55:53] [error] Access is denied.
[2013-05-02 11:55:53] [error] Commons Daemon procrun failed with exit value:
7 (Failed to )
[2013-05-02 11:55:53] [error] Access is denied.
```

Solution

The above message means that the logged in user does not have privileges to install the Audit Vault Agent as a Windows Service. If you get the above message, try launching the command shell with the **Run As Administrator** option, and then execute `java -jar agent.jar` in that command shell.

Unable to Start the Agent Through the Services Applet On The Control Panel

Problem

I did the following:

1. Installed the Audit Vault Agent using the java -jar agent.jar command.

2. Activated the Audit Vault Agent.
3. Started the Audit Vault Agent using the `agentctl start -k` *key* command.

   The agent started up and is in `RUNNING` state.
4. Stopped the Audit Vault Agent.
5. Tried to start the Audit Vault Agent using the Services Applet on the Windows Control Panel.

   The Audit Vault Agent errored out immediately.

Solution

This means that the Audit Vault Agent is configured to use a Windows account that does not have privileges to connect to the Audit Vault Server.

Take the following steps:

1. Go to **Control Panel**, then to **Services Applet**.
2. Select the **Oracle Audit Vault Agent** service.
3. Right click and select the **Properties** menu.
4. Click the **Log on** tab.
5. Select **This account:** and then enter a valid account name and password.
6. Save and exit.
7. Start the Audit Vault Agent through the Services Applet.

Error When Starting the Agent

Problem

After I installed the Audit Vault Agent, I set the username and password in the `OracleAVAgent` Windows Service Properties **Log On** tab. However, when I try to start the `OracleAVAgent` service, I see the following error in the *Agent_Home*`\av\log\av.agent.prunsvr.`*date*`.log` file:

```
[info]  Commons Daemon procrun (1.0.6.0 32-bit) started
[info]  Running 'OracleAVAgent' Service...
[info]  Starting service...
[error] Failed creating java
[error] ServiceStart returned 1
[info]  Run service finished.
[info]  Commons Daemon procrun finished
```

Solution

This means that the `OracleAVAgent` service is not able to launch the Java process. Try the following:

1. Uninstall all JDKs and/or JREs in the system.
2. Reinstall JDK SE or JRE and then start the OracleAVAgent service.
3. If this doesn't help, you can install 32 bit JDK SE or JRE and then start the OracleAVAgent service.

Error When Running Host Monitor Setup

Problem

I am setting up a Host Monitor. When I run the command `bin/hostmonsetup install`, the following error is displayed:

```
[root@dbsec1 av]# bin/hostmonsetup install
/usr/bin/ld: cannot find -lpcap
collect2: ld returned 1 exit status
make: *** [hostmonitor] Error 1
Line 105: Failed to generate executables for Host monitor.
```

Solution

This means the host computer does not have the required libraries for the host monitor. Install the required libraries listed in "Prerequisites for Host Monitoring" on page 7-2.

Alerts on Oracle Database Secured Target are not Triggered for a Long Time

Problem

I configured an Oracle Database secured target to audit to XML files, configured an audit trail in Oracle AVDF of type DIRECTORY, and then configured an alert to trigger on certain events. My alert did not get triggered for a long time.

Solution

This issue can occur if the Oracle Database secured target is not flushing the audit records to the file immediately. Contact Oracle Support in order to access support note *1358183.1 Audit Files Are Not Immediately Flushed To Disk*.

Internal capacity exceeded messages seen in the /var/log/messages file

Problem

Not all the expected traffic is being captured or logged by the DBFW, and error messages are present in the /var/log/messages file containing the text "Internal capacity exceeded".

Solution - 1

Increase the processing resources available for the Secured Target on which the issue is observed through the setting of the MAXIMUM_ENFORCEMENT_POINT_THREADS collection attribute. For more information, refer to "Registering Secured Targets"

Solution - 2

The size of the buffer used for inter-process communication on the DBFW can be increased to improve throughput, though at the cost of more memory being allocated by the relevant processes. Please note that this setting is in units of Megabytes, and has a default value of 16. To change the configuration for this value execute the following procedure:

1. Log in to the DBFW console as the ***root*** user.
2. Edit the file */usr/local/dbfw/etc/dbfw.conf*. Look for an entry with the key `IPC_PRIMARY_BUF_SIZE_MB`. If it exists, this is the line to change. If it does not exist, add a new line beginning with `IPC_PRIMARY_BUF_SIZE_MB`.

3. Change the `IPC_PRIMARY_BUF_SIZE_MB` line to reflect the required buffer size. For example, if you wished to change the buffer size to 24 megabytes, the configuration line should be `IPC_PRIMARY_BUF_SIZE_MB="24"`. Save the changes.
4. From the command line restart the DBFW processes so that the new setting is used with the command line `/etc/init.d/dbfw restart`.

There is also a second setting available to alter the maximum size that the inter-process communication buffer can grow to. It's units are in megabytes, and has a default value of 64 megabytes. To change the configuration for this value execute the following procedure:

1. Log in to the DBFW console as the ***root*** user.
2. Edit the file */var/dbfw/va/N/etc/appliance.conf*, where ***N*** is the number of the enforcement point in question. Look for an entry with the key `IPC_BUF_SIZ_MB`. If it exists, this is the line to change. If it does not exist, add a new line beginning with `IPC_BUF_SIZ_MB`.
3. Change the `IPC_BUF_SIZ_MB` to reflect the desired maximum buffer size. For example, if you wished to change the buffer size to 80 megabytes, the configuration line should be `IPC_BUF_SIZ_MB="80"`. Save the changes.
4. From the command line restart the DBFW processes so that the new setting is used with the command line `/etc/init.d/dbfw restart`.

If the problem persists and after altering the above settings the `Internal capacity exceeded` error is still encountered, then further investigation by support is required. Perform the following:

1. Log in to the DBFW console as the ***root*** user.
2. Edit the file */usr/local/dbfw/etc/logging.conf*
3. Find the line `log4j.logger.com.oracle.dbfw.Metrics=ERROR`
4. Comment out this line by placing a **#** character at the beginning of the line `log4j.logger.com.oracle.dbfw.Metrics=ERROR`. Save the changes.
5. From the command line restart the DBFW processes so that the new setting is used with the command line `/etc/init.d/dbfw restart`
6. Leave the DBFW running for several hours under load even while the `Internal capacity exceeded` error is still encountered.
7. After this period, get the diagnostics output from the DBFW as detailed in MOS note **How to Collect Diagnostic Logs From Audit Vault Server (Doc ID 2144813.1)**. Provide the diagnostics output to support for further analysis.

F

Audit Vault Error Messages

This section lists the Oracle Audit Vault error messages.

46501: invalid *string*.

Cause: Invalid value specified.

Action: Provide a valid non-NULL value with valid length.

46502: NULL in *string*

Cause: NULL value specified.

Action: Provide a non-NULL value.

46503: object *string* already exists

Cause: Object specified was already present in the system.

Action: Provide a different value.

46504: duplicate *string*

Cause: Value was repeated in the input.

Action: Remove the duplicates.

46505: object *string* does not exist

Cause: Object specified was not present in the system.

Action: Provide a different value.

46506: attribute *string* exists in *string*

Cause: Attribute specified was already present.

Action: Provide a different attribute.

46507: invalid data or type name for attribute *string*

Cause: Data type of the value specified was different from the type name of the Attribute.

Action: Change the type name or the type of the value for the Attribute.

46508: too many attributes of type *string* specified

Cause: Specified number of attributes of this type exceeded the maximum number supported.

Action: Specify fewer number of attributes of this type.

46509: offset "*string*" is incorrectly formatted

Cause: The specified offset value is not in the format +/-hh:mm

Action: Specify the offset in the correct format +/-hh:mm

46510: specified audit trail can be collected by more than one plugin. please resolve the conflict by explicitly specifying a plugin using the USING PLUGIN clause

Cause: multiple plug-ins are registered that can collect from this audit trail

Action: Explicitly specify the plug-in ID by using the USING PLUGIN clause

46511: missing plugin for trail at agent on host "*string*"

Cause: Agent at the specified host does not have the plug-in to handle the trail

Action: Deploy the plug-in on the server that can handle this trail and deploy the agent with this plug-in on the host

46512: no agent running on host "*string*"

Cause: Agent at the specified host does not seem to be running

Action: Start the agent using **agentctl start** command and re-try the operation

46513: insufficient privileges

Cause: User performed an operation for which they did not have sufficient privileges

Action: Check privileges for user and re-try the operation

46514: invalid syntax "*string*". Run HELP *string* for help.

Cause: User entered an invalid command

Action: Check syntax and re-try the command with the correct syntax

46515: invalid host attribute "*string*". Run HELP *string* for help.

Cause: User attempted to alter an invalid attribute for HOST

Action: Check syntax and re-try the command with the correct syntax

46516: audit data is being actively collected from the specified trail "*string*". cannot drop trail.

Cause: User attempted to drop a trail which is currently active

Action: Stop the trail using STOP COLLECTION command and re-try

46517: Cannot drop trail of type "*string*" at "*string*" for secured target "*string*"; audit trail does not exist.

Cause: User attempted to drop a trail which does not exist

Action: One cannot drop audit trail which does not exist

46518: start collection failed for plug-in:"*string*". plug-in does not exist.

Cause: User attempted to start collection for a secured target using a plug-in that does not exist

Action: Check the plug-in specified in the command and re-try the command with a valid plug-in

46519: start collection failed. host "*string*" is not registered with the audit vault server

Cause: User attempted to start a collection using a host which is not registered with the audit vault server

Action: Register the host with the audit vault server, activate it, and then re-try the command.

46520: host with ip address "*string*" is already registered with the audit vault server

Cause: User attempted to register a host with an Ip address that is already registered with an existing host

Action: User cannot register two hosts with the same IP address

46521: NULL value passed for a mandatory attribute

Cause: A mandatory attribute was set to a NULL value.

Action: Provide a non-NULL value for the mandatory attribute.

46522: mandatory attribute *string* missing in the input

Cause: Mandatory attribute name was missing in the attribute value list.

Action: Provide the value for mandatory attribute.

46523: attempting to drop Event Category with active Events

Cause: Event Category specified had active Events.

Action: Drop the active Events before dropping this Event Category.

46524: at least one audit trail being collected for secured target

Cause: Secured Target specified had trails which were active.

Action: Stop all the active trails for the given Secured Target.

46525: Sourcetype-specific extension for Category already exists

Cause: Event Category was specified which already has a Format extension for the given Source type.

Action: Provide an Event Category which does not have a Source type specific extension.

46526: attempting to drop an in-use Event mapping

Cause: Event mapping specified was in use.

Action: Provide an Event mapping that is not being used.

46527: attempting to change an immutable attribute

Cause: An immutable attribute was specified.

Action: Provide a mutable attribute.

46528: attempting to drop system-defined Event

Cause: Event specified was system-defined.

Action: Provide a user-defined Event.

46529: attempting to drop Event with active mappings

Cause: Event specified had active Event mappings.

Action: Drop the active mappings before dropping this Event.

46530: attempting to drop Sourcetype with active Sources

Cause: Source type specified had active Sources.

Action: Drop the active Sources before dropping this Source type.

46531: unsupported Source version

Cause: Version specified for the Source was not supported.

Action: Provide a Source version which is equal to or greater than the minimum supported version for the corresponding Source type.

46532: Attribute '*string*' is not set for secured target '*string*'.

Cause: The specified attribute was not set for the secured target.

Action: Set the specified attribute for the secured target.

46533: Invalid lock type '*string*' specified.

Cause: An invalid plug-in lock type was specified.

Action: Valid plug-in lock types are 'DEPLOY' and 'UNDEPLOY'.

46534: Plug-in deployment/undeployment operation already in progress.

Cause: A plug-in deployment or removal operation is already in progress and a corresponding lock already exists.

Action: Wait for the current operation to end before attempting to deploy or remove another plug-in.

46535: failed to add secured target address: duplicate secured target address

Cause: The user tried to add a duplicate address for a secured target

Action: Check existing address for the secured target

46536: firewall cannot be paired with itself

Cause: user tries to pair a firewall with itself

Action: choose a different firewall and try again

46537: firewall *string* is not registered with the Audit Vault Server

Cause: User tries to create a resilient pair using a non-existent firewall

Action: Register the firewall first and then try again

46538: invalid enforcement point attribute "*string*". Run HELP *string* for help.

Cause: User attempted to alter an invalid attribute for the enforcement point

Action: Check syntax and re-try the command with the correct syntax

46539: Secured Target Name is too long.

Cause: Secured Target Name failed length validation checks.

Action: Provide valid Secured Target Name.

46540: Secured Target Description is too long.

Cause: Secured Target Description failed length validation checks.

Action: Provide valid Secured Target Description.

46541: attempting to drop Collector Type with active Collectors

Cause: One or more Collectors for this Collector Type were active.

Action: Drop all active Collectors for this Collector Type.

46542: attempting to drop an Agent with active Collectors

Cause: One or more Collectors for this Agent were active.

Action: Drop all active Collectors for this Agent.

46543: attempting to drop a Collector before disabling the collection

Cause: The collection for the Collector specified was not disabled.

Action: Disable the collection before dropping the Collector.

46544: attempting to drop an Agent before disabling it

Cause: The Agent specified was not disabled.

Action: Disable the Agent before dropping it.

46545: failed to start collection; trail is already being collected.

Cause: the user tried to start a trail which had already been started

Action: check the status of the trail before starting it

46546: Failed to drop host; one or more audit trails associated with the host are being collected.

Cause: user tried to drop a host which has active trails associated with it

Action: stop the active trails associated with this host and then try again

46547: Enabling Secured Target Location requires setting User Name and Password; please specify User Name and Password along with the Secured Target Location.

Cause: the user tried to set secured target location without setting user name and password

Action: set user name and password along with the secured target location

46548: Failed to generate secured target location string.

Cause: user did not specify the correct components of secured target location string

Action: specify the correct components of secured target location string and then try again

46549: No NTP servers are specified.

Cause: the user chose to enable NTP synchronization, but did not specify any NTP server

Action: specify NTP server and then try again

46550: Secured Target Location is required for registering this secured target.

Cause: user tried to register a secured target without providing secured target location, which is required to connect to the secured target

Action: provide secured target location and try again

46551: attempting to change the type of an attribute currently in use

Cause: Attribute specified was in use.

Action: Provide an attribute that is not being used.

46552: attempting to drop an attribute currently in use

Cause: Attribute specified was in use.

Action: Provide an attribute that is not being used.

46553: attempting to change the type of an attribute without providing a new default value

Cause: Current type of the default value did not match with the new type specified.

Action: Provide a new default value for the attribute.

46554: Secured Target Location is too long.

Cause: Secured Target Location failed length validation checks.

Action: Provide valid Secured Target Location.

46555: User Name is too long.

Cause: User Name failed length validation checks.

Action: Provide valid User Name.

46556: Single and double quotes are not allowed in the User Name.

Cause: Illegal characters were supplied in the User Name.

Action: Remove single and double quotes from User Name.

46557: Password must contain at least 8 characters and at most 30 characters.

Cause: Password failed length validation checks.

Action: Provide valid Password.

46558: Secured Target Attribute Name is too long.

Cause: Secured Target Attribute Name failed length validation checks.

Action: Provide valid Secured Target Attribute Name.

46559: Secured Target Attribute Value is too long.

Cause: Secured Target Attribute Value failed length validation checks.

Action: Provide valid Secured Target Attribute Value.

46560: Setting User Name and Password requires enabling Secured Target Location; please specify Secured Target Location along with User Name and Password.

Cause: the user tried to set user name and password without enabling secured target location

Action: set secured target location along with user name and password

46561: no Format defined for the Source Type and Category

Cause: Format for the specified Source Type and Category pair was not present in the system.

Action: Provide Source Type and Category pair which already has a Format defined.

46562: error in Alert condition

Cause: Invalid Alert condition was specified.

Action: Correct the Alert condition.

46563: Attempt to delete alert '*string*' failed.

Cause: User is trying to drop an alert he does not own.

Action: Ask the owner of the alert to drop it.

46564: Setting alert threshold value to *string* failed.

Cause: An invalid value was specified for the alert threshold.

Action: Provide an alert threshold value in the valid range (> 1).

46565: Failed to update alert '*string*' due to insufficient privileges.

Cause: User is trying to update an alert he does not own.

Action: Ask the owner of the alert to update it.

46566: no changes specified

Cause: The user attempted to alter an alert, but no changes were specified.

Action: No action is required.

46567: Cannot modify, or delete built-in alert

Cause: The user attempted to alter, or delete a built-in alert.

Action: No action is required.

46568: Setting alert duration value to *string* failed.

Cause: An invalid value was specified for the alert duration.

Action: Provide an alert duration value in the valid range (>= 0).

46581: notification profile "*string*" already exists

Cause: Notification Profile already exists.

Action: Please try creating the Notification Profile with another name.

46582: cannot delete notification profile "*string*" as it is being used in alert definitions

Cause: Notification Profile is being used in Alert Definitions.

Action: Please try changing the Alert Definition to use a different Notification Profile name before deleting this one.

46583: notification profile "*string*" does not exist

Cause: Notification Profile does not exist.

Action: Please try specifying a valid Notification Profile name.

46584: "*string*" is not a well-formed e-mail address list

Cause: The specified e-mail address list was not well formed.

Action: Please try specifying a well-formed e-mail address list.

46585: notification template "*string*" already exists

Cause: Notification Template already exists.

Action: Please try creating the Notification Template with another name.

46586: "*string*" is not a well-formed e-mail address

Cause: The specified e-mail address was not well formed.

Action: Please try specifying a well-formed e-mail address.

46587: remedy *string* trouble ticket template "*string*" already exists

Cause: Trouble Ticket Template already exists.

Action: Please try creating the Template with another name.

46588: *string* is not one of *string* values

Cause: The specified value is not in the list of values expected for this entity.

Action: Please try choosing from the list of values.

46589: Warning level Alert and Critical level Alert cannot be mapped to the same Remedy Urgency level

Cause: Warning Alert and Critical Alert is mapped to the same Remedy Urgency level.

Action: Please try mapping them to different Remedy Urgency levels.

46591: No Enforcement Point configured for the Secured Target.

Cause: user tried to start a collection of type network for a secured target which has no enforcement point configured

Action: configure an enforcement point for the secured target and then try again

46592: firewall with name *string* and/or IP address *string* already exists.

Cause: user tries to register a firewall which already exists

Action: check the name and/or IP of the firewall then try again

46593: secured target address does not exist. cannot drop secured target address.

Cause: user tries to drop a secured target address which does not exist

Action: check the secured target address and then try again

46594: unable to resolve host *string*

Cause: the user did not provide an IP address when registering a host and the host name is not resolvable

Action: provide a valid IP address or a resolvable host name

46595: failed to drop host *string*. agent process may be running and needs to be stopped first before dropping. if you already stopped the agent, please wait for the agent to be fully stopped.

Cause: user tries to drop a host on which an agent process is running or the agent has not been fully stopped

Action: stop the agent process first and then try again

46596: host *string* has already been activated.

Cause: user tries to activate a host which has already been activated

Action: check the current status of the host

46597: no pending activation request for host *string*.

Cause: Activation request for agent on host was not found.

Action: Request activation for the agent.

46598: stop collection failed for plug-in:"*string*". plug-in does not exist.

Cause: User attempted to stop collection for a secured target using a plug-in that does not exist

Action: Check the plug-in specified in the command and re-try the command with a valid plug-in

46599: internal error *string string string string string*

Cause: Internal error occurred in Audit Vault.

Action: Contact Oracle Support Services.

46601: The authenticated user is not authorized with audit source

Cause: User is not authorized to send audit data on behalf of this audit source.

Action: Connect as the user who is associated with the source. Or grant this user appropriate authorization by changing the source's properties.

46602: Error on audit record insert as RADS partition full

Cause: RADS partition table is full.

Action: Purge the RADS partition table through archive.

46603: Error on audit record insert as RADS_INVALID table full

Cause: RADS_INVALID table is full.

Action: Need to purge RADS_INVALID table or make its size larger.

46604: Error on insert as Error table full

Cause: Error table is full.

Action: Need to purge the error table.

46605: There are more recovery entries than the maximum member can be returned

Cause: There are more recovery entries for this collector.

Action: Need to purge the old entries from the recovery table.

46606: There is no recovery entry for the given name

Cause: There was no recovery context matching to the given name.

Action: Need to check if the name was correct or if the recovery context was saved for this name.

46607: There are more configuration entries than the maximum member can be returned

Cause: There were more configuration entries for this collector.

Action: Need to reduce the configuration entries for this collector.

46608: Failed to drop Secured Target; Stored Procedure Auditing collection is in progress.

Cause: user tried to drop secured target while SPA job is running

Action: wait for SPA job to complete and then try again

46620: invalid interval *string* for data warehouse duration; must be positive

Cause: Invalid interval was specified for data warehouse duration.

Action: Specify valid interval, the interval should be positive.

46621: invalid start date *string* for data warehouse operation; must be less than *string*

Cause: Invalid start date was specified for data warehouse load/purge operation.

Action: Specify valid start date, the start date must be less than current date - warehouse duration.

46622: invalid number of days *string* for data warehouse operation; must be greater than 0

Cause: Invalid number of days was specified for data warehouse load/purge operation.

Action: Specify valid number of days, the number of days must be positive

46623: cannot execute warehouse operation; another operation is currently running

Cause: A warehouse operation was executed while another operation is currently running.

Action: Wait for the operation to complete before reissuing the command.

46624: invalid schedule *string* for data warehouse refresh schedule

Cause: Invalid schedule was specified for data warehouse refresh.

Action: Specify valid non-null schedule.

46625: invalid repeat interval *string* for data warehouse refresh schedule

Cause: Invalid schedule was specified for data warehouse refresh.

Action: Specify valid non-null repeat interval.

46626: invalid number of years *string* for audit data retention; must be positive

Cause: Invalid number of years was specified for audit data retention

Action: Specify valid number, the number should be positive.

46640: specified source name *string* was not found

Cause: Invalid source name was specified.

Action: Specify a valid source name.

46641: archive does not exist

Cause: Invalid archive id was specified.

Action: Specify valid archive ID.

46642: database audit type invalid

Cause: Invalid database audit type specified.

Action: Database audit type must be S for standard or F for FGA.

46643: audit frequency invalid

Cause: Invalid audit frequency specified.

Action: Audit frequency must be A for "by access" or S for "by session".

46644: return type invalid

Cause: Return type was invalid.

Action: Return type must be S for "success", F for "failure", or B for "both".

46645: privilege flag invalid

Cause: Privilege flag is invalid.

Action: The privilege flag must be Y or N.

46646: specified Agent name *string* was not found

Cause: Invalid Agent name was specified.

Action: Specify a valid Agent name.

46647: enforcement point does not exist

Cause: user tried to start/stop/remove an enforcement point which does not exist

Action: check if the enforcement point has actually been created and then try again

46648: Enforcement point is already suspended

Cause: user tried to stop an enforcement point which has already been stopped

Action: user cannot stop an enforcement point which has already been stopped

46649: Enforcement point is in resume state

Cause: user tried to start an enforcement point which has already been started

Action: user cannot start an enforcement point which has already been started

46650: At least one Enforcement Point is monitoring the Secured Target *string*.

Cause: user tried to drop a secured target which an enforcement point is monitoring

Action: stop the enforcement point and try again

46651: Retention Policy *string* is in use.

Cause: Operation failed because Retention Policy is in use.

Action: Delete the assignment of this Retention Policy to Secured Target(s) and try again.

46652: Cannot delete built-in Retention Policies.

Cause: Cannot delete built-in Retention Policies.

Action: None

46661: Service Name is too long.

Cause: Service Name failed length validation checks.

Action: Provide valid Service Name.

46671: High Availability is not configured.

Cause: Cannot perform operation as system is not configured for HA.

Action: Please configure HA and try again.

46672: unable to stage diagnostic file "*string*" for download

Cause: File copy operation failed while staging diagnostics file for download.

Action: Check for available disk space on /tmp and see if the diagnostics file exists in /usr/local/dbfw/tmp folder.

46673: IP address '*string*' is already in use on the network.

Cause: IP address is already in use on the network.

Action: Please specify a different IP address and try again.

46674: Illegal characters were supplied in password. Password must not contain characters outside of a-z, A-Z, 0-9, and . , + : _

Cause: Illegal characters were supplied in password. Password must not contain characters outside of a-z, A-Z, 0-9, dot, comma, plus, colon and underscore.

Action: Specify valid characters and try again.

46675: Current password is incorrect.

Cause: The current password supplied for authentication is incorrect.

Action: The user must supply the correct password associated with the account.

46676: User '*string*' already exists in the system.

Cause: User by that name already exists in the system.

Action: Please specify a different user name and try again.

46677: User name '*string*' is reserved for internal use.

Cause: User with specified name is reserved for internal use.

Action: Please specify a different user name and try again.

46800: normal, successful completion

Cause: Normal exit.

Action: None

46801: out of memory

Cause: The process ran out of memory.

Action: Increase the amount of memory on the system.

46821: generic CSDK error (line *number*)

Cause: There was a generic error in CSDK.

Action: Contact Oracle Support Services.

46822: no collector details for collector *string*

Cause: Collector is not properly set up in AV tables.

Action: Configure collector.

46823: attribute *string* is not valid for category

Cause: Collector attempted to set invalid attribute.

Action: Contact collector owner.

46824: type is not valid for attribute *string*

Cause: Collector attempted to set value of wrong type to attribute.

Action: Contact collector owner.

46825: invalid record

Cause: Collector attempted to pass invalid record.

Action: Contact collector owner.

46826: invalid parameter *string* (line *number*)

Cause: Collector attempted to pass invalid parameter.

Action: Contact collector owner.

46827: invalid context

Cause: Collector attempted to pass invalid context.

Action: Contact collector owner.

46828: OCI layer error *number*

Cause: OCI layer returned error.

Action: Contact collector owner.

46829: category *string* unknown

Cause: Collector attempted to pass category not configured in AV.

Action: Contact collector owner.

46830: null pointer (line *number*)

Cause: Collector attempted to pass null pointer.

Action: Contact collector owner.

46831: invalid source event id (*string*)

Cause: Collector passed source event id not suitable for category.

Action: Contact collector owner.

46832: internal error (line *number*), additional information *number*

Cause: Internal error occurred in CSDK.

Action: Contact Oracle Support Services.

46833: invalid error record

Cause: Collector attempted to pass invalid error record.

Action: Contact collector owner.

46834: missing attribute in error record

Cause: One or more attributes of error record is missing.

Action: Contact collector owner.

46835: duplicate error attribute

Cause: Collector attempted to set already set attribute.

Action: Contact collector owner.

46836: error record in use

Cause: Attempt to create a new error record before sending or dropping the previous one.

Action: Contact collector owner.

46837: missing eventid attribute in audit record

Cause: Event ID attributes of audit record is missing.

Action: Contact collector owner.

46838: Internal Error: Failed to insert *string* into *string* hash table

Cause: Core hash table insertion function failed.

Action: Contact collector owner.

46840: no smtp server registered

Cause: SMTP server is not registered.

Action: Please register SMTP server using avca register_smtp first.

46841: smtp server already registered

Cause: SMTP server is already registered.

Action: Please unregister SMTP server using avca register_smtp -remove first or use avca alter_smtp to update SMTP parameters.

46842: *string* command requires the *string* parameter

Cause: A required parameter is missing

Action: Please provide all the required parameters for the command.

46843: invalid value "*string*" specified for parameter *string*

Cause: A parameter was specified an invalid or incorrect value.

Action: Please provide correct values for the indicated parameter.

46844: no value specified for "*string*" in parameter *string*

Cause: No value was specified for a sub-parameter in a main parameter.

Action: Please provide correct values for the indicated parameter.

46845: input value "*string*" exceeds maximum allowed length of *string*

Cause: Input value exceeds the maximum allowed length.

Action: Please input a value within the allowed length limits.

46846: input value "*string*" in parameter *string* is not a number

Cause: Input value for port number must be a numeric value.

Action: Please input a numeric value for the port number.

46847: input value "*string*" for parameter *string* is not a valid email address

Cause: Input value does not seem to be a valid email address.

Action: Please input a valid email address in the form user@domain.

46848: smtp server is already in secure mode using protocol "*string*"

Cause: The specified SMTP server configuration is already secure using the protocol specified.

Action: Please use avca alter_smtp to change the protocol settings.

46849: smtp server is not configured to use a secure protocol

Cause: The specified SMTP server is not configured to use a secure protocol.

Action: Please use avca secure_smtp to specify a secure SMTP protocol first.

46850: file "*string*" does not exist

Cause: The specified file does not exist.

Action: Please specify a valid file.

46851: smtp integration is already enabled

Cause: The SMTP configuration registered with Audit Vault is already in enabled state.

Action: None

46852: smtp integration is already disabled

Cause: The SMTP configuration registered with Audit Vault is already in disabled state.

Action: None

46853: parameters "*string*" and "*string*" cannot be specified together

Cause: The user specified two mutually exclusive parameters

Action: Please provide one of the two parameters

46854: unsupported remedy version: "*string*"

Cause: The user specified an unsupported Remedy version.

Action: Please specify 6 or 7 for remedy.version.

46855: remedy server already registered

Cause: Remedy server is already registered.

Action: Please unregister the remedy server using avca register_remedy -remove first or use avca alter_remedy to update remedy parameters.

46856: no remedy server registered

Cause: Remedy server is not registered.

Action: Please register Remedy server using avca register_remedy first.

46857: remedy integration is already enabled

Cause: The Remedy configuration registered with Audit Vault is already in enabled state.

Action: None

46858: remedy integration is already disabled

Cause: The Remedy configuration registered with Audit Vault is already in disabled state.

Action: None

46859: remedy server is already in secure mode using protocol "*string*"

Cause: The specified Remedy server configuration is already secure using the protocol specified.

Action: None

46860: remedy server is not configured to use a secure protocol

Cause: The specified Remedy server is not configured to use a secure protocol.

Action: Please use avca secure_remedy to specify a secure Remedy protocol first.

46861: specified ticket id "*string*" does not exist in the remedy server database

Cause: Specified ticket does not exist in the Remedy Server.

Action: Please provide a ticket ID which exists in the Remedy Server.

46862: Email Template Name is too long.

Cause: Email Template Name failed length validation checks.

Action: Provide a valid Email Template Name.

46863: Email Template Description is too long.

Cause: Email Template Description failed length validation checks.

Action: Provide a valid Email Template Description.

46864: Email Template Subject is too long.

Cause: Email Template Subject failed length validation checks.

Action: Provide a valid Email Template Subject.

46901: internal error, *string*

Cause: There was a generic internal exception for OS Audit Collector.

Action: Contact Oracle Support Services.

46902: process could not be started, incorrect arguments

Cause: Wrong number of arguments or invalid syntax used.

Action: Please verify that all the required arguments are provided. The required arguments are Host name, Source name, Collector name and the Command.

46903: process could not be started, operating system error

Cause: The process could not be spawned because of an operating system error.

Action: Please consult the log file for detailed operating system error.

46904: collector *string* already running for source *string*

Cause: Collector specified was already running.

Action: Provide a different collector or source name.

46905: collector *string* for source *string* does not exist

Cause: Collector specified was not running.

Action: Provide a different collector or source name.

46906: could not start collector *string* for source *string*, reached maximum limit

Cause: No more collectors could be started for the given source.

Action: None

46907: could not start collector *string* for source *string*, configuration error

Cause: Some collector parameters were not configured correctly.

Action: Check the configuration parameters added during ADD_COLLECTOR.

46908: could not start collector *string* for source *string*, directory access error for *string*

Cause: Access to specified directory was denied.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46909: could not start collector *string* for source *string*, internal error: [*string*], Error code[*number*]

Cause: An internal error occurred while starting the collector.

Action: Contact Oracle Support Services.

46910: error processing collector *string* for source *string*, directory access error for *string*

Cause: Access to specified directory was denied.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46911: error processing collector *string* for source *string*, internal error: [*string*], [*number*]

Cause: An internal error occurred while processing the collector.

Action: Contact Oracle Support Services.

46912: could not stop collector *string* for source *string*

Cause: An error occurred while closing the collector.

Action: None

46913: error in recovery of collector *string* for source *string*: *string*

Cause: An error occurred while accessing the file.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46914: error in recovery of collector *string* for source *string*, internal error: [*string*], [*number*]

Cause: An internal error occurred while getting recovery information for collector.

Action: Contact Oracle Support Services.

46915: error in parsing of collector *string* for source *string*: *string*

Cause: An error occurred while accessing the file.

Action: Verify the path is correct and the collector has read permissions on the specified directory.

46916: error in parsing of collector *string* for source *string*, internal error [*string*], [*number*]

Cause: An internal error occurred while parsing data for collector.

Action: Contact Oracle Support Services.

46917: error processing request, collector not running

Cause: OS Audit Collector was not running and a command was issued.

Action: Start the collector using command START.

46918: could not process the command; invalid command

Cause: An invalid value was passed to the command argument.

Action: Please verify that a valid value is passed to command argument. The valid values are START, STOP and METRIC.

46919: error processing METRIC command; command is not in the required format

Cause: METRIC command was not in the required METRIC:XYZ format.

Action: Please verify that metric passed is in METRIC:XYZ format where XYZ is the type of metric (Example:- METRIC:ISALIVE).

46920: could not start collector *string* for source *string*, directory or file name *string* is too long

Cause: The name of directory or file was too long.

Action: Verify the length of the path is less than the system-allowed limit.

46921: error processing collector *string* for source *string*, directory or file name *string* is too long

Cause: The name of directory or file was too long.

Action: Verify the length of the path is less than the system-allowed limit.

46922: collector *string* for source *string* is not able to collect from event log, cannot open or process Windows event log :[*string*] Error code [*number*]

Cause: Windows event log could not be opened or processed.

Action: Verify event log exists.

46923: OCI error encountered for source database *string* access, audit trail cleanup support disabled.

Cause: An error was encountered while attempting to connect to or execute SQL statements on the source database.

Action: Verify source database and listener are up and connect information is correct.

46924: Corrupted recovery information detected for collector *string* for source *string*

Cause: Corrupted recovery information detected.

Action: Contact Oracle Support Services.

46925: error in parsing XML file *string* for collector *string* and source database *string* : error code *number*

Cause: An internal error occurred while parsing data for collector.

Action: Verify that collector has read permissions on the file and the file is in proper XML format. Contact Oracle Support Services for patch set.

46926: error in recovery of XML file *string* for collector *string* and source database *string* : error code *number*

Cause: An internal error occurred while parsing data for collector.

Action: Verify that collector has read permissions on the file and the file is in proper XML format. Contact Oracle Support Services for patch set.

46927: Syslog is not configured or error in getting audit files path for syslog for collector *string* and source database *string*.

Cause: One of the following occurred.

- facility.priority was not valid.

- There was no corresponding path for facility.priority setting.

- Source database was only returning facility and there was no corresponding path for facility.* setting.

Action: Configure syslog auditing to valid facility.priority setting and corresponding valid path. If source database only returning facility then contact Oracle Support Services for patch set.

46928: Collector *string* for source database *string* cannot read complete file *string*

Cause: File size is more than 2GB.

Action: File size should be less than 2GB. Please use log rotation to limit the file size to less than 2GB.

46941: internal error, on line *number* in file ZAAC.C, additional information *number*

Cause: There was a generic internal exception for AUD$ Audit Collector.

Action: Contact Oracle Support Services.

46942: invalid AUD Collector context

Cause: The AUD Collector context passed to collector was invalid.

Action: Make sure that context passed is the context returned by ZAAC_START.

46943: NULL AUD Collector context

Cause: The pointer to AUD Collector context passed to collector was NULL.

Action: Make sure that context passed is the context returned by ZAAC_START.

46944: conversion error in column *string* for <*string*>

Cause: The VARCHAR retrieved from AUD$ or FGA_LOG$ table could not be converted to ub4.

Action: Correct value in source database.

46945: bad recovery record

Cause: The recovery record retrieved from Audit Vault was damaged.

Action: None. The record will be corrected automatically.

46946: too many active sessions

Cause: The number of active sessions exceeded the specified number in the GV$PARAMETER table.

Action: Contact Oracle Support Services.

46947: CSDK layer error

Cause: CSDK layer returned error indication.

Action: Action should be specified in CSDK error report.

46948: already stopped

Cause: AUD collector already stopped because of previous fatal error.

Action: Restart collector.

46949: log level

Cause: Specified log level was invalid.

Action: Use legal log level (1,2,3).

46950: log file

Cause: An error occurred during the opening of the log file.

Action: Make sure that the log directory exists, and that the directory and log file are writable.

46951: bad value for AUD collector attribute

Cause: Specified collector attribute was invalid.

Action: Correct attribute value in Audit Vault table AV$ATTRVALUE.

46952: bad name for AUD collector metric

Cause: The specified metric name was undefined.

Action: Use a correct metric name.

46953: unsupported version

Cause: The specified version of the source database is not supported.

Action: Update to supported version.

46954: recovery context of 10.x

Cause: Source database (9.x) was incompatible with 10.x recovery context.

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46955: recovery context of 9.x

Cause: Source database (10.x) was incompatible with 9.x recovery context.

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46956: FGA_LOG$ table of 9.x

Cause: Source database (10.x) was incompatible with 9.x rows of FGA_LOG$.

Action: Clean up FGA_LOG$ table.

46957: RAC recovery context

Cause: Non-RAC source database was incompatible with RAC recovery context.

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46958: Non-RAC recovery context

Cause: RAC source database was incompatible with non-RAC recovery context.

Action: Clean up AUD$ and FGA_LOG$ tables and recovery context.

46959: bad authentication information

Cause: Incorrect format of authentication information in the column COMMENT$TEXT.

Action: Contact Oracle Support Services.

46960: bad metric request

Cause: Unknown metric name (%s) was provided in metric request.

Action: Contact Oracle Support Services.

46961: internal error on line *number* in file ZAAC.C; additional info |*string*|

Cause: There was a generic internal exception for AUD$ Audit Collector.

Action: Contact Oracle Support Services.

46962: Database Vault audit table is not accessible

Cause: Database Vault was not set up properly or the proper role was not granted to user being used by the collector.

Action: Set up Database Vault and make sure that DVSYS.AUDIT_TRAIL$ is accessible to the user being used by the collector.

46963: Some rows may have been missed by Audit Vault or may be duplicated

Cause: Collector encountered rows in the SYS.AUD$ or FGA_LOG$ tables with SESSIONID <= 0.

Action: Contact Oracle Support Services.

46964: Connector was not able to reconnect to Source Database

Cause: Maximum number of attempts to reconnect was exceeded.

Action: Verify connectivity and that the database is started.

46965: Attribute *string* is longer than 4000 bytes and was clipped

Cause: When attribute was converted to UTF8 encoding, it became longer than 4000 bytes.

Action: None. It was clipped automatically after conversion.

46966: Function AV_TRUNCATE_CLOB does not exist in source database

Cause: Latest version of script ZARSSPRIV.SQL was not run.

Action: None. Function created automatically.

46967: Audit Trail Cleanup package is not proper. Audit Trail Cleanup cannot be performed for source database.

Cause: Audit Trail Cleanup package was not proper.

Action: Contact Oracle Support Services.

46980: Firewall *string* part of a resilient pair

Cause: Operation not permitted when firewall is part of a resilient pair.

Action: Break the resilience and try the operation again.

46981: Unable to connect to Database Firewall with IP *string*.

Cause: Database Firewall is shutdown or unreachable, Audit Vault Server certificate is invalid or not yet valid because the date on the Database Firewall is out of sync with the Audit Vault Server certificate.

Action: Restart the Database Firewall, Copy the correct certificate and ensure that the date on Database Firewall is in sync with the Audit Vault Server and try again.

46982: Network configurations not identical. *string*

Cause: You may be trying to perform an operation like adding a resilient pair. Such operations require the network configuration on the Firewalls to be identical.

Action: Ensure that the network configuration is identical on the Firewalls and try again.

46983: Bridged interface *string* is not enabled on Firewall *string*.

Cause: When the mode is DPE, bridged interfaces must be enabled.

Action: Enable the bridged interface on the Firewall and retry operation.

46984: Firewalls not in the same resilient pair.

Cause: Only a resilient pair can be swapped. You cannot swap Firewalls from different resilient pairs.

Action: Ensure that the Firewalls are part of the same resilient pair and retry operation.

46985: Unable to create resilient pair because Firewall *string* has Enforcement Points configured.

Cause: The Firewalls being paired for resilience must not have any Enforcement Points configured.

Action: Please delete all Enforcement Points and try again.

46986: Firewall at IP address *string* does not have a valid Audit Vault Server certificate.

Cause: Audit Vault Server certificate is not present on the Firewall, or is invalid.

Action: Please supply server certificate on the Firewall UI.

46987: Firewall Name is too long.

Cause: Firewall Name failed length validation checks.

Action: Provide a valid Firewall Name.

46988: Invalid IP address '*string*'. IP address must be a valid IPv4 address.

Cause: IP address does not confirm to IPv4 standard.

Action: Please specify an IPv4 address and try again.

46990: More than one proxy interface specified.

Cause: In DPE mode, only one proxy interface must be specified.

Action: Specify one proxy most and retry the operation.

46991: Invalid monitoring mode (DAM) for proxy interface.

Cause: Monitoring mode must be DPE when proxy interface is specified.

Action: Specify DAM as monitoring mode.

46992: Enforcement Point mode cannot be DPE when the Firewall is in a resilient pair configuration.

Cause: Monitoring mode must be DAM when Firewall is in a resilient configuration.

Action: Specify DAM as monitoring mode.

46993: Full error message reporting can only be enabled if database response monitoring is enabled.

Cause: Database response monitoring not enabled.

Action: Please enable database response and try again.

46994: Enforcement Point Name is too long.

Cause: Enforcement Point Name failed length validation checks.

Action: Provide a valid Enforcement Point Name.

46995: Secured Target Address cannot be deleted.

Cause: There must be at least one address defined when there are active Enforcement Points.

Action: Add a new Secured Target Address and try again.

46996: Invalid IP addresses list. IP addresses list must be a space-separated list of valid IPv4 addresses. For example, '10.240.114.168 10.240.114.169'.

Cause: Invalid IP address list specified.

Action: The IP addresses must be valid IPv4 addresses and separated by spaces.

46997: Invalid Port '*string*'. Port must be a number between 1 and 65535.

Cause: Port Number is not between 1 and 65535.

Action: Specify a value between 1 and 65535 and try again.

46998: Invalid WAF session timeout '*string*'. WAF session timeout value is specified in minutes, and must be at least 30 and at most 1440.

Cause: WAF session time out must be at least 30 minutes and no more than a day.

Action: Please specify a valid time out value and try again.

46999: Database address, port number, database name and credentials must be specified in order to enable Database Interrogation.

Cause: User tried to enable database interrogation without specifying database address/port/database name/credentials

Action: Specify database address/port/database name/credentials and then try again

47000: Activation approval for agent on host *string* failed.

Cause: Activation request for agent on host was not found.

Action: Request activation for the agent.

47001: Agent deactivation for host *string* failed.

Cause: Agent Deactivation failed.

Action: Check if agent on the host is activated.

47002: Agent version *string* is invalid.

Cause: Agent version must be in 'YYYY-MM-DD HH24:MI:SS.FF3 TZHTZM' format

Action: Check the agent version.

47003: Agent on host *string* is incompatible with Audit Vault Server.

Cause: Agent version is not supported by the Audit Vault Server.

Action: Upgrade the agent to the latest version.

47101: Invalid job name specified.

Cause: Job name must be a valid SQL identifier.

Action: Enter a valid job name.

47102: Repository storage is not upgraded to use ASM.

Cause: Repository storage is not upgraded to use ASM.

Action: Upgrade repository storage to ASM and try again.

47103: ARCHIVE disk group does not exist.

Cause: ARCHIVE disk group must exist.

Action: Please create ARCHIVE disk group and try again.

47104: Invalid transfer type.

Cause: Specified transfer type is not supported.

Action: Please specify a transfer type that is supported and try again.

47105: Invalid authentication method.

Cause: Specified authentication method is not supported.

Action: Please specify a valid authentication method and try again.

47106: Archive Location Name is too long.

Cause: Archive Location Name failed length validation checks.

Action: Provide valid Archive Location Name.

47107: Invalid Archive Location Name.

Cause: Archive Location Name contains illegal characters.

Action: Provide a valid Archive Location Name.

47108: Failed to create Archive Location "*string*". The name is reserved.

Cause: Reserved name cannot be used for Archive Location Names.

Action: Use another name for Archive Location Name.

47109: Failed to modify Archive Location "*string*". Reserved Archive Locations can not be modified.

Cause: A reserved archive location, once added, cannot be modified.

Action: Do not delete or change reserved archive location.

47110: Failed to create Archive Location "*string*". Another Archive Location with the same name exists.

Cause: An existing Archive Location Name conflicts with a reserved name.

Action: Delete or rename the existing Archive Location Name and retry operation.

47111: Cannot drop disk from 'ARCHIVE' disk group with archived data.

Cause: Archived data is present in the disk group.

Action: Add another disk to disk group or wait until the archive period expires.

47112: Cannot drop Archive Location. It is being used to store archived data.

Cause: Specified Archive Location is being used to store archive data.

Action: Wait until the archive period expires.

47201: Operation not permitted. User must be an admin.

Cause: The user passed in is not an admin.

Action: Specify an admin and retry the operation.

47202: Operation not permitted. User must be an auditor.

Cause: The user passed in is not an auditor.

Action: Specify an auditor and retry the operation.

47203: Operation not permitted. User must be a super admin.

Cause: The user passed in is not a super admin.

Action: Specify a super admin and retry the operation.

47204: Operation not permitted. User must be a super auditor.

Cause: The user passed in is not a super auditor.

Action: Specify a super auditor and retry the operation.

47205: Operation not permitted on this user

Cause: This is operation not permitted on this user.

Action: None

47301: SAN Server with the name '*string*' already exists.

Cause: Storage names are unique across the system.

Action: Specify a different storage name and try again.

47302: SAN Server with the name '*string*' does not exist.

Cause: A SAN Server with that name already exists in the system.

Action: Specify a different storage name and try again.

47303: iSCSI Target already in session.

Cause: An attempt was made to log into a target that is already in session.

Action: Specify another target or logout from this target and try again.

47304: iSCSI Target not in session.

Cause: An attempt was made to logout from a target that is not in session.

Action: Specify another target or login to this target and try again.

47305: No SAN Server found for IP Address=*string*, Port=*string* and Method=*string*.

Cause: No matching SAN Servers were found.

Action: Please register this SAN Server or specify different values

47306: Invalid method *string* for iSCSI target discovery. Must be 'SENDTARGETS' or 'iSNS'.

Cause: Discovery method must be 'SENDTARGETS' or 'iSNS'

Action: Specify a valid method and try again.

47307: SAN Server with IP Address=*string*, Port=*string* and Method = *string* already exists.

Cause: SAN Server with the specified configuration already exits.

Action: Try with different values for IP Address, Port and Method.

47308: Disk *string* does not exist.

Cause: Disk specified is not an existing disk in the system.

Action: Specify an existing disk and try again.

47309: Disk *string* not is part of the disk group *string*.

Cause: Disk specified is not part of an existing disk group.

Action: Specify a disk that is a member of a disk group and try again.

47310: Disk *string* cannot be removed. Please try after *number* minutes

Cause: ASM rebalance operation is in progress.

Action: Please try again.

47311: Invalid disk group *string* specified.

Cause: disk group must be one of 'SYSTEMDATA', 'RECOVERY', 'EVENTDATA' or 'ARCHIVE'.

Action: Please try again with a valid disk group.

47312: Disk *string* already member of a disk group.

Cause: Disk already part of disk group

Action: Please try again with a different disk.

47314: SAN Server Name is too long.

Cause: SAN Server Name failed length validation checks.

Action: Provide valid SAN Server Name.

47315: Unable to logout from iSCSI target. Disk *string* in use

Cause: The disk is being used by a disk group.

Action: Drop the disk from the disk group and try again.

47316: Illegal characters were supplied in CHAP secret.

Cause: Illegal characters were supplied in CHAP secret.

Action: Specify valid characters and try again.

47317: Illegal characters were supplied in CHAP name.

Cause: Illegal characters were supplied in CHAP name.

Action: Specify valid characters and try again.

47318: CHAP secret must contain at least 8 characters and at most 30 characters.

Cause: CHAP secret failed length validation checks.

Action: Provide valid CHAP secret.

47319: CHAP Name is too long.

Cause: CHAP Name failed length validation checks.

Action: Provide valid CHAP Name.

47320: iSCSI Name is too long.

Cause: iSCSI Name failed length validation checks.

Action: Provide valid iSCSI Name.

47321: Invalid iSCSI Name.

Cause: iSCSI Name does not conform to standards.

Action: Provide a valid iSCSI Name.

47322: Invalid SAN Server Name.

Cause: SAN Server contains illegal characters.

Action: Provide a valid SAN Server Name.

47323: Invalid Disk Name.

Cause: ASM disk name contains illegal characters.

Action: Provide a valid ASM disk name.

47324: Connection to IP Address = *string*, Port = *string* timed out.

Cause: Network connection to the specified address timed out.

Action: Please check the address and try again.

47325: Connection to IP Address = *string*, Port = *string* refused.

Cause: Network connection to the specified address was refused by the remote server.

Action: Please check the address and try again.

47326: Login failed. Invalid CHAP name/secret.

Cause: Incorrect CHAP credentials specified.

Action: Please specify correct CHAP credentials and try again.

47327: Specified target is not a discovered target.

Cause: Target must be first discovered before performing this operation.

Action: Please discover the target and try this operation again.

47328: Cannot drop SAN Server. Active sessions found.

Cause: Active sessions for nodes from this SAN server exist.

Action: Please logout of these sessions and try again.

47329: iSCSI subsystem may have been manually configured. Please delete the configuration and try again.

Cause: iSCSI subsystem is not configured using AVDF UI or AVCLI.

Action: Please delete the configuration and try again.

47330: Cannot drop disk from *string* disk group. This operation requires *number* MB of free space in the disk group

Cause: Disk group rebalance operation will fail.

Action: Add more disks to the disk group and try again.

47401: The remote file system is busy.

Cause: There are open file(s) on the file system.

Action: Close file(s) and retry operation; or use force option.

47402: Unable to mount export *string* from host *string*.

Cause: AVS is not given client access or cannot contact server.

Action: Check server export and add AVS system to allowed client list

47403: The path *string* is not a relative path.

Cause: Remote location destination path must be a relative path

Action: Provide a relative path without the leading / character

47404: The path *string* is not an absolute path.

Cause: Remote location destination path must be a relative path

Action: Provide a relative path without the leading / character

47405: Remote file system mount point still exists.

Cause: Remote file system was not unmounted before delete operation.

Action: Unmount the remote file system (with force option if necessary).

47406: Unexpected character(s) in remote destination path.

Cause: Remote destination path contains illegal character(s).

Action: Remove characters that are not letters, numbers, space or _ . : , +

47407: file system name *string* is not unique.

Cause: A duplicate file sytem name is already in use.

Action: Pick a different file system name.

47408: Location name *string* is not unique.

Cause: A duplicate location name is already in use.

Action: Pick a different location name.

47409: Absolute path does not exist on remote file system

Cause: The constructed path is missing or outside of the remote file system.

Action: Make sure remote location resolves to a valid directory on the remote file system.

47410: User Oracle cannot write to absolute path

Cause: The constructed path's permission does not allow oracle write access.

Action: Change the NFS export permission or directory permission to allow oracle write access.

47503: Cannot stop trail of type "*string*" at "*string*" for secured target "*string*"; audit trail does not exist.

Cause: User attempted to stop a trail which does not exist

Action: One cannot stop audit trail which does not exist

47504: Cannot stop trail of type "*string*" at "*string*" for secured target "*string*"; audit trail is already stopped.

Cause: User attempted to stop a trail which is already stopped

Action: User cannot stop an audit trail which is already stopped

47552: Invalid user name *string*. User name should contain only alphanumeric characters, underscore (_), dollar sign ($), and pound sign (#).

Cause: An invalid user name is specified.

Action: Provide a simple SQL name as user name, which should be a non quoted identifier contains only alphanumeric characters from your database character set and the underscore (_), dollar sign ($), and pound sign (#).

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X