Oracle® Audit Vault and Database Firewall

Administrator's Guide

Release 20
E93408-33
February 2025

Oracle Audit Vault and Database Firewall Administrator's Guide, Release 20

E93408-33

Contents

3 General Security Guidelines

4 Configuring Audit Vault Server

5 Configuring Database Firewall

6 Registering Hosts and Deploying the Agent

7 Configuring Targets, Audit Trails, and Database Firewall Monitoring Points

8 Using the Host Monitor Agent

9 High Availability in Oracle AVDF

15 Managing the Audit Vault Server and Database Firewalls

B System Configuration Utilities

C Plug-In Reference

D Transaction Log Audit Data Collection for Oracle Database

E Transaction Log Audit Data Collection for Microsoft SQL Server

M Multiple Network Interface Cards

Preface

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

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

See Oracle Audit Vault and Database Firewall Release 20 Books.

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.

Translation

This topic contains translation (or localization) information for Oracle AVDF User Interface and Documentation.

The Web based User Interface or the Audit Vault Server console is translated and made available in the following languages. This includes the User Interface, error messages, and help text.

- French
- German
- Italian
- Japanese
- Korean
- Spanish
- Portuguese - Brazil
- Chinese - Traditional
- Chinese - Simplified

Oracle AVDF Documentation is available in the following languages:

- English
- Japanese

Quick Reference for Common Tasks

This section lists some of the common tasks performed using Oracle Audit Vault and Database Firewall.

About this Quick Reference

This chapter is intended for users who are familiar with Oracle Audit Vault and Database Firewall (Oracle AVDF), and who want to locate step-by-step instructions for common tasks. If you are new to Oracle AVDF, then we recommend that you read the documentation to understand the product and plan your configuration.

See Summary of Configuration Steps to understand the workflows for configuring Oracle Audit Vault and Database Firewall

Audit Vault Server

System Settings

"Specifying the Server Date, Time, and Keyboard Settings"

"Changing the Primary Audit Vault Server Network Configuration"

"Changing the UI (Console) Certificate for Audit Vault Server"

"Configuring or Changing the Audit Vault Server Services"

"Configuring Audit Vault Server Syslog Destinations"

"Configuring Email Notifications"

"Testing Audit Vault Server System Operations"

"Data Encryption on Upgraded Instances"

Archiving and Retrieving

"Defining Archive Locations"

"Creating Archive and Retention Policies"

"Deleting Archive and Retention Policies"

"Starting an Archive Job Manually"

"Retrieving Oracle Audit Vault and Database Firewall Audit Data"

High Availability Configuration of Audit Vault Servers

"Configure the Designated Standby Audit Vault Server"

"Configure the Designated Primary Audit Vault Server"

"Checking the High Availability Status of an Audit Vault Server"

"Post High Availability Pairing Steps"

"Disabling or Enabling Failover of the Audit Vault Server"

AVCLI (Command Line Interface)

"Downloading the AVCLI Command Line Utility and Setting JAVA_HOME"

"About Logging in to AVCLI"

"Displaying Help and the Version Number of AVCLI"

"Running AVCLI Scripts"

"Specifying Log Levels for AVCLI"

"AVCLI Commands Reference"

Other Operations

"Backup and Restore of Audit Vault Server"

"Rotating the Master Key for Repository Encryption"

"Changing the Keystore Password"

"Enabling Oracle Database In-Memory for the Audit Vault Server"

"Monitoring Jobs"

"Checking Server Status and System Operation"

"Accessing the Audit Vault Server Certificate and Public Key"

"Restarting or Powering Off the Audit Vault Server"

"Changing the Keyboard Layout"

"Running Diagnostics Checks for the Audit Vault Server"

Database Firewall

Firewall System Settings

"Configuring Network Settings for Oracle Database Firewall"

"Configuring Network Services for Oracle Database Firewall"

"Setting the Date and Time in Database Firewall"

"Specifying the Audit Vault Server Certificate and IP Address"

"Viewing the Status and Diagnostics Report for Database Firewall"

Firewall Network Configuration

"Configuring Network Settings"

"Configuring the Database Firewall As a Traffic Proxy"

"Viewing Network Traffic for a Database Firewall"

Managing Database Firewalls in the Audit Vault Server

"Registering Database Firewall in Audit Vault Server"

"Restarting or Powering Off Database Firewall"

"Removing Database Firewall from Audit Vault Server"

"Fetching an Updated Certificate from Database Firewall"

High Availability Pairing of Database Firewalls

"High Availability for Database Firewall in Host Monitor Agent or Out of Band Modes"

"Swapping Roles Between Primary and Standby Database Firewalls"

"Unpair Primary and Standby Database Firewalls"

Hosts

"Registering Hosts on the Audit Vault Server"

"Changing Host Names"

"Deleting Hosts from Audit Vault Server"

"Deploying Plug-ins and Registering Plug-in Hosts"

"Removing Plug-ins"

Agent

Agent Deployment

"Steps Required to Deploy and Activate the Audit Vault Agent"

"Deploying the Audit Vault Agent"

"Activating and Starting the Audit Vault Agent"

"Unregistering the Audit Vault Agent as a Windows Service"

"Stopping and Starting the Agent on Unix Hosts"

"Stopping and Starting the Agent on Windows Hosts"

"Changing the Logging Level for the Audit Vault Agent"

"Deactivating and Removing Audit Vault Agent"

Updating Agent

"Updating Audit Vault Agent"

Host Monitor Agent

Host Monitor Agent Installation

"Registering the Host Machine That Will Run the Host Monitor Agent"

"Deploying the Host Monitor Agent on a Windows Host Machine" or "Deploying the Host Monitor Agent on a Unix Host Machine"

"Creating a Target for the Host-Monitored Database"

"Creating a Monitoring Point for the Host Monitor Agent"

Host Monitor Agent Operations

"Starting the Host Monitor Agent"

"Stopping the Host Monitor Agent"

"Changing the Logging Level for a Host Monitor Agent"

"Checking the Status of a Host Monitor Agent Audit Trail"

"Uninstalling a Host Monitor Agent (Unix Hosts Only)"

Updating

"Updating a Host Monitor Agent (Unix Hosts Only)"

Host Monitor Agent Security

"Using Mutual Authentication for Communication Between the Database Firewall and the Host Monitor Agent"

Targets

Registering and Managing

"Registering Targets"

"Removing Targets"

"Creating a Target Group"

"Managing User Access Rights to Targets and Groups"

Auditing

Preparing for Auditing

"Preparing Targets for Audit Data Collection"

"Using an NTP Service to Set Time on Targets"

"Ensuring that Auditing is Enabled on the Target"

"Setting User Account Privileges on Targets"

"Scheduling Audit Trail Cleanup"

Audit Trails

"Adding Audit Trails with Agent-Based Collection"

"Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server"

"Checking the Status of Trail Collection on the Audit Vault Server"

"Deleting an Audit Trail"

"Running the XML Transformation Utility for MySQL Audit Formats"

Monitoring with Database Firewall

Database Firewall Monitoring Points

"Creating and Configuring a Database Firewall Monitoring Point"

"Modifying a Database Firewall Monitoring Point"

"Starting, Stopping, or Deleting Database Firewall Monitoring Points"

"Viewing the Status of Database Firewall Monitoring Points"

"Finding the Port Number Used by a Database Firewall Monitoring Point"

Native Network Encrypted Traffic Monitoring

"Configuring Advanced Settings for Database Firewall"

"Changing the Database Firewall Host Name"

"Configuring Database Firewall for Databases That Use Native Network Encryption"

"Monitor Native Network Encrypted Traffic Through Database Firewall for Oracle Databases"

"Disabling Encrypted Traffic Monitoring for Oracle Databases"

Other Administrator Tasks

"Downloading the Oracle Audit Vault and Database Firewall SDK"

"Monitoring and Adding Server Tablespace Space Usage"

"Monitoring Server Archive Log Disk Space Use"

"Monitoring Server Flash Recovery Area"

"Backup and Restore of Audit Vault Server"

Reference Information

Plug-ins

About Plug-ins

Summary of Data Collected for Each Audit Trail Type

Scripts for Oracle AVDF Account Privileges on Targets

Audit Trail Cleanup

Target Locations (Connect Strings)

Audit Collection Attributes

Audit Trail Locations

Other Reference Information

AVCLI Commands Reference

Transaction Log Audit Data Collection for Oracle Database

Ports Used by Oracle Audit Vault and Database Firewall

Troubleshooting Oracle Audit Vault and Database Firewall

Oracle AVDF 20 Cookbook

Cookbook: Oracle Audit Vault and Database Firewall 20 for Beginners

Part I

Getting Started with Oracle Audit Vault and Database Firewall

Learn to configure Oracle Audit Vault and Database Firewall.

Part I describes how to configure a basic Oracle Audit Vault and Database Firewall system. Part I takes you from a new installation through the process of configuring the Oracle Audit Vault and Database Firewall components.

This part contains the following chapters:

1

Changes in Oracle Audit Vault and Database Firewall Release 20

To learn what's new in the latest release of Oracle AVDF, 20.13, see the Oracle AVDF Release Notes guide.

2

Introducing Oracle Audit Vault and Database Firewall

To begin using Oracle Audit Vault and Database Firewall (Oracle AVDF), perform preliminary tasks, such as downloading the latest version of this manual and understanding the basic Oracle AVDF concepts.

2.1 Downloading the Latest Version of This Manual

Learn how to download the latest documentation for Oracle Audit Vault and Database Firewall.

Download the latest version of this manual from the following website:

https://docs.oracle.com/en/database/oracle/audit-vault-database-firewall/20/sigad/index.html

Find documentation for other Oracle products at the following website:

https://docs.oracle.com

2.2 Learning About Oracle Audit Vault and Database Firewall

Understanding the basic concepts of Oracle Audit Vault and Database Firewall is key to a successful Oracle AVDF deployment.

Oracle recommends that you read *Oracle Audit Vault and Database Firewall Concepts Guide* to understand the features, components, users, and deployment procedures of Oracle AVDF.

2.3 Supported Platforms for Oracle Audit Vault and Database Firewall

You can run Oracle Audit Vault and Database Firewall on various platforms.

Oracle Audit Vault and Database Firewall (Oracle AVDF) consolidates activity audit data from Oracle and non-Oracle databases, operating systems, and directories. It provides security and compliance reports through an accurate SQL grammar based engine. Database Firewall monitors SQL traffic and blocks unauthorized SQL.

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

2.4 Oracle Audit Vault and Database Firewall System Features

Learn about the system features of Oracle Audit Vault and Database Firewall.

Topics

2.4.1 About Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (Oracle AVDF) protects your IT infrastructure by monitoring activity, blocking intrusion attempts, collecting audit data, enacting customizable firewall rules, and assessing Oracle database configuration.

Oracle AVDF secures databases and other critical components of your IT infrastructure, such as operating systems, in the following ways:

- Provides a database firewall that monitors activity and can block SQL statements on the network based on your firewall policy.
- Collects audit data and presents the data in audit reports.
- Enables you to 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*.

We strongly recommend that you read *Oracle Audit Vault and Database Firewall Concepts Guide* for more information on the features, components, users, and deployment of Oracle AVDF.

2.4.2 Security Technical Implementation Guides for Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (Oracle AVDF) is compliant with the Security Technical Implementation Guides (STIG) standards.

To learn about Oracle AVDF compliance with STIG standards see the Security Technical Implementation Guides.

2.4.3 System Requirements for Oracle Audit Vault and Database Firewall

Read about the Oracle AVDF hardware and software requirements.

For hardware and software requirements, see *Oracle Audit Vault and Database Firewall Installation Guide*.

2.4.4 Supported Targets for Oracle Audit Vault and Database Firewall

Learn about Oracle Audit Vault and Database Firewall targets.

A target is a database or non-database product that you secure using either the Audit Vault Agent, the Database Firewall, or both. If the target, whether or not it is a database, is supported by the Audit Vault Agent, then you can deploy the Agent on that target's host computer and collect audit data from the internal audit tables and operating system audit files.

If the target is a database, then you can monitor or block its incoming SQL traffic with Database Firewall.

Oracle Audit Vault and Database Firewall supports various target products out of the box in the form of built-in plug-ins.

See Also:

- About Plug-ins
- Plug-In Reference for detailed information on each plug-in.
- Table C-1 for supported target products and versions.
- Table C-22 for the data collected and platforms supported for each audit trail type.
- Configuring Quick JSON Target Type to Collect Audit Data from MongoDB
- *Oracle Audit Vault and Database Firewall Developer's Guide* for information on creating custom plug-ins to capture audit trails from more target types using the Oracle AVDF SDK.

2.4.5 Oracle Audit Vault and Database Firewall Administrative Features

You can use Oracle Audit Vault and Database Firewall administrative features to manage targets and their hosts, firewalls, and other features.

You can use Oracle Audit Vault and Database Firewall administrative features to configure and manage the following:

- Targets
- Database Firewalls
- High Availability
- Third party integrations
- Audit Vault Agent deployment
- Audit trail collection
- Audit data lifecycle, archiving, and purging
- Microsoft Active Directory or OpenLDAP

2.4.6 Oracle Audit Vault and Database Firewall Auditing Features

Learn about Oracle Audit Vault and Database Firewall auditing features.

Oracle Audit Vault and Database Firewall auditing features enable you 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 e-mail notifications
- Security assessment and drift management

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed information about these auditing features

2.4.7 Integrating Oracle Audit Vault and Database Firewall with Oracle Key Vault

You can integrate Oracle Audit Vault and Database Firewall with Oracle Key Vault.

Oracle Key Vault events are collected by Oracle Audit Vault and Database Firewall.

See *Oracle Key Vault Administrator's Guide* for instructions about integrating Oracle Key Vault with Oracle Audit Vault and Database Firewall

2.5 Separation of Duties

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

To provide greater security, the Oracle Audit Vault and Database Firewall **administrator** and **auditor** roles have different user interfaces, and different user accounts. This separation of interfaces and accounts ensures that there is a separation of duties between these two roles. In addition to these Oracle Audit Vault and Database Firewall user accounts, you can also set up user accounts on your targets as necessary to access targets for collecting audit data. This is needed by the Audit Vault Agent for connecting to the target and collecting the audit data from the audit trails. Oracle Audit Vault and Database Firewall provides scripts to set up these user accounts on database targets, and guidance for other types of targets.

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

Table 2-1 Oracle Audit Vault and Database Firewall User Accounts

Account	Description
Super Administrator	Super administrators configure and maintain the Oracle Audit Vault and Database Firewall system, including Audit Vault Server settings such as network settings, high availability, data retention policies, etc. The super administrator can create other administrators or super administrators, and has access to all targets. The super administrator can also grant access to specific targets to other administrators.
Administrator	The administrator can perform a subset of the system configuration tasks that a super administrator can, such as registering hosts and targets, running archive jobs, etc. Administrators can also manage targets for which they have been granted access by a super administrator. An administrator cannot create another administrator. This can be performed by a super administrator only.

Table 2-1 (Cont.) Oracle Audit Vault and Database Firewall User Accounts

Account	Description
Super Auditor	The super auditor can create firewall policies, provision audit policies for Oracle Database targets, and specify settings for target such as whether to enable stored procedure auditing. Super auditors also generate reports, and create alerts and notifications. The super auditor can access all targets, create auditor or super auditor users, and grant access to specific targets to those users.
Auditor	Auditors can perform all the functions of super auditors, but only for the targets to which they have access.

Additional accounts are provided for diagnostics and used under the guidance of Oracle Support.

2.6 Understanding the Administrator's Role

Oracle AVDF administrators can configure system settings, create connections and targets, deploy agents, configure audit trails, and more.

Oracle AVDF Administrator Tasks

As an Oracle Audit Vault and Database Firewall administrator, your tasks include:

- Configuring the system settings on Audit Vault Server.
- Configuring connections to host computers on which you deployed Audit Vault Agent. This is usually the same computer as your targets.
- Creating targets on Audit Vault Server for each database or operating system that you are monitoring.
- Deploying and activating Audit Vault Agent on target host computers.
- Configuring audit trails for targets that Audit Vault Agent monitors.
- Configuring Database Firewall on your network.
- Creating Database Firewall monitoring points for targets.
- Backing up and archiving audit and configuration data.
- Creating administrative users and managing access (super administrator only).
- Configuring Microsoft Active Directory or OpenLDAP.
- Creating high availability for Audit Vault Server.

Administrator Roles in Oracle AVDF

There are two Oracle AVDF administrator roles with different target access levels:

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

2.7 Planning Your Oracle Audit Vault and Database Firewall System Configuration

Learn about planning your system configuration for Oracle AVDF.

2.7.1 Guidance for Planning Your Oracle Audit Vault and Database Firewall Configuration

Learn about the steps for planning your Oracle Audit Vault and Database Firewall configuration.

The steps in this section summarize the planning steps with links to specific instructions in this user guide.

> **See Also:**
>
> Oracle Audit Vault and Database Firewall Concepts Guide for guidance on planning deployments of Oracle Audit Vault Server, Oracle Audit Vault Agent, and Oracle Database Firewall.

2.7.2 Step 1: Plan Your Oracle Audit Vault Server Configuration

Plan your Oracle Audit Vault Server configuration.

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

> **See Also:**
>
> - Configuring Audit Vault Server for information on the Oracle Audit Vault Server configuration settings.
> - High Availability in Oracle AVDF for information about setting up resilient pairs of Oracle Audit Vault Servers.
> - Integrating Oracle Audit Vault and Database Firewall with Microsoft Active Directory or OpenLDAP for authenticating users connecting to the Audit Vault Server console.

2.7.3 Step 2: Plan Your Oracle Database Firewall Configuration

Learn how to plan your Oracle Database Firewall configuration.

If you are using Oracle Database Firewall, then plan how many you need, which target databases they will protect, where to place them in the network, whether they will be for monitoring only or for monitoring and blocking mode, and whether to configure a resilient pair

of firewalls. Also plan whether to change the Oracle Database Firewall network configuration that was specified during installation.

Following are the list of activities you would like to review:

- Overview of Oracle Database Firewall Deployment for information on different deployment types available.
- Configuring Database Firewall for information about the Oracle Database Firewall configuration settings.
- High Availability in Oracle AVDF for information on setting up resilient pairs of firewalls.

2.7.4 Step 3: Plan Your Oracle Audit Vault Agent Deployments

If you're deploying the Audit Vault Agent, determine the targets for which you want to collect audit data and identify their host computers.

You register these hosts with Oracle Audit Vault and Database Firewall (Oracle AVDF) and deploy the Audit Vault Agent on each of them. Then you register each target in the Audit Vault Server.

Note:

Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

See Also:

- Registering Hosts and Deploying the Agent
- Discovering and Registering Targets and Creating Groups

2.7.5 Step 4: Plan Your Audit Trail Configurations

If you're deploying the Audit Vault Agent or using agentless collection (Oracle AVDF 20.9 and later) to collect audit data, then you need to configure audit trails.

Use these guidelines to plan audit trail configurations for the targets from which you want to extract audit data. The type of audit trail that you select depends on the target type, and in the case of an Oracle Database target, the type of auditing that you've enabled in Oracle Database.

To plan the target audit trail configuration:

1. Ensure that auditing is enabled on the target. For Oracle Database targets, find the type of auditing that Oracle Database uses.

   See Ensuring that Auditing is Enabled in a Target.

2. If you're deploying the Audit Vault Agent, ensure that it's installed on a host computer. This is also called the agent machine.

   See Deploying the Audit Vault Agent on Host Computers.

   > **Note:**
   >
   > Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

3. Determine which type of audit trail to collect.

   See Table C-22 for the types of audit trails that you can configure for each target type and supported platform.

4. Familiarize yourself with the procedures to register a target and configure an audit trail.
   - Discovering and Registering Targets and Creating Groups
   - Configuring and Managing Audit Trail Collection

5. If you're collecting audit data from MySQL or IBM DB2 targets, see the additional steps in the following topics:
   - Prerequisites for Adding Audit Trails in Oracle Audit Vault Server
   - Requirements for SQL Server, Sybase ASE, and IBM DB2 Databases
   - Running the XML Transformation Utility for MySQL Audit Formats

> **See Also:**
>
> Requirements for Collecting Audit Data from Targets

2.7.6 Step 5: Plan for High Availability

Learn how to plan for high availability.

In this step, consider the high availability options that are outlined in "High Availability in Oracle AVDF".

2.7.7 Step 6: Plan User Accounts and Access Rights

Learn how to plan your user accounts and their access rights.

As a super administrator, you can create other super administrators and administrators. Super administrators can see and modify any target. Administrators have access to the targets that you enable them to access. In this step, determine how many super administrators and

administrators you create accounts for, and to which targets the administrators will have access.

> **See Also:**
>
> Managing User Accounts and Access

2.8 Summary of Configuration Steps

Learn about the Oracle AVDF configuration steps.

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

2.8.1 Configuring Oracle Audit Vault and Database Firewall and Deploying the Agent

Use this procedure to configure Oracle Audit Vault and Database Firewall (Oracle AVDF) and deploy the Audit Vault Agent or configure agentless collection (Oracle AVDF 20.9 and later).

1. Configure the Audit Vault Server. See Configuring Audit Vault Server.
2. If you're deploying the Audit Vault Agent, register the host computers where you'll deploy the Audit Vault Agent. Then deploy and start the Audit Vault Agent on those hosts. See Registering Hosts and Deploying the Agent.

   > **Note:**
   >
   > Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

3. Create user accounts on your targets for Oracle AVDF. See Scripts for Oracle AVDF Account Privileges on Targets.
4. Register the targets that you're monitoring in the Audit Vault Server, configure data retention policies, and configure audit trails for these targets. See Configuring Targets, Audit Trails, and Database Firewall Monitoring Points.

After you configure the system as an administrator, the Oracle AVDF auditor creates and provisions audit policies for targets and generates various reports.

2.8.2 Configuring Oracle Audit Vault and Database Firewall and Deploying Oracle Database Firewall

Configure and deploy Oracle Audit Vault and Database Firewall to enable you to create firewall policies and assign them to the targets.

Complete this procedure to configure and deploy Oracle Audit Vault and Database Firewall.

1. Configure the basic Oracle Database Firewall settings and associate the firewall with Oracle Audit Vault Server. Then configure the firewall on your network.

   See "Configuring Database Firewall".

2. Configure Oracle Audit Vault Server and associate each Oracle Database Firewall with the server.

   See "Configuring Audit Vault Server".

3. Register the targets that you are monitoring with Oracle Database Firewall in Oracle Audit Vault Server. Then configure the monitoring points for these targets. Optionally, if you want to also monitor the database response to SQL traffic, then use the scripts and configuration steps.

   See "Configuring Targets, Audit Trails, and Database Firewall Monitoring Points"

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

2.9 Using Audit Vault Server Console

Learn how to log in and use Audit Vault Server console.

2.9.1 Log in to Audit Vault Server Console

Learn how to log in to Audit Vault Server console.

When you first log in after installing Audit Vault Server:

- you must set up a password for *root* user
- create a super administrator or super auditor

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Installation Guide* for information on post-installation tasks.

To log in to Oracle Audit Vault Server Console:

1. From a browser, enter the following URL:

   `https://host/`

   where `host` is the server on which you installed Oracle Audit Vault Server.

For example:

```
https://192.0.2.1/
```

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

> **See Also:**
>
> Changing the UI (Console) Certificate for Audit Vault Server for more information on providing a new UI Certificate to avoid the certificate message in future

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

   The Dashboard page appears.

> **Note:**
>
> The Audit Vault Server console has a maximum idle time of 30 minutes. Upon launching the console, it can be used up to a maximum of 8 hours actively. The session times out if the idle time reaches 30 minutes or 8 hours after the initial launch.

2.9.2 Log in to Database Firewall Console

Learn how to log in to Database Firewall Console.

Starting with Oracle Audit Vault and Database Firewall release `20.1.0.0.0`, you can perform Database Firewall related tasks on the Audit Vault Server console.

1. Log in to Audit Vault Server console.
2. Click the **Database Firewalls** tab on the main page.

As administrator, use the **Database Firewalls** tab in the Audit Vault Server console to configure the network, services, and system settings for Database Firewall. You can also use the console to identify the Audit Vault Server that manages each firewall instance, to configure network traffic sources, monitor, and block threats to your target databases.

> **See Also:**
>
> Configuring Database Firewall for detailed information on configuring the Database Firewall using the Audit Vault Server console.

2.9.3 Understanding the Tabs and Menus in Audit Vault Server Console

Audit Vault Server Console tabs and menus enable you to see statuses for Agents, audit trails, targets, and more.

Oracle Audit Vault Server Console includes the following six tabs:

- **Home** - Displays a dashboard showing high-level information and status for:

  - System Alerts
  - Targets
  - Audit Collection
  - Database Firewall Monitoring
  - Collection summary
  - Jobs summary
  - Data Retention summary
  - System overview
- **Targets** - Provides menus for registering targets, managing target groups, managing access rights, and monitoring audit trails.
- **Agents** - Provides menus for registering, deploying, activating, and managing Audit Vault Agents.
- **Database Firewalls** - Provides menus for registering Database Firewalls in Audit Vault Server, for creating resilient firewall pairs for high availability, managing, and monitoring.
- **Data Retention** - Provides menus for viewing details of online and archived data, viewing and creating archiving policies, assigning archive policies to targets, and viewing and creating remote archiving locations.
- **Settings** - Provides menus for managing security, storage, archiving, users, certificates, password, and system settings. From here, you can also download the AVCLI command line utility.

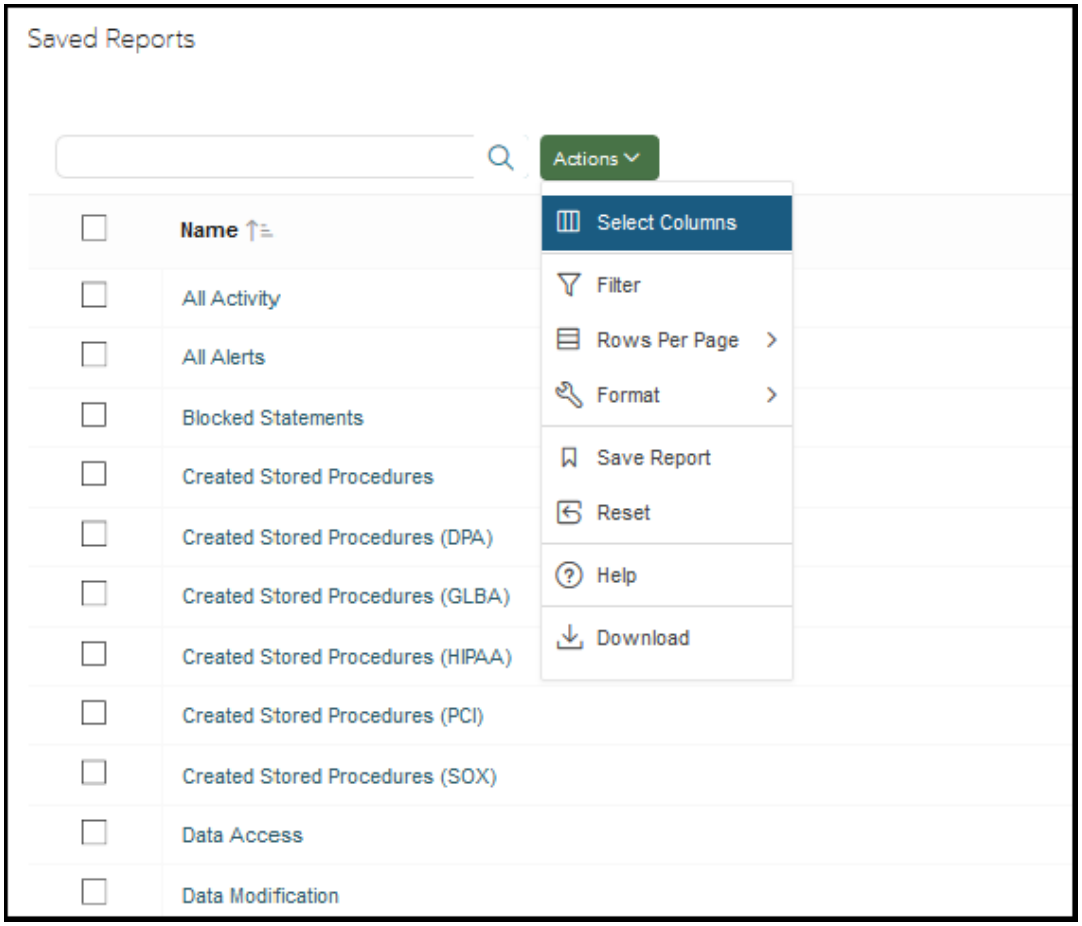
2.9.4 Working with Lists of Objects in the Audit Vault Server Console

Learn how to work with lists of objects in the Audit Vault Server console.

In the Audit Vault Server console, you can view lists of objects such as users, monitoring points, and so on. You can also filter and customize the lists of objects using the **Actions** menu and other filters. 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 console:

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 the name in the search box.
3. To customize the list, from the **Actions** menu, select any of the following:
   - **Select Columns:** Select the columns to display.
   - **Filter:** Filter the list by column or by row using regular expressions with the available operators. Rows provide more control and 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**

     Enter the criteria for each option as needed and click **Apply**.
   - **Save Report:** Save the current view of the list. Enter a name, 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) to download.

2.10 Using the Audit Vault Command Line Interface

Learn about using the Audit Vault Command Line Interface (AVCLI).

You can download AVCLI and use it as an alternative to Audit Vault Server Console for:

- configuring and managing Oracle Audit Vault and Database Firewall
- creating Database Firewall monitoring points
- managing audit trails
- registering hosts and performing other Agent related tasks
- configuring both database and non database targets for Audit Vault Server
- managing archive locations

> **See Also:**
>
> - Downloading and Using the AVCLI Command Line Interface for information on downloading and using AVCLI
> - AVCLI Commands Reference for details of available commands and syntax

2.11 Using the Oracle Audit Vault and Oracle Database Firewall Enterprise Manager Plug-In

Learn about using the Oracle Audit Vault and Database Firewall Enterprise Manager plug-in.

With Oracle Enterprise Manager Cloud Control you can install the Oracle Audit Vault and Database Firewall plug-in. Use this plug-in to manage and monitor Oracle Audit Vault and Database Firewall through Oracle Enterprise Manager.

You can perform the following tasks:

- View Audit Vault and Database Firewall topologies
- Monitor the availability and performance of Oracle Audit Vault components
- Provision Oracle Audit Vault Agent on targets
- Initialize and integrate Oracle Audit Vault and Database Firewall with targets including Oracle Database, hosts, and audit trails for hosts as well as Oracle Database.
- Perform discovery of sensitive columns on targets
- Monitor targets

Using Oracle Enterprise Manager Audit Vault and Database Firewall plug-in, the following components can be managed to perform certain operations:

Components	Operations Performed
Database Firewall	• Restart • Delete • Power Off
Audit Vault Agent	• Activate • Deactivate • Delete • Start • Stop
Monitoring Point	• Start • Stop • Delete
Audit Trail	• Start • Stop • Delete
Target	• Delete

Related Topics

- Managing Oracle AVDF in Cloud Control
- Manually Installing the Enterprise Manager Management Agent
- Compatibility with Oracle Enterprise Manager
- Issue with Configuring or Managing Oracle AVDF through Oracle Enterprise Manager Cloud Control
  Learn how to solve an issue with configuring or managing Oracle AVDF through Oracle Enterprise Manager Cloud Control.

> **See Also:**
>
> Refer to MOS note (*Doc ID 2855345.1*) for more information to manually deploy Oracle Enterprise Manager 13.x Agent on Audit Vault Server using the pull method.

2.12 Logging In to Oracle AVDF Appliances Through SSH

When installing or administering Oracle Audit Vault and Database Firewall (Oracle AVDF), you sometimes need to log in to the Audit Vault Server or Database Firewall appliance through SSH.

1. Log in to the appliance through SSH as the `support` user.

   The `support` user is set up during the post-installation process. See Post-Install Configuration Tasks.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

```
ssh support@<appliance_ip_address>
```

2. Switch to the `root` user.

```
su - root
```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

> **Caution:**
>
> Logging in as `root` during install or upgrade uses tmux, a terminal multiplexer, to display persistent information. A user with access to these screens can create new root shells. If you plan to leave the session unattended, Oracle recommends disconnecting from the blue screen by using the `CTRL-b d` command. To reconnect, log in as `root` once more.

Related Topics

- Connecting to Oracle AVDF Instance
  Learn how to access Audit Vault Server and Database Firewall instances on Oracle Cloud Infrastructure (OCI).
- Unable to Connect to Audit Vault Server through Console or SSH
  Learn how to resolve if you are unable to log in to Audit Vault Server through the console or SSH.

3
General Security Guidelines

Learn about general security guidelines for Oracle Audit Vault and Database Firewall.

3.1 Installing Oracle Audit Vault and Database Firewall Securely to Protect Your Data

Learn how to securely install Oracle AVDF to protect your data.

3.1.1 Installing Oracle Audit Vault and Database Firewall Securely

Learn to securely install Oracle Audit Vault and Database Firewall.

Oracle Audit Vault Server installs in a secure state by default. Therefore, it is important to be careful if you change any of the default settings because your changes may compromise the security of your setup.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Installation Guide* for details of the installation.

3.1.2 Protecting Your Data

Consider account naming, password use, and other guidelines to better enable Oracle AVDF to protect your data.

Consider following these guidelines to protect your data:

- Account Names and Passwords: Use secure passwords for the Oracle Audit Vault Server console UI, as well as for the `root`, `support`, and `sys` accounts and keep these passwords safe.
- Administrator Accounts: Do not share Oracle Audit Vault and Database Firewall Administrator accounts.
- Strong Password Policies: Encourage users to adopt strong passwords.
- Installed Accounts: Oracle Audit Vault and Database Firewall embeds operating system and database accounts. Do not add new accounts of this type. Do not unlock the existing accounts. Doing so may compromise the security of the Oracle Audit Vault and Database Firewall system.
- Secure Archiving: Oracle Audit Vault and Database Firewall sends archive data over the network. Secure both the archive destination and intermediate network infrastructure.
- Remote Access: The **Settings** tab of the services page of Oracle Audit Vault Server console controls access to:

- web console
- shell (ssh)
- 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 by the documentation or by Oracle support.

3.2 General Security Recommendations

Follow these general security recommendations for Oracle Audit Vault Server and Database Firewall (Oracle AVDF).

- If you are using the Database Firewall to block unwanted traffic, then ensure that all data flowing from the database clients to the database and back passes through the Oracle Database Firewall. This includes both requests and responses.
- Use the appropriate security measures for your site to control access to the computer that contains Oracle AVDF. Give access only to specific and trusted users, because someone with physical or virtual access to the console during installation can compromise the security of the installed system.
- Ensure that passwords conform to best practice.
- Separate the duties of administrators and auditors by assigning these roles to different people.
- Assign the Audit Vault Server user the appropriate administrator, super administrator, auditor, and super auditor roles.
- By default, the following accounts that are related to Oracle AVDF are locked: the Oracle OS user account, Oracle Grid accounts, any Oracle Database Vault accounts (for example, users who have been granted the `DV_OWNER` and `DV_ACCTMGR` roles). Ensure that these accounts remain locked.
- Avoid sharing passwords between users and login sessions. Add new operating system users to distinguish access by different people.
- When configuring system log forwarding, use suitable encryption to avoid giving actors with network access (such as network administrators) access to potentially sensitive data. See Configuring Remote Syslog Over TLS.
- Database accounts `AGENTUSR#` and `AVSRCUSR#` belong to the `AVS_NONINTERACTIVE` profile prior to Oracle AVDF 20.9 and the `AVS_AGENT_NONINTERACTIVE` profile starting with Oracle AVDF 20.9. These accounts are created whenever a new agent or target is added. The passwords for these accounts are generated internally and starting in Oracle AVDF 20.9, the passwords are also rotated periodically. Oracle recommends that you do not modify the `AGENTUSR#` and `AVSRCUSR#` accounts including modifying password lifetime, failed login attempts, or the password. For more information, see Updating the Passwords of the AGENTUSR# and AVSRCUSR# Accounts.
- Database account `AVREPORTUSER` belongs to the `AVS_NONINTERACTIVE` profile. Oracle recommends that you do not modify the `AVREPORTUSER` account including modifying password lifetime or failed login attempts.

3.3 External Network Dependencies

Ensure the security of your Oracle AVDF configuration by considering important external network dependencies.

When you add an external network service to Audit Vault Server or Database Firewall, you include these services to the trust model of your deployment.

For example, when you add a DNS server to an appliance, you trust the DNS server to provide the correct information about the host names that you look up. If someone compromises the DNS server, then they can control the network endpoints that are accessed by Audit Vault Server or Database Firewall using the host name.

There are analogous trust relationships in other services too, for example, NFS or NTP.

For this reason, add network services to Audit Vault Server or Database Firewall only when the following are adequately secure:

- the service
- the host server
- the intermediate network

3.4 Considerations for Deploying Network-Based Solutions

Learn about what to consider when deploying network-based solutions.

3.4.1 Monitoring Encrypted Traffic with the Database Firewall

The Database Firewall supports monitoring Native Network Encrypted (NNE) traffic if it is configured between a database client and an Oracle Database.

Starting with Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.7, the Database Firewall supports monitoring TLS-encrypted SQL traffic between a database client and an Oracle Database when the Database Firewall is deployed in proxy mode. The Database Firewall acts a TLS proxy terminating the session from the database client and creating a new TLS outbound session to the database server.

Starting with Oracle AVDF release 20.8, the Database Firewall supports monitoring TLS-encrypted SQL traffic between the database client and Oracle Real Application Clusters (Oracle RAC).

To monitor TLS traffic for non-Oracle databases, you can use TLS termination solutions to terminate TLS traffic just before it reaches the Database Firewall.

3.4.2 Managing Database Firewall Server Side SQL and Context Configurations

Learn how to manage Database Firewall SQL and context configurations.

Database Firewall policy enforcement relies on capturing and understanding SQL traffic between the database client and server. Because Database Firewall only analyzes network traffic between the application tier and the database server, the firewall cannot examine SQL that is directly sent from the database server. Some of the types of SQL statements that Database Firewall cannot examine are system provided and user defined SQL that you run

from stored procedures and callouts. The firewall also cannot examine SQL that you run from background jobs, such as those that created by the `DBMS_JOB` or `DBMS_SCHEDULER` PL/SQL packages in Oracle databases, or SQL that is indirectly run from DDLs or other SQL statements. You can use the Oracle AVDF auditing features to capture these types of SQL statements.

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. Any lack of context affects the resolution of identifiers that you use in database objects.

3.4.3 How Oracle AVDF Works with Various Database Access Paths

Learn how Oracle AVDF works with database access paths.

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 in the database. The Database Firewall provides policy enforcement only for SQL based access to the database. The protocols that 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.
- Non TCP based Connections: Database Firewall only supports TCP based network connections to database servers. It cannot monitor connections that are made to database servers using non TCP protocols such as Systems Network Architecture (SNA), Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

3.4.4 Database Firewall Configuration for Oracle Database Target Configured in Shared Server Mode

Learn about managing Database Firewall shared server configuration.

Shared server architectures enable databases to permit user processes to share server processes. A 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
> - *Oracle Database Reference* for more information about the `DISPATCHERS` parameter

3.4.5 Additional Client and Listener Behavior Considerations

Learn about additional issues to be aware of with clients and shared listeners.

- Client-side context: You can configure Oracle Database Firewall policies to use client-side context information such as client program name, client operating system username, and so on. After the client transmits this information to the database, Oracle Database Firewall captures it from the network. Oracle Database Firewall does not control or enforce the integrity of the client side or network. Consider the integrity of this information before using it to define security policies.
- Multiple databases and services on a shared listener: Oracle Database Firewall supports policies based on Oracle Database service names. For non-Oracle databases, Oracle 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, Oracle Database Firewall cannot differentiate traffic that is directed to each individual database.

3.5 Security Considerations for Custom Collector Development

Learn about security considerations for Custom Collector Development.

3.5.1 Custom Collector Development

Learn about custom collector development.

Note the following if you develop custom collectors:

- Prevent resource leaks. Ensure that JDBC resources are closed appropriately. These resources include the connections, result sets, and statements.
- Prevent data loss. Ensure that your audit data is purged from the target system only after it has been successfully collected by the custom collector.
- Avoid frequent queries to the target system.
- Ensure that the custom collector does not consume a lot of system resources such as CPU and memory on the target host.
- Avoid logging audit data because the audit records contain sensitive information.
- Grant only the required privileges on the target system to users who have access to the Agent.
- Ensure that only necessary files are added to custom collector `.jar` file.
- Ensure that your custom collector code collects the audit data from your target system securely.

> **Note:**
>
> The collection framework ensures that audit data is transferred from the collector to Oracle Audit Vault Server securely.

3.6 About Setting Transport Layer Security Levels

Learn about setting Transport Layer Security (TLS) levels in Oracle AVDF.

This topic describes the different levels of connection encryption deployed on Oracle Audit Vault and Database Firewall appliances. Oracle AVDF uses TLS for inter component communication.

You can change the TLS levels and cipher suites for the following:

- Connection between Audit Vault Server and the Agent or Host Monitor Agent
- Connection between Host Monitor Agent and Database Firewall
- Connection between Audit Vault Server and Database Firewall
- Audit Vault Server console and the end user browsers

> **Note:**
>
> - Adhere to Host Monitor Agent Requirements.
> - If any Agent is using `Java 1.6`, then upgrade the `Java` version to `1.8`.

Connection Encryption Strength Used On Oracle AVDF Appliances

TLS Level	TLS Version	Description
Level-4 (Default on new installation)	`TLSv1.2`	This level is the strongest, restricting TLS to version 1.2 for inter communication between all the components in Oracle Audit Vault and Database Firewall. **Note:** It is recommended to use *Level-4* for all services unless the supported service explicitly requires a lower level of TLS.
Level-3	`TLSv1.2`	This level supports everything that *Level-4* does. For Oracle AVDF releases 20.1 to 20.3: • If any Audit Vault Agent has to be deployed on *IBM AIX*, then set the TLS level to *Level-3* or below (refer to row # 5 in the table below). • *Level-3* uses TLS 1.2 or TLS 1.1 for Audit Vault Agent to Audit Vault Server communication. It is the same for Host Monitor Agent to Database Firewall communication. Starting Oracle AVDF 20.4, *Level-3* uses TLS 1.2 for Audit Vault Agent to Audit Vault Server communication. It is the same for Host Monitor Agent to Database Firewall communication.

TLS Level	TLS Version	Description
Level-2	TLSv1.2 TLSv1.1	This level adds support for legacy and deprecated ciphers. **Note:** • While upgrading to Oracle AVDF releases 20.1 to 20.3, the upgrade process does not automatically set to *Level-4* to maintain connectivity while upgrading a multiple-appliance deployment. Upon completion of the upgrade, set to *Level-4* unless interoperability with legacy systems is required. • While upgrading to Oracle AVDF releases 20.4 (or later), the upgrade process does not automatically set to *Level-4* in all cases. After the upgrade process is complete (including Agents), it is strongly advisable to set to *Level-4*.
Level-1 (Custom)	TLSv1.2	This is a customizable cipher set that is configured with *Level-4* strength by default.

How To Change TLS Levels and Other Tasks

Row No.	Task	Command	Detailed Information
1	To check the existing TLS levels for Audit Vault Server and Database Firewall.	`grep CIPHER_LEVEL /usr/local/dbfw/etc/dbfw.conf`	Log in as *support* user and run this command. Use this command to check the actual configuration of the Audit Vault Server and Database Firewall.
2	To set the TLS level and to find more options.	`/usr/local/dbfw/bin/priv/configure-networking --help`	Log in as *root* user and run this command. By default, on a new installation the TLS level is set to *Level-4*. On upgrade it is set to *Level-2* by default. This is appropriate to most of the situations. It is possible to change the level set. Use this command to find the options available.
3	To set TLS level for the Audit Vault Sever console.	`/usr/local/dbfw/bin/priv/configure-networking --wui-tls-cipher-level [LEVEL]`	Log in as *root* user and run this command. This command sets the TLS level for web browser connections to the AVS GUI. The levels can be set to `1, 2, 3, or 4`.
4	To set TLS level for communication between Audit Vault Server and Database Firewall.	`/usr/local/dbfw/bin/priv/configure-networking --internal-tls-cipher-level [LEVEL]`	Log in as *root* user and run this command. This command sets the desired TLS level and restarts the internal services. The levels can be set to `1, 2, 3, or 4`.

Row No.	Task	Command	Detailed Information

5	To set the TLS level for Audit Vault Agent to Audit Vault Server, and Host Monitor Agent to Database Firewall communication.	`/usr/local/dbfw/bin/priv/configure-networking --agent-tls-cipher-level [LEVEL]`	Log in as *root* user and run this command. This command sets the TLS level for communication between the Audit Vault Agent to Audit Vault Server, and Host Monitor Agent to Database Firewall. The levels can be set to `1, 2, 3, or 4`.
			Note:
			Perform the following steps to upgrade all Agents to the specified TLS levels after executing the `configure-networking` command:
			1. Log in to the Audit Vault Server console as *root* user.
			2. Change the directory by using the command:
			`cd /usr/local/dbfw/bin/priv`
			3. Execute the script using the command:
			`./send_agent_update_signal.sh`
			This command must not be executed more than once in a period of one hour.

Row No.	Task	Command	Detailed Information

6	To apply customized cipher set.	For Audit Vault Server console:
		• Edit: `/usr/local/dbfw/etc/platform-configuration/tls_configuration_custom_group.xml`
		Run:
		`/usr/local/dbfw/bin/priv/configure-networking --wui-tls-cipher-level 1`
		For Audit Vault Agent or Host Monitor Agent:
		• Edit: `/usr/local/dbfw/etc/platform-configuration/tls_configuration_custom_group_agent.xml`
		• Run:
		`/usr/local/dbfw/bin/priv/configure-networking --agent-tls-cipher-level 1`
		For inter appliance communication:
		• Edit: `/usr/local/dbfw/etc/platform-configuration/tls_configuration_custom_group_services.xml`
		• Run:
		`/usr/local/dbfw/bin/priv/configure-networking --internal-tls-cipher-level 1`
			By default, on a new installation the product is set to *Level-4*. On upgrade it is set to *Level-2*. This is appropriate to most of the situations. It is possible to customize. There are prompts and warning messages during the upgrade process which indicate that the cipher levels are not set to maximum security. The cipher levels are not automatically changed during upgrade.
			Use this command to apply the custom defined level from the file created. These commands set the TLS level for web browser connections and restart the internal services and Audit Vault Server.
			Note:
			After running the command to apply customized cipher set, verify the error output in the system log file available at `/var/log/messages` to confirm that there are no errors in the file.
			Log in as *root* user to run the command to edit the custom level configuration file. The customizable set of cipher suites is defined in this file. By default, on a new installation the product is set to *Level-4*. This file can be modified to further restrict the cipher suite and include ciphers available on the product.

7	To display the complete list of available cipher suites.	`openssl ciphers -v`	Log in as *support* user to run this command. Use this command to display the current set of available cipher suites.
8	To change TLS levels for inbound connection from the database client to the Database Firewall monitoring point.	See Modifying a Database Firewall Monitoring Point for complete information.	Starting with Oracle AVDF release 20.7, Database Firewall supports TLS encrypted SQL traffic. The TLS levels can be changed in the *Advanced* settings of the Database Firewall monitoring point using the Audit Vault Server console.

Row No.	Task	Command	Detailed Information
9	To change TLS levels for outbound connection from Database Firewall monitoring point to Oracle Database.	See Modifying a Database Firewall Monitoring Point for complete information.	Starting with Oracle AVDF release 20.7, Database Firewall supports TLS encrypted SQL traffic. The TLS levels can be changed in the *Advanced* settings of the Database Firewall monitoring point using the Audit Vault Server console.

When To Change TLS Levels

Oracle recommends leaving the internal TLS level at *Level-4*. Here is some more information on when to change the TLS levels:

Component	Situation
Internal communication	Oracle recommends to set at *Level–4* for increased security.
Audit Vault Server console (GUI)	To support old browsers, set the TLS level to match the browser.
Audit Vault Agent / Host Monitor Agent / Audit Vault Server	Oracle recommends to set at *Level–4* for increased security.
Audit Vault Agent deployed with *IBM AIX*	On a fresh installation of Oracle AVDF releases 20.1 to 20.3, it is set to *Level–4*. Change the TLS level to *Level-3* if any of the Audit Vault Agents are deployed on *IBM AIX*. On a fresh installation of Oracle AVDF 20.4 and later, it is set to *Level–4* and there is no change required.

Setting Custom Cipher Sets

Log in as *root* user to run this procedure for setting the custom cipher set. Do this by creating a custom file that defines the TLS levels and later applying the file.

1. The customizable set of TLS levels are defined in the following files:
   - `/usr/local/dbfw/etc/platform-configuration/tls_configuration_custom_group.xml`
   - `/usr/local/dbfw/etc/platform-configuration/tls_configuration_custom_group_agent.xml`
   - `/usr/local/dbfw/etc/platform-configuration/tls_configuration_custom_group_ssl_services.xml`
2. The `tls_configuration_custom_group.xml` file can be modified as desired to include available ciphers on the product.
3. Execute the following command to display the complete list of available ciphers:

```
openssl ciphers -v
```

4. Open the `tls_configuration_custom_group.xml` file and verify the format of the file. The format must be similar to the following:

```
<?xml version="1.0" encoding='UTF-8' standalone='yes'?>

<tls_configuration_groups xmlns='http://www.oracle.com/avdf'>

<tls_configuration level="1">

<ssl_protocols>

<ssl_protocol>...</ssl_protocol>

</ssl_protocols>

<ssl_cipher_suite>

<ssl_cipher>...</ssl_cipher>

</ssl_cipher_suite>

</tls_configuration>

</tls_configuration_groups>
```

5. In the customizable `tls_configuration_custom_group.xml` file, only the following tags can be added or removed as required:

```
<ssl_protocol>...</ssl_protocol>
```

6. Multiple tags can be applied in a sequence as follows:

```
<ssl_cipher>...</ssl_cipher>
```

7. The values must be any of the following Apache protocol values:

   a. `TLSv1.2`

   b. `TLSv1.1`

   c. `TLSv1 (Deprecated)`

8. Execute the following command to apply the custom set.

```
/usr/local/dbfw/bin/priv/configure-networking --wui-tls-cipher-level 1 --
internal-tls-cipher-level 1 --agent-tls-cipher-level 1
```

> **See Also:**
>
> Monitoring TLS Encrypted SQL Traffic

3.7 Certificates

Learn about different certificates in Oracle AVDF.

3.7.1 Platform Certificates

Learn all about Oracle AVDF platform certificates.

Oracle AVDF uses platform certificates for internal communication by various services.

Oracle AVDF release 20.6.0.0.0 and later provides the ability to renew platform certificates for Audit Vault Server and Database Firewall appliances before they expire. If the expiry period is less than 90 days, a warning message (`ODF 10729`) is displayed in the `/var/log/messages` file. See the action column against `ODF 10729` in the section Database Firewall Messages for detailed procedure for renewing the certificates manually.

If the certificates are not renewed manually and if they are about to expire in less than 30 days, then the platform certificates are automatically renewed and all the relevant services are restarted.

3.7.2 Rotating Audit Vault Agent Certificates

Learn how to rotate Audit Vault Agent certificates.

Audit Vault Agent uses certificates for internal communication with various components and services. These certificates are valid for a specific duration according to the following table:

Table 3-1 Audit Vault Agent Certificate Validity

Audit Vault Server Release	Audit Vault Agent Certificate Validity
Oracle AVDF 12.2	10 years
Oracle AVDF 20.1 and later	27 months

Follow these steps to rotate the Audit Vault Agent certificates.

> **Tip:**
>
> Starting with Oracle AVDF 20.9, if you have received a system alert that the certificate of your Audit Vault Agent is about to expire, you can skip to Step 4: Rotate the Audit Vault Agent Certificates.

3.7.2.1 About Audit Vault Agent Certificates

Learn about Audit Vault Agent certificates.

Audit Vault Agent certificates are used for communication between the Agent and Audit Vault Server. These Audit Vault Agent certificates have to be rotated or renewed for uninterrupted Oracle AVDF services.

Starting with Oracle AVDF release 20.7, the certificates can be renewed manually. For Oracle AVDF release 20.6 and prior, a patch needs to be applied before renewing the certificates.

After the Audit Vault Agent certificates are rotated or renewed, they are valid for a period of 27 months across all releases.

> **Note:**
>
> The certificate rotation or renewal is applicable to Audit Vault Agent and Host Monitor Agent.

3.7.2.2 Step 1: Download the Patch for Validating Audit Vault Agent Certificates (Oracle AVDF 20.1 to 20.9)

Download this patch to check the validity of the Audit Vault Agent certificates to determine when they will expire.

Applying patch 34412167 may restart the Audit Vault Agent. Before certificate rotation you should disable the autostart feature of Audit Vault Agent. See Autostarting the Agent on Windows Host for more information.

1. Log in to My Oracle Support.
2. Search for patch number *34412167*.
3. Download
   - For Oracle AVDF 20.1-20.7: `p34412167_201000_Linux-x86-64.zip`
   - For Oracle AVDF 20.8-20.9: `p34412167_208000_Linux-x86-64.zip`
4. Extract the contents of the zip file.
5. Copy `show-agent-certificate.py` from the extracted location to the `/tmp` directory on the Audit Vault Server.

3.7.2.3 Step 2: Check the Validity of the Audit Vault Agent Certificates (Oracle AVDF 20.1 to 20.9)

Check the validity of the Audit Vault Agent certificates to determine when they will expire.

1. Connect to the Audit Vault Server through SSH as the *root* user.
2. Switch to the *oracle* user:

   ```
   su - oracle
   ```

3. Copy `/tmp/show-agent-certificate.py` to the `$ORACLE_HOME/bin` directory.

4. Run the following command to check the validity of the Audit Vault Agent certificates:

   ```
   ./show-agent-certificate.py
   ```

5. Note the expiration date.

3.7.2.4 Step 3: Patch the Audit Vault Agents to Enable Certificate Rotation (Oracle AVDF 20.1 to 20.6 Only)

If the results of Step 2 indicate that the agent certificates are already expired or will expire within the next three months, then you need to rotate the agent certificates. For Oracle AVDF release 20.1 to 20.6, you first need to patch the Audit Vault Agents to enable certificate rotation.

> **Note:**
>
> In a high availability environment, apply the patch on both the primary and standby Audit Vault Servers.

1. Request a bundle patch for enhancement request (ER) 33869404.
2. Follow the instructions in the README that comes with the patch to apply the patch on the Audit Vault Agents through the Audit Vault Server.

> **Note:**
>
> Apply this patch before rotating the Audit Vault Server certificate. See Rotating Audit Vault Server Certificates.

3. Check the state of the Audit Vault Agents after the patching is complete.
   - If the certificates were already expired, then the agents will be in the `STOPPED` state.
   - If the certificates were not already expired, then the agents should be in the `RUNNING` state. If the agents are in the `STOPPED` state, then contact Oracle Support.

3.7.2.5 Step 4: Rotate the Audit Vault Agent Certificates

If the results of Step 2 indicate that the agent certificates are already expired or will expire within the next 30 days, then you need to rotate the agent certificates.

- Oracle AVDF 20.11 and later
- Oracle AVDF 20.10
- Oracle AVDF 20.1-20.9

Oracle AVDF 20.11 and later

If certificates have expired, you will have to manually rotate certificates through the steps for Oracle AVDF 20.10.

Ensure that all components of your AVDF system, Audit Vault Server(s), Audit Vault Agent(s), and Database Firewall(s), are up prior to performing certificate rotation. If certificates are rotated while a component is down, the component may not work the next time it is brought back up.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Settings** tab.
3. In the **Security** section, click the **Certificates** tab.
4. Click the **Rotate Certificates** tab.
5. Click either **Rotate CA Certificates** to rotate all certificate authorities (CA) and service certificates or **Rotate Service Certificates** to only rotate the service certificates on the following:
   - The primary Audit Vault Server, including the UI certificate if it is not externally signed. The SSO certificate will not be rotated as this must be done manually. See Rotating the Audit Vault Server SSO Certificate for more information.
   - The secondary Audit Vault Server, if set up in a high availability environment
   - Any registered Audit Vault Agents
   - Any registered Database Firewalls

   > **Note:**
   >
   > If the certificate authority is rotated, it will invalidate the certificates that have been signed by the Database Firewall certificate authority. Therefore, TLS proxy certificates should be signed externally by an appropriate certificate authority. See Creating TLS Proxy Certificates for Database Firewall for more information.
6. Click **OK** to confirm certificate rotation.
   While the certificates are being rotated the UI may be unavailable for some time.

Oracle AVDF 20.10

> **Note:**
>
> In a high availability environment, follow these steps for the primary Audit Vault Server only.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Change the directory:

   ```
   cd /opt/avdf/lib/ruby/avdf
   ```

3. Run the following command to rotate the Audit Vault Agent certificates:

```
ruby update_agent_cert_task.rb
```

4. If the certificate was already expired and you're using agentless collection,
   a. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.
   b. Run the below command to redeploy Agentless Collection Service

```
/usr/local/dbfw/bin/deploy_default_agent.py
```

Oracle AVDF 20.1-20.9

> **Note:**
>
> In a high availability environment, follow these steps for the primary Audit Vault Server only.

1. Connect to the Audit Vault Server through SSH as the *root* user.
2. Change the directory:

```
cd /opt/avdf/lib/ruby/avdf
```

3. Run the following command to rotate the Audit Vault Agent certificates:

```
ruby update_agent_cert_task.rb
```

4. If the certificates were already expired:
   a. Log in to the Audit Vault Server Console as an `administrator`.
   b. Click the **Agents** tab.
   c. Select the check box for all stopped agents, and then click **Deactivate**.
   d. Select the check box of all agent that were deactivated, and then click **Activate**.
   e. Copy or make a note of the agent activation key for all agents.
   f. Click **Downloads** in the left navigation menu.
   g. Download the `agent.jar`
   h. Transfer the `agent.jar` file to all the agent machines.
   i. Start all the Audit Vault Agents by running the bellow commands:
      i. `agentctl start -k`
      ii. Paste or enter the agent activation key in the following format:
      `<Agent Name>::XXXX-XXXX-XXXX-XXXX-XXXX`

      The activation key is not displayed as you type it.

If you're using agentless collection in Oracle AVDF 20.9, perform these steps if the certificate was already expired

a. Log in to the destination Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

b. Run the below command to redeploy Agentless Collection Service

```
/usr/local/dbfw/bin/deploy_default_agent.py
```

5. If the certificates were not already expired:

   a. Validate the Audit Vault Agent certificate after the rotation. See Step 2: Check the Validity of the Audit Vault Agent Certificates (Oracle AVDF 20.1 to 20.9).
   The Audit Vault Agent takes at most 12 hours to update the new certificates. The time depends on the number of agents that are registered on the Audit Vault Server.

   b. After 12 hours, verify that the Audit Vault Agents are in the *RUNNING* state. If they are in the *STOPPED* state, then contact Oracle Support.

6. If you disabled the autostart feature of Audit Vault Agent prior to applying patch 34412167, re-enable it. See Autostarting the Agent on Windows Host for more information.

3.7.3 Rotating Audit Vault Server Certificates

Learn how to rotate Audit Vault Server certificates.

Audit Vault Server uses certificates for internal communication with various components and services. Oracle AVDF enables you to rotate Audit Vault Server certificates before they expire.

- Oracle AVDF 20.11 and later
- Oracle AVDF 20.9 and 20.10 Standalone
- Oracle AVDF 20.9 and 20.10 High Availability
- Oracle AVDF 20.1 - 20.8 Standalone
- Oracle AVDF 20.1 - 20.8 High Availability

Oracle AVDF 20.11 and later

If certificates have expired, you will have to manually rotate certificates through the steps for Oracle AVDF 20.10.

Ensure that all components of your AVDF system, Audit Vault Server(s), Audit Vault Agent(s), and Database Firewall(s), are up prior to performing certificate rotation. If certificates are rotated while a component is down, the component may not work the next time it is brought back up.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Settings** tab.
3. In the **Security** section, click the **Certificates** tab.

4. Click the **Rotate Certificates** tab.
5. Click either **Rotate CA Certificates** to rotate all certificate authorities (CA) and service certificates or **Rotate Service Certificates** to only rotate the service certificates on the following:
   - The primary Audit Vault Server, including the UI certificate if it is not externally signed. The SSO certificate will not be rotated as this must be done manually. See Rotating the Audit Vault Server SSO Certificate for more information.
   - The secondary Audit Vault Server, if set up in a high availability environment
   - Any registered Audit Vault Agents
   - Any registered Database Firewalls

   > **Note:**
   >
   > If the certificate authority is rotated, it will invalidate the certificates that have been signed by the Database Firewall certificate authority. Therefore, TLS proxy certificates should be signed externally by an appropriate certificate authority. See Creating TLS Proxy Certificates for Database Firewall for more information.

6. Click **OK** to confirm certificate rotation.
   While the certificates are being rotated the UI may be unavailable for some time.

Oracle AVDF 20.9 and 20.10 Standalone

1. Generate new certificate authority (CA) certificates on the Audit Vault Server by the following command as the `root` user. This process updates the central, self-signed CA certificate on the Audit Vault Server.

   ```
   /usr/local/bin/gensslcert destroy-certs create-ca
   ```

2. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

   ```
   systemctl reload httpd


   systemctl restart controller
   ```

3. Update and regenerate the CA certificate bundles and services.
   a. Run the following command as the `root` user on the primary Audit Vault Server appliance:

      ```
      cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/dbfw/etc/ca.crt
      > /etc/pki/tls/certs/dbfw-ca.crt
      ```

b. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart controller
```

4. Run the following command as the `root` user on the primary server:

```
systemctl start monitor
```

5. Copy and transfer the new CA certificates from the Audit Vault Server to each of the linked Database Firewall instances:
   Run as the `root` user on the primary server:

```
scp /usr/local/dbfw/etc/ca.crt support@<dbfw-ip>:/tmp/primary.ca
```

   Run as the `root` user on the Database Firewall:

```
cp /tmp/primary.ca /usr/local/dbfw/etc/controller.crt


cp /tmp/standby.ca /usr/local/dbfw/etc/controller_second.crt
```

6. Update the Database Firewall and Audit Vault Server controllers:
   Run as the `root` user on the Database Firewall:

```
cat /tmp/primary.ca | /opt/avdf/config-utils/bin/config-avs set
avs=primary address=<primary-ip> certificate=-


cat /tmp/standby.ca | /opt/avdf/config-utils/bin/config-avs set
avs=secondary address=<standby-ip> certificate=-
```

7. Restart the Database Firewall appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart stund
```

8. Verify that the local and peer certificates are valid.
   Verify the following local certificates:
   - `/usr/local/dbfw/etc/ca.crt`
   - `/etc/pki/tls/certs/localhost_internal.crt`
   - `/usr/local/dbfw/etc/cert.crt`
   - `/usr/local/dbfw/etc/avs/avs_apex_client.crt`
   - `/usr/local/dbfw/etc/avs/avswallet`
   - `/etc/pki/tls/certs/localhost.crt`

Verify the following peer certificates:

- `/usr/local/dbfw/etc/avs/fwcerts/fw-[ip].cert`
- `/usr/local/dbfw/etc/ha_partner.crt`
- `/var/lib/oracle/dbfw/av/conf/ava.cer`
- `/var/lib/oracle/dbfw/av/conf/avs.cer`

Use the `config-diagnostics`, `sappdiag`, or `openssl x509` command to verify the certificate validity:

```
/usr/local/dbfw/bin/sappdiag


openssl x509 -enddate -startdate -noout -in /usr/local/dbfw/etc/ca.crt
```

Oracle AVDF 20.9 and 20.10 High Availability

1. Generate new certificate authority (CA) certificates on the primary Audit Vault Server by the following command as the `root` user. This process updates the central, self-signed CA certificate on the Audit Vault Server.

   ```
   /usr/local/bin/gensslcert destroy-certs create-ca
   ```

2. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

   ```
   systemctl reload httpd


   systemctl restart controller
   ```

3. Transfer the CA certificates from the primary Audit Vault Server to the standby Audit Vault Server:

   Run as the `root` user on the primary server:

   ```
   scp /usr/local/dbfw/etc/ca.crt support@<standby-ip>:/tmp/ha_partner.crt
   ```

   Run as the `root` user on the standby server:

   ```
   cp /tmp/ha_partner.crt /usr/local/dbfw/etc/ha_partner.crt
   ```

4. Restart the standby Audit Vault Server appliance. As the `root` user run the following commands:

   ```
   systemctl reload httpd


   systemctl restart controller
   ```

5. Regenerate the CA certificates and all certificates on the standby Audit Vault Server instance.

Run as the `root` user on the standby server:

```
/usr/local/bin/gensslcert destroy-certs create-ca
```

6. Restart the standby Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart controller
```

7. Transfer the standby CA certificates to the primary instance:
   Run as the `root` user on the primary server:

```
cp /tmp/ha_partner.crt /usr/local/dbfw/etc/ha_partner.crt
```

   Run as the `root` user on the standby server:

```
scp /usr/local/dbfw/etc/ca.crt support@<primary-ip>:/tmp/ha_partner.crt
```

8. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart controller
```

9. Update and regenerate the CA certificate bundles and services. Perform these steps on the primary and standby Audit Vault Server instances one at a time.
   a. Run the following command as the `root` user on the primary Audit Vault Server appliance:

```
cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/dbfw/etc/ca.crt
> /etc/pki/tls/certs/dbfw-ca.crt
```

   b. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart controller
```

   c. Run the following command as the `root` user on the standby Audit Vault Server appliance:

```
cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/dbfw/etc/ca.crt
> /etc/pki/tls/certs/dbfw-ca.crt
```

d. Restart the standby Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart controller
```

10. Restart the observer on the primary Audit Vault Server server:
Run as the `root` user on the primary server:

```
systemctl stop monitor
```

Switch to the `oracle` user.

```
su - oracle
```

Run as the `oracle` user on the primary server:

```
/usr/local/dbfw/bin/observerctl --stop
```

```
/usr/local/dbfw/bin/observerctl --start
```

11. Wait for two minutes for the observer process to come up.
To check the observer status:

a. Log in to the Audit Vault Server through SSH as the `support` user.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

```
ssh support@<audit_vault_server_ip_address>
```

b. Switch to the `root` user.

```
su - root
```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

c. Switch to the `oracle` user.

```
su - oracle
```

d. Run the following command:

```
/usr/local/dbfw/bin/setup_ha.rb -status
```

This displays all statuses, including the Data Guard observer status. It displays `Data guard observer = yes` when the observer is running.

12. Run the following command as the `root` user on the primary server:

```
systemctl start monitor
```

13. Copy and transfer the new CA certificates from the primary and standby instances to each of the linked Database Firewall instances:
Run as the `root` user on the primary server:

```
scp /usr/local/dbfw/etc/ca.crt support@<dbfw-ip>:/tmp/primary.ca
```

Run as the `root` user on the standby server:

```
scp /usr/local/dbfw/etc/ca.crt support@<dbfw-ip>:/tmp/standby.ca
```

Run as the `root` user on the Database Firewall:

```
cp /tmp/primary.ca /usr/local/dbfw/etc/controller.crt


cp /tmp/standby.ca /usr/local/dbfw/etc/controller_second.crt
```

14. Update the Database Firewall and Audit Vault Server controllers:
Run as the `root` user on the Database Firewall:

```
cat /tmp/primary.ca | /opt/avdf/config-utils/bin/config-avs set
avs=primary address=<primary-ip> certificate=-


cat /tmp/standby.ca | /opt/avdf/config-utils/bin/config-avs set
avs=secondary address=<standby-ip> certificate=-
```

15. Restart the Database Firewall appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart stund
```

16. Verify that the local and peer certificates are valid.
Verify the following local certificates:

- `/usr/local/dbfw/etc/ca.crt`
- `/etc/pki/tls/certs/localhost_internal.crt`
- `/usr/local/dbfw/etc/cert.crt`

- /usr/local/dbfw/etc/avs/avs_apex_client.crt
- /usr/local/dbfw/etc/avs/avswallet
- /etc/pki/tls/certs/localhost.crt

Verify the following peer certificates:

- /usr/local/dbfw/etc/avs/fwcerts/fw-[ip].cert
- /usr/local/dbfw/etc/ha_partner.crt
- /var/lib/oracle/dbfw/av/conf/ava.cer
- /var/lib/oracle/dbfw/av/conf/avs.cer

Use the `config-diagnostics`, `sappdiag`, or `openssl x509` command to verify the certificate validity:

```
/usr/local/dbfw/bin/sappdiag
```

```
openssl x509 -enddate -startdate -noout -in /usr/local/dbfw/etc/ca.crt
```

Oracle AVDF 20.1 - 20.8 Standalone

1. Log in to My Oracle Support.
2. Search for patch number *34378212*.
3. Download `p34378212_191000_Linux-x86-64.zip`.
4. Extract the contents of the zip file.
5. Copy `gensslcert.avs.tar.gz` from the extracted location to the `/tmp` directory on the Audit Vault Server.
6. Complete the installation on the Audit Vault Server:
   a. Log in to the Audit Vault Server through SSH as the `support` user.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

```
ssh support@<audit_vault_server_ip_address>
```

   b. Switch to the `root` user.

```
su - root
```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

c. Create a new directory:

```
mkdir /root/gensslcert
```

d. Copy `gensslcert.avs.tar.gz` to the new directory:

```
cp /tmp/gensslcert.avs.tar.gz /root/gensslcert
```

e. Change to the new directory:

```
cd /root/gensslcert
```

f. Extract the files:

```
tar xvfz gensslcert.avs.tar.gz
```

7. Generate new certificate authority (CA) certificates on the Audit Vault Server by running the following command as the `root` user. This process updates the central, self-signed CA certificate on the Audit Vault Server.

```
/root/gensslcert/gensslcert destroy-certs create-ca
```

8. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart controller
```

9. Update and regenerate the CA certificate bundles and services.

a. Run the following command as the `root` user on the Audit Vault Server appliance:

```
cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/dbfw/etc/ca.crt
> /etc/pki/tls/certs/dbfw-ca.crt
```

b. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart controller
```

10. Run the following command as the `root` user on the primary server:

```
systemctl start monitor
```

11. Copy and transfer the new CA certificates from the Audit Vault Server to each of the linked Database Firewall instances:

Run as the `root` user on the primary server:

```
scp /usr/local/dbfw/etc/ca.crt support@<dbfw-ip>:/tmp/primary.ca
```

Run as the `root` user on the Database Firewall:

```
cp /tmp/primary.ca /usr/local/dbfw/etc/controller.crt
```

```
cp /tmp/standby.ca /usr/local/dbfw/etc/controller_second.crt
```

12. Update the Database Firewall and Audit Vault Server controllers:
    Run as the `root` user on the Database Firewall:

```
cat /tmp/primary.ca | /opt/avdf/config-utils/bin/config-avs set
avs=primary address=<primary-ip> certificate=-
```

```
cat /tmp/standby.ca | /opt/avdf/config-utils/bin/config-avs set
avs=secondary address=<standby-ip> certificate=-
```

13. Restart the Database Firewall appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart stund
```

14. Verify that the local and peer certificates are valid.
    Verify the following local certificates:
    - `/usr/local/dbfw/etc/ca.crt`
    - `/etc/pki/tls/certs/localhost_internal.crt`
    - `/usr/local/dbfw/etc/cert.crt`
    - `/usr/local/dbfw/etc/avs/avs_apex_client.crt`
    - `/usr/local/dbfw/etc/avs/avswallet`
    - `/etc/pki/tls/certs/localhost.crt`

    Verify the following peer certificates:
    - `/usr/local/dbfw/etc/avs/fwcerts/fw-[ip].cert`
    - `/usr/local/dbfw/etc/ha_partner.crt`
    - `/var/lib/oracle/dbfw/av/conf/ava.cer`
    - `/var/lib/oracle/dbfw/av/conf/avs.cer`

    Use the `config-diagnostics`, `sappdiag`, or `openssl x509` command to verify the certificate validity:

```
/usr/local/dbfw/bin/sappdiag
```

```
openssl x509 -enddate -startdate -noout -in /usr/local/dbfw/etc/ca.crt
```

Oracle AVDF 20.1 - 20.8 High Availability

1. Log in to My Oracle Support.

2. Search for patch number *34378212*.
3. Download `p34378212_191000_Linux-x86-64.zip`.
4. Extract the contents of the zip file.
5. Copy `gensslcert.avs.tar.gz` from the extracted location to the `/tmp` directory on the Audit Vault Server.
6. Complete the installation on the Audit Vault Server:
   a. Log in to the Audit Vault Server through SSH as the `support` user.

      > **Note:**
      >
      > If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

      ```
      ssh support@<audit_vault_server_ip_address>
      ```

   b. Switch to the `root` user.

      ```
      su - root
      ```

      > **Note:**
      >
      > If you're using the OCI marketplace image, use the `sudo su -` command.

   c. Create a new directory:

      ```
      mkdir /root/gensslcert
      ```

   d. Copy `gensslcert.avs.tar.gz` to the new directory:

      ```
      cp /tmp/gensslcert.avs.tar.gz /root/gensslcert
      ```

   e. Change to the new directory:

      ```
      cd /root/gensslcert
      ```

   f. Extract the files:

      ```
      tar xvfz gensslcert.avs.tar.gz
      ```

7. Generate new certificate authority (CA) certificates on the primary Audit Vault Server by running the following command as the `root` user. This process updates the central, self-signed CA certificate on the Audit Vault Server.

   ```
   /root/gensslcert/gensslcert destroy-certs create-ca
   ```

8. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart controller
```

9. Transfer the CA certificates from the primary Audit Vault Server to the standby Audit Vault Server:
   Run as the `root` user on the primary server:

```
scp /usr/local/dbfw/etc/ca.crt support@<standby-ip>:/tmp/ha_partner.crt
```

   Run as the `root` user on the standby server:

```
cp /tmp/ha_partner.crt /usr/local/dbfw/etc/ha_partner.crt
```

10. Restart the standby Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart controller
```

11. Regenerate the CA certificates and all certificates on the standby Audit Vault Server instance by running the following command as the `root` user.

```
/root/gensslcert/gensslcert destroy-certs create-ca
```

12. Restart the standby Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart controller
```

13. Transfer the standby CA certificates to the primary instance:
    Run as the `root` user on the primary server:

```
cp /tmp/ha_partner.crt /usr/local/dbfw/etc/ha_partner.crt
```

    Run as the `root` user on the standby server:

```
scp /usr/local/dbfw/etc/ca.crt support@<primary-ip>:/tmp/ha_partner.crt
```

14. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart controller
```

15. Update and regenerate the CA certificate bundles and services. Perform these steps on the primary and standby Audit Vault Server instances one at a time.
    a. Run the following command as the `root` user on the primary Audit Vault Server appliance:

```
cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/dbfw/etc/ca.crt
> /etc/pki/tls/certs/dbfw-ca.crt
```

    b. Restart the primary Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart controller
```

    c. Run the following command as the `root` user on the standby Audit Vault Server appliance:

```
cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/dbfw/etc/ca.crt
> /etc/pki/tls/certs/dbfw-ca.crt
```

    d. Restart the standby Audit Vault Server appliance. As the `root` user run the following commands:

```
systemctl reload httpd


systemctl restart controller
```

16. Restart the observer on the primary Audit Vault Server server:
    Run as the `root` user on the primary server:

```
systemctl stop monitor
```

    Switch to the `oracle` user.

```
su - oracle
```

Run as the `oracle` user on the primary server:

```
/usr/local/dbfw/bin/observerctl --stop


/usr/local/dbfw/bin/observerctl --start
```

17. Wait for two minutes for the observer process to come up.
    To check the observer status:
    a. Log in to the Audit Vault Server through SSH as the `support` user.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

```
ssh support@<audit_vault_server_ip_address>
```

    b. Switch to the `root` user.

```
su - root
```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

    c. Switch to the `oracle` user.

```
su - oracle
```

    d. Run the following command:

```
/usr/local/dbfw/bin/setup_ha.rb -status
```

    This displays all statuses, including the Data Guard observer status. It displays `Data guard observer = yes` when the observer is running.

18. Run the following command as the `root` user on the primary server:

```
systemctl start monitor
```

19. Copy and transfer the new CA certificates from the primary and standby instances to each of the linked Database Firewall instances:
    Run as the `root` user on the primary server:

```
scp /usr/local/dbfw/etc/ca.crt support@<dbfw-ip>:/tmp/primary.ca
```

Run as the `root` user on the standby server:

```
scp /usr/local/dbfw/etc/ca.crt support@<dbfw-ip>:/tmp/standby.ca
```

Run as the `root` user on the Database Firewall:

```
cp /tmp/primary.ca /usr/local/dbfw/etc/controller.crt
```

```
cp /tmp/standby.ca /usr/local/dbfw/etc/controller_second.crt
```

20. Update the Database Firewall and Audit Vault Server controllers:
    Run as the `root` user on the Database Firewall:

```
cat /tmp/primary.ca | /opt/avdf/config-utils/bin/config-avs set
avs=primary address=<primary-ip> certificate=-
```

```
cat /tmp/standby.ca | /opt/avdf/config-utils/bin/config-avs set
avs=secondary address=<standby-ip> certificate=-
```

21. Restart the Database Firewall appliance. As the `root` user run the following commands:

```
systemctl reload httpd
```

```
systemctl restart stund
```

22. Verify that the local and peer certificates are valid.
    Verify the following local certificates:
    - `/usr/local/dbfw/etc/ca.crt`
    - `/etc/pki/tls/certs/localhost_internal.crt`
    - `/usr/local/dbfw/etc/cert.crt`
    - `/usr/local/dbfw/etc/avs/avs_apex_client.crt`
    - `/usr/local/dbfw/etc/avs/avswallet`
    - `/etc/pki/tls/certs/localhost.crt`

    Verify the following peer certificates:
    - `/usr/local/dbfw/etc/avs/fwcerts/fw-[ip].cert`
    - `/usr/local/dbfw/etc/ha_partner.crt`
    - `/var/lib/oracle/dbfw/av/conf/ava.cer`
    - `/var/lib/oracle/dbfw/av/conf/avs.cer`

Use the `config-diagnostics`, `sappdiag`, or `openssl x509` command to verify the certificate validity:

```
/usr/local/dbfw/bin/sappdiag
```

```
openssl x509 -enddate -startdate -noout -in /usr/local/dbfw/etc/ca.crt
```

3.7.4 Rotating Database Firewall Certificates

Learn how to rotate Database Firewall certificates.

Database Firewall uses certificates for internal communication with various components and services. Oracle AVDF enables you to rotate Database Firewall certificates before they expire.

> **Note:**
>
> Rotate certificates for each Database Firewall instance including those paired for high availability.

- Oracle AVDF 20.11 and later
- Oracle AVDF 20.9 and 20.10
- Oracle AVDF 20.1 - 20.8

Oracle AVDF 20.11 and later

If certificates have expired, you will have to manually rotate certificates through the steps for Oracle AVDF 20.10.

Ensure that all components of your AVDF system, Audit Vault Server(s), Audit Vault Agent(s), and Database Firewall(s), are up prior to performing certificate rotation. If certificates are rotated while a component is down, the component may not work the next time it is brought back up.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Settings** tab.
3. In the **Security** section, click the **Certificates** tab.
4. Click the **Rotate Certificates** tab.
5. Click either **Rotate CA Certificates** to rotate all certificate authorities (CA) and service certificates or **Rotate Service Certificates** to only rotate the service certificates on the following:
   - The primary Audit Vault Server, including the UI certificate if it is not externally signed. The SSO certificate will not be rotated as this must be done manually. See Rotating the Audit Vault Server SSO Certificate for more information.
   - The secondary Audit Vault Server, if set up in a high availability environment

- Any registered Audit Vault Agents
- Any registered Database Firewalls

> **Note:**
>
> If the certificate authority is rotated, it will invalidate the certificates that have been signed by the Database Firewall certificate authority. Therefore, TLS proxy certificates should be signed externally by an appropriate certificate authority. See Creating TLS Proxy Certificates for Database Firewall for more information.

6. Click **OK** to confirm certificate rotation.
While the certificates are being rotated the UI may be unavailable for some time.

Oracle AVDF 20.9 and 20.10

1. Generate the new certificate authority (CA) certificates on the Database Firewall appliance. First regenerate the local CA certificates on the Database Firewall appliance by running one of the following commands.

```
dbfw(root)$ /usr/local/bin/gensslcert destroy-certs create-ca
```

2. Run the following commands to restart the Database Firewall services:

```
dbfw(root) $ systemctl reload httpd
```

```
dbfw(root) $ systemctl restart stund
```

3. Update the Database Firewall certificate on the Audit Vault Server and regain control of the Database Firewall. See Fetching an Updated Certificate from Database Firewall.
4. Verify that the following local certificates are valid:
   - `/usr/local/dbfw/etc/ca.crt`
   - `/etc/pki/tls/certs/localhost_internal.crt`
   - `/usr/local/dbfw/etc/cert.crt`

   Use the `config-diagnostics`, `sappdiag`, or `openssl x509` command to verify the certificate validity.

```
/usr/local/dbfw/bin/sappdiag
```

```
openssl x509 -enddate -startdate -noout -in /usr/local/dbfw/etc/ca.crt
```

5. Verify that the following peer certificates are valid:
   - `/usr/local/dbfw/etc/controller.crt`
   - `/usr/local/dbfw/etc/controller_second.crt`
   - `/usr/local/dbfw/etc/fw_ca.crt`

Oracle AVDF 20.1 - 20.8

1. Log in to My Oracle Support.
2. Search for patch number *34378217*.
3. Download `p34378217_191000_Linux-x86-64.zip`.
4. Extract the contents of the zip file.
5. Copy `gensslcert.dbfw.tar.gz` from the extracted location to the `/tmp` directory on the Database Firewall server.
6. Follow these steps to complete the installation on the Database Firewall Server:
   a. Connect to the Database Firewall appliance through SSH as the *support* user.
   b. Switch to the *root* user:

      ```
      su - root
      ```

   c. Create a new directory:

      ```
      mkdir /root/gensslcert
      ```

   d. Copy `gensslcert.dbfw.tar.gz` to the new directory:

      ```
      cp /tmp/gensslcert.dbfw.tar.gz /root/gensslcert
      ```

   e. Change to the new directory:

      ```
      cd /root/gensslcert
      ```

   f. Run the following command:

      ```
      tar xvfz gensslcert.dbfw.tar.gz
      ```

7. Generate the new certificate authority (CA) certificates on the Database Firewall appliance. First regenerate the local CA certificates on the Database Firewall appliance by running one of the following commands.

   ```
   dbfw(root)$ /root/gensslcert/gensslcert destroy-certs create-ca
   ```

8. Run the following commands to restart the Database Firewall services:

   ```
   dbfw(root) $ systemctl reload httpd


   dbfw(root) $ systemctl restart stund
   ```

9. Update the Database Firewall certificate on the Audit Vault Server and regain control of the Database Firewall. See Fetching an Updated Certificate from Database Firewall.
10. Verify that the following local certificates are valid:
    - `/usr/local/dbfw/etc/ca.crt`
    - `/etc/pki/tls/certs/localhost_internal.crt`
    - `/usr/local/dbfw/etc/cert.crt`

Use the `config-diagnostics`, `sappdiag`, or `openssl x509` command to verify the certificate validity.

```
/usr/local/dbfw/bin/sappdiag
```

```
openssl x509 -enddate -startdate -noout -in /usr/local/dbfw/etc/ca.crt
```

11. Verify that the following peer certificates are valid:
    - `/usr/local/dbfw/etc/controller.crt`
    - `/usr/local/dbfw/etc/controller_second.crt`
    - `/usr/local/dbfw/etc/fw_ca.crt`

3.7.5 Rotating the Audit Vault Server SSO Certificate

Starting in Oracle AVDF 20.11, you can configure single sign-on (SSO) for Audit Vault Server console users. Learn how to rotate the SSO key and certificate.

Rotation of the SSO certificate must be done manually as it does not rotate through the functionality available in the **Rotate Certificates** tab of the Audit Vault Server.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Go to the `/usr/local/dbfw/etc` directory:

   ```
   cd /usr/local/dbfw/etc
   ```
3. Create a backup directory and move the current Apex SAML key and certificate files there.

   ```
   mkdir apexsaml_backup
   mv apexsaml.key ./apexsaml_backup
   mv apexsaml.crt ./apexsaml_backup
   ```
4. Generate the Apex SAML key and certificate:

   ```
   /usr/local/dbfw/etc/privileged-migrations/gen_saml_apex_cert.sh
   ```
5. Register them with Audit Vault Server:

   ```
   /usr/local/dbfw/etc/privileged-migrations/register_apex_key_cert.py
   ```
6. Test the SSO configuration by logging in to the Audit Vault Server console.
   See Logging In to Oracle AVDF Appliances Through SSO for more information.
7. Remove the backup directory for Apex SAML key and certificate if the SSO connection testing is working fine:

   ```
   rm -r /usr/local/dbfw/etc/apexsmal_backup
   ```
8. If your identity provider requires the Audit Vault Server SSO certificate, update the identity provider configuration with the new SSO certificate.

9. If configured in high availability, copy the `/usr/local/dbfw/etc/apexsaml.key` and `/usr/local/dbfw/etc/apexsaml.crt` to the standby Audit Vault Server.

Related Topics

- Configuring Single Sign-On (SSO) for Audit Vault Server Console Users

3.7.6 Creating TLS Proxy Certificates for Database Firewall

Learn how to create and upload TLS proxy certificates for Database Firewall.

Oracle Audit Vault and Database Firewall (Oracle AVDF) release 20.8 (and later) supports managing TLS proxy certificates for Database Firewall from the Audit Vault Server console.

Database Firewall uses certificates for inbound (database client to Database Firewall) and outbound (Database Firewall to target database) TLS connections. You can create and manage certificates for both inbound and outbound TLS connections through the Audit Vault Server console.

> **Note:**
>
> - This functionality is available to Oracle Database versions that are supported by Oracle AVDF. It is not applicable to Oracle Real Application Clusters (Oracle RAC) instances in Oracle AVDF release 20.7. It is supported starting with Oracle AVDF release 20.8.
> - This functionality is applicable to Database Firewall instances that are deployed in **Monitoring / Blocking (Proxy)** mode only.
> - When using Database Firewall as a TLS proxy, password-based user authorization with the database is supported. Certificate-based authorization and third-party user authorization (RADIUS, Kerberos, LDAP, and so on) with the database are not supported.

The following types of certificate signing methods are supported:

- Certificates that are signed by the Database Firewall certificate authority (CA)

  You can use out-of-the-box certificates that are signed by the Database Firewall CA for inbound and outbound TLS connections. Oracle strongly recommends that you use third-party, externally signed certificates for production deployments.

  You can choose this option when configuring monitoring points for a target database.

- Certificates that are signed by an external CA

  To use a certificate that is signed by an external CA, create a certificate signing request (CSR) with the relevant information, download it, get the certificate signed, and upload it using the Audit Vault Server console.

  After you upload the certificate, you can use it when configuring monitoring points for a target database.

Follow these steps to generate a CSR, download the CSR, and upload the duly signed certificate to the Database Firewall:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.

3. Click the **Security** tab in the left navigation menu.

   Only super administrators can see the subtabs and settings on the main page of the **Security** tab.
4. Click the **Certificate** subtab on the main page.
5. Click the **Database Firewall** subtab.
6. Click the **Generate CSR** button.

   The **Generate Certificate Signing Request (CSR)** dialog box appears.
7. Select the specific **Database Firewall** instance from the drop-down list.
8. Enter a common name.
9. Enter the organization name for the certificate.
10. Select the country or region.
11. (Optional) Complete the following fields:
    - **Organizational Unit**
    - **State/Province**
    - **City**
    - **Email**
12. Click **Create** to submit the CSR.
13. Click **Download CSR** and save the certificate to the local machine.
14. Get the certificate duly signed by a CA.
15. After the CA approves the certificate, click **Upload Certificate**.

    The **Upload Certificate** dialog box appears.
16. Select the file from the local machine.
17. Click **Upload**.
18. Use the newly uploaded certificate when configuring monitoring points for a target database.

    See Modifying a Database Firewall Monitoring Point for complete instructions.

Viewing Certificate Details

In the Audit Vault Server console, you can view the details for each TLS proxy certificate, including the status, start and end dates, expiry time, common name, and so on.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. Click the **Security** tab in the left navigation menu.
4. Click the **Certificate** subtab on the main page.
5. Click the **Database Firewall** subtab.

Rotating Certificates

You can also rotate the TLS proxy certificates for Database Firewall.

For Database Firewall CA signed certificates, rotating creates new certificates and assigns them to the same monitoring points.

For externally signed CA certificates, rotating creates a new CSR using the previously configured values. You need to download the certificate and follow the same procedure that you followed to create it, get it signed, and upload it.

4
Configuring Audit Vault Server

Learn about configuring Audit Vault Server.

4.1 About Configuring Audit Vault Server

Learn about configuring Audit Vault Server.

This chapter explains how to perform the initial Audit Vault Server configuration.

> **Note:**
>
> Audit Vault Server and Database Firewall are software appliances. You must not make changes to the Linux operating system through the command line on these servers unless you are following procedures as described in the official Oracle documentation or you are working under the guidance of Oracle Support.

The main steps involved in the configuration process are as follows:

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) Configure the Audit Vault Agents.
3. (Optional) Define resilient pairs of servers for high availability.
4. (Optional) Add each Database Firewall at Audit Vault Server.
5. (Optional) Configure Oracle Audit Vault and Database Firewall to work with third party Security Information Event Management (SIEM) products that can read from Syslog.
6. (Optional) Configure Microsoft Active Directory or Open LDAP.
7. Check that the system is functioning correctly.

> **See Also:**
>
> - Configuring High Availability for Audit Vault Servers for more information about configuring a resilient pair of Audit Vault Servers for high availability. Perform the initial configuration that is described in this chapter for both Audit Vault Servers.
> - Summary of Configuration Steps to understand the high level workflow for configuring Oracle Audit Vault and Database Firewall.

4.2 Changing the UI (Console) Certificate for Audit Vault Server

Learn how to change the UI certificate for Audit Vault Server.

When you first access the Audit Vault Server console, you see a certificate warning or message. To avoid this type of message, you can upload a new UI certificate signed by a relevant certificate authority.

Prerequisite

Log in to Audit Vault Server console as a super administrator. See Using Audit Vault Server Console for more information

To change the UI certificate for the Audit Vault Server:

1. Click **Settings**.
2. Click the **Security** tab in the left navigation menu.
3. Click the **Certificate** sub-tab on the main page.
4. Click **Console Certificate**.
5. Click **Generate Certificate Request**.

   The **Generate Certificate Request** dialog is displayed with the **Common Name** for the certificate.
6. If you want to change the common name that is displayed, then click **Change**.

   The certificate warnings are based on the common name used to identify Audit Vault Server. To suppress the warning when you access Audit Vault Server console using its IP address instead of the host name, also check **Suppress warnings for IP based URL access**.
7. Complete the form and enter content in the mandatory fields.
8. Click **Submit and Download**.
9. Save the `.csr` file and then submit this file to a certificate authority. Ensure that the certificate contains the following details. The `COMMON NAME` field is filled by default.

   ```
   COMMON NAME


   ISSUER COMMON NAME
   ```
10. After the certificate authority issues a new certificate, upload it by returning to the **Console Certificate** sub tab, and then click **Upload Certificate**.

> **Note:**
>
> You may need to install the public certificate of the Certificate Authority in your browser, particularly if you are using your own public key infrastructure.

The certificate is valid for a specific duration as listed in the table below:

Oracle AVDF Release	Validity Duration

20.1 to 20.3	10 years
20.4	27 months

4.3 Specifying Initial System Settings and Options on Audit Vault Server (Required)

Learn how to specify initial system settings and options on Audit Vault Server.

4.3.1 Specifying the Server Date, Time, and Keyboard Settings

Learn how to specify the Audit Vault Server date, time, and keyboard settings.

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

About Timestamps

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

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

> **WARNING:**
>
> Do not change the Audit Vault Server database time zone through any configuration files. Doing so causes serious problems in Audit Vault Server.

Prerequisite

Log in to Audit Vault Server console as super administrator. See Using Audit Vault Server Console for more information.

Set the Server Date, Time, and Keyboard Settings

1. Click **Settings** tab.
2. Click on the **System** tab in the left navigation menu.
3. In the **Configuration** tab on the main page:

Click	For Oracle AVDF Release

Manage	20.1 and 20.2
System Settings	20.3 and later

4. For Oracle AVDF 20.3 and later, click the **Time & Keyboard** tab in the **System Settings** dialog box.
5. From the **Timezone Offset** drop down list, select your local time in relation to Coordinated Universal Time (UTC). **Timezone Offset** is used in non-interactive scheduled PDF or XLS reports. The time set here is converted to local time and is displayed in **Event Time** field of the report.

   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.

   > **Note:**
   >
   > To change the time only for the console and to the specific user session, follow the steps in Changing the Time Zone. This functionality is available starting with Oracle AVDF release 20.6.

6. From the **Keyboard** drop down list, select the keyboard setting.
7. In the **System Time** field, select **Set Manually** or **Use NTP**.

   Selecting NTP synchronizes time with the average of the time recovered from the time servers specified in the NTP Server 1/2/3 fields.
8. Select **Use NTP**, and then select **Synchronize Periodically** to start using the NTP Server time.

   If you do not enable time synchronization in this step, then you can still enter NTP Server information in the steps below and enable NTP synchronization later.
9. Optionally select **Synchronize Once After Save**, to synchronize the time once when you click **Save**.
10. In the **NTP Server 1**, **NTP Server 2**, and **NTP Server 3** sections enter the IP addresses or names of your preferred time servers.

    If you specify a name, then the DNS server that is specified in the **Services** dialog under **System** tab is used for name resolution.
11. 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**.
12. Click **Save**.

> **Note:**
>
> - In case of high availability environment the steps above change the time only on the primary Audit Vault Server.
> - In case of NTP, specify the IP address of the default gateway and a DNS server to enable time synchronization.

Set the Time on Secondary Audit Vault Server

In case of high availability environment it is important that the primary and secondary Audit Vault Servers must have same time. Follow the steps below to manually set the time on the secondary Audit Vault Server.

For Oracle AVDF 20, follow these steps:

1. Log in to the secondary Audit Vault Server as *root* user.
2. Run the following commands:

```
systemctl stop monitor

systemctl stop controller

systemctl stop dbfwdb

systemctl stop asmdb
```

3. Set the date and time by running the following command:

```
date -s "Day Month DD HH:MM:SS UTC YYYY"
```

   For example:

```
date -s "Fri Jun 02 07:51:17 UTC 2021"
```

4. Run the following commands:

```
systemctl start asmdb

systemctl start dbfwdb

systemctl start controller

systemctl start monitor
```

5. Verify the high availability status. It should be `High Availability mode is enabled`.

For Oracle AVDF 12.2, follow these steps:

1. Log in to the secondary Audit Vault Server as *root* user.

2. Run the following commands:

```
/etc/init.d/monitor stop

/etc/init.d/controller stop

/etc/init.d/dbfwdb stop

/etc/init.d/asmdb stop
```

3. Set the date and time by running the following command:

```
date -s "Day Month DD HH:MM:SS UTC YYYY"
```

   For example:

```
date -s "Fri Jun 02 07:51:17 UTC 2021"
```

4. Run the following commands:

```
/etc/init.d/asmdb start

/etc/init.d/dbfwdb start

/etc/init.d/controller start

/etc/init.d/monitor start
```

5. Verify the high availability status. It should be `High Availability mode is enabled`.

See Also:

- Updating the Audit Vault Server IP Address in the NTP Configuration File
- Unable to Access the AVS Console After Changing the AVS Time Manually or using NTP Server
- Changing the Primary Audit Vault Server Network Configuration
- Configuring or Changing the Audit Vault Server Services
- Setting the Date and Time in Database Firewall

4.3.2 Changing the Time Zone

Learn how to change the time zone in the Audit Vault Server console only for the active session.

The time can be changed in the Audit Vault Server console only for the active session. This is limited only for the console (User Interface). This functionality is available starting with Oracle AVDF release 20.6. Follow these steps:

1. Log in to the Audit Vault Server console as **Administrator**, **Super Auditor**, **Auditor**, or **Readonly Auditor**.
2. Click the drop down icon next to the user name in the top right corner. For example, **Admin** or **Auditor** user icon.
3. Click **Change Timezone** option.
4. In the **Change Timezone** dialog, select your time zone in relation to Coordinated Universal Time (UTC).
5. Click **Save**.

> **Note:**
>
> - The time zone changed here is applicable only to the user's active session. The timestamps in the Audit Vault server console also reflect the selected time zone.
> - This time zone changed here is not reflected in the non-interactive (PDF/ XLS) reports. To change the time in the reports, follow the steps mentioned in Specifying the Server Date, Time, and Keyboard Settings.

4.3.3 Specifying Audit Vault Server System Settings

Learn about configuring Audit Vault Server system settings.

4.3.3.1 Changing the Primary Audit Vault Server Network Configuration

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

1. Log in to the Audit Vault Server console as a *super administrator*.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. Under **Configuration**, click **Network Settings**.
5. In the **Network Settings** dialog box, edit any of the following fields:
   - **Host Name:** Enter the fully qualified domain name of the Audit Vault Server. The host name must start with a letter, can contain a maximum of 64 characters, and cannot contain spaces.

> **Note:**
>
> – Changing the host name reconfigures the Audit Vault Server automatically. After changing the host name and clicking **Save**, the system prompts for confirmation and reconfigures the Audit Vault Server. The Audit Vault Server console is unavailable for a minimum of 10 minutes. After this, the updated host name appears in the **Network Settings** dialog box.
>
> – In Oracle AVDF releases 20.1 to 20.6, you can't change the host name in a high availability environment. If you need to change the host name, unpair the Audit Vault Servers, change the host name, and pair them again.
>
> – In Oracle AVDF release 20.7 and later, you can change the host name of the primary and standby Audit Vault Servers by using the primary Audit Vault Server console.

- **IP Address:** If you need to update the IP address of the Audit Vault Server that was set during the installation, enter the new IP address.

  The IP address is static and must be obtained from the network administrator. 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.

> **Note:**
>
> If you have a high availability configuration, then you need to unpair the primary and standby Audit Vault Servers before changing the IP address, network mask, and gateway. After you update the network settings on the primary or standby Audit Vault Server, pair the two servers again. After you complete the pairing process, redeploy the Audit Vault Agents to ensure that they are updated with the new settings for the primary and standby Audit Vault Servers.

- **Network Mask:** Enter the subnet mask of the Audit Vault Server.
- **Gateway:** Enter 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.
- **Link properties:** Don't change the default setting unless your network has been configured to not use autonegotiation.

6. Click **Save**.
7. Complete the following post-configuration steps:
   a. If the audit trails are not configured to start automatically, start them manually. See Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server.
   b. Reconfigure the resilient pair of Database Firewalls if you previously configured them. See Configuring High Availability for Database Firewalls.
   c. If you changed the IP address of the Audit Vault Server, update the IP address information in the Database Firewall configuration. See Specifying the Audit Vault Server Certificate and IP Address.

d. If you changed the IP address of the Audit Vault Server, redeploy the Audit Vault Agents. See Deploying the Audit Vault Agent.

Related Topics

- Ports Used by Oracle Audit Vault and Database Firewall
  Oracle Audit Vault and Database Firewall uses specific TCP and UDP ports.

4.3.3.2 Changing the Standby Audit Vault Server Network Configuration

Learn how to change the standby Audit Vault Server network configuration.

Starting with Oracle AVDF release 20.7, the network settings of the standby Audit Vault Server can be configured using the primary Audit Vault Server console.

To configure the standby Audit Vault Server network settings:

1. Log in to the primary Audit Vault Server console as a super administrator.
2. Click **Settings** tab.
3. Click **System** tab in the left navigation menu.
4. Under the **Configuration** sub tab in the main page, click **Network Settings**.
5. In the **Network Settings** dialog, the **Settings** sub tab is selected by default. Click **Standby Server** radio button.
6. Edit the **Host Name**. The host name must be a fully qualified domain name of Audit Vault Server. The host name can contain maximum of 64 characters, and cannot contain spaces. The host name of the standby Audit Vault Server cannot be the same as the primary.
7. Click **Save**.

   The following confirmation dialog is displayed:

   ```
   This operation reconfigures the standby Audit Vault Server. This process takes at least 10 minutes. Do you want to continue?
   ```

8. Click **OK**.

> **Note:**
>
> During this time, the standby Audit Vault Server is unavailable for a minimum of 10 minutes. An error message is displayed in the **Network Settings** and **System Settings** dialog on the Audit Vault Server console for failing to reach the standby Audit Vault Server.

> **See Also:**
>
> - Ports Used by Oracle Audit Vault and Database Firewall for a list of default Audit Vault Server port numbers
> - Configuring High Availability for Database Firewalls to configure a resilient pair of Database Firewalls
> - Specifying the Audit Vault Server Certificate and IP Address to update Audit Vault Server's IP address in the Database Firewall

4.3.3.3 Configuring or Changing the Audit Vault Server Services

Learn how to configure and change the Audit Vault Server sevices.

To configure the Audit Vault Server services:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click **Settings** tab.
3. Click **System** tab in the left navigation menu.
4. In the **Configuration** section on the main page:

Click	For Oracle AVDF Release
System Services	20.1 and 20.2
System Settings	20.3 and later

5. Under the **DNS** tab, turn on the button and enter the IP address in the specific fields. Enter the IP addresses of up to three DNS servers on the network. Audit Vault Server uses these IP addresses to resolve host names. Keep the fields disabled if you do not use DNS servers. Enabling these fields could degrade system performance if you use DNS servers.

> **Note:**
>
> The **Client Host** (host name of the client) value is displayed in the reports only if the DNS is configured here.

6. In the dialog, click **Web/SSH/SNMP** tab.
7. Complete the following fields as necessary:

> **Caution:**
>
> When allowing access to Oracle Audit Vault and Database Firewall you must be careful to take proper precautions to maintain security.

- **Web Access:** If you want to allow only selected computers to access the Audit Vault Server console, select **IP Addresses** and enter specific IP addresses in the box, separated by spaces. Using the default value **All** allows access from any computer in your site.
- **SSH Access:** You can specify a list of IP addresses that are allowed to access the Audit Vault Server through SSH, from a remote console by selecting **IP Addresses** and entering them in this field, separated by spaces. Using the value **All** allows access from any computer in your site. Using the value **Disabled** prevents SSH 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 Addresses**. Then enter them in this field, separated by spaces. Selecting **All** allows access from any computer. If you disable this, it prevents SNMP access. The SNMP community string is `gT8@fq+E`.

8. Click **Save**. A message is displayed.
9. Click **OK** in the confirmation dialog.

> **See Also:**
>
> Protecting Your Data for a list of recommendations and precautions to maintain security

4.3.3.4 Changing the Standby Audit Vault Server System Settings

Learn how to change the system settings for the standby Audit Vault Server.

Starting with Oracle AVDF release 20.7, the system settings of the standby Audit Vault Server can be changed using the primary Audit Vault Server console.

To configure the standby Audit Vault Server system settings:

1. Log in to the primary Audit Vault Server console as a super administrator.
2. Click **Settings** tab.
3. Click **System** tab in the left navigation menu.
4. Under the **Configuration** sub tab in the main page, click **System Settings**.
5. In the **System Settings** dialog, the **DNS** sub tab is selected by default. Click **Standby Server** radio button.
6. Enter the IP address in the specific fields. Enter the IP addresses of up to three DNS servers on the network. Audit Vault Server uses these IP addresses to resolve host names. Keep the fields disabled if you do not use DNS servers. Enabling these fields could degrade system performance if you use DNS servers.
7. In the **System Settings** dialog, click on the **Web/SSH/SNMP** tab.
8. Click **Standby Server** radio button.
9. Complete the **Web/SSH/SNMP** fields as necessary. The requirements are similar to the primary Audit Vault Server as mentioned in the previous topic.
10. Click **Save**.

    The following confirmation dialog is displayed:

    ```
    This operation reconfigures the standby Audit Vault Server. This process takes
    at least 2 minutes. Do you want to continue?
    ```

11. Click **OK**.

> **See Also:**
>
> Protecting Your Data for a list of recommendations and precautions to maintain security

4.3.3.5 Changing IP Addresses of Active and Registered Agents

Learn about changing the IP addresses of active and registered Agents.

Use this procedure to change the IP address of a live registered Agents without affecting the functionality of the Audit Vault Agent.

Prerequisites

1. Stop all audit trails managed by the specific Audit Vault Agent. See section Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server for more information.
2. Stop Audit Vault Agent before changing the IP address of the target server. See section Stopping, Starting, and Other Agent Operations for more information to stop the Audit Vault Agent.

To change the IP address of a live registered Agent

1. Change the IP address of the machine on which agent is installed.
2. Change the IP address of the previously registered Agent entity of Oracle Audit Vault and Database Firewall using the Audit Vault Server console or Audit Vault command-line interface.
3. Run the following to start the Audit Vault Agent with the `-k` option:

   ```
   agentctl start -k
   ```

4. Enter an Activation Key.
5. Start Audit Trails.

> **See Also:**
>
> Changing the IP Address on a Single Instance of the Database Firewall Server

4.3.3.6 Updating the Audit Vault Server IP Address in the NTP Configuration File

After updating the Audit Vault Server IP address, if you're using Network Time Protocol (NTP), you need to update the `/etc/ntp.conf` file.

Prerequisite

Update the Audit Vault Server IP address. See Changing the Primary Audit Vault Server Network Configuration.

Procedure

1. Log into the Audit Vault Server console as an *administrator*.
2. Click the **Settings** tab.
3. Click the **System** in the left navigation menu.
4. Under **Configuration**, click **System Settings** (**Manage** in Oracle AVDF 20.2 and earlier).

5. For Oracle AVDF 20.3 and later, click the **Time & Keyboard tab** in the **System Settings** dialog box.
6. Select **Set Manually**.

   This updates `/etc/ntp.conf`.
7. Check the `/etc/ntp.conf` file to verify that the IP address has changed.
8. In the **System Settings** dialog box, select **Use NTP** and enter the NTP server IP addresses or names.

   For details on the field values, see Specifying the Server Date, Time, and Keyboard Settings.
9. Click **Save**.

4.3.4 Configuring Audit Vault Server Syslog Destinations

Learn how to configure Audit Vault Server syslog destinations.

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

Configuring Syslog enables integration with popular SIEM vendors such as Splunk, IBM QRadar, LogRhythm, ArcSight and others.

> **Note:**
>
> Syslog message is sent to the destination machine. The message is not written to the Audit Vault Server /var/log/message file.

Prerequisites

- Log in to the Audit Vault Server console as a super administrator. See Using Audit Vault Server Console for more information.
- Ensure that the IP addresses provided for syslog destinations are on a different host than the Audit Vault Server.

1. Click the **Settings** tab.
2. Click on **System** tab in the left navigation menu.
3. Under the **Configuration** section, click **Connectors**.
4. In the **Connectors** dialog, click on **Syslog** tab.
5. Complete the fields, as necessary:
   - **Syslog Destinations (UDP):** Use this box if you are using User Datagram Protocol (UDP) to communicate syslog messages from 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 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 messages to be sent to Syslog as follows:
  - **Alert:** Alerts based on alert conditions that an Oracle Audit Vault and Database Firewall auditor specifies.

    To forward Oracle Audit Vault and Database Firewall alerts to syslog. In addition to this setting, the Oracle Audit Vault and Database Firewall auditor must configure alert forwarding.
  - **Debug:** Engineering debug messages (for Oracle support use only).
  - **Info:** General Oracle Audit Vault and Database Firewall messages and property changes.
  - **System:** System messages generated by Oracle Audit Vault and Database Firewall or other software that has a syslog priority level of at least `INFO`.

6. Click **Save**.
7. Repeat the initial system settings and options set on the second Audit Vault Server, in case of high availability.

> **See Also:**
>
> - Specifying Initial System Settings and Options on Audit Vault Server (Required)
> - *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed instructions and information about Oracle Audit Vault and Database Firewall syslog alert formats

4.3.5 Configuring Custom Ports on Network Interfaces

Learn how to configure custom ports on network interfaces in standalone and high availability environment.

Oracle Audit Vault and Database Firewall requires TCP and TCPS based external SQL access. By default, the TCP and TCPS ports are 1521 and 1522 respectively. Oracle Audit Vault and Database Firewall supports the configuration of more than one set of custom ports. User-defined ports are also used for SQL connections. As a `super administrator` user you can specify a custom TCP and TCPS port for SQL communication on Oracle Audit Vault Server. Custom ports can be configured for network interfaces in standalone and high availability environment. Upon configuring a custom port, SQL communication is enabled and added to the network configuration.

Follow these instructions while performing backup and restore operations. If you configured a custom port before performing the backup operation, then the port should remain as you configured it during the restore operation.

To configure custom ports on a primary network interface:

> **Note:**
>
> The commands in the procedure below must be executed only on the primary Audit Vault Server in a high availability environment.

1. Log in to the appliance as root user.
2. Switch user to oracle.
3. Use SQL*Plus and connect as super admin user by entering the ID and password as follows.

   `<super-admin>/<password>`

> **Note:**
>
> - Other users cannot configure custom ports. If this operation is attempted by another user, then a message is displayed on the SQL*Plus that there are insufficient privileges for the user.
> - Only root users can access error or debug logs.

4. To configure custom ports and related operations, run the following commands:

Operation	Command
To configure custom TCP and TCPS ports on the Audit Vault Server.	`exec management.server.custom_listener_ports(<tcp_custom_port>, <tcps_custom_port>);`
To disable default ports (`1521`, `1522`) on the Audit Vault Server.	`exec management.server.disable_std_listener_port_access;` After disabling the default listener ports: • The ports will not be disabled at the listener level. • Listener will listen on the custom ports in addition to the default ports. However, the default ports will only be accessbile from the local AVDF server and will be blocked for access from any remote clients. • The AVDF database will only be accessible through the new custom ports from any remote clients.

Upon configuring a new custom port, ensure all the Audit Vault Agents are updated with the new port. After all the Agents are updated, ensure the trails continue to run after the Agents are updated with the new custom ports. The standard ports must be disabled after this verification. If standard ports are disabled before the Agents are updated, then those Agents stop running and need to be manually updated. This can be done by updating the connect string in the `av/conf/bootstrap.prop` file of the Agent home directory.

> **Tip:**
>
> In a high availability environment:
>
> - The same ports are configured on the standby Audit Vault Server
> - The TCPS port configured on the standby is same as primary server during pairing. Else, pairing results in an error.

5. To disable custom ports, run the following commands:

Operation	Command
To rollback custom ports and restore ports 1521 and 1522 as the default ports	`exec management.server.enable_std_listener_port_access` After the standard ports are enabled again, do not disable the custom ports in immediate succession as this may disrupt the communication between the Audit Vault Agent and the Audit Vault Server. In such an event, the Audit Vault Agents have to be reinstalled. Before disabling the custom port and changing back to default ports, ensure the Audit Vault Agents are updated and are in `RUNNING` state.
To disable custom ports	`exec management.server.disable_custom_listener_port_access`

4.4 Configuring the Email Notification Service

Learn about configuring the email notification service.

4.4.1 About Email Notifications in Oracle Audit Vault and Database Firewall

Learn about Oracle Audit Vault and Database Firewall email notifications.

An auditor can configure Oracle Audit Vault and Database Firewall to send users email notifications when alerts or reports are generated. To do this, you must configure an SMTP server to enable email notifications. The email notifications can be sent in text format to mobile devices or they can be routed through an SMS gateway.

> **Note:**
>
> - You can configure one SMTP (or ESMTP) server for Oracle Audit Vault and Database Firewall.
> - You can configure Oracle Audit Vault and Database Firewall to work with both unsecured SMTP servers as well as with secured and authenticated SMTP servers.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Auditor's Guide* for information about configuring alerts and generating reports.

4.4.2 Configuring Email Notifications

To configure email notifications, you need to configure an SMTP server.

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

   See Using Audit Vault Server Console for more information.

2. Click the **Settings** tab.

3. Click **System** in the left navigation menu.
4. Under **Configuration**, click **Connectors**.
5. In the **Connectors** dialog box, enter the IP address of the SMTP server in **SMTP Server Address**.
6. In the **SMTP Port** field, enter the SMTP server port.
7. In the **From Name** field, enter the user name to be used as the sender of the email.
8. In the **From Address** field, enter the sender's address that appears in the email notifications.
9. If this SMTP server requires credentials, then select **Require Credentials**, and enter a user name and password.
10. If this SMTP server requires authentication, then select **Require Secure Connection**, and select the authentication protocol (SSL or TLS).
11. Click **Register** to register the SMTP server.
12. (Optional) Enter the email address and click **Test** to test the email configuration.
13. Click **Save**.

4.5 Configuring Archive Locations and Retention Policies

Learn about configuring archive locations and retention policies.

Note:

Remember the following rules while archiving and restoring tablespaces:

- The restore policy must follow the guidelines in this section.
- Check the tablespace that needs to be archived and the corresponding tablespace that needs to be purged as explained in the policy.
- Restoring data into empty tablespaces is not possible. Check accordingly.
- In case the tablespace enters the delete period, it is deleted automatically from Oracle Audit Vault Server.
- Every tablespace is uniquely identified using the name of the month that it moves offline and the month that it is purged. The tablespaces are created automatically based on the policies that you create.
- When the retention policy changes, the new policy is applied to the incoming data in the following month. It does not affect the existing tablespaces which adhere to the old policy.
- You can archive the tablespace when it enters the offline period.
- After restoring the tablespace, it is actually online. After you release the tablespace, it goes offline. You must rearchive the tablespace after it is released.
- Deleting or truncating records in the `<AVSYS>.EVENT_LOG` table is not supported in Oracle Audit Vault and Database Firewall (AVDF) 12.2. This table is automatically managed and partitioned by the appliance. To remove all test data, the only option is to rebuild the Oracle AVDF server. The `EVENT_LOG` data is encrypted, unmodifiable, and managed internally by retention policies.

4.5.1 About Archiving and Retrieving Data in Oracle Audit Vault and Database Firewall

Learn about archiving and retrieving data in Oracle Audit Vault and Database Firewall.

Data files are archived as part of an information lifecycle strategy. Oracle Audit Vault and Database Firewall release 20.1.0.0.0 supports automatic archival of a job only for NFS configured locations. When the online period of the data on the tablespace expires, it is automatically archived without your intervention. You have a choice to enable automatic archival during a fresh installation of Oracle Audit Vault and Database Firewall in release 20.1.0.0.0. Or, you can manually archive jobs with the desired settings.

When you upgrade to Oracle Audit Vault and Database Firewall release 20.1.0.0.0 from an older release, the system continues to use manual archiving. You have to enable automatic archiving of jobs post upgrade.

You can switch between automatic and manual job archiving. If there is a job in progress during the switch over, then the change occurs after the active job is completed. A suitable message is displayed to the user. After you switch to automatic archiving, all of the existing NFS locations are configured into an automatic archiving list. They are listed under **Manage Archive Locations**. If the space in archive location is full or inaccessible, then automatic archiving chooses the next archive location from the list. The automatic archival functionality runs on a daily basis and archives the data that is available for archiving.

> **Note:**
>
> After you enable automatic archiving, manual archiving is disabled. When upgrading to a newer version in release 20.1.0.0.0, the system continues to use either the automatic or the manual archiving that you configured prior to the upgrade.

You create retention policies and archive locations so that the archived data is transferred in accordance with your policies. Oracle recommends that you archive regularly in accordance with your company's policy.

Automatic archival is supported only on Network File Systems (NFS). 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 Oracle Audit Vault Server. Therefore, you must ensure that there is sufficient space in your file system. Otherwise, the data file copying may fail. Transferring large files using SCP or SMB may take a long time.

What Is a Retention Policy?

Retention policies (also called archive policies) determine how long data is retained in Oracle Audit Vault Server, when data is available for archiving, and for how long archived data can be retrieved to Oracle Audit Vault Server. An administrator creates these policies and an auditor assigns a specific policy to each target as well as to scheduled reports. The settings that you can specify in a policy are as follows:

- Months Online: The audit data is available in Oracle Audit Vault Server for the number of months online that you specify. During this period, data is available for viewing in reports. When this period elapses, the audit data files are available for archiving, and are no longer visible for reports. When the administrator archives these data files, the data is physically removed from Oracle Audit Vault Server.

- Months Archived: The archived audit data can be retrieved to Oracle Audit Vault Server for the number of months specified in `Months Archived`. If you retrieve the data during this period, then it will be available again in reports. When the months archived period expires, the data can no longer be retrieved to Oracle Audit Vault Server.

> **Note:**
>
> Retention times are based on the event time (time it is generated). If the auditor does not select a retention policy for a target or scheduled report, Audit Vault Server uses the default retention policy (12 months for online retention, and 12 months in archives).

Example

Suppose your retention policy is:

- Months Online: 2
- Months Archived: 4

With this retention policy, audit data that is generated during the last two months is available in Audit Vault Server. Data that is older than two months is available for archiving, and is no longer visible in reports. Archived data is available to retrieve for four months. This data is older than two months but newer than six months, and can be retrieved from the archives to Oracle Audit Vault Server. Data that is older than six months is no longer available.

Updating Retention Policies Assigned to Targets

Changing the retention policy will not apply to already collected data. It will be applied to new data and in some cases can take a month for it to be applied. The cases where it takes a month is because of the optimization we have to pre-create underlying data partitions.

For example, if it is currently April and the current policy is six months online and six months in archive and then the policy is modified to be 12 months online and 12 months in archive on April 28th, the data collected in May will use the original six months online and six months in archive policy. However, starting in June the data collected will have the new 12 months online and 12 months in archive retention policy.

When new Data Collected is Older than Retention Policy Limits

When you collect audit data for a newly configured target, or from a new audit trail on an existing target, the data collected from that target may be older than the Months Online period. In fact, the data may be even be older than the Months Archived period.

For instance, suppose your retention policy is the same as the above Example. Now suppose you begin collecting audit data from a newly configured target. If some of this data is over six months old, it is older than the months online period and the months archived period combined. In this case, Oracle Audit Vault and Database Firewall automatically drops any newly collected audit records that are older than six months.

However, if some of this audit data is older than two months but newer than six months, that is, it falls within the months archived period, then Oracle Audit Vault and Database Firewall does one of the following:

- If this is an audit trail for a newly configured target, then Oracle Audit Vault and Database Firewall automatically archives that data as the audit trail is collected.

- If this is a new audit trail for an existing target, then Oracle Audit Vault and Database Firewall attempts to archive these records automatically as the audit trail is collected. However, you may have to make required data files available during this process.

> **Note:**
>
> In case the archive location is not defined, once the months online period expires and before the completion of offline period, the audit data for the specific target is moved offline. The data remains on the Audit Vault Server and can be retrieved and viewed in the Reports section of the Audit Vault Server console. This is applicable for the default and user defined archival and retention policy.

> **See Also:**
>
> Handling New Audit Trails with Expired Audit Records for information to make required data files available

4.5.2 Defining Archive Locations

You need to 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 sufficient space in the file system. Otherwise the data file copying may fail. Transferring large files using SCP or SMB may take a long time.

> **Note:**
>
> The backup functionality does not back up archived files. The data files in the archive location are not backed up by `avbackup` because they may be located on a remote file system. In case those files are on NFS mount point, then they are accessible after restoring on a new system with the same mount points that were previously configured.

- Oracle AVDF Release 20.1 - 20.8
- Oracle AVDF Release 20.9 and later

Oracle AVDF Release 20.1 - 20.8

1. Log in to the Audit Vault Server as an *administrator*.
   See Using Audit Vault Server Console for more information.
2. Click the **Settings** tab.

3. Click **Archiving** in the left navigation menu.
4. Click **Manage Archive Locations**.
5. Click the **Create** button, and complete the fields. See the following field descriptions for more information.
6. Click **Save**.

Oracle AVDF Release 20.9 and later

1. Log in to the Audit Vault Server as an *administrator*.
   See Using Audit Vault Server Console for more information.
2. Click the **Data Retention** tab.
3. Click the **Remote Archiving** tab in the left navigation.
4. Click the **Create** button, and complete the fields. See the following field descriptions for more information.
5. Click **Save**.

Field	Value
Transfer Method	Select the method to transfer data from Oracle 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 System (NFS)**: Select if you're using a network file share or NAS. If you do not select a transfer method, then the archive files will be retained in Event Data in the Audit Vault Server.
Location Name	Enter the name of the archiving destination. This name appears as the archiving destination when you start an archive.

Field	Value
Remote Filesystem	If you use the NFS transfer method, then you can select an existing file system, or one will be created automatically based on the details of this archive location. **Note:** In a standalone system, you can use the `AVCLI` utility to register a remote file system. Then you can select this file system in the Audit Vault Server console. This is not possible in a high availability environment. In a high availability environment, you create the archive locations through the Audit Vault Server console by selecting the **Create New Filesystem** option. See Downloading and Using the AVCLI Command Line Interface for details about using the `AVCLI` utility.
Address	Enter the host name or IP address of the NFS server that the Audit Vault Server uses for archiving. If you use the Windows File Sharing transfer method, then specify the IP address.
Export Directory	If you use the NFS transfer method, then enter the export directory of the NFS server. For example, you can create this directory in the `/etc/exports` file of the NFS server. Ensure that the *oracle* user (User ID: 503) has appropriate `read` and `write` permissions to this directory. **Note:** Special characters (such as $, #, and !) are not allowed in export directory names.

Field	Value
Path	Enter the path to the archive storage location. Enter a path to a directory (not a file) and follow these requirements for each transfer method: • 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 share name, followed by a forward slash and the name of the folder. For example: `/sharename/myfolder`. • Network File System (NFS): Enter the path relative to the export directory. For example, if the export directory is `/export_dir` and the full path to the directory that you want to designate as an archive location is `/export_dir/dir1/dir2`, then enter `/dir1/dir2` in the **Path** field. To put archives directly in the NFS server's export directory, enter `/` (forward slash) for the path. Click the **Test** button to validate the NFS location.
Port	This is the port number that secure copy (scp) uses or the Windows file share service on the machine that archives the data. You can normally use the default port number. If you selected Windows file sharing (SMB) as the transfer method, then use port 445.
Username	Enter the account name on the machine to which the archive data will be transferred.
Authentication Method	If you use secure copy (scp) as the transfer method, then you can select **Password Authentication** and enter the login password. If you use a Linux machine, then you can select **Key-based Authentication**. If you use key-based authentication, then 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 (SMB), or if you selected the password authentication method, then enter the login password for the machine that archives the data.
Public Key	This field appears if you selected key-based 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`.

Related Topics

- Support for External Systems

- REGISTER REMOTE FILESYSTEM
  Use the `REGISTER REMOTE FILESYSTEM` command to register remote file systems with Oracle Audit Vault Server.
- Archiving and Retrieving in High Availability
  Learn about archiving and retrieving audit and network event data in a high availability scenario.
- Error OAV-47402 While Defining Archive Locations Using NFS Mount Point
  Learn what to do when you receive the `OAV-47402` error while defining archive locations.

4.5.3 Creating and Deleting Archive and Retention Policies

Learn about creating and deleting policies.

4.5.3.1 Creating Archive and Retention Policies

You can create retention policies (also called archive policies) that an Oracle Audit Vault and Database Firewall (Oracle AVDF) auditor can apply to targets.

- Oracle AVDF Release 20.1-20.8
- Oracle AVDF Release 20.9 and later

Oracle AVDF Release 20.1-20.8

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. Click **Archiving** in the left navigation menu.
4. Click **Manage Policies**.
5. Click **Create**.
6. Enter a name for the policy.
7. In the **Months Online** field, enter the number of months to retain audit data on the Oracle Audit Vault Server before the data is marked for archiving.
8. In the **Months Archived** field, enter the number of months to retain audit data in the archive location. After this time the data will be purged.
9. Optional - Starting with Oracle AVDF Release 20.7, if you're signed in as a super administrator you can set the policy as the default by selecting **Set as default**.

Oracle AVDF Release 20.9 and later

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Data Retention** tab.
3. Click **Retention Policies** in the left navigation menu.
4. Click **Create**.
5. Enter a name for the policy.
6. In the **Months Online** field, enter the number of months to retain audit data on the Oracle Audit Vault Server before the data is marked for archiving.

7. In the **Months Archived** field, enter the number of months to retain audit data in the archive location. After this time the data will be purged. The default value is 6.
8. Optional - If you're signed in as a super administrator you can set the policy as the default by selecting **Set as default**.
9. Click **Save**.

Months Online

When a target uses an assigned retention policy, the audit data will be available online in the Audit Vault Server for the specified amount of months before moving to the archive location.

> **Note:**
>
> After the months online period expires, the data is no longer visible in reports. Data is removed from the online view and is available in the archive location. You can't delete the online data manually.

Months Archived

When a target uses an assigned retention policy, the audit data will be available in the archive location for the specified amount of months before being purged. While it is in the archive location it is available to be retrieved back online to the Audit Vault Server.

> **Note:**
>
> See Setting a Data Retention (Archiving) Policy for instructions on assigning retention policies.

4.5.3.2 Deleting Archive and Retention Policies

You can delete user-defined retention policies (also called archive policies) that are not assigned to any target databases.

- Oracle AVDF Release 20.1-20.8
- Oracle AVDF Release 20.9 and later

Oracle AVDF Release 20.1-20.8

1. Log in to the Oracle Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. Click **Archiving** in the left navigation menu.
4. Click **Manage Policies**.
5. Under **User-defined Policy**, select the policy to delete.

6. Click **Delete**.

Oracle AVDF Release 20.9 and later

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Data Retention** tab.
3. Click **Retention Policies** in the left navigation menu.
4. Select a minimum of one user-defined retention policies from the list.
5. Click **Delete**.
6. Click **Ok** in the dialog box to confirm deletion of the selected policies.

4.5.4 Viewing Archived Datafiles

Learn how to view archived datafiles.

1. Log in to the Audit Vault Server console as *administrator*.
2. Click the **Settings** tab.
3. Click the **Archiving** tab in the left navigation menu.

   This page lists the archived datafiles with the following details:

Table Field	Description
Target	Name of the target.
Event Month	The specific month in which the events occurred.
Datafiles	Name of the datafile.
Online data expiration date	Data is online until the specified month. Later it is offline.
Offline data expiration date	Data is offline until the specified month. Later it is purged.
Retention Policy	Specifies the online and offline duration of the data.
Archived	Specifies if data is archived externally on SCP, SMB, or NFS locations.
Archive Location	If the data is archived externally, then this field is enabled. It contains the name of the archive location. If you hover the mouse on this field, it displays the type of archive location (SCP, SMB, or NFS), IP address of the archive location, and the path to the archive directory.

> **Note:**
>
> - A *super administrator* can view datafiles pertaining to all targets. An *administrator* can view datafiles only for the targets they have access to.
> - This functionality of viewing the archived datafiles is available starting with Oracle AVDF release 20.6.

4.5.5 Running Archive and Retrieval Jobs

Learn how to run archive and retrieval jobs.

See "Archiving and Retrieving Audit Data".

4.6 Managing Archival and Retrieval in High Availability Environments

Learn how to manage archival and retrieval in high availability environments.

Oracle Audit Vault and Database Firewall supports archiving. Prior to release 12.2.0.11.0, archiving was configured only on the primary Audit Vault Server and there was no ability to configure archiving on the standby server. After a failover, archive locations had to be manually set on the former standby (new primary). Starting with release 12.2.0.11.0, you can now configure NFS archive locations on both the primary and standby Audit Vault Servers, reducing the amount of manual work that needs to be performed following a failover.

Oracle Audit Vault and Database Firewall release 12.2.0.11.0 and later ensures that the primary and secondary Audit Vault Servers have the same number of NFS archive locations. This is crucial for archiving and file management functionality to work effectively in a high availability environment.

> **Note:**
>
> - Any user with admin privileges can perform archival and retrieval tasks.
> - It is recommended that NFS archive locations for primary and secondary Audit Vault Servers are on separate NFS servers.
> - It is recommended to have these NFS servers within the same Data Center as the Audit Vault Server. As in the NFS server for primary Audit Vault Server should be in the same data center and NFS server for secondary Audit Vault Server should be in the same data center.
> - NFS is a mount point on the Audit Vault Server. If you want to replace NFS server, then make sure the Audit Vault Server does not access the mount point.

Prerequisite

Ensure that all of the Prerequisites for Configuring High Availability for Audit Vault Servers are satisfied before configuring high availability.

After you complete the high availability pairing, the NFS locations pertaining to both the primary and secondary Audit Vault Servers are displayed under **Manage Archive Locations** of the primary Audit Vault Server console. These NFS locations include those created on both the primary and secondary Audit Vault Servers before and after configuring high availability. The names of these NFS locations have the primary location name or the name defined while creating the location once high availability is configured. The Audit Vault Server console provides details of the host, export directory, and destination path for both the primary and secondary Audit Vault Servers.

> **Note:**
>
> Oracle Audit Vault and Database Firewall release 20.1.0.0.0 supports automatic archival on both primary and secondary Audit Vault Servers. If automatic archival is enabled on the primary Audit Vault Server, it is enabled on the corresponding secondary Audit Vault Server as well. The Audit Vault Server console displays the archive locations of the primary host with their mapped corresponding secondary locations.

Upgrade and archiving functionality in high availability environment

Archiving functionality is disabled during the upgrade process only when there are datafiles archived to the NFS locations. Upon completion of the upgrade process the *admin* user must enable the archive functionality to start archiving.

Updating or Deleting NFS locations

The *super admin* can update or delete the NFS locations after high availability pairing of primary and secondary Audit Vault Servers. The NFS locations on both the primary and secondary Audit Vault Servers can be updated or deleted. In case the datafiles are archived, the location cannot be updated or deleted. The **Location Name** and the **Primary Server Path** or the **Secondary Server Path** can be updated in case high availability is enabled. However, the NFS mount point is internal and cannot be changed.

> **See Also:**
>
> - Monitoring Jobs
> - Defining Archive Locations

4.7 Defining Resilient Pairs for High Availability

Learn how to define resilient pairs for high availability.

You can define resilient pairs of Oracle Audit Vault Servers, Oracle Database Firewalls, or both.

When you define a resilient pair of Oracle Audit Vault Servers, you must perform all of the configuration tasks. These tasks include adding database firewalls to the server and registering the targets on the primary Oracle Audit Vault Server.

> **See Also:**
>
> High Availability in Oracle AVDF

4.8 Registering Database Firewall in Audit Vault Server

Use this procedure to register an Database Firewall with the Audit Vault Server.

Prerequisites

- If you are deploying more than one Database Firewall, then you must register each firewall in Audit Vault Server to enable communication among the servers. We suggest that you first configure Database Firewall using the instructions in Configuring Database Firewall.
- You must register Database Firewalls in Audit Vault Server before you can pair them for high availability. See Configuring High Availability for Database Firewalls for more information.
- Provide the Audit Vault Server certificate and IP address to the Database Firewall that you are registering. See Specifying the Audit Vault Server Certificate and IP Address.
- Log in to Audit Vault Server as an administrator. See Using Audit Vault Server Console for more information.

To register Database Firewall in Audit Vault Server:

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

   The Firewalls page displays the currently registered firewalls and their statuses.
3. Click **Register**.
4. Enter a *Name* for Database Firewall and its *IP Address*.
5. Click **Save**.

> **Note:**
>
> - If a message indicates that there is a problem with the certificate, then ensure that the date and time settings are identical on both Database Firewall and Audit Vault Server.
> - If the following error message is encountered, then check the Audit Vault Server certificate is copied properly to the Database Firewall. Also check the date and time settings are identical on both the Database Firewall and Audit Vault Server.
>
>   ```
>   OAV-46981 Unable to connect to Database Firewall with IP
>   ```

4.9 Testing Audit Vault Server System Operations

Learn about testing Audit Vault Server system operations.

Verify that your system is fully operational before beginning your normal, day-to-day operations.

Prerequisite

Log in to Audit Vault Server as an administrator. See Using Audit Vault Server Console for more information.

To test your system's operation:

1. Check the date and time settings of Audit Vault Server.
2. Click the **Settings** tab.
3. Click on the **System** tab in the left navigation menu.
4. Under **Monitoring** section in the main page, click **Diagnostics**.
5. Click the **Run Diagnostics** button to run a series of diagnostic tests and review the results.

   These diagnostics include testing:

   - Existence and access permissions of configuration files
   - File system sanity
   - Network configuration
   - Status of various processes that are required to run on the system. For example, database server processes, event collection process, Java framework process, HTTP server process, and so on.
6. You can use the **Download Diagnostics** button to download the diagnostic results for further analysis.
7. You can use the **Clear Diagnostic Logs** button to clear the current set of diagnostic logs on the Audit Vault Server.
8. Click the **Home** tab, and check the status of **Database Firewalls** and **Targets**.

4.10 Configuring Fiber Channel-Based Storage for Audit Vault Server

Learn about configuring fiber channel-based storage for Audit Vault Server.

Audit Vault Server supports fiber channel-based storage. You can configure this storage during installation by performing this procedure.

To configure fiber channel-based storage for Audit Vault Server:

1. Install Audit Vault Server on the local disk of your server. During installation, Audit Vault Server attempts to use all of the disks in your system. Use the configuration tools for the fiber channel controller such as Fast!UTIL, to ensure that other disks are not accessible.

> **Note:**
>
> - If the other disks are accessible, then they are formatted and erased during installation.
> - Audit Vault Server looks for the devices with the names of sd*, xvd*, hd*, cciss*, fio* in `/sys/block`. The installation succeeds if the fiber channel disks are exposed as one of these block devices.
> - The device xvd* is not supported for multipath.
> - The first disk must be a local disk with a minimum of 300 GB available space. If the available space is less than 300 GB, then the boot partition is allocated to a SAN fiber channel disk which is not supported. It is recommended that the sizes of the other disks be greater than that of the first disk.

2. If you are using fiber channel-based storage, then perform the following remaining steps after your installation has successfully completed to ensure that Oracle Automatic Storage Management uses the active path. Otherwise, reboot your system to complete the configuration process.

> **Note:**
>
> Fiber channel-based storage with multipath is supported by Oracle Audit Vault and Database Firewall release 20.1 and onwards.

4.11 Fiber Channel Based Multipath in Oracle AVDF

Learn about support for multipath in Oracle AVDF.

Oracle Audit Vault and Database Firewall 20.1 and later supports fiber channel based storage with multipath. The redundant paths in multipath can enhance performance and utilize features like dynamic load balancing, traffic shaping, automatic path management, and dynamic reconfiguration. The connection to the disk can be made through two fiber channel ports.

Here are some important aspects of multipath in Oracle AVDF:

- It is not supported with ISCSI storage.
- It does not support the device xvd*.
- Multipath is supported only for Audit Vault Server installation.
- Multipath is not supported for Database Firewall installation.
- It does not support removable block devices. Check for removable block devices in the system as they can lead to installation failure.

Note:

In case there are removable block devices in the system, the following error may be encountered during Audit Vault Server installation:

```
ERROR: Failed to check if the disk is in multipath
Traceback (most recent call last):
  File "/run/install/repo/partitions.py", line 386, in <module>
    main()
  File "/run/install/repo/partitions.py", line 372, in main
    write_partition_table( None )
  File "/run/install/repo/partitions.py", line 322, in write_partition_table
    part_table = generate_partition_table_data(dev_list)
  File "/run/install/repo/partitions.py", line 243, in
generate_partition_table_data
    raise RuntimeError("No disks detected")
RuntimeError: No disks detected
```

4.12 Adding Network Address Translation IP Addresses to Audit Vault Agent

You can add Network Address Translation (NAT) IP addresses to Audit Vault Agent.

Network Address Translation (NAT) is a method of remapping one IP address space into another. This is done by modifying network address information in the IP header of packets when they are in transit across traffic routing devices. Use this procedure to manually add the NAT IP address of the Audit Vault Server to the Audit Vault Agent.

In some deployments, Audit Vault Servers are within NAT networks. The Agents are deployed in a network outside of the NAT configured network with actual IP addresses of Audit Vault Server. In such cases, the Agents cannot reach Audit Vault Server.

In this case, you can add the NAT IP address and port mapping information to the `dbfw.conf` file of Audit Vault Server. This ensures adding an extra connection string in the Agent's `bootstrap.prop` file so that Agents can be deployed in both NAT and non NAT networks. This functionality is available from Oracle AVDF 12.2.0.8.0 and later.

Use Cases

Case	Configuration Type	Description
Case 1	Audit Vault Server configuration without high availability.	• There is only one Audit Vault Server. This server is behind NAT. • Agents in this set up can either connect to Audit Vault Server directly without NAT, or connect to the Audit Vault Server through NAT. • Agents connecting to Audit Vault Server directly, use IP address and port of Audit Vault Server. • Agents connecting to Audit Vault Server through NAT use the IP address and port of Audit Vault Server.

Case	Configuration Type	Description
Case 2	Audit Vault Server configuration with high availability.	• Both the primary and secondary Audit Vault Servers are behind the same NAT. The primary NAT IP address and secondary NAT IP address is the same. The primary NAT port and secondary NAT port are different. • Agents in this set up can either connect to Audit Vault Server directly without NAT, or through NAT. • Agents connecting to Audit Vault Server directly use the IP address and port of Audit Vault Server. In case of a failover of the primary Audit Vault Server, the Agents continue to connect to the secondary Audit Vault Server using the IP address and port of the secondary Audit Vault Server. • Agents connecting to Audit Vault Server through NAT use the IP address and port of the primary Audit Vault Server. In case of failover of the primary Audit Vault Server, the Agents continue to connect to the secondary Audit Vault Server using the IP address and port of the secondary Audit Vault Server.
Case 3	Primary and secondary Audit Vault Servers with different NAT IP addresses.	• Both the primary and secondary Audit Vault Servers are behind two different NAT IP addresses. The primary NAT IP address and secondary NAT IP address are different. The primary NAT port and secondary NAT port can be the same or different. • Agents in this setup can either connect to Audit Vault Server directly without NAT or through NAT. • Agents connecting to Audit Vault Server directly use the IP address and port of the Audit Vault Server. In case of failover of the primary Audit Vault Server, the Agents continue to connect to the secondary Audit Vault Server using the IP address and port of the secondary Audit Vault Server. • Agents connecting to the Audit Vault Server through NAT use the IP address and port of the primary Audit Vault Server. In case of failover of the primary Audit Vault Server, the Agents continue to connect to the secondary Audit Vault Server using the IP address and port of the secondary Audit Vault Server.

To add the NAT IP address of Audit Vault Server into Audit Vault Agent, follow these steps:

1. Log in to the Audit Vault Command Line Interface (AVCLI) as the *admin* or *oracle* user.
2. Take a backup of the configuration file before proceeding:

   ```
   cp /usr/local/dbfw/etc/dbfw.conf /usr/local/dbfw/etc/dbfw.conf.backup
   ```

3. Edit the `dbfw.conf` file to include the NAT IP address in the Audit Vault Server as follows:

   ```
   NAT_PRIMARY_IP_ADDRESS=<xx.yyy.zzz.aaa>
   NAT_PRIMARY_AGENT_PORT_TLS=<12345>
   NAT_PRIMARY_AGENT_PORT=<12346>
   ```

4. Save the changes.

5. Regenerate the agent by running the following command:

```
avca configure_bootstrap
```

After this, all of the Agents downloaded contain one of the strings with the NAT IP address. To verify, check the contents of the bootstrap file at `/var/lib/oracle/dbfw/av/conf/bootstrap.prop` which should be as follows:

```
SYS.CONNECT_STRING999=(DESCRIPTION=(ENABLE=BROKEN)(ADDRESS=(PROTOCOL=TCP)
(HOST=10.240.114.167)(PORT=13031))
(CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB)))
SYS.SSL_CONNECT_STRING999=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)
(HOST=10.240.114.167)(PORT=13032))
(CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB)(SERVER=DEDICATED))(SECURITY=
(SSL_SERVER_CERT_DN="DC=com,CN=avserver,OU=db,O=oracle")))
```

6. The above case is applicable in Case 1 that is mentioned in the table above. In Case 2 and Case 3, Audit Vault Server is in high availability mode. In these cases, you need to configure the `dbfw.conf` file with an additional set of parameters as follows:

```
NAT_PRIMARY_IP_ADDRESS=<xx.yyy.zzz.aaa>
NAT_PRIMARY_AGENT_PORT_TLS=<12345>
NAT_PRIMARY_AGENT_PORT=<12346>
NAT_SECONDARY_IP_ADDRESS=<xx.yyy.zzz.ccc>
NAT_SECONDARY_AGENT_PORT_TLS=<56789>
NAT_SECONDARY_AGENT_PORT=<12678>
```

7. Save the changes.
8. After this, the Agent's `bootstrap.prop` file is configured with a high availability connect string to include the above set of IP addresses and ports. To verify this, check the contents of the bootstrap file at `/var/lib/oracle/dbfw/av/conf/bootstrap.prop` which should be as follows:

```
SYS.CONNECT_STRING999=(DESCRIPTION_LIST=(LOAD_BALANCE=off)(FAILOVER=on)
(DESCRIPTION=(ENABLE=BROKEN)(ADDRESS_LIST=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)(HOST=<NAT_PRIMARY_AGENT_PORT>)
(PORT=<NAT_PRIMARY_AGENT_PORT>)))

(CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB)))(DESCRIPTION=(ENABLE=BROKEN)
(ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)
(HOST=<NAT_SECONDARY_IP_ADDRESS>)(PORT=NAT_SECONDARY_AGENT_PORT>)))
(CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB))))

SYS.SSL_CONNECT_STRING999=(DESCRIPTION_LIST=(LOAD_BALANCE=off)(FAILOVER=on)
(DESCRIPTION=(ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCPS)
(HOST=<NAT_PRIMARY_IP_ADDRESS>)(PORT=<NAT_PRIMARY_AGENT_PORT_TLS>)))
(CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB)(SERVER=DEDICATED))(SECURITY=
(SSL_SERVER_CERT_DN="DC=com,CN=avserver,OU=db,O=oracle")))
(DESCRIPTION=(ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCPS)
(HOST=<NAT_SECONDARY_IP_ADDRESS>)(PORT=<NAT_SECONDARY_AGENT_PORT_TLS>)))
(CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB)(SERVER=DEDICATED))
(SECURITY=(SSL_SERVER_CERT_DN="DC=com,CN=avserver,OU=db,O=oracle"))))
```

4.13 Monitoring Audit Vault Server

Learn how to monitor Audit Vault Server.

Monitoring enables investigation of suspicious activity, accountability for actions, and address auditing requirements for compliance.

Starting in Oracle AVDF 20.13 application auditing is enabled by default on the Audit Vault Server. Additionally, along with application audit reports, the OS audit and embedded repository audit reports are available out of the box. Application Auditing and OS and Repository Auditing in AVDF 20.13 and later

In Oracle AVDF 20.7 - 20.12, monitoring involves configuring auditing (in both embedded repository and operating system) and collecting the generated records into a shadow Audit Vault Server for analysis and reporting. The Audit Vault Server automatically configures auditing for both the operating system and the embedded repository: OS and Repository Auditing in AVDF 20.7-20.12.

4.13.1 Application Auditing

Learn how to monitor the AVDF application in Oracle AVDF 20.13 and later.

Starting in Oracle AVDF 20.13, application auditing which audits administrator and auditor operations on both the Audit Vault Server and the Database Firewall is enabled by default. The following operations are audited:

- Administrator operations
  - User management and activities
  - Target management
  - Audit trail management
  - Audit Vault Agent management
  - Database Firewall management
- Auditor operations
  - User management
  - Global Sets management
  - Audit, Database Firewall, and Alert policy activities
  - Alert status changes
  - Assessment report
  - Target - Schedule Retrieval Jobs

Application audit records are automatically collected and available as reports for analysis. These reports are purged after six months from the date of the event.

By default, the application audit trail is purged every seven days by the `AVS_MAINTENANCE_JOB`.

Oracle recommends a minimum of 12 GB and a maximum of 30 GB of free space on the `EVENTDATA` disk for application auditing.

4.13.1.1 Viewing AVDF Application Auditing Reports

The application audit reports can be viewed by a `super auditor` on the **AVDF System Report** page.

1. Log in to the Audit Vault Server Console as a `super auditor`.
2. Click on the **Reports** tab.
3. Click on **AVDF System Reports**.
4. Select either the **All Activity** or **Application Auditing** report.
   The All Activity report includes all the audited activities of the AVDF appliance's application, embedded repository, and operating system.

   The Application Auditing report includes all the audited activities of the AVDF appliance's application.

Records in the AVDF System Reports will be purged after six months.

You can schedule and generate these reports, Scheduling and Generating PDF or XLS Reports.

Related Topics

- AVDF System Reports - Auditor Guide

4.13.1.2 Disable AVDF Application Auditing

Perform the following steps to disable AVDF application auditing which is enabled by default in AVDF 20.13 and later.

> **Note:**
>
> Disabling application auditing is not recommended, but if application auditing is causing operational issues then it may be necessary to temporarily disable it.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Unlock the `avsys` account.
   a. Switch to the `dvaccountmgr` user.

      ```
      su - dvaccountmgr
      ```

   b. Start SQL*Plus without the user name and password.

      ```
      sqlplus /
      ```

   c. Run the following command to unlock `avsys`:

      ```
      alter user avsys identified by <password> account unlock;
      ```

d. Exit SQL*Plus.

```
exit
```

> **Note:**
>
> Remember to relock the `avsys` account when you've completed this task.

3. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. Switch to the `oracle` user.

```
su - oracle
```

5. Start SQL*Plus as the `avsys` user.

```
sqlplus avsys
```

6. Execute the following to stop the AVDF application audit trail:

```
avsys.app_audit.disable;
```

   If this trail is stopped, the `AVS_MAINTENANCE_JOB` will purge the records after 28 days.

7. (Optional) Execute the following to stop the collection of the audit trail:

```
avsys.avdf_system_audit.stop_app_audit_trail
```

   If the application audit trail is stopped then it is redundant to stop the collection of the audit trail as the trail will be empty.

8. Lock the `avsys` account.

   a. Switch to the `dvaccountmgr` user.

```
su - dvaccountmgr
```

   b. Start SQL*Plus without the user name and password.

```
sqlplus /
```

   c. Run the following command to lock `avsys`:

```
alter user avsys account lock;
```

   d. Exit SQL*Plus.

```
exit
```

4.13.1.3 Enable AVDF Application Auditing

Perform the following steps to re-enable AVDF application auditing which is enabled by default in AVDF 20.13 and later.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Unlock the `avsys` account.

   a. Switch to the `dvaccountmgr` user.

   ```
   su - dvaccountmgr
   ```

   b. Start SQL*Plus without the user name and password.

   ```
   sqlplus /
   ```

   c. Run the following command to unlock `avsys`:

   ```
   alter user avsys identified by <password> account unlock;
   ```

   d. Exit SQL*Plus.

   ```
   exit
   ```

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

3. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. Switch to the `oracle` user.

   ```
   su - oracle
   ```

5. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

6. Execute the following to start the AVDF application audit trail:

   ```
   avsys.app_audit.enable;
   ```

7. If you previously stopped the collection of the application audit trail, execute the following to re-start the collection:

   ```
   avsys.avdf_system_audit.start_app_audit_trail
   ```

8. Lock the `avsys` account.

a. Switch to the `dvaccountmgr` user.

```
su - dvaccountmgr
```

b. Start SQL*Plus without the user name and password.

```
sqlplus /
```

c. Run the following command to lock `avsys`:

```
alter user avsys account lock;
```

d. Exit SQL*Plus.

```
exit
```

4.13.2 Operating System and Repository Auditing

Learn how to audit AVDF's operating system (OS) and embedded repository.

4.13.2.1 OS and Repository Auditing in AVDF 20.13 and later

Learn how to audit the AVDF OS and repository in Oracle AVDF 20.13 and later.

4.13.2.1.1 About Auditing Operating System

Learn all about auditing of the operating system.

Audit Vault Sever enables default Oracle Linux audit configuration. The configuration settings are available in `/etc/audit/auditd.conf` file and the audit logs are recorded in `/var/log/audit directory`.

4.13.2.1.2 Audit Policies Used in Application Auditing

Learn what audit policies are used to configure application auditing in Oracle AVDF 20.13 and later.

Table 4-1 Oracle Predefined Policies Configured for Audit Vault Server

Policy Name	Description
`ORA_LOGON_FAILURES`	Any failed log in events.
`AVDF_ORA_SECURECONFIG`	This policy is the same as `ora_secureconfig`, secure configuration defined by Oracle Database except for the `AVSYS` and `MANAGEMENT` users.
`AVSYS_DV_UA_POLICY`	Database Vault protected `AVSYS` realm. The Database Vault `AVSYS` realm protects all objects owned by the `AVSYS` database schema.
`MANAGEMENT_DV_UA_POLICY`	Database Vault protected `MANAGEMENT` realm. The Database Vault `MANAGEMENT` realm protects all objects owned by the `MANAGEMENT` database schema.
`AUDIT_DB_MGMT_POLICY`	Database management operations.

Table 4-1 (Cont.) Oracle Predefined Policies Configured for Audit Vault Server

Policy Name	Description
AUDIT_SELECT_DICTIONARY_POLICY	Select any dictionary privilege except for AVSYS and MANAGEMENT user.

> **See Also:**
>
> - Logon Failures Predefined Unified Audit Policy
> - Secure Options Predefined Unified Audit Policy

AVDF_ORA_SECURECONFIG

The AVDF_ORA_SECURECONFIG policy audits the following except for AVSYS and MANAGEMENT users.

```
CREATE AUDIT POLICY AVDF_ORA_SECURECONFIG
    PRIVILEGES ALTER ANY TABLE, CREATE ANY TABLE, DROP ANY TABLE,
    CREATE ANY PROCEDURE, DROP ANY PROCEDURE, ALTER ANY PROCEDURE,
    GRANT ANY PRIVILEGE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE,
    AUDIT SYSTEM, CREATE EXTERNAL JOB, CREATE ANY JOB,
    CREATE ANY LIBRARY,
    EXEMPT ACCESS POLICY,
    CREATE USER, DROP USER,
    ALTER DATABASE, ALTER SYSTEM,
    CREATE PUBLIC SYNONYM, DROP PUBLIC SYNONYM,
    CREATE SQL TRANSLATION PROFILE, CREATE ANY SQL TRANSLATION
PROFILE,
    DROP ANY SQL TRANSLATION PROFILE, ALTER ANY SQL TRANSLATION
PROFILE,
    TRANSLATE ANY SQL,
    EXEMPT REDACTION POLICY,
    PURGE DBA_RECYCLEBIN, LOGMINING,
    ADMINISTER KEY MANAGEMENT, BECOME USER
    ACTIONS  ALTER USER, CREATE ROLE, ALTER ROLE, DROP ROLE,
    SET ROLE, CREATE PROFILE, ALTER PROFILE,
    DROP PROFILE, CREATE DATABASE LINK,
    ALTER DATABASE LINK, DROP DATABASE LINK,
    CREATE DIRECTORY, DROP DIRECTORY,
    CREATE PLUGGABLE DATABASE,
    DROP PLUGGABLE DATABASE,
    ALTER PLUGGABLE DATABASE,
    EXECUTE ON DBMS_RLS,
    ALTER DATABASE DICTIONARY
WHEN
    'sys_context(''''USERENV'''',''''CURRENT_USER'''')
    NOT IN (''''AVSYS'''', ''''MANAGEMENT'''')'
    EVALUATE PER STATEMENT;
```

AVSYS_DV_UA_POLICY

`CREATE AUDIT POLICY` statement shows the `AVSYS_DV_UA_POLICY` unified audit policy definition as follows:

```
create audit policy AVSYS_DV_UA_POLICY actions component=dv
realm violation on "Audit Vault Realm",
realm success on "Audit Vault Realm",
realm access on "Audit Vault Realm",
rule set failure on "AVSYS audit command",
rule set success on "AVSYS audit command",
rule set eval on "AVSYS audit command"
```

Unified Audit Policy for Database Vault AVSYS Realm

`AVSYS` Database Vault realm protects all `AVSYS` objects including `AVSYS` tables, packages, and others. `AVSYS_DV_UA_POLICY` audits all activities on the Database Vault `AVSYS` realm.

The following commands are audited by Database Vault AVSYS realm:

- `drop database link`
- `drop index`
- `drop package`
- `drop package body`
- `drop procedure`
- `drop sequence`
- `drop synonym`
- `drop table`
- `drop type`
- `drop type body`
- `drop view`
- `delete`
- `revoke`
- `truncate table`

MANAGEMENT_DV_UA_POLICY

`CREATE AUDIT POLICY` statement shows the `MANAGEMENT_DV_UA_POLICY` unified audit policy definition as follows:

```
create audit policy MANAGEMENT_DV_UA_POLICY actions component=dv
realm violation on "Audit Vault Account Manager Realm",
realm success on "Audit Vault Account Manager Realm",
realm access on "Audit Vault Account Manager Realm",
rule set failure on "MANAGEMENT audit command",
```

```
rule set success on "MANAGEMENT audit command",
rule set eval on "MANAGEMENT audit command"
```

Unified Audit Policy for Database Vault MANAGEMENT Realm

Management Database Vault realm protects all the `MANAGEMENT` object, includes `MANAGEMENT` tables, packages, etc. `MANAGEMENT_DV_UA_POLICY` audits all activities on the Database Vault `MANAGEMENT` realm.

The following commands are audited by Database Vault `MANAGEMENT` realm:

- `drop database link`
- `drop index`
- `drop package`
- `drop package body`
- `drop procedure`
- `drop sequence`
- `drop synonym`
- `drop table`
- `drop type`
- `drop type body`
- `drop view`
- `delete`
- `revoke`
- `truncate table`

AUDIT_DB_MGMT_POLICY

`CREATE AUDIT POLICY` statement shows the `AUDIT_DB_MGMT_POLICY` unified audit policy definition and audits all users:

```
create audit policy audit_db_mgmt_policy
privileges
ALTER PUBLIC DATABASE LINK,
AUDIT ANY, AUDIT SYSTEM,
CREATE ANY TRIGGER, CREATE PUBLIC DATABASE LINK,
DROP ANY DIRECTORY, DROP PUBLIC DATABASE LINK
actions
ALTER FUNCTION, ALTER PACKAGE, ALTER PROCEDURE,
ALTER TRIGGER,
CREATE PACKAGE, CREATE PACKAGE BODY, CREATE PROCEDURE,
CREATE SPFILE, CREATE TRIGGER,
DROP FUNCTION, DROP PACKAGE, DROP PROCEDURE,
DROP TRIGGER;
```

AUDIT_SELECT_DICTIONARY_POLICY

`CREATE AUDIT POLICY` statement shows the `AUDIT_SELECT_DICTIONARY_POLICY` unified audit policy definition and audits all users except `AVSYS` and `MANAGEMENT`:

```
CREATE AUDIT POLICY  AUDIT_SELECT_DICTIONARY_POLICY
        PRIVILEGES
        SELECT ANY DICTIONARY
    WHEN 'sys_context(''''USERENV'''',''''CURRENT_USER'''')
        NOT IN (''''AVSYS'''', ''''MANAGEMENT'''')'
        EVALUATE PER STATEMENT;
```

4.13.2.1.3 Viewing AVDF OS and Repository Audit Report

The OS and repository audit reports can be viewed by a `super auditor` on the **AVDF System Report** page.

1. Log in to the Audit Vault Server Console as a `super auditor`.
2. Click on the **Reports** tab.
3. Click on **AVDF System Reports**.
4. Select one of the following reports:
   - **All Activity** - The All Activity report includes all the audited activities of the AVDF appliance's application, embedded repository, and operating system.
   - **Database Auditing** - The Database Auditing report includes all the audited activities of the AVDF appliance's embedded repository.
   - **OS Auditing** - The OS Auditing report includes all the audited activities of the AVDF appliance's embedded operating system.

Records in the AVDF System Reports will be purged after six months.

You can schedule and generate these reports, Scheduling and Generating PDF or XLS Reports.

Related Topics

- AVDF System Reports - Auditor Guide

4.13.2.1.4 Stop AVDF Operating System and Repository Auditing

Perform the following steps to stop auditing of the AVDF operating system and embedded repository in AVDF 20.13 and later.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Unlock the `avsys` account.
   a. Switch to the `dvaccountmgr` user.

      ```
      su - dvaccountmgr
      ```

b. Start SQL*Plus without the user name and password.

```
sqlplus /
```

c. Run the following command to unlock `avsys`:

```
alter user avsys identified by <password> account unlock;
```

d. Exit SQL*Plus.

```
exit
```

> **Note:**
>
> Remember to relock the `avsys` account when you've completed this task.

3. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. Switch to the `oracle` user.

```
su - oracle
```

5. Start SQL*Plus as the `avsys` user.

```
sqlplus avsys
```

6. Execute one the following to stop the collection of the listed audit trail:

   - `avsys.avdf_system_audit.stop_database_trail` to stop the collection of the embedded repository's unified audit trail
   - `avsys.avdf_system_audit.stop_os_trail` to stop the collection of the OS trail
   - `avsys.avdf_system_audit.stop_avdf_trails` to stop the collection of the above trails in addition to the application audit trail - Application Auditing

   It is not possible to disable the audit trail for the AVDF OS or embedded repository, however stopping the collection will prevent additional records from being stored in the AVDF System Reports.

7. Lock the `avsys` account.

   a. Switch to the `dvaccountmgr` user.

```
su - dvaccountmgr
```

   b. Start SQL*Plus without the user name and password.

```
sqlplus /
```

   c. Run the following command to lock `avsys`:

```
alter user avsys account lock;
```

d. Exit SQL*Plus.

```
exit
```

4.13.2.1.5 Start AVDF Operating System and Repository Auditing

Perform the following steps to start auditing of the AVDF operating system and embedded repository in AVDF 20.13 and later.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Unlock the `avsys` account.

   a. Switch to the `dvaccountmgr` user.

   ```
   su - dvaccountmgr
   ```

   b. Start SQL*Plus without the user name and password.

   ```
   sqlplus /
   ```

   c. Run the following command to unlock `avsys`:

   ```
   alter user avsys identified by <password> account unlock;
   ```

   d. Exit SQL*Plus.

   ```
   exit
   ```

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

3. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. Switch to the `oracle` user.

   ```
   su - oracle
   ```

5. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

6. Execute one the following to start the collection of the listed audit trail:

   - `avsys.avdf_system_audit.start_database_trail` to start the collection of the embedded repository's unified audit trail
   - `avsys.avdf_system_audit.start_os_trail` to start the collection of the OS trail
   - `avsys.avdf_system_audit.start_avdf_trails` to start the collection of the above trails in addition to the application audit trail - Application Auditing

7. Lock the `avsys` account.
   a. Switch to the `dvaccountmgr` user.

      ```
      su - dvaccountmgr
      ```

   b. Start SQL*Plus without the user name and password.

      ```
      sqlplus /
      ```

   c. Run the following command to lock `avsys`:

      ```
      alter user avsys account lock;
      ```

   d. Exit SQL*Plus.

      ```
      exit
      ```

4.13.2.1.6 About Purging Unified Audit Trail on the Main Audit Vault Server

Learn how to configure a purge job for unified audit data pertaining to the Audit Vault Server.

Unified audit trail data that is older than 7 days is purged by default. This is done as part of the `AVS_MAINTENANCE_JOB` that is scheduled to run daily by default. The schedule can be changed using the Audit Vault Server console.

> **See Also:**
>
> Schedule Maintenance Jobs

It is recommended to configure a unified audit trail purge job in the Audit Vault Server. Follow these steps to configure unified audit trail purge job:

1. Log in to the Audit Vault Server as *root* OS user.
2. Run the command to switch to *oracle* user:

   ```
   su - oracle
   ```

3. Start *SQL*Plus* connection as `sqlplus /nolog` without the username or password.
4. In *SQL*Plus* run the following command:

   ```
   connect <sysdba>
   ```

   Enter the password when prompted. Alternatively, run the command:

   ```
   connect <sysdba/password>
   ```

5. Run the following SQL script to create a purge job with the job name `AVS_UNIFIED_AUDIT_CLEANUP` for Unified Audit Trail:

```
begin
      dbms_audit_mgmt.create_purge_job(
        audit_trail_type => dbms_audit_mgmt.audit_trail_unified,
        audit_trail_purge_interval => 1,
        audit_trail_purge_name => 'AVS_UNIFIED_AUDIT_CLEANUP',
        use_last_arch_timestamp => true,
        container => dbms_audit_mgmt.container_current);
  end;
```

This job runs once every hour to clean up the unified audit trail based on the archived timestamp updated by the Audit Vault Server Database auditing collection.

> **Best Practice:**
>
> It is recommended to configure unified audit trail purge job.

> **Note:**
>
> When you configure unified audit trail purge job, the cleanup performed as part of `AVS_MAINTENANCE_JOB` is automatically removed and the following message is displayed in the **Job Status** page:
>
> ```
> Audit Trail cleanup for Audit Vault Server is enabled, so not
> purging audit data by Maintenance
> ```

> **Note:**
>
> To check the status of `AVS_UNIFIED_AUDIT_CLEANUP`, run the following SQL statement:
>
> ```
> select * from dba_scheduler_job_run_details where
> job_name='AVS_UNIFIED_AUDIT_CLEANUP';
> ```
>
> Refer to Audit Trail Management Data Dictionary Views for more information.

4.13.2.2 OS and Repository Auditing in AVDF 20.7-20.12

Learn how to audit the AVDF OS and repository in Oracle AVDF versions 20.7 to 20.12.

4.13.2.2.1 About Auditing Operating System

Learn all about auditing of the operating system.

Audit Vault Sever enables default Oracle Linux audit configuration. The configuration settings are available in `/etc/audit/auditd.conf` file and the audit logs are recorded in `/var/log/audit directory`.

4.13.2.2.2 About Auditing Audit Vault Server Repository

Learn all about auditing of Audit Vault Server repository.

Prior to Oracle AVDF release 20.7, Audit Vault Server enables the default mixed mode auditing with the following settings:

```
audit_file_dest = /var/lib/oracle/admin/dbfwdb/adump
audit_sys_operations = TRUE
audit_trail = DB
```

> **Note:**
>
> The above default configuration prior to release 20.7 audits `SYS` operations and does not audit application level schemas `AVSYS` and `MANAGEMENT`.

Starting with Oracle AVDF release 20.7, pure unified auditing is automatically enabled with additional policies to audit application schemas `AVSYS` and `MANAGEMENT`.

With pure unified auditing enabled, the Audit Vault Server centralizes all auditing to a unified audit trail. For example, Database Vault audit records go to the unified audit trail. The Unifed Audit Policies are configured by default. This includes fresh installations and upgrades of Audit Vault Server to release 20.7.

With traditional auditing, operations by all administrative users (such as SYS and SYSDBA) are audited by default.

With unified auditing, if the database is not open, the top-level operations by all administrative users (such as SYS and SYSDBA) are audited. If the database is open, all secure configurations are audited (in new databases). To audit administrative users, create a unified audit policy, and then apply this policy to the users.

> **Note:**
>
> Your Oracle Database installation configuration might affect the auditing behavior. See the Oracle Database Security Guide for more details.

Table 4-2 Oracle Predefined Policies Configured for Audit Vault Server

Policy Name	Description
ORA_LOGON_FAILURES	Any failed log in events.

Table 4-2 (Cont.) Oracle Predefined Policies Configured for Audit Vault Server

Policy Name	Description
ORA_SECURECONFIG	Secure configuration defined by Oracle Database.
AVSYS_DV_UA_POLICY	Database Vault protected AVSYS realm. The Database Vault AVSYS realm protects all objects owned by the AVSYS database schema.
MANAGEMENT_DV_UA_POLICY	Database Vault protected MANAGEMENT realm. The Database Vault MANAGEMENT realm protects all objects owned by the MANAGEMENT database schema.
AUDIT_DB_MGMT_POLICY	Database management operations.
AUDIT_SELECT_DICTIONARY_POLICY	Select any dictionary privilege.

See Also:

- Logon Failures Predefined Unified Audit Policy
- Secure Options Predefined Unified Audit Policy

AVSYS_DV_UA_POLICY

CREATE AUDIT POLICY statement shows the AVSYS_DV_UA_POLICY unified audit policy definition as follows:

```
create audit policy AVSYS_DV_UA_POLICY actions component=dv
realm violation on "Audit Vault Realm",
realm success on "Audit Vault Realm",
realm access on "Audit Vault Realm",
rule set failure on "AVSYS audit command",
rule set success on "AVSYS audit command",
rule set eval on "AVSYS audit command"
```

Unified Audit Policy for Database Vault AVSYS Realm

AVSYS Database Vault realm protects all AVSYS objects including AVSYS tables, packages, and others. AVSYS_DV_UA_POLICY audits all activities on the Database Vault AVSYS realm.

The following commands are audited by Database Vault AVSYS realm:

- drop database link
- drop index
- drop package
- drop package body
- drop procedure
- drop sequence
- drop synonym

- drop table
- drop type
- drop type body
- drop view
- delete
- revoke
- truncate table

MANAGEMENT_DV_UA_POLICY

CREATE AUDIT POLICY statement shows the MANAGEMENT_DV_UA_POLICY unified audit policy definition as follows:

```
create audit policy MANAGEMENT_DV_UA_POLICY actions component=dv
realm violation on "Audit Vault Account Manager Realm",
realm success on "Audit Vault Account Manager Realm",
realm access on "Audit Vault Account Manager Realm",
rule set failure on "MANAGEMENT audit command",
rule set success on "MANAGEMENT audit command",
rule set eval on "MANAGEMENT audit command"
```

Unified Audit Policy for Database Vault MANAGEMENT Realm

Management Database Vault realm protects all the MANAGEMENT object, includes MANAGEMENT tables, packages, etc. MANAGEMENT_DV_UA_POLICY audits all activities on the Database Vault MANAGEMENT realm.

The following commands are audited by Database Vault MANAGEMENT realm:

- drop database link
- drop index
- drop package
- drop package body
- drop procedure
- drop sequence
- drop synonym
- drop table
- drop type
- drop type body
- drop view
- delete
- revoke
- truncate table

AUDIT_DB_MGMT_POLICY

`CREATE AUDIT POLICY` statement shows the `AUDIT_DB_MGMT_POLICY` unified audit policy definition and audits all users:

```
create audit policy audit_db_mgmt_policy
privileges
ALTER PUBLIC DATABASE LINK,
AUDIT ANY, AUDIT SYSTEM,
CREATE ANY TRIGGER, CREATE PUBLIC DATABASE LINK,
DROP ANY DIRECTORY, DROP PUBLIC DATABASE LINK
actions
ALTER FUNCTION, ALTER PACKAGE, ALTER PROCEDURE,
ALTER TRIGGER,
CREATE PACKAGE, CREATE PACKAGE BODY, CREATE PROCEDURE,
CREATE SPFILE, CREATE TRIGGER,
DROP FUNCTION, DROP PACKAGE, DROP PROCEDURE,
DROP TRIGGER;
```

AUDIT_SELECT_DICTIONARY_POLICY

`CREATE AUDIT POLICY` statement shows the `AUDIT_SELECT_DICTIONARY_POLICY` unified audit policy definition and audits all users except `AVSYS` and `MANAGEMENT`:

```
create audit policy audit_select_dictionary_policy
privileges
SELECT ANY DICTIONARY;
```

4.13.2.2.3 About Purging Unified Audit Trail on the Main Audit Vault Server

Learn how to configure a purge job for unified audit data pertaining to the main Audit Vault Server.

Unified audit trail data that is older than 7 days is purged by default. This is done as part of the `AVS_MAINTENANCE_JOB` that is scheduled to run daily by default. The schedule can be changed using the Audit Vault Server console.

> **See Also:**
>
> Schedule Maintenance Jobs

After configuring the unified audit trail collection in the shadow Audit Vault Server, it is recommended to configure a unified audit trail purge job in the main Audit Vault Server.

Follow these steps to configure unified audit trail purge job:

1. Log in to the Audit Vault Server as *root* OS user.
2. Run the command to switch to *oracle* user:

   ```
   su - oracle
   ```

3. Start *SQL*Plus* connection as `sqlplus /nolog` without the username or password.
4. In *SQL*Plus* run the following command:

   ```
   connect <sysdba>
   ```

   Enter the password when prompted. Alternatively, run the command:

   ```
   connect <sysdba/password>
   ```

5. Run the following SQL script to create a purge job with the job name `AVS_UNIFIED_AUDIT_CLEANUP` for Unified Audit Trail:

   ```
   begin
         dbms_audit_mgmt.create_purge_job(
           audit_trail_type => dbms_audit_mgmt.audit_trail_unified,
           audit_trail_purge_interval => 1,
           audit_trail_purge_name => 'AVS_UNIFIED_AUDIT_CLEANUP',
           use_last_arch_timestamp => true,
           container => dbms_audit_mgmt.container_current);
     end;
   ```

   This job runs once every hour to clean up the unified audit trail based on the archived timestamp updated by the shadow Audit Vault Server trail collection.

> **Best Practice:**
>
> It is recommended to configure unified audit trail purge job when configuring trails on the shadow Audit Vault Server, to collect data from the main Audit Vault Server.

> **Note:**
>
> When you configure unified audit trail purge job, the cleanup performed as part of `AVS_MAINTENANCE_JOB` is automatically removed and the following message is displayed in the **Job Status** page:
>
> ```
> Audit Trail cleanup for Audit Vault Server is enabled, so not
> purging audit data by Maintenance
> ```

> **Note:**
>
> To check the status of `AVS_UNIFIED_AUDIT_CLEANUP`, run the following SQL statement:
>
> ```
> select * from dba_scheduler_job_run_details where
> job_name='AVS_UNIFIED_AUDIT_CLEANUP';
> ```
>
> Refer to Audit Trail Management Data Dictionary Views for more information.

4.13.2.2.4 Storage Requirement for Main Audit Vault Server

Learn about the storage requirement for the main Audit Vault Server when auditing is enabled.

For every 1 million audit records and network events collected, the Audit Vault Server generates 3 GB of audit records as part of self auditing. The administrator must complete the sizing exercise to account for this space usage as per the deployment.

For a fresh installation of Audit Vault Server, refer to Audit Vault Sizing Guide. For an upgrade of Audit Vault Server from an older version, follow these guidelines:

1. Collect the data on the number of records (in million) generated by the Audit Vault Server for a duration of 8 days. Take this as `X`. For example, if 2 million records are generated per day, then `X is 2 * 8 = 16`.
2. Now calculate the space required (`Y`) for Audit Vault Server self auditing. This includes `SYSTEMDATA` and `EVENTDATA`. For every million records the space required is 3 GB.

   `Y = X multiplied by 3 GB`

The administrator needs to allocate `Y` GB of space in `SYSTEMDATA` and `EVENTDATA` disk groups. For example, if the system is processing 2 million audit records per day, then it requires 48 GB storage space in both `SYSTEMDATA` and `EVENTDATA` for auditing Audit Vault Server. (`2 million records * 8 days * 3 GB = 48 GB`).

```
X = 2 * 8 = 16
Y = 16 * 3 GB = 48 GB
```

For auditing of Audit Vault Server to process about 2 million audit records per day, the *administrator* must allocate 48 GB space in `SYSTEMDATA` and `EVENTDATA`.

4.13.2.2.5 Collecting Audit Records to Shadow Audit Vault Server

Learn how to collect audit records to the shadow Audit Vault Server.

You can configure a shadow Audit Vault Server to monitor the audit trails of the main Audit Vault Server. For example, if someone logs in to the main Audit Vault Server and drops an `AVSYS` package, the activity is audited, and the trail is collected in the shadow Audit Vault Server for reporting and analysis. The audit records are found in the activity reports that an *auditor* can access in the Audit Vault Server console. For example, **All Activity** report.

When you configure a shadow Audit Vault Server, you should configure collection from both unified and OS audit trails.

Configuring these trails involves the following steps:

1. Deploying Audit Vault Agent on the main Audit Vault Server
2. Adding a trail on the shadow Audit Vault Server to collect data from unified audit trail in the main Audit Vault Server
3. Adding a trail on the shadow Audit Vault Server to collect data from operating system audit trail in the main Audit Vault Server

4.13.2.2.6 Deploying the Audit Vault Agent on the Main Audit Vault Server

Learn how to deploy Audit Vault Agent on the main Audit Vault Server.

A shadow Audit Vault Server can be configured to monitor the audit trail of the main Audit Vault Server. To accomplish this an Audit Vault Agent must be deployed on the main Audit Vault Server.

Follow these steps:

1. Log in to the shadow Audit Vault Server as an *administrator*.
2. Register the main Audit Vault Server in the **Agents** tab.
3. Log in to the main Audit Vault Server as *root* user.
4. Run the following commands to create a `/var/lib/oracle/avs_agent` directory in the main Audit Vault Server:

```
cd /var/lib/oracle


mkdir avs_agent


chown avsagent:osaudit avs_agent
```

5. Run the `sudo -u avsagent /bin/bash` command to create a bash shell for the *avsagent* OS user.

> **Note:**
>
> There is no log in the shell defined for the *avsagent* OS user. To run the command as *avsagent* user, log in as *root* user. It can either be done by running the command `sudo -u avsagent /bin/bash` and use the created bash shell to run the command as *avsagent* user, or by running the command `sudu -u avsagent <command>`.

6. Log in to the shadow Audit Vault Server console as an *administrator*.
7. Click the **Agents** tab, and then click **Downloads**.
8. Download the `agent.jar` file to `/var/lib/oracle/avs_agent` directory and copy it to the main Audit Vault Server as *avsagent* OS user.
9. Add a line `export PATH=/var/lib/oracle/avs_agent/bin:$PATH` in the `/home/avsagent/.bashrc`. This ensures the future bash shell created by `sudo -u avsagent /bin/bash` has the `PATH` to access the `agentctl`.

10. Deploy the Audit Vault Agent in the main Audit Vault Server as *avsagent* OS user in the shell created earlier.

    Make sure `/var/lib/oracle/avs_agent/bin` is in the `PATH`. Or run `export PATH=/var/lib/oracle/avs_agent/bin:$PATH`.

11. Running the following command:

    ```
    java -jar /var/lib/oracle/avs_agent/agent.jar
    ```

12. Running the following command to start the Agent as *avsagent* OS user:

    ```
    agentctl start -k
    ```

13. Enter the activation key when prompted. The activation key is available in the **Agents** tab of the shadow Audit Vault Server. Ensure to enter the complete activation key including the name of the Agent.

4.13.2.2.7 Adding a Trail to Collect Data From Unified Audit Trail on the Main Audit Vault Server

Learn how to add a trail to collect data from unified audit trail on the main Audit Vault Server as an Oracle Database target.

This involves two steps on a high level:

1. Registering the main Audit Vault Server as an Oracle Database target.
2. Configuring the trail to collect data from the unified audit trail on the main Audit Vault Server.

4.13.2.2.7.1 Registering the Main Audit Vault Server as an Oracle Database Target

Learn how to register the main Audit Vault Server as an Oracle Database target.

1. Log in to the main Audit Vault Server as *dvaccountmgr*.
2. Update the password of *AVSAUDIT* user and unlock the account.
3. Start *SQL*Plus* connection as `sqlplus /nolog` without the username or password.
4. In *SQL*Plus* run the following command:

    ```
    connect <sysdba>
    ```

    Alternatively, run the command:

    ```
    connect <sysdba/password>
    ```

5. Enter the password when prompted.
6. Run the following command:

    ```
    @oracle_user_setup.sql AVSAUDIT setup
    ```

    The `oracle_user_setup.sql` is located at `/var/lib/oracle/avs_agent/av/plugins/com.oracle.av.plugin.oracle/config`.

7. Log in as *dvowner*.

8. Start *SQL*Plus* and run the following command:

```
GRANT DV_MONITOR TO "AVSAUDIT"
```

9. Log in to the shadow Audit Vault Server as *administrator*.
10. Create an archive location and define the archiving policy for the main Audit Vault Server target. It is recommended to create an archiving policy for 6 months online and 0 months archived.
11. Register the main Audit Vault Server as an Oracle Database target. During the target registration, select `6 months online, 0 months` as the retention policy. Use `AVSAUDIT` in the **Database User Name** field. Enter `AVSAUDIT` password in the **Password** field.

4.13.2.2.7.2 Configuring Trail to Collect Data from Unified Audit Trail on the Main Audit Vault Server

Learn how to add an audit trail to collect data from the unified audit trail on the main Audit Vault Server as an Oracle Database target.

1. Log in to the shadow Audit Vault Server as *administrator*.
2. Add an audit trail for the main Audit Vault Server Oracle Database target.
3. Click **Targets** tab.
4. Identify and click the main Audit Vault Server Oracle Database target.
5. In the **Audit Data Collection** section, click **Add**.
6. Select the table for **Audit Trail Type** field.
7. Select `UNIFIED_AUDIT_TRAIL` in the **Trail Location** field.
8. Select the Audit Vault Agent deployed in the **Agent Host** field.
9. In the **Agent Plugin** field, select `com.oracle.av.plugin.oracle`.
10. Click **Save**.
11. The audit trail is started automatically.

4.13.2.2.8 Adding a Trail to Collect Data from OS Audit Trail on the Main Audit Vault Server

Learn how to add a trail to collect data from OS audit trail on the main Audit Vault Server as a Linux target.

This involves two steps on a high level:

1. Registering the main Audit Vault Server as a Linux target.
2. Configuring trail to collect data from OS audit trail on the main Audit Vault Server.

4.13.2.2.8.1 Registering the Main Audit Vault Server as a Linux Target

Learn how to register the main Audit Vault Server as a Linux target.

1. Log in to the shadow Audit Vault Server as an *administrator*.
2. Click **Targets** tab, and then click **Register**.
3. Select `Linux` in the **Type** field.
4. Select `6 months online and 0 months` as the **Retention Policy**.

5. Enter the **Host Name** of the main Audit Vault Server if DNS is configured.
6. Enter the IP address of the main Audit Vault Server.
7. Click **Save**.

4.13.2.2.8.2 Configuring a Trail to Collect Data from OS Audit Trail on the Main Audit Vault Server

Learn how to add an audit trail for unified auditing for the main Audit Vault Server as a Linux target.

1. Log in to the shadow Audit Vault Server as *administrator*.
2. Add an audit trail for the main Audit Vault Server as Linux target.
3. Click **Targets** tab.
4. Identify and click the main Audit Vault Server Linux target.
5. In the **Audit Data Collection** section, click **Add**.
6. Select `DIRECTORY` in the **Audit Trail Type** field.
7. In the **Trail Location** field, enter `/var/log/audit/audit*.log`.
8. Select the Audit Vault Agent deployed in **Agent Host** field. This is the Agent that was earlier deployed in the main Audit Vault Server.
9. In the **Agent Plugin** field, select `com.oracle.av.plugin.linuxos`.
10. Click **Save**.
11. The audit trail is started automatically.

> **Best Practice:**
>
> - It is recommended to configure a shadow Audit Vault Server to collect unified audit data and OS audit data from the main Audit Vault Server.
> - The shadow Audit Vault Server must be highly restricted to capturing audit data from only the main Audit Vault Server.
> - It is recommended not to provision or modify the audit policies through the shadow Audit Vault Server for the main Audit Vault Server without careful consideration. Increased auditing of the main Audit Vault Server impacts the performance.

4.13.2.2.9 Creating an Alert Policy to Monitor `AVREPORTUSER`, `AVSAUDIT`, and `ORDS_PUBLIC_USER` Users

Oracle recommends creating an alert policy with email notifications to monitor the `AVREPORTUSER`, `AVSAUDIT`, and `ORDS_PUBLIC_USER` users.

Create an alert policy with email notification with the following condition:

```
upper(:EVENT_STATUS)='FAILURE' and upper(:EVENT)='LOGON' and
(upper(:USER)='AVREPORTUSER' or upper(:USER)='AVSAUDIT' or
upper(:USER)='ORDS_PUBLIC_USER')
```

For more information see, Creating Alerts and Writing Alert Conditions in the *Oracle Audit Vault and Database Firewall Auditor's Guide*.

If you receive an alert you should check the event details and take action to prevent further login attempts for the `AVREPORTUSER`, `AVSAUDIT`, and `ORDS_PUBLIC_USER` users.

5
Configuring Database Firewall

Learn about configuring Database Firewall.

You can use Database Firewall to configure traffic sources and proxies.

5.1 About Configuring Database Firewall

Learn how to configure Database Firewall.

The way in which you configure the system and firewall settings for each Database Firewall depends on your overall plan for deploying Oracle Audit Vault and Database Firewall.

When you configure a Firewall instance, you identify the Audit Vault Server that will manage the specific Firewall. Depending on your plan for the overall Oracle Audit Vault and Database Firewall system configuration, you also configure the traffic sources, and determine the deployment types. The following are the Database Firewall deployment types:

- Monitoring (Out-of-Band)
- Monitoring (Host Monitor)
- Monitoring / Blocking (Proxy)

> **Note:**
>
> - 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.
> - The Database Firewall introduces very minimal latency overhead of less than 100 microseconds per SQL statement with 100K transactions per second. This is based on internal performance tests.
> - Traffic transfers from the Database Firewall to the Audit Vault Server as quickly as possible given the available resources and design limits. There's always a small gap between the moment that an audit record is recorded in the target database and when it is stored on the Audit Vault Server.

Basic firewall configuration consists of these four steps:

1. Specifying the Audit Vault Server Certificate and IP Address
2. Managing the Oracle Database Firewall Network and Services Configuration
3. Setting the Date and Time in Database Firewall
4. Configuring the Database Firewall and Its Traffic Sources on Your Network

After configuring the Database Firewalls, perform the following tasks:

- Configure Database Firewall monitoring points for each database target.

- You can optionally set up resilient pairs of Database Firewalls for a high availability environment.

> **See Also:**
>
> - Summary of Configuration Steps to understand the high level workflow for configuring the Oracle Audit Vault and Database Firewall system.
> - Planning Your Oracle Audit Vault and Database Firewall System Configuration for an overview of the planning steps.
> - Configuring Database Firewall Monitoring Points
> - High Availability in Oracle AVDF to set up resilient pairs of Database Firewalls for a high availability.

5.2 Introduction to Database Firewall Deployment

Depending on your operational needs you can monitor SQL traffic only, or you can monitor and block SQL traffic to the target database.

When configuring the Database Firewall, you can choose one of the following deployment modes:

Deployment Mode	Minimum Number of Network Interface Cards (NICs)	Operational Notes
Monitoring/Blocking (Proxy)	3 (for deployment with network separation) 1 (for deployment without network separation)	This mode enables the Database Firewall to both monitor and block SQL traffic, as well as optionally substitute SQL statements. You configure clients to connect to the Database Firewall instead of the database so that the firewall can intercept all SQL traffic and take the necessary actions, based on policies that you define.
Monitoring (Host Monitor)	1	To use this mode, you install the Audit Vault Agent and Host Monitor Agent on the host machine that's running the target database. The Host Monitor Agent captures traffic from the NIC on the host machine and securely forwards it to the Database Firewall.
Monitoring (Out-of-Band)	2	In this mode, the Database Firewall monitors and alerts on SQL traffic, but it can't block or substitute SQL statements. To copy database traffic to the Database Firewall, you can use a switch with a SPAN port (as shown in the diagram), a network tap, a packet replicator, or other similar technology.

One Database Firewall can monitor traffic from multiple targets deployed in different modes. For example, one Database Firewall can be deployed in Monitoring/Blocking (Proxy) mode for

some targets and in Monitoring (Host Monitor) mode and Monitoring (Out-of-Band) mode for other targets.

> **Note:**
>
> - A single NIC is required when the client and database are on the same subnet. There is no network separation.
> - Additional NICs are required when the client and database are on different subnets.
> - When there are three NICs, the network separation requires you to have a management network interface, which is usually attached to the default gateway. The first NIC is placed in the client subnet. The second NIC is placed in the database subnet. No additional routing is required in this configuration. All the addresses for clients and databases are local to the networks that are accessible to the Database Firewall NICs.

5.2.1 Monitoring/Blocking (Proxy)

Monitoring/Blocking (Proxy) mode enables the Database Firewall to both monitor and block SQL traffic, as well as optionally substitute SQL statements.

You configure clients to connect to the Database Firewall instead of the database so that the firewall can intercept all SQL traffic and take the necessary actions, based on policies that you define. In all cases, the database server identifies the Database Firewall as the client.

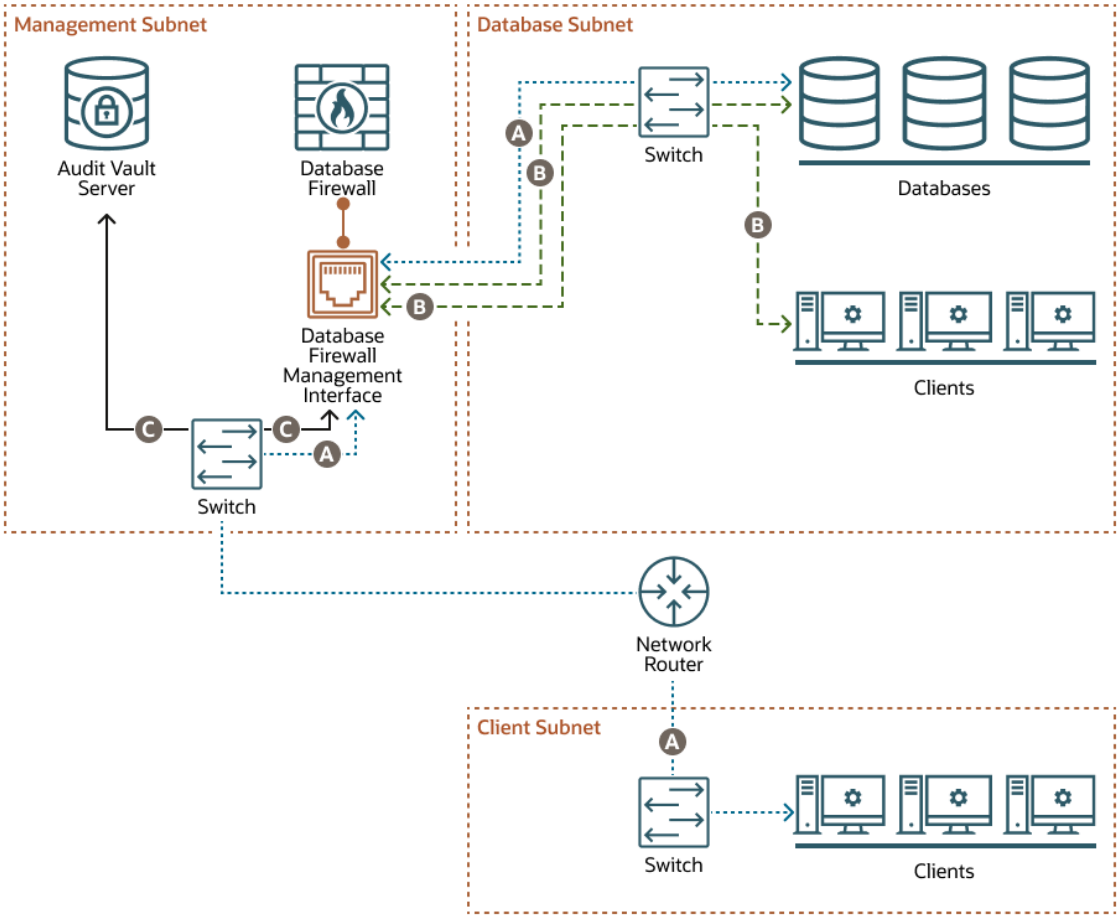
Oracle recommends that you configure the database to reject all connections that do not come from the Database Firewall.

> **Note:**
>
> To simplify the modification required for applications to connect to the Database Firewall proxy mode deployments, configure local domain name servers (DNS) to resolve the fully-qualified domain name (FQDN) of the target database to the IP address of the Database Firewall.

You can deploy the **Monitoring/Blocking (Proxy)** mode in the following ways:

- Proxy without network separation
- Proxy without network separation using a dedicated network interface card (NIC)
- Proxy with network separation

Proxy Without Network Separation



When you deploy the Database Firewall as a proxy without network separation, the Database Firewall has one NIC called the Database Firewall management interface, which handles all communication between the clients and databases, as well as between the Database Firewall and the Audit Vault Server. This NIC is deployed in the management subnet.

The example in this diagram has three subnets:

- The management subnet contains the Audit Vault Server, the Database Firewall, the Database Firewall management interface, and a switch.
- The client subnet contains three clients and a switch.
- The database subnet contains three databases, three clients, and a switch.

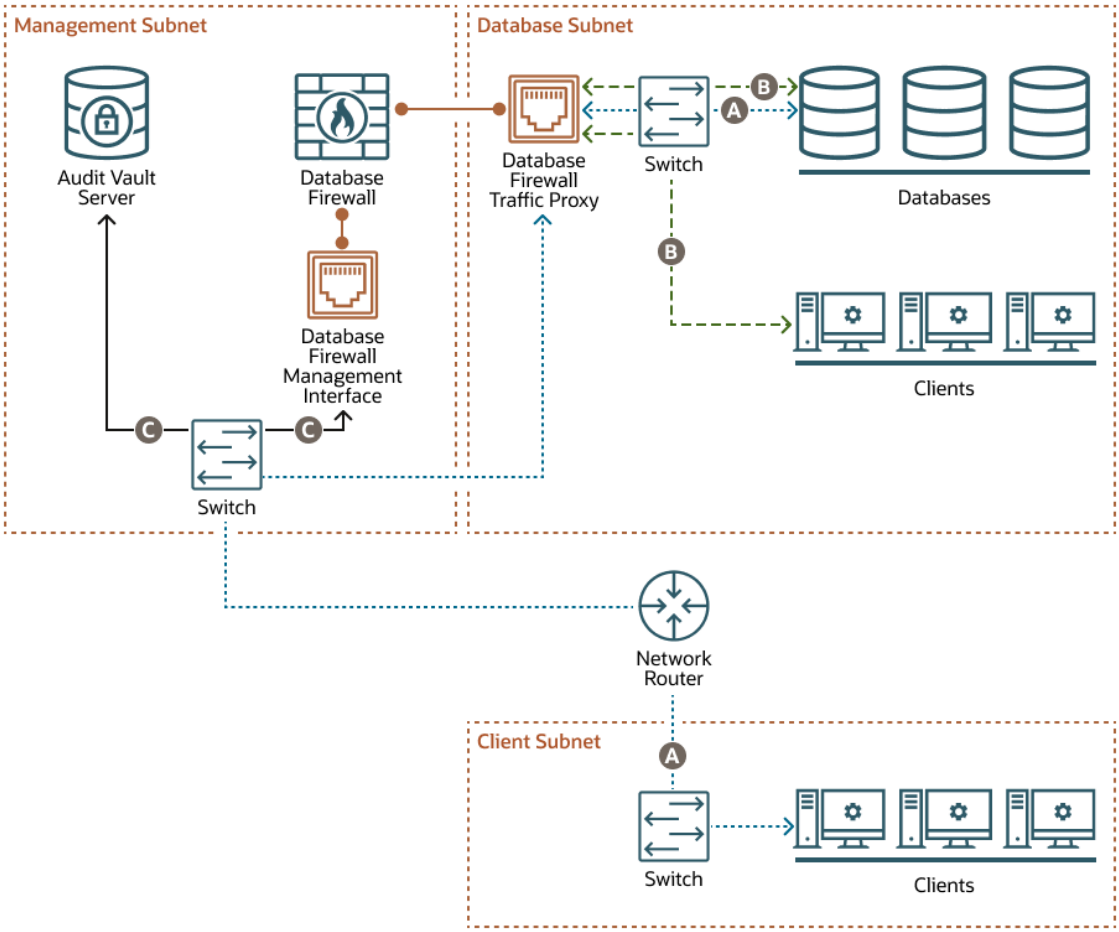
The following letter callouts describe how traffic flows to and from the Database Firewall in the diagram:

- A: In the client subnet, traffic travels from the clients through a switch to the network router. The router sends the traffic to the switch in the management subnet, which forwards the traffic to the Database Firewall traffic management interface. From there the traffic travels to the databases through the switch in the database subnet. The database responses return to the clients through the same path.
- B: In the database subnet, traffic travels from the clients through the switch in the database subnet to the Database Firewall traffic management interface in the management subnet.

From there the traffic travels to the databases through the switch in the database subnet. The database responses return to the clients through the same path.

- C: The Database Firewall extracts and analyzes SQL data from the client traffic and sends it through the Database Firewall management interface to the switch in the management subnet and then to the Audit Vault Server, based on the Database Firewall policy.

Proxy Without Network Separation Using a Dedicated NIC for the Proxy Service



When you deploy the Database Firewall as a proxy without network separation using a dedicated NIC, the Database Firewall has two NICs:

- The Database Firewall traffic proxy handles traffic from all clients to the databases. This NIC is deployed in the database subnet.
- The Database Firewall management interface handles communication between the Database Firewall and the Audit Vault Server. This NIC is deployed in the management subnet.

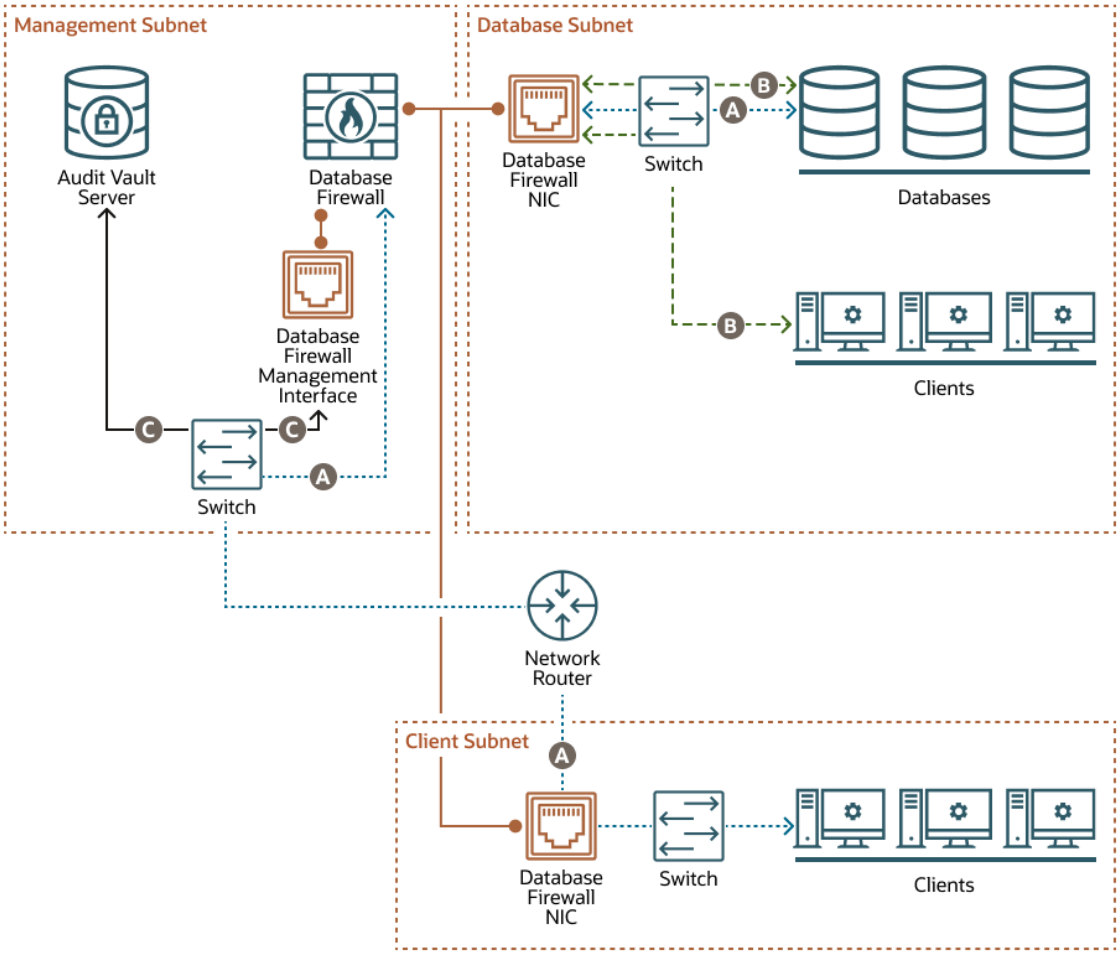
The example in this diagram has three subnets:

- The management subnet contains the Audit Vault Server, the Database Firewall, the Database Firewall management interface, and a switch.
- The client subnet contains three clients and a switch.
- The database subnet contains three databases, three clients, a switch, and the Database Firewall traffic proxy.

The following letter callouts describe how traffic flows to and from the Database Firewall in the diagram:

- A: In the client subnet, traffic travels from the clients through a switch to the network router. The router sends the traffic to the switch in the management subnet, which forwards the traffic to the Database Firewall traffic proxy in the database subnet. From there the traffic travels to the databases through the switch in the database subnet. The database responses return to the clients through the same path.
- B: In the database subnet, traffic travels from the clients through the switch in the database subnet to the Database Firewall traffic proxy in the database subnet. From there the traffic travels to the databases through the switch in the database subnet. The database responses return to the clients through the same path.
- C: The Database Firewall extracts and analyzes SQL data from the client traffic and sends it through the Database Firewall management interface to the switch in the management subnet and then to the Audit Vault Server, based on the Database Firewall policy.

Proxy With Network Separation



When you deploy the Database Firewall as a proxy with network separation, the Database Firewall has a minumum of three NICs:

- Each client subnet has a Database Firewall NIC that handles all traffic to and from the clients in that subnet.

- The database subnet has a Database Firewall NIC that handles all traffic to the databases, as well as traffic from any clients in the database subnet.
- The Database Firewall management interface handles communication between the Database Firewall and the Audit Vault Server. This NIC is deployed in the management subnet.

The example in this diagram has three subnets:

- The management subnet contains the Audit Vault Server, the Database Firewall, the Database Firewall management interface, and a switch.
- The client subnet contains three clients, a switch, and a Database Firewall NIC.
- The database subnet contains three databases, three clients, a switch, and a Database Firewall NIC.

The following letter callouts describe how traffic flows to and from the Database Firewall in the diagram:

- A: In the client subnet, traffic travels from the clients through a switch to the Database Firewall NIC in the client subnet and then to the network router. The router sends the traffic to the switch in the management subnet, which forwards the traffic to the Database Firewall. From there the traffic travels to the databases through the NIC and switch in the database subnet. The database responses return to the clients through the same path.
- B: In the database subnet, traffic travels from the clients through the switch in the database subnet to the Database Firewall NIC in the database subnet. From there the traffic travels to the databases through the switch in the database subnet. The database responses return to the clients through the same path.
- C: The Database Firewall extracts and analyzes SQL data from the client traffic and sends it through the Database Firewall management interface to the switch in the management subnet and then to the Audit Vault Server, based on the Database Firewall policy.

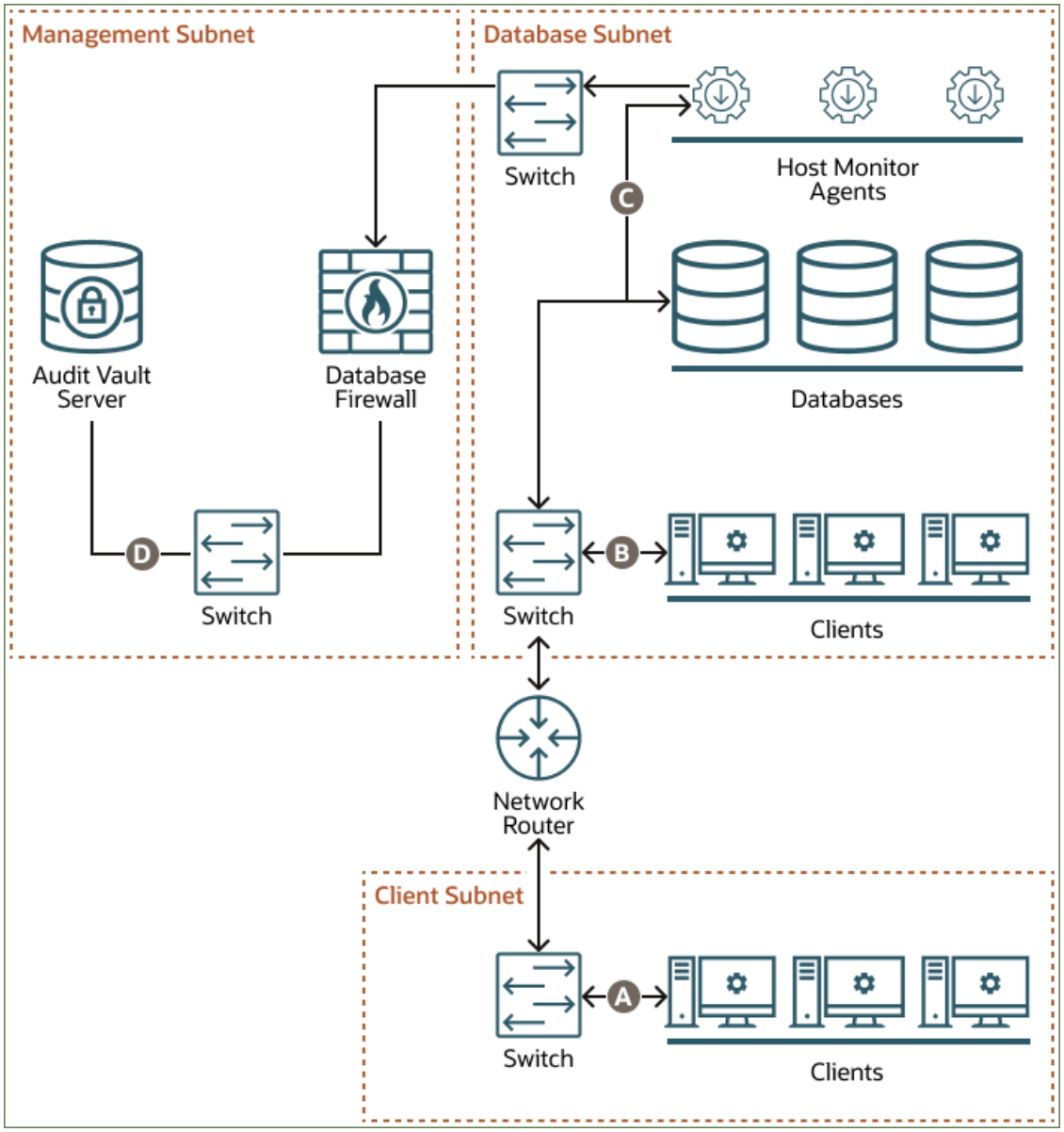
5.2.2 Monitoring (Host Monitor)

In **Monitoring (Host Monitor)** mode, the Database Firewall monitors and alerts on SQL traffic, but it can't block or substitute SQL statements.

To use **Monitoring (Host Monitor)** mode, you install the Audit Vault Agent and Host Monitor Agent on the host machine that's running the target database. The Host Monitor Agent captures traffic from the network interface card (NIC) on the host machine and securely forwards it to the Database Firewall.

> **Note:**
>
> In Oracle AVDF 20.3 and later, you can add any NIC (with an IP address configured) on the Database Firewall to the monitoring point. See Creating a Monitoring Point for the Host Monitor Agent.

Monitoring (Host Monitor) mode is helpful if the network topology prevents deployment of other Database Firewall modes. Host monitoring captures only the relevant traffic, whereas **Monitoring (Out-of-Band)** mode captures all the network traffic. **Monitoring (Host Monitor)** mode can monitor SQL traffic using the Host Monitor Agent deployed on the database server when there are multiple network paths from clients to the database host.



The example in the diagram has three subnets: client, database, and management. The client subnet contains three clients that connect to the network router through a switch in the client subnet. The database subnet contains three databases and three Host Monitor Agents. The Host Monitor Agents connect to the Database Firewall through a switch in the database subnet. The database subnet also contains three clients that connect to a second switch in the database subnet. That switch connects to the databases and to the network router. The management subnet contains the Database Firewall and the Audit Vault Server, which connect to each other through a switch in the management subnet.

The following points refer to the letter callouts in the diagram:

- A: The clients in the client subnet connect directly to the database through the network router and a switch in the database subnet.
- B: The clients in the database subnet connect directly to the database through the switch in the database subnet.

- C: The Host Monitor Agents record traffic between the clients and the databases and forward the traffic to the Database Firewall through a switch in the database subnet.
- D: The Database Firewall extracts and analyzes SQL data from the client traffic and sends it through the switch in the management subnet to the Audit Vault Server, based on the Database Firewall policy.

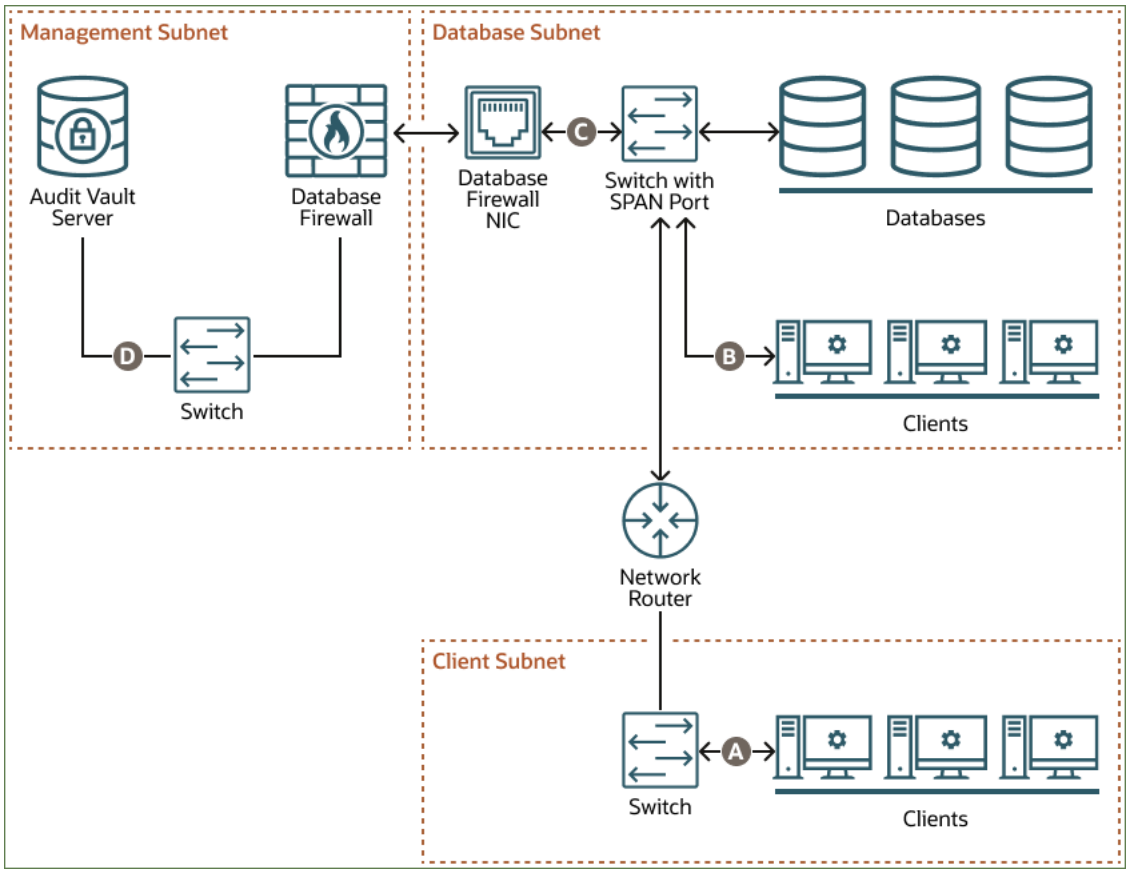
5.2.3 Monitoring (Out-of-Band)

In **Monitoring (Out-of-Band)** mode, the Database Firewall monitors and alerts on SQL traffic, but it can't block or substitute SQL statements.

You can use several technologies to copy database traffic to the Database Firewall, including (but not limited to) SPAN ports, network taps, and packet replicators.

Monitoring (Out-of-Band) mode is the simplest deployment mode overall for a non-blocking policy requirement. There is no additional load on the database or the clients. The Database Firewall does not introduce any latency or a single point of failure.

Oracle Audit Vault and Database Firewall (Oracle AVDF) supports high availability in this deployment mode.



The example in the diagram has three subnets: client, database, and management. The client subnet contains three clients that connect to the network router through a switch in the client subnet. The database subnet contains three databases that connect directly to the Database Firewall through a switch with a SPAN port and then a Database Firewall NIC in the database subnet. The database subnet also contains three clients that, along with the network router, connect to the same switch with a SPAN port. The management subnet contains the Database

Firewall and the Audit Vault Server, which connect to each other through a switch in the management subnet.

The following points refer to the letter callouts in the diagram:

- A: The clients in the client subnet connect directly to the database through the network router and the switch with the SPAN port in the database subnet.
- B: The clients in the database subnet connect directly to the database through the switch with the SPAN port in the database subnet.
- C: The Database Firewall monitors database activity through the Database Firewall NIC, which connects to a SPAN port on the switch in the database subnet.
- D: The Database Firewall extracts and analyzes SQL data from the client traffic and sends it through the switch in the management subnet to the Audit Vault Server, based on the Database Firewall policy.

5.3 Specifying the Audit Vault Server Certificate and IP Address

You associate each Database Firewall with an Audit Vault Server so that the Audit Vault Server can manage the firewall. If you're using a resilient pair of Audit Vault Servers for high availability, then you associate the firewall with both servers.

> **Note:**
>
> - Complete the Database Firewall Post-Install Tasks before beginning this procedure.
> - Complete this procedure before you register the firewall on the Audit Vault Server. See Registering Database Firewall in Audit Vault Server for instructions.

1. Log in to the Audit Vault Server console as an *administrator*.
2. Find and copy the Audit Vault Server certificate and IP address.

   For standalone Audit Vault Servers or primary Audit Vault Servers in a high availability environment:

   a. Click the **Settings** tab.
   b. Click **Security** in the left navigation menu.
   c. Click the **Certificate** tab on the main page, and then click **Server Certificate**.
   d. Copy the certificate.

   For standby Audit Vault Servers in a high availability environment:

   a. Click the **Settings** tab.
   b. Click **System** in the left navigation menu.
   c. In the **Configuration** section, click **High Availability**.
   d. Copy the standby server certificate and IP address.
3. Log in to the Database Firewall through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

4. Copy the server certificate of the Audit Vault Server into a file on the Database Firewall server.
5. Run the following commands to associate the primary or standby Audit Vault Server with the Database Firewall:

Task	Command
Display the Audit Vault Servers that are paired with the Database Firewall	`/opt/avdf/config-utils/bin/config-avs show`
Add or update the primary Audit Vault Server for the Database Firewall	`/opt/avdf/config-utils/bin/config-avs set avs=primary address=<Ip address of the primary AVS> certificate=<Path of the certificate>`
Add or update the standby Audit Vault Server for the Database Firewall	`/opt/avdf/config-utils/bin/config-avs set avs=secondary address=<Ip address of the standby AVS> certificate=<Path of the certificate>`

6. Run the following command to synchronize the system clocks of the Database Firewall server and the Audit Vault Server.

```
/opt/avdf/config-utils/bin/config-ntp set servers=<Comma separated IP
addresses or hostnames of NTP servers> sync_on_save=true enabled=true
```

See CONFIG-NTP for more information about this command.

> **Note:**
>
> To perform the same procedure by using the Audit Vault Server console, seeSetting the Date and Time in Database Firewall.

To remove the primary or standby Audit Vault Server from the Database Firewall, use the following commands.

Task	Command
Remove the primary Audit Vault Server from the Database Firewall	`/opt/avdf/config-utils/bin/config-avs delete avs=primary`

Task	Command
Remove the standby Audit Vault Server from the Database Firewall	`/opt/avdf/config-utils/bin/config-avs delete avs=secondary`

5.4 Managing the Oracle Database Firewall Network and Services Configuration

Learn how to manage the Oracle Database Firewall network and services configuration.

5.4.1 Configuring Network Settings for Oracle Database Firewall

Learn how to configure the network settings for Oracle Database Firewall.

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 Audit Vault Server console as administrator.
2. Click the **Database Firewalls** tab.
3. Click the specific Database Firewall instance for which the network settings needs to be configured or changed.
4. Click **Network Settings** link under the **Configuration** section in the main page.
5. Starting in Oracle AVDF 20.12, if the **Synchronize NICs** button is disabled, proceed to the next step. If the **Synchronize NICs** is active, click it, as the AVS detects NIC name changes in the Database Firewall which must be synchronized.
   a. Select a NIC name on the Database Firewall for all the devices. If a device is no longer available on the Database Firewall and is no longer required on the AVS, select **not required**.
   b. After mapping each device, select **Save**.
6. In the **Network Settings** dialog, click the specific network interface.
7. In the **Network Interface Settings** dialog, complete the following fields as necessary:
   - **IP Address**: The IP address of the network interface. 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.

     The network interface which has the same IP address as that of Database Firewall is the Management Interface. If the IP address of the Management Interface is changed, then the IP address of the Database Firewall is also changed. After changing the IP address of the Management Interface, in the **Network Interface Settings** dialog, then change the IP address on the Database Firewall details page.
   - **Network Mask**: The subnet mask of the Database Firewall. If you want to use a different network mask, then you can change it here.
   - **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. This is optional.

8. Click **Save**.

> **Note:**
>
> The following error may be encountered while changing the IP address of the Management Interface. This can be ignored and no action required.
>
> `Operation failed OAV-46981: Unable to connect to Database Firewall with IP`

5.4.2 Configuring Network Services for Oracle Database Firewall

Learn about configuring network services for Oracle Database Firewall.

The network services configuration determines how administrators can access Oracle Database Firewall. See the guidelines to protect data and ensure that you take the appropriate security measures when configuring network services.

To configure network services for a Database Firewall:

1. Click **Database Firewalls** tab in the Audit Vault Server console.
2. In the left navigation menu, click **Database Firewalls**.
3. Click on the specific Database Firewall instance.
4. Under **Configuration** tab, click on **System Services**.
5. In the **System Services** dialog, the following options are available:
   - DNS: If you require host names to be translated, then enter the IP address of at least one DNS server on the network. Turn on the button and enter IP addresses for up to three DNS servers (`DNS Server 1`, `DNS Server 2`, and `DNS Server 3`). Keep the button turned off if there is no DNS server. Otherwise, your system's performance may be impaired.

     If you want to use DNS, then ensure that the servers are reliable. If the DNS servers are unavailable, then many services on the Database Firewall do not work. For example, the Database Firewall may pass traffic that it would otherwise block.
   - SSH/SNMP: If you want to allow selected computers to have secure shell access to the Database Firewall, then turn on the button for **SSH Access**. You can select **All** to allow unrestricted access or click on **IP Addresses** and enter their IP addresses separated by space or comma.

     SSH setting can also be configured using command line interface. Use these commands for the same.

Task	Command
To display the current settings of SSH	`/opt/avdf/config-utils/bin/config-ssh show`
To allow unrestricted access from all systems	`/opt/avdf/config-utils/bin/config-ssh set access=all`
To block SSH access from all systems	`/opt/avdf/config-utils/bin/config-ssh set access=disabled`

Task	Command
To allow a selected computer to have secure shell access to the Database Firewall	`/opt/avdf/config-utils/bin/config-ssh set access=192.0.2.11`
To allow a multiple computers to have secure shell access to the Database Firewall	`/opt/avdf/config-utils/bin/config-ssh set access='192.0.2.11 192.0.2.12'`

- SNMP Access: If you want to enable access to the network configuration of the Database Firewall through SNMP, then turn on the button for **SNMP Access**. You can select **All** to allow unrestricted access or click on IP Addresses and enter their IP addresses separated by space or comma.

6. Click **Save**.

> **See Also:**
>
> Protecting Your Data

5.4.3 Configuring SNMPv3 Users in Oracle Audit Vault and Database Firewall

Learn how to configure SNMPv3 users.

Simple Network Management Protocol version 3 (SNMPv3) is an interoperable, standards-based protocol. SNMPv3 involves User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. With USM, messages exchanged between the SNMP Manager and the SNMP Agent can have data integrity checking and data origin authentication. Oracle Audit Vault and Database Firewall 20.1 and later supports SNMPv3 as the default version. This topic contains the steps needed to configure SNMPv3 users for making use of the USM model of SNMPv3.

To create an SNMPv3 user, follow these steps:

1. Log in to the Audit Vault Server or Database Firewall instance as *root* user.
2. Run the following command to turn off the `snmpd` service:

   ```
   systemctl stop snmpd
   ```

3. Run the following command to create a new SNMP user:

   ```
   net-snmp-create-v3-user
   ```

4. Enter the user name and password (or passphrase) following the prompt.
5. Enter the encryption passphrase following the prompt. If you want to use the same passphrase for encryption, then press the **Enter** key to continue.
6. The following output confirms the user creation.

   ```
   adding the following line to /var/lib/net-snmp/snmpd.conf:
   createUser <user name> SHA <password> AES <encryption password>
   adding the following line to /etc/snmp/snmpd.conf:
   ```

```
rwuser <user name>
```

> **Note:**
>
> The new user created has read and write access by default. This can be modified to read only privileges. This can be done by modifying the file available at `/etc/snmp/snmpd.conf`:
>
> ```
> rouser <user name>
> ```
>
> In the configuration file, find the line or entry where `rwuser <user name>` is mentioned. Change the entry to `rouser <user name>` for read only access.

7. After the user is created, you can assign the user to an existing group. Or you can create a new group and assign the user.
   a. Follow this step to assign the newly created user to an existing group. In Oracle Audit Vault and Database Firewall, the default group name is `notConfigGroup`. Edit the `/etc/snmp/snmpd.conf` file and include the following line in the group creation table. Ensure the user name of the new user is under the **UserName** column.

      ```
      #      groupName      securityModel  userName
      group notConfigGroup      usm          <user name>
      ```

      Example of adding the user to a predefined group:

      ```
      #      groupName      securityModel  userName
      group notConfigGroup      usm          myUser
      ```

   b. Follow this step to assign the newly created user to a new group.

      ```
      #      groupName      securityModel  userName
      group <new group name>      usm          <user name>
      ```

      Example of adding the user to a new group:

      ```
      #      groupName      securityModel  userName
      group newGroup      usm          myUser
      ```

8. Run the following command to start the `snmpd` service:

   ```
   systemctl start snmpd
   ```

9. Run the following command to test and confirm that the SNMPv3 user is created and assigned to the group:

> **Note:**
>
> Install the `net-snmp-utils` package to run the following `snmpwalk` command. It is not installed as part of Audit Vault Server or Database Firewall installation by default. Other standard SNMP querying tools can also be used.
>
> ```
> snmpwalk -v3 -u <user name> -a SHA -A "<authentication password>" -
> x AES -X "<privacy password>" -l authPriv <IP address of the
> system> <standard SNMP MIB>
> ```
>
> For example:
>
> ```
> snmpwalk -v3 -u myUser -a SHA -A "myAuthPassword" -x AES -X
> "myPrivacyPassword" -l authPriv 192.0.2.24 system
> ```

5.5 Setting the Date and Time in Database Firewall

Learn how to set the date and time in Database Firewall.

Use this procedure to set the Database Firewall date and time:

1. Log in to the Audit Vault Server console as administrator.
2. Click **Database Firewalls** tab in the Audit Vault Server console main page.
3. In the left navigation menu, click **Database Firewalls**.
4. Click on the specific Database Firewall instance.
5. Under **Configuration** tab, click **System Services**.
6. Click **Date and Time** tab.
7. In the **System Time** field, select the date and time in Coordinated Universal Time (UTC).
8. Optionally you can enable NTP synchronization. You can turn on the button against **NTP Server1** and enter the NTP server address in the field. You can add 1 and upto 3 NTP server addresses.

   It keeps the time synchronized with the average of the time recovered from the time servers specified in the **NTP Server1**, **NTP Server2**, and **NTP Server3** fields, which contain an IP address or a name. If you specify a name, then the DNS server specified in the **DNS** tab is used for name resolution.

   To enable time synchronization, you also must specify the IP address of the default gateway and a DNS server.

   > **WARNING:**
   >
   > In Monitoring / Blocking mode, changing the time causes all monitoring points to restart, dropping existing connections to protected databases. This causes a temporary disruption to traffic, and will happen when you choose to enter the time directly.

9. Click **Save**.

> **See Also:**
>
> Managing the Oracle Database Firewall Network and Services Configuration to specify the IP address of the default gateway and DNS server.

5.6 Changing the IP Address on a Single Instance of the Database Firewall Server

Learn how to change the IP address on a single instance of the Database Firewall server.

Prerequisites

- Because changing the IP address of the Database Firewall Server is a system-level change and requires downtime, plan to change the IP address during a safe period to avoid interrupting the log collection processing.
- Stop any monitoring points before changing the IP address. See Starting, Stopping, or Deleting Database Firewall Monitoring Points.

To change the IP address of the Database Firewall Server:

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

   Database Firewalls is selected in the left navigation menu by default.
3. Click the name of the Database Firewall instance.

> **Note:**
>
> In Oracle AVDF 20.1, don't change the IP address in the **IP Address** field here. Follow the remaining steps.

4. Click **Network Settings** under **Configuration**.
5. Starting in Oracle AVDF 20.12, if the **Synchronize NICs** button is disabled, proceed to the next step. If the **Synchronize NICs** is active, click it, as the AVS detects NIC name changes in the Database Firewall which must be synchronized.
   a. Select a NIC name on the Database Firewall for all the devices. If a device is no longer available on the Database Firewall and is no longer required on the AVS, select **not required**.
   b. After mapping each device, select **Save**.
6. Click the name of the network interface in the **Network Interface Card** column.
7. In the **Network Interface Settings** dialog box, edit the IP address, gateway, and network mask, as needed.
8. Click **Save** and **Close**. Don't click the X button in the top, right corner of the dialog box.

> **Note:**
>
> In Oracle AVDF 20.1, you may encounter the following error while changing the IP address of the management interface:
>
> ```
> Operation failed OAV-46981: Unable to connect to Database Firewall
> with IP <ipaddress>
> ```
>
> Ignore the error and close the window. The IP address is changed successfully. This error is fixed in Oracle AVDF 20.2.

This change is effective immediately on the Database Firewall. However, it may take a few seconds for the network update on the Database Firewall and for the system to settle.

> **Note:**
>
> Continue with the remaining steps only if the IP address to be changed belongs to the management interface and your current installation is Oracle AVDF 20.1. The following steps are not required for Oracle AVDF 20.2 and later.
>
> The management interface IP address is the IP address of the Database Firewall that was used to register the Database Firewall in the Audit Vault Server console.

9. On the Database Firewall details page, update the IP address with the new IP address of the Database Firewall.

   The IP address of the Database Firewall appears next to the **Firewall Name** field.

10. Click **Save**.

    The `Firewall updated successfully` message appears.

11. If the certification validation fails after saving the changes, click the name of the Database Firewall, and then click **Update Certificate**.

    The **Update Certificate** button appears only if an error is detected.

    After the certificate is updated, the **Database Firewalls** tab appears and the Database Firewall server is online.

12. As the *root* user, update the IP address in the `/etc/hosts` file on the Audit Vault Server appliance to the new IP address of the Database Firewall.

> **Note:**
>
> When the Database Firewall Server is back online, it begins to download any monitoring point log data that was not downloaded while it was offline.

> **See Also:**
>
> Changing IP Addresses of Active and Registered Agents

5.7 Changing the Database Firewall Host Name

Learn how to change the Database Firewall host name.

To change the Database Firewall host name using the Audit Vault Server console:

1. Log in to the Audit Vault Server console as administrator.
2. Click **Database Firewalls** tab in the Audit Vault Server console main page. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Locate and click the name of the specific Database Firewall instance for which the host name needs changing. The **Firewall Details** page is displayed.
4. Change the **Host Name** in the main page. This is the name of the host machine on which the Database Firewall is installed.
5. Click **Save** button in the top right corner.

5.8 Configuring the Database Firewall and Its Traffic Sources on Your Network

Learn about configuring the Database Firewall and its traffic sources on your network.

5.8.1 About Configuring Oracle Database Firewall and Traffic Sources On Your Network

Learn about configuring Oracle Database Firewall and its traffic sources on the network.

During your planning of the network configuration, you must decide the Database Firewall deployment type. The following are the Database Firewall deployment types:

- Monitoring (Out-of-Band)
- Monitoring (Host Monitor)
- Monitoring / Blocking (Proxy)

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 monitoring only or will include blocking mode as well.

You will use traffic and proxy sources of a Firewall to configure monitoring points for each target database you are monitoring with that firewall.

> **See Also:**
>
> Configuring Database Firewall Monitoring Points

5.8.2 Configuring Network Settings

Learn about configuring network setting (traffic sources).

The installation process applies network settings like the IP address, network mask, and so on, to a network interface card (NIC), also referred to as a management interface. It also detects and lists all NICs.

Use the following steps to change the settings for the management interface or to configure any other available NIC that can be used as a traffic source:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Click the specific Database Firewall instance that you want to configure as a proxy. The details of the specific Database Firewall instance are displayed in the main page.
4. In the **Configuration** section, click **Network Settings**.

   The **Network Settings** dialog lists all the details like the current network settings, proxy ports, and traffic sources (network interface cards) of the specific Database Firewall instance.
5. Starting in Oracle AVDF 20.12, if the **Synchronize NICs** button is disabled, proceed to the next step. If the **Synchronize NICs** is active, click it, as the AVS detects NIC name changes in the Database Firewall which must be synchronized.
   a. Select a NIC name on the Database Firewall for all the devices. If a device is no longer available on the Database Firewall and is no longer required on the AVS, select **not required**.
   b. After mapping each device, select **Save**.
6. To make changes to the IP address or the network mask, click the specific network interface card in the **Network Interface Card** column.
7. In the **Network Interface Settings** dialog, edit the **IP Address**, **Network Mask**, or **Gateway** fields as necessary. A user friendly name can also be specified for the network interface card in the **Network Interface Name** field.
8. Click **Save**.

5.8.3 Configuring the Database Firewall As a Traffic Proxy

You can specify multiple ports to be used as different proxy monitoring points. After you set up the Database Firewall as a traffic proxy, your database clients connect to the database by using the Database Firewall proxy IP address and port.

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
   Database Firewalls is selected in the left navigation menu by default.
3. Click the name of the Database Firewall instance that you want to configure as a proxy.
4. In the **Configuration** section, click **Network Settings**.
5. Starting in Oracle AVDF 20.12, if the **Synchronize NICs** button is disabled, proceed to the next step. If the **Synchronize NICs** is active, click it, as the AVS detects NIC name changes in the Database Firewall which must be synchronized.

a. Select a NIC name on the Database Firewall for all the devices. If a device is no longer available on the Database Firewall and is no longer required on the AVS, select **not required**.

b. After mapping each device, select **Save**.

6. In the **Network Settings** dialog box, click the name of the network interface card in the **Network Interface Card** column.
7. In the **Network Interface Settings** dialog box, click **Add** in the **Proxy Ports** section.
8. Enter the name and port number.
   When specifying a proxy mode target, you can enter one target address, consisting of IP:port:Oracle Service Name (OSN). The OSN can be left blank, meaning that all Oracle database services at the provided IP:port will be processed.

> **Note:**
>
> If you plan to monitor more than one OSN on a target database:
>
> - Oracle AVDF 20.1-20.9: You need to configure a proxy target for each OSN. This is because a single proxy port cannot service multiple OSN's on the same target database. Add more traffic proxy ports as required.
> - Oracle AVDF 20.10 and later: You can use one proxy port and specify multiple OSN's on the target database that are going to be processed. Specify the OSN's in a list delimited by the "|" character. For example, target1|target2|target 3.

9. (Optional) To specify more than one proxy port, click **Add**, and enter another port name and number.
10. Click **Save**.
11. The traffic proxy is now available to use in the Database Firewall monitoring point.

> **See Also:**
>
> Configuring Database Firewall Monitoring Points

5.9 Viewing the Status and Diagnostics Report for Database Firewall

Learn how to view Database Firewall status and diagnostics reports.

To view the status or diagnostic reports for Database Firewall:

1. Log in to the Audit Vault Server console.
2. Click the **Database Firewalls** tab.
3. Click the name of a specific Database Firewall instance for which the diagnostics needs to be viewed.
4. In the **Diagnostics** section on the main page, click **Download Diagnostics**.

   The **Download Diagnostics** dialog is displayed.

5. Select one of the following buttons on the dialog:
   - **Run Diagnostics** to run diagnostics.
   - **Download** to download all diagnostics files.
   - **Delete** to clear the diagnostic logs.

5.10 Configure and Download the Diagnostics Report File

Learn about configuring and downloading the diagnostics report file.

This section contains information about enabling, configuring, and modifying the way diagnostic reports are generated using CLI.

> **Note:**
>
> You need root user privileges to perform these tasks.

The diagnostic report is not enabled by default. You must enable the feature to capture the diagnostic report. Once enabled, you must configure the information that is to be captured in the diagnostic report. You can customize and package the diagnostics report with flexibility.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run the following command on the appliance:

   ```
   /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --install
   ```

   The `diagnostics-not-enabled.readme` file is downloaded when the diagnostics package is not enabled.
3. After the package has been installed, the diagnostics configuration must be modified to allow the utility to collect information about the appliance. Collection of all elements and files can be enabled with:

   ```
   /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --enable ALL
   ```

   Alternatively, the collection of the SOS report can be enabled with:

   ```
   /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --enable SOS_REPORT
   ```
4. Optionally, further options are available by viewing the utility help:

   ```
   /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --help
   ```
5. Run the following command to capture the enabled diagnostic information for the appliance:

   ```
   /usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb
   ```

   When you run the diagnostics collection command, deployment information will be collected by default. See the table below to learn what deployment information is collected.

The location of the saved zip file is displayed at the end of the command execution.

6. When you have collected the diagnostics, remove the package with the following command:

```
/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --remove
```

Table 5-1 Deployment Information Collected By the Diagnostics Log When Run With the `ALL` Option on the Audit Vault Server (AVS)

Deployment Information	Details
Number of targets and type of targets	Number of each type of target
Audit trail type	Number of each type of audit trail
Number of Database Firewall (DBFW) servers	Number of DBFW servers (individual servers)
High Availability (HA) Configuration - AVS	Yes or No
High Availability (HA) Configuration - DBFW	Yes or No If yes, the number of primary/secondary firewall servers
DBFW deployment model	Count of each type of deployment if present • Monitoring/Blocking (Proxy) • Monitoring (Host Monitor) • Monitoring (Out-Of-Band)
List of audit policies enabled	Are unified auditing policies provisioned? Yes or No
	Are traditional auditing policies provisioned? Yes or No
	The number of predefined policies that are enabled
	The number of custom policies
DBFW policies and rules deployed	The number of policies with Database Object rule
	The number of policies with Session Context rule
	The number of policies with Default rule
	The number of policies with SQL Statement rule
Entitlement report	Is it scheduled? Yes or No
Sensitive Object job	Is it scheduled? Yes or No
Security Assessment	Is it scheduled? Yes or no?
Number of Alert policies	Number of alerts enabled
Email notification	Is it enabled for alert policies? Yes or No
	Is it enabled for system alerts? Yes or No
Sensitive object upload	Have you uploaded a file? Yes or No
Number of generated reports	Number of reports per category generated
Number of scheduled reports	Number of reports per category Scheduled
STIG	Is it enabled? Yes or No
TLS	Is it enabled? Yes or No
FIPS	Is it enabled? Yes or No
Stored procedure auditing	Is it scheduled? Yes or No
Number of events per second	Number of events per second
Use of network-based storage	Is it being used? Yes or No
Archive policy	The archive policies being used for targets: number of months online and offline.
Backup frequency	Backup frequency

Table 5-1 (Cont.) Deployment Information Collected By the Diagnostics Log When Run With the `ALL` Option on the Audit Vault Server (AVS)

Deployment Information	Details
Hardware configuration (core/RAM) of AVS and DBFW server	Hardware configuration (core/RAM) of AVS
	Total memory space (KB)
	Total disk space (Bytes)
	CPU utilization percent

Related Topics

- Viewing the Status and Diagnostics Report for Database Firewall
  Learn how to view Database Firewall status and diagnostics reports.

5.11 Configuring Encapsulated Remote Switched Port Analyzer with Database Firewall

Learn how to configure Database Firewall when the SQL traffic is mirrored using Encapsulated Remote Switched Port Analyzer.

Encapsulated Remote Switched Port Analyzer (ERSPAN) mirrors the traffic from one or more source ports and delivers the mirrored traffic to one or more destination ports on another device.

This functionality enables the Database Firewall to interpret the SQL traffic received. This functionality is available only in **Monitoring (Out of Band)** deployment mode of Database Firewall.

Configuring ERSPAN with Database Firewall includes the following steps on a high level:

1. Configuring the ERSPAN source or the switch.
2. Configuring the Database Firewall.

Configuring the ERSPAN source or the switch includes the following steps:

1. Configure the network device or switch to span the SQL traffic to the target databases that are being monitored.
2. Consider the following aspects during ERSPAN configuration:
   - Avoid spanning the database response traffic unless it requires to be analyzed.
   - Avoid spanning empty TCP packets. For example, empty ACK packets.
3. Ensure the ERSPAN traffic is directed to the appropriate network interface card (NIC) configured on the Database Firewall.

Configuring the Database Firewall for this functionality includes the following steps:

1. Configure the Database Firewall monitoring point only in **Monitoring (Out of Band)** mode.
2. List all the IP addresses and ports of the SQL traffic expected from the target databases.

> **Note:**
>
> For Oracle Real Application Cluster databases, this is not just the scan IP addresses. It also includes all the relevant Oracle RAC nodes.

3. Configure the Database Firewall monitoring point. During configuration, select the NIC to which the ERSPAN traffic is forwarded.
4. The Database Firewall does not process the ERSPAN traffic by default. It has to be enabled on the Database Firewall monitoring points. Follow these steps to enable:
   a. Log in to the Database Firewall through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.
   b. Change to `/var/dbfw/va` directory.
   c. Identify the Database Firewall monitoring point by searching for the target name configured in the Audit Vault Server. Run the following command:

      ```
      grep -lr <TARGET NAME> *
      ```

   d. Find the monitoring point number from the output which contains the name and path of the configuration file. For example: `1/etc/appliance.conf`. In this example, `1` is the monitoring point number.
   e. Find the target database `va` number from the output as well. It will be before the monitoring point number, i.e. `va/1/etc/appliance.conf`
   f. Enable ERSPAN in the Database Firewall monitoring point by editing the file: `/usr/local/dbfw/va/<N>/etc/appliance.conf` where `N` is the monitoring point number and `va` is the target database number..
   g. In the file, edit the setting: `DAM_TRAFFIC_IS_ERSPAN="0" to DAM_TRAFFIC_IS_ERSPAN="1"`.
   h. Save the changes.
   i. Restart the Database Firewall processes so that the new configuration comes into effect. Run the command to restart: `/usr/local/dbfw/bin/dbfwctl restart`
5. Verify the ERSPAN traffic received. Access the `/var/log/messages` file in the Database Firewall. Navigate and locate the string `ODF-10524: Encapsulated protocol detected`. This string is logged when the ERSPAN traffic is first received.

Related Topics

- Configuring Network Settings for Oracle Database Firewall
  Learn how to configure the network settings for Oracle Database Firewall.

6

Registering Hosts and Deploying the Agent

If you're deploying the Audit Vault Agent, you register the host computers for the targets for which you want to collect audit data and deploy the Audit Vault Agent on each of them.

> **Note:**
>
> Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

6.1 About Registering Hosts and Deploying the Agent

Learn how to register hosts and deploying the Audit Vault Agent.

Register a host computer from where audit data is collected. After registering the host, you can deploy the Audit Vault Agent on that host. The Audit Vault Agent is a component of Oracle Audit Vault and Database Firewall (Oracle AVDF) that you can download from the Audit Vault Server console. After being deployed, Audit Vault Agents are ready to collect data from targets. A target is a system that you want to monitor and protect.

Step	Task	Reference Topic
1	Check the requirements.	Audit Vault Agent Requirements
2	Check the documentation about deploying the Audit Vault Agent.	Deploying the Audit Vault Agent on Host Computers
3	Register the host machine (agent machine).	Registering Hosts on the Audit Vault Server
4	Download the Audit Vault Agent software from the Audit Vault Server console and deploy the agent.	Deploying the Audit Vault Agent
5	Activate and start the Audit Vault Agent.	Activating and Starting the Audit Vault Agent
6	In case of any error or issue, refer to the troubleshooting documentation and known issues.	Troubleshooting Oracle Audit Vault and Database Firewall Known Issues

After registering the hosts on the Audit Vault Server, perform the following steps to be able to collect audit records:

1. Download the Audit Vault Agent software from the Audit Vault Server console.
2. Deploy the Audit Vault Agent.
3. Activate the Audit Vault Agent.
4. Register one or more targets from which you want to collect audit data.
5. Start collecting data from the targets' audit trails by using the Audit Vault Server console.

See Also:

- Registering Targets
- Configuring and Managing Audit Trail Collection
- Summary of Configuration Steps to understand the high-level workflow for configuring the Oracle Audit Vault and Database Firewall system
- Using the Audit Vault Command Line Interface
- Deploying the Audit Vault Agent on Host Computers

6.2 Registering Hosts on the Audit Vault Server

Learn about registering hosts on the Audit Vault Server.

Prerequisite: Check Product Compatibility Matrix for supported cluster/platforms for Agent deployment and before proceeding with the host registration.

To register a host computer in the Audit Vault Server:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Agents** tab.
3. In the left navigation menu, click **Agents** tab.

   A list of registered Agents is displayed on the page.
4. Click **Register**.
5. In **Name** field, enter the name of the Audit Vault Agent. This field is mandatory and must not contain special characters. The system connects to the host using the IP address. The name defined here is a logical name of the Agent and is used for descriptive identification. You may use the host name as the Agent name for easy identification.
6. The **IP Address** field is mandatory.

   Enter the IP address of the host computer where the Audit Vault Agent is expected to run.

   Audit Vault Server validates the connections from the Audit Vault Agent using the registered IP address. In case the host machine contains more than one IP address (for example, the Audit Vault Agent is expected to run on a host with multiple IP addresses or network interfaces), all of the IP addresses have to be registered with the Audit Vault Server. Follow these steps:

   a. Enter one of the IP addresses or a unique logical IP address.
   b. After setting the IP address, set all the physical IP addresses using which the Audit Vault Agent is expected to connect to the Audit Vault Server as host attributes. Click **Add** button in the **Attributes** section.
   c. Enter `AGENT_PHYSICAL_ADDRESS_XX` in the **Name** field where XX can be any value between 01 and 99.
   d. Enter a valid IP address in the corresponding **Value** field.
7. Click **Save**.

   An Agent Activation Key is automatically generated when you register the host.

Agent Deployment in a High Availability System

Audit Vault Agent may be associated with multiple IP addresses in the following cases:

1. Agent installed on a host with multiple network interface cards
2. Agent installed on a node of high availability cluster
   a. Only one Audit Vault Agent installation is necessary for high availability cluster deployment. The Agent installation is needed only on active node of the cluster. Ensure the Audit Vault Agent installation directory is accessible from all nodes of the cluster.
   b. Cluster management software must be configured to start, stop, and monitor the Agent by providing the necessary input. The Agent must be started automatically by the cluster management software on the active node and stopped automatically on passive nodes.

Use the following commands in the cluster manager software:

Action	Command
To stop the Agent	`Agent_Home/bin/agentctl stop`
To start the Agent	`Agent_Home/bin/agentctl start`
To monitor the Agent	`Agent_Home/bin/agentctl status`

See Also:

- REGISTER HOST for the command line syntax to register a host.
- Configuring or Changing the Audit Vault Server Services to configure DNS server.
- Using Audit Vault Server Console
- Configuring Network Settings for Oracle Database Firewall

6.3 Deploying the Audit Vault Agent on Host Computers

Learn about how to deploy the Audit Vault Agent on host computers.

Note:

When you register a host on the Audit Vault Server, an activation key is generated. When you deploy the Audit Vault Agent on the host computer, you need to provide the corresponding activation key, as discussed in the following procedures.

6.3.1 Audit Vault Agent Requirements

Learn about the Audit Vault Agent requirements.

> **Note:**
>
> Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

Recommended Prerequisites for Installing Audit Vault Agent

1. Ensure that you meet the system requirements. See Product Compatibility Matrix.
2. Ensure that you meet the following Java requirements:
   - Install the supported Java version on the Audit Vault Agent. See Audit Vault Agent: Supported and Tested Java Runtime Environment.
   - Apply the latest Java patches.
   - Point the `JAVA_HOME` to the JRE/JDK directory and set the path before installing the Audit Vault Agent.
3. Ensure that the host machine on which the Audit Vault Agent is deployed has at least 512 MB RAM.
4. Apply the latest security patches for the OpenSSL libraries that are available from the OS vendor for the specific OS version on the host machine.
5. Ensure that the host machine on which the Audit Vault Agent is deployed has connectivity to the Audit Vault Server.

   In a high availability environment, it must have connectivity to both primary and standby Audit Vault Servers.
6. Ensure that two Audit Vault Server ports (1521 and 1522 by default) are configured for communication with the Audit Vault Agent.
7. If you use Network Address Translation (NAT) in the network between the Audit Vault Server and the host machine where the agent is deployed, then ensure that the IP address of the host machine is resolvable from the Audit Vault Server.
8. Ensure that the user has the required OS permissions to install the agent.

   For directory audit trails, the user must be able to access the audit trail location. See About Deploying the Audit Vault Agent for the OS permissions that are required for installing the agent.
9. Ensure that the Audit Vault Agent home directory is access protected.

   Only the *Agent* user should have write or execute permissions on the agent home directory.
10. Ensure that the Audit Vault Agent host machine system settings are access protected to prevent malicious users from making modification.
11. Ensure that the system time of the Audit Vault Agent and the target are synchronized.

They can be in different time zones. The time difference between these two systems (considering time zone conversion) should not exceed two seconds.

Additional Requirements for Starting the Audit Vault Agent as a Service on Windows

For Oracle AVDF 20.4 and earlier releases, comply with one of the following prerequisites:

- Install the Visual C++ Redistributable for Visual Studio 2012 Update 4 package from Microsoft on the Windows host machine.

  Ensure that the `msvcr110.dll` file is available in the `C:\Windows\System32` directory.
- If the `msvcr110.dll` file is not present, then add it to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` directories.

For Oracle AVDF 20.6 and later releases, comply with one of the following prerequisites:

- Install the Visual C++ Redistributable for Visual Studio 2017 package from Microsoft on the Windows host machine.

  Ensure that the `vcruntime140.dll` file is available in the `C:\Windows\System32` directory.
- If the `vcruntime140.dll` file is not present, then add it to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` directories.

> **Note:**
>
> There is a known issue in Oracle AVDF 20.5 for starting Audit Vault Agent as a service on Windows. See Error When Starting Audit Vault Agent as a Service on Windows in Oracle AVDF 20.5 for complete information. This issue is resolved in Oracle AVDF 20.6 and later.

6.3.2 Audit Vault Agent Machine Java Best Practices

Learn some best practices regarding Java on the Audit Vault Agent machine.

1. Ensure installation of Java and the Java home directory is managed by a trusted user.
2. If Java is upgraded to a major version or if it is patched with security updates, then restart the Audit Vault Agent. This ensures the Audit Vault Agent runs with the updated Java.

6.3.3 Validation During Audit Vault Agent Deployment

Learn about validations performed by Oracle AVDF when deploying the Audit Vault Agent.

Starting Oracle AVDF release 20.6, some validations are performed when deploying Audit Vault Agent.

The following validations are performed when running the `agentctl start` command. These requirements are mandatory and have to be complied, without which the Audit Vault Agent installation cannot be completed.

- Minimum java version is installed on the host machine as per Audit Vault Agent: Supported and Tested Java Runtime Environment.
- Audit Vault Agent is being installed on the supported operating system version as per Product Compatibility Matrix.

- The Agent machine on which the Audit Vault Agent is being deployed can connect to the Audit Vault Server.

Ensure to comply with the requirements on the Agent machine:

- The Agent machine has a minimum of 512MB available space.
- The Agent machine must be able to connect to the Audit Vault Server.
- Sufficient permissions required to install the Audit Vault Agent are available.

6.3.4 About Deploying the Audit Vault Agent

Audit Vault Agent collects audit trail data from targets. The host computer where you deploy the Audit Vault Agent depends on the type of audit trail that you want to collect. The Audit Vault Agent includes plug-ins for each target type.

Use the following guidelines to choose the host computer where you need to deploy the Audit Vault Agent:

Trail Type	Guideline for Host Computer
`TABLE`	Deploy the Audit Vault Agent on a remote host or on the host machine where the database is running.
`DIRECTORY`	Deploy the Audit Vault Agent on the host machine where the `DIRECTORY` path exists or on a machine from which the `DIRECTORY` path can be accessed.
`TRANSACTION LOG`	Deploy the Audit Vault Agent on the host machine where the GoldenGate Integrated Extract path exists or on a machine from which it can be accessed.
`NETWORK`	Deploy the Audit Vault Agent on the host machine where the database is running.

OS Permissions for Installing the Agent

Operating System	User
Linux/Unix	Any user
Windows	Any user for running the Audit Vault Agent from the command prompt The *admin* user for registering as a service

Note:

- Host Monitor Agent on Linux/Unix/AIX/Solaris platforms must be installed as *root* user.
- If directory trails are used then Agent installation user should have *read* permission on the audit files.
- Host Monitor Agent on Windows platform, must be installed as *admin* user.
- Ensure that the host machine has *OpenSSL 1.0.1* (or later) installed for Audit Vault Agent.
  OpenSSL 1.1.1 and earlier on Windows platforms was deprecated in Oracle AVDF 20.11, and it will be desupported in one of the future releases. To prevent issues, you should move to OpenSSL 3.0.13 or later.

Deploying Audit Vault Agent Remotely or Locally

Table 6-1 Remote Agent or Local Agent

Trail Type	Audit Vault Server Location	Agent Type	Detailed Information
Directory	On-premises	Remote Agent Not installed on the target machine	• Audit data is written to the local disk. • The local disk is mounted on the remote Agent machine as NFS (Network File System). • Remote Agent is not installed on the target machine. • Remote Agent should have access to the mounted NFS. • Audit data read time includes the network latency involved in accessing NFS. • This deployment can be used when the operating system of the target machine is not supported for Audit Vault Agent installation. • This deployment can be used when the target machine does not have sufficient memory or CPU resources for the Audit Vault Agent processes. • For Oracle Linux operating system, it is recommended to use Kerberos to secure NFS. • For non Oracle Linux operating systems, follow the respective OS recommendations to secure NFS.
Directory	On-premises	Local Agent Installed on the target machine	• Audit data is written to the local disk. • The local Audit Vault Agent is installed on the target machine. • The local Audit Vault Agent should have access to the local disk. • Audit data read time has no network latency. • This deployment can be used when the operating system of the target machine is supported for Audit Vault Agent installation. • This deployment can be used when the target machine has sufficient memory and CPU resources for the Audit Vault Agent processes.

Table 6-1 (Cont.) Remote Agent or Local Agent

Trail Type	Audit Vault Server Location	Agent Type	Detailed Information
Directory	OCI (Oracle Cloud Infrastructure)	Remote Agent Not installed on the target machine	• Audit data is written to the local disk. • The local disk is mounted on the remote Agent machine as NFS. • Remote Agent should have access to the mounted NFS. • Remote Agent is not installed on the target machine. • If the target is on-premises, then the remote Agent must also be installed on-premises. • If the target is on OCI, then the remote Agent must be installed on OCI. • OCI virtual firewall for VCN must be configured to allow ingress traffic on ports 1521 and 1522 for Audit Vault Server. • This deployment can be used when the operating system of the target machine is not supported for Audit Vault Agent installation. • This deployment can be used when the target machine does not have sufficient memory or CPU resources for the Audit Vault Agent processes. • For Oracle Linux operating system, it is recommended to use Kerberos to secure NFS. • For non Oracle Linux operating systems, follow the respective OS recommendations to secure NFS.
Directory	OCI (Oracle Cloud Infrastructure)	Local Agent Installed on the target machine	• Audit data is written to the local disk. • The local Audit Vault Agent is installed on the target machine. • The local Audit Vault Agent should have access to the local disk. • Audit data read time has no network latency. • This deployment can be used when the operating system of the target machine is supported for Audit Vault Agent installation. • This deployment can be used when the target machine has sufficient memory and CPU resources for the Audit Vault Agent processes.
Table	On-premises	Remote Agent Not installed on the target machine	• Audit data is written to the table. • Remote Agent is not installed on the target machine. • Remote Agent uses connection string to connect to the target. • Audit data read time includes the network latency involved in accessing the audit table. • This deployment can be used when the operating system of the target machine is not supported for Audit Vault Agent installation. • This deployment can be used when the target machine does not have sufficient memory or CPU resources for the Audit Vault Agent processes.

Table 6-1 (Cont.) Remote Agent or Local Agent

Trail Type	Audit Vault Server Location	Agent Type	Detailed Information
Table	On-premises	Local Agent Installed on the target machine	• Audit data is written to the table. • The local Audit Vault Agent is installed on the target machine. • The local Audit Vault Agent uses connection string to connect to the target. • Audit data read time has no network latency. • This deployment can be used when the operating system of the target machine is supported for Audit Vault Agent installation. • This deployment can be used when the target machine has sufficient memory and CPU resources for the Audit Vault Agent processes.
Table	OCI (Oracle Cloud Infrastructure)	Remote Agent Not installed on the target machine	• Audit data is written to the table. • Remote Agent is not installed on the target machine. • Remote Agent uses connection string to connect to the target. • If the target is on-premises, then the remote Agent must also be installed on-premises. • If the target is on OCI, then the remote Agent must also be installed on OCI. • Audit data read time includes the network latency involved in accessing the audit table. • OCI virtual firewall for VCN must be configured to allow ingress traffic on ports 1521 and 1522 for Audit Vault Server. • This deployment can be used when the operating system of the target machine is not supported for Audit Vault Agent installation. • This deployment can be used when the target machine does not have sufficient memory or CPU resources for the Audit Vault Agent processes.
Table	OCI (Oracle Cloud Infrastructure)	Local Agent Installed on the target machine	• Audit data is written to the table. • The local Audit Vault Agent is installed on the target machine. • The local Audit Vault Agent uses connection string to connect to the target. • Audit data read time has no network latency. • OCI virtual firewall for VCN must be configured to allow ingress traffic on ports 1521 and 1522 for Audit Vault Server. • This deployment can be used when the operating system of the target machine is supported for Audit Vault Agent installation. • This deployment can be used when the target machine has sufficient memory and CPU resources for the Audit Vault Agent processes.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features
- Registering Hosts on the Audit Vault Server
- Discovering and Registering Targets and Creating Groups
- Configuring and Managing Audit Trail Collection

6.3.5 Steps Required to Deploy and Activate the Audit Vault Agent

Learn about the procedures to deploy and activate Oracle 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.
3. Activating and Starting the Audit Vault Agent.

6.3.6 Registering the Host

Learn about the procedure for registering the host.

To register the host on which you deployed the Audit Vault Agent, follow the procedure in Registering Hosts on the Audit Vault Server.

6.3.7 Deploying the Audit Vault Agent

Learn about deploying the Audit Vault Agent.

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:**
>
> Ensure that all security patches from the OS vendor is applied on the host machine.

> **See Also:**
>
> The Audit Vault Agent is supported on Unix and Microsoft Windows platforms. It requires Java version 1.8 to be installed on the host machine. See Product Compatibility Matrix for Agent platform support details for the current release and for the supported Java versions.

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

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Agents** tab.
3. In the left navigation menu:

For release	Action
20.1 and 20.2	Click **Agent Software**
20.3 and later	Click **Downloads**

A list of downloadable agent software files are displayed on the page.

4. Click the **Download** button against the platform type, and then save the `agent.jar` file to a location of your choice.

   The download process copies the `agent.jar` file from the Audit Vault Server. Ensure that you always use this `agent.jar` file when you deploy the Agent.

5. Using an OS user account, copy the `agent.jar` file to the host machine where you're deploying the Audit Vault Agent.

> **Best Practice:**
>
> Do not install the Audit Vault Agent as *root* user.

6. On a Microsoft Windows system, 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 Microsoft Windows system, this command automatically registers a Microsoft 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, then do not delete the existing `Agent_Home` directory.

> **Note:**
>
> If you run into any issues, see the following topics for more information:
>
> - Troubleshooting Oracle Audit Vault and Database Firewall
> - Known Issues

6.3.8 Activating and Starting the Audit Vault Agent

Learn how to activate and start Audit Vault Agent.

In this step, you activate the Audit Vault Agent with the Agent activation key and start the Agent.

Prerequisites

- Follow and complete the procedure in Registering Hosts on the Audit Vault Server.
- Log in to the Audit Vault Server console as an *administrator*. See Using Audit Vault Server Console for more information.

To activate and start the agent:

1. Click the **Agents** tab.
2. In the left navigation menu, click **Agents**.

   A list of registered hosts are displayed on the page.
3. Copy or 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 above.
5. Run the following command:

   ```
   agentctl start -k
   ```
6. The system prompts as follows:

   ```
   Enter Activation Key:
   ```
7. Paste or enter the agent activation key in the following format:

   ```
   <Agent Name>:: XXXX-XXXX-XXXX-XXXX-XXXX
   ```

   The activation key is not displayed as you type it.

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

> **See Also:**
>
> - Registering and Unregistering the Audit Vault Agent as a Windows Service to start or stop the agent Windows service through the Windows Services applet in the Windows Control Panel, in case the Agent is deployed on a Microsoft Windows host computer.
> - ACTIVATE HOST for the command line syntax to activate the Agent.

6.3.9 Changing Host Names

Learn about changing host name.

To change the name of a registered host:

1. If the Audit Vault Agent is already deployed on that host and the Agent is running, then stop the Agent by executing the command below.

   For Linux platform:

   ```
   Agent_Home/bin/agentctl stop
   ```

For Windows platform, if Agent is running as a process:

```
Agent_Home/bin/agentctl stop
```

For Windows platform, if Agent is running as a service:

```
Agent_Home/bin/agentctl stopsvc
```

2. Log in to the Audit Vault Server console as an administrator. See Using Audit Vault Server Console for more information.
3. Click the **Agents** tab.
4. In the left navigation menu, click **Agents**.

   A list of registered Agents is displayed on the page.
5. Click the name of the Agent that you want to change.
6. In the dialog, change the **Name** or the **IP Address** field, and then click **Save**.
7. If you have changed either the Agent name or the IP address, and if the Agent has already been deployed on that host, then start the Agent by executing the below command. Enter the new activation key when prompted.

   For Linux platform:

   ```
   Agent_Home /bin/agentctl start -k
   ```

   For Windows platform, if Agent is running as a process:

   ```
   Agent_Home /bin/agentctl start -k
   ```

   For Windows platform, if Agent is running as a service:

   ```
   Agent_Home /bin/agentctl startsvc -k
   ```

6.3.10 Configuring Agent Auto Restart Functionality

Learn how to configure the Audit Vault Agent auto restart functionality.

Audit Vault Agent collects audit data from the target and sends it to the Audit Vault Server. The Agent must continuously run to carry out this task seamlessly. In some cases where the host machine (Agent machine) is restarted or the Agent goes down, then the Agent may stop running. It needs to be manually restarted so that it can continue to collect audit data.

Starting with Oracle AVDF release 20.7, the Audit Vault Agent can be configured to restart automatically. This functionality can be configured by the *agent* user. It periodically monitors the status of the Agent and restarts whenever required.

> **Note:**
>
> In Oracle AVDF releases 20.3 to 20.6, there is an existing functionality which involves configuring a service to restart the Agent. In case you have configured this functionality as mentioned in Audit Vault Agent Auto Start Configuration, then disable this previously configured functionality before proceeding with the below commands.

Run the following commands in the `Agent_Home/bin` directory to enable or disable the Agent auto restart functionality:

Task	Command
To enable Agent auto restart functionality and to start the Agent	`agentctl startsvc`
To enable Agent auto restart functionality, if the Agent is not activated	`agentctl startsvc -k`
To disable Agent auto restart functionality and to stop the Agent	`agentctl stopsvc`
To enable Agent auto restart functionality when the Agent is already in `RUNNING` status	`agentctl registersvc`
To disable Agent auto restart functionality without stopping the Agent	`agentctl unregistersvc`

> **Note:**
>
> - Use the commands wisely as it involves two tasks (enabling or disabling the Agent auto restart functionality and starting or stopping the Agent). In case the Agent is manually stopped and the auto start service is still in effect, then the Agent is automatically started again. If the Audit Vault Agent service is started, do not stop the Agent alone without stopping the service.
> - The Agent auto restart functionality must be enabled again, after updating the Java version on the Audit Vault Agent.
> - The Agent auto restart functionality may not work, if the Audit Vault Agent is not properly installed or if it is not registered in the Audit Vault Server console.
> - In case the Audit Vault Agent is being managed by another application such as cluster manager, then do not use the Agent auto restart functionality.

6.3.11 Configuring Agent Auto Restart Functionality Remotely

Learn how to configure Agent auto restart functionality remotely.

Agent auto restart functionality can be configured remotely starting with Oracle AVDF release 20.8. The administrator can enable this functionality through Audit Vault Server for multiple Audit Vault Agents at a time.

> **Note:**
>
> This functionality is applicable for Audit Vault Agents deployed on Linux/Unix/AIX/Solaris platforms only. It is not applicable for Audit Vault Agents deployed on Windows platform.

Prerequisite

The Audit Vault Agent must be in `RUNNING` state.

Follow these steps to enable or disable this functionality:

1. Log in to the AVCLI as an *administrator*.
2. Run the following commands:

Task	Command
To configure the Agent auto restart service remotely.	`ALTER HOST <host name> SET AUTO_RESTART=Y`
To disable the Agent auto restart service configuration remotely.	`ALTER HOST <host name> SET AUTO_RESTART=N`

> **See Also:**
>
> Viewing the Status and Details of Audit Vault Agent

6.3.12 Check if Audit Vault Agent Has Auto Restart Functionality Enabled

Learn how to check if the Audit Vault Agent is configured for auto restart functionality.

Follow these steps:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Agents** tab.
3. The **Agents** sub tab in the left navigation menu is selected by default. A list of registered Audit Vault Agents is displayed on the page.
4. In the list of registered Agents, identify the specific Agent.
5. Check the **Agent Details** column. The **Agent Auto Restart Status** field confirms if the Audit Vault Agent has auto restart functionality enabled.

> **Note:**
>
> Alternately, the auto restart status can be checked by running the following command from `<agent_home>/bin` directory:
>
> ```
> agentctl svcstatus
> ```

6.3.13 Registering and Unregistering the Audit Vault Agent as a Windows Service

Learn about registering and unregistering Oracle Audit Vault Agent as a Windows service.

> **Note:**
>
> The Audit Vault Agent as a Windows Service is not supported in Oracle Audit Vault and Database Firewall release 12.2.0.7.0. Use the console mode to stop or start the Agent.

6.3.13.1 About the Audit Vault Agent Windows Service

Learn about the Audit Vault Agent Windows service.

When you deploy the Audit Vault Agent on a Microsoft Windows host computer, during agent deployment, a Microsoft Windows service named OracleAVAgent is automatically registered. Additionally, you can register and unregister the agent service using the `agentctl` command.

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.

> **See Also:**
>
> Deploying the Audit Vault Agent

6.3.13.2 Registering the Audit Vault Agent as a Windows Service

You can register Audit Vault Agent as a Windows service.

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

Prerequisite

Ensure to comply with one of the following prerequisites for Oracle AVDF 20.4 and earlier releases:

- Install Visual C++ Redistributable for Visual Studio 2012 Update 4 package from *Microsoft* on the Windows target machine. Ensure `msvcr110.dll` file is available in `C:\Windows\System32` directory.
- If the `msvcr110.dll` file is not present, then add it to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` directories.

Ensure to comply with one of the following prerequisites for Oracle AVDF 20.6 and later releases:

- Install Visual C++ Redistributable for Visual Studio 2017 package from *Microsoft* on the Windows target machine. Ensure `vcruntime140.dll` file is available in `C:\Windows\System32` directory.
- If the `vcruntime140.dll` file is not present, then add it to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` directories.

> **Note:**
>
> There is a known issue in Oracle AVDF 20.5 for starting Audit Vault Agent as a service on Windows. See Error When Starting Audit Vault Agent as a Service on Windows in Oracle AVDF 20.5 for complete information. This issue is resolved in release Oracle AVDF 20.6 and later.

Registering Audit Vault Agent as a Windows Service

Run the following command on the host machine from the *Agent_Home*`\bin` directory:

```
agentctl registersvc
```

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

> **Note:**
>
> - 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 dialog box.
> - 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.

6.3.13.3 Unregistering the Audit Vault Agent as a Windows Service

You can use two methods to unregister the Oracle Audit Vault Agent as a Windows service.

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

- **Method 1 (Recommended)**

  On the host machine, run the 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
  ```

6.4 Stopping, Starting, and Other Agent Operations

Learn about starting and stopping the agent and other operations.

6.4.1 Stopping and Starting Audit Vault Agent

Learn about stopping and starting Audit Vault Agent.

Topics

> **Important:**
>
> Stop and start the Audit Vault Agent as the same OS user account that you used during installation.

> **See Also:**
>
> Audit Vault Agent Auto Start Configuration

6.4.1.1 Stopping and Starting the Agent on Unix Hosts

Learn about stopping and starting the Agent on Unix hosts.

To start the Audit Vault Agent after initial activation, run the following command from the *Agent_Home*`/bin` directory on the host machine:

```
agentctl start
```

To stop the Audit Vault Agent run the following command from the *Agent_Home*`/bin` directory on the host machine:

```
agentctl stop
```

> **Note:**
>
> - After the `agentctl stop` command, execute `agentctl status` command to ensure the Agent is in `STOPPED` state before executing the `agentctl start` command again.
> - In case the Agent auto start service (Oracle AVDF release 20.7 and onwards) is configured and if the Agent alone is manually stopped, then the Agent is automatically started again. See Configuring Agent Auto Restart Functionality for complete information and run the right commands.

6.4.1.2 Stopping and Starting the Agent on Windows Hosts

Learn about stopping and starting the Agent on Microsoft 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 a Windows service so that it can keep running after the user logs out.

See Also: Registering and Unregistering the Audit Vault Agent as a Windows Service

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 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
```

To forcibly stop the Agent in console mode

```
agentctl stop -force
```

> **Note:**
>
> This is not a recommended option to stop the Agent. Use it only in case the Agent goes into an unreachable state for a long time and cannot be restarted or stopped. In such a scenario, use this option to forcibly stop and later restart the Agent.
>
> To restart the Agent use the `agentctl start` command.

6.4.1.3 Autostarting the Agent on Windows Hosts

Learn about autostarting the agent on Microsoft Windows hosts.

You can configure the agent service to start automatically on a Windows host.

1. Open the Services Management Console.

   From the **Start** menu, select **Run**, and in the Run dialog box, enter `services.msc` to start the Services Management Console.
2. Right-click **Oracle Audit Vault Agent** and from the menu, select **Properties**.
3. In the Properties dialog box, set the **Startup type** setting to **Automatic**.
4. Click **OK**.
5. Close the Services Management Console.

6.4.2 Changing the Logging Level for the Audit Vault Agent

Learn how to change the logging level for Oracle Audit Vault Agent.

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

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

The following logging levels are listed in the order of the amount of information written to log files, where debug provides 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

Using the Audit Vault Server Console to Change Logging Levels

To change the logging level for the Audit Vault Agent using the Audit Vault Server UI, see "Clearing Diagnostic Logs".

Using AVCLI to Change the Agent Logging Level

To change the logging level for the Audit Vault Agent using the AVCLI utility:

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`.

6.4.3 Viewing the Status and Details of Audit Vault Agent

Learn about viewing the status and details of Audit Vault Agent.

You can view an Audit Vault Agent's status and details such as activation key, platform, version, location, and other details.

Prerequisite

Log in to the Audit Vault Server console as an administrator. See Using Audit Vault Server Console for more information.

To view the status and details of an Audit Vault Agent:

1. Click the **Agents** tab.
2. In the left navigation menu, click **Agents**.

   A list of registered Agents is displayed on the page.
3. In this list of registered Agents, check the **Agent Status**, **Host Monitor Status**, **Activation Key**, **Agent Details**, and **Host Monitor Details** columns for the Agent that you are interested in.
4. To see the audit trails for a specific Agent host, click **View Audit Trails** in the **Agent Details** column.

6.4.4 Deactivating and Removing Audit Vault Agent

Learn about deactivating and removing Audit Vault Agent.

Use this procedure to deactivate and remove Audit Vault Agent.

> **See Also:**
>
> If you have registered the Audit Vault Agent as a Windows service, see Registering and Unregistering the Audit Vault Agent as a Windows Service to unregister the service.

1. Stop all audit trails being collected by the Audit Vault Agent.
   a. In the Audit Vault Server console, click the **Targets** tab.
   b. Click **Audit Trails** in the left navigation menu.
   c. Select the check boxes for each audit trail that you want to stop, 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 **Agents** tab, and then in the left navigation menu, select **Agents**.
   b. Select the check box for each host name that you want to deactivate, and then click **Deactivate**.
   c. Optionally, drop the host by selecting the check box for it, and then clicking **Delete**.
   d. Delete the Audit Vault Agent home directory on the host computer.

> **Note:**
>
> The Audit Vault Agent deployed on a host is associated with the specific Audit Vault Server from where it was downloaded. This Audit Vault Agent collects audit data from the configured targets. It sends this data to the specific Audit Vault Server. To configure the audit trail collection from the existing targets to a different Audit Vault Server, you should deactivate, remove the existing Agent, download the Audit Vault Agent installation file from the new Audit Vault Server, and install it on the target host. This scenario is different from updating the existing Auditing Vault Agent.

6.5 Updating Audit Vault Agent

Learn about updating Audit Vault Agent.

When you update the Audit Vault Server, the Audit Vault Agent is automatically updated. When you upgrade the Audit Vault Server to a later version, or restart the Audit Vault Agent, you no longer need to restart audit trails manually. The audit trails associated with the Audit Vault Agent automatically restart if you have not explicitly stopped them. If you upgrade the Audit Vault Server, the audit trails associated with the updated Agents will automatically restart if the trails have a single plug-in.

> **See Also:**
>
> Oracle Audit Vault and Database Firewall Installation Guide for information about downloading upgrade software.

6.6 Deploying Plug-ins and Registering Plug-in Hosts

Learn about deploying plug-ins and registering plug-in hosts.

6.6.1 About Plug-ins

Learn about plug-ins for Audit Vault Server.

Each type of 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 Audit Vault and Database Firewall, in order to collect audit data from more target types.

A plug-in supports only one target type. However, you may deploy more than one plug-in for the same 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 target type. You can select the specific plug-in to use when you configure audit trail collections.

To start collecting audit data from the target type associated with a plug-in, you must also add the target in the Audit Vault Server, then configure and manually start audit trail collection.

> **See Also:**
>
> Configuring Targets, Audit Trails, and Database Firewall Monitoring Points

Deploying a plug-in consists of three steps:

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

6.6.2 Ensuring that Auditing is Enabled in a Target

Learn how to ensure that auditing is enabled in a target.

Ensure that auditing has been enabled in the target. See the target's product documentation for more information.

> **See Also:**
>
> Ensuring that Auditing is Enabled on the Target for information on plug-ins for Oracle Database.

6.6.3 Registering the Plug-in Host in Audit Vault Server

Learn about registering a plug-in host in Audit Vault Server.

To register a host in the Audit Vault Server, see Registering Hosts on the Audit Vault Server.

Oracle AVDF provides out-of-the-box plug-ins for most commonly used trails. See Plug-In Reference for a complete list. You don't need to deploy plug-ins for targets that have existing out-of-the-box plug-ins.

6.6.4 Deploying and Activating the Plug-in

Learn about deploying and activating a plug-in in Audit Vault Server.

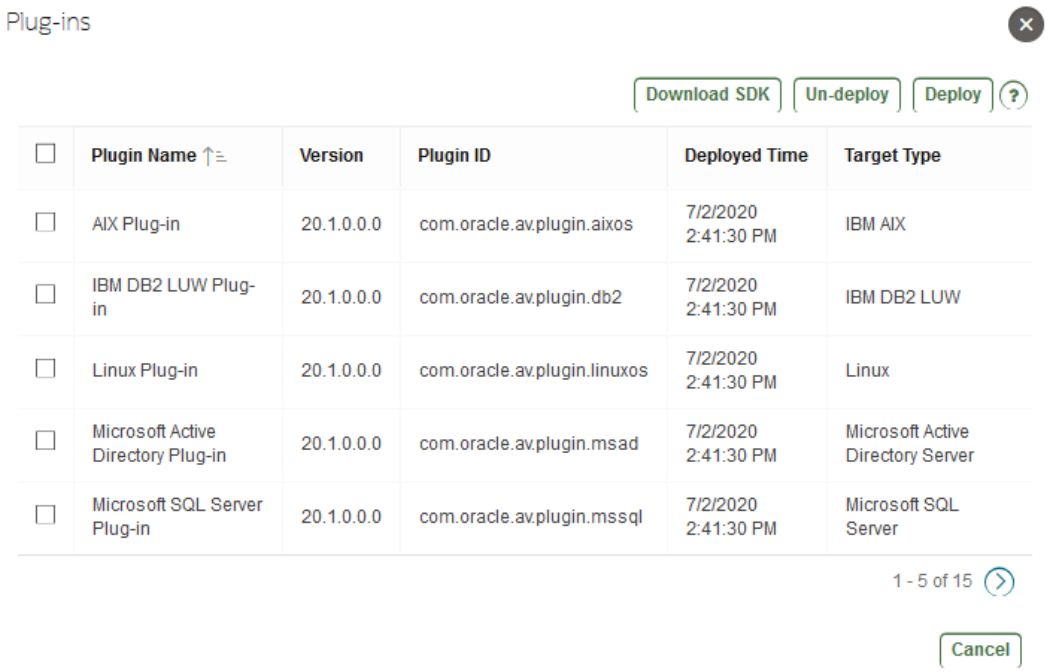
To deploy and activate a plug-in:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Settings** tab.
3. In the left navigation menu, select **System**.

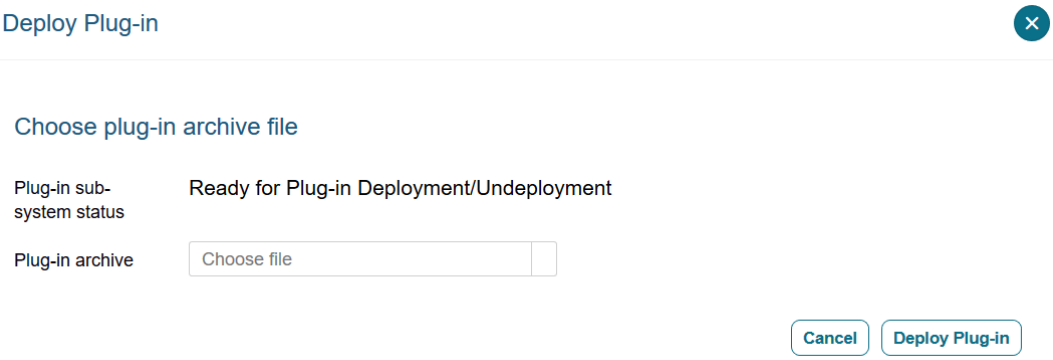
A status page appears, with pane for **Configuration** and **Monitoring**.

4. In the **Monitoring** pane, click **Plug-ins**.

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



5. Copy the plug-in archive to the Audit Vault Server, and make a note of the location of the file. Click **Deploy**, and in the **Plug-in Archive** field, enter or browse for the name of the plug-in archive file.



6. Click **Deploy Plug-in**, then click **Deploy**.

   The new plug-in is listed in the Plug-ins page. The updated `agent.jar` file has a new Deployed Time shown in this page.

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

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

Register the host machine in case it is not registered.

8. On the host machine, extract the agent:

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

> **Note:**
>
> Do not download the Agent during the same login session in which the plug-in is deployed, as the `agent.jar` file is being updated. However, users in other sessions can download the most current version of the `agent.jar` file after the plug-in deployment process is complete and a new version is available.

> **See Also:**
>
> - Using Audit Vault Server Console
> - Registering Hosts on the Audit Vault Server

6.6.5 Removing Plug-ins

Learn about removing plug-ins.

To remove a plug-in:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **System**.

   A status page appears, with pane for Configuration and Monitoring.
4. In the Monitoring pane, click **Plug-ins**.
5. Select the plug-in that you want, and then click **Un-deploy**.

> **See Also:**
>
> Using Audit Vault Server Console

6.7 Deleting Hosts from Audit Vault Server

Learn how to delete hosts from Audit Vault Server.

When you delete a host, if you want to register it again to collect audit data, then 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 **Agents** tab.
3. In the left navigation menu, click **Agents**.

   A list of registered Agents is displayed on the page.
4. Select the check boxes for the hosts that you want to delete, and then click **Delete**.

> **See Also:**
>
> - Working with Lists of Objects in the Audit Vault Server Console to control the view of registered hosts listed.
> - Using Audit Vault Server Console

7

Configuring Targets, Audit Trails, and Database Firewall Monitoring Points

Learn about configuring targets, audit trails, and Database Firewall monitoring points.

7.1 About Configuring Targets

Learn about configuring targets.

Targets can be supported databases or operating systems that Audit Vault and Database Firewall monitors. You must register all of the 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 targets, you must configure an audit trail for each target and start collection manually.

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

For Oracle Database targets that you monitor with the Database Firewall, you can configure Oracle Audit Vault and Database Firewall to monitor the native network encrypted traffic. To do so, you must run scripts on the target computers to configure the necessary privileges.

If you are using the Database Firewall, you can also monitor the target database's responses to incoming SQL traffic. The following sections contain the high-level workflow for configuring the Oracle Audit Vault and Database Firewall system.

See Also:

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

7.2 Discovering and Registering Targets and Creating Groups

Learn about discovering and registering targets and creating groups.

7.2.1 Discovering Databases for Target Registration

Starting in Oracle AVDF 20.12, `super administrators` can import XML files resulting from the Nmap scan command of specified IP address and port ranges to determine which Oracle, Microsoft SQL, MySQL, DB2, PostgreSQL, or Sybase databases in your database fleet are yet to be registered with AVDF.

7.2.1.1 About Discovering Databases for Target Registration

Starting in Oracle AVDF 20.12, `super administrators` can import the XML file resulting from the Nmap scan command of specified IP address and port ranges to identify databases available for registration with AVDF. Discovered databases can then be assigned to `administrators` for registration with AVDF.

If you have many databases in your fleet, it may be difficult to determine which ones are not yet registered with Oracle AVDF. The Database Discovery feature introduced in Oracle AVDF 20.12 allows you to scan specified IP address and port ranges using Nmap commands to determine which databases haven't been registered with AVDF. The results of the Nmap scan will inform you which Oracle, Microsoft SQL, MySQL, DB2, PostgreSQL or Sybase databases have not been registered as targets.

The XML file that is the output of the Nmap scan command is the list of un-registered databases. This file can be imported to the Audit Vault Server console by a `super administrator` and each database can be either hidden from future scans or assigned to an `administrator` for target registration.

7.2.1.2 Executing Nmap Scan Commands

In order to use the Database Discovery feature available in Oracle AVDF starting in 20.12, you need to execute the Nmap scan command to discover un-registered databases in your database fleet. A `super administrator` will need to upload the results of the Nmap scan command to the Audit Vault Server.

Prerequisites

1. Contact your network administrator or check your organization's policies before executing Nmap scan command.
2. Download the Nmap command tool.
   Nmap Download

> **Note:**
>
> Only Nmap version 7.92 and 7.94 are supported.

Procedure

1. While on a Windows or Linux platform, run the following command on a host in your network:

```
nmap -sV -n -p T:<p1-p2> <ip range> --host-timeout <time in minutes>  -oX
<xml filepath>
```

   Attributes:

   - **sV** - Optional, Probes open ports to determine service/version information.
   - **n** - Optional, No DNS resolution. This option slashes scanning time
   - **p T:<p1 to p2>** - This option scans TCP protocol for port range p1 to p2.
     If you do not know the port range, it is recommended to scan the complete port range of 0 - 65536.

- **IP Range** - IP range that need to scanned. One example is given above, but for more type of ranges refer to the Nmap command documentation
- **host-timeout** - Enter a time in minutes after which the scan on the host will stop. Some hosts simply take a long time to scan. This may be due to poorly performing or unreliable networking hardware or software, packet rate limiting, or a restrictive firewall.
- **oX** - XML output file location

For example:

```
nmap -sV -n -p T:1430-6607 10.89.89.0-10.89.89.255 --host-timeout 2m -
oX /tmp/tmp.xml
```

2. Ensure that the XML file is accessible by a `super administrator`.

Related Topics

- Nmap documentation

7.2.1.3 Importing the XML File for Database Discovery as a `Super Administrator`

After successfully running the Nmap scan command, the XML file needs to be imported to the Audit Vault Server Console by a `super administrator`. Databases can then be assigned to `administrators` for registration.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Targets** tab.
3. In the left menu, click **Database Discovery**.
4. Click **Import Nmap XML**.
5. Click **Choose File**.
6. Navigate to location of the Nmap output file.
7. Click **Save** to import the XML file.
8. After the XML has been successfully imported, delete the XML file from your local system.

A `super administrator` will be able to see the list of databases discovered in the Nmap scan and their registration status with AVDF in **Database Discovery** in the Audit Vault Server Console.

Related Topics

- Viewing the Status of the XML Import Job
  Once the XML file has been imported, `administrators` can view the details and status of the Database Discovery job.

7.2.1.4 Assigning Databases for Registration in Database Discovery as a `Super Administrator`

After importing the XML file, a `super administrator` can see the list of discovered databases and their registration status with AVDF. A `super administrator` can then assign the unregistered databases to other `administrator` users for target registration.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Targets** tab.

3. In the left menu, click **Database Discovery**.
4. Select the database(s) you want to assign to an `administrator` for registration.
5. Click **Assign admin**.
6. Select the `administrator` user to assign the database(s) to.
   Select **Select** in the drop down of users if you'd like to unassign the database(s).
7. Click **Save**.

7.2.1.5 Registering Assigned Databases in Database Discovery

If you are an `administrator` with assigned databases or a `super administrator` you can register discovered databases with AVDF directly from **Database Discovery**.

1. Log in to the Audit Vault Server Console as a `super administrator` or an `administrator`.
2. Click the **Targets** tab.
3. In the left menu, click **Database Discovery**.
4. Select a database you want to register with AVDF.
   You can only select one database at a time.
5. Click **Register**.
6. Complete registration of the selected database.
   For more information see Registering or Removing Targets in Audit Vault Server.

7.2.1.6 Managing Discovered Databases as a `Super Administrator`

`Super administrators` can manage the table of discovered databases by either ignoring, showing, or deleting databases.

Ignore a Database

An ignored database will be listed in the **Ignored databases** report. Ignored database again can be moved to discovered databases list or deleted.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Targets** tab.
3. In the left menu, click **Database Discovery**.
4. Optional, apply or remove filters to the table.
5. Select the database(s) from the **Discovered databases** lists that you want to ignore.

> **Note:**
>
> Registered databases can't be ignored.

6. Click **Ignore**.
   All selected databases will be moved to the **Ignored databases** list.
7. Optional, leave a comment as to why the database(s) is to ignored.
8. Click **Save**.

Move Ignored Databases Back to Discovered List

An ignored database can be moved to discovered databases list.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Targets** tab.
3. In the left menu, click **Database Discovery**.
4. Optional, apply or remove filters to the table.
5. Select the database(s) from the **Ignored databases** list that you want to move back to the discovered databases.
6. Click **Move to discovered databases**.
   All selected databases will be moved to the discovered databases list.
7. Optional, leave a comment as to why the database(s) is being moved.
8. Click **Save**.

Delete a Database

A deleted database is removed from the table of discovered databases. However, if an XML file from the Nmap scan is imported again, any removed databases will once again show up in the table.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Targets** tab.
3. In the left menu, click **Database Discovery**.
4. Optional, apply or remove filters to the table.
5. Select the database(s) you want to delete.
6. Click **Delete**.

7.2.1.7 Viewing the Status of the XML Import Job

Once the XML file has been imported, `administrators` can view the details and status of the Database Discovery job.

1. Log in to the Audit Vault Server Console as an `administrator`.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. In the **Monitoring** section, click **Jobs**.
5. Find a **Database discovery job** to view the details.
6. Click the job details icon to see more details about the job including:
   - The user that performed the import
   - The time it took for the import to complete
   - The number of databases discovered on how many IP addresses

7.2.2 Registering or Removing Targets in Audit Vault Server

Learn about registering and removing targets in Audit Vault Server.

7.2.2.1 About Targets in the Audit Vault Server

Oracle Audit Vault and Database Firewall (Oracle AVDF) super administrators can create targets and grant other administrators access on those targets.

Administrators can also create targets, but the targets that they create are accessible only to the creator and to the super administrator who created the administrator.

The following guidelines apply when creating and accessing targets:

- Both super administrators and administrators can create targets.
- Super administrators can grant access on targets or target groups to specific administrators.
- Super administrators have access to all targets, and administrators have access only to those targets on which they have been granted access.

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

7.2.2.2 Registering Targets

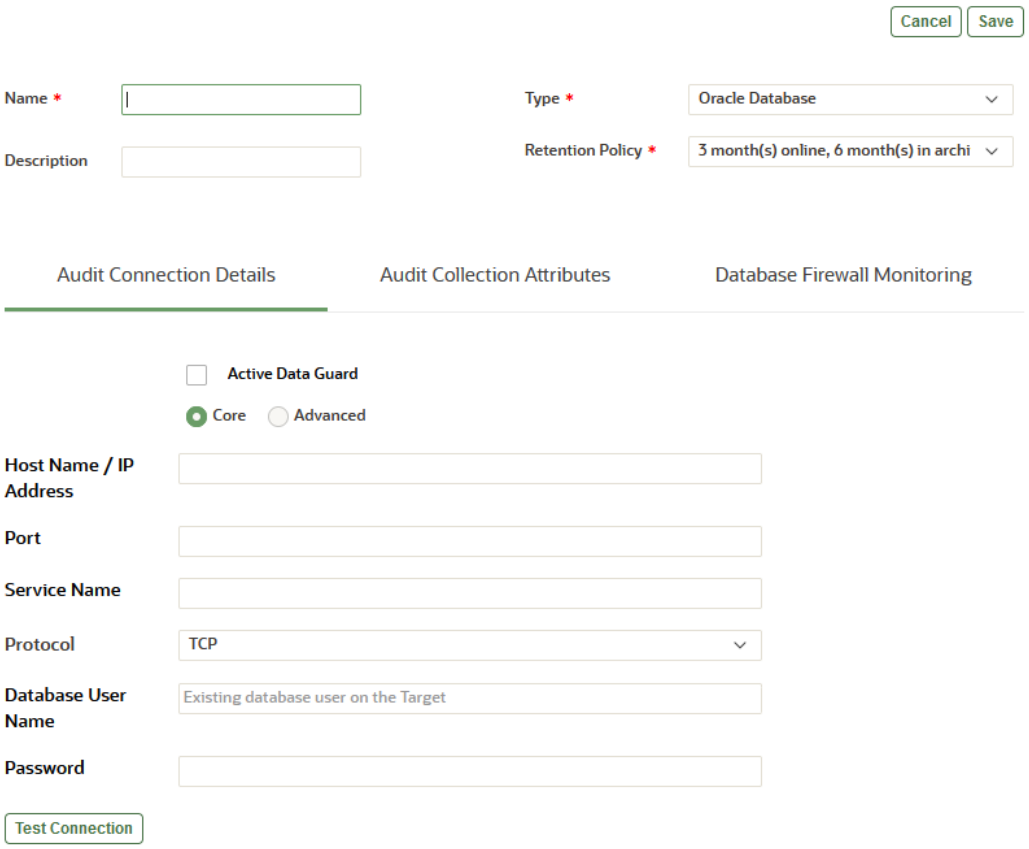
Before you can begin audit collection and Database Firewall monitoring, you need to register the targets that you want to audit or monitor.

Target Information

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

   Targets is selected in the left navigation menu by default. This page contains a list of configured targets. You can sort or filter the list of targets.
3. Click **Register** in the top, right corner.

   The following page appears:



4. Enter the name and optionally the description for the new target.
5. Select the target type from the **Type** drop-down list. For example, **Oracle Database**.
6. Starting with Oracle AVDF 20.7, select a policy from the **Retention Policy** drop-down list.

   This list displays all the pre-configured policies and user-defined policies from the **Archiving** tab. If the super administrator has set a user-defined policy as the default, then that policy is selected by default. Otherwise the default value is **3 month(s) online, 6 month(s) in archive**.

Audit Connection Details Tab

Enter the details to connect to the target.

The fields in this section change, depending on the target type. The following list describes all the possible fields and options that may appear.

1. **Active Data Guard**: For Oracle Database targets, select this check box if the target is an Active Data Guard database. For details, see Additional Information for Audit Collection from Oracle Active Data Guard.
2. **Core** (previously **Basic**) or **Advanced**: For database targets, select **Advanced** if you know the connection string. Otherwise, select **Core**.
3. **Host Name / IP Address**: You can use a virtual IP address.

> **Tip:**
>
> To improve the accuracy of using Database Discovery (available Oracle AVD 20.12 and later) to discover unregistered databases, host name/IP address should be provided. This will prevent a database from being falsely labeled as unregistered.

4. **Port**

> **Tip:**
>
> To improve the accuracy of using Database Discovery (available Oracle AVD 20.12 and later) to discover unregistered databases, port information should be provided. This will prevent a database from being falsely labeled as unregistered.

5. **Service Name**: If the target is an Oracle Database, enter the Oracle Database service name or SID.
6. **Protocol**: Select **TCP** or **TCPS**.
7. **Connection String** (previously **Target Location**): If you selected the **Advanced** option for a database target, enter the connection string or connection URL for the database. This connection string is required for the Audit Vault Agent to collect audit data, but it's not required to deploy the Database Firewall only.

> **Note:**
>
> - For Oracle Database, the string may look like the following: `jdbc:oracle:thin:@//<IP address of the Database server host>:<port number>/hrdb`
> - When you configure Oracle Real Application Clusters (Oracle RAC) as a target for Audit Vault Agent data collection, enter the SCAN listener host name.
> - If the target is a Microsoft SQL Server Cluster, you need to set a mandatory collection attribute. See Microsoft SQL Server Plug-in for Oracle Audit Vault and Database Firewall for details.

8. **Database User Name** (previously **User Name**): Enter the name of an existing database user that has access to the audit data that's generated on the target.

> **Note:**
>
> Only case insensitive database user names are supported for Oracle Database.

9. **Password**: Enter the password for the database user.
10. **Test Connection**: Starting with Oracle AVDF 20.10, for Oracle Database and Microsoft SQL Server targets, click this button to test the connection details that you just entered.

    If Oracle AVDF is unable to connect to the host or database, or if there are other issues, an error message displays more details so you can resolve the issue before continuing.

Audit Collection Attributes Tab

Enter audit collection attributes for the target.

1. Click **Add** to enter the attribute details in the **Name** and **Value** columns.

   The Audit Vault Agent may require collection attributes for some target types. The following table lists the mandatory collection attributes to enter for different target types.

Target Type	Mandatory Collection Attributes
Microsoft SQL Server Cluster	`av.collector.clusterEnabled`
PostgreSQL	`av.collector.securedTargetVersion`
Oracle Database for Transaction Log Audit Collection	`AV.COLLECTOR.TIMEZONEOFFSET` **Note:** This is the timezone offset of the Oracle Database.
Microsoft SQL Server for Transaction Log Audit Collection	`AV.COLLECTOR.TIMEZONEOFFSET` **Note:** This is the timezone offset of the SQL Server database.
MySQL for Transaction Log Audit Collection	`AV.COLLECTOR.TIMEZONEOFFSET` **Note:** This is the timezone offset of the MySQL database.

> **Note:**
>
> For PostgreSQL, enable the `pgaudit` extension. If this extension is disabled, the audit collection is incomplete and reports will be missing operational details.

2. Optionally use the following information to improve the audit collection rate or effectively utilize the resources of the Audit Vault Agent and Audit Vault Server.

> **Note:**
>
> This functionality is not applicable to the Host Monitor Agent or network trails.

- Starting in Oracle AVDF 20.4, you can improve audit collection performance and increase the audit collection rate by setting the `av.collfwk.MULTI_THREADED` attribute to `true`.

  This applies to all audit trails belonging to the target. While this configuration improves the audit collection rate, the resource (CPU and memory) requirements on the Audit Vault Agent machine also increase. There may also be an increase in resource utilization on the Audit Vault Server. Oracle recommends that you use this configuration if the target audit record generation rate is between 86 and 172 million records per day (or between 1000 to 2000 records per second).
- Starting In Oracle AVDF 20.5, the Audit Vault Agents automatically choose the best possible configuration for improving audit collection rate. This dynamic multithreaded collector functionality effectively utilizes the resources of the Audit Vault Server and Audit Vault Agent.

This functionality is the default behavior and increases the throughput of the audit trail by increasing the number of threads when the target audit generation rate is high. It also reduces the number of threads when the target audit generation rate is low. This functionality improves the audit collection rate and can support targets generating records up to 2000 per second or 172 million per day. When the target audit generation rate is very high, the resource (CPU and memory) requirements on the Audit Vault Agent machine also increase. There may also be an increase in resource utilization on the Audit Vault Server.

Oracle recommends that you avoid setting the `av.collfwk.MULTI_THREADED` attribute and rely on the dynamic multithreaded collector functionality.

If high throughput is not required due to Audit Vault Agent machine resource constraints, then use the single-threaded collector by setting the `av.collfwk.MULTI_THREADED` attribute to `false`. This is the default behavior in Oracle AVDF 20.5 and earlier.

If high throughput is always required due to an audit data generation rate of 86 to 172 million records per day, then use the static multithreaded collector (always uses maximum threads) by setting the `av.collfwk.MULTI_THREADED` attribute to `true`.

3. If you're configuring audit collection, click **Save** to complete the target registration.

   To configure Database Firewall monitoring, continue with the remaining steps.

Database Firewall Monitoring Tab

Enter Database Firewall monitoring details.

1. Click **Add**.
2. In the **Database Firewall Monitor** dialog box, enter the following information on the **Core** tab (previously **Basic**):
   a. **Database Firewall**: Select a value from the list.
   b. **Mode**: Select one of the following deployment modes:
      - **Monitoring (Out-of-Band)**: The Database Firewall can monitor and alert on SQL traffic, but it can't block or substitute SQL statements.
      - **Monitoring (Host Monitor)**: The Database Firewall can monitor and alert on SQL traffic, but it can't block or substitute SQL statements.
      - **Monitoring / Blocking (Proxy)**: The Database Firewall can block or substitute SQL statements.

      > **Note:**
      >
      > Ensure that you select the right mode in accordance with the Database Firewall policy defined for the target. If the Database Firewall policy contains SQL blocking rules, but you select a mode for monitoring only, SQL statements are not blocked. Therefore, if you want to block SQL statements according to policy rules, use **Monitoring / Blocking (Proxy)** mode.

      For more information about deployment modes, see Introduction to Database Firewall Deployment.

   c. **Network Interface Card**: Select a value from the list.
   d. **Proxy Ports**: Select a value from the list.

> **Note:**
>
> For an Oracle RAC instance, select the network interface card (NIC) and proxy ports if you selected **Monitoring / Blocking (Proxy)** mode. The proxy port is not mandatory for monitoring-only modes.

3. If the target is Oracle Real Application Clusters (Oracle RAC), select the **RAC Instance/ Autonomous DB** check box (**RAC Instance** check box in Oracle AVDF 20.7 and earlier).

> **Caution:**
>
> If you set up an Oracle RAC protected database to be a scan listener, you also need to select the **RAC Instance/Autonomous DB** check box when registering the database as a target. If you don't identify the target as a RAC database, the scan listener could redirect the client to a different IP address, bypassing the Database Firewall entirely.

4. In the **Connection Details** section, click **Add** to add a target.

   Enter the following information for each available connection to the database:

   - **Host Name / IP Address**
   - **Port**
   - **Service Name** (Optional, for Oracle Database only)
     For **Monitoring Only (Host-Monitor)** and **Monitoring Only (Out-Of-Band)** mode, you can enter multiple SIDs or service names, each on a separate line. For **Monitoring/ Blocking (proxy-mode)** mode,
     - Oracle AVDF 20.1-20.9: You need to configure a proxy target for each OSN. This is because a single proxy port cannot service multiple OSN's on the same target database. Add more traffic proxy ports as required.
     - Oracle AVDF 20.10 and later: You can use one proxy port and specify multiple OSN's on the target database that are going to be processed. Specify the OSN's in a list delimited by the "|" character. For example, target1|target2|target 3.

     If you provide a service name or SID, Database Firewall applies policies only to the sessions that match that service name or SID. All other traffic is ignored by default. In **Monitoring/Blocking(proxy-mode)** mode, that traffic is passed to the target database. Starting with Oracle AVDF 20.8, you can block those sessions by selecting the **Block Traffic for Unregistered Service Names** check box on the **Advanced** tab.

5. Click the **Advanced** tab.
6. Enter a number for **Database Firewall Monitor Threads**.

   The minimum and default value is 1. This controls the number of traffic handling threads in the Database Firewall monitoring point. Use due caution before modifying this value.

7. If the target database is an Oracle Database and **Mode** is set to **Monitoring / Blocking (proxy)**, optionally select the **Block Traffic for Unregistered Service Names** check box to have the Database Firewall block sessions that use service names other than the one that is configured in the target **Connection Details** section.
8. If the database client and server are communicating over the TLS protocol, enable TLS.

   With this option, the Database Firewall acts as a TLS proxy. It serves as a TLS server for the database client and acts as a TLS client to the database server. The Database Firewall

and the Audit Vault Server have access to the decrypted SQL traffic for further analysis. This feature applies only for Database Firewalls that are deployed in **Monitoring / Blocking (Proxy)** mode.

a. Select **Enable TLS support**.

> **Note:**
>
> If you select this option, the **Decrypt With Native Network Encryption Key** check box is hidden.

b. In Oracle AVDF release 20.8 and later, select the certificate type under **Inbound TLS (From client to DBFW)**.

   The TLS protocol uses the certificate to authenticate the communication participant. You can use the default certificate that is signed by the Database Firewall or a certificate that is signed by an external Certificate Authority (CA).

c. If you use the default self-signed certificate, then click **Download DBFW Certificate**.

   You need to install this certificate on the database client to enable Database Firewall authentication.

d. If you use the external CA signed certificate, then select the certificate from the drop-down list.

e. Select the cipher suite level.

   Level 4 - strongest, is the default.

   Starting with Oracle AVDF 20.13, Oracle Database 23ai is supported as a target which supports TLSv1.3 and TLSv1.2. However, Oracle AVDF does not support TLSv1.3 so you will have to modify the `sqlnet.ora` file of your Oracle Database 23ai to support TLSv1.2 by either removing the `SSL_VERSION` parameter or explicitly listing TLSv1.2 in the `SSL_VERSION` parameter. See Specifying TLS Protocol and TLS Cipher Suites in the *Oracle Database Security Guide* for more information.

f. If you don't need database client authentication, then deselect **Client Authentication**.

   This option is available only for the inbound connection. The outbound connection is always authenticated. If you deselect this option, the **Client Trusted Certificates** button is disabled.

g. To manage certificates for client authentication, click **Client Trusted Certificates**.

h. Click **Choose File** and select the certificate on the local machine.

i. Click **Open** to load the certificate and add it to the Database Firewall.

   The details of the uploaded certificate appear in the dialog box.

j. Click **Cancel** to exit the dialog box.

k. Follow a similar process to select and manage certificates and the cipher suite level under **Outbound TLS (From DBFW to Database)**.

   To manage the certificates for server authentication, click **Database Trusted Certificates**.

9. If Oracle Database uses native network encryption, select **Decrypt With Native Network Encryption Key** to enable the decryption of traffic.

> **Note:**
>
> If the **Enable TLS support** check box is selected, the **Decrypt With Native Network Encryption Key** check box is hidden.
>
> For Oracle AVDF release 20.5 and earler, the check box is **Decrypt With Network Native Encryption Key**.

This option also supports the retrieval of session information for Oracle Database. Complete the remaining fields as applicable.

For Oracle Real Application Clusters (Oracle RAC) targets (if the **RAC Instance/ Autonomous DB** check box is selected on the **Core** tab), enter the SCAN Listener IP address.

(In Oracle AVDF 20.7 and earlier, it's the **RAC Instance** check box, and in Oracle AVDF 20.2 and earlier, it's the **Basic** tab.)

For Oracle standalone database targets, enter the IP address of the database listener.

For Sybase SQL Anywhere (Oracle AVDF 20.1-20.6 only) and Microsoft SQL databases, the field is **Retrieve session information from target DB**. Retrieving session information is not available for any other non-Oracle database types.

> **Note:**
>
> Ensure that the Database Firewall is allowed to make a network connection to the database listener.

10. Optionally select the **Capture Database Response** check box to have the Database Firewall monitor the SQL response from the database.
11. Optionally select the **Full Error Message** check box to capture the database response codes and error codes.
12. Click **Save** in the dialog box to save the configuration for the monitoring point.
13. Click **Save** on the main page to save the target.

> **Note:**
>
> TCPS must be configured for registering Hybrid Cloud Oracle Databases. See Securing the Agent and Oracle Database Target Connection.

Note:

After registration is complete for Oracle Database targets, the following jobs are automatically submitted.

- Audit policy retrieval job
- User entitlement retrieval job
- Security assessment
- Sensitive objects retrieval job
- Stored procedure auditing

See Viewing and Changing Settings for a Target for more details about these jobs.

See Also:

- Plug-ins That are Shipped with Oracle Audit Vault and Database Firewall
- Audit Collection Attributes to look up requirements for a specific target type.
- Using Oracle Database Firewall with Oracle RAC to configure Oracle Database Firewall in an Oracle RAC environment.
- Working with Lists of Objects in the Audit Vault Server Console to sort or filter the list of targets.
- Target Locations (Connect Strings)
- Using Audit Vault Server Console
- Setting User Account Privileges on Targets
- Monitoring Jobs
- Assessment Reports

7.2.2.3 Modifying Targets

You can modify a target after it's been registered.

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

   Targets is selected in the left navigation menu by default. This page contains a list of configured targets. You can sort or filter the list of targets.
3. Click the name of the target that you want to modify.
4. You can update the name, decription, and retention policy of the target.
5. To modify the target's **Audit Connection Details** or **Audit Collection Attributes**, click **Modify**.
6. Made your changes.
   - Starting with Oracle AVDF 20.10, if you change audit connection details for an Oracle Database or Microsoft SQL Server target, click the **Test Connection** button to test the connection details that you just entered.

If Oracle AVDF is unable to connect to the host or database, or if there are other issues, an error message displays more details so you can resolve the issue before continuing.

7. Click **Save**.

> **Note:**
>
> If you change the name of a target, it will have the following affects:
>
> - The new name won't appear in Oracle Audit Vault and Database Firewall reports until you restart the Audit Vault Agent.
> - There will not be duplicates enteries for the modified target because the `secured_target_id` will remain the same. Additionally, there will be no impact to the audit trails or retention policies for the target.
> - In the Event log and Alerts table, the target name will not get changed for old events, but new events will get logged with new target name. So it recommended that if you are querying the Event log or Reports for any targets, that you use `secured_target_id` to get all the entries for the target, instead of the target name.

Related Topics

- Registering Targets
- Working with Lists of Objects in the Audit Vault Server Console
- Using Audit Vault Server Console

7.2.2.4 Removing Targets

Learn about removing targets.

If you no longer need to have a target registered with Oracle Audit Vault and Database Firewall, then you can use either the console or the command-line utility to remove the target. After you have removed the target, the audit data pertaining to the target still resides in the data warehouse within its retention period (according to the archiving policy).

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

To remove a target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab.
3. The **Targets** tab in the left navigation menu is selected by default. Select the check boxes against the targets that you want to remove.
4. Click **Delete** button in the top right corner of the page.

> **See Also:**
>
> - Creating and Deleting Archive and Retention Policies for information on archiving (retention) policies.

7.2.3 Creating a Target Group

Learn how to create target groups.

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

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Targets** tab.
3. In the left navigation menu, click **Target Groups**.
4. Click **Create** button in the top right corner.
5. In the **Create Target Group** dialog, do the following:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. **Name** field: Enter a name for the target group. b. **Description**: Optionally, enter a description for this target group. c. Under **Members** section, select one or more members by clicking the check box against the member name. d. Click the **Add** button.	a. **Group Name** field: Enter a name for the target group. b. **Description**: Optionally, enter a description for this target group. c. Under **Members** section, select one or more members by moving them from the **Available** column to **Selected** column. You can also search for the targets in the field below the **Members** section using the target name. d. To remove the targets, select one or more members and move them back to the **Available** column from the **Selected** column.

6. Click **Save**.

7.2.4 Modifying a Target Group

You can modify the contents of a target group or change the target group name and description.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Targets** tab.
3. In the left navigation menu, click **Target Groups**.
4. Click the name of the target group that you want to modify.
5. In the **Modify Target Group** dialog, perform any of the following modifications:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Change the **Name** of the target group. b. Optionally edit the **Description**. c. Under the **Members** section, add or remove members by selecting the check box against the member. d. Click **Add** or **Remove** buttons accordingly.	a. Change the **Group Name**. b. Optionally edit the **Description**. c. Under the **Members** section, add or remove members by moving them in between the **Available** and **Selected** columns. You can also search for the targets in the field below the **Members** section using the target name.

6. Click **Save**.

7.2.5 Controlling Access to Targets and Target Groups

Learn about controlling access to targets and target groups.

Oracle Audit Vault and Database Firewall super administrators can control which administrators have access to targets or target groups. You can control access for an individual user or for an individual target or group.

> **See Also:**
>
> Managing User Access Rights to Targets and Groups

7.2.6 Moving a Target from One Host Machine to Another

Learn how to handle when a target is moved from one host machine to another.

There are a few changes to be made in Audit Vault Server console when a target is moved from one host machine to another. This depends on the type of the Audit Vault Agent.

An Audit Vault Agent can be of two types:

1. When the Audit Vault Agent is installed on the target host machine, it is called as a local Agent.
2. When the Audit Vault Agent is not installed on the target host machine and is installed remotely, it is called as a remote Agent.

The following table contains the configuration and the steps to be followed in the Audit Vault Server console when the target is moved from one host machine to another.

> **Note:**
>
> Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was desupported in Oracle AVDF release 20.8
>
> Sybase SQL Anywhere was desupported in Oracle AVDF release 20.8
>
> Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

Agent Type	Trail Type	Target Type	Steps in Audit Vault Server Console
Local	TABLE	Oracle Database Oracle Key Vault Sybase ASE	**Step 1:** Update the target **Connection Details** by following these steps: 1. Log in to the Audit Vault Server console as an *administrator*. 2. Click the **Targets** tab. The **Targets** tab in the left navigation menu is selected by default. 3. Select and click the specific target. 4. In the **Database Firewall Monitoring** section on the main page, click to modify the connection details. The **Database Firewall Monitor** dialog is displayed. 5. Modify and update the **Connection Details** in the dialog. 6. Click **Save**. 7. Click **Save** in the main page. **Step 2:** Delete existing trail by following these steps: 1. Click the **Targets** tab. 2. Click **Audit Trails** in the left navigational menu. 3. Select the specific audit trail and click **Stop**. 4. Click **Delete**. **Step 3:** Create a new trail and configure the Audit Vault Agent installed on the new host machine. Refer to Adding Audit Trails with Agent-Based Collection
Local	DIRECTORY SYSLOG EVENT LOG TRANSACTION LOG	Oracle Database	**Step 1:** Update the target **Connection Details**. **Step 2:** Delete the existing trail. **Step 3:** Create a new trail by configuring the Audit Vault Agent installed on the new host machine and using the new trail location of the new host machine.

Agent Type	Trail Type	Target Type	Steps in Audit Vault Server Console
Local	DIRECTORY SYSLOG EVENT LOG TRANSACTION LOG	MySQL Microsoft SQL Server PostgreSQL IBM DB2 Quick JSON Oracle Solaris Linux IBM AIX Microsoft Windows Microsoft Active Directory Oracle ACFS	**Step 1:** Delete the existing trail. **Step 2:** Create a new trail by configuring the Audit Vault Agent installed on the new host machine and using the new trail location of the new host machine.
Local	NETWORK	Oracle Database MySQL Microsoft SQL Server IBM DB2 Sybase ASE Sybase SQL Anywhere	**Step 1:** Delete the existing trail. **Step 2:** Create a new trail by configuring the Audit Vault Agent installed on the new host machine.
Remote	TABLE	Oracle Database Oracle Key Vault Sybase ASE	**Step 1:** Update the target **Connection Details**. **Step 2:** There is no need to delete and recreate the trails. Stop the existing trail. **Step 3:** Start the trail.
Remote	DIRECTORY SYSLOG EVENT LOG TRANSACTION LOG	Oracle Database	**Step 1:** Update the target **Connection Details**. **Step 2:** In case the trail location has changed, then delete the existing trail. **Step 3:** Create a new trail and specify the new trail location.
Remote	DIRECTORY SYSLOG EVENT LOG TRANSACTION LOG	MySQL Microsoft SQL Server PostgreSQL IBM DB2 Quick JSON Oracle Solaris Linux IBM AIX Microsoft Windows Microsoft Active Directory Oracle ACFS	**Step 1:** In case the trail location has changed, then delete the existing trail. **Step 2:** Create a new trail and specify the new trail location.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

7.3 Preparing Targets for Audit Data Collection

Learn about preparing targets for audit data collection.

7.3.1 Using an NTP Service to Set Time on Targets

Learn how to use NTP Service to configure time settings on targets.

Oracle recommends that you use an It is recommended that you also use a Network Time Protocol (NTP) service on both your targets and the Audit Vault server. This will help to avoid confusion on timestamps on the alerts raised by the Audit Vault Server.

> **See Also:**
>
> Specifying the Server Date, Time, and Keyboard Settings for instructions on using an NTP server to set time for the Audit Vault Server.

7.3.2 Ensuring that Auditing is Enabled on the Target

Learn how to enable auditing.

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

To check if auditing is enabled on an Oracle Database 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 Audit Vault and Database Firewall.

7.3.3 Setting User Account Privileges on Targets

Some target types require credentials for Oracle Audit Vault and Database Firewall (Oracle AVDF) to access them.

If you plan to collect audit data from a target, perform stored procedure auditing (SPA) or entitlements auditing, or monitor native network encrypted traffic for Oracle Database, then you must create a user account on the target with the appropriate privileges to enable Oracle AVDF to access the required data.

For database targets, Oracle AVDF provides scripts to configure user account privileges for database target types. For Oracle Database targets, you can download the setup scripts from the Audit Vault Server console by clicking the **Target Setup Script** button on the **Targets** tab.

For non-database targets, create a user that has the appropriate privileges to access the audit trail. For example, for a Windows target, this user must have administrative permissions to read the security log.

> **Note:**
>
> Oracle AVDF does not accept user names with quotation marks. For example, "J'Smith" is not a valid user name for an Oracle AVDF user account on targets.

See Scripts for Oracle AVDF Account Privileges on Targets for information on the scripts to configure user account privileges for database target types.

7.3.4 Scheduling Audit Trail Cleanup

Learn about scheduling audit trail cleanup.

Oracle AVDF supports audit trail cleanup for Oracle Database, Microsoft SQL Server, IBM DB2, and MySQL.

> **See Also:**
>
> Audit Trail Cleanup

7.4 Preparing Targets for Use With Global Sets (Previously Called Data Discovery)

Starting with Oracle AVDF 20.9, you can create global sets of privileged users and sensitive objects on your Oracle Databases as part of Data Discovery (Oracle AVDF 20.9) or Global Sets (Oracle AVDF 20.10 and later).

In order to create these global sets, privileged users and sensitive objects need to be discovered on your Oracle Database by adding privileges to the database user and gathering statistics, respectively.

Related Topics

- Global Sets/Data Discovery

7.4.1 Prerequisites for Enabling Global Sets or Data Discovery

Complete these prerequisites before enabling Global Sets or Data Discovery in Oracle Audit Vault and Database Firewall.

- Update Oracle AVDF to release 20.10 or later for Global Sets. Update to Oracle AVDF to release 20.9 for Data Discovery. See Patching Oracle Audit Vault and Database Firewall Release 20 or Upgrading Oracle Audit Vault and Database Firewall from Release 12.2 to Release 20.
- If you don't have an existing user for auditing, create a user account for Oracle Audit Vault and Database Firewall on the Oracle Database. For example:

  ```
  SQL> CREATE USER username IDENTIFIED BY password
  ```

  You will use this user name and password when registering this Oracle Database as a target in the Audit Vault Server.
- Add the Oracle Database as a target in the Audit Vault Server. See Registering or Removing Targets in Audit Vault Server

7.4.2 Managing Privileges for Discovering Privileged Users

Before global Privileged User Sets can be used, download and run the target setup script on the Oracle Database to add privileges to the user as follows.

Downloading Oracle Database Setup Scripts

To download the scripts from the Audit Vault Server console:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab.
3. Click the **Target Setup Script** button.

Download and run the target setup script on the Target Oracle database to add privileges to the user.

You can also access the scripts in the following directory (Linux example):

```
/opt/avdf/defaultagent/av/plugins/com.oracle.av.plugin.oracle/config/
```

Enabling User Privileges for Oracle Database for Discovering Privileged Users

To add the required privileges, run the setup scripts from the previous steps:

> **Note:**
>
> The downloaded zip file contains SQL scripts for several functions, this workflow is only to enable the discovery of privileged user.

1. Connect as the `SYS` user with the `SYSDBA` privilege. For example:

   ```
   SQL> CONNECT SYS / AS SYSDBA
   ```

2. Run the following script:

   ```
   SQL> @oracle_user_setup.sql username DBSAT_DISCOVERY
   ```

Revoking User Privileges for Oracle Database for Discovering Privileged Users

To disable discovery of privileged users for the target, revoke the privileges of the user:

1. Connect to the database as the `SYS` user with the `SYSDBA` privilege.
2. Run the following script:

   ```
   SQL> @oracle_drop_db_permissions.sql username DBSAT_DISCOVERY
   ```

7.4.3 Managing Statistics Gathering for Discovering Sensitive Objects

Before global Sensitive Object Sets can be used, statistics need to be gathered on the Oracle Database.

1. Connect as the `SYS` user with the `SYSDBA` privilege. For example:

   ```
   SQL> CONNECT SYS / AS SYSDBA
   ```

2. Run this command:

   ```
   exec DBMS_STATS.GATHER_DATABASE_STATS
   ```

   Alternatively, you can run the `DBMS_STATS` procedure for all objects in a particular schema:

   ```
   exec DBMS_STATS.GATHER_SCHEMA_STATS(schema_name);
   ```

> **Note:**
>
> To invoke this procedure you must be the owner of the table, or you need the `ANALYZE ANY` privilege. For objects owned by `SYS`, you must be either the owner of the table, or you need the `ANALYZE ANY DICTIONARY` privilege or the `SYSDBA` privilege.

7.5 Using SQL Firewall with AVDF

Starting with Oracle AVDF 20.13, you can use AVDF to collect SQL Firewall violation logs on Oracle Database 23ai targets.

SQL Firewall is part of the Oracle Database kernel, see Using Oracle SQL Firewall in the *Oracle Database Security Guide* for detailed information about the capabilities and configuration of SQL Firewall.

Prerequisites

Complete these prerequisites before using SQL Firewall in Oracle Audit Vault and Database Firewall.

- Update Oracle AVDF to release 20.13 or later for SQL Firewall. See Patching Oracle Audit Vault and Database Firewall Release 20 or Upgrading Oracle Audit Vault and Database Firewall from Release 12.2 to Release 20.
- If you don't have an existing user for auditing, create a user account for Oracle Audit Vault and Database Firewall on the Oracle Database. For example:

  ```
  SQL> CREATE USER username IDENTIFIED BY password
  ```

  You will use this user name and password when registering this Oracle Database as a target in the Audit Vault Server.
- Add the Oracle Database 23ai as a target in the Audit Vault Server. See Registering or Removing Targets in Audit Vault Server

Grant Privileges to the AVDF User

Before SQL Firewall can be used with AVDF, download and run the target setup script on the Oracle Database to add privileges to the user as follows.

1. Download the Oracle Database setup script:
   a. Log in to the Audit Vault Server console as an administrator.
   b. Click the **Targets** tab.
   c. Click the **Target Setup Script** button.
2. Run the setup script:

   > **Note:**
   >
   > The downloaded zip file contains SQL scripts for several functions, this workflow is only to provide privileges for SQL Firewall.

   a. Connect as the `SYS` user with the `SYSDBA` privilege. For example:

   ```
   SQL> CONNECT SYS / AS SYSDBA
   ```

   b. Run the following script:

   ```
   SQL> @oracle_user_setup.sql username SQL_FIREWALL
   ```

   > **Note:**
   >
   > The `SQL_FIREWALL` privilege provides administrator access for all SQL Firewall actions on the Oracle Database. AVDF will use this privilege only for collecting and, if enabled, purging of SQL Firewall violation logs.

Start the SQL Firewall Violations Audit Trail

Use the procedure documented in Configuring and Managing Audit Trail Collection to start the `SYS.DBA_SQL_FIREWALL_VIOLATIONS` audit trail.

Enable Automated Cleanup of the SQL Firewall Violation Logs

If the `av.collector.enable_trail_cleanup` audit collection attribute is set to `yes`, then SQL Firewall violation logs that are over one week old with be purged from the database automatically. This purge job will run once every 24 hours, running for the first time after the `SYS.DBA_SQL_FIREWALL_VIOLATIONS` audit trail has been running continuously for 24 hours.

See Modifying Targets and Audit Trail Cleanup for more information on how to set the audit collection attribute.

Related Topics

- Oracle Database Setup Scripts
  Download and use these scripts to set up user account privileges for Oracle Audit Vault and Database Firewall (Oracle AVDF) to audit Oracle Database targets.

7.6 Configuring and Managing Audit Trail Collection

Learn about configuring and managing audit trail collection.

7.6.1 Prerequisites for Adding Audit Trails in Oracle Audit Vault Server

Complete these prerequisites before adding audit trails in Oracle Audit Vault Server.

- To configure transaction log audit trails for Oracle Database, Microsoft SQL Server, or MySQL install Oracle GoldenGate. See the Transaction Log Audit Data Collection for Oracle Database, Microsoft SQL Server, and MySQL for more information.
- Add the target in the Audit Vault Server. See Registering or Removing Targets in Audit Vault Server.
- Register the host machine. This machine is where the Audit Vault Agent is deployed and the target resides for directory trails. See Registering Hosts and Deploying the Agent.
- If you're deploying the Audit Vault Agent, deploy and start the Audit Vault Agent on the host machine. See Deploying the Audit Vault Agent on Host Computers.

> **Note:**
>
> Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20. See Adding Audit Trails with Agentless Collection.

- For IBM DB2 targets, ensure that the binary audit file has been converted to ASCII format before starting an audit trail.
- For MySQL targets, run the XML transformation utility. See Running the XML Transformation Utility for MySQL Audit Formats.

7.6.2 Adding Audit Trails with Agentless Collection

Starting in Oracle AVDF 20.9, you can use agentless collection instead of the Audit Vault Agent for up to 20 Oracle Database table audit trails. Starting in Oracle AVDF 20.10, you can also use agentless collection for Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events). The total number of audit trails for agentless collection should not exceed 20.

With agentless collection, you use the agentless collection service that comes with the Audit Vault Server instead of deploying the Audit Vault Agent on the target host machines. The agentless collection service is automatically installed when you install the Audit Vault Server or when you update Oracle AVDF to release 20.9 or later.

> **Note:**
>
> - From Oracle AVDF 20.9 to 20.12, agentless collection was supported only on a standalone, unpaired Audit Vault Server (AVS). If the Audit Vault Server was paired for high availability, the agentless collection service would stop running. Starting in Oracle AVDF 20.13, agentless collection is supported on both standalone and high availability AVS

Prerequisites

1. Update Oracle AVDF to the latest release update based on the following requirements:
   - For Oracle Database table audit trails, update to Oracle AVDF 20.9 or later.
   - For Microsoft SQL Server directory audit trails for `.sqlaudit` and `.xel` (extended events) targets, update to Oracle AVDF 20.10 or later.

   For update instructions, see one of the following chapters:
   - To update Oracle AVDF 20 to the latest release update, see Patching Oracle Audit Vault and Database Firewall Release 20.
   - To upgrade from Oracle AVDF 12 to Oracle AVDF 20, see Upgrading Oracle Audit Vault and Database Firewall from Release 12.2 to Release 20.
2. Ensure that the Audit Vault Server is not paired for high availability. To unpair the Audit Vault server, see Unpair Primary and Standby Audit Vault Servers.
3. Register the Oracle Database or Microsoft SQL Server target. See Registering Targets.
4. Prepare the target. See Preparing Targets for Audit Data Collection.

Agentless Collection Support for Microsoft SQL Server

Starting with Oracle AVDF 20.10, ensure that Microsoft SQL Server targets meet the following conditions for agentless collection support:

- Agentless and remote collection are supported for the following versions of Microsoft SQL Server:
  - `.sqlaudit` audit events: All supported versions of Microsoft SQL Server.
  - `.xel` audit events: Microsoft SQL Server 2017 and later.

- Agentless and remote collection are not supported in Microsoft SQL Server clustered environments.
- Agentless and remote collection may be slow when there's a large number of files. In this case, Oracle recommends that you use local, agent-based collection.
- Audit trail cleanup (ATC) is not supported for agentless and remote collection.

  You need to set up the file rollover count properly so that the audit file is purged automatically and doesn't lose audit data. See the Microsoft SQL Server documentation for more information about the file rollover count.

Procedure

1. Click the **Targets** tab.
2. Click the link for the Oracle Database or Microsoft SQL Server target for which you want to add the audit trail.
3. Under **Audit Data Collection**, click **Add**.
4. For **Audit Trail Type**, select one of the following values:
   - For Oracle Database, select **TABLE**.
   - For Microsoft SQL Server, select **DIRECTORY**.

   For details on these audit trail types, see the plug-in reference:
   - Oracle Database Plug-in for Oracle Audit Vault and Database Firewall
   - Microsoft SQL Server Plug-in for Oracle Audit Vault and Database Firewall
5. In the **Trail Location** field, enter or select the location of the audit trail on the target computer.

   For example:
   - Oracle Database example: `UNIFIED_AUDIT_TRAIL`
   - Microsoft SQL Server examples: *`directory_path`*`\*.sqlaudit` or *`directory_path`*`\*.xel`
6. Select **Agentless Collection**. This option is only visible for Oracle Database TABLE trails and Microsoft SQL Server DIRECTORY trails.
7. Click **Save**.
   The agent name for the audit trail appears as **Agentless Collection** on the **Audit Trails** and **Targets** pages.

7.6.3 Adding Audit Trails with Agent-Based Collection

To begin collecting audit data with the Audit Vault Agent, configure an audit trail for each target that's registered on the Audit Vault Server and then start the audit trail collection.

> **Note:**
>
> When using the Audit Vault Agent to collect directory trails, the agent must be installed on the same host that contains the directory.

1. Create a new target.

2. Click the **Targets** tab.
3. Click the link for the target for which you want to add the audit trail.
4. Under **Audit Data Collection**, click **Add**.
5. For **Audit Trail Type**, select one of the following trail types:.
   - CUSTOM
   - DIRECTORY
   - EVENT LOG
   - NETWORK
     For monitoring multiple nodes of an Exadata or RAC database using network trail, create a separate target for each node.
   - SYSLOG

     This trail type can collect from `syslog` or `rsyslog` files. If both are present, you must provide the exact trail location in the next step if you want to collect audit data from `rsyslog` files.

     > **Note:**
     >
     > Ensure that records generated by rsyslog have the same time zone information as the Audit Vault Agent that's running on the collection host.

   - TABLE
   - TRANSACTION LOG

   > **Note:**
   >
   > For details on which types of audit trails can be collected for each target type, see Table C-22.
   >
   > For complete details on all audit trail types, see Plug-ins That are Shipped with Oracle Audit Vault and Database Firewall.

6. In **Trail Location**, enter the location of the audit trail on the target computer. The trail location depends on the type of target.

   For example, for Oracle Database, the trail location might be `unified_audit_trail`.

   For supported trail locations, see Audit Trail Locations.

   > **Note:**
   >
   > If you select `DIRECTORY` or `TRANSACTION LOG` for **Audit Trail Type**, then the trail location must be a directory mask.

7. Select **Agent-based Collection** if it's visible. If it's not visible, then agent-based collection is used by default for the audit trail.
8. For **Agent Host**, select the host computer where the Audit Vault Agent is deployed.
9. Click **Save**.

The audit trail should now appear on the **Audit Trails** tab. The collection status is stopped (a red circle) initially. The audit trail starts automatically shortly after you add it.

> **See Also:**
>
> About Plug-ins

7.6.4 Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server

Lean about stopping, starting, and setting up autostart of audit trails in Oracle Audit Vault Server.

An audit trail starts automatically shortly after you add it. To start an audit trail, the Audit Vault Agent must be running on a host computer.

Audit trails that are started will automatically restart if the Audit Vault Agent is restarted, or updated due to an Audit Vault Server update.

An audit trail can go down at times such as when the target goes down temporarily. With Autostart, the system automatically attempts to restart an audit trail if it goes down. Autostart is normally enabled unless you have manually stopped the trail. You can set parameters on when and how many times the system attempts Autostart using the AVCLI utility.

Starting with AVDF 20.10, audit trails are monitored daily. Alerts are generated and email notifications are sent if audit trail is in `STOPPED_ERROR` state even after 20 retries.

Starting with AVDF 20.10, network trails are monitored hourly. Alerts are generated and email notifications are sent out if network trail is in `STOPPED_ERROR` state.

To start or stop audit trail collection for a target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab. The **Targets** tab in the left navigation menu is selected by default.
3. Select the specific target by clicking on the name.
4. Under the **Audit Data Collection** section, select the targets that have the audit trails that you want to start or stop.
5. Click **Stop** or **Start** accordingly.

> **Note:**
>
> - You cannot start an audit trail while the Audit Vault Agent is updating.
> - If your environment has a large number of audit files to collect, for example one million or more, then the audit trail may take a few minutes to start.

> **See Also:**
>
> - ALTER SYSTEM SET to set parameters on when and how many times the system attempts Autostart using the AVCLI utility.
> - Deploying the Audit Vault Agent on Host Computers
> - Updating Audit Vault Agent
> - Using Audit Vault Server Console

7.6.5 Checking the Status of Trail Collection on the Audit Vault Server

Learn about checking the status trail collection in Audit Vault Server.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab. The **Targets** tab in the left navigation menu is selected by default.
3. Click **Audit Trails** tab in the left navigation menu.

   It lists targets that have audit trails configured. Check the **Collection Status** column. The status can be one of the following:

   - Idle - Trail is up and running, no new audit data to collect. In this state, the trail is waiting for the target to generate new audit data.
   - Starting - Collection process is starting.
   - Collecting - Trail is currently actively collecting audit data.
   - Stopping - Collection process is stopping.
   - Stopped - Trail is currently stopped.
   - Recovering - Trail is recovering after it has been stopped previously. The trail was stopped before updating the checkpoint for the records collected. In the recovery state, the trail reads records starting from the current checkpoint and filter out the duplicate records which were already read. The recovery state 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 30 minutes. This status is temporary unless the trail has crashed. The Audit Vault Server checks the status of the audit trail. It attempts to check the status 5 times (by default) in Oracle AVDF releases 20.1 to 20.6. In Oracle AVDF release 20.7 and onwards, the Audit Vault Server attempts 20 times (by default) to reach the audit trail before concluding it is `Unreachable`.
   - Archive data files are required (link) - If you see this link, it means a new audit trail contains expired audit records that must be archived, and that the required archive data files are not available.

   The **Trail Autostart Details** column indicates whether autostart is enabled for a trail, and whether there have been attempts to restart a failed audit trail (for example, if a target goes down temporarily).

Tip: You can sort and filter the audit trail list.

> **Note:**
>
> - To view audit trails status for a specific agent host, click the name of the trail.
> - If an audit trail fails to start, then you can get more information by looking at the **Error Message** column.

> **See Also:**
>
> Handling New Audit Trails with Expired Audit Records

Check the Audit Trail Status with SQL*Plus

To check the audit trail status with SQL*Plus, query `avsys.audit_trail_view`.

For example:

```
SQL> SELECT location, host_name, status FROM audit_trail_view
LOCATION
HOST_NAME            STATUS
-------------------------------------------------------------
-------------------- -----------
unified_audit_trail
xxxxxxxx             IDLE
sys.unified_audit_trail_DELETED_2016-06-28 11:56:25.203 +00:00
xxxx                 STOPPED
/var/log/audit/audit.log_DELETED_2016-06-29 08:49:04.446 +00:00
xxxx                 STOPPED
/var/log/audit_DELETED_2016-06-29 08:53:00.906 +00:00
xxxx                 STOPPED
dvsys.audit_trail$
xxxx                 IDLE
```

> **Note:**
>
> If the `AVSYS` account is locked or the password is unknown, see Unlocking and Locking the AVSYS User.

Check the Audit Trail Status with AVCLI

To check the audit trail status with AVCLI, use the `LIST TRAIL FOR SECURED TARGET` command.

For example:

```
AVCLI> LIST TRAIL FOR SECURED TARGET TARGET_NAME;
-------------------------------------------------------------------------------
-------------------------------------------------------|
AUDIT_TRAIL_TYPE | HOST | LOCATION | STATUS | REQUEST_STATUS |
AUTO_START_STATUS | AUTOSTART_ATTEMPTS | LAST_START_TIME | ERROR_MESSAGE |
```

```
================================================================================
============================================================|
TABLE | xxx.xxx.com | UNIFIED_AUDIT_TRAIL | STARTING | | ENABLED | 3 |
2016-07-28 | 20:06:42.802312 GMT ||
--------------------------------------------------------------------------------
------------------------------------------------------------
```

Checking Downtime History of the Trail

Audit Vault Server console displays the current status of the trail. Starting Oracle AVDF 20.6, the Audit Vault Server console maintains record of the trail downtime. It also displays the reason for the downtime. This information is available in the **Downtime Report**. This report contains downtime information of every trail and a cumulative downtime report of all the trails in the Audit Vault Server. It captures the intervals during which the specific trail may have gone down either due to an error, or if it was manually stopped through the Audit Vault Server console, or it had changed status to one of the following:

Status	Description
STOPPED_ERROR	If this status is seen, then the trail has gone down due to an error. In this case there is an additional column **Error Message** that specifies the reason the trail was stopped.
UNREACHABLE	This status is dynamically calculated and is seen when the trail is unable to connect to the Audit Vault Server for more than 30 minutes.
STOPPED_UNKNOWN	If this status is seen, then the trail downtime data has been purged as the trail is down for more than the specified retention period.
STOPPED	The trail has stopped and is not collecting data.
STARTING	The trail is about to start with collection.
STOPPING	The trail is about to stop collecting data.
COLLECTING	The trail is active and collecting data.
IDLE	The trail is idle and not collecting data.
RECOVERING	The trail is in recovering mode.

> **Note:**
>
> Not all the status information is available in the reports.

To capture downtime report for the trail and to view the history of the trail, follow these steps:

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

2. Click the **Targets** tab.
3. Click **Audit Trails** in the left navigation menu.
4. Select the trails for which the downtime report needs to be generated.
5. Click **Downtime** button. The downtime report for the selected trails is displayed. Use the filter option, download the report, or click the back button to navigate to the **Audit Trails** tab.

The downtime of the Audit Vault Agent, the specific time as to when the Agent went down, the duration for which the data has not been captured, and the reason for the Agent going down is also made available in the reports.

> **Note:**
>
> - This downtime data is available, archived, and purged like any other data managed by Oracle AVDF. By default in release 20.6, the downtime data is available for a period of one month and is purged after that.
> - The history of trails configured prior to upgrade to Oracle AVDF 20.6 is not captured or available.
> - The report for new trails configured after upgrade to Oracle AVDF 20.6 is available.
> - Data for the trails configured after upgrade to Oracle AVDF 20.6 is available from the time the trail was started.

7.6.6 Audit Collection Best Practices

Follow these best practices for audit collection.

- Periodically purge the records that have already been read by the audit trail.

  For some targets, the Audit Vault Agent contains scripts for cleanup. See Audit Trail Cleanup for more information. If there are remaining targets where the records have already been read by the audit trail, you can manually clean up the audit trail.

  If you don't purge the records, the following issues might occur:

  – There may be too many records (more than a million) in a table audit trail. This can slow down audit data collection and reduce the throughput of the table audit trail.

  – For directory trails, there may be too many files (more than a thousand) with a size of more than 1 GB. This can slow down audit data collection and reduce throughput of the directory trail.

- Ensure that the directories of transaction log audit trails, directory audit trails, and Oracle GoldenGate are access controlled.
- For directory and transaction log audit trails, if the `agent` user does not have read permission on audit files, then provide the `agent` user with read permission on the audit files by running the following commands.

Operating System	Command

Linux	`setfacl -Rm u:<agent user name>:r-x <audit data directory>`
	
	`setfacl -Rdm u:<agent user name>:r-- <audit data directory>`

Solaris	`chmod A+user:<agent user name>:rx:fd:allow <audit data directory>`
	
	`chmod A+user:<agent user name>:r:allow <audit data directory>/*`

AIX/HP-UX	Add the `agent` user to the group that has read permission on the audit data.

7.6.7 Handling New Audit Trails with Expired Audit Records

Learn about handling new audit trails with expired audit records.

With established audit trail collection, audit data is retained in Oracle Audit Vault Server for the Months Online period of a retention (or archiving) policy. After this period, the data files are made available for archiving. The data is then kept in archives for the Months Archived period of the retention policy, and is available to retrieve to the Audit Vault Server during that period.

However, when you add a new audit trail to an existing target, the audit data collected may contain records that fall into the Months Archived period in the retention policy assigned to this target. That is, the online period for these audit records has expired and they should be archived according to the retention policy.

In this case, Oracle Audit Vault and Database Firewall attempts to automatically archive these expired records during the new audit trail collection. In some cases, you may need to make the archive data files available in order for the audit trail to complete collection.

When collecting a new audit trail for an existing target, follow these instruction if you see an **Archive data files are required** link in the **Collection Status** of the audit trail.

To make archive data files accessible:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab, and then click **Audit Trails**.
3. In the **Collection Status** column, if applicable, click the Archive data files are required link.

   The required archive data files are listed.
4. Check that required data files are available in the archive location, and that the connection to the location is set up correctly.
5. After you make the required data files available, restart this audit trail.

> **See Also:**
>
> - Defining Archive Locations to check the required data files are available in the archive location and the connection to the location is established.
> - About Archiving and Retrieving Data in Oracle Audit Vault and Database Firewall
> - Using Audit Vault Server Console

7.6.8 Deleting an Audit Trail

Learn how to delete an audit trail.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab.
3. In the left navigational menu, click **Audit Trails**.
4. Select the audit trails that you want to delete and then, if necessary, click **Stop** to stop the audit trail.
5. Select the audit trails that you want to delete, and then click **Delete**.

7.6.9 Converting Audit Record Formats for Collection

You can use special tools to convert audit record formats so that Audit Vault and Database Firewall can collect these records.

7.6.9.1 Prerequisites for Converting Oracle Audit Vault Record MySQL Formats

Learn about the prerequsites for converting Oracle Audit Vault record MySQL formats.

Before you begin the format conversion process, ensure that you have completed the following tasks.

- Register the MySQL target in the Audit Vault Server. See Registering or Removing Targets in Audit Vault Server.
- Deploy the Audit Vault Agent on the MySQL host machine. See Deploying the Audit Vault Agent.

7.6.9.2 Running the XML Transformation Utility for MySQL Audit Formats

Learn how to run the XML transformation utility for MySQL audit formats.

Audit records of some databases are in the format that cannot be read directly by Oracle Audit Vault and Database Firewall collectors. Such audit records are first converted to a readable format and then collected.

For MySQL targets, Oracle Audit Vault and Database Firewall provides a utility to transform the MySQL XML audit format 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.

> **Note:**
>
> This procedure is only applicable for the old audit format. The default audit format of MySQL 5.5 and 5.6 is old. The default audit format of MySQL 5.7 is new. The audit format can be changed by modifying the configuration on MySQL Server.

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
   ```

   This command contains the following variables:

   - *path_to_log_folder*:
     - For MySQL version prior to `5.7.21`: The path to the MySQL log folder listed in `my.ini`
     - For MySQL version `5.7.21` and later: The path to the MySQL log folder listed in `my.ini\<audit file name>.*.log`
   - *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 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 target registered in the Audit Vault Server.

   Example:

   For MySQL version prior to `5.7.21`: `MySQLTransformationUtility.bat inputPath=D:\MySQLLog outputPath=D:\ConvertedXML agentHome=E:\MySQLCollector interval=1 securedTargetName=MYSQL_DEV`

   For MySQL version `5.7.21` and later: `MySQLTransformationUtility.bat inputPath=D:\MySQLLog\audit.*.log outputPath=D:\ConvertedXML agentHome=E:\MySQLCollector interval=1 securedTargetName=MYSQL_DEV`

7.6.9.3 Converting Binary Audit Files to ASCII Format for IBM DB2

Learn about converting binary audit files to ASCII format for IBM DB2.

IBM DB2 creates its audit log files in a binary file format that is separate from the DB2 database. For IBM DB2 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.
>
> In case of multiple instances, if the instances are not owned by the same user, it is recommended to extract audit data corresponding to each instance in a separate location. To collect the audit data, use one agent per instance. Ensure that the agent user is same as the instance user.

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

   This user will extract the binary files to the text files.
2. This user must have execute privileges to run the conversion script from the Oracle AVDF directory. The script name is `DB295ExtractionUtil` (for Microsoft Windows, this file is called `DB295ExtractionUtil.bat`.)
3. This user identified in the initial step, must have 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.
8. Run one of the following scripts, depending on the version of DB2 that you have installed:
   - **For supported DB2 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.

  - *audittrailcleanup 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.
  - *audittrailcleanup 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`.

- **Support for IBM DB2 Database Partition Feature**

  Starting Oracle AVDF 20.5, IBM DB2 Database Partition Feature is supported on Linux and AIX platforms. This functionality is supported for DB2 version 10.5 and later. The Database Partition functionality is not supported on Windows platform.

  Specify the following parameters in the `DB295ExtractionUtil` script:

  - *databasepartition yes/no*: (Optional) Enter `yes` if current DB2 setup has Database Partition Feature setup, else enter `no`. If you omit this value, then the default is `no`.
  - *nodes*: (Optional) This is the name of the node (or multiple nodes) separated by spaces, of the DB2 Database Partition Feature setup.

> **Note:**
>
> - If the archive path and extraction path are on the shared location, that is accessible by all the nodes in the Database Partition Feature (DPF) setup, then you can exclude the `nodes` input parameter. The script generates the archive data and audit data for all the nodes in the Database Partition Feature setup, in the shared location.
> - If the archive path and extraction path are host machine specific locations, that are accessible only by the nodes on that machine, then it is recommended to run the script on every machine of the Database Partition Feature setup. Include the nodes input parameter with only the nodes present on the specific machine.
>
>   For example: `Machine 1` has `Node 0` and `Node 1`. `Machine 2` has `Node 2` and `Node 3`. The script must be run on `Machine 1` with parameters `-databasepartition yes -nodes 0 1`. The script must be run on `Machine 2` with parameters `-databasepartition yes -nodes 2 3`.

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

```
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, places the file in the `/home/extract_dir` directory, and deletes the archive files after audit data is collected:

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

Example 3: The following command creates an ASCII file for all the nodes of the database instance with Database Partition Feature setup, places the file in the `/home/extract_dir` directory, and deletes the archive files after audit data is collected:

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

Example 4: The following command creates an ASCII file for the specified nodes (0, 1, and 2) of the database instance with Database Partition Feature setup, places the file in the `/home/extract_dir` directory, and deletes the archive files after audit data is collected:

```
DB295ExtractionUtil -archivepath /home/archive_dir -extractionpath /home/
extract_dir -audittrailcleanup yes -databasepartition yes -nodes 0 1 2
```

Example 5: The following command creates an ASCII file for all the nodes of the *TOOLSDB* database with Database Partition Feature setup, places the file in the `/home/extract_dir` directory, and deletes the archive files after audit data is collected:

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

Example 6: The following command creates an ASCII file for the specified nodes (0, 1, and 2) of the *TOOLSDB* database with Database Partition Feature setup, places the file in the `/home/extract_dir` directory, and deletes the archive files after audit data is collected:

```
DB295ExtractionUtil -archivepath /home/archive_dir -extractionpath /home/
extract_dir -audittrailcleanup yes -databasename TOOLSDB -
databasepartition yes -nodes 0 1 2
```

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 target database name in the scheduled task.

7.6.10 Configuring Audit Trail Collection for Oracle Real Application Clusters

You can configure audit trail collection for Oracle Real Application Clusters (Oracle RAC).

Configure a SCAN listener for the RAC and use the SCAN listener IP as the single IP during target registration.

To configure Audit Trail collection for Oracle Real Application Clusters (RAC), follow these guidelines.

Audit Trail Type	Number of Audit Trails
`TABLE`	To configure table trail audit data collection from Oracle RAC environment, 1 audit trail is sufficient.
`DIRECTORY`	To configure directory audit data collection from Oracle RAC environment, separate audit trails are required. The trail location must be different directories in the shared storage of the Oracle RAC environment.
`TRANSACTION LOG`	To configure Transaction Log audit data collection from Oracle RAC environment, 1 audit trail is sufficient.

See Also:

Adding Audit Trails with Agent-Based Collection to configure an audit trail.

7.6.11 Configuring Audit Trail Collection for CDBs and PDBs

Learn about configuring audit trail collection for CDBs and PDBs.

Oracle Database can work as Container Database (CDB) or Pluggable Databases (PDB). A PDB is a portable collection of schemas, schema objects, and nonschema objects that appears to an Oracle Net client as a non-CDB. All Oracle databases before Oracle Database 12*c* are non-CDB.

The PDB and CDB can be registered as targets. Oracle Audit Vault and Database Firewall supports CDB and PDB level audit collection. To collect audit data from multiple PDB instances within a CDB, adopt either one of the following approaches:

Approach 1: Create a separate target for each PDB instance and create audit trail for each PDB target, which collects data from `UNIFIED_AUDIT_TRAIL` table.

Approach 2: Create one target for the CDB and create audit trail which collects data from `CDB_UNIFIED_AUDIT_TRAIL` table.

Note:

- In Oracle AVDF 20 data will be collected from `CDB_UNIFIED_AUDIT_TRAIL`, only if all the PDBs are up and running.
- `CDB_UNIFIED_AUDIT_TRAIL` provides audit records from all PDB instances in a multitenant environment. The performance of audit collection from `CDB_UNIFIED_AUDIT_TRAIL` is lower than audit collection from `UNIFIED_AUDIT_TRAIL` of every PDB instance. If the number of audit records generated per day in `CDB_UNIFIED_AUDIT_TRAIL` is higher than 8 million, then configure audit collection from `UNIFIED_AUDIT_TRAIL` of every PDB instance.

To configure Audit Trail collection for CDB or PDB, follow these guidelines:

Audit Trail Type	Guidelines
`TABLE`	• Audit records specific to CDB activities can be collected from `UNIFIED_AUDIT_TRAIL` table of the CDB target. Audit records corresponding to CDB activities and all PDB activities can be collected from `CDB_UNIFIED_AUDIT_TRAIL`. • Every PDB stores it's own audit data in it's own `UNIFIED_AUDIT_TRAIL` table which does not contain audit data of other PDBs. Separate audit trails can be configured for the PDB target to collect data corresponding to that specific PDB only. • For PDB target, collection from `CDB_UNIFIED_AUDIT_TRAIL` is not supported. **Note:** Audit collection from `CDB_UNIFIED_AUDIT_TRAIL` is supported in release 20.1.0.0.0.
`DIRECTORY`	• Audit from directory trail can be collected for CDB, by providing directory trail location as `<value of AUDIT_FILE_DEST>` (database parameter). • Audit from directory trail can be collected for each PDB, by providing directory trail location as `<value of AUDIT_FILE_DEST>/<GUID of the PDB>`. **Note:** If you are using a multitenant container database (CDB) in Oracle Database 12c, then for a CDB you must register a target for the CDB as well as for every PDB.

CDB Trail Enhancement in Oracle AVDF 20.2

In Oracle AVDF 20.2.0.0.0 (or 20 RU2), audit data is collected from `CDB_UNIFIED_AUDIT_TRAIL` for PDBs that are up and running, even if some of the PDBs are down. When a PDB is down, the data corresponding to the PDB with status down is not visible in `CDB_UNIFIED_AUDIT_TRAIL`. When the PDB which was earlier down comes up, then the data corresponding to the specific PDB is collected from `CDB_UNIFIED_AUDIT_TRAIL`.

If any PDB is down, then the last archive timestamp is not set on the `CDB_UNIFIED_AUDIT_TRAIL`, even if other PDBs are up and running. Hence those records that have already been read by the audit trail are not purged from the `CDB_UNIFIED_AUDIT_TRAIL` and this can lead to severe performance degradation of the audit trail.

If there are any PDBs that are permanently taken down or taken down for few days, then they must be specified in the `AV.COLLECTOR.IGNORE_PDB_IF_DOWN_LIST` target attribute. The value

of the `AV.COLLECTOR.IGNORE_PDB_IF_DOWN_LIST` target attribute is a list of PDBs separated by a colon. For example, `PDB1:PDB2:PDB5`.

If a PDB is down, but is present in the `AV.COLLECTOR.IGNORE_PDB_IF_DOWN_LIST`, then the audit trail ignores the specific PDB if it is down and sets the last archive timestamp on the `CDB_UNIFIED_AUDIT_TRAIL` if all the other PDBs are up and running.

Audit data collection from PDBs which are mentioned in the `AV.COLLECTOR.IGNORE_PDB_IF_DOWN_LIST` is not completely accurate. Some of the audit records for these PDBs may be missed. It is also possible that the data is purged from these PDBs, depending on when the last archive timestamp was set.

If there is a PDB with status down, that was present in the `AV.COLLECTOR.IGNORE_PDB_IF_DOWN_LIST`, and has to brought up, then first remove it from `AV.COLLECTOR.IGNORE_PDB_IF_DOWN_LIST`. Wait for 10 minutes so that the audit trail reads and processes the updated `AV.COLLECTOR.IGNORE_PDB_IF_DOWN_LIST` attribute. After approximately 10 minutes, bring up the PDB. This ensures that all future records are successfully collected from this PDB without any data loss.

> **See Also:**
>
> Adding Audit Trails with Agent-Based Collection to configure an audit trail.

7.6.12 Migrating Audit Trails from Agentless Collection to Agent-Based Collection

In Oracle AVDF 20.9 and 20.10, use this procedure to migrate audit trails from agentless collection to agent-based collection (for example, if you decide to pair the Audit Vault Server for high availability).

1. Log in to the Audit Vault Console as an administrator.
2. Stop the audit trail that you need to migrate.

   See Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server.
3. On the **Audit Trails** page, record the time in the **Data Collected Until** column for the audit trail.

   This indicates the time and date until which audit records have been collected.
4. On the target database or machine, purge the audit records that have already been collected.

   See Audit Trail Cleanup.
5. Delete the audit trail that you need to migrate.

   See Deleting an Audit Trail.
6. Create a new audit trail for the target and select **Agent-based Collection** when adding the audit trail.

   See Adding Audit Trails with Agent-Based Collection.

> **Note:**
>
> If records that have already been collected by the agentless collection service are not deleted from the target, then the newly created agent-based audit trail will collect duplicate records.
>
> Even after following the preceding steps, there's a possibility that a small set of duplicate data will be collected.

7.6.13 Migrating Audit Trails to Another Audit Vault Agent

Starting in Oracle AVDF 20.11, you can use the UI console or AVCLI commands to migrate an audit trail from one Audit Vault Agent to another. The same process can also be used to migrate trails from agent-based collection to agentless collection and vice versa. This can be beneficial if an Audit Vault Agent is facing CPU or memory shortages due to a large number of audit trails.

- Use the UI Console
- Use AVCLI Commands

Use the UI Console

1. Log in to the Audit Vault Server Console as an `administrator`.
2. Click the **Targets** tab.
3. Click on **Audit Trails** in the left navigation menu.
4. Select which audit trail(s) you'd like to move.
5. Click **Move**.
6. Select **Agent-based Collection** to move the audit trails to another Audit Vault Agent or select **Agentless Collection**.
7. If you selected to move the audit trails to another Audit Vault Agent in the previous step, select the Audit Vault Agent.
8. Click **Move**.

Use AVCLI Commands

1. Login to AVCLI with `administrator` privileges.
   Logging in to AVCLI
2. Use the `LIST COLLECTION` command to see a list of available Audit Vault Agents.
   List Collection for Agent
3. Use the `MOVE COLLECTION FOR SECURED TARGETS` command to move the audit trails.
   Move Collection for Secured Targets

Related Topics

- Adding Audit Trails with Agentless Collection

7.6.14 Audit Collection Downtime Alerts

Starting in Oracle AVDF 20.10, audit and network trails are monitored frequently and a system alert is generated if the trails are in the `STOPPED_ERROR` state.

Starting with AVDF 20.10, audit trails are monitored daily. Alerts are generated and email notifications are sent if audit trail is in `STOPPED_ERROR` state even after 20 retries.

Starting with AVDF 20.10, network trails are monitored hourly. Alerts are generated and email notifications are sent out if network trail is in `STOPPED_ERROR` state.

Related Topics

- Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server
- Creating a Network Audit Trail
- System Alerts

7.7 Configuring Database Firewall Monitoring Points

Learn about configuring Database Firewall monitoring points.

> **Note:**
>
> If you are using Transparent Application Failover (TAF), Fast Application Notification (FAN), or the Oracle Notification Service (ONS), then SQL commands are not sent through this channel. There is no need to route them through Oracle Database Firewall. ONS communications bypass the Database Firewall and connect directly to the ONS listener. ONS communications, including destination host and port, are configured in the ons.config properties file located on the ONS server.

7.7.1 About Configuring Database Firewall Monitoring Points for Targets

Learn about configuring Database Firewall monitoring points for the target.

If you are monitoring databases with a Database Firewall, you must configure one monitoring point for every target database that you want to monitor with the firewall. The monitoring point configuration allows you to specify:

- Firewall monitoring mode
- Database Firewall used for the monitoring point
- Identify the target database being monitored
- Network traffic sources to the database

Oracle Database Firewall can be deployed in the following modes:

- **Monitoring (Out-of-Band)** - In this deployment mode, Oracle Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.

- **Monitoring (Host Monitor)** - In this deployment mode, Oracle Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.
- **Monitoring / Blocking (Proxy)** - In this deployment mode the Database Firewall can monitor, alert, block, and substitute SQL statements.

Before configuring monitoring points, configure network traffic sources as part of database firewall configuration.

> **See Also:**
>
> Configuring the Database Firewall and Its Traffic Sources on Your Network

7.7.2 Creating and Configuring a Database Firewall Monitoring Point

Learn about creating and configuring Database Firewall monitoring points.

Configure Database Firewall monitoring points using the Audit Vault Server console. If you have configured a resilient pair of Audit Vault Servers, configure the monitoring points on the primary server.

Prerequisites

- The Database Firewall instances must be paired before configuring the monitoring points, targets, and policies.
- Ensure that you have configured traffic sources on the Database Firewall you plan to use for this monitoring point. See Configuring the Database Firewall and Its Traffic Sources on Your Network for more information.

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

   The **Targets** tab in the left navigation menu is selected by default.
3. Select and click the target you wish to modify.
4. From the **Database Firewall Monitoring** section on the main page, click on **Add**. The **Database Firewall Monitor** dialog is displayed.
5. In the **Basic** tab (for 20.3 or later the name of the tab is **Core**), enter the name for this **Database Firewall** instance or select one from the list.
6. Select a **Mode** from the following:
   - **Monitoring (Out-of-Band)**
   - **Monitoring (Host Monitor)**
   - **Monitoring / Blocking (Proxy)**
7. In the **Network Interface Card** (NIC) field, select from the list of NIC's. You may select a bonded NIC. Select from the list of NIC's based on your monitoring mode:
   - Monitoring (Out-of-Band) - You may select multiple NIC's from the list by holding the *Control* key on Windows or the *Command* key on Mac while selecting the NIC's.
   - Monitoring / Blocking (Proxy) - You may select only one NIC from the list.
   - Monitoring (Host Monitor) - See Creating a Monitoring Point for the Host Monitor Agent

8. Select the **Proxy Ports** from the list for **Monitoring / Blocking (Proxy)** mode. This field does not apply to other modes of Database Firewall deployment.
9. In the **Connection Details** section, select one or more targets. You can **Add** the targets from the list.

> **Note:**
>
> - Select the **RAC Instance/Autonomous DB** check box (**RAC Instance** check box in Oracle AVDF 20.7 and earlier) if the target is Oracle Real Application Clusters. Select this option for Oracle Databases where the monitoring point is in **Monitoring / Blocking (Proxy)** mode. For **Monitoring (Out-of-Band)** mode, uncheck this box. Enter the IP address of the individual RAC node in **Target Connections** field.
> - Select the **Network Interface Card** and **Proxy Ports** for **Monitoring / Blocking (Proxy)** mode. The proxy port is not applicable for monitoring only modes.

Enter the following information for each network location of the database. Click the **Add** button to configure the following additional details of the target instance:

- **Host Name / IP Address**

  > **Note:**
  >
  > For an Oracle RAC target, if the **RAC Instance/Autonomous DB** check box (**RAC Instance** check box in Oracle AVDF 20.7 and earlier) is selected, enter the FQDN of the SCAN Listener as the host name.

- **Port**
- **Service Name** (Optional, for Oracle Database only). SID can be used in this field. To enter multiple service names and/or SIDs, enter a new line for each of them, and then click **Add**. Multiple entries are allowed for monitoring only mode. For Monitoring / Blocking (Proxy) mode,
  - Oracle AVDF 20.1-20.9: You need to configure a proxy target for each OSN. This is because a single proxy port cannot service multiple OSN's on the same target database. Add more traffic proxy ports as required.
  - Oracle AVDF 20.10 and later: You can use one proxy port and specify multiple OSN's on the target database that are going to be processed. Specify the OSN's in a list delimited by the "|" character. For example, target1|target2|target 3.

> **Note:**
>
> Targets are listed here with the policy details. Choose the right deployment mode as per the requirement. Choose **Monitoring / Blocking (Proxy)** for monitoring, blocking, and alerting. Choose **Monitoring (Out-of-Band)** or **Monitoring (Host Monitor)** modes for monitoring and alerting only.

10. In the **Advanced** tab, enter the number of **Database Firewall Monitor Threads** (minimum and default value is 1). This controls the number of traffic handling threads in the Database Firewall monitoring point. Use due caution before modifying the value.
11. If the target database is an Oracle Database and **Mode** is selected as **Monitoring / Blocking (proxy)**, the check box for **Block Traffic for Unregistered Service Names** is available for selection. When this check box is selected, Database Firewall blocks sessions that use service names other than the one that is configured in the target **Connection Details** section.
12. If the database client and server are communicating over the TLS protocol, enable TLS.

    With this option, the Database Firewall acts as a TLS proxy. It serves as a TLS server for the database client and acts as a TLS client to the database server. The Database Firewall and the Audit Vault Server have access to the decrypted SQL traffic for further analysis. This feature applies only for Database Firewalls that are deployed in **Monitoring / Blocking (Proxy)** mode.

    a. Select **Enable TLS support**.

    > **Note:**
    >
    > If you select this option, the **Decrypt With Native Network Encryption Key** check box is hidden.

    b. In Oracle AVDF release 20.8 and later, select the certificate type under **Inbound TLS (From client to DBFW)**.

    The TLS protocol uses the certificate to authenticate the communication participant. You can use the default certificate that is signed by the Database Firewall or a certificate that is signed by an external Certificate Authority (CA).

    c. If you use the default self-signed certificate, then click **Download DBFW Certificate**.

    You need to install this certificate on the database client to enable Database Firewall authentication.

    d. If you use the external CA signed certificate, then select the certificate from the drop-down list.

    e. Select the cipher suite level.

    Level 4 - strongest, is the default.

    Starting with Oracle AVDF 20.13, Oracle Database 23ai is supported as a target which supports TLSv1.3 and TLSv1.2. However, Oracle AVDF does not support TLSv1.3 so you will have to modify the `sqlnet.ora` file of your Oracle Database 23ai to support TLSv1.2 by either removing the `SSL_VERSION` parameter or explicitly listing TLSv1.2 in the `SSL_VERSION` parameter. See Specifying TLS Protocol and TLS Cipher Suites in the *Oracle Database Security Guide* for more information.

    f. If you don't need database client authentication, then deselect **Client Authentication**.

    This option is available only for the inbound connection. The outbound connection is always authenticated. If you deselect this option, the **Client Trusted Certificates** button is disabled.

    g. To manage certificates for client authentication, click **Client Trusted Certificates**.

    h. Click **Choose File** and select the certificate on the local machine.

    i. Click **Open** to load the certificate and add it to the Database Firewall.

The details of the uploaded certificate appear in the dialog box.

j. Click **Cancel** to exit the dialog box.

k. Follow a similar process to select and manage certificates and the cipher suite level under **Outbound TLS (From DBFW to Database)**.

To manage the certificates for server authentication, click **Database Trusted Certificates**.

13. If Oracle Database uses native network encryption, select **Decrypt With Native Network Encryption Key** to enable the decryption of traffic.

> **Note:**
>
> If the **Enable TLS support** check box is selected, the **Decrypt With Native Network Encryption Key** check box is hidden.
>
> For Oracle AVDF release 20.5 and earler, the check box is **Decrypt With Network Native Encryption Key**.

This option also supports the retrieval of session information for Oracle Database. Complete the remaining fields as applicable.

For Oracle Real Application Clusters (Oracle RAC) targets (if the **RAC Instance/ Autonomous DB** check box is selected on the **Core** tab), enter the SCAN Listener IP address.

(In Oracle AVDF 20.7 and earlier, it's the **RAC Instance** check box, and in Oracle AVDF 20.2 and earlier, it's the **Basic** tab.)

For Oracle standalone database targets, enter the IP address of the database listener.

For Sybase SQL Anywhere (Oracle AVDF 20.1-20.6 only) and Microsoft SQL databases, the field is **Retrieve session information from target DB**. Retrieving session information is not available for any other non-Oracle database types.

> **Note:**
>
> Ensure that the Database Firewall is allowed to make a network connection to the database listener.

14. Select the check box for **Capture Database Response** field. If you check this field, the Database Firewall monitors the SQL response from the database. Select **Full Error Message** check box to capture the database response codes and error codes.

15. Click **Save** at the bottom of the dialog to save the configuration of the monitoring point.

The new monitoring point appears in the list and starts automatically.

> **Note:**
>
> `Default Database Firewall Policy will be applied for this Database Firewall Monitoring Point`. This message is displayed at the bottom of the dialog.

16. Click **Save** in the main page.
17. To stop or restart the monitoring point, select it from the **Database Firewall Monitoring** section and click **Stop** or **Start**.

> **Note:**
>
> When you use the **Monitoring / Blocking (Proxy)** 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.

> **See Also:**
>
> - High Availability in Oracle AVDF for details on configuring a resilient pair of servers.
> - *Oracle Audit Vault and Database Firewall Concepts Guide* for more information on different modes.
> - Configuring Network Settings for more information on traffic sources.
> - Configuring the Database Firewall As a Traffic Proxy

7.7.3 Modifying a Database Firewall Monitoring Point

After you create a Database Firewall monitoring point, you can modify the settings, enable database response monitoring, monitor native network encrypted traffic for Oracle Database, and host monitoring.

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

   The **Targets** tab in the left navigation menu is selected by default.
3. Select and click on a specific target from the list.
4. From the **Database Firewall Monitoring** section on the main page, click the name of the monitoring point you want to modify.
5. In the **Database Firewall Monitor** dialog, you can change some of the settings.
6. Select a different **Mode** from the following:
   - **Monitoring (Out-of-Band)** - In this deployment mode, Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.
   - **Monitoring / Blocking (Proxy)** - In this deployment mode, the Database Firewall can block or substitute SQL statements.
   - **Monitoring (Host Monitor)** - In this deployment mode, Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements.

> **Note:**
>
> - For Oracle AVDF 20.2 and earlier, while configuring the **Monitoring (Host Monitor)** deployment mode, you must select a network interface card that is not used as a Management Interface.
> - For Oracle AVDF release 20.3 and later, while configuring the **Monitoring (Host Monitor)** deployment mode, you must select a NIC which has an IP address configured. This may be the Management Interface. This is the NIC to which the Host Monitor Agent will connect. When you select **Monitoring (Host Monitor)** as the deployment type, only those network interface cards which have IP address configured are displayed in the **Network Interface Card** field.

7. Select a different traffic source in the field **Network Interface Card**.
8. In the **Advanced** tab, enter the number of **Database Firewall Monitor Threads** (minimum value is 1). This controls the number of traffic handling threads in the Database Firewall monitoring point. This value should be left at the default (1) unless there are indications that the Database Firewall is unable to cope with the amount of traffic it is receiving.
9. If the target database is an Oracle Database and **Mode** is selected as **Monitoring / Blocking (proxy)**, the check box for **Block Traffic for Unregistered Service Names** is available for selection. When this check box is selected, Database Firewall blocks sessions that use service names other than the one that is configured in the target **Connection Details** section.
10. If the database client and server are communicating over the TLS protocol, enable TLS.

    With this option, the Database Firewall acts as a TLS proxy. It serves as a TLS server for the database client and acts as a TLS client to the database server. The Database Firewall and the Audit Vault Server have access to the decrypted SQL traffic for further analysis. This feature applies only for Database Firewalls that are deployed in **Monitoring / Blocking (Proxy)** mode.

    a. Select **Enable TLS support**.

    > **Note:**
    >
    > If you select this option, the **Decrypt With Native Network Encryption Key** check box is hidden.

    b. In Oracle AVDF release 20.8 and later, select the certificate type under **Inbound TLS (From client to DBFW)**.

    The TLS protocol uses the certificate to authenticate the communication participant. You can use the default certificate that is signed by the Database Firewall or a certificate that is signed by an external Certificate Authority (CA).

    c. If you use the default self-signed certificate, then click **Download DBFW Certificate**.

    You need to install this certificate on the database client to enable Database Firewall authentication.

    d. If you use the external CA signed certificate, then select the certificate from the drop-down list.

    e. Select the cipher suite level.

Level 4 - strongest, is the default.

Starting with Oracle AVDF 20.13, Oracle Database 23ai is supported as a target which supports TLSv1.3 and TLSv1.2. However, Oracle AVDF does not support TLSv1.3 so you will have to modify the `sqlnet.ora` file of your Oracle Database 23ai to support TLSv1.2 by either removing the `SSL_VERSION` parameter or explicitly listing TLSv1.2 in the `SSL_VERSION` parameter. See Specifying TLS Protocol and TLS Cipher Suites in the *Oracle Database Security Guide* for more information.

f. If you don't need database client authentication, then deselect **Client Authentication**.

This option is available only for the inbound connection. The outbound connection is always authenticated. If you deselect this option, the **Client Trusted Certificates** button is disabled.

g. To manage certificates for client authentication, click **Client Trusted Certificates**.

h. Click **Choose File** and select the certificate on the local machine.

i. Click **Open** to load the certificate and add it to the Database Firewall.

The details of the uploaded certificate appear in the dialog box.

j. Click **Cancel** to exit the dialog box.

k. Follow a similar process to select and manage certificates and the cipher suite level under **Outbound TLS (From DBFW to Database)**.

To manage the certificates for server authentication, click **Database Trusted Certificates**.

11. If Oracle Database uses native network encryption, select **Decrypt With Native Network Encryption Key** to enable the decryption of traffic.

> **Note:**
>
> If the **Enable TLS support** check box is selected, the **Decrypt With Native Network Encryption Key** check box is hidden.
>
> For Oracle AVDF release 20.5 and earler, the check box is **Decrypt With Network Native Encryption Key**.

This option also supports the retrieval of session information for Oracle Database. Complete the remaining fields as applicable.

For Oracle Real Application Clusters (Oracle RAC) targets (if the **RAC Instance/ Autonomous DB** check box is selected on the **Core** tab), enter the SCAN Listener IP address.

(In Oracle AVDF 20.7 and earlier, it's the **RAC Instance** check box, and in Oracle AVDF 20.2 and earlier, it's the **Basic** tab.)

For Oracle standalone database targets, enter the IP address of the database listener.

For Sybase SQL Anywhere (Oracle AVDF 20.1-20.6 only) and Microsoft SQL databases, the field is **Retrieve session information from target DB**. Retrieving session information is not available for any other non-Oracle database types.

> **Note:**
>
> Ensure that the Database Firewall is allowed to make a network connection to the database listener.

12. Select the check box for **Capture Database Response** field. If you check this field, the Database Firewall monitors the SQL response from the database. Select **Full Error Message** check box to capture the database response codes and error codes.
13. Click **Save** at the bottom of the dialog to save the configuration of the monitoring point.
14. Click **Save** in the main page.

> **See Also:**
>
> - Creating TLS Proxy Certificates for Database Firewall
> - Configuring and Using Database Response Monitoring
> - Configuring Advanced Settings for Database Firewall

7.7.4 Starting, Stopping, or Deleting Database Firewall Monitoring Points

Learn about starting, stopping, and deleting Database Firewall monitoring points.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab.
3. Click on a specific target. The details of the target are displayed on the main page.
4. Under **Database Firewall Monitoring** tab, select a specific Database Firewall monitoring point.
5. Click one of the following buttons:
   - **Start** - To start the monitoring point
   - **Stop** - To stop the monitoring point
   - **Delete** - To delete the monitoring point

> **See Also:**
>
> Using Audit Vault Server Console

7.7.5 Viewing the Status of Database Firewall Monitoring Points

Learn about viewing Database Firewall monitoring point status.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab.
3. Select a specific target. The details of the specific target are displayed on the main page.

4. Under **Database Firewall Monitoring** section, click on a specific Database Firewall monitoring point.

   A list of monitoring points and their status is displayed. Possible status values are:

   - **Up** - The monitoring point is up and running, and there are no errors.
   - **Suspended** - The user has stopped the monitoring point, and there are no errors.
   - **Down** - The monitoring point is not working, probably due to errors.
   - **Unreachable** - There are communication errors between the Database Firewall and the Audit Vault Server.

> **See Also:**
>
> Using Audit Vault Server Console

7.7.6 Finding the Port Number Used by a Database Firewall Monitoring Point

Learn about finding Database Firewall monitoring point port numbers.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab.
3. Select a specific target. The details of the specific target are displayed on the main page.
4. Under **Database Firewall Monitoring** section, click on a specific Database Firewall monitoring point.
5. The port number is displayed in the field **Proxy Ports**.

> **See Also:**
>
> Using Audit Vault Server Console

7.7.7 Configuring a Database Firewall to Connect to an Oracle Autonomous Database

Learn how to configure a Database Firewall to connect to an Oracle Autonomous Database.

Prerequisite: Log in to the Oracle Cloud Infrastructure (OCI) account and download the wallet credentials ZIP file that is associated with the user account.

1. Create a TLS-enabled Database Firewall monitoring point for the Oracle Autonomous Database target.
   - On the **Core** tab, select **RAC Instance/Autonomous DB**.
   - On the **Advanced** tab, select **Enable TLS support**.

   For complete instructions, see Creating and Configuring a Database Firewall Monitoring Point.
2. Complete the TLS configuration for inbound connections.

See Modifying a Database Firewall Monitoring Point.

3. Import the wallet ZIP file that is associated with the user account (which you downloaded earlier) to the Database Firewall instance.
   a. Copy the wallet ZIP file to the file system on the Database Firewall (for example, `/tmp/Wallet_DBXXXXXXXXXX.zip`).
   b. Log in to the Database Firewall through SSH and switch to the *root* user.
   c. Extract the contents of the wallet ZIP file.

      ```
      unzip /tmp/Wallet_DBXXXXXXXXXX.zip -d my_cloud_wallet
      ```

   d. Run the following command to deploy the wallet for the appropriate Database Firewall secured target:

      ```
      /opt/avdf/bin/deploy-wallet  <PATH-TO-UNZIPPED-CLOUD-WALLET>  <SECURED-TARGET-NAME>
      ```

> **Note:**
>
> To view the list of all available secured targets, run the following command:
>
> ```
> /opt/avdf/bin/deploy-wallet --list-targets
> ```

7.8 Configuring Stored Procedure Auditing (SPA)

Learn about configuring stored procedure auditing (SPA).

Stored procedure auditing (SPA) enables Oracle Audit Vault and Database Firewall auditors to audit changes to stored procedures on target databases. Oracle Audit Vault and Database Firewall connects to the database server at scheduled intervals and discovers any changes or additions that have been made to stored procedures.

To enable SPA, you simply configure the user account privileges necessary for Oracle Audit Vault and Database Firewall to do stored procedure auditing on a target. Oracle Audit Vault and Database Firewall provides scripts for setting up these privileges. Run the scripts specific to the target type.

An Oracle Audit Vault and Database Firewall auditor can view changes to stored procedures in reports if the auditor enables Stored Procedure Auditing in the target configuration.

> **See Also:**
>
> - Scripts for Oracle AVDF Account Privileges on Targets
> - Supported Targets for Oracle Audit Vault and Database Firewall
> - *Oracle Audit Vault and Database Firewall Auditor's Guide*

7.9 Configuring Database Firewall for Databases That Use Native Network Encryption

Learn about monitoring native network encrypted traffic for Oracle Database.

You can monitor native network encrypted traffic for Oracle 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 is then made available in the reports.

> **Note:**
>
> In order to fetch the session information successfully, the target database should have configuration to do a reverse DNS lookup under certain cases where client machine is a Windows instance or uses network host names.

To configure monitoring of native network encrypted traffic for Oracle Database, follow the steps in this section.

7.9.1 Step 1: Apply the Specified Patch to the Oracle Database

Learn how to apply the specified patch to Oracle Database.

> **Note:**
>
> This step is not required for Oracle Database versions 11.2.0.4 or later. For all versions prior to 11.2.0.4, apply the patch specified in this section on 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.

7.9.2 Step 2: Run the Oracle Advance Security Integration Script

Learn how to run the Oracle Advance Security integration script.

To run the Network Encryption integration script:

1. Download and uncompress the integration script:

   - Oracle AVDF 20.13 and later
   - Oracle AVDF 20.1-20.12

   ## Oracle AVDF 20.13 and later

   a. Log in to the Audit Vault Server Console as an `administrator`.
   b. Click the **Targets** tab.
   c. Click the **Target Setup Script** button to download the integration script.
   d. Move the downloaded .zip file to a desired location.
   e. In this location, go to the `oracle_user_privilege_scripts` directory and extract the `advanced_security_integration.sql` file into a separate directory.

   ## Oracle AVDF 20.1-20.12

   a. From the Oracle Audit Vault and Database Firewall utilities file `dbfw-utility.zip` (downloaded with the software), copy the `database` directory to a location from which you can connect to the Oracle Database being patched.
   b. 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`.

   The desired directory now contains the uncompressed file: `advanced_security_integration.sql`.

2. Only perform this step if Database Vault is enabled on the target database.

   If Database Vault is not enabled then the script you run in the following step creates the users.

   a. Connect to the target database as a Database Vault Account Manager
   b. Create a user:

      ```
      CREATE USER <username> IDENTIFIED BY <password>
      ```

      The username and password created here will be used as `<param1>` and `<param2>`, respectively, in the following step when running the advanced_security_integration script.

   c. Create an `avsys` user:

      - If your database is 18c or later:

        ```
        CREATE USER avsys NO AUTHENTICATION ACCOUNT LOCK DEFAULT TABLESPACE
        SYSAUX;
        ```

- If your database is older than 18c:

```
CREATE USER avsys IDENTIFIED BY VALUES
'S:1000000000000000000000000000000000000000000000007000000000000000'
PASSWORD EXPIRE ACCOUNT LOCK DEFAULT TABLESPACE SYSAUX;
```

3. Execute the following command as a user with privileges to create users and grant privileges.

   `sqlplus / as sysdba @advanced_security_integration <param1> <param2> <param3>`

   where `<param1>` is the schema or username

   `<param2>` is the password to be set for the username

   `<param3>` valid values are *ASO* and *SESSION_INFO*

   Use `ASO` if you want to monitor native network encrypted traffic and fetch session information that is not captured from traffic.

   Use `SESSION_INFO` if the traffic is plain text and you just want to retrieve session information like username, OS username, client program name, and so on.

> **Note:**
>
> The third parameter (`<param3>`) is mandatory. In case it is missed, the system prompts with a help message.
>
> In case value of the third parameter (`<param3>`) is incorrect, the following help message is displayed:

```
Invalid value is provided for <param3>
The valid values are ASO, SESSION_INFO.
ASO retrieves oracle native network encryption key and session
information
SESSION_INFO retrieves session information
```

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

Learn how to provide Database Firewall public keys to Oracle Database.

In order to decrypt traffic using native network encrypted traffic for Oracle Database, you must provide the Database Firewall public key.

To provide the public key to the Oracle Database:

1. Log in to the Audit Vault Server console as administrator.
2. Click **Database Firewall** tab.
3. Click the specific Database Firewall instance from the list.
4. Click **Oracle Native Encryption** under **Configuration** section.
5. Click **Copy Key** to copy the public key 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 monitoring point resiliency, when you have more than one Database Firewall monitoring this 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.

6. Modify the `sqlnet.ora` file in the Oracle Database to include the public key and to require native network traffic encryption:
   a. Put the file you created in the earlier step 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.ENCRYPTION_SERVER=REQUIRED
```

> **Note:**
>
> - If the `sqlnet.ora` file contains the optional parameter `SQLNET.ENCRYPTION_CLIENT`, its value must not be `REJECTED`. Otherwise, an error will occur.
> - It is not mandatory for the `SQLNET.ENCRYPTION_SERVER` parameter to be set as `REQUIRED`. Native Network Encryption (NNE) can be enabled from the client side as well. But if you want to monitor NNE traffic, `SQLNET.ENCRYPTION_SERVER` must never have the value `REJECTED`.

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

> **See Also:**
>
> *Oracle Database Security Guide* for more information on network encryption.

7.9.4 Step 4: Enable Native Network Encrypted Traffic Monitoring for Oracle Database

You can enable native network encrypted traffic monitoring for Oracle Database.

Follow the procedure in Monitor Native Network Encrypted Traffic Through Database Firewall for Oracle Databases to complete the configuration for Oracle Databases that use network encryption.

7.10 Configuring Advanced Settings for Database Firewall

Learn about configuring database connection details under advanced options.

7.10.1 About Native Network Encryption for Oracle Databases

Learn about using native network encryption for Oracle Databases.

If you are using the Database Firewall to monitor an Oracle Database target that uses network encryption, then you must use native network encryption monitoring in order to decrypt statements sent to, and responses received from, that database so they can be analyzed.

Limitations on Decryption of Oracle Database Statements

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

- 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.
- Supported versions of Oracle Database.
- Database Firewall doesn't support running the Oracle Advance Security Integration Script on root container databases (CDB$ROOT). It also doesn't monitor and apply policies on traffic with native network encryption for root container databases (CDB$ROOT).

> **Note:**
>
> When dealing with encrypted connections from tools like Microsoft OSTRESS, it is advised to use the `-T146` flag to prevent the interference of Microsoft's encryption with the Audit Vault Database Firewall's examination of the data traffic. Additionally, it is suggested to use database interrogation to extract information such as the name of the database user, operating system, and client program that initiated a SQL statement from monitored Microsoft SQL Server and Sybase SQL Anywhere databases.

> **See Also:**
>
> Configuring Database Firewall for Databases That Use Native Network Encryption

7.10.2 Monitor Native Network Encrypted Traffic Through Database Firewall for Oracle Databases

Learn how to enable monitoring of native network encrypted traffic through Database Firewall for Oracle Databases.

This functionality enables Database Firewall to monitor native network encrypted traffic for supported Oracle Database targets.

> **Note:**
>
> Native Network Encrypted traffic monitoring was earlier known as Database Interrogation.

Prerequisite

Log in to the Audit Vault Server console as administrator. See Using Audit Vault Server Console for more information.

To enable this functionality for a Database Firewall monitoring point:

1. Click the **Targets** tab. The **Targets** tab in the left navigation menu is selected.
2. Click on the specific target. The details of the target are displayed on the main page.
3. Under **Database Firewall Monitoring** section, select the monitoring point for which native network encrypted traffic monitoring needs to be enabled.
4. In the **Advanced** tab, select the check box **Decrypt With Native Network Encryption Key**, for enabling decryption of traffic if Oracle Database is using Native Network Encryption. Decrypt with native network encryption key option also supports retrieval of session information for Oracle Database. Fill in the remaining fields as applicable.

   For an Oracle RAC target (if the **RAC Instance/Autonomous DB** check box is selected on the **Core** tab), enter the SCAN Listener IP address.

   (In Oracle AVDF 20.7 and earlier, it's the **RAC Instance** check box, and in Oracle AVDF 20.2 and earlier, it's the **Basic** tab.)

   For Oracle standalone database targets, enter the IP address of the database listener.

   > **Note:**
   >
   > Ensure the Database Firewall is allowed to make a network connection to the above mentioned database listener.

5. Once the above mentioned field is checked, the following fields are populated. Enter the values in the appropriate fields.
   - **Host Name / IP Address** - Enter the host name or the IP address of the target database. For Oracle standalone Database targets, enter the IP address of the database host machine. For Oracle RAC target, enter the SCAN Listener IP address.
   - **Port** - Enter the port number of the target database.
   - **Service Name** - Enter the service name of the database or database instance.
   - **User Name** - Enter the user name that was set up for this target.
   - **Password** - Enter the password for the user name.
6. Click **Save**.

7.10.3 Disabling Encrypted Traffic Monitoring for Oracle Databases

Learn about disabling encrypted traffic monitoring for Oracle Databases.

You can temporarily disable encrypted traffic monitoring. Oracle AVDF saves the configuration information that you have created for the next time that you want to enable it.

To disable encrypted traffic monitoring:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab. The **Targets** tab in the left navigation menu is selected.
3. Click on the specific target. The details of the target are displayed on the main page.
4. Under **Database Firewall Monitoring** section, select the monitoring point for which native network encrypted traffic monitoring needs to be disabled.

   Alternatively, navigate to **Database Firewalls** tab and then click **Database Firewall Monitoring** tab in the left navigation menu. A list of monitoring points are displayed on the page. The list can be sorted or filtered. Select the monitoring point for which native network encrypted traffic monitoring needs to be disabled.
5. In the **Advanced** tab, uncheck the box against **Decrypt With Native Network Encryption Key** for disabling decryption of traffic if Oracle Database is using Native Network Encryption. Upon deselection the remaining fields disappear.
6. Click **Save**.

> **See Also:**
>
> Changing the Database Firewall Host Name

7.10.4 Retrieve Session Information for Microsoft SQL Server and Sybase SQL Anywhere Databases

Learn how to obtain session information for non Oracle databases.

You can retrieve session information for Sybase SQL Anywhere (Oracle AVDF 20.1 - 20.6 only) and Microsoft SQL Server databases to obtain the name of the database user, operating system, and client program that originated a SQL statement. Enable this functionality only if this information is not available from the network traffic. This information is then made available in the reports.

While configuring this functionality choose the field **Retrieve session information from target DB** in the **Advanced** tab.

7.10.4.1 Setting Permissions to Retrieve Session Information in Microsoft SQL Server

Learn about retrieving session information in Microsoft SQL Server.

Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

- With a Script
- Manually

With a Script

1. Create a user account for Oracle AVDF for querying session information on the database. This database should be registered as a target in the Audit Vault Server console.

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

2. Download the necessary `mssql_ddi_script.sql` script from the utilities `V<part_number>.zip` file available as part of the Oracle AVDF install files from Oracle Software Delivery Cloud.
   Starting in Oracle AVDF 20.13, you can alternatively download the script from the Audit Vault Server console:
   a. Log in to the Audit Vault Server Console as an `administrator`.
   b. Click the **Targets** tab.
   c. Click the **Target Setup Script** button to download the integration script.
   d. The `mssql_ddi_script.sql` script is located in the `mssql_user_privilege_scripts` directory.
3. Execute the following command as a user with privileges to create schemas, logon triggers and jobs, and grant privileges:

> **Caution:**
>
> The script will create a logon trigger on the database and a few tables to be used by the Database Firewall.

```
sqlcmd -S tcp:<IP>,<PORT> -U sa -P <Password> -i mssql_ddi_script.sql -v
AVDF_DDI_USER="<username>"
```

The password is the password for the `sa` user and the username is the same as from step one.

4. Enable retrieving session information for the Database Firewall monitoring point that is associated with this target database, using the credentials created in the earlier step. Ensure the following steps are accurate while registering Microsoft SQL Server as a target.
   a. Log in to the Audit Vault Server Console as an `administrator`.
   b. Click on the **Targets** tab.
   c. Select the Microsoft SQL Server database from the list.
   d. Select the monitoring point from the **Database Firewall Monitoring** section.
   e. Click the **Advanced** tab.
   f. Select **Retrieve session information from target DB**.
   g. In the **User Name** field, enter the user name of the user created in the earlier step.
   h. In the **Password** field, enter the password of the user.
   i. In the **Host Name / IP Address** field, enter the IP address of the SQL Server.
   j. In the **Port** field, enter the port of the SQL server listening port.
   k. In the **Database Name** field, enter a valid database service name on SQL Server. In case the database service name is not correct, then SQL server DDI requests fail on the SQL Server with invalid request error.

Manually

> **Note:**
>
> It is possible for direct database interrogation (DDI) to fail to fetch information for shorter sessions using this method. Follow the alternate steps that involve running a script to avoid this.

1. Create a user account for Oracle AVDF for querying session information on the database. This database should be registered as a target in the Audit Vault Server console. Make a note of the user name and password for this account.
2. Grant the following permissions to the user account you created in the previous step:
   - `VIEW ANY DEFINITION` and `VIEW SERVER STATE` for SQL Server
   - `SELECT` on the `master.dbo.sysdatabases` table
3. Enable retrieving session information for the Database Firewall monitoring point that is associated with this target database, using the credentials created in the earlier step. Ensure the following steps are accurate while registering Microsoft SQL Server as a target.
   a. Log in to the Audit Vault Server Console as an `administrator`.
   b. Click on the **Targets** tab.
   c. Select the Microsoft SQL Server database from the list.
   d. Select the monitoring point from the **Database Firewall Monitoring** section.
   e. Click the **Advanced** tab.
   f. Select **Retrieve session information from target DB**.
   g. In the **User Name** field, enter the user name of the user created in the earlier step.
   h. In the **Password** field, enter the password of the user.
   i. In the **Host Name / IP Address** field, enter the IP address of the SQL Server.
   j. In the **Port** field, enter the port of the SQL server listening port.
   k. In the **Database Name** field, enter a valid database service name on SQL Server. In case the database service name is not correct, then SQL server DDI requests fail on the SQL Server with invalid request error.

Related Topics

- Monitor Native Network Encrypted Traffic Through Database Firewall for Oracle Databases
  Learn how to enable monitoring of native network encrypted traffic through Database Firewall for Oracle Databases.

7.10.4.2 Disable Retrieving Session Information in Microsoft SQL Server

After using the `mssql_ddi_script.sql` script which created a logon trigger and a few tables on the database to configure direct database interrogation (DDI), you can use the `mssql_ddi_removal.sql` script to disable DDI.

1. Execute the following command as a user with privileges to drop schemas, logon triggers and jobs, and revoke privileges:

   ```
   sqlcmd -S tcp:<IP>,<PORT> -U sa -P<Password> -i mssql_ddi_removal.sql -v
   AVDF_DDI_USER="<username>"
   ```

   The password is the password for the `sa` user and the username is that of the user account on the database for Oracle AVDF.
2. On the Audit Vault Server console, disable DDI for the Microsoft SQL Server:
   a. Log in to the Audit Vault Server Console as an `administrator`.
   b. Click on the **Targets** tab.
   c. Select the Microsoft SQL Server database from the list.
   d. Select the monitoring point from the **Database Firewall Monitoring** section.
   e. Click the **Advanced** tab.
   f. Deselect **Retrieve session information from target DB**.

7.10.4.3 Setting Permissions to Retrieve Session Information in Sybase SQL Anywhere Database

Learn about retrieving session information in Sybase SQL Anywhere databases.

> **Note:**
>
> - Sybase SQL Anywhere was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.
> - Before you can use Sybase SQL Anywhere, you must download and install the SQL Anywhere ODBC driver for Linux.

1. Create a user account Oracle AVDF for querying session information on the database. This database should be registered as a target in the Audit Vault Server console.

   Make a note of the user name and password for this account.
2. Grant the following permissions to the user account created in the earlier step:
   - `CONNECT`
   - `SELECT` on these system tables:

     ```
     sys.sysuser
     sys.sysuserauthority
     sys.sysremoteuser
     sys.sysloginmap
     sys.sysgroup
     ```
3. Enable retrieving session information for the Database Firewall monitoring point that is associated with this target database, using the credentials created in the earlier step.

> **See Also:**
>
> Monitor Native Network Encrypted Traffic Through Database Firewall for Oracle Databases

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

7.11 Monitoring TLS Encrypted SQL Traffic

Learn how to enable monitoring of TLS encrypted SQL traffic between the database clients and Oracle Database.

> **Note:**
>
> - This functionality does not support database clients using PKI authentication.
> - This functionality is not supported for Oracle Real Application Cluster (RAC) as a target in Oracle AVDF release 20.7.
> - This functionality is supported for Oracle Real Application Cluster (RAC) as a target starting with Oracle AVDF release 20.8.
> - The Database Firewall acts as a proxy and terminates TLS session from the database clients. In all cases, Database Firewall becomes the client for the database server.
> - Native Network Encryption is disabled in case this functionality is enabled.

7.11.1 Using Default Self Signed Certificates Created During Monitoring Point Creation

Learn how to use self signed certificates created by default when creating a Database Firewall monitoring point.

Starting with Oracle AVDF release 20.7, Database Firewall supports monitoring of TLS encrypted SQL traffic between the database client and Oracle Database. Database Firewall acts a TLS proxy terminating the session from the database client and creating a new TLS outbound session to the database server. Different TLS levels can be set for:

1. Inbound connection from the database client to Database Firewall
2. Outbound connection from Database Firewall to Oracle Database

TLS *Level-4* is the strictest and set by default. Mutual authentication is enabled by default for both inbound and outbound connections.

Database Firewall decrypts the network traffic from the database clients, extracts SQL traffic, and acts on the SQL statements based on the configured policies. It creates a new TLS session to the database server if the traffic needs to be passed on.

> **Note:**
>
> For production instances it is recommended to use third party CA signed certificates than self signed certificates as per your organizational policy.

Follow these steps to enable TLS encrypted traffic monitoring capability for a target database:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab. The **Targets** tab in the left navigation menu is selected.
3. Click the specific target. The details of the target are displayed on the main page.
4. Under **Database Firewall Monitoring** section, click **Add** to create a new monitoring point. The **Database Firewall Monitor** dialog is displayed.
5. In the **Core** tab, select the Database Firewall instance from the list.
6. Select **Monitoring / Blocking (Proxy)** as the deployment mode from the list.
7. Enter the remaining details.
8. In the **Advanced** tab, select the check the box against **Enable TLS Support** field. All the necessary self signed certificates for this monitoring point are created. Mutual authentication is also enabled by default for inbound and outbound TLS connections.
9. Complete the configuration of mutual authentication for the monitoring point.

> **See Also:**
>
> - Disabling Mutual Authentication for Inbound or Outbound TLS Communication
> - Creating and Configuring a Database Firewall Monitoring Point
> - About Setting Transport Layer Security Levels

7.11.2 Configuring Mutual Authentication for Inbound or Outbound TLS Communication

Learn how to configure mutual authentication for inbound or outbound TLS communication between the database clients and Oracle Database.

You can configure mutual authentication for TLS communication between:

1. Database client to Database Firewall (inbound connection)
2. Database Firewall to Oracle Database (outbound connection)

The configuration file for the Database Firewall monitoring point is `/var/dbfw/va/x/etc/appliance.conf`. In this case `x` is the Database Firewall monitoring point identifier. The database client always authenticates the associated Database Firewall it is connecting to.

Follow these steps:

1. Log in to the Database Firewall through SSH and switch to the `root` user.

2. Configure the mutual authentication of database client and Database Firewall by following these steps:

   a. Import the monitoring point inbound certificate (`/usr/local/dbfw/va/N/pki/in/in.crt`) into the key store of the database client as a trusted CA certificate. In this case `N` refers to the monitoring point number. To find the monitoring point number:

      i. Log in to the Database Firewall through SSH and switch to the `root` user.

         See Logging In to Oracle AVDF Appliances Through SSH.

      ii. Change to `/var/dbfw/va` directory.

      iii. Identify the Database Firewall monitoring point by searching for the target name configured in the Audit Vault Server. Run the following command:

```
grep -lr <TARGET NAME> *
```

      iv. Find the monitoring point number from the output which contains the name and path of the configuration file. For example: `1/etc/appliance.conf`. In this example, `1` is the monitoring point number.

   For Oracle Database clients, this involves importing the inbound certificate of the monitoring point into the client's wallet. Refer to the *SQLNET Administrator Guide* for complete information.

   For other (non Oracle) database clients, refer to respective database documentation.

   b. Copy the database client's trusted CA certificate into the monitoring point's inbound CA directory `/usr/local/dbfw/va/xx/pki/in/ca`.

   In this case `xx` refers to the monitoring point identifier. The permissions of the CA certificate for the clients must be `0440:dbfw:dbfw`.

3. Configure the mutual authentication of Database Firewall and database server by following these steps:

   a. Configure mutual authentication for outbound TLS connection. Copy the trusted CA certificate of the target database into the corresponding outbound CA directory of the monitoring point `/usr/local/dbfw/va/xx/pki/out/ca`.

   In this case `xx` refers to monitoring point identifier. The permissions of database CA certificate must be `0440:dbfw:dbfw`.

   b. Import the outbound certificate of the monitoring point `/usr/local/dbfw/va/xx/pki/out/out.crt` into the key store of the target database as trusted CA certificate.

   For Oracle Database target this involves importing the outbound CA certificate of the monitoring point into wallet of the target database. Refer to the *SQLNET Administrator Guide* for complete information.

   For other (non Oracle) database clients, refer to respective database documentation.

4. Restart the services. Run the following commands to restart the monitoring points which had changes to the configuration:

```
systemctl stop monitor

/usr/local/dbfw/bin/dbfwctl stop xx

systemctl start monitor
```

   In this case `xx` refers to monitoring point identifier.

5. Test the connections. TLS connection initiated from the database client to the above monitoring point should result in a successful connection.

> **See Also:**
>
> - Creating and Configuring a Database Firewall Monitoring Point
> - Modifying a Database Firewall Monitoring Point
> - About Setting Transport Layer Security Levels

7.11.3 Using External Certificates Signed by Certificate Authority

Learn how to use certificates signed by an external CA in Database Firewall.

You can use a certificate signed by an external Certification Authority (CA) based on your organization policy. Starting with Oracle AVDF release 20.7, Database Firewall supports external CA signed certificates for inbound and outbound TLS connections. Database Firewall provides a utility (`config-pki_identity`) to generate a CSR (Certificate Signing Request) which can be signed externally.

Follow these steps to use one pair of externally signed certificates for all Database Firewall monitoring points:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Create Database Firewall monitoring points and enable TLS encrypted SQL traffic monitoring. Select the appropriate TLS levels in the **Inbound TLS (From client to DBFW)** and **Outbound TLS (From DBFW to Database)** sections. See Creating and Configuring a Database Firewall Monitoring Point for details.

   Relevant self signed certificates are created for these Database Firewall monitoring points.
3. Connect to the Database Firewall through SSH as *support* user.
4. Switch user to *root*.
5. Delete the self signed certificates for above Database Firewall monitoring points using the `/opt/avdf/config-utils/bin/config-pki_identity` utility.
6. Create a CSR (Certificate Signing Request) to be signed externally.

Note:

Important aspects to be noted while creating a CSR:

- The `alt_*` values are optional, depending on the certificate usage requirements.
- The `key_path` and `cert_path` directories must exist.
- The value of `cert_uid/gid/mode` must always be `dbfw:dbfw:444`.
- The value of `key_uid/gid/mode` must always be `root:arbitercerts:440`.
- Use the add command in `/opt/avdf/config-utils/bin/config-pki_identity` utility to create a CSR.

For example: To create a CSR (`in.csr`) for the key (`in.key`), then use the following:

```
/opt/avdf/config-utils/bin/config-pki_identity add \
key_path=/usr/local/dbfw/va/in.key \
cert_path=/usr/local/dbfw/va/in.csr \
cert_uid=dbfw \
cert_gid=dbfw \
cert_mode=444 \
key_uid=root \
key_gid=arbitercerts \
key_mode=440 \
common_name=test.certificate \
country=--- \
email=first.last@example.invalid \
locality=city \
organisation=company \
organisational_unit=group \
state=area \
alt_dns=foobar.example.org,foobar2.example.org \
alt_email=first.last2@example.invalid,first.last3@example.invalid \
alt_ip='192.0.2.0,192.0.2.1' \
alt_uri=https://<exampleuri.1>,https://<exampleuri.2>
```

7. Use the example to create a `/usr/local/dbfw/va/out.csr`.
8. Get both the CSRs signed externally:
   a. `/usr/local/dbfw/va/in.csr`
   b. `/usr/local/dbfw/va/out.csr`
9. Copy both the externally signed certificates (`in.crt` and `out.crt`) to the `/usr/local/dbfw/va` directory.
10. Validate and import both the externally signed certificates using the following example command:

```
/opt/avdf/config-utils/bin/config-pki_identity set cert_path=/usr/local/
dbfw/va/in.crt
```

11. Create a symbolic link for the `in.crt` from every Database Firewall monitoring point inbound directory to `/usr/local/dbfw/va/in.crt`.

> **Note:**
>
> Add all the trusted certificates that constitute the certificate chain in the corresponding `pki/in/ca` path before adding externally signed certificate into `pki/in` path of a monitoring point.

12. Create a symbolic link for the `in.key` from every Database Firewall monitoring point inbound directory to `/usr/local/dbfw/va/in.key`.
13. Create a symbolic link for the `out.crt` from every Database Firewall monitoring point outbound directory to `/usr/local/dbfw/va/out.crt`.

> **Note:**
>
> Add all the trusted certificates that constitute the certificate chain in the corresponding `pki/out/ca` path before adding externally signed certificate into `pki/out` path of a monitoring point.

14. Create a symbolic link for the `out.key` from every Database Firewall monitoring point outbound directory to `/usr/local/dbfw/va/out.key`.

    For example:

    ```
    ln -s /var/dbfw/va/in.crt /var/dbfw/va/xx/pki/in/in.crt ; ln -s /var/
    dbfw/va/out.crt /var/dbfw/va/xx/pki/out/out.crt
    ```

    In this case `xx` refers to the Database Firewall monitoring point identifier.
15. Configure mutual authentication for the inbound TLS connection. The inbound connection is the connection from the database client to the Database Firewall.
16. Configure mutual authentication for the outbound TLS connection. The outbound connection is the connection from the Database Firewall to Oracle Database.
17. Restart all the modified Database Firewall monitoring points.

> **See Also:**
>
> - CONFIG-PKI_IDENTITY
> - Disabling Mutual Authentication for Inbound or Outbound TLS Communication
> - Using Default Self Signed Certificates Created During Monitoring Point Creation

7.11.4 Disabling Mutual Authentication for Inbound or Outbound TLS Communication

Learn how to disable mutual authentication for inbound or outbound TLS communication between the database clients and Oracle Database.

You can disable mutual authentication for TLS communication between:

1. Database client to Database Firewall (inbound connection)
2. Database Firewall to Oracle Database (outbound connection)

Mutual authentication can be optionally disabled for inbound or outbound TLS communication. The configuration file for the Database Firewall monitoring point is `/var/dbfw/va/N/etc/appliance.conf`. In this case `N` is the Database Firewall monitoring point number. The database client always authenticates the associated Database Firewall it is connecting to.

To find the monitoring point number:

1. Log in to the Database Firewall through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Change to `/var/dbfw/va` directory.
3. Identify the Database Firewall monitoring point by searching for the target name configured in the Audit Vault Server. Run the following command:

   ```
   grep -lr <TARGET NAME> *
   ```
4. Find the monitoring point number from the output which contains the name and path of the configuration file. For example: `1/etc/appliance.conf`. In this example, `1` is the monitoring point number.

Follow these steps to disable mutual authentication for inbound TLS communication:

1. Modify the following value in the configuration file `/var/dbfw/va/N/etc/appliance.conf`:

   ```
   TLS_CLIENT_AUTH="0"
   ```
2. Import the Database Firewall monitoring point inbound certificate (`/usr/local/dbfw/va/N/pki/in/in.crt` or `/usr/local/dbfw/va/in.crt`) into the SQL client's key store as a trusted CA certificate.

   Note: For Oracle SQL clients this involves importing the Database Firewall monitoring point CA certificate into the SQL client's wallet. Refer to the SQLNET Administrator Guide for complete information. For other (non Oracle) SQL clients, refer to the respective database documentation.

Database Firewall authenticates the database it is connecting to. Follow these steps to disable mutual authentication for outbound TLS communication:

1. Modify the following value in the `sqlnet.ora` configuration file:

   ```
   SSL_CLIENT_AUTHENTICATION = FALSE
   ```
2. Copy the trusted CA certificate of the target database into the corresponding Database Firewall monitoring point's outbound CA directory (`/usr/local/dbfw/va/N/pki/out/ca`).

See Also:

- Configuring Mutual Authentication for Inbound or Outbound TLS Communication
- Creating and Configuring a Database Firewall Monitoring Point
- Modifying a Database Firewall Monitoring Point
- About Setting Transport Layer Security Levels

7.11.5 Configuring a TLS Proxy for an Oracle Real Application Clusters Database

Learn about additional steps that are required to configure a TLS proxy for Oracle Real Application Clusters (Oracle RAC).

Oracle AVDF release 20.7 supports monitoring TLS encrypted SQL traffic between the database clients and Oracle Database. Starting with Oracle AVDF release 20.8, this functionality is supported for Oracle RAC.

Prerequisites

- The database client must have a wallet that is configured with credentials to communicate with the Oracle RAC database instance.
- The Oracle RAC database instance must have a wallet that is configured to communicate with the client.
- The client and the Oracle RAC database instance must be able to connect by using TCPS.
- You must have an externally created Oracle wallet for the Database Firewall to use, and it must be configured with credentials to communicate with the Oracle RAC database instance. See Managing Oracle Wallets with the orapki Utility for creating and managing oracle wallets.

1. Create a TLS-enabled Database Firewall monitoring point for the Oracle RAC target. Select **Oracle RAC** and **TLS** in the Audit Vault Server console. See Creating and Configuring a Database Firewall Monitoring Point.
2. Complete the TLS configuration for inbound connections. See Modifying a Database Firewall Monitoring Point.
3. Import the externally created wallet to the Database Firewall instance.
   a. Copy the externally created wallet to the file system in the Database Firewall (for example, `/tmp/my_rac_wallet`).
   b. Switch to the *root* user.
   c. Run the following command to deploy the wallet for the appropriate Database Firewall secured target:

```
/opt/avdf/bin/deploy-wallet  <PATH-TO-WALLET>
      <SECURED-TARGET-NAME>
```

> **Note:**
>
> To view a list of all available secured targets, run the following command:
>
> ```
> /opt/avdf/bin/deploy-wallet
>     --list-targets
> ```

7.11.6 (Optional) Enabling Common Name Verification for the Database Server

In addition to verifying that the target database's certificate is valid, you can verify the database server's common name from the database certificate. This verification matches the server's common name against a set of allowed common names that you configure.

To enable this additional check of the database certificate's common name, follow these steps:

1. Log in to the Database Firewall through SSH and switch to the `root` user.See Logging In to Oracle AVDF Appliances Through SSH.
2. Identify the secured target for which you want to enable this feature.
3. Edit the `appliance.conf` file for the secured target.

   Find the monitoring point number:

   a. Log in to the Database Firewall through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

   b. Change to `/var/dbfw/va` directory.

   c. Identify the Database Firewall monitoring point by searching for the target name configured in the Audit Vault Server. Run the following command:

      ```
      grep -lr <TARGET NAME> *
      ```

   d. Find the monitoring point number from the output which contains the name and path of the configuration file. For example: `1/etc/appliance.conf`. In this example, `1` is the monitoring point number.

   For example, in the following file path, *N* represents the monitoring point number: `/usr/local/dbfw/va/N/etc/appliance.conf`

   a. Locate the following keyword in the file: `TLS_PROXY_OUTBOUND_ALLOWED_CN_LIST`

   b. Provide an allowed list of values in one of the following formats, depending on whether the secured target type is an Oracle Real Application Clusters (Oracle RAC) database.

Secured Target Type	Description of Allowed List of Values	Example
Non-Oracle RAC database	Provide a list of allowed common names that the Database Firewall is allowed to connect to	`TLS_PROXY_OUTBOUND_ALLOWED_CN_LIST = "CN=<db_cn_name>:CN=<other_db_cn_name>"`
Oracle RAC database	Provide the distinguished name for the peer RAC database	`TLS_PROXY_OUTBOUND_ALLOWED_CN_LIST = "CN=<db_cn_name>, O=<db_org_name>, L=<db_location_name>"`

4. Save the edited configuration.
5. Restart the monitoring point.

   For instructions, see Starting, Stopping, or Deleting Database Firewall Monitoring Points.

7.12 Configuring and Using Database Response Monitoring

Learn about configuring and using database response monitoring.

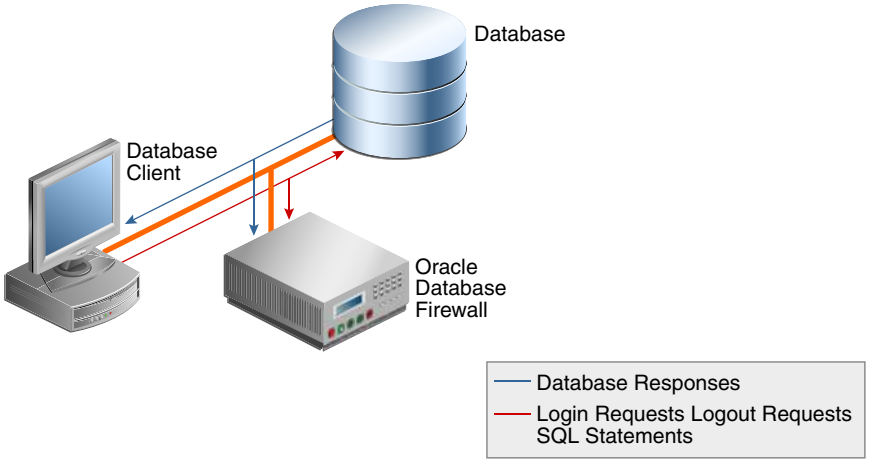
7.12.1 About Database Response Monitoring

Learn about database response monitoring.

Enabling the Database Response Monitoring feature enables Oracle Database Firewall to record responses that the target database makes to login requests, logout requests and SQL statements sent from database clients, as shown in Figure 7-1. 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 7-1 illustrates the process flow of database response monitoring.

Figure 7-1 Database Response Monitoring



The Oracle Audit Vault and Database Firewall auditor can view database responses in audit reports.

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

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

> **Note:**
>
> The **Event Status** value in the reports is displayed only if Database Response Monitoring is enabled for the respective monitoring point.

7.12.2 Enabling Database Response Monitoring

Learn about enabling database response monitoring.

To enable database response monitoring for a target:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab. The **Targets** tab in the left navigation menu is selected.
3. Click on the specific target. The details of the target are displayed on the main page.
4. Under **Database Firewall Monitoring** section, select the monitoring point for which native network encrypted traffic monitoring needs to be enabled.
5. In the **Database Firewall Monitor** dialog, click the **Advanced** tab.
6. Select the check box against **Capture Database Response** field.

   After this field is checked, the **Full error message** check box is displayed. If this field is checked, any detailed error message text generated by the database is logged along with the error code.
7. Click **Save**.

> **See Also:**
>
> - Working with Lists of Objects in the Audit Vault Server Console to sort or filter the monitoring points list.
> - Using Audit Vault Server Console
> - *Oracle Audit Vault and Database Firewall Auditor's Guide* for more information on configuring Firewall policies.

7.13 Securing the Agent and Oracle Database Target Connection

Learn how secure the Agent and Oracle Database target connection.

Data security between an Audit Vault Agent and an Oracle Database target is achieved by default, through network encryption over TCP connection. Data security can also be achieved by using a TCPS/SSL connection.

If the target has been setup to accept TCPS/SSL connections, then follow these steps to configure the Agent:

1. Ensure that in the target's `sqlnet.ora` file, the following parameters are set:
   - `SQLNET.ENCRYPTION_SERVER` = `REQUESTED`, `REJECTED`, or the default, `ACCEPTED`.
   - `SQLNET.CRYPTO_CHECKSUM_SERVER` = `REJECTED` or the default, `ACCEPTED`
2. Log in to the Audit Vault Server console as an administrator.
3. Click the **Targets** tab.
4. In the left navigation menu, select **Targets**.
5. Select the name of the target that you want to modify.
6. In the target page, do the following:
   a. In the **Audit Data Collection** section, enter the details in **Host Name/IP Address**, choose **TCPS** protocol, **Server DN**, and upload the wallet file.
   b. Or alternately, select the **Advanced** option, choose **TCPS** protocol, upload the wallet file, and then in the **Target Location** field, provide the TCPS connection string.

      For example:

      ```
      jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=host_ip)
      (PORT=port_number))(CONNECT_DATA=(SERVICE_NAME=service_name)(SERVER=DEDICATED))
      (SECURITY= (SSL_SERVER_CERT_DN="dn")))
      ```

   c. Click **Save**.

> **See Also:**
>
> - *Oracle Database Net Services Reference* for more information about the parameters.
> - Using Audit Vault Server Console

7.14 Upgrading the Target Database

If you're upgrading the target database, perform the following tasks to ensure that Oracle Audit Vault and Database Firewall (Oracle AVDF) continues to function properly.

- If the Database Firewall is deployed in **Monitoring/Blocking (Proxy)** mode, then stop the monitoring point of the target.

  See Starting, Stopping, or Deleting Database Firewall Monitoring Points.
- Ensure that there are no changes to the database listener ports.

If the database listener ports have changed, then make the corresponding change to the monitoring point and restart the network trail.

- If the target database details like the IP address and host name haven't changed, then after the target database upgrade is complete, enable the monitoring point. The traffic should flow through the monitoring point as before.

  See Starting, Stopping, or Deleting Database Firewall Monitoring Points.

- Run the script on the target database to grant privileges after the database upgrade is complete.

  See Scripts for Oracle AVDF Account Privileges on Targets.

8

Using the Host Monitor Agent

When you deploy the Database Firewall in **Monitoring (Host Monitor)** mode, the Host Monitor Agent captures SQL traffic from the network interface card of the host machine that is running the target database and securely forwards it the Database Firewall.

8.1 About Host Monitoring

You can deploy Database Firewall in **Monitoring (Host Monitor)** mode.

Database Firewall monitors and analyzes the SQL traffic to the database. You can configure Database Firewall in the following deployment modes:

- **Monitoring / Blocking (Proxy)**
- **Monitoring (Out-of-Band)**
- **Monitoring (Host Monitor)**

For descriptions of these deployment modes, see Introduction to Database Firewall Deployment.

The **Monitoring (Host Monitor)** deployment mode requires a Host Monitor Agent to be deployed on the host machine where the target database is running. You can configure the Host Monitor Agent to capture SQL traffic on ports that the database is listening on. The Host Monitor Agent can capture SQL traffic of multiple databases that are running on a single host machine, and it can capture SQL traffic when there are multiple network paths from clients to the target database.

After you deploy and configure the Host Monitor Agent on the agent machine, it performs the following actions:

- Captures SQL traffic on ports that the database is listening on.
- Forwards the SQL traffic securely to Database Firewall.

Starting in AVDF 20.13, the Host Monitoring Agent can inspect SQL commands issued using local connections to the database through loopback (non-Oracle and Oracle) and bequeath (Oracle) when the Database Firewall is deployed in Monitoring (Host Monitor) mode. With this feature, the Host Monitoring Agent has complete visibility into database activities performed by all users including administrators accessing the database server as such. For a comprehensive visibility, it is recommended to augment network monitoring with database auditing. Database auditing running inside the Oracle Database has complete visibility into the internal jobs or procedure execution which typically network monitoring might not have access to. Database auditing cannot be bypassed by the use of synonyms or dynamically generated names, while network monitoring policies should be trained for all such possible combinations to make it foolproof.

Related Topics

- Monitoring (Host Monitor)
  In **Monitoring (Host Monitor)** mode, the Database Firewall monitors and alerts on SQL traffic, but it can't block or substitute SQL statements.
- *Oracle Audit Vault and Database Firewall Auditor's Guide*

8.2 Installing and Enabling the Host Monitor Agent

Use this process to install and enable the Host Monitor Agent.

1. Deploy the Host Monitor Agent on all the database servers where the database is running.
2. Register the target.
3. Create a Database Firewall monitoring point in **Monitoring (Host Monitor)** mode.
4. Change the Database Firewall policy for the target from *Default* to the appropriate policy, if needed.

   See Types of Database Firewall Policies for the different policy types.
5. Configure a `NETWORK` audit trail for the monitored target.

> **Note:**
>
> - The Host Monitor Agent is supported on Linux, Solaris, AIX, and Windows platforms. It can monitor any database that is supported by the Database Firewall. See Table C-1 for supported databases.
> - The Host Monitor Agent supports the Solaris IPNET link type on Oracle Solaris SPARC64 and x86-64.
> - The Host Monitor Agent supports the Ethernet (EN10MB) link type for all supported platforms.
> - Starting in AVDF 20.13, the Host Monitoring Agent can inspect SQL commands issued using local connections to the database through loopback (non-Oracle and Oracle) and bequeath (Oracle) when the Database Firewall is deployed in Monitoring (Host Monitor) mode. With this feature, the Host Monitoring Agent has complete visibility into database activities performed by all users including administrators accessing the database server as such. For a comprehensive visibility, it is recommended to augment network monitoring with database auditing. Database auditing running inside the Oracle Database has complete visibility into the internal jobs or procedure execution which typically network monitoring might not have access to. Database auditing cannot be bypassed by the use of synonyms or dynamically generated names, while network monitoring policies should be trained for all such possible combinations to make it foolproof.

Related Topics

- Host Monitoring Agent Installation Fails With Error About Inability to Retrieve Agent Details

8.2.1 Host Monitor Agent Requirements

The Host Monitor Agent has different requirements for installation, depending on the platform.

To install the Host Monitor Agent on the Windows platform, follow these requirements:

- Ensure that the Audit Vault Agent is running on the database server machine.
- Follow the Npcap installation requirements for your Oracle Audit Vault and Database Firewall (Oracle AVDF) release.

Host Monitoring on Windows requires Npcap for capturing network traffic.

  - For Oracle AVDF release 20.6 and later, Npcap is automatically installed along with the agent installation.

    Installing Npcap removes any existing installation of Npcap or WinPcap from the Windows host machine.

  - For Oracle AVDF release 20.5, Npcap is automatically downloaded along with the agent software (`agent.jar`) file.

    Use the Npcap installer file that is available under the `Agent_Home\hm` directory.

  - For Oracle AVDF release 20.4 and earlier, install Npcap from the `avdf20-utility.zip` bundle on Oracle Software Delivery Cloud. It is part of the Oracle AVDF installable files. Select the *WinPcap-API-compatible* option when installing Npcap.

- Install the latest version of the OpenSSL (1.1.1g or higher) libraries.
  OpenSSL 1.1.1 and earlier on Windows platforms was deprecated in Oracle AVDF 20.11, and it will be desupported in one of the future releases. To prevent issues, you should move to OpenSSL 3.0.13 or later.
- Ensure that the Windows target machine has the latest update of the Visual C++ Redistributable for Visual Studio 2015 (`MSVCRT.dll (*)` or later) package from Microsoft installed.
- If a network firewall is present, allow communication on port range 2050 - 5200.

  This is required for communication between the database server and the Database Firewall.

To install the Host Monitor Agent on a Linux, Unix, AIX, or Solaris platform, follow these requirements:

- Ensure that the Audit Vault Agent is running on the database server machine.
- Ensure that the latest version of the following packages from the operating system vendor are installed for the specific operating system version on the database server machine:
  - Libcap (for Linux hosts only)
  - LibPcap
  - OpenSSL
- Ensure that `gmake` is installed for AIX database servers.

  For other Unix database server types (Linux, Unix, or Solaris), ensure that `make` is installed. This is required for the Host Monitor Agent to run successfully.
- If a network firewall is present, allow communication on port range 2050 - 5200.

  This is required for communication between the database server and the Database Firewall.
- Ensure that the input output completion ports (IOCP) setting is `available` for IBM AIX on Power Systems (64-bit).

  It's set to `defined` by default.
- Ensure that all directories in the path of the Host Monitor Agent install location have 755 as the permission bits, starting from the root directory.

  This is required because the Host Monitor Agent has to be installed in a *root*-owned location.

- Ensure that the Host Monitor Agent is installed by the *root* user.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

> **See Also:**
>
> Enabling and Using Host Monitoring for host monitoring instructions and prerequisites.

8.2.2 Validation During Host Monitor Agent Deployment

Learn about validations performed by Oracle AVDF when deploying the Host Monitor Agent.

Starting with Oracle AVDF release 20.6, the following validations are performed on the Linux/Unix/AIX/Solaris platforms when deploying the Host Monitor Agent. These requirements are mandatory and must be complied with; without meeting them, the Host Monitor Agent installation cannot be completed.

- The Host Monitor Agent is being installed as *root* user.
- When installing the Host Monitor Agent on a Windows platform, it must be installed by an administrator user.
- If Host Monitor Agent process is already running on the host machine.
- If the Input Output Completion Ports (IOCP) is set to `available` for IBM AIX on Power Systems (64-bit).
- If *gmake* is installed for AIX database servers. For other Unix database server types (Linux/Unix/Solaris), check if *make* is installed.
- If symlinks of `libssl`, `libcrypto`, `libnsl` libraries are present. In case of Linux, a check for additional symlink `libaio` is performed.

> **Note:**
>
> If you run into any issues, see the following topics for more information:
>
> - Troubleshooting Oracle Audit Vault and Database Firewall
> - Known Issues

8.2.3 Registering the Host Machine That Will Run the Host Monitor Agent

Learn how to register the host machine (such as a database server) on the Audit Vault Server.

To register a host on the Audit Vault Server, see Registering Hosts on the Audit Vault Server.

8.2.4 Deploying the Audit Vault Agent and Host Monitor Agent

Learn how to deploy the Audit Vault Agent and Host Monitor Agent on platforms like Linux, Solaris (x86-64), Solaris (Sparc64), AIX, and Windows.

8.2.4.1 Deploying the Host Monitor Agent on a Windows Host Machine

On Windows, the Host Monitor Agent is installed by the Audit Vault Agent. There are no separate Host Monitor Agent installable bundles available for download in the Audit Vault Server console. No separate action is required to install the Host Monitor Agent on Windows.

Follow these instructions before installing the Host Monitor Agent or updating from an older Oracle AVDF release.

Prerequisites

- Audit Vault Agent Requirements
- Host Monitor Agent Requirements

Related Topics

- Deploying the Audit Vault Agent
  Learn about deploying the Audit Vault Agent.
- Registering and Unregistering the Audit Vault Agent as a Windows Service
  Learn about registering and unregistering Oracle Audit Vault Agent as a Windows service.

8.2.4.1.1 Installing OpenSSL

The Host Monitor Agent uses OpenSSL to communicate with the Audit Vault Server and Database Firewall. OpenSSL 1.1.1g (or later) must be installed on the Windows host machine.

OpenSSL 1.1.1 and earlier on Windows platforms was deprecated in Oracle AVDF 20.11, and it will be desupported in one of the future releases. To prevent issues, you should move to OpenSSL 3.0.13 or later.

> **Note:**
>
> While installing OpenSSL on Windows machine, you are prompted to choose a location to copy the OpenSSL DLLs as an additional configuration step. It is recommended that you choose the **Windows System Directory** option, as this location is added to the `Path` environment variable on Windows machine by default. Else, if you choose the **OpenSSL bin directory** option, then ensure the location is added to the `Path` environment variable.

Follow these steps to change environment variables after installing OpenSSL:

1. In the Windows host machine, navigate to **Control Panel**.
2. Click **System**, and then click **Advanced system settings**.
3. In the **Advanced** tab, click on **Environment Variables** button.
4. The **Environment Variables** dialog is displayed. In the **System variables box**, select `Path` under the **Variable** column.
5. Click **Edit** button. The **Edit environment variable** dialog is displayed.
6. Add the location of the OpenSSL *bin* directory at the beginning of the `Path` variable.
7. Click **OK** to save the changes, and then exit all the dialogs.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

8.2.4.1.2 Installing Npcap

Host Monitoring on Windows requires Npcap for capturing network traffic.

8.2.4.1.2.1 Installing Npcap for a Fresh Installation of the Host Monitor Agent

Follow these steps to install Npcap for a fresh installation of the Host Monitor Agent.

> **Note:**
>
> For Oracle AVDF release 20.6 and later, Npcap is automatically installed along with the Agent installation. Installing Npcap removes any existing installation of Npcap or WinPcap from the Windows host machine. The following steps are not required for release 20.6 and later.

1. Log in to Oracle Software Delivery Cloud.
2. Note and follow Npcap manual installation details:
   - For Oracle AVDF release 20.5 and later, Npcap is automatically downloaded along with the Agent software (`agent.jar`) file. The Npcap installer file is available under `Agent_Home\hm` directory.
   - For Oracle AVDF release 20.4 and earlier, install Npcap that is available in the `avdf20-utility.zip` bundle in Oracle Software Delivery Cloud. It is part of the Oracle Audit Vault and Database Firewall installable files. Ensure to install Npcap in *WinPcap-API-compatible* mode.
3. Install Npcap. For Oracle AVDF releases 20.5 and earlier, complete the Npcap installation on the Windows host machine. Ensure to install in *WinPcap-API-compatible* mode. Installing Npcap in WinPcap API compatible mode removes any existing installation of WinPcap from the Windows machine.

8.2.4.1.2.2 Updating from Oracle AVDF 12.2 BP13, 12.2 BP14, or 20.1 - 20.4 to Oracle AVDF 20.5 or Later

Before updating from Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 BP13, 12.2 BP14, or 20.1 - 20.4 to Oracle AVDF 20.5 or later, follow these steps to reinstall Npcap.

1. Log in to Oracle Software Delivery Cloud.
2. Reinstall the Npcap that is available in the `avdf20-utility.zip` bundle on the Oracle Software Delivery Cloud. It's part of the Oracle AVDF installable files.

   Be sure to reinstall Npcap in *WinPcap-API-compatible* mode. This removes any existing installations of Npcap or WinPcap from the Windows machine.

8.2.4.1.2.3 Updating from Oracle AVDF 12.2 BP9 or 12.2 BP10 to Oracle AVDF 20.1 or Later

Before updating from Oracle Audit Vault and Database Firewall (Oracle AVDF) 12.2 BP9 or 12.2 BP10 to Oracle AVDF 20.1 or later, follow these steps to reinstall Npcap.

Host Monitoring on Windows functionality requires Npcap. Follow these steps to continue using Host Monitor Agent on Windows from 12.2.0.9.0 or 12.2.0.10.0, before upgrading to Oracle Audit Vault and Database Firewall release 20:

1. Stop the Audit Vault Agent running on the Windows host machine.
2. Log in to 12.2 Audit Vault Server console as administrator.
3. Verify the audit trails and the Audit Vault Agent are in `STOPPED` state.
4. Log in to My Oracle Support, and download Npcap that is available with Oracle AVDF release 20 upgrade files.
5. Complete the Npcap installation on the Windows host machine. Ensure to install in *WinPcap-API-compatible* mode.

> **Note:**
>
> Installing Npcap in *WinPcap API compatible* mode removes any existing installation of WinPcap from the Windows machine.

6. Follow verification steps below to ensure Npcap installation is completed successfully.
7. Restart the Audit Vault Agent on the Windows host machine.
8. Start the network trails using the Audit Vault Server console.
9. The Host Monitor Agent is now powered by Npcap during runtime. Verify the network trail collection.
10. Proceed with the Audit Vault Server upgrade.

> **Note:**
>
> - Ensure the audit trails and the Audit Vault Agent are in `STOPPED` state, before installing Npcap. Else, an error may be encountered.
> - Do not delete the DLL files as they are created newly by Npcap installation.

8.2.4.1.2.4 Verifying the Npcap Installation

After you install or upgrade Npcap, verify that the installation was successful.

1. In addition to the Windows `System` directory, Npcap copies the DLL files to the Npcap sub-directory inside the Windows `System` directory. Do not remove the DLL files from the Windows `System` directory.

> **Note:**
>
> Installing Npcap in *WinPcap API compatible* mode, adds the Npcap DLL files to the Windows `System` directory which is already there in the system `Path` environment variable.

2. Add the `Npcap` sub directory inside the Windows `System` directory to the `Path` environment variable by following the steps below:

a. Navigate to **Control Panel**.

b. Click **System**, and then click **Advanced system settings**.

c. In the **Advanced** tab, click on **Environment Variables** button.

d. The **Environment Variables** dialog is displayed. In the **System variables box**, select `Path` under the **Variable** column.

e. Click **Edit** button. The **Edit environment variable** dialog is displayed.

f. Add the location of the Npcap DLL files at the beginning of the `Path` variable. For example: `C:\Windows\System32\Npcap`

g. Click **OK** to save the changes, and then exit all the dialogs.

3. Confirm the changes in the `Path` environment variable.

8.2.4.2 Deploying the Host Monitor Agent on a Unix Host Machine

Learn about deploying the Host Monitor Agent on Unix hosts.

Prerequisite
Host Monitor Agent Requirements

1. Before you install the Host Monitor Agent, ensure you have deployed the Audit Vault Agent.

   See Deploying the Audit Vault Agent.

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 Agent.

   Note: The entire directory hierarchy must be `root`-owned. All the directories in this hierarchy must have `read` and `execute` permission for other users or groups, but not `write` permission.

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

4. Click the **Agents** tab.

5. In the left navigation menu:

For release	Action
20.1 and 20.2	Click **Agent Software**
20.3 and later	Click **Downloads**

6. On the page listing the agent software, click the **Download** button corresponding to your Unix version, 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`.

7. As `root` user, unzip the Host Monitor Agent file, `agent-<platform>-hmon-one.zip` (for example, `agent-linux-x86-64-hmon-one.zip`).

   This creates a directory named `hm`. This is your *`HM_Home`* directory, which in this example is `/usr/local/hm`.

8. Ensure that the `hostmonsetup` file (in the `hm` directory) has the *execute* permission for the owner.

9. Run the following command from the `HM_Home` directory:

   `HM_Home``/hostmonsetup install [agentuser=`*`Agent_Username`*`] [agentgroup=`*`Agent_Group`*`]`

- *HM_Home* - The directory created in Step 7.
- *Agent_Username* - (Optional) Enter the user name of the user who installed the Audit Vault Agent (the user who executed the `java -jar agent.jar` command).
- *Agent_Group* - (Optional) Enter the group to which the *Agent_Username* belongs.

> **See Also:**
>
> Using Audit Vault Server Console

8.2.5 Creating a Target for the Host-Monitored Database

Learn how to create a target for the host-monitored database.

To create a target, see Registering or Removing Targets in Audit Vault Server.

8.2.6 Creating a Monitoring Point for the Host Monitor Agent

A monitoring point is a logical entity on the Database Firewall host that contains the configuration and rules for monitoring the SQL traffic that is received.

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

   The **Targets** tab in the left navigation menu is selected by default.
3. Select and click on a specific target from the list.
4. From the **Database Firewall Monitoring** section on the main page, click on **Add**. The **Database Firewall Monitor** dialog is displayed.
5. In the **Basic** tab (for 20.3 or later the name of the tab is **Core**), enter the name for the **Database Firewall** instance or select one from the list.
6. Select **Monitoring (Host Monitor)** as the deployment type from the list. In this mode, the Database Firewall can only monitor the SQL traffic.
7. Choose a **Network Interface Card** for the Database Firewall host from the list.

> **Note:**
>
> - For Oracle AVDF 20.2 and earlier, it is recommended to select a network interface card that is not used as a Management Interface. This segregates the traffic from Host Monitor Agent to the Database Firewall and the traffic from the Database Firewall to Audit Vault Server.
> - For Oracle AVDF release 20.3 and later, you must select a network interface card which has an IP address configured. All the network interface cards which have an IP address configured are displayed in the **Network Interface Card** list. It is recommended to select a network interface card that is not used as a Management Interface. This segregates the traffic from Host Monitor Agent to the Database Firewall and the traffic from the Database Firewall to Audit Vault Server.

8. In the **Connection Details** section, select one or more targets for which the traffic needs to be monitored. You can **Add** the targets from the list.

> **Note:**
>
> For Exadata or Oracle RAC, enter both the physical and virtual IP's of the nodes but not the SCAN IPs in the **Target Connections** field.

> **Note:**
>
> For Oracle RAC, enter the IP address of the individual RAC node in the **Target Connections** field.

Enter the following information for each available connection of the database. Click the **Add** button to add more targets and enter the following fields:

- **Host Name / IP Address**
- **Port**
- **Service Name** (Optional, for Oracle Database only). SID can be used in this field. To enter multiple service names and/or SIDs, enter a new line for each of them, and then click **Add**. Multiple entries are allowed for monitoring only mode.
  - Oracle AVDF 20.1-20.9: You need to configure a proxy target for each OSN. This is because a single proxy port cannot service multiple OSN's on the same target database. Add more traffic proxy ports as required.
  - Oracle AVDF 20.10 and later: You can use one proxy port and specify multiple OSN's on the target database that are going to be processed. Specify the OSN's in a list delimited by the "|" character. For example, target1|target2|target 3.

> **Note:**
>
> Starting with Oracle AVDF release 20.7, for Linux hosts with multiple network devices, add a row for every network device from which the database traffic is expected to arrive.

9. Click the **Advanced** tab, enter the number of **Database Firewall Monitor Threads** (minimum value is 1). This controls the number of traffic handling threads in the Database Firewall monitoring point. The default value is 1. This value can be increased when high transactions are reported (per second traffic) and packet dropped messages are reported in the `/var/log/messages` file. Contact Oracle Support while changing this number.
10. Select the check box for **Decrypt With Network Native Encryption Key** field only for Oracle Database targets. This is for enabling decryption of traffic if the database is using Oracle Native encryption. Decrypt with network native encryption key option also supports retrieval of session information for Oracle Database. Complete the remaining fields as applicable.

    For Oracle standalone database targets, enter the IP address of the database listener in the **IP Address** field.

For Sybase SQL Anywhere (Oracle AVDF 20.1-20.6 only) and Microsoft SQL databases, the field is **Retrieve session information from target DB**. Retrieving session information is not available for any other non-Oracle database types.

Select this field to retrieve session information such as OS User Name, DB User Name, client application name, and IP address from the target database.

> **Note:**
>
> Ensure the Database Firewall is allowed to make a network connection to the above mentioned database.

11. Click **Save** at the bottom of the dialog to save the configuration of the monitoring point.

    The new monitoring point appears in the list and starts automatically.

> **Note:**
>
> `Default Database Firewall Policy will be applied for this Database Firewall Monitoring Point`. This message is displayed at the bottom of the dialog.

12. Click **Save** in the main page.
13. To stop or restart the monitoring point, select it from the **Database Firewall Monitoring** section and click **Stop** or **Start**.

> **See Also:**
>
> Configuring Database Firewall Monitoring Points

8.2.7 Create a Network Audit Trail

Learn how to create network audit trails.

Specify NETWORK for the audit trail type, see Adding Audit Trails with Agent-Based Collection for more information.

For monitoring multiple nodes of an Exadata or RAC database using network trail, create a separate target for each node.

> **Note:**
>
> For Oracle AVDF versions prior to 20.13: Ensure that the collection attribute `network_device_name_for_hostmonitor` is configured for the targets monitored by the Host Monitor Agent. The name of the network interface card (NIC) is the attribute value. The NIC receives all the network traffic of the target database.

> **Note:**
>
> Starting with Oracle AVDF 20.13: A network trail can be added with a location that points directly to the network interface card. The `network_device_name_for_hostmonitor` attribute is no longer required.
>
> - If you're upgrading to Oracle AVDF 20.13, the trail location will automatically populate based on the value of the `network_device_name_for_hostmonitor` attribute, if it was set in the previous version.
> - If the attribute was not set, a random value will be selected and populated as the trail location. If this is incorrect, you can drop the trail and add it again with the correct location.

Starting with AVDF 20.10, network trails are monitored hourly. Alerts are generated and email notifications are sent out if network trail is in `STOPPED_ERROR` state.

Related Topics

- Check the Value of the network_device_name_for_hostmonitor Attribute

8.2.8 Check the Value of the `network_device_name_for_hostmonitor` Attribute

The collection attribute `network_device_name_for_hostmonitor` should be configured for the targets that are monitored by the Host Monitor Agent. The attribute value is the name of the network interface card. The network interface card receives all the network traffic of the target database. Follow these steps to check the value of the `network_device_name_for_hostmonitor` attribute.

> **Note:**
>
> Starting with Oracle AVDF 20.13, this section is no longer necessary.

Linux/AIX/Solaris Hosts

1. Determine the IP address on which the target database is configured to accept TCP traffic. Make a note of the IP address.
2. Execute the following command to list the network device details present in the host machine:

   ```
   ifconfig -a
   ```

3. From the output displayed, search for the IP address that was noted in the initial step. The corresponding name of the network card is the value of the collection attribute `network_device_name_for_hostmonitor`.

Windows Hosts

1. Determine the IP address on which the target database is configured to accept TCP traffic. Make a note of the IP address.

2. Execute the following command to list the network device details present in the host machine:

   ```
   ipconfig /all
   ```

   > **Note:**
   >
   > This command displays the Physical Address, IPv4 Address, and other details for every device.

3. From the output displayed, search for the device which has an IPv4 Address that was noted in the initial step. Make a note of the corresponding Physical Address.
4. Execute the command:

   ```
   getmac
   ```

   This will display the device name against the corresponding Physical Address. Make a note of the Device Name for the Physical Address determined in the previous step.
5. After the Device Name is determined, observe it is in the following form:`\Device\Tcpip_{********-****-****-****-************}`.
6. Copy this Device Name to use as the attribute value by replacing `Tcpip` with `NPF`. For example, for a network card with the name `\Device\Tcpip_{********-****-****-****-************}` the attribute value is, `\Device\NPF_{********-****-****-****-************}`.

8.3 Starting, Stopping, and Other Host Monitor Agent Operations

Learn about starting, stopping, and other Host Monitor Agent operations.

8.3.1 Starting the Host Monitor Agent

Starting the Host Monitor Agent involves starting collection for the NETWORK audit trail on the host that you're monitoring.

To start the Host Monitor Agent 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 Create a Network Audit Trail.

> **See Also:**
>
> - Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server
> - Using Audit Vault Server Console

8.3.2 Stopping the Host Monitor Agent

To stop the Host Monitor Agent, stop the audit trail that you created for the target that is being monitored.

See Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server.

8.3.3 Changing the Logging Level for a Host Monitor Agent

Learn about changing the logging level for Host Monitor Agents.

See Changing the Logging Level for the Audit Vault Agent.

8.3.4 Viewing Host Monitor Agent Status and Details

You can view whether a Host Monitor Agent is installed and information like its location, version, update time, and other details.

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Agents** tab.
3. In the left navigation menu, select **Agent Hosts**.
4. In the page that appears, check the Host Monitor Status and the Host Monitor Details columns for the host you are interested in.

> **See Also:**
>
> Using Audit Vault Server Console

8.3.5 Checking the Status of a Host Monitor Agent Audit Trail

Learn how to check the status of a Host Monitor Agent audit trail.

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab, and then from the left navigation menu, select **Audit Trails**.
3. In the status page that appears, in the Audit Trail Type column, search for audit trails of type NETWORK to find audit trails for Host Monitor Agents.

8.3.6 Uninstalling a Host Monitor Agent (Unix Hosts Only)

This procedure applies to Unix hosts only. On Windows hosts, the Host Monitor Agent is installed as part of the Audit Vault Agent, so you don't need to uninstall the Host Monitor Agent. However after uninstalling the Audit Vault Agent from a Windows host, you should also uninstall Npcap.

1. Log in to the host computer as `root`.
2. From the *`HM_Home`* directory (where you installed the Host Monitor Agent in Step 7) run the following command:

   ```
   hostmonsetup uninstall
   ```

8.4 Updating a Host Monitor Agent (Unix Hosts Only)

When you update the Audit Vault Server to a new release, the Host Monitor Agent is automatically updated.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Installation Guide*

8.5 Using Mutual Authentication for Communication Between the Database Firewall and the Host Monitor Agent

By default, the Database Firewall allows the Host Monitor Agent connection based on one-way authentication. To provide mutual authentication, follow these steps after installing the Host Monitor Agent.

1. Stop the network trail associated with the firewall where mutual authentication needs to be enabled.
2. On the Database Firewall, log in as `root` and run the following commands:
   - For Oracle AVDF release 20.7 and later:

     ```
     cp /usr/local/dbfw/etc/controller.crt /usr/local/dbfw/etc/fw_ca.crt

     chown arbiter:arbiter /usr/local/dbfw/etc/fw_ca.crt

     chmod 400 /usr/local/dbfw/etc/fw_ca.crt

     /usr/local/dbfw/bin/dbfwctl restart
     ```

   - For Oracle AVDF release 20.6 and earlier:

     ```
     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

     /usr/local/dbfw/bin/dbfwctl restart
     ```

3. On the Audit Vault Server, log in as `root` and complete the following steps:
   a. Change to the `/usr/local/dbfw/etc` directory.

b. Run the following commands:

```
openssl genrsa -out hmprivkey.perm 2048
```

```
openssl req -new -key hmprivkey.perm -out hmcsr.csr -subj "/
CN=Hostmonitor_Cert_hostname/"
```

The *hostname* is the name of the database server where the Host Monitor Agent is installed.

c. Generate a signed certificate by running the following command:

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

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

4. Copy the following files from the Audit Vault Server to the HOSTMON_HOME directory on the database server where the Host Monitor Agent is installed:
   - `/usr/local/dbfw/etc/hmcert.crt`
   - `/usr/local/dbfw/etc/hmprivkey.perm`
5. (Unix 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
```

6. (Windows hosts only) Ensure that the `hmcert.crt` and `hmprivkey.perm` have `agent` user ownership and appropriate permissions to prevent unwanted user access.
7. Repeat steps three to six for every Host Monitor Agent that is using the Database Firewall from step 2 .
8. Start all the network trails to capture the network traffic.
9. If more than one Database Firewall is used, repeat all the above steps for each.

Related Topics

- Starting, Stopping, and Other Host Monitor Agent Operations
  Learn about starting, stopping, and other Host Monitor Agent operations.

9

High Availability in Oracle AVDF

Oracle AVDF supports high availability for Audit Vault Server and Database Firewall.

9.1 About High Availability in Oracle AVDF

Learn about high availability in Oracle AVDF.

High availability in Oracle AVDF increases reliability by ensuring continuity in Database Activity Monitoring services like audit data collection, network event data collection, analysis, reporting, etc. High availability requires a pair of Audit Vault Server instances or a pair of Database Firewall instances. One instance works as the primary and another instance works as the standby.

9.2 Configuring High Availability for Audit Vault Servers

Learn about configuring, monitoring, or updating high availability for Audit Vault Servers.

9.2.1 About High Availability in Audit Vault Servers

High availability in Audit Vault Server involves two Audit Vault Server instances that are paired for business continuity.

In this configuration, you designate one Audit Vault Server instance as the primary and the other as the standby. The primary Audit Vault Server is the active server that provides the Audit Vault Server functionality. The standby is automatically synchronized (audit data and network event data) and has a consistent copy of the primary.

If the primary Audit Vault Server becomes unavailable because of an unplanned outage for a period of 10 minutes, the configuration automatically fails over (failover) to the standby server. The earlier standby becomes the new primary.

In high availability, configuration data pertaining to target registration, Audit Vault Agent machine registration, and Database Firewall configuration is automatically synchronized with the standby.

The high availability in Audit Vault Server is internally managed by using Oracle Data Guard. You deploy the pair of Audit Vault Servers in maximum performance mode. This ensures the highest level of data protection without affecting the performance of the primary Audit Vault Server instance.

> **Note:**
>
> The *archivelog* mode is enabled after you set up high availability. High availability requires *archivelog* mode, so don't disable it after you set up high availability.

> **Best Practice:**
>
> Oracle recommends that you configure high availability for the Audit Vault Servers before deploying Audit Vault Agents and Database Firewalls.

> **See Also:**
>
> Oracle Data Guard Protection Modes

The Audit Vault Servers in high availability communicate through HTTPS and Oracle Net. There are no restrictions on where the Audit Vault Servers are located, as long as they can communicate with each other.

Important Points to Consider Before Configuring High Availability

Because existing data on the designated standby Audit Vault Server is purged during high availability configuration, consider the following points:

- Impact on existing Database Firewalls: All Database Firewalls that are registered with the designated standby Audit Vault Server must be registered again after high availability is configured.
- Impact on existing Audit Vault Agents: There is no impact on the Audit Vault Agents that are registered on the designated primary Audit Vault Server.

  However, all the registered Audit Vault Agents on the designated standby Audit Vault Server must be redeployed on the primary after high availability is configured. See Post High Availability Pairing Steps.
- Impact on existing audit trails and Database Firewall monitoring points: Because audit and network event data that is collected from targets by the designated standby Audit Vault Server is purged during high availability configuration, you must reconfigure these audit trails and Database Firewall monitoring points on the Audit Vault Server after high availability is configured to ensure that these targets continue to be protected.
- From Oracle AVDF 20.9 to 20.12, agentless collection was supported only on standalone, unpaired Audit Vault Servers (AVS). Starting with Oracle AVDF 20.13, agentless collection is supported on both standalone and high availability AVS.

Audit Vault Server High Availability Configuration Process

To configure Audit Vault Servers for high availability, follow this high-level process:

1. Install two standalone Audit Vault Servers to use as the primary and standby servers.

   > **Best Practice:**
   >
   > Place the two Audit Vault Servers in two different data centers.

2. Configure the designated standby Audit Vault Server.
3. Configure the designated primary Audit Vault Server.

9.2.2 Prerequisites for Configuring High Availability for Audit Vault Servers

Ensure that you meet these prerequisites before configuring high availability for Audit Vault Servers.

1. Install two standalone Audit Vault Servers to use as the primary and standby servers.
2. Ensure that the designated primary and standby Audit Vault Servers have identical configurations so that they can stand in for each other. All of the following configurations should be the same:
   - Oracle Audit Vault and Database Firewall (Oracle AVDF) version
   - Total system memory
   - Total repository storage size
   - Number of NFS archive locations
   - Repository encryption status
3. Ensure that the system time difference between the two Audit Vault Servers is less than 60 seconds.

Related Topics

- Specifying Initial System Settings and Options on Audit Vault Server (Required)
  Learn how to specify initial system settings and options on Audit Vault Server.

9.2.3 Configure the Designated Standby Audit Vault Server

Learn how to configure the designated standby Audit Vault Server.

1. Make a note of the IP address of the designated primary Audit Vault Server.
2. Copy the server certificate of the designated primary Audit Vault Server:
   a. Log in to primary Audit Vault Server console as *super administrator*.
   b. Click the **Settings** tab. The **Security** tab in the left navigation menu is selected by default.
   c. Now, click the **Certificate** sub tab in the main page.
   d. Click the **Server Certificate** sub tab.
   e. Click the **Copy Certificate** button.
3. In the left navigation menu of the designated standby Audit Vault Server, perform these steps:
   a. Select **System** tab.
   b. Click **High Availability** link under the **Configuration** section on the main page.
   c. In the **Configure High Availability** dialog, the **Current status** field indicates the status of the current Audit Vault Server, which is *Standalone*.
   d. In the **Configure this server as** field, select the **Standby server** option.
   e. In the expanded **Configure High Availability** dialog, enter the following settings:
      - **Primary server IP address**: Enter the IP address of the designated primary Audit Vault Server.

- **Primary server certificate**: Paste the certificate that you copied from the designated primary Audit Vault Server.

f. Click **Save**. The designated primary Audit Vault Server's IP address and certificate is now saved on the standby Audit Vault Server, and is now ready to be paired.

9.2.4 Configure the Designated Primary Audit Vault Server

Learn how to configure the designated primary Audit Vault Server.

1. Make a note of the IP address of the designated standby Audit Vault Server.
2. Copy the server certificate from the designated standby Audit Vault Server:
   a. Log in to the designated standby Audit Vault Server console as *super administrator*.
   b. Click the **Settings** tab. The **Security** tab in the left navigation menu is selected by default.
   c. Now click the **Certificate** sub tab in the main page.
   d. Click **Server Certificate** sub tab.
   e. Click the **Copy Certificate** button.
3. Log in to the designated primary Audit Vault Server console as *super administrator* and perform these steps:
   a. In the left navigation menu, select **System** tab.
   b. Click **High Availability** link under the **Configuration** section in the main page.
   c. In the **Configure High Availability** dialog, the **Current status** field indicates the status of the current Audit Vault Server, which is *Standalone*.
   d. In the **Configure this server as** field, select the **Primary server** option.
   e. In the expanded **Configure High Availability** window, enter the following settings:
      - **Standby server IP address**: Enter the IP address of the standby Audit Vault Server.
      - **Standby server certificate**: Paste the certificate that you copied from the standby Audit Vault Server.
   f. Click **Initiate Pairing** button at the bottom of the dialog, to initiate high availability pairing. To get the updated status, refresh the Audit Vault Server console periodically, as the process can take at least 15 minutes. This process can take longer depending on the amount of data in the repository. When the high availability pairing is complete, the **High Availability Status** field in the main page displays the current status.

> **Note:**
>
> - After high availability pairing is successfully completed, perform all the configuration tasks on the primary Audit Vault Server only. This includes tasks such as downloading the Audit Vault Agent, registering targets and hosts, adding Database Firewalls and monitoring points. To perform tasks like setting system time or changing IP address for the standby Audit Vault Server refer to section Specifying the Server Date, Time, and Keyboard Settings.
> - During high availability pairing, the NFS archive locations pertaining to the primary and standby Audit Vault Servers are mapped. The mapping of these locations is displayed in the primary Audit Vault Server console after high availability pairing is successful.

9.2.5 Checking the High Availability Status of an Audit Vault Server

Learn how to check the high availability status of an Audit Vault Server.

After high availability pairing is successfully completed, the standby Audit Vault Server console is not accessible. Perform all tasks on the primary Audit Vault Server console. If you attempt to access the standby Audit Vault Server console, it redirects to the primary Audit Vault Server console.

Check High Availability Status Through the Console

1. In the Audit Vault Server console, click the **Settings** tab.
2. In the left navigation menu, select **System**.
3. Under the **Status** section, check the **High Availability Status** field.
   The possible values are:
   - **Standalone** - This server is not configured for high availability and is a standalone instance.
   - **Primary** - This server is currently the primary Audit Vault Server.
   - **Disconnected** - This primary Audit Vault Server switches to this mode if it detects that the standby Audit Vault Server changed its role to standalone or primary. This indicates that the high availability pairing is broken. Contact Oracle Support for further assistance.

Check High Availability Status Through Commands

1. Log in to the Audit Vault Server through SSH as the `support` user.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

```
ssh support@<audit_vault_server_ip_address>
```

2. Switch to the `root` user.

```
su - root
```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

3. Switch to the `oracle` user.

```
su - oracle
```

4. Run the following command

```
/usr/local/dbfw/bin/setup_ha.rb --status
```

The output of above command will tell the current high availability (HA) status and different properties such as Data Guard broker status, fast recovery area usage, and apply lag of HA system.

9.2.6 Post High Availability Pairing Steps

Learn post high availability pairing steps for Audit Vault Agents and Host Monitor Agents.

Audit Vault Agents and Host Monitor Agents deployed on the designated primary Audit Vault Server require no further action. The information of Audit Vault Agents is replicated to the standby Audit Vault Server during high availability pairing.

Audit Vault Agents and Host Monitor Agents deployed on the designated standby Audit Vault Server will be unable to communicate with the designated primary Audit Vault Server after high availability pairing. To redeploy the Agents on the specific Agent machines, follow these steps:

1. Clean up the `Agent_Home` folder on the Agent machine.

Agent installed on Windows host machine	Agent installed on Linux (or other Unix) machine
a. Run the command `agentctl.bat unregistersvc` from the `Agent_Home` directory. b. Remove the contents in the `Agent_Home` directory on the Agent host machine.	Remove the contents in the `Agent_Home` directory on the Agent host machine.

2. Register the Agent on the Audit Vault Server and activate.
3. Download the `agent.jar` file from the Audit Vault Server console.
4. Copy the `agent.jar` file to the `Agent_Home` directory on the Agent host machine.
5. In the `Agent_Home` directory, run the following command:

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

6. Run the following command and provide the Agent activation key when prompted. The key is available on the Audit Vault Server console.

```
agentctl start -k
```

> **Note:**
>
> This key is not displayed as you type.

> **See Also:**
>
> Deploying the Audit Vault Agent on Host Computers

9.2.7 Audit Vault Agent Communication with Audit Vault Server in High Availability

Learn how Audit Vault Agent communicates with Audit Vault Server.

Audit Vault Agent software is packaged with the connection details pertaining to Audit Vault Server. In case of high availability environment, the Audit Vault Agent software is packaged with the connection details pertaining to both the primary and standby Audit Vault Servers.

Existing Audit Vault Agents on the designated primary Audit Vault Server receive the connection details of both the primary and standby Audit Vault Servers during high availability configuration. New Audit Vault Agents that are deployed after high availability configuration are also packaged with the connection details pertaining to both the primary and standby Audit Vault Servers.

In the event of Audit Vault Server failover, the Audit Vault Agents reconnect to the new primary Audit Vault Server (previous standby).

9.2.8 Swapping Roles Between a Primary and Standby Audit Vault Server

Learn how to swap the roles of the primary and standby Audit Vault Servers.

1. If automatic failover is disabled, enable it. See Disabling or Enabling Failover of the Audit Vault Server.
2. Ensure that the status of the Oracle Data Guard observer is `YES`. To check the status, run the following commands on each Audit Vault Server:
   a. Using the ssh utility, run the following command:

      ```
      ssh support@<IP address of Audit Vault Server>
      ```

   b. Log in as the *root* user.

      ```
      su root
      ```

   c. Switch to the *oracle* user.

      ```
      su oracle
      ```

d. Run the following command:

```
/usr/local/dbfw/bin/setup_ha.rb --status
```

The `Data guard observer` field in the output should say `YES`.

3. Log in to the Audit Vault Server console as a *super administrator*.
4. Click the **Settings** tab.
5. In the left navigation menu, select **System**.
6. In the **Configuration** section, click **High Availability**. The **Configure High Availability** dialog appears.
7. Click **Switch Roles**.
8. In the confirmation window, click **OK**.

   A message shows the progress of the high availability configuration. During this process, which takes at least 10 minutes, the console is unavailable. Refresh the browser periodically. When the configuration is complete, it redirects to the new primary Audit Vault Server.

Related Topics

- Using Audit Vault Server Console
  Learn how to log in and use Audit Vault Server console.

9.2.9 Initiating a Switchover Between Primary and Standby Audit Vault Servers

You can initiate a switchover if you know that your primary Audit Vault Server is going to be offline for an extended period of time (more than 10 minutes) and you wish to maintain the high availability configuration. You can also initiate a switchover if you wish to promote the standby Audit Vault Server to primary because the designation of primary data center has changed.

1. Log in to the Audit Vault Server through SSH as the `support` user.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

```
ssh support@<audit_vault_server_ip_address>
```

2. Switch to the `root` user.

```
su - root
```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

3. Switch to the `oracle` user.

   ```
   su - oracle
   ```

4. Run the switchover command on the existing primary Audit Vault Server:

   ```
   /usr/local/dbfw/bin/setup_ha.rb --switchover
   ```

9.2.10 Handling a Failover Scenario

In a high availability environment, automatic failover mechanism is enabled by default. You can disable it manually through the Audit Vault Server console.

When automatic failover is in effect, the system periodically monitors the availability of the primary Audit Vault Server. If the primary becomes unavailable for more than 10 minutes, then the failover to the standby Audit Vault Server is automatically triggered. However, if the primary Audit Vault Server has been gracefully shut down by the user, then no failover is automatically triggered. In this case, to manually initiate the failover, carefully examine the situation as required, and run the following command as the *oracle* user on the standby Audit Vault Server:

```
/usr/local/dbfw/bin/setup_ha.rb --failover
```

In a failover, the standby Audit Vault Server becomes the new primary. If the previous primary comes back within 20 minutes, it is reinstated as the new standby and both systems will be in a high availability configuration.

If the previous primary does not come back within 20 minutes, then it becomes unusable. The new primary unpairs and becomes a standalone instance. Perform the following procedure to bring the system back into high availability configuration:

1. Install a new Audit Vault Server for the new designated standby.
2. Follow the configuration steps again to configure the Audit Vault Servers for high availability. See Configuring High Availability for Audit Vault Servers.

Related Topics

- Specifying Audit Vault Server System Settings
  Learn about configuring Audit Vault Server system settings.

9.2.11 Unpair Primary and Standby Audit Vault Servers

Learn how to unpair primary and standby Audit Vault Servers in high availability environment.

1. Log in to the Audit Vault Server console as a *super administrator*.
2. Click **Settings** tab.
3. In the left navigation menu, select **System**.
4. In the **Status** page, click **High Availability** link under the **Configuration** section.
5. To unpair Audit Vault Servers in high availability mode, click **Unpair**.

   After unpairing, the Audit Vault Servers are not synchronized. Make a note of the following details:

- The primary Audit Vault Server goes into `Standalone` mode and the standby Audit Vault Server stays in `Standby` mode. However, there is no communication between these two Audit Vault Servers.
- In case you attempt to connect to the standby Audit Vault Server console, it directs you to the primary Audit Vault Server console, which is the `Standalone`.
- The Audit Vault Agents communicate only with the standalone Audit Vault Server (previous primary).
- Do not try to pair the standby server with primary server; it will not work, as standby server is unusable after unpair. If you want to use the standby server to do the pairing, reinstall the standby server, and do the pairing.

> **Note:**
>
> - You can continue to perform backup operation on the standalone (previous primary) Audit Vault Server.
> - You can restore high availability after unpairing. See Handling a Failover Scenario for complete information.

9.2.12 Disabling or Enabling Failover of the Audit Vault Server

Learn how to enable or disable failover for Audit Vault Servers.

When you configure high availability, the system is configured for automatic failover. However, in some cases, you may want to disable automatic failover. For example, you may need to disconnect the Audit Vault Servers for maintenance or you may be in an environment with an unstable network that may cause frequent failover. In these cases, you may choose to disable automatic failover, and trigger the failover manually by following the steps mentioned below.

To enable or disable automatic failover using the Audit Vault Server console:

1. Log in to the primary Audit Vault Server as a *super administrator*.
2. Click the **Settings** tab, and then in the left navigation menu, select **System** tab.
3. Click the **High Availability** link under the **Configuration** section.
4. Click the **Enable Failover** or **Disable Failover** button as needed.

Alternately, you can execute the following commands to disable or enable the failover as *oracle* user:

```
/usr/local/dbfw/bin/setup_ha.rb --disable_failover
```

```
/usr/local/dbfw/bin/setup_ha.rb --enable_failover
```

> **Note:**
>
> You can run the following command to determine if failover is currently disabled or enabled.
>
> ```
> sudo -u oracle /usr/local/dbfw/bin/setup_ha.rb --status
> ```

9.2.13 Archiving and Retrieving in High Availability

Learn about archiving and retrieving audit and network event data in a high availability scenario.

Archive and retrieve functionality in high availability automatically handles the necessary steps to process the datafiles on both the primary and standby Audit Vault Server instances. In order to archive, you must provide an NFS archive location. An NFS archive location in a high availability environment contains separate NFS details for primary and standby Audit Vault Servers.

In case there is no NFS archive location, then follow these steps to create a new NFS archive location:

1. Log in to the Audit Vault Server console as *super administrator*.
2. Click **Settings** tab, and then click **Archiving** tab in the left navigation menu.
3. Click **Manage Archive Locations** sub tab in the main page.
4. Click **Create**, to create a new archive location using NFS.
5. **Network File System (NFS)** option is selected by default. Enter the following details to create a new NFS archive location:

Field	Description
Location Name	The name of the NFS archive location.
Remote Filesystem	Select an existing filesystem, or one will be created automatically based on the details of this archive location.
NFS Server for Primary	NFS Server IP address or host name for mounting the remote filesystem on primary Audit Vault Server.
NFS Server for Standby	NFS Server IP address or host name for mounting the remote filesystem on standby Audit Vault Server.
NFS Export Directory for Primary	Export directory on the NFS server for primary Audit Vault Server.
NFS Export Directory for Standby	Export directory on the NFS server for standby Audit Vault Server.

NFS Server Path for Primary	The destination path relative to **NFS Export Directory for Primary**.
NFS Server Path for Standby	The destination path relative to **NFS Export Directory for Standby**.

> **Note:**
>
> The combination of NFS server, export directory, and the path specified for primary and standby Audit Vault Servers must be unique.

6. Click **Save**.

> **Note:**
>
> Each Audit Vault Server instance has its own copy of the datafiles. When you archive or retrieve, the datafiles associated with each instance are automatically archived to, or retrieved from the associated archive location.

> **Best Practice:**
>
> Place the NFS servers for primary and standby Audit Vault Servers in separate data centers.

9.2.14 Backup and Restore of Audit Vault Server in High Availability

Learn about backup and restore of Audit Vault Server in high availability.

In a high availability configuration, you must perform the backup operation on the primary Audit Vault Server and not on the standby. To recover from a disaster, you can restore from the backup taken earlier. However, the restored system is not automatically configured for high availability. You need to once again configure for high availability after completing the restore from backup.

> **See Also:**
>
> 1. Prerequisites for Configuring High Availability for Audit Vault Servers
> 2. Configure the Designated Standby Audit Vault Server
> 3. Configure the Designated Primary Audit Vault Server

9.2.15 Removing High Availability Configuration

You may wish to remove the high availability configuration from the primary Audit Vault Server if the secondary host has failed and you need to re-create the high availability pair with a new standby host.

1. Log in to the Audit Vault Server through SSH as the `support` user.

   > **Note:**
   >
   > If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

   ```
   ssh support@<audit_vault_server_ip_address>
   ```

2. Switch to the `root` user.

   ```
   su - root
   ```

   > **Note:**
   >
   > If you're using the OCI marketplace image, use the `sudo su -` command.

3. Switch to the `oracle` user.

   ```
   su - oracle
   ```

4. Ensure the standby host is offline and removed from the network. Its IP address must not be accessible from the existing primary.
5. Run the setup_ha.rb script on the primary Audit Vault Server to remove the high availability configuration:

   ```
   /usr/local/dbfw/bin/setup_ha.rb -v
   --password --unconfigure
   ```

9.3 Configuring High Availability for Database Firewalls

Learn how to manage, configure, switch roles, and unpair a Database Firewall pair.

9.3.1 High Availability for Database Firewall

Learn about high availability in Database Firewall.

High availability in Database Firewall ensures uninterrupted network event monitoring in the event of network or Database Firewall failure. It also ensures that the corporate security policies for monitoring the database targets are enforced at all times.

High availability for Database Firewall can be accomplished in the following two ways:

1. A pair of Database Firewall instances in **Monitoring (Host Monitor)** or **Monitoring (Out of Band)** modes.
2. Multiple Database Firewall instances operating in **Monitoring/Blocking (Proxy)** mode.

Prerequisite

First, create the Database Firewall instances and register them in the Audit Vault Server console. Afterward, configure these instances for high availability to ensure system resilience. Later, create monitoring points, register targets, and define policies for the Database Firewall instances configured for high availability.

Starting with Oracle AVDF 20.6, Database Firewall instances can be paired with existing monitoring points in **Monitoring (Host Monitor)** or **Monitoring (Out of Band)** modes. See Configuring High Availability of Database Firewall Instances With Monitoring Points for more information.

High Availability in Monitoring (Host Monitor) Or Monitoring (Out of Band) Modes

In this configuration:

- High availability (primary and standby) is configured through Audit Vault Server.
- In case of Monitoring (Host Monitor) mode, the Host Monitor Agent is configured to capture and forward the traffic to the primary and standby Database Firewall instances.
- In case of Monitoring (Out of Band) deployment mode, the network switch is configured to mirror and forward the traffic to both the primary and standby Database Firewall instances.
- The configuration of targets, monitoring points, and policies is automatically applied to the primary and standby Database Firewall instances by Audit Vault Server.

The Audit Vault Server collects network events from the primary or standby Database Firewall instance. If the Audit Vault Server is unable to contact the primary Database Firewall for a specified period of time (default of 10 minutes), then the Audit Vault Server collects the network events from the standby Database Firewall. The Audit Vault Server deletes the network events from both instances of Database Firewall after storing the data in the Audit Vault Server repository.

High Availability in Monitoring/Blocking (Proxy) Mode

Database Firewall instances deployed in **Monitoring/Blocking (Proxy)** mode can be configured for high availability in the following ways:

1. Active (primary) and passive (standby)
2. Active and active

In active and passive configuration:

- Client programs are configured to connect to the primary Database Firewall instance. If the primary Database Firewall instance is not reachable or is down, then they connect to the standby.
- Audit Vault Server collects the network events from the Database Firewall instance (either active or passive) that receives the traffic.

In active and active configuration:

- Multiple Database Firewall instances can be part of this configuration.
- Client programs can connect to any of the active Database Firewall instances that are part of this configuration.
- Once a client establishes a session with an active Database Firewall instance, it communicates with the same instance throughout the session.

- Audit Vault Server collects the network events from all the active Database Firewall instances that are part of this configuration.

Related Topics

- Configuring Database Firewall
  Learn about configuring Database Firewall.
- Specifying the Audit Vault Server Certificate and IP Address
  You associate each Database Firewall with an Audit Vault Server so that the Audit Vault Server can manage the firewall. If you're using a resilient pair of Audit Vault Servers for high availability, then you associate the firewall with both servers.

9.3.2 High Availability for Database Firewall in Host Monitor Agent or Out of Band Modes

Learn how to configure a Database Firewall high availability pair in Host Monitor Agent or Out of Band modes.

Prerequisites

- Register both of the Database Firewall instances in the Audit Vault Server console.
- If you have Audit Vault Servers in high availability mode, then you must provide the primary and standby Audit Vault Server's IP address and certificate to each Database Firewall instance during registration.
- For Oracle AVDF release 20.5 and earlier, ensure there are no monitoring points configured on either of the Database Firewall instances. In case there are any existing monitoring points, then they must be deleted.
- For Oracle AVDF release 20.6 and later, pairing of Database Firewall instances with existing monitoring points is possible.

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click **Database Firewalls** tab.
3. In the left navigation menu, select **High Availability**.
4. Click **Create**.
5. In the **Create Resilient Pair** dialog, select the Database Firewall instances for **Primary** and **Standby** fields from the drop down list.
6. Click **Save**.
7. Starting with Oracle AVDF 20.6, the pairing process of the Database Firewall instances is a background job. See the **Jobs** dialog in the Audit Vault Server console to check the status of high availability pairing. Locate for the job against the entry `Create DBFW resilient pair`. After completion of the pairing process, navigate to the **Database Firewalls** tab and then to **High Availability** tab in left navigation menu to verify the resilient pair.

9.3.3 Swapping Roles Between Primary and Standby Database Firewalls

Learn to swap the roles of primary and standby Database Firewall instances in a high availability.

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. In the left navigation menu, select **High Availability**.

4. Select the specific pair for which you want to swap roles.
5. Click the **Swap** button.
6. In the confirmation dialog, click **OK**.

> **Note:**
>
> In case of Database Firewall configured for high availability, the settings must be the same for all the Database Firewall instances. In the event of a failover, the standby Database Firewall instance becomes the primary. The SYSLOG settings on the standby Database Firewall instance are in effect. In this case, some SYSLOG settings and logging is turned off. This is done to avoid duplicate logs sent by both the instances.
>
> When the previous primary becomes active again, there is no transfer or sharing of settings between the Database Firewall instances. Manual modification of the `rsyslog.conf` must be avoided as any changes result in erasing the settings during the following failover. The actual saved values in the SYSLOG settings should not be changed on failover.

9.3.4 Unpair Primary and Standby Database Firewalls

Learn to unpair Database Firewall instances in high availability.

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. In the left navigation menu, select **High Availability**.
4. Select the specific pair of Database Firewalls that you want to unpair.
5. Click the **Unpair** button.

> **Note:**
>
> For releases Oracle AVDF 20.4 and prior, click **Break** button.

9.3.5 Configuring High Availability of Database Firewall Instances With Monitoring Points

Learn how to configure high availability in Database Firewall instances with monitoring points.

Starting with Oracle AVDF release 20.6 if there are monitoring points on the designated primary Database Firewall instance or on the standby instance, or on both, they can be paired. The existing monitoring points on the designated primary instance are replicated on the standby Database Firewall instance after pairing. Likewise, the existing monitoring points of the designated standby Database Firewall instance are replicated on the primary instance after pairing. The monitoring points are shared between the resilient pair.

If a target has monitoring points on both the Database Firewall instances, the configuration data of the monitoring points is merged. The data on the primary instance takes precedence.

> **Note:**
>
> Starting Oracle AVDF 20.6, Database Firewall instances can be paired with existing monitoring points in **Monitoring (Host Monitor)** or **Monitoring (Out of Band)** modes. This is not supported for Database Firewall instances deployed in **Monitoring/Blocking (Proxy)** mode. An error is displayed if an attempt is made to pair Database Firewall instances deployed in **Monitoring/Blocking (Proxy)** mode with existing monitoring points.
>
> `Unable to create resilient pair in Monitoring/Blocking(Proxy) mode.`

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. In the left navigation menu, select **High Availability**.
4. Click **Create**.
5. In the **Create Resilient Pair** dialog, select the Database Firewall instances for `Primary` and `Standby` fields from the drop down list.
6. Click **Save**.
7. If there are monitoring points on the both the Database Firewall instances, the following a confirmation message is displayed:

   `Pairing will merge settings of both monitoring points. Do you wish to continue?`
8. Click **OK** to continue.
9. The following message is displayed:

   `Request submitted successfully.`
10. The pairing process of the Database Firewall instances is a background job. See the **Jobs** dialog to check the status of high availability pairing. Locate for the job against the entry `Create DBFW resilient pair`. After completion of the pairing process, navigate to the **Database Firewalls** tab and then to **High Availability** tab in left navigation menu to verify the resilient pair.

9.4 Configuring High Availability for Database Firewalls in Proxy Mode

Learn how to configure Database Firewall instances for high availability **Monitoring / Blocking (Proxy)** mode.

Oracle AVDF provides an option to set up the high availability configuration for multiple Database Firewall instances deployed in **Monitoring / Blocking (Proxy)** mode. These multiple instances are installed and configured independently.

Prerequisites

- Install and register all Database Firewall instances that will be part of the high availability.
- For each Database Firewall instance:

  - The configuration of the monitoring points must be same. For example Database Firewall instances `DBFW1` and `DBFW2` should have the same number of monitoring points and the configuration of these monitoring points should also be the same.
  - Deploy the same Database Firewall policy for a specific target. For example, deploy Database Firewall policy `P1` (for target `T1`) on instances `DBFW1` and `DBFW2`.

High availability configuration in proxy mode can be achieved in the following ways:

- Through Client Configuration for Oracle Databases
- Using DNS for Oracle and Other Database Types

9.4.1 Configuring High Availability for Database Firewall in Proxy Mode through Client Configuration

Learn how to configure high availability for two or more Database Firewall instances in proxy mode using the `tnsnames.ora` the for Oracle databases.

OCI (Oracle Call Interface) based clients use `tnsnames.ora` file to connect to Oracle database. The following parameters in this file should be modified as part of this configuration:

1. `ADDRESS_LIST`
2. `CONNECT_TIMEOUT`
3. `LOAD_BALANCE`

ADDRESS_LIST

Include addresses of all the Database Firewall instances in the `ADDRESS_LIST`. The client programs connect to the first Database Firewall instance. In case of a failed attempt, the client connects to the next instance in the order.

For example:

```
dbfw1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=192.0.2.1)
(PORT=1111))

                                  (ADDRESS=(PROTOCOL=TCP)(HOST=192.0.2.2)
(PORT=2222)))(CONNECT_DATA=(SERVICE_NAME=dbfwdb)))
```

where:

`dbfw1` is referred to as `net_service_name`.

Host = `192.0.2.1` and Host = `192.0.2.2` are the IP addresses of Database Firewall instances configured for high availability.

If you are using *SQL*Plus* client, then use the following command:

```
sqlplus <username>/<password>@<net_service_name>
```

The *SQL*Plus* client attempts to connect to the first Database Firewall instance with IP `192.0.2.1`. In case the first instance is down or not reachable, then the client attempts to connect to the second Database Firewall instance with IP address `192.0.2.2`.

CONNECT_TIMEOUT

Use `CONNECT_TIMEOUT` (seconds) parameter to quickly detect if the Database Firewall instance is down.

For example:

```
dbfw1=(DESCRIPTION=(CONNECT_TIMEOUT=10)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=192.0.2.1)(PORT=1111))(ADDRESS=(PROTOCOL=TCP)(HOST=192.0.2.2)
(PORT=2222)))(CONNECT_DATA=(SERVICE_NAME=dbfwdb)))
```

The client attempts to connect to the first Database Firewall instance with IP `192.0.2.1`. In case the first instance is down or not reachable, then the client waits for the duration (seconds) mentioned in the `CONNECT_TIMEOUT` parameter. In the above example it is 10 seconds. Next, the client attempts to connect to the second Database Firewall instance with IP address `192.0.2.2`.

> **Note:**
>
> - By default the value of `CONNECT_TIMEOUT` is 60 seconds.
> - Refer to *Oracle Database Net Services Administrator's Guide* for more details.

LOAD_BALANCE

Use `LOAD_BALANCE` parameter for client connections to connect to Database Firewall instances in a random sequence.

For example:

```
dbfw1=(DESCRIPTION=(ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)
(HOST=192.0.2.1)(PORT=1111))(ADDRESS=(PROTOCOL=TCP)(HOST=192.0.2.2)
(PORT=2222)))(CONNECT_DATA=(SERVICE_NAME=dbfwdb)))
```

Here, clients will connect to either `192.0.2.1` or `192.0.2.2` in a random sequence.

> **Note:**
>
> - When set to `on`, the `LOAD_BALANCE` parameter instructs clients to progress through the list of Database Firewall addresses in a random sequence. When set to `off`, instructs clients to try the addresses sequentially until one succeeds.
> - Refer to *Oracle Database Net Services Administrator's Guide* for more details.

9.4.2 Configuring High Availability for Database Firewall in Proxy Mode using DNS

Learn how to configure high availability for multiple Database Firewall instances in **Monitoring / Blocking (Proxy)** mode using DNS for Oracle and other database types.

Prerequisites

1. Install and register Database Firewall instances.
2. For each Database Firewall instance:
   - The configuration of the monitoring points must be same. For example Database Firewall instances `DBFW1` and `DBFW2` should have the same number of monitoring points and the configuration of these monitoring points should also be the same.
   - Deploy the same Database Firewall policy for a specific target. For example, deploy Database Firewall policy `P1` (for target `T1`) on instances `DBFW1` and `DBFW2`.
3. Client programs should be able to connect to the configured DNS server.

Setup a fully qualified Domain Name in DNS

1. Create a fully qualified domain name to represent IP addresses of the Database Firewall instances.
2. Configure the selected DNS server as the name resolution server on the client hosts.
3. Clients should use the fully qualified domain name in the connection string to connect to the Database Firewall instance.
4. For example, if you are using *SQL*Plus*, then follow these steps:
   a. Start the *SQL*Plus* connection as `sqlplus /nolog` without the username or password.
   b. Run the command: `connect <username>/<password>@<fully qualified domain name>:<port/service>`
5. DNS can be configured in one of the following ways:
   a. Configure DNS to always connect to an ordered list of Database Firewall instances (for example `DBFW1`, `DBFW2`, etc). If a client is not able to connect to the first instance (`DBFW1`), then it attempts to connect to the second instance (`DBFW2`).
   b. Configure DNS to use round-robin algorithm for connecting to Database Firewall instances.

10

Integration with Third Party SIEM and Log-data Analysis Tools

Oracle Audit Vault and Database Firewall supports integration with third-party SIEM (Security Information and Event Management) and log-data analysis tools.

Oracle Audit Vault and Database Firewall can push alerts to an external system using SYSLOG. It also allows third party tools to connect directly to the database and extract (pull) data from the event log table using a collector provided by the SIEM.

Integration with any SIEM tool is achieved through one of two methods:

1. Oracle AVDF pushes alerts into the SIEM using SYSLOG. For the push method where Oracle Audit Vault and Database Firewall sends alerts to the SIEM using SYSLOG, see Configuring Audit Vault Server Syslog Destinations for information.
2. Configure SIEM to pull events from the **AVSYS.EVENT_LOG** table in Oracle AVDF. Use the SIEM's database table connector to configure this functionality. For the pull method, configure SIEM to view and extract all of the data from the **AVSYS.EVENT_LOG** table using the collector provided by the SIEM. This requires creating a user in Oracle Audit Vault and Database Firewall with the auditor role. Ensure that this user has access to the targets whose data has to be sent to SIEM. This is the database user the SIEM will use to connect to the database. The remaining configuration needs to completed in the SIEM. The Oracle Audit Vault and Database Firewall schema and the specific mapping in the **AVSYS.EVENT_LOG** table to the SIEM depends on the SIEM. A description of the **EVENT_LOG** table is available in Appendix Oracle Audit Vault and Database Firewall Database Schemas.

> **Note:**
>
> In case of Database Firewall configured for high availability, the settings must be the same for all the Database Firewall instances. In the event of a failover, the standby Database Firewall instance becomes the primary. The SYSLOG settings on the standby Database Firewall instance is in effect. In this case, some SYSLOG settings and logging are turned off. This is done to avoid duplicate logs being sent by both the instances.
>
> When the previous primary becomes active again, there is no transfer or sharing of settings between the Database Firewall instances. Manual modification of the `rsyslog.conf` must be avoided as any changes result in erasing the settings during the following failover. The actual saved values in the SYSLOG settings should not be changed on failover.

See Also:

- START COLLECTION FOR SECURED TARGET
- Oracle Database Plug-in for Oracle Audit Vault and Database Firewall

11

Using Oracle Database Firewall with Oracle RAC

You can configure Oracle Database Firewall to work with Oracle Real Application Clusters (Oracle RAC) so that it can block and substitute statements or log SQL statements and raise alerts.

11.1 Configuring a Database Firewall with Oracle RAC for Monitoring and Blocking

Learn how to configure a database firewall with Oracle Real Application Clusters (Oracle RAC) for monitoring and blocking.

11.1.1 About Configuring Database Firewall with Oracle RAC for Monitoring and Blocking

Oracle Database Firewall has monitoring and blocking features that you can use with Oracle RAC.

To use blocking, you must use the **Monitoring / Blocking (Proxy)** mode.

The Database Firewall when configured in **Monitoring / Blocking (Proxy)** mode, the following takes place:

1. SQL client connects to Database Firewall.
2. Database Firewall connects to SCAN Listener.
3. SCAN Listener redirects the connection to a RAC node.
4. Database Firewall handles the redirection, makes a outbound connection to the re-directed RAC node.
5. The response from Oracle RAC node is passed to the client.

> **Caution:**
>
> If you set up an Oracle RAC protected database to be a scan listener, you also need to select the **RAC Instance/Autonomous DB** check box when registering the database as a target. If you don't identify the target as a RAC database, the scan listener could redirect the client to a different IP address, bypassing the Database Firewall entirely.
>
> See Registering Targets for instructions.

11.1.2 Configure a Proxy Using the Audit Vault Server Console

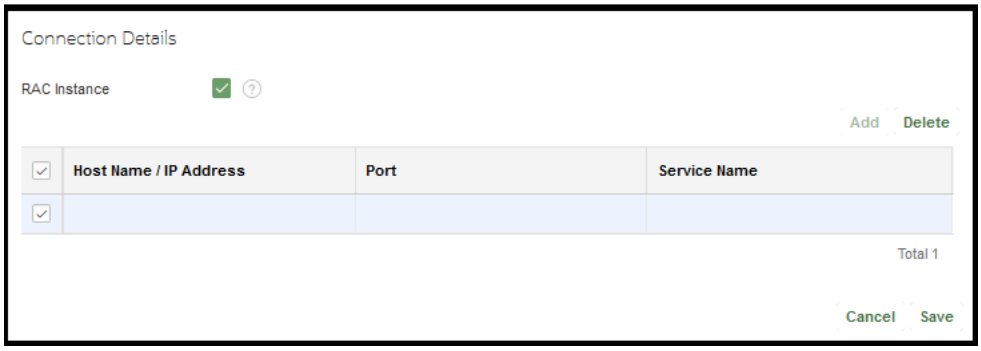
You can use the Oracle Audit Vault Server Console to configura a proxy.

1. Log in to the Audit Vault Server console as administrator.
2. Complete the steps for Configuring the Database Firewall As a Traffic Proxy.
3. Complete the steps for Creating and Configuring a Database Firewall Monitoring Point.

   Be sure to select the **RAC Instance/Autonomous DB** check box (**RAC Instance** check box in Oracle AVDF 20.7 and earlier) in the **Connection Details** section.
4. Ensure **Network Interface Card** and **Proxy Ports** fields are selected. After selecting them, the **RAC Instance/Autonomous DB** check box (**RAC Instance** check box in Oracle AVDF 20.7 and earlier) is enabled.
5. After selecting the **RAC Instance/Autonomous DB** check box (**RAC Instance** check box in Oracle AVDF 20.7 and earlier) and adding the SCAN fully qualified domain name (FQDN) in the **Host Name / IP Address** field, the following message is displayed:

   ```
   Configure SCAN Listener Domain Name as target. For more details refer: Real
   Application Clusters Installation Guide.
   ```

Figure 11-1 Connection Details



6. Ensure that the SCAN FQDN is entered in the **Host Name / IP Address**.
7. Enter the **Port** number of SCAN Listener.
8. Enter the **Service Name** or SID (optional).
9. Click **Add**.
10. Click **Save** on the dialog.
11. Click **Save** on the main page. The target is created and shows up under the **Database Firewall Monitoring** sub tab on the main page.
12. Click the newly created RAC target to verify the details.

11.2 Configuring a Database Firewall with Oracle RAC for Monitoring

You can configure an Oracle Database Firewall with Oracle RAC to use Host Monitoring and Out-of-Band deployment modes.

Oracle recommends that you configure Oracle Database Firewall with Oracle RAC in one of the following deployment modes:

- **Monitoring (Out-of-Band)** - In this deployment mode, Oracle Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements. Create a monitoring point using IP addresses of all the RAC nodes. Select this option only while creating the monitoring point.
- **Monitoring (Host Monitor)** - In this deployment mode, Oracle Database Firewall can monitor and alert on SQL traffic, but cannot block or substitute SQL statements. For this deployment mode, install the Host Monitor Agent on each RAC node and create a monitoring point for each RAC node. Select this option only while creating the monitoring point.

> **Note:**
>
> Complete the steps for Creating and Configuring a Database Firewall Monitoring Point. While executing this procedure, ensure to select the deployment mode as mentioned above.

12

Oracle Audit Vault and Database Firewall on Oracle Cloud Infrastructure

You can deploy Oracle AVDF on Oracle Cloud Infrastructure (OCI).

12.1 About Oracle AVDF on Oracle Cloud Infrastructure

Learn about Oracle AVDF on Oracle Cloud Infrastructure (OCI).

Oracle Cloud Infrastructure Marketplace is an online store that offers solutions specifically for customers of Oracle Cloud Infrastructure (OCI). Oracle Cloud Marketplace images are templates of virtual hard drives that determine the operating system and software to run on an instance. Oracle AVDF instances (Audit Vault Server instance or Database Firewall instance) can be provisioned on Oracle Cloud Infrastructure's Virtual Machine standard shapes using Oracle AVDF Cloud Marketplace images.

Oracle AVDF Cloud Marketplace images consist of the Audit Vault Server image and the Database Firewall image that is used to provision Audit Vault Server and Database Firewall instances respectively.

> **See Also:**
>
> Oracle Cloud Marketplace

12.2 Benefits of Provisioning Oracle AVDF on Oracle Cloud Infrastructure

Learn about the benefits of provisioning Oracle AVDF on Oracle Cloud Infrastructure (OCI).

Quick Provisioning

Oracle AVDF instances can be provisioned within minutes, without the need to procure and manage hardware.

Ease of Scaling up

Scaling up Oracle AVDF instance to meet increased workload needs, is simple and easy. Ease of scaling up gives you the option to start with a small VM shape and scale up as workload increases.

12.3 Supported Oracle Cloud Infrastructure Virtual Machine Shapes

List of supported VM standard shapes for deploying Oracle AVDF on Oracle Cloud Infrastructure (OCI).

The following Oracle Cloud Infrastructure VM standard shapes are supported for Oracle AVDF instances:

- VM.Standard2.2
- VM.Standard2.4
- VM.Standard2.8
- VM.Standard2.16
- VM.Standard2.24
- VM.Standard1.2
- VM.Standard1.4
- VM.Standard1.8
- VM.Standard1.16
- VM.Standard.E3.Flex
- VM.Standard.E4.Flex (Supported starting with Oracle AVDF release 20.7)
- VM.Standard.E5.Flex (Supported starting with Oracle AVDF release 20.12)

> **See Also:**
>
> Oracle Cloud Infrastructure compute shapes

12.4 Provisioning Oracle AVDF with the Oracle Cloud Marketplace Image

Learn about provisioning Audit Vault Server or Database Firewall with Oracle Cloud Marketplace image.

The following are required prior to provisioning Oracle AVDF instances using the Oracle Cloud Marketplace image:

1. A VM standard shape with a minimum memory of 8GB.
2. Block storage with a minimum of 220 GB.
3. A Virtual Cloud Network (VCN) in your tenancy.
4. SSH key pair for `ssh` access to the instance. Oracle AVDF instance accepts the following key types:
   - `ssh-ed25519`
   - `ssh-ed25519-cert-v01@openssh.com`

- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp384-cert-v01@openssh.com`
- `rsa-sha2-512 key types`

Generate an SSH key pair of these types. For example: Run the following command to generate a public key of `ssh-ed25519` type:

```
ssh-keygen -t ed25519
```

12.4.1 Accessing the Oracle AVDF Cloud Marketplace Image

Learn how to access the Oracle AVDF Cloud Marketplace image.

The Oracle AVDF Cloud Marketplace image is available on the Oracle Cloud Marketplace website. Follow these steps:

1. Go to Oracle Cloud Marketplace.
2. In the **Applications** search field, enter `Oracle Audit Vault and Database Firewall`.
3. Click **Go**.
4. Under the search results, click **Oracle Audit Vault and Database Firewall** to navigate to the Oracle AVDF Cloud Marketplace page.

> **Note:**
>
> Access the latest **Audit Vault Server 20.x** for Audit Vault Server image or **Database Firewall 20.x** for Database Firewall image from Oracle Cloud Marketplace website. Other artifacts (or installable files) can be downloaded from Oracle Software Delivery Cloud. Refer to About Oracle AVDF Installable Files.

12.4.2 Creating an Oracle AVDF instance with Oracle Cloud Marketplace Image

Learn how to create an Oracle AVDF instance with Oracle Cloud Marketplace image.

Follow these steps:

1. In the Oracle AVDF Cloud Marketplace page, click the **Get App** button.
2. If you already have an OCI account, select the **OCI region**, and then click **Sign In**. Else, click **Sign Up** to create a new account.
3. In the **Get Version** menu, select the latest **Audit Vault Server 20.x** for Audit Vault Server image or **Database Firewall 20.x** for Database Firewall image.
4. In the **Compartment** menu, select a compartment.
5. Check the **I have reviewed the terms and conditions** box.
6. Click **Launch Instance**.
7. The **Create Compute Instance** page is displayed. Fill in the required details:
   a. Provide a **NAME** for the Oracle AVDF instance.
   b. Choose the **AVAILABILITY DOMAIN**.

c. Under **Shape**, click **Change Shape**.

d. Choose `Virtual Machine` as the **Instance Type**.

e. Select the **Shape series**.

f. Then click **Select Shape**. Choose the shape for the instance.

8. In the **Configure networking** section, select the following fields:

   a. **VIRTUAL CLOUD NETWORK COMPARTMENT**

   b. **SELECT A VIRTUAL CLOUD NETWORK**

   c. **SUBNET COMPARTMENT**

   d. **SUBNET**

9. Check one of the following options for IP address:

   - **ASSIGN A PUBLIC IP ADDRESS**
   - **DO NOT ASSIGN A PUBLIC IP ADDRESS**

> **Note:**
>
> See IP Addresses in your VCN (Virtual Cloud Network) to understand more about public and private IP addresses in Oracle Cloud Infrastructure.

10. In the **Add SSH Keys** section, provide your ssh public key by selecting **Choose public key files** or **Paste public keys**. If you select any other option, you will not be able to connect to the Oracle AVDF instance.

11. Under **Boot volume** section, specify a custom boot volume size if you want the boot volume to be larger than the default size of 220 GB.

> **Note:**
>
> The custom boot volume size should not exceed 2TB. Refer to Scaling Up Oracle AVDF Instances section for more details on expanding storage.

12. Click **Advanced Options**, and then choose the default options in all the tabs.

13. Click **Create** to start creating the instance.

14. After the instance state changes to `Running` in the Oracle Cloud Infrastructure console, wait for a few minutes for the underlying services to start up before accessing the instance.

15. Perform the post instance creation steps.

> **Note:**
>
> For production workload, follow the sizing guidelines (My Oracle Support Doc ID 2092683.1) to calculate shape and storage requirements.

> **See Also:**
>
> Creating an instance in Oracle Cloud Infrastructure

12.4.3 Post Instance Creation Steps

Perform one time post instance creation steps.

After the instance creation is completed, you must perform these steps once.

For Audit Vault Server Instance

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Change root user password by running the following command. The root password is required to troubleshoot the instance using OCI instance console connection.

   ```
   sudo passwd root
   ```
3. Generate a one time passphrase by running the command:

   ```
   sudo -u oracle /usr/local/dbfw/bin/generate_post_install_passphrase.py
   ```
4. Copy the passphrase that is returned by the above command.
5. Access the Audit Vault Server console by entering `https://<IP address of the instance>` as the URL in the browser.
6. Enter the passphrase copied from the earlier step in the **Post Install Authentication** page of the Audit Vault Server console.
7. Fill in the details in the **Post Install Configuration** page.
8. In the **AVS IP for Agent Communication** section, specify the public IP of the Audit Vault Server if you are expecting to collect audit data from any target outside of OCI. See section Deploying Audit Vault Agents for more details.

   > **Note:**
   >
   > After the post installation step is complete, changing the AVS IP for Agent communication is not supported.
9. Click **Save**.
   DNS is automatically set to 169.254.169.254.

   > **See Also:**
   >
   > DNS in Your Virtual Cloud Network

For Database Firewall Instance

1. Log in to the appliance through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

2. Change root user password by running the following command. The root password is required to troubleshoot the instance using OCI instance console connection.

```
sudo passwd root
```

12.5 Connecting to Oracle AVDF Instance

Learn how to access Audit Vault Server and Database Firewall instances on Oracle Cloud Infrastructure (OCI).

Connecting through SSH

Prerequisite: OCI virtual firewall for your VCN must be configured to allow ingress traffic on SSH port 22. See OCI Access and Security for complete information.

The public key specified during instance creation is installed on Oracle AVDF instance for SSH authentication. After the instance creation is completed, connect to the instance as *opc* user using the matching private key.

Using the `ssh` utility, run the following command:

```
ssh -i <path to private key file> opc@<IP address of Oracle AVDF instance>
```

See Also:

- Unable to Connect to Audit Vault Server through Console or SSH
- Connecting to Oracle Cloud Infrastructure Instance
- Oracle Cloud Infrastructure Access and Security
- IP Addresses in your VCN

Note:

Oracle AVDF instances accept the following public key types:

- `ssh-ed25519`
- `ssh-ed25519-cert-v01@openssh.com`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp384-cert-v01@openssh.com`
- `rsa-sha2-512`

Connecting through Audit Vault Server console

Prerequisite: OCI virtual firewall for your VCN must be configured to allow ingress traffic on port 443. See OCI Access and Security for complete information.

Access the Audit Vault Server console by entering `https://<IP address of the Audit Vault Server instance>` as the URL in your browser.

12.6 Scaling Up Oracle AVDF Instances

Learn to scale up Oracle AVDF instances on OCI.

CPU, memory, network bandwidth, and repository storage of Oracle AVDF instance can be scaled up without recreating the instance. This allows for increased performance to meet growing workload needs.

Changing the Shape of Oracle AVDF Instance

CPU, memory, and network bandwidth can be scaled up by changing the shape of the instance to one of the supported VM standard shapes.

Use the OCI console to edit the shape of the instance. Refer to Using the Console for more details.

> **Note:**
>
> Changing a shape to a smaller one than the current shape is not supported. For example, changing the shape from VM.Standard2.4 to VM.Standard2.2 is not supported.

Expanding Repository Storage for Audit Vault Server

Each Audit Vault Server instance has a repository that stores the collected audit and network event data. The storage requirements increase as the collection workload grows. To meet the storage needs, expand the Audit Vault Server repository storage in the following ways:

- During Instance creation: When specifying the boot volume larger than the default for Audit Vault Server instance, the underlying repository storage is automatically expanded. Refer to section Creating an Oracle AVDF instance with Oracle Cloud Marketplace Image on how to specify custom boot volume size.
- Post instance creation: Follow these steps:
  1. Attach additional OCI Block storage to the instance. Follow the steps listed in Attaching the Volume to an Instance.
  2. Ensure the disks are visible at the OS level, by running the following command:

     ```
     lsblk
     ```

  3. Expand the repository storage. See Adding Local Disks to the Audit Vault Server ASM Disk Groups.

> **Note:**
>
> - Ensure the attached OCI Block storage is not shared with any other instance as it may lead to data loss.
> - SAN storage is not supported.

12.7 Changes in Functionality for Oracle AVDF Instances on OCI

Learn about the changes in functionality of Oracle AVDF deployed on Oracle Cloud Infrastructure (OCI).

Table 12-1 Functional Differences Between Oracle AVDF Deployed On-premises and on OCI

Functionality	Oracle AVDF instance deployed on-premises	Oracle AVDF instances deployed on OCI
SSH authentication	Password based authentication	Key based authentication
Network settings (IP address and Host Name)	Network settings can be modified using the Audit Vault Server console.	These settings are read only in the Audit Vault Server console. However, they can be modified from the OCI console.
Time synchronization	NTP settings can be modified using the Audit Vault Server console.	NTP is automatically configured during instance creation and the NTP server settings cannot be changed.
DNS	DNS setting can be modified using the Audit Vault Server console.	DNS is automatically set to 169.254.169.254 during instance creation. The settings can be changed on the Audit Vault Server console.
Repository storage expansion	SAN Storage	OCI Block Storage must be used for storage expansion.
Archive or backup location	NFS	OCI File Storage (Recommended)
Database Firewall deployment modes	• Monitoring / Blocking (Proxy) • Monitoring (Host Monitor) • Monitoring (Out-of-Band)	• Monitoring / Blocking (Proxy) • Monitoring (Host Monitor) • Monitoring (Out-of-Band) is not supported.
Secondary Network Interface Cards on Audit Vault Server	Supported	Not supported. (Only the primary network interface card that is associated with the primary Audit Vault Server's private IP address of the instance is supported.)
Secondary Network Interface Cards on Database Firewall	Supported	Not supported

12.8 Ports for Communication between Oracle AVDF Components

Learn about different ports used by Oracle AVDF for communication between different components.

The list of ports used by Oracle AVDF is listed in Ports Used by Oracle Audit Vault and Database Firewall.

> **See Also:**
>
> Security Lists in OCI

12.9 High Availability for Oracle AVDF Instance

Learn about high availability for Oracle AVDF instance.

High availability in Oracle AVDF makes the deployment more reliable by ensuring continuity of functionality (for example, audit and network event data collection).

Configuring High Availability in Audit Vault Server

Prerequisite: OCI virtual firewall for your VCN must be configured to allow ingress traffic on port 7443, 1521, and 1522. See OCI Access and Security for complete information.

To configure high availability you need two Audit Vault Server instances. The first instance is the primary server and the other as the secondary server. The steps to configure high availability is similar to on-premises deployment. However, private IP addresses of the Audit Vault Server instances must be used during high availability configuration.

Configuring High Availability in Database Firewall

Configuring high availability for Database Firewall instance is supported only for Monitoring / Blocking (Proxy) mode.

Prerequisite: OCI virtual firewall for your VCN must be configured to allow ingress traffic on proxy ports for Database Firewall nodes. See OCI Access and Security for complete information.

To configure high availability you need two Database Firewall instances. The first instance is the primary and the other as the secondary. The steps to configure high availability is similar to on-premises deployment.

> **See Also:**
>
> High Availability in Oracle AVDF

12.10 Deploying Audit Vault Agents

Learn about deploying Audit Vault Agents.

Audit Vault Agent is a component of Oracle AVDF that you deploy on a machine (usually the same host as the target) to collect audit data from targets.

Prerequisite: OCI virtual firewall for your VCN must be configured to allow ingress traffic on ports 1521 and 1522 for Audit Vault Server. See OCI Access and Security for complete information.

Follow these steps to deploy an Audit Vault Agent:

1. Register the Audit Vault Agent machine on Audit Vault Server. In some cases, you need to specify `AGENT_PHYSICAL_ADDRESS_XX` (where XX can be a number from 01 to 99) Agent attribute. See Registering Hosts on the Audit Vault Server for complete information.
2. Download the Audit Vault Agent software from Audit Vault Server console to the Agent machine.
3. Install the Audit Vault Agent software on the Agent machine.

4. Activate and start the Audit Vault Agent.

> **See Also:**
>
> Registering Hosts and Deploying the Agent

Audit Vault Agent communicates to Audit Vault Server using a JDBC connect string that contains the IP address of the Audit Vault Server. The connect string is automatically generated after post instance creation steps. Specify the IP address that must be used in the connect string by filling in the **AVS IP for Agent Communication** section in the **Post installation configuration page** of the Audit Vault Server console. If an IP address is not specified, the private IP address of the Audit Vault Server is used.

Follow these guidelines for the type of IP address to be specified in the **Post installation configuration page** of the Audit Vault Server:

- If you are expecting to collect audit data from any target outside of OCI, then specify a public IP address of the Audit Vault Server.
- If you are expecting to collect audit data from targets only in OCI, then specify a private IP address of the Audit Vault Server.
- If you are expecting to deploy Database Firewall in **Monitoring (Host Monitor)** mode for targets only in OCI, then specify the private IP address of the Audit Vault Server.

Table 12-2 Platform Support Matrix for Audit Vault Agent and Host Monitor Agent Deployment

Platform	Audit Vault Agent Deployment	Host Monitor Agent Deployment
Oracle Linux 64 bit (OCI)	Yes	Yes
Oracle Linux 64 bit (outside OCI)	Yes	No
Microsoft Windows Server (x86-64) (OCI)	Yes	Yes
Microsoft Windows Server (x86-64) (outside OCI)	Yes	No

12.11 Configuring Audit Trail Collection

Learn how to configure audit trails.

The steps to configure audit trails is similar to on-premises deployment.

> **See Also:**
>
> - Deploying Audit Vault Agents
> - Configuring and Managing Audit Trail Collection

12.12 Deploying Database Firewall for Monitoring

Learn about deploying Database Firewall on Oracle Cloud Infrastructure (OCI).

The following Database Firewall deployment modes are supported on OCI:

- **Monitoring / Blocking (Proxy)**
- **Monitoring (Host Monitor)**

Prerequisites:

- For Database Firewall deployed in Monitoring (Host Monitor) mode, the virtual firewall for your Database Firewall VCN must be configured to allow ingress traffic on ports ranging from 2051 to 5100. See OCI Access and Security for complete information.
- For Database Firewall deployed in Monitoring / Blocking (Proxy) mode, the virtual firewall for your Database Firewall VCN must be configured to open the specific proxy port.
- For Audit Vault Server to collect network event data from Database Firewall, you must configure virtual firewall of your Database Firewall VCN to allow ingress traffic on port 1514.

When deploying Database Firewall, consider these points:

- You can use either public or private IP address of the Database Firewall to register with the Audit Vault Server.
- When configuring a Database Firewall monitoring point, use the primary VNIC as the network interface card.
- Use private IP address of the target when enabling native network encrypted traffic monitoring for Oracle Database.
- When configuring the Database Firewall monitoring point for Oracle Real Application Clusters (Oracle RAC), enter the FQDN of the SCAN Listener as the host name.

See Also:

- Configuring Database Firewall for Databases That Use Native Network Encryption
- Configuring Database Firewall

Note:

- Database Firewall monitoring and protection is not supported for targets outside OCI.
- For deploying Host Monitor Agent follow the same guidelines mentioned in section Deploying Audit Vault Agents.

12.13 Monitoring Oracle Autonomous Database Services

Learn how to monitor Oracle Autonomous Database services with Oracle Audit Vault and Database Firewall on Oracle Cloud Infrastructure (OCI).

Clients connect to Autonomous Database services by using a public or private endpoint. Use the public endpoint when configuring the Autonomous Database services as a target on the Audit Vault Server.

Configuring Audit Trails

To configure audit trails for collection, see Configuring Audit Trail Collection, with the following changes:

- Provide the public endpoint, credentials wallet, and user credentials of your Autonomous Database during target registration. See Step 2: Create User Accounts on Oracle Cloud Instances.
- Deploy the Audit Vault Agent remotely and ensure access to the public endpoint.

Configuring Audit Provisioning and Entitlement Retrieval

For Audit Provisioning and Entitlement Retrieval, the Audit Vault Server connects to the Autonomous Database by using the audit connection details that you provided during target registration. Ensure that the Audit Vault Server can access the public endpoint of your Autonomous Database.

Configuring Database Firewall

To configure the Database Firewall to connect to an Autonomous Database, see Configuring a Database Firewall to Connect to an Oracle Autonomous Database.

Related Topics

- Connect to Autonomous Database Using a Client Application

12.14 Monitoring DB Systems on OCI

Learn how to monitor DB Systems with Oracle AVDF on OCI.

OCI DB Systems allow you to configure SSH key based access to the machine hosting the database. You can install the Audit Vault Agent on the DB Systems.

In addition, all SQL connections use native network encryption by default.

Configuring Audit Trail Collection

Refer to the following sections:

- Deploying Audit Vault Agents
- Configuring Audit Trail Collection

Configuring Audit Provisioning and Entitlement Retrieval

For Audit Provisioning and Entitlement Retrieval, the Audit Vault Server connects to the DB Systems on OCI using the audit connection details provided during the target registration. Therefore, you must ensure that Audit Vault Server has JDBC access to your database.

Configuring Database Firewall Monitoring

Refer to section Deploying Database Firewall for Monitoring.

12.15 Backup and Restore of Oracle AVDF Instances in OCI

Learn about back up and restore functionality for Oracle AVDF instances in OCI.

The purpose of backup and restore is to protect against data loss and to restore the instance from a backup taken earlier.

Backup and Restore of Audit Vault Server

The steps to perform backup and restore of Audit Vault Server is similar to on-premises deployment with the following changes:

- Use OCI File Storage when configuring backup location.
- When configuring restore, you must set `USE_NEW_IP` parameter to `Y`.

> **See Also:**
>
> Backup and Restore of Audit Vault Server

Backup and Restore of Database Firewall

The Database Firewall does not need to be backed up. As part of Audit Vault Server backup, all the existing configuration is backed up. After restoring the Audit Vault Server, the existing configuration to the Database Firewall is restored. Follow the steps mentioned in section Backing Up and Restoring the Database Firewall to complete the restore process.

12.16 Archiving and Retrieving Audit Data

Learn about archiving and retrieving audit data of Oracle AVDF on OCI.

Archiving and retrieving audit data is similar to the on-premises deployment. Use OCI File Storage when specifying the archive locations.

To comply with corporate guidelines, all enterprises have data retention policies for audit and network event data. Retention policies define how long the collected data is kept online (so it is visible in reports) and for how long it is to be kept in archive. Using Oracle AVDF, you can set the data retention policies for every target. Data is visible in reports during the online period. For archiving, Oracle AVDF supports both manual and automatic modes. When manual archiving mode is enabled, as soon as the online period expires, data is made offline, but stays on Audit Vault Server. It has to be moved manually to a remote location. If the mode is set to automatic archiving, data is automatically moved to an NFS configured location, after the online period expires. Oracle AVDF allows switching between manual and automatic archiving modes. For Audit Vault Server deployed in OCI, use OCI File Storage for configuring NFS locations.

> **See Also:**
>
> Archiving and Retrieving Audit Data

12.17 Starting or Stopping the Oracle AVDF Instance

Learn how to start or stop the Oracle AVDF instance.

Audit Vault Server console or the OCI console can be used to start or stop the instances. Instances that are stopped can only be started using the OCI console.

Refer to Stopping and Starting an Instance using OCI console.

From the Audit Vault Server console, you can stop or reboot the Oracle AVDF instance.

To Power Off or Reboot the Audit Vault Server instance

1. Log in to the Audit Vault Server console as a super administrator.
2. Click **Settings** tab.
3. Click **System** tab in the left navigation menu.
4. In the main page to the top right corner, click **Power Off** to stop the instance. Click **Reboot** to restart the instance.

To Power Off or Reboot the Database Firewall instance

The Database Firewall instance must be registered in the Audit Vault Server console.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click **Database Firewalls** tab.
3. Select the checkbox against the specific Database Firewall instance.
4. Click **Power Off** to stop the instance. Click **Reboot** to restart the instance.

12.18 Terminating Oracle AVDF Instance

Learn about terminating Oracle AVDF instance.

You can terminate the Oracle AVDF instance using the OCI console by following the steps in section Terminating an Instance.

> **Note:**
>
> When the instance is terminated, all audit and network event data is permanently lost, unless you have taken a backup from which you can restore. Terminated instances are temporarily visible in the list of instances with the status `Terminated`.

13

Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment

To use Oracle Audit Vault and Database Firewall Hybrid Cloud Deployment, you must perform some preliminary tasks.

13.1 Oracle Audit Vault and Database Firewall Hybrid Cloud Deployment and Prerequisites

You can configure Oracle Audit Vault and Database Firewall for hybrid cloud deployments.

Oracle AVDF hybrid cloud deployment models:

1. Audit Vault Server deployed on-premises and the targets are deployed in cloud or on-premises
2. Audit Vault Server deployed on cloud and the targets are deployed in cloud or on-premises

In Oracle Public Cloud deployment model, the Audit Vault Server is either deployed on-premises or in Oracle Cloud. It monitors Oracle Database Cloud Service, Oracle Exadata Cloud Service, and on-premises database instances. It uses Audit Vault Agents that can collect audit data from on-premises or cloud targets. These Agents connect to the target database and to the Audit Vault Server. Connections to the Audit Vault Server are made through JDBC on ports 1521 and 1522. This chapter uses Oracle Public Cloud as an example.

For non-Oracle clouds, the concepts are similar but the actual execution of configuring network connectivity between Agents and databases differ. There is a wide variety of network configurations, firewalls, and cloud providers, each with their own unique ways of configuring network connectivity. When using the hybrid cloud deployment model for Oracle Databases running in non-Oracle clouds, support is limited to Agent interaction with the database. Due to wide variety of network configuration paradigms used by different cloud providers, support for network connectivity issues must remain with the cloud provider.

When using the hybrid cloud deployment model for Oracle Databases running on-premises, the Audit Vault Server is running in Public Cloud. In such cases, the configuration of the on-premises network to enable connectivity between the Agents and Audit Vault Server is the responsibility of the customer. Oracle AVDF support is limited to the Audit Vault Agent, and not to the underlying network components involved in allowing the connections.

TCP and TCPS are the two connection options in Oracle Database Cloud Service. Setting up connections for TCP and TCPS is similar. The difference is the port numbers. The following are the key characteristics of Oracle Database Cloud Service cloud target configuration settings:

- TCP connections have encryption enforced by default.
- TCPS connections are configured between Audit Vault Agents and cloud targets.
  - On the Audit Vault Server the TCPS option must be set for cloud targets.
  - Additional Audit Vault Agents can be used to collect audit data from on-premises databases, directories, and operating systems.

> **Note:**
>
> * The user can have multiple Audit Vault Agents to collect data from DBCS instances.
> * Only one Audit Vault Agent can be installed on a host for a single Audit Vault Server. Multiple audit trail collections can be started using a single Audit Vault Agent.

– This deployment offers great flexibility for customers to address consistent audit or security policies across on-premises and cloud environments.

Prerequisites for deploying Audit Vault and Database Firewall Hybrid Cloud

There are many factors to consider before deploying Oracle Audit Vault and Database Firewall Hybrid. The table outlines the availability of Audit Vault and Database Firewall features for databases on-premises against OPC, in case of DBCS and for Exadata Express Cloud Service.

Feature	DBs On-premises	DBs in OPC	Exadata Express Cloud Service	Data Warehouse Cloud Service
Database Table based audit collection (SYS.AUD$; SYS.FGA_LOG$ etc..)	Yes	Yes	No	No
Unified Audit Table Trail	Yes	Yes	Yes	Yes
Database File based audit collection	Yes	No	No	No
REDO log support	Yes	No	No	No
OS audit collection	Yes	No	No	No
Retrieve Entitlements	Yes	Yes	Yes	Yes
Policy retrieval/provisioning for Traditional audit trails	Yes	Yes	No	No
View Interactive reports	Yes	Yes	Yes	Yes
View Scheduled reports	Yes	Yes	Yes	Yes
Stored Procedure Auditing	Yes	No	No	No

Prerequisites for auditing Oracle Audit Vault and Database Firewall Hybrid Cloud

There are multiple aspects that have to be considered while auditing DBCS targets. Audit requirements and audit policies on DBCS cloud targets are critical as the number and type of enabled audit policies directly affects the number of audit records sent to the Audit Vault Server. DBCS instances may have various audit settings. Hence users must review this information either on the Audit Vault Server or directly on the database instance.

Note:

The audit data collection from table based audit trails is only supported. The version specific information is listed below:

Release	Audit information supported
Oracle Database 11*g* Release 11.2	• Fine Grained Audit • Database Vault Audit • Traditional Audit data stored in *sys.AUD$*
Oracle Database 12*c* and later	• Unified Audit • Database Vault Audit • Fine Grained Audit • Traditional Audit data stored in *sys.AUD$*

Note:

The *SYS.AUD$* and *SYS.FGA_LOG$* tables have an additional column *RLS$INFO*. The Unified Audit trail table has *RLS_INFO* column. This column describes row level security policies configured. This is mapped to the extension field in Oracle Audit Vault and Database Firewall. In order to populate this column, the user needs to set the `AUDIT_TRAIL` parameter of the target to `DB EXTENDED`.

13.2 Opening Ports on Oracle Database Cloud Service

You can open ports on Oracle Database Cloud Service.

This procedure is used to open up a specific port. This is one of the pre-requisites before deploying Audit Vault and Database Firewall Hybrid Cloud.

To open a port, execute the following procedure:

1. Log in to the DBCS service.
2. Click on the navigation menu that is located next to the Oracle logo on the top.
3. Select **Oracle Cloud Infrastructure Compute for Oracle Public Cloud** service.
4. In the next screen, click on **Network** tab that is located at the top of setup port or allowlist.
5. Click the **Security Application** tab to display the list of available ports.
6. Click **Create Security Application** and specify the port that must be enabled.
7. Click **Security Rules** tab, and then click **Create Security Rule** button.
8. In the **Security Application** field select the application previously chosen.
9. Enter the remaining fields.
10. Click **Create.**

13.3 Configuring Hybrid Cloud Target Using TCP

You can configure cloud targets for DBCS instances in TCP mode. The Audit Vault server and Audit Vault agent are installed on-premises.

13.3.1 Step 1: Registering On-premises Host on the Audit Vault Server

This configuration step registers the on-premises host in the Audit Vault server.

In case there is already a registered on-premises host in the Audit Vault server installed on the agent for monitoring Oracle Database Cloud Services instances, bypass this procedure. Otherwise, the steps are similar for all target databases that are on-premises.

> **See Also:**
>
> Registering Hosts on the Audit Vault Server

13.3.2 Step 2: Installing Audit Vault Agent on Registered On-premises Hosts

This configuration step installs Oracle Audit Vault agents on registered on-premises hosts.

> **Note:**
>
> If there is already an Audit Vault agent installed on an on-premises host that is planned for monitoring DBCS instances then ignore this step. In case there are no agents installed, there are specific requirements for the Audit Vault agents that monitor DBCS instances. The requirements or features are as follows:
>
> 1. The agent has to run on-premise.
> 2. A minimum of one agent must be dedicated to monitor only DBCS instances. There may be multiple agents dedicated to monitor only DBCS instances.
> 3. The agent should not run on the Audit Vault server.

1. Install the Audit Vault agent on the on-premises host.

   > **See Also:**
   >
   > Deploying the Audit Vault Agent on Host Computers for detailed steps on installing on-premises host.

2. Start the Audit Vault agent.

13.3.3 Step 3: Creating User Accounts on Oracle Database Cloud Service Target Instances

This configuration step creates user accounts on Oracle Database Cloud Service target instances.

> **Note:**
>
> The connection methodology is different in case on-premises deployment, for TCP connections.

Prerequisite

- Port 1521 has to be opened on the DBCS instance for TCP connection so that later SQL*Plus and SQL*Developer can be used. TCP connection is encrypted by default. It utilizes the native encryption. See Opening Ports on Oracle Database Cloud Service for detailed steps.

Procedure for installation:

1. Ensure that the connection has been established to the DBCS instances through TCP as user with *SYSDBA* administrative privilege.
2. Scripts and respective actions:

Script	Action
`oracle_AVDF_dbcs_user_setup.sql`	To setup target user account.
`oracle_AVDF_dbcs_drop_db_permissions.sql`	To revoke permission from user.

3. Execute the script in order to setup target user account in specific mode:

   ```
   oracle_AVDF_dbcs_user_setup.sql <username> <mode>
   ```

   Where `<username>` is the user name of the Hybrid cloud target user.

   The <mode> can be one of the following:

Mode	Purpose
`AUDIT_COLLECTION`	To collect data from Oracle Cloud instance *TABLE* audit trail in Oracle Audit Vault and Database Firewall.
`AUDIT_SETTING_PROVISIONING`	To set up privileges for managing the Oracle Cloud instance audit policy from Oracle Audit Vault and Database Firewall.
`STORED_PROCEDURE_AUDITING`	To enable stored procedure auditing for the Oracle Cloud instance.
`ENTITLEMENT_RETRIEVAL`	To enable user entitlement retrieval for Oracle Cloud instance.
`ALL`	To enable all the above mentioned options.

13.3.4 Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Database Cloud Service Instances

This configuration step explains how to manage audit policies on target Oracle Database Cloud Service instances.

Check the audit polices that are enabled and change them as needed. For Oracle Database 11*g* release 11.2 and Oracle Database 12*c* instances where the Unified audit is not enabled, it is possible to provision audit policies from the Audit Vault server. If the Unified Trail is enabled on Oracle12*c* instances, ensure to change the audit policies manually on the DBCS instance.

> **Note:**
>
> Ensure to understand the audit settings on the DBCS instances before starting the audit data collection process. Currently one Audit Vault agent supports up to a maximum of 10 cloud target audit trails. The collection speed is up to 25 million audit records per target audit trail, per day. The recommended Audit Vault agent configuration can be found in the *Oracle Audit Vault and Database Firewall Installation Guide.*

Run the `DBMS_AUDIT_MGMT` package on the DBCS instances for audit clean up, after the data is collected by on-premises Audit Vault Server. The Audit Vault Server supports data retention policies for every target and meets compliance requirements. It allows configuring different retention policies for on-premises and DBCS instances.

Storage requirements on the Audit Vault Server also must be reviewed to ensure enough storage is available, while adding more on-premises or DBCS instance targets to the Audit Vault Server.

13.3.5 Step 5: Creating Targets on Oracle Audit Vault Server for Oracle Database Cloud Service Instances

This configuration step creates targets on Oracle Audit Vault Servers for Oracle Database Cloud Service instances.

To connect to the DBCS instance the configuration is the same as for on-premise targets. The user must define these specific settings on the target configuration page.

1. Log in to Audit Vault console with as an administrator.
2. Click the **Targets** tab.
3. Click the **Register** button on the right.
4. Enter a **Name** for the target and select from the **Type** menu.
5. Optionally fill in the **Description** field.
6. Under the **Audit Connection Details** sub tab, choose the **Advanced** option.
7. In the **Protocol** menu, select **TCP**.

8. In the **Target Location** field, enter the following settings:

   ```
   jdbc:oracle:thin:@//host_ip:port_number/service_name
   ```

   Alternatively, you can accomplish this uing the **Basic** option. Enter the details in **Host Name/IP Address**, **Port**, **Service Name** fields.
9. Enter the **User Name** and **Password**.
10. Click **Save** to save the configuration changes.

13.3.6 Step 6: Starting Audit Trail on Audit Vault Server for Oracle Database Cloud Service Instances

This configuration step starts the audit trail on Oracle Audit Vault Server for Oracle Database Cloud Service instances.

Use this procedure to start an audit trail on the Audit Vault Server for the DBCS instance.

1. Log in to the Audit Vault console as an administrator.
2. In the **Targets** tab, select the newly registered target.
3. Under **Audit Data Collection** section, click **Add**. The **Add Audit Trail** dialog is displayed.
4. Select **Audit Trail Type** as `TABLE`.

   > **Note:**
   >
   > Other trail types are not supported for DBCS target instances.

5. Select the appropriate values in the **Trail Location** from the drop down menu.

   The supported table trails for Oracle DBCS target are:

   a. `UNIFIED_AUDIT_TRAIL`
   b. `SYS.AUD$`
   c. `SYS.FGA_LOG$`
   d. `DVSYS.AUDIT_TRAIL$`
6. Select the **Agent Host**.
7. Click **Save** to add the audit trail.

13.4 Configuring TCPS Connections for DBCS Instances

Learn how to configure TCPS connections for DBCS instances.

13.4.1 Step 1: Creating Server Wallet and Certificate

This configuration step shows you how to create server wallets and certificates.

1. Ensure that port 1522 is open on the DBCS instance for TCPS connection. .

See Opening Ports on Oracle Database Cloud Service for detailed information. Later some standard tools such as SQL*Plus and SQL*Developer can be used

2. Create a new auto-login wallet by executing the `orapki` utility.

```
mkdir -p <wallet path>

orapki wallet create -wallet <wallet path> -auto_login
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
orapki wallet create -wallet /u01/app/example/demowallet -auto_login
```

3. Create a self-signed certificate and load it into the wallet, by executing the command:

```
orapki wallet add -wallet <wallet path> -dn
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

```
CN=hostname -keysize 1024 -self_signed -validity 365
```

Example:

```
orapki wallet add -wallet /u01/app/example/demowallet -dn

CN=CloudAB2.abcdXY.example.somedomain -keysize 1024 -self_signed -validity 365
```

4. Check the contents of the wallet by executing the following command:

```
orapki wallet display -wallet <wallet path>
```

Result:

Displays the self-signed certificate which is both a user and trusted certificate.

```
Requested Certificates:
User Certificates:
Subject:          CN=<hostname>
Trusted Certificates:
Subject:          CN=<hostname>
```

Example:

```
orapki wallet display -wallet /u01/app/example/demowallet
```

Result:

```
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights
reserved.

Requested Certificates:
User Certificates:
```

```
Subject:         CN=CloudAB2.abcdXY.example.somedomain
Trusted Certificates:
Subject:         CN=CloudAB2.abcdXY.example.somedomain
```

5. Export the certificate to the client wallet for future use, by executing the command:

```
orapki wallet export -wallet <wallet path> -dn CN=hostname
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

```
-cert <certificate file name>.crt
```

Example:

```
orapki wallet export -wallet /u01/app/example/demowallet -dn
CN=CloudAB2.abcdXY.example.somedomain -cert CloudAB2-certificate.crt
```

6. Check that the certificate has been exported as expected, by executing the command:

```
cat <certificate file name>.crt
```

Example:

```
cat CloudAB2-certificate.crt
```

Result:

```
-----BEGIN CERTIFICATE-----
MIIB0TCCAToCAQAwDQYJKoZIhvcNAQEEBQAwMTEvMC0GA1UEAxMmQ2xvdWRTVDIuZGViZGV2MTk
u
b3JhY2xlY2xvdWQuaW50ZXJuYWwwHhcNMTYwNTExMTEyMDI2WhcNMjYwNTA5MTEyMDI2WjAxMS8
w
LQYDVQQDEyZDbG91ZFNUMi5kZWJkZXYxOS5vcmFjbGVjbG91ZC5pbnRlcm5hbDCBnzANBgkqhki
G
9w0BAQEFAAOBjQAwgYkCgYEAr6fhuQly2t3i8gugLVzgP2kFGVXVOzqbggEIC+Qazb15JuKs0nt
k
En9ERGvA0fxHkAkCtIPjCzQD5WYRU9C8AQQOWe7UFHae7PsQX8jsmEtecpr5Wkq3818+26qU3Jy
i
XxxK/rRydwBO526G5Tn5XPsovaw/PYJxF/
fIKMG7fzMCAwEAATANBgkqhkiG9w0BAQQFAAOBgQCu
fBYJj4wQYriZIfjij4eac/
jnO85EifF3L3DU8qCHJxOxRgK97GJzD73TiY20xpzQjWKougX73YKV
Tp9yusAx/T/
qXbpAD9JKyHlKj16wPeeMcS06pmDDXtJ2CYqOUwMIk53cK7mLaAHCbYGGM6btqP4V
KYIjP48GrsQ5MOqd0w==
-----END CERTIFICATE-----
```

13.4.2 Step 2: Creating Client (Agent) Wallet and Certificate

This configuration step explains how to create client wallets and certificates.

1. Run the following command to create a new auto-login wallet:

```
c:\>mkdir -p <client wallet dir>


c:\>orapki wallet create -wallet "<wallet path>" -auto_login
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
C:\Work\CloudWallet>orapki wallet create -wallet C:\Work\CloudWallet -
auto_login
```

Result:

```
Oracle PKI Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights
reserved.
```

2. Run the following command to create a self-signed certificate and load it into the wallet:

```
c:\>orapki wallet add -wallet <client wallet path> -dn
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

```
CN=%client computer name% -keysize 1024 -self_signed -validity 365
```

Example:

```
C:\Work\CloudWallet>orapki wallet add -wallet C:\Work\CloudWallet -dn


CN=machine1.somedomain.com -keysize 1024 -self_signed -validity 365
```

Result:

```
Oracle PKI Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights
reserved.
```

3. Check the contents of the wallet by running the command:

```
orapki wallet display -wallet <client wallet path>
```

> **Note:**
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
C:\Work\CloudWallet>orapki wallet display -wallet C:\Work\CloudWallet
```

Result:

```
Oracle PKI Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights
reserved.

Requested Certificates:
User Certificates:
Subject:        CN=machine1.foobar.example.com
Trusted Certificates:
Subject:        OU=Class 3 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
Subject:        CN=GTE CyberTrust Global Root,OU=GTE CyberTrust Solutions\,
Inc.,O=GTE Corporation,C=US
Subject:        OU=Class 2 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
Subject:        OU=Class 1 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
Subject:        CN=machine1.foobar.example.com
```

4. Run the following command to export the certificate and load it onto the server:

```
orapki wallet export -wallet <client wallet path> -dn
```

> **Note:**
> This command will prompt you to enter and re-enter a wallet password.

```
CN=<client computer name> -cert <clent computer name>-certificate.crt
```

Example:

```
C:\Work\CloudWallet>orapki wallet export -wallet C:\Work\CloudWallet -dn


CN=machine1.foobar.example.com -cert machine1-certificate.crt
```

Result:

```
Oracle PKI Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights
reserved.
```

5. Check the certificate by running the command:

```
more c:\%computername%-certificate.crt
```

Example:

```
C:\Work\CloudWallet>more machine1-certificate.crt
```

Result:

```
-----BEGIN CERTIFICATE-----
MIIBsTCCARoCAQAwDQYJKoZIhvcNAQEEBQAwITEfMB0GA1UEAxMWZ2JyMzAxMzkudWsub3JhY2x
l
LmNvbTAeFw0xNjA1MTExMTQzMzFaFw0yNjA1MDkxMTQzMzFaMCExHzAdBgNVBAMTFmdicjMwMTM
5
LnVrLm9yYWNsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKH8G8sFS6l0llu+RMf
l
7Yt+Ppw8J0PfDEDbTGP5wtsrs/
22dUCipU9l+vif1VgSPLE2UPJbGM8tQzTC6UYbBtWHe4CshmvD
EVlcIMsEFvD7a5Q+P45jqNSEtV9VdbGyxaD6i5Y/
Smd+B87FcQQCX54LaI9BJ8SZwmPXgDweADLf
AgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAai742jfNYYTKMq2xxRygGJGn1LhpFenHvuHLBvnTup1
N
nZOBwBi4VxW3CImvwONYcCEFp3E1SRswS5evlfIfruCZ1xQBoUNei3EJ6O3OdKeRRp2E+muXEtf
e
U+jwUE+SzpnzfpI23Okl2vo8Q7VHrSalxE2KEhAzC1UYX7ZYp1U=
-----END CERTIFICATE-----
```

13.4.3 Step 3: Exchanging Client (Agent) and Server Certificates

This configuration step explains how to exchange client (agent) and server certificates.

1. Exchange client (agent) and server certificates. Each side of the connection has to trust the other. Hence ensure to load the certificate from the server as a trusted certificate into the client wallet and vice versa. Load the server certificate into the client wallet by executing the command:

```
orapki wallet add –wallet <client wallet path> -trusted_cert -cert <server
certificate path>
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
C:\Work\CloudWallet>orapki wallet add -wallet C:\Work\CloudWallet -
trusted_cert -cert C:\Work\CloudWallet\CloudAB2-certificate.crt
```

Result:

```
Oracle PKI Tool : Version 12.1.0.1

Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights reserved.
```

2. Check the contents of the client wallet by executing the command:

```
orapki wallet display -wallet <client wallet path>
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
C:\Work\CloudWallet>orapki wallet display -wallet C:\Work\CloudWallet
```

Notice the self-signed certificate is a trusted user certificate.

Result:

```
Oracle PKI Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights
reserved.

Requested Certificates:
User Certificates:
Subject:       CN=machine1.foobar.example.com
Trusted Certificates:
Subject:        OU=Class 1 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
Subject:        CN=machine1.foobar.example.com
Subject:        CN=GTE CyberTrust Global Root,OU=MNO CyberTrust
Solutions\, Inc.,O=MNO Corporation,C=US
Subject:        CN=CloudAB2.abcxy10.example.somedomain
Subject:        OU=Class 3 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
Subject:        OU=Class 2 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
```

3. Load the client certificate into server by executing the command:

```
orapki wallet add -wallet <server wallet path> -trusted_cert -cert <client
certificate file>
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
orapki wallet add -wallet /u01/app/example/demowallet -trusted_cert -cert
machine1-certificate.crt
```

Result:

```
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights
reserved.
```

4. Check the contents of the client wallet by executing the command:

```
orapki wallet display -wallet <client wallet path>
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
C:\Work\CloudWallet>orapki wallet display -wallet C:\Work\CloudWallet
```

The server certificate is now included in the list of trusted certificates.

Result:

```
Oracle PKI Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights
reserved.


Requested Certificates:
User Certificates:
Subject:        CN=machine1.foobar.example.com
Trusted Certificates:
Subject:        OU=Class 1 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
Subject:        CN=machine1.foobar.example.com
Subject:        CN=GTE CyberTrust Global Root,OU=MNO CyberTrust
Solutions\, Inc.,O=MNO Corporation,C=US
Subject:        CN=CloudAB2.abcdXY.example.somedomain
Subject:        OU=Class 3 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
Subject:        OU=Class 2 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US
```

5. Load the client certificate into server by executing the command:

```
orapki wallet add -wallet <server wallet path> -trusted_cert -cert <client
certificate file>
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
orapki wallet add -wallet /u01/app/example/demowallet -trusted_cert -cert
machine1-certificate.crt
```

Result:

```
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights
reserved.
```

6. Check the contents of the server wallet by executing the command:

```
orapki wallet display -wallet <wallet path>
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

Example:

```
orapki wallet display -wallet /u01/app/example/demowallet
```

Result:

```
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights
reserved.

Requested Certificates:
User Certificates:
Subject:        CN=CloudAB2.abcdXY.example.somedomain
Trusted Certificates:
Subject:        CN=CloudAB2.abcdXY.example.somedomain
Subject:        CN=machine1.foobar.example.com
```

13.4.4 Step 4: Configuring Server Network

This step explains how to configure the server network.

Data security between an Audit Vault Server and an Oracle Database target is achieved by default, through network encryption over TCP connection. Data security can also be achieved by using a TCPS/SSL connection.

1. Configure the server network. Add the following entries on the server and into the `$ORACLE_HOME/network/admin/sqlnet.ora` file:

```
orapki wallet add -wallet <client wallet path> -trusted_cert -cert <server
certificate path>
```

> **Note:**
>
> This command will prompt you to enter and re-enter a wallet password.

```
WALLET_LOCATION =
   (SOURCE =
     (METHOD = FILE)
     (METHOD_DATA =
       (DIRECTORY = /u01/app/oracle/demowallet)
     )
   )

SQLNET.AUTHENTICATION_SERVICES = (TCPS,TCP,NTS,BEQ)
SSL_CLIENT_AUTHENTICATION = TRUE

SQLNET.ENCRYPTION_SERVER = ACCEPTED/REQUESTED/REJECTED
SQLNET.CRYPTO_CHECKSUM_SERVER = ACCEPTED/REQUESTED/REJECTED
```

Note:

a. The server encryption is set to *REQUIRED* on the DBCS instance and on-premises by default. Set the server encryption to *ACCEPTED* or *REQUESTED* or *REJECTED*.

b. *REJECTED* is not a recommended option. The following table describes these options in detail.

Option	Description
ACCEPTED	The server does not allow both encrypted and non-encrypted connections. This is the default value in case the parameter is not set.
REJECTED	The server does not allow encrypted traffic.
REQUESTED	The server requests encrypted traffic if it is possible, but accepts non-encrypted traffic if encryption is not possible.
REQUIRED	The server accepts only encrypted traffic.

2. Configure the listener to accept SSL or TLS encrypted connections. Edit the `$ORACLE_HOME/network/admin/listener.ora` file. Add the wallet information and the TCPS entry. Set the values as follows, using the directory location that you specified for your environment:

```
SSL_CLIENT_AUTHENTICATION = TRUE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = /u01/app/oracle/demowallet)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = <host name>.localdomain)(PORT =
1521))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
      (ADDRESS = (PROTOCOL = TCPS)(HOST = <host name>.localdomain)(PORT =
1522))
    )
  )
```

3. Restart the listener by executing the following commands:

```
$ lsnrctl stop
```

Example:

```
$ lsnrctl start
```

13.4.5 Step 5: Connecting to DBCS instances in TCPS mode

To connect Oracle Database Cloud Service instances with TCPS follow these steps:

1. Enable port 1522 on the cloud service.
2. Configure TCPS connection for the DBCS instance once port 1522 has been opened.
3. Create the server wallet and certificate.
4. Create client (agent) wallet and certificate.
5. Exchange the client (agent) and server certificates.
6. Configure the server network.
7. Connect to the DBCS instance through TCPS using the Audit Vault agent or tools like **SQL*Plus** or **SQL*Developer**.

> **See Also:**
>
> - Configuring TCPS Connections for DBCS Instances for detailed steps on configuring TCPS for DBCS instance.
> - Opening Ports on Oracle Database Cloud Service

13.5 Configuring Hybrid Cloud Target Using TCPS

Learn how to configure cloud targets for DBCS instances in TCPS mode. The Audit Vault server and Audit Vault agent are installed on-premises.

13.5.1 Step 1: Registering On-premises Host on Oracle Audit Vault Server

Follow this configuration procedure to register on-premises hosts on Oracle Audit Vault Server.

This step registers the on-premises host on the Audit Vault server.

> **Note:**
>
> If there is already a registered on-premises host in the Audit Vault Server installed on the Agent for monitoring DBCS instances, then skip this procedure. Otherwise, the steps are similar for all target databases that are on-premises. See Registering Hosts on the Audit Vault Server for detailed steps.

13.5.2 Step 2: Installing Oracle Audit Vault Agent on Registered On-premises Hosts and Configuring TCPS

This configuration procedure installs Oracle Audit Vault Agent on registered on-premises hosts and configures TCPS.

> **Note:**
>
> If there is already an Audit Vault agent installed on an on-premises host that is planned for monitoring DBCS instances then ignore this step. In case there are no agents installed, there are specific requirements for the Audit Vault agents that monitor DBCS instances. The requirements or features are as follows:
>
> 1. The agent has to run on-premise.
> 2. A minimum of one agent must be dedicated to monitor only DBCS instances. There may be multiple agents dedicated to monitor only DBCS instances.
> 3. The agent should not run on the Audit Vault server.

1. Install the Audit Vault agent on the on-premises host. See Deploying the Audit Vault Agent on Host Computers for detailed steps on installing on-premises host.
2. Start the Audit Vault agent.

13.5.3 Step 3: Creating User Accounts on Oracle Database Cloud Service Target Instances

This step creates a user account on the Oracle Database Cloud Service instance.

> **Note:**
>
> The connection methodology and scripts utilized are different in case on-premises deployment.

Prerequisite

- Port 1522 has to be opened up on the DBCS instance for TCP connection so that later SQL*Plus and SQL*Developer can be used. TCP connection is encrypted by default. It utilizes the native encryption. See Opening Ports on Oracle Database Cloud Service for detailed steps.

Procedure:

1. Ensure that the connection has been established to the DBCS instances through TCPS as user with *SYSDBA* administrative privilege.
2. Create Server Wallet and certificate.
3. Create Client Wallet and certificate.
4. Exchange Client and Server certificates.

5. Configure Server network.

> **Note:**
>
> See “Configuring TCPS Connections for DBCS Instances” for creating Server Wallet, Client Wallet, certificates, and exchanging certificates.

6. Once the above steps are complete, the user can now connect to the DBCS instances in TCPS using the Audit Vault Agent or tools like SQL*Plus and SQL*Developer.
7. Execute the following commands to create audit retrieval user account creation scripts:
   a. `oracle_AVDF_dbcs_user_setup.sql`
   b. `oracle_AVDF_dbcs_drop_db_permissions.sql`

> **Note:**
>
> These scripts are different from those of the on-premises database instances.

13.5.4 Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Database Cloud Service Instances

Use this procedure to set up and review audit policies on target Oracle Database Cloud Service instances.

Check the audit polices that are enabled and change them as needed. For Oracle Database 11g, Oracle Database 11.2, and Oracle Database 12c release instances where the unified audit is not enabled, you can provision audit policies from the Audit Vault Server. If the Unified Trail is enabled on Oracle Database 12c instances, change the audit policies manually on the DBCS instance.

> **Note:**
>
> - Understand the audit settings on the DBCS instances, before starting the audit data collection process. Currently one Audit Vault Agent supports up to a maximum of 10 cloud target audit trails. The collection speed is up to 25 million audit records per target audit trail, in a day. The recommended Audit Vault Agent configuration can be found in the Oracle Audit Vault and Database Firewall Installation Guide.
> - Run the DBMS_AUDIT_MGMT package on the DBCS instances for audit clean up, once the data is collected by the on-premises Audit Vault Server. The Audit Vault Server supports data retention policies for every target and meets compliance requirements. It allows configuring different retention policies for on-premises and DBCS instances.

13.5.5 Step 5: Creating Targets on Audit Vault Server for Oracle Database Cloud Service Instances

This configuration step creates target on Oracle Audit Vault Servers for Oracle Database Cloud Service instances.

The user must define these specific settings on the target configuration page. Use the following procedure:

1. Log in to Audit Vault console as an administrator.
2. Click **Targets** tab.
3. Click the **Register** button on the right.
4. Enter a **Name** for the target and select from the **Type** menu.
5. Optionally fill in the **Description** field.
6. Under the **Audit Connection Details** sub tab, choose the **Advanced** option.
7. In the **Protocol** menu, select **TCPS**.
8. In the **Wallet** field, choose the client wallet by navigating to the location of the wallet where it was previously created.
9. Enter the following TCPS connection string in the **Target Location** field:

   ```
   jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=<Host IP>)
   (PORT=<Port Number>))(CONNECT_DATA=(SERVICE_NAME=<service name>)
   (SERVER=DEDICATED))(SECURITY= (SSL_SERVER_CERT_DN="DN")))
   ```

   This can also be accomplished in the **Basic** option. Enter the details in **Host Name/IP Address**, **Server DN**, and the **Wallet** fields.
10. Enter the **User Name** and **Password**.
11. Click **Save** to save the configuration changes.

> **See Also:**
>
> Configuring TCPS Connections for DBCS Instances for information on creating a wallet.

13.5.6 Step 6: Starting Audit Trail on Audit Vault Server for Oracle Database Cloud Services Instances

This configuration step starts an audit trail on Oracle Audit Vault Server for Oracle Database Cloud Service instances.

Use this procedure to start audit trail on the Audit Vault Server for the DBCS instance:

1. Log in to the Audit Vault console as an administrator.
2. In the **Targets** tab, select the newly registered target.
3. Under **Audit Data Collection** section, click **Add**. The **Add Audit Trail** dialog is displayed.

4. Select **Audit Trail Type** as `TABLE`.

> **Note:**
>
> Other trail types are not supported for the DBCS target instance.

5. Select the appropriate values in the **Trail Location** from the drop down menu. The supported table trails for Oracle DBCS target are:
   a. `UNIFIED_AUDIT_TRAIL`
   b. `SYS.AUD$`
   c. `SYS.FGA_LOG$`
   d. `DVSYS.AUDIT_TRAIL$`
6. Select the **Agent Host**.
7. Click **Save** to add the audit trail.

13.6 Configuring Oracle Database Exadata Express Cloud Service Target Using TCPS

Learn how to configure Oracle Database Exadata Express Cloud Service targets in TCPS mode.

13.6.1 Step 1: Installing Audit Vault Agent on registered On-premises Hosts and Configuring TCPS

This step installs Oracle Audit Vault Agent on registered on-premises hosts and configures TCPS.

See Step 2: Installing Oracle Audit Vault Agent on Registered On-premises Hosts and Configuring TCPS.

Prerequisites

- Ensure the right version of JDK is installed. The supported JDK versions are:
  - JDK7u80 or higher
  - JDK8u71
  - JCE Unlimited Strength Jurisdiction Policy Files with both JDK7 and JDK8. JDK 8 .jar files can be downloaded from: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

13.6.2 Step 2: Creating User Accounts on Oracle Exadata Express Cloud Service Instances

This configuration step creates user accounts on Oracle Exadata Express Cloud Service Instances.

Procedure:

1. Ensure that the connection has been established to the Oracle Database Cloud Service instances through TCPS as user with SYSDBA administrative privilege.
2. Create Server Wallet and certificate.
3. Create Client Wallet and certificate.
4. Exchange Client and Server certificates.
5. Configure Server network.
6. After the above steps are complete, you can now connect to the DBCS instances in TCPS using the Audit Vault Agent or tools like SQL*Plus and SQL*Developer.
7. Run the following commands to create audit retrieval user account scripts:

   ```
   oracle_AVDF_E1_user_setup.sql
   ```

   ```
   oracle_AVDF_E1_drop_db_permissions.sql
   ```

> **See Also:**
>
> Configuring TCPS Connections for DBCS Instances for creating Server Wallet, Client Wallet, certificates, and exchanging certificates.

13.6.3 Step 3: Creating Targets on Oracle Audit Vault Server for Oracle Exadata Express Cloud Service Instances

This configuration step creates targets on Oracle Audit Vault Server for Oracle Exadata Express Cloud Service instances.

1. Create a target on Oracle Audit Vault Server for the DBCS Instance. See Step 5: Creating Targets on Audit Vault Server for Oracle Database Cloud Service Instances.
2. Execute the following command to set mandatory target attribute for SSL version:

   ```
   av.collector.stconn.oracle.net.ssl_version = 1.2
   ```

13.7 Configuring Oracle Database Exadata Express Cloud Service Target Using TCP

Learn how to configure Exadata Express Cloud Targets in TCP mode. The Audit Vault Server and Audit Vault Agent are installed on-premises.

13.7.1 Step 1: Registering On-premises Hosts on Oracle Audit Vault Server

This configuration step explains how to register on-premises hosts on Oracle Audit Vault Server.

See Step 1: Registering On-premises Host on the Audit Vault Server.

13.7.2 Step 2: Installing Audit Vault Agents on Registered On-Premises Hosts

This configuration step installs agents on registered on-premises hosts.

See Step 2: Installing Audit Vault Agent on Registered On-premises Hosts.

13.7.3 Step 3: Creating User Accounts on Oracle Exadata Express Cloud Target Instances

This configuration step creates user accounts on Oracle Exadata Express Cloud targets.

1. Log in with SYSDBA administrative privilege and establish a connection to the DBCS instances through TCP.
2. Execute the following commands to create audit retrieval user account scripts:

   ```
   oracle_AVDF_E1_user_setup.sql
   ```

   ```
   oracle_AVDF_E1_drop_db_permissions.sql
   ```

13.7.4 Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Exadata Express Cloud Instances

This configuration step enables you to set up and review audit policies on target Oracle Exadata Express Cloud instances.

> **Note:**
>
> This is not supported for Oracle Exadata Express Cloud Service instance.

13.7.5 Step 5: Creating Targets on Oracle Audit Vault Servers for Oracle Exadata Express Cloud Instances

This configuration step creates targets on Oracle Audit Vault Servers for Oracle Exadata Express Cloud instances.

See Step 5: Creating Targets on Oracle Audit Vault Server for Oracle Database Cloud Service Instances.

13.7.6 Step 6: Starting Audit Trail on Oracle Audit Vault Server for Oracle Exadata Express Cloud Instances

This configuration step starts audit trails on Oracle Audit Vault Server for Oracle Exadata Express Cloud instances.

Use this procedure to start audit trail on Oracle Audit Vault Server for Oracle Exadata Express Cloud instances:

1. Log in to the Audit Vault console as an administrator.
2. In the **Targets** tab, select the newly registered target.
3. Under **Audit Data Collection** section, click **Add**. The **Add Audit Trail** dialog is displayed.
4. Select **Audit Trail Type** as `TABLE`.

> **Note:**
>
> Other trail types are not supported for the Express Exadata Cloud target instance.

5. Select the appropriate values in the **Trail Location** from the drop-down menu. The supported table trails for Oracle Express Exadata Cloud target are:
   a. `UNIFIED_AUDIT_TRAIL`
6. Click **Save** to add the audit trail.

13.8 Configuring Autonomous Data Warehouse and Autonomous Transaction Processing

Learn how to configure Oracle Database Cloud Service types as targets in TCPS mode for Autonomous Data Warehouse and Autonomous Transaction Processing.

13.8.1 Step 1: Install Audit Vault Agent on Registered Host

This configuration step installs Audit Vault Agents on registered host.

Prerequisites

Ensure the right version of JDK is installed. The supported JDK versions are:

- JDK7u80 or higher
- JDK8u71
- JCE Unlimited Strength Jurisdiction Policy Files with both JDK7 and JDK8. JDK 8 .jar files can be downloaded from: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

Follow these steps:

1. Install the Audit Vault Agent on the host machine. See Deploying the Audit Vault Agent on Host Computers for detailed steps.
2. Start the Audit Vault Agent.

13.8.2 Step 2: Create User Accounts on Oracle Cloud Instances

This configuration step creates user account on Oracle Cloud instances.

Complete this procedure to create a user account on an Autonomous Data Warehouse or on an Autonomous Transaction Processing Cloud instance:

1. Ensure that the connection has been established to the Autonomous Data Warehouse Cloud instances through TCPS as user with *SYSDBA* administrative privilege.

2. Create a user that is used to collect audit data from the database.
3. Run the script to provide relevant privileges to the user:
`oracle_AVDF_dbcs_user_setup.sql`

> **See Also:**
>
> Configuring TCPS Connections for DBCS Instances

13.8.3 Step 3: Create Targets on Audit Vault Server for the Cloud Instances

This configuration step creates a target on Audit Vault Server for the Autonomous Data Warehouse and Autonomous Transaction Processing Cloud instances.

Prerequisites

1. The user must download the client wallet using Oracle Cloud Infrastructure Console. See Download Client Credentials (Wallets) for complete information.
2. Unzip the client wallet. The wallet contains the Single Sign On Wallet file (cwallet.sso).
3. The user can get connection string Using Oracle Cloud Infrastructure Console.

The user must enter these details and specific settings on the target configuration page. Follow the below steps:

1. Log in to Audit Vault Server console as an *administrator*.
2. Click **Targets** tab.
3. Click the **Register** button on the right.
4. Enter a **Name** for the target and select the **Type** as Oracle Database.
5. Optionally fill in the **Description** field.
6. Under the **Audit Connection Details** sub tab, choose the **Advanced** option.
7. In the **Protocol** menu, select `TCPS`.
8. In the **Wallet** field, upload the Single Sign On Wallet file (`cwallet.sso`).
9. Enter the TCPS connection string in the **Target Location** field:
`jdbc:oracle:thin:@<Connection string from OCI Console>`
10. Enter the **User Name** and **Password**.
11. Click **Save** to save the configuration changes.

13.8.4 Step 4: Start Audit Trail on Audit Vault Server for the Autonomous Data Warehouse and Autonomous Transaction Processing Cloud Instances

This configuration step starts an audit trail on Audit Vault Server for the Autonomous Data Warehouse and Autonomous Transaction Processing Cloud instances.

Create audit trail using the Audit Vault Server console for the Autonomous Data Warehouse and Autonomous Transaction Processing Cloud instances. See Step 6: Starting Audit Trail on Audit Vault Server for Oracle Database Cloud Services Instances for complete information.

13.8.5 Step 5: (Optional) Revoke Audit Vault and Database Firewall Privileges for a User

Use this configuration step to revoke user privileges on Oracle Cloud instances.

If a user no longer requires access to audit data on the database, revoke the privileges by running the following script as the *SYS* user with the *SYSDBA* privilege: `oracle_AVDF_dbcs_drop_db_permissions.sql`.

Part II
General Administration Tasks

Learn about Oracle AVDF general administration tasks.

Part II assumes that you have completed the steps in Part I to configure Oracle Audit Vault and Database Firewall. This part covers general administrative tasks.

14

Managing User Accounts and Access

To manage user accounts and access, you can use both the command line and the Audit Vault Server console.

14.1 About Oracle Audit Vault and Database Firewall Administrative Accounts

Oracle Audit Vault and Database Firewall administrative accounts help you manage user access.

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 Audit Vault and Database Firewall has two 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 targets and target groups
  - Grants access to targets or target groups to administrators
- **Audit Vault Server Administrator:** Has access to specific targets or target groups granted by a super administrator. Administrators cannot manage system-wide settings.

After installing Oracle Audit Vault and Database Firewall, 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. This super administrator and super auditor created during post installation are Audit Vault Server database users. There is at least one Audit Vault Server database user as super administrator and one as super auditor.

The Audit Vault Server console can be configured to be authenticated using the following methods:

- Local AVDF: Authentication for local users is through local passwords. See Configuring Administrative Accounts for Oracle Audit Vault Server for more information.
- AD/LDAP: Authentication for AD/LDAP users is through Microsoft Active Directory(AD) or OpenLDAP. See Integrating Oracle Audit Vault and Database Firewall with Microsoft Active Directory or OpenLDAP for more information.
- SSO: Single sign-on (SSO) can be configured starting in Oracle AVDF 20.11. Authentication for SSO users is through SAML 2.0 integration with Microsoft Active Directory Federation Service, Microsoft Entra ID (MS-EI), or Oracle Access Manager. See Configuring Single Sign-On (SSO) for Audit Vault Server Console Users for more information.

Thereafter, the Audit Vault Server super administrator can create other administrative users, and the super auditor can create other auditor users, for the server.

This chapter describes managing user accounts and passwords for the Oracle Audit Vault and Database Firewall administrator user interfaces.

See Also:

- *Oracle Audit Vault and Database Firewall Installation Guide* for information on post-installation configuration.
- *Oracle Audit Vault and Database Firewall Auditor's Guide* for information on managing auditor accounts.

14.2 Security Technical Implementation Guides and Implementation for User Accounts

Oracle Audit Vault and Database Firewall follow STIG guidelines for user accounts.

Oracle Audit Vault and Database Firewall follows the Security Technical Implementation Guides (STIG) and implementation rules for user accounts.

- The default Oracle Audit Vault and Database Firewall user accounts must have custom passwords.
- The number of consecutive failed login attempts is 3.
- When a user exceeds the maximum number of unsuccessful login attempts, the account is locked until a super administrator releases it.
- Account lockouts will persist until a super administrator resets the user account.

See Also:

Security Technical Implementation Guides for more information about STIG compliance

14.3 Configuring Administrative Accounts for Oracle Audit Vault Server

Learn how to configure administrative accounts for Oracle Audit Vault Server.

14.3.1 Guidelines for Securing Oracle Audit Vault and Database Firewall User Accounts

Review the guidelines for securing Oracle Audit Vault and Database Firewall user accounts.

As a best practice, use the installed Oracle 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 Audit Vault and Database Firewall operations.

> **Note:**
>
> Oracle Audit Vault and Database Firewall does not accept user names with quotation marks. For example, `"jsmith"` is not a valid user name for an Oracle Audit Vault and Database Firewall user account, or an account created on a target for use by Oracle Audit Vault and Database Firewall.

14.3.2 Creating Local Administrative User

You can create Audit Vault Server administrative accounts to manage administration.

Audit Vault Server super administrators can create both super administrator and administrator user accounts.

1. Log in to the Audit Vault Server console as a *super administrator*.
2. Click the **Settings** tab.
   The **Manage Admins** subtab on the main page is selected by default.
3. Click **Add** in the top, right corner.
4. In the **Add Admin** dialog box, select **Local AVDF User**.
5. For **Local AVDF User**, enter the details to create a database administrator.
6. Enter the newly created **Admin Name**.
7. Select the **Admin Type**.
8. Enter the **Password** and **Re-type Password**.
   Oracle Audit Vault and Database Firewall does not accept user names with quotation marks, such as `"jsmith"`.
9. Click **Save**.

Related Topics

- About Oracle Audit Vault and Database Firewall Administrative Accounts
  Oracle Audit Vault and Database Firewall administrative accounts help you manage user access.

14.3.3 Viewing the Status of Administrator User Accounts

Learn how to view the status of administrator accounts.

As a super administrator, you can view the status of administrator accounts by clicking the **Settings** tab. The **Manage Admins** sub tab lists all administrator and super administrator accounts, with their statuses, password expiry dates, the targets and target groups they have access to, etc.

14.3.4 Changing User Account Types for Audit Vault Server

You can change Audit Vault Server administrative account type from administrator to super administrator, or vice versa.

You can change an administrative account type from administrator to super administrator, or vice versa.

> **Note:**
>
> If you change a user's account type from administrator to super administrator, then the user will have access to all targets and target groups.

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.

   The **Manage Admins** section appears by default. It displays existing users and the targets or groups to which they have access.
3. Click the name of the user account that you want to change.
4. In the **Modify Admin** dialog, click the edit icon against the **Type** field.
5. You can change the type from **Admin** to **Super Admin**. If you want to change the type from **Super Admin** to **Admin**.
6. You can also grant or revoke access to any targets or groups as necessary for this user.

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Select the targets or groups to which you want to grant or revoke access. b. Click **Grant** or **Revoke** button. A green check mark indicates access granted. A red cross mark (X) indicates access revoked.	a. Select the targets or groups to which you want to grant or revoke access. You can also search for the targets or groups in the field under **Targets & Target Groups**. b. Choose the access rights in the **Available** column and move them to the **Selected** column, to grant access. Choose the access rights in the **Selected** column and move them to the **Available** column, to revoke access.

7. Click **Save**.

14.3.5 Unlocking User Accounts

This procedure explains how to unlock user accounts.

An Oracle Audit Vault and Database Firewall administrator account is locked after at least 3 failed login attempts. A super administrator must unlock user accounts.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.

   The **Manage Admin** sub tab is selected by default. It displays a list of existing users.
3. Click the name of the user account you want to unlock.
4. In the dialog, click **Unlock**.

> **See Also:**
>
> ALTER USER

14.3.5.1 Unlocking Super Administrator or Super Auditor Users

The below process should be used to unlock the last super administrator or last super auditor users. It can also be used as an alternative to unlocking other users through the console.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `dvaccountmgr` user.

   ```
   su - dvaccountmgr
   ```

3. Start SQL*Plus without the user name and password.

   ```
   sqlplus /
   ```

4. If the account is locked, run the following command to unlock the account:

   ```
   alter user <user name> account unlock;
   ```

14.3.6 Deleting Oracle Audit Vault Server Administrator Accounts

You may need to delete Oracle Audit Vault Server Administrator accounts with this procedure.

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.

   The Manage Admin page appears by default, and displays existing users and the targets or groups to which they have access.

3. Select the users you want to delete, and then click **Delete**.

14.4 Configuring sudo Access for Users

Learn about configuring sudo access for users.

14.4.1 About Configuring sudo Access

Learn about configuring sudo access.

The `sudo` command enables trusted users to have administrative access to systems without having to log in using `root` user passwords.

When users have `sudo` access, they can precede an administrative command with `sudo`, and then be prompted to enter their password. After authentication is complete, and assuming that the command is permitted, the command is processed as if it had been run by the `root` user.

14.4.2 Configuring sudo Access for Users

Learn about configuring sudo access for users.

You need `root` privileges to configure `sudo` access for users.

1. Log in to the system as the `root` user.

2. Create a new user account using the `useradd` command with the `-G support` option. This ensures the new user is added to the `support` group, granting them SSH access to the appliance.

   For example, to create a normal user account for the user `psmith`:

   ```
   # useradd -G support psmith
   ```

3. Set a password for the user using the `passwd` command.

   For example:

   ```
   # passwd psmith
   Changing password for user psmith.
   New password: new_password
   Retype new password: new_password
   passwd: all authentication tokens updated successfully
   ```

4. Run the `visudo` utility to edit the `/etc/sudoers` file.

   ```
   # visudo
   ```

   The `sudoers` file defines the policies that the `sudo` command applies.

5. Find the lines in the `sudoers` file that grant access to users in the wheel group when enabled.

   ```
   ## Allows people in group wheel to run all commands
   # %wheel        ALL=(ALL)       ALL
   ```

6. Remove the comment character (`#`) at the start of the second line, which begins with `%wheel`.

   This enables the configuration option.

7. Save your changes and exit the editor.

8. Add the user account that you created earlier to the `wheel` group using the `usermod` command.

   For example:

   ```
   usermod -aG wheel psmith
   ```

9. Test that the updated configuration enables the user that you created to run commands using `sudo`.

   a. Use the `su` command to switch to the new user account that you created.

      ```
      # su psmith
      ```

   b. Use the `groups` command to verify that the user is in the wheel group.

      ```
      $ groups
      psmith wheel
      ```

   c. Use the `sudo` command to run the `whoami` command.

      Because this is the first time that you have run a command using `sudo` from this user account, the banner message is displayed. You will be prompted to enter the password for the user account.

      ```
      $ sudo whoami
      ```

      The following output should appear:

      ```
      We trust you have received the usual lecture from the local System
      Administrator. It usually boils down to these three things:
      ```

```
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
```

Enter the password when prompted:

```
[sudo] password for psmith: password
root
```

The last line of the output is the user name that is returned by the `whoami` command. If `sudo` access has been configured correctly, then this value is `root`.

14.5 Managing User Access Rights to Targets and Groups

Learn about managing users access rights to targets and groups.

14.5.1 About Managing User Access Rights

Learn about managing user access rights.

Super administrators have access to all targets and target groups and can grant access to specific targets and groups to administrators.

You control access to targets or groups in two ways:

- Modify a 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 targets or groups.

14.5.2 Controlling Access Rights by User

Learn about controlling access rights by user.

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.

   Click the **Manage Admins** sub tab. It displays existing users and the targets or groups to which they have access.
3. Click the name of the user account you want to modify.

   The **Modify Admin** dialog appears.
4. In the **Targets & Target Groups** section:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Select the access rights to which you want to grant or revoke access. b. Click **Grant** or **Revoke** button. A green check mark indicates access granted. A red cross mark (X) indicates access revoked.	a. Select the access rights to which you want to grant or revoke access. You can also search for the access rights in the field under **Targets & Target Groups**. b. Choose the access rights in the **Available** column and move them to the **Selected** column, to grant access. Choose the access rights in the **Selected** column and move them to the **Available** column, to revoke access.

5. Click **Save**.

14.5.3 Controlling Access Rights by Targets or Group

You can control access rights by targets or groups.

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **Security** (which should be selected by default).
3. Under **Manage Admins** sub tab, select the name of the administrator whose target access you want to change.

   The **Modify Admin** window appears.
4. Click on the edit icon against **Type**. Select the appropriate type in the list.
5. In the **Targets & Target Groups** section:

Release Oracle AVDF 20.1 and 20.2	Release Oracle AVDF 20.3 and later
a. Select the target or target groups to which you want to grant or revoke access. b. Click **Grant** or **Revoke** button. A green check mark indicates access granted. A red cross mark (X) indicates access revoked.	a. Select the target or target groups to which you want to grant or revoke access. You can also search for the targets or groups in the field under **Targets & Target Groups**. b. Choose the target or target groups in the **Available** column and move them to the **Selected** column, to grant access. Choose the target or target groups in the **Selected** column and move them to the **Available** column, to revoke access.

6. Click **Save**.

14.6 Changing User Passwords in Oracle Audit Vault and Database Firewall

Learn how to manage password changes.

14.6.1 Password Requirements

There are several password requirements that you must meet for Oracle Audit Vault and Database Firewall.

You should have a policy in place for changing passwords for Oracle 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.

Requirements for Passwords Containing Unicode Characters

If your password contains unicode characters (such as non-English characters with accent marks), then the password requirement is that it:

- Be between 8 and 30 characters long.

Requirements for English-Only (ASCII) Passwords

If you are using English-only ASCII printable characters, then Oracle AVDF requires that passwords:

- Be between 8 and 30 characters long.
- Contain at least one of each of the following:
  - Lowercase letters: a-z.
  - Uppercase letters: A-Z.
  - Digits: 0-9.
  - Punctuation marks: comma (,), period (.), plus sign (+), colon(:), exclamation mark (!), and underscore (_)
- Not contain double quotes ("), back space, or control characters.

In addition, Oracle recommends that passwords:

- Not be the same as the user name.
- Not be an Oracle reserved word.
- Not be an obvious password (such as welcome, account, database, and user).
- Not contain any repeating characters.

14.6.2 Changing the Audit Vault Server Administrator Password

Learn how to change the password of an administrator.

Administrators can change their own password. A super administrator can also change the password of other administrators. If a super administrator changes the password of another administrator, then the password automatically expires immediately after it is changed.

14.6.2.1 Changing Your Own Password

Learn how to change your own password as an administrator.

1. Log in to the Audit Vault Server as an administrator.
2. In the upper right corner, to the right of your login name, select the menu icon.
3. Select **Change Password** from this menu.
4. In the **Change Password** window, enter the following fields:
   - **Current Password**
   - **New Password**
   - **Re-enter New Password**
5. Click **Save**.

Related Topics

- Password Requirements
  There are several password requirements that you must meet for Oracle Audit Vault and Database Firewall.

14.6.2.2 Changing the Password of Another Administrator

Learn how to change the password of another administrator as a super administrator.

A super administrator can change the passwords of other administrators. However, the password automatically expires immediately after it is changed by the super administrator. The administrator must follow the instructions in the topic Changing the Expired Password of an Administrator.

1. Log in to the Audit Vault Server as super administrator.
2. Click the **Settings** tab and then if necessary, select **Security** in the left navigational menu.
3. Under **Manage Admins**, select the name of the administrator whose password you want to change.
4. In the **Modify Admin** window, click **Change Password**.
5. In the **Change Password** window, enter the following fields:
   - **New Password**
   - **Re-enter New Password**
6. Click **Save**.

Related Topics

- Password Requirements
  There are several password requirements that you must meet for Oracle Audit Vault and Database Firewall.

14.6.2.3 Changing the Expired Password of an Administrator

Your password might be expired if a super administrator changes your password, or if it passes the password expiry date.

For Oracle AVDF release 20.4 or earlier, follow these steps:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `dvaccountmgr` user.

   ```
   su - dvaccountmgr
   ```
3. Start SQL*Plus without the user name and password.

   ```
   sqlplus /
   ```
4. If the account is locked, run the following command to unlock the account:

   ```
   alter user <user name> account unlock;
   ```
5. Run the following command to change the password:

   ```
   alter user <user name> identified by <new_password>;
   ```

For Oracle AVDF release 20.5 or later, follow these steps:

1. Log in to AVCLI with your user name.
2. AVCLI prompts to enter the password. Enter the expired password.

   The following message is displayed:

   ```
   The password has expired. Enter the new password:
   ```
3. Enter the new password of your choice. Follow the password requirements.

   The following message is displayed:

   ```
   Re-enter password:
   ```
4. Re-enter the new password.
5. If the following message is displayed, then you have successfully logged in to AVCLI with the new password, and your account is active again:

   ```
   Connected to:
           Oracle Audit Vault Server - Version : 20.x.0.0.0
   ```

> **Note:**
>
> If your attempt to log in fails for 3 times or more, then your account gets locked. You need to unlock your account and retry the above mentioned steps.

Related Topics

- Logging in to AVCLI
  You can log in to the Audit Vault command line interface by using different methods.
- Password Requirements
  There are several password requirements that you must meet for Oracle Audit Vault and Database Firewall.
- Unlocking User Accounts
  This procedure explains how to unlock user accounts.

14.7 Integrating Oracle Audit Vault and Database Firewall with Microsoft Active Directory or OpenLDAP

You can use Microsoft Active Directory or OpenLDAP to control access to Oracle Audit Vault and Database Firewall.

14.7.1 About Microsoft Active Directory or OpenLDAP Integration

You can integrate a Microsoft Active Directory or OpenLDAP server to authenticate users who connect to the Audit Vault Server console.

When users log in to the Audit Vault Server console, they're prompted to select a group from a list of groups. Users are authorized from the group to which they belong and select. After a user is authenticated, access is granted based on the Microsoft Active Directory or OpenLDAP groups to which the user belongs and selects.

A super user can assign the roles to the groups on Oracle Audit Vault Database Firewall. For example, super administrator, super auditor, administrator, or auditor. Oracle Audit Vault and Database Firewall release 20.1 and later supports Microsoft Active Directory and OpenLDAP.

> **Note:**
>
> - While other LDAP servers may work, they are not tested or certified with Oracle Audit Vault and Database Firewall release 20.1.
> - Oracle AVDF does not support the default local accounts of Microsoft Active Directory (for example administrator). Refer to Microsoft documentation for complete information on default local accounts in Active Directory.
> - Microsoft Active Directory and OpenLDAP users and groups must belong to the domain specified in the topic Configuring an LDAP Server.

14.7.2 Configuring an LDAP Server

You can configure an LDAP server to authenticate users by using Microsoft Active Directory or OpenLDAP.

Prerequisite: The LDAP user must have access to the Microsoft Active Directory or OpenLDAP groups that are being provisioned for access to Oracle AVDF.

1. Get the SSL/TLS certificate to connect to Microsoft Active Directory or OpenLDAP. This can be sourced from Microsoft Active Directory or OpenLDAP administrator. Using the command `certutil -ca.cert client.crt` is a common way to generate Active Directory client SSL/TLS certificate.
2. Copy the SSL/TLS certificate in Base64 encoding format.
3. Launch the Audit Vault Server console.
4. Log in to the console as a super administrator.
5. Click the **Settings** tab.
6. Click the **LDAP Configuration** tab (or **Active Directory/LDAP Configuration** tab starting with Oracle AVDF release 20.8) in the main page.
7. Click the **Add** button.
8. Enter the Microsoft Active Directory or OpenLDAP server details. In the **Active Directory/ LDAP Configuration** dialog, select either **Active Directory (AD)** or **LDAP** radio button.
9. Provide a new **Name** for the LDAP server.
10. Enter the AD/LDAP **Host Name / IP Address**.
11. Enter the **Port** number for the SSL/TLS connection.
12. Enter the **Active Directory/LDAP Username** and **Password**.

    The user must be able to retrieve all groups from the AD/LDAP server.
13. Enter the **Domain Name**. For example, `foobar.example.com`.
14. Provide the **AD/LDAP Server Certificate** (SSL/TLS) in Base64 encoding format that was sourced earlier in the initial step.
15. Enter a new password as the **Wallet Password for Storing Certificate**. This wallet stores the SSL/TLS certificate you provided for LDAP SSL/TLS connection earlier.

16. Enter the password again in **Re-enter Wallet Password** field.
17. Click **Test Connection** to verify the details. Fix any errors encountered and proceed to the next step.
18. Click **Save**.

> **Note:**
>
> Click **Delete** to delete the Microsoft Active Directory or OpenLDAP configuration. Starting Oracle AVDF 20.4, a dialog appears and prompts for your confirmation.

14.7.3 Creating New Users

Create new users for Microsoft Active Directory or OpenLDAP authentication.

1. Log in to the Audit Vault Server console as a *super administrator* or *super auditor*.
2. Click the **Settings** tab.
   The **Manage Admins** or **Manage Auditors** subtab on the main page is selected by default.
3. Click **Add** in the top, right corner.
4. In the **Add Admin** (or **Add Auditor**) dialog box, select **Active Directory/LDAP Group**.
5. For **Active Directory/LDAP Group**, select the **Import Mode**.
   OpenLDAP or Active Directory users and groups have to exist in the LDAP server before you can create the admin or auditor on the Audit Vault Server for the same.
6. If you have selected import mode as **Fetch**, then provide an LDAP **User Name** and **Password**. Alternatively, you can register an Microsoft Active Directory or OpenLDAP group in Oracle Audit Vault Database Firewall that corresponds to an existing group by providing the distinguished name. The LDAP user needs the correct access privileges to view all the groups that exist on the LDAP server.

   > **Note:**
   >
   > The user credentials are not stored. Therefore, each time that you choose the **Fetch** option, you must enter the credentials.

7. In the **Group Name Like** field, enter a keyword to search in order to fetch details from a group that has a similar name. Click **Fetch** at the bottom of the dialog. For example, enter `admin` keyword to fetch AD or OpenLDAP groups containing `admin` string in the group name.

> **Note:**
>
> A user can be added to a group. A group can have administrator or auditor privileges, but not both. For example, a group with the name *AdminAndAuditor* can have administrator privileges assigned. However, the same group cannot have auditor privileges. In case there is an attempt to add both the privileges, then it fails. The user *SpecialUser* can be part of both, the *Admin* group and the *Auditor* group. This user *SpecialUser* may choose to connect with *Admin* group as administrator, or with *Auditor* group as auditor.

8. Select the **Domain**.
9. Click the **Fetch** button at the bottom of the dialog. The values in the **Group** and **User Type** fields are populated.
10. Select the right **Group** from the drop down menu.
11. Select the **User Type** from the drop-down menu, such as, **Admin**, **Super Admin**, **Auditor**, or **Super Auditor**.
12. If you have selected the import mode as **Manual**, then enter the **Group Name** as distinguished name.
13. Click **Save**.

14.7.4 Logging In as an OpenLDAP or Microsoft Active Directory User

After OpenLDAP or Microsoft Active Directory is configured, users can log in to the Audit Vault Server console.

1. Open the Audit Vault Server console.
2. Select **Active Directory/LDAP Group**.
3. Enter the user name and password.

   For database users, enter the user name and password. For Microsoft Active Directory users, enter the user name (`sAMAccountName`) and password. Select the domain name from the drop-down list.

> **Note:**
>
> The domain name is appended to the user name. This may cause issues if a user has been created with a domain in the user name.
> For example, if you attempt to login as user `user@example.com` and select the domain `company.example.com`, then the Audit Vault Server will attempt to look for the user `user@example.com@company.example.com`.

> **Note:**
>
> You must add the user to the Microsoft Active Directory or OpenLDAP group and register the group with the Audit Vault Server. See Creating New Users.

4. On the following page, select a **Group** from the drop-down list.

5. Click **Save** to log in and complete the authorization.

> **Note:**
>
> Microsoft Active Directory and OpenLDAP users can connect to the Audit Vault Server only through the Audit Vault Server console. They cannot connect to the Audit Vault Server through AVCLI or SQL*Plus.

14.8 Configuring Single Sign-On (SSO) for Audit Vault Server Console Users

Starting in Oracle AVDF 20.11, you can configure SSO for Audit Vault Server console users.

14.8.1 About SSO for Audit Vault Server Console Users

The Audit Vault Server can integrate with an identity provider (IdP) through SAML 2.0 integration, and the IdP can provide single sign-on (SSO) and multifactor authentication (MFA) support. Audit Vault Server doesn't store the SSO user credentials except for the SSO user name.

You can configure SSO for all types of Audit Vault Server console users, including normal administrators and auditors, readonly auditors, and super administrators and super auditors.

To manage SSO configurations, you need to log in to the Audit Vault Server console as a `super administrator` that is configured as a local AVDF user. You can't create or change SSO configurations in an SSO session.

As always, you cannot drop the last super administrator and super auditor configured as local AVDF user.

14.8.2 Adding SSO Configurations

To configure single sign-on (SSO), add your identity provider (IdP) information to the Audit Vault Server.

> **Note:**
>
> You can add multiple SSO configurations, but only one configuration can be enabled at any time.

1. Log in to the Audit Vault Server console as a super administrator that's configured as a local AVDF user.
2. Click the **Settings** tab.
3. Click the **Single Sign-On (SSO)** subtab.
4. Enter the following information:

Field	Description
Identity Provider Name	A name to identify the IdP in the Audit Vault Server.
Provider Type	Identity provider type, such as the following: • **Microsoft Active Directory Federation Service** • **Microsoft Entra ID (MS-EI)** • **Oracle Access Manager (OAM)** **Note:** Oracle AVDF 20.11 only: Though OAM is a valid identity provider, there is no option to select it. Instead, select any other identify provider, but in the following fields enter in the information for OAM. **Note:** You can't change the provider type after you add an SSO configuration to the Audit Vault Server. To change the provider type, add a new SSO configuration with the new provider type.
Identity Provider Domain	Domain name for the IdP. For example: `login.example.com`
Protocol	The protocol is always **SAML 2.0**.
SSO Sign-in URL	URL that you use to sign in to the IdP. For example: `https://login.example.com/177306dd-a070-419a-b50f-6f71fc63b993/saml2`
SSO Sign-out URL	URL that you use to sign out of the IdP. For some providers, this might be the same as the sign-in URL. For example: `https://login.example.com/177306dd-a070-419a-b50f-6f71fc63b993/saml2`
Identity Provider Issuer	URI for the IdP. For example: `https://sts.example.net/177306dd-a070-419a-b50f-6f71fc63b993`
Identity Provider Signing Certificate	Certificate from the IdP in base-64 format. Either copy and paste the certificate or choose the file and upload it here.

5. Click **Save**.
6. If using Microsoft Azure Active Directory, you will need to include `https://<AVDF_IP>/ords/apex_authentication.saml_callback` in the **Identifier (Entity ID)**, **Reply URL**

(Assertion Consumer Service URL), and **Logout URL** fields when configuring Microsoft Azure Active Directory.

7. To begin using the SSO configuration, you need to enable it. See Enabling SSO Configurations.

14.8.3 Copying the Audit Vault Server SSO Certificate to the Identity Provider

Some identity providers require the Audit Vault Server single sign-on (SSO) certificate and you might need to copy the SSO certificate from the Audit Vault Server.

1. Log in to the Audit Vault Server console as a super administrator that's configured as a local AVDF user.
2. Click the **Settings** tab.
3. Click the **Single Sign-On (SSO)** subtab.
4. Click **Copy Certificate**.

   The SSO certificate is copied to the clipboard.

14.8.4 Enabling SSO Configurations

To begin using a single sign-on (SSO) configuration, you need to enable it in the Audit Vault Server.

> **Note:**
>
> You can add multiple SSO configurations, but only one configuration can be enabled at any time.

Prerequisites

- Add the SSO configuration if it's not already defined in the Audit Vault Server. See Adding SSO Configurations.
- If another SSO configuration is already enabled, you need to disable it in the Audit Vault Server before enabling another SSO configuration. See Disabling an SSO Configuration.

Procedure

1. Log in to the Audit Vault Server console as a super administrator that's configured as a local AVDF user.
2. Click the **Settings** tab.
3. Click the **Single Sign-On (SSO)** subtab.
4. Select the SSO configuration that you want to enable.
5. Click **Enable**.

14.8.5 Configuring ORDS After Enabling Oracle Access Manager as the SSO Identity Provider

After enabling Oracle Access Manager (OAM) as the SSO identity provider, you will need to configure Oracle Rest Data Services (ORDS).

Prerequisites

- Enable the SSO configuration. See Enabling SSO Configurations.
- Take note of:
  - The fully qualified host name (FQHN) of the Audit Vault Server
  - The FQHN of the OAM server
  - The FQHN of the LDAP server

Procedure

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `oracle` user.

   ```
   su - oracle
   ```
3. Set the `JAVA_PATH` variable:

   ```
   export JAVA_PATH=/usr/java/jdk-11/bin
   ```
4. Set the `PATH` variable:

   ```
   export PATH=$JAVA_PATH:/var/lib/oracle/ords/bin:$PATH
   ```
5. Set the following configuration:

   ```
   ords --config /var/lib/oracle/ords_conf config set --global
   security.forceHTTPS true
   ```
6. Set the following configuration through either of the following:
   - Ensure that you input the appropriate FQHN's where necessary.

     ```
     ords --config /var/lib/oracle/ords_conf config set --global
     security.externalSessionTrustedOrigins "https://<FQHN of AV
     server>:443, http://<FQHN of OAM server>:<port>, https://<FQHN LDAP
     server configured on OAM server>:<port>, null"
     ```
   - You can alternatively use the following since the parameters in the above are optional:

     ```
     ords --config /var/lib/oracle/ords_conf config set --global
     security.externalSessionTrustedOrigins "null"
     ```
7. Exit back to `root`.

8. Restart ORDS:

```
systemctl restart ords
```

9. Test the connection by creating a new OAM user and logging into the Audit Vault Server console as that OAM user.
See Creating New SSO Users and Logging In to the Audit Vault Server Console as an SSO User for more information.
10. If configured in high availability, repeat the above steps on the standby Audit Vault Server.

14.8.6 Creating New SSO Users

To create new users for single sign-on (SSO) authentication, follow these steps.

Prerequisite

Ensure the SSO is enabled for users on the identity provider.

Procedure

1. Log in to the Audit Vault Server console as a `super administrator`.
2. Click the **Settings** tab.
3. On the **Manage Admins** subtab, click **Add**.
4. In the dialog box, select **SAML SSO**.
5. Enter the SSO user name.

   Allowed characters include uppercase and lowercase letters, numbers, and symbols (@.-_!^~+%). The total length of the SSO user name can't exceed 127 characters.

   > **Note:**
   >
   > Though AVDF accepts uppercase and lowercase letters, it will store the user name in only uppercase. The identity providers perform a case in-sensitive comparison of the user names.

6. Select the admin type, **Admin** or **Super Admin**.
7. Click **Save**.

14.8.7 Logging In to the Audit Vault Server Console as an SSO User

When you log in to the Audit Vault Server console as a single sign-on (SSO) user, you're redirected to the enabled identity provider (IdP) SSO login page.

1. On the Audit Vault Server console login page, select **Single Sign-On**.
2. Click **Login**.
3. Enter your SSO user name and password on the SSO login page.

> **Note:**
>
> Log out and close your browser at the end of the session. Otherwise, your browser will still be logged in as your SSO user and will allow access to the Audit Vault Server.

14.8.8 Modifying SSO Users

You can change the admin type for an existing single sign-on (SSO) user.

1. Log in to the Audit Vault Server console as a `super administrator`.
2. Click the **Settings** tab.
3. On the **Manage Admins** subtab, click the user that you want to modify.
4. Click the Change icon next to the **Type** field.
5. Select a new admin type.
6. Click **Save**.

14.8.9 Disabling an SSO Configuration

You might need to disable a single sign-on (SSO) configuration if you want to modify, delete, or switch to another SSO configuration.

1. Log in to the Audit Vault Server console as a super administrator that's configured as a local AVDF user.
2. Click the **Settings** tab.
3. Click the **Single Sign-On (SSO)** subtab.
4. Select the SSO configuration that you want to disable.
5. Click **Disable**.

   You should see the following message:

   ```
   Do you want to continue to disable this identity provider?
   ```
6. Click **OK** to disable the configuration.

14.8.10 Configuring ORDS After Disabling Oracle Access Manager as the SSO Identity Provider

After disabling Oracle Access Manager (OAM) as the SSO identity provider, you will also need to configure Oracle Rest Data Services (ORDS).

Prerequisites

- Disable the SSO configuration. See Disabling an SSO Configuration.

Procedure

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

```
su - oracle
```

3. Set the `JAVA_PATH` variable:

```
export JAVA_PATH=/usr/java/jdk-11/bin
```

4. Set the `PATH` variable:

```
export PATH=$JAVA_PATH:/var/lib/oracle/ords/bin:$PATH
```

5. Execute the following command:

```
ords --config /var/lib/oracle/ords_conf config delete --global
security.forceHTTPS true
```

6. Execute the following command:

```
ords --config /var/lib/oracle/ords_conf config delete --global
security.externalSessionTrustedOrigins true
```

7. Exit back to `root`.
8. Restart ORDS:

```
systemctl restart ords
```

9. If configured in high availability, optionally repeat the above steps on the standby Audit Vault Server.

14.8.11 Modifying an SSO Configuration

You can modify a single sign-on (SSO) configuration if it's disabled in the Audit Vault Server.

> **Note:**
>
> You can't change the provider type after you add an SSO configuration to the Audit Vault Server. To change the provider type, add a new SSO configuration with the new provider type.

Prerequisite

Disable the SSO configuration if it's currently enabled in the Audit Vault Server. See Disabling an SSO Configuration.

Procedure

1. Log in to the Audit Vault Server console as a super administrator that's configured as a local AVDF user.
2. Click the **Settings** tab.
3. Click the **Single Sign-On (SSO)** subtab.

4. Update any of the following information:

Field	Description
Identity Provider Name	A name to identify the IdP in the Audit Vault Server.
Provider Type	Identity provider type, such as the following: • **Microsoft Active Directory Federation Service** • **Microsoft Entra ID (MS-EI)** • **Oracle Access Manager (OAM)** **Note:** Oracle AVDF 20.11 only: Though OAM is a valid identity provider, there is no option to select it. Instead, select any other identify provider, but in the following fields enter in the information for OAM. **Note:** You can't change the provider type after you add an SSO configuration to the Audit Vault Server. To change the provider type, add a new SSO configuration with the new provider type.
Identity Provider Domain	Domain name for the IdP. For example: `login.example.com`
Protocol	The protocol is always **SAML 2.0**.
SSO Sign-in URL	URL that you use to sign in to the IdP. For example: `https://login.example.com/177306dd-a070-419a-b50f-6f71fc63b993/saml2`
SSO Sign-out URL	URL that you use to sign out of the IdP. For some providers, this might be the same as the sign-in URL. For example: `https://login.example.com/177306dd-a070-419a-b50f-6f71fc63b993/saml2`
Identity Provider Issuer	URI for the IdP. For example: `https://sts.example.net/177306dd-a070-419a-b50f-6f71fc63b993`
Identity Provider Signing Certificate	Certificate from the IdP in base-64 format. Either copy and paste the certificate or choose the file and upload it here.

5. Click **Save**.

14.8.12 Deleting an SSO Configuration

You can delete a single sign-on (SSO) configuration if it's disabled in the Audit Vault Server.

Prerequisite

Disable the SSO configuration if it's currently enabled in the Audit Vault Server. See Disabling an SSO Configuration.

Procedure

1. Log in to the Audit Vault Server console as a super administrator that's configured as a local AVDF user.
2. Click the **Settings** tab.
3. Click the **Single Sign-On (SSO)** subtab.
4. Select the SSO configuration that you want to delete.
5. Click **Delete**.

   After deleting the SSO configuration, existing sessions will receive the following message when logging out:

   ```
   Invalid value for parameter: SAML_SIGN_IN_URL
   ```

14.9 Unlocking and Locking the AVSYS User

When installing or administering Oracle Audit Vault and Database Firewall (Oracle AVDF), you sometimes need to unlock and relock the `AVSYS` user.

14.9.1 Unlocking the AVSYS User

Use these steps to temporarily unlock the `AVSYS` user to complete an installation or administration task.

Prerequisite

Log in to the Audit Vault Server through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

Procedure

1. Switch to the `dvaccountmgr` user.

   ```
   su - dvaccountmgr
   ```

2. Start SQL*Plus without the user name and password.

   ```
   sqlplus /
   ```

3. Run the following command to unlock `avsys`:

   ```
   alter user avsys identified by <password> account unlock;
   ```

4. Exit SQL*Plus.

```
exit
```

14.9.2 Locking the AVSYS User

Use these steps to lock the AVSYS user after you've unlocked it to complete an installation or administration task.

Prerequisite

Log in to the Audit Vault Server through SSH and switch to the root user.

See Logging In to Oracle AVDF Appliances Through SSH.

Procedure

1. Switch to the dvaccountmgr user.

```
su - dvaccountmgr
```

2. Start SQL*Plus without the user name and password.

```
sqlplus /
```

3. Run the following command to lock avsys:

```
alter user avsys account lock;
```

4. Exit SQL*Plus.

```
exit
```

14.10 Updating the Passwords for the AGENTUSR# and AVSRCUSR# Accounts

Though updating the passwords of the AGENTUSR# or AVSRCUSR# database accounts is not recommended, in rare situations, it may be necessary.

To update the AGENTUSR# password

1. Deactivate the Audit Vault Agents for which the password needs to be updated. See Deactivating and Removing the Audit Vault Agent
2. Activate all the Audit Vault Agents that were deactivated. See Activating and Starting the Audit Vault Agent
   Be sure to redeploy the Audit Vault Agent using new activation key that is displayed on the Audit Vault Server console.

To update the AVSRCUSR# password

1. Stop all audit trails. See Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server.

2. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

3. For all the accounts that need their passwords updated:

   ```
   alter user <user_name> identified by <password>;
   ```

4. Lock the `avsys` user.

   See Locking the AVSYS User.

5. Start all audit trails. See Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server

14.11 Rotate the AVREPORTUSER Password

- Oracle AVDF 20.13 and later
- Oracle AVDF 20.1-20.12

Oracle AVDF 20.13 and later

Starting in Oracle AVDF 20.13, the password for the `AVREPORTUSER` user will automatically rotate every 60 days under normal circumstances. More specifically, the password for the `AVREPORTUSER` user will expire after 90 days, but there is a daily check that will automatically rotate the password if there are less than 30 days until the expiration date, i.e. the password will automatically rotate every 60 days. However, if there are repeated technical issues and the password can't be automatically rotated at any point from days 60-90, then the password can be manually rotated using the following steps.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the following command:

   ```
   /usr/bin/python3/usr/local/dbfw/lib/python/avs/scripts/
   update_avreportuser_user_password.py -FORCE
   ```

3. Force the rotation of the `AVREPORTUSER` user's password.

   ```
   -FORCE
   ```

Oracle AVDF 20.1-20.12

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Unlock the `avsys` and `avreportuser` account.
   a. Switch to the `dvaccountmgr` user.

      ```
      su - dvaccountmgr
      ```

   b. Start SQL*Plus without the user name and password.

      ```
      sqlplus /
      ```

   c. Run the following command to unlock `avsys` and `avreportuser` and alter the password:

      ```
      alter user avsys identified by <avsys_password> account unlock;
      alter user avreportuser identified by <avreportuser_new_password>
      account unlock;
      ```

   d. Exit SQL*Plus.

      ```
      exit
      ```

   > **Note:**
   >
   > Remember to relock the `avsys` and `avreportuser` accounts when you've completed this task.

3. Switch to the `oracle` user.

   ```
   su - oracle
   ```

4. Execute the following command with the new password for the `avreportuser` account:

   ```
   /var/lib/oracle/dbfw/bin/avca create_credential -wrl $ORACLE_HOME/network/
   admin/avwallet -dbalias AV_AUDITOR_USER
   ```

   a. Follow the prompt to enter `avreportuser` for `source user name`.
   b. Provide the new `avreportuser` password `<avreportuser_new_password>` twice.

5. Drop the existing database link `avrptusr_link.dbfwdb` as `oracle` user through SQL*Plus:

   ```
   sqlplus avsys/<avsys_password>
   drop database link avrptusr_link.dbfwdb;
   exit
   ```

6. Recreate the `avrptusr_link.dbfwdb` database link as `oracle` user:

   ```
   /var/lib/oracle/dbfw/bin/avca create_report_user_dblink
   ```

7. Lock the `avsys` user.

   See Locking the AVSYS User.

8. Log in to the Audit Vault Server through SSH and switch to the `root` user.

See Logging In to Oracle AVDF Appliances Through SSH.

9. Switch to the `oracle` user.

```
su - oracle
```

10. Run the following command:

```
/usr/local/dbfw/bin/javafwk restart
```

14.12 Rotating the `ORDS_PUBLIC_USER` User Password

Oracle AVDF 20.13 and later

Starting in Oracle AVDF 20.13, the password for the `ORDS_PUBLIC_USER` user will automatically rotate every 60 days under normal circumstances. More specifically, the password for the `ORDS_PUBLIC_USER` user will expire after 90 days, but there is a daily check that will automatically rotate the password if there are less than 30 days until the expiration date, i.e. the password will automatically rotate every 60 days. However, if there are repeated technical issues and the password can't be automatically rotated at any point from days 60-90, then the password can be manually rotated using the following steps.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run the following command:

```
/usr/bin/python3/usr/local/dbfw/lib/python/avs/scripts/
update_ords_public_user_user_password.py
```

3. Force the rotation of the `ORDS_PUBLIC_USER` user's password.

```
-FORCE
```

Oracle AVDF 20.9 - 20.12

1. Unlock the `ORDS_PUBLIC_USER` user:
   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.

   b. Switch to the `dvaccountmgr` user.

```
su - dvaccountmgr
```

c. Start SQL*Plus without the user name and password.

```
sqlplus /
```

d. Run the following command to unlock `ORDS_PUBLIC_USER`:

```
alter user ORDS_PUBLIC_USER identified by new_password account unlock;
```

e. Exit SQL*Plus.

```
exit
```

2. Update the password in the wallet file

a. Switch to the `root` user.

```
su - root
```

> **Note:**
> If you're using the OCI marketplace image, use the `sudo su -` command.

b. Switch to the `oracle` user.

```
su - oracle
```

c. Set the `JAVA_PATH` and `PATH` variables:

```
 JAVA_PATH=/usr/java/jdk-11/bin
export PATH=/var/lib/oracle/ords/bin:$PATH
export PATH=$JAVA_PATH:$PATH
```

d. Open the wallet file and update the password when prompted:

```
ords --config /var/lib/oracle/ords_conf config secret db.password
```

3. Restart ORDS

a. Switch to the `root` user.

```
su - root
```

> **Note:**
> If you're using the OCI marketplace image, use the `sudo su -` command.

b. Run the following command:

```
systemctl stop ords
```

c. Run the following command:

```
systemctl start ords
```

Oracle AVDF 20.6 - 20.8

1. Unlock the `ORDS_PUBLIC_USER` user:
   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.
   b. Switch to the `dvaccountmgr` user.

      ```
      su - dvaccountmgr
      ```
   c. Start SQL*Plus without the user name and password.

      ```
      sqlplus /
      ```
   d. Run the following command to unlock `ORDS_PUBLIC_USER`:

      ```
      alter user ORDS_PUBLIC_USER identified by new_password account unlock;
      ```
   e. Exit SQL*Plus.

      ```
      exit
      ```
2. Update the `apex.xml` file with the new `ORDS_PUBLIC_USER` password:
   a. Change directories to where the `apex.xml` file is located:

      ```
      cd var/lib/oracle/ords/conf/ords/conf
      ```
   b. Open the `apex.xml` file for editing:

      ```
      vi apex.xml
      ```
   c. Update the password. Make sure to put a `!` before the password:

      ```
      <entry key="db.password">!new_password</entry>
      ```
   d. Save changes and exit editting:

      ```
      :wq!
      ```
3. Restart ORDS
   a. Switch to the `root` user.

      ```
      su - root
      ```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

b. Run the following command:

```
systemctl stop ords
```

c. Run the following command:

```
systemctl start ords
```

15

Managing the Audit Vault Server and Database Firewalls

Learn how to manage day-to-day Audit Vault Server and Database Firewall operations after the initial configuration is completed.

15.1 Managing Audit Vault Server Settings, Status, and Maintenance Operations

Learn how to manage the Audit Vault Server settings, status, and maintenance operations.

15.1.1 Checking Server Status and System Operation

This procedure enables you to check the server status and system operation.

1. Log in to the Audit Vault Server as an administrator.
2. Use one of the following methods to find the system status:
   - Select the **Home** tab. The page displays overall system status information (some of which you can drill down into) for Agents, Audit Trails, Targets, Disk Space, Database Firewalls, and CPU Usage.
   - Select the **Settings** tab, and then in the left navigational menu, select **System**. The status page displays detailed information for areas such as the overall server status, configuration status, and monitoring status.

15.1.2 Managing Diagnostics

You can generate diagnostic reports to find the source of errors, warnings, and other issues in Audit Vault and Database Firewall.

15.1.2.1 About Managing Diagnostics

You can run diagnostic tools to help you debug problems that may arise.

You can adjust the amount of diagnostics information gathered by setting the `LOGLEVEL` for different server components using the `AVCLI ALTER SYSTEM SET` command. When you perform the download operation, the process captures the log and trace file information, along with configuration information that is available at that time. Be aware that a change in the log level only affects those trace or log files that are generated after the change is made. For example, if you encounter a problem after you set the log level to `DEBUG`, then you must reproduce the issue before you run the procedure in this section to download the diagnostic report. Otherwise, the debug or trace is not captured in the report.

Be aware, however, that the `DEBUG` setting will generate many files, which can affect the performance of your system. Therefore, only use this setting on a temporary basis, when you are trying to diagnose problems. After you find and correct the problem, then set `DEBUG` to the original setting, such as `ERROR`.

Logging Levels

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

- **Error**: Reports only critical information. This generates the least amount of log messages.
- **Warning**: (Default) Reports warning and error messages (not supported for Web Console UI).
- **Info**: Writes informational, warning, and error messages. This level is appropriate for testing environments but not for production.
- **Debug**: Writes detailed messages for debugging purposes. This generates the most amount of log messages. Debug logs may contain sensitive information about the state of your system. Add the debug log level only when necessary, and remove it once debugging is complete.

System Components

You can set different logging levels for these system components:

Table 15-1 Components with Variable Logging Levels

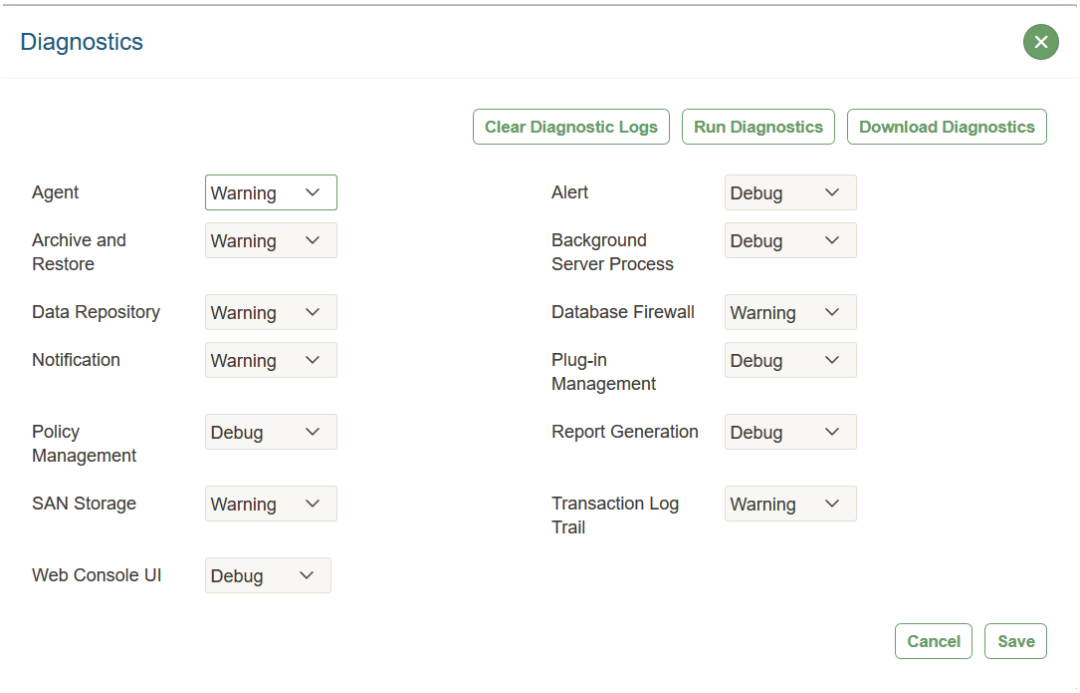
Agent	Alert
Archive and Retrieve	**Background Server Process**
Data Repository	**Database Firewall**
Notification	**Plug-in Management**
Policy Management	**Report Generation**
SAN Storage	**Transaction Log Trail**
Web Console UI (has three logging levels only)	N/A

15.1.2.2 Running Diagnostics Checks for the Audit Vault Server

Follow this procedure to run diagnostics checks for Oracle Audit Vault Server.

You can run a diagnostics check for the Audit Vault Server that tracks activities such as whether necessary files exist, whether the HTTP server is running, whether the Oracle listener and other processes are running.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, click the **System** tab.
4. Under **Monitoring** section, click the **Diagnostics** link. The **Diagnostics** dialog is displayed as follows:



5. In the **Diagnostics** dialog, do one of the following:
   - Set the diagnostic category that you want to use for diagnostic (for example, for Agent, selecting Warning), and then click **Save**.
   - Set the diagnostic categories that you want, and then click **Run Diagnostics**. A second window **Test Diagnostics** appears listing the diagnostics as they are being captured.
   - To download the diagnostics report, click **Download Diagnostics**. A diagnostics log file (`.zip`) is downloaded to the location that you select. Be aware that the diagnostics zip file may contain sensitive data from your appliance. Take appropriate precautions when you transfer and store this file.
   - Click **Clear Diagnostic Logs** to clear the current set of diagnostic logs on the Audit Vault Server.

15.1.2.3 Downloading Detailed Diagnostics Reports for Oracle Audit Vault Server

You can download diagnostics reports for Oracle Audit Vault Server to review activity and to assess other operations.

To download zip 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 **Diagnostics**.
3. Click the **Download Diagnostics** button.

   A download window appears for the diagnostics zip file.
4. Select a file location and then click **Save**.

> **See Also:**
>
> - ALTER SYSTEM SET for details about setting the `LOGLEVEL` parameter.

15.1.2.4 Clearing Diagnostic Logs

Follow this process to empty your Oracle Audit Vault and Database Firewall diagnostic logs.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **System**.
4. Under Monitoring, click **Diagnostics**.
5. In the Diagnostics window, click **Clear Diagnostic Logs**, then in the confirmation window, click **OK**.

15.1.3 Accessing the Audit Vault Server Certificate and Public Key

You can use the Audit Vault Server console to access the Audit Vault server certificate and public key.

15.1.3.1 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.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **Security**.
4. In the status page, click **Certificate**.

   The server's certificate is displayed. You can copy the certificate and provide it to each Database Firewall.
5. In the **Security** menu, click **Certificate**.

Related Topics

- Specifying the Audit Vault Server Certificate and IP Address
  You associate each Database Firewall with an Audit Vault Server so that the Audit Vault Server can manage the firewall. If you're using a resilient pair of Audit Vault Servers for high availability, then you associate the firewall with both servers.

15.1.3.2 Accessing the Server Public Key

You can access the Audit Vault Server public key from the Manage Archive Locations area.

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 `0600`, or even `0400`.

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

2. Click the **Settings** tab.
3. In the left navigation menu, select **Archiving**.
4. In the page that appears, click **Manage Archive Locations**, and then click **Create**.
5. In the Create Archive Location window, in the **Public Key** field, copy this key and past it into the appropriate file on another system.

15.1.4 Changing the Keyboard Layout

You can change the keyboard layout for Audit Vault and Database Firewall depending your geographic location.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **System**.
4. In the page that appears, under Configuration, select **Manage**.
5. In the Manage window, select the keyboard you want from the **Keyboard** menu.
6. Click **Save**.
7. In the confirmation dialog box, select **OK**.

   You may be logged out if your selection affects the server's time changes significantly.

15.1.5 Restarting or Powering Off the Audit Vault Server

You must be a super administrator to restart or power off the Audit Vault Server.

1. Log in to the Audit Vault Server as super administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **System**.
4. Under Configuration, select **Manage**.
5. In the Manage window, click **Reboot** or **Power Off**.

15.2 Changing Oracle Audit Vault Server Network and Services Configurations

Use this procedure to change Oracle Audit Vault Server network and services configurations.

To set or change the network or services configuration, follow the relevant procedure below:

- "Changing the Primary Audit Vault Server Network Configuration"
- "Configuring or Changing the Audit Vault Server Services"

15.3 Managing Server Connectors for Email and Syslog

Follow this procedure to manage server connectors for email and syslog.

To set or change connector information, follow the relevant procedure below:

- Configuring the Email Notification Service

- Configuring Audit Vault Server Syslog Destinations

15.4 Configuring Remote Syslog Over TLS

Use this procedure to configure remote syslog over TLS.

Syslog provides a convenient mechanism to transfer logs from one device to another. The logs contain sensitive information. Therefore, it is important that you secure the logs during transfers. Do this by authenticating and encrypting the connection beween the client and the server. The remote feature in the syslog supports this functionality. Use this procedure to establish secure communications between the syslog clients and servers.

Prerequisites

- Ensure that the normal or unencrypted remote syslog functionality works using TCP.
- Complete the server side configuration. Load the `imtcp` module and specify the listener port.
- Complete the client side configuration. Specify the remote machine to which the logs are sent.
- Upon completion of the server side and client side configuration. Restart the syslog service.
- Restart the syslog service in case any of the devices were added, modified, or activated.
- Ensure the logs from the client are listed in the log file of the server. This is a confirmation and you can proceed to securing the communication channel.

To load the `imtcp` module and to specify the listener port, modify the `/etc/rsyslog.conf` file as follows:

```
# listen for tcp input
$ModLoad imtcp
# listening on port <port number>
$InputTCPServerRun <port number>
# Remote logs written to /var/log/messages.
*.* /var/log/messages
```

To specify the destination remote machine to which the logs will be sent, modify the `/etc/rsyslog.conf` file as follows:

```
# Forward messages to remotehost:port
*.* @@<Ip address of the remote host>:<port number>
```

Syslog contains modules, protective transport layer, and digital certificates to ensure mutual authentication. It covers many aspects. The syslog messages are encrypted in transit. The syslog sender authenticates to the syslog receiver. The receiver is able to identify and in return authenticates to the syslog sender. The receiver performs few checks to validate if it is the valid recipient of the messages. This kind of mutual authentication and hand shake prevents any kind of attacks.

The syslog mutual authentication system makes use of CA certificate and peer certificates. In case there is no signed certificate available, the user can create a self signed certificate using OpenSSL. The server must have the CA (certificate authority) certificate and it’s own digital

certificate. These certificates enable SSL operation that provides the necessary crypto keys used to secure the connection.

Syslog makes use of GTLS module as the network stream driver. Syslog has TLS protected transport security feature and ensures messages are encrypted. It makes use of digital certificates to ensure mutual authentication.

Configuring the server

The server configuration involves specifying the location of the certificates, the GTLS driver to be used, and starting of the listener. The following example is applicable to Linux based remote server only. It is different for other platforms. To make any changes to the server's syslog configuration, refer to the documentation of the specific syslog server. Modify the `/etc/rsyslog.conf` file as follows:

```
# listen for tcp input
$ModLoad imtcp
# make gtls driver the default
$DefaultNetstreamDriver gtls
# certificate files
$DefaultNetstreamDriverCAFile /path/to/cacert.pem
$DefaultNetstreamDriverCertFile /path/to/servercert.pem
$DefaultNetstreamDriverKeyFile /path/to/serverkey.pem
# Auth mode and permitted peers
$InputTCPServerStreamDriverAuthMode x509/name
$InputTCPServerStreamDriverPermittedPeer <permittedHost>
$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
# Listening on port <port number>
$InputTCPServerRun <port number>
# Generic log file watching
$WorkDirectory /var/cache/rsyslog
# Remote logs
*.* /var/log/messages
```

Configuring the client

Syslog sends messages to a remote system from the client (Audit Vault Server or the Database Firewall). The client configuration involves specifying the location of the certificates, the GTLS driver to be used, and specifying the destination of the messages. Modify the `/etc/rsyslog.conf` as follows:

```
# make gtls driver the default
$DefaultNetstreamDriver gtls
# certificate files
$DefaultNetstreamDriverCAFile /usr/local/dbfw/syslog/certs/cacert.pem
$DefaultNetstreamDriverCertFile /usr/local/dbfw/syslog/certs/clientcert.pem
$DefaultNetstreamDriverKeyFile /usr/local/dbfw/syslog/certs/clientkey.pem
# Auth modes and permitted peers
$ActionSendStreamDriverAuthMode x509/name
$ActionSendStreamDriverPermittedPeer avs08002719479d
$ActionSendStreamDriverMode 1 # run driver in TLS-only mode
# Send to remote system
*.* @@<Ip address>:<port number>
```

> **Note:**
>
> The `rsylog.conf` is generated from the template file:
>
> `/usr/local/dbfw/templates/template-rsyslog-conf`
>
> The client settings must also be made to the template file. Any changes made to this template is persistent and preserved even after the reboot of the appliance.

Creating and Using SSL Certificates

1. Execute the following command to create CA certificates:

   ```
   openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem -days 365 -
   config openssl.cnf
   ```

2. Execute the following commands to create server certificates using the CA certificate:

   ```
   openssl req -nodes -new -x509 -keyout serverkey.pem -out serverreq.pem -days
   365 -config openssl.cnf

   openssl x509 -x509toreq -in serverreq.pem -signkey serverkey.pem -out tmp.pem

   openssl ca -config openssl.cnf -policy policy_anything -out servercert.pem -
   infiles tmp.pem
   ```

3. Execute the following commands to create client certificates using CA certificate:

   ```
   openssl req -nodes -new -x509 -keyout clientkey.pem -out clientreq.pem -days
   365 -config openssl.cnf

   openssl x509 -x509toreq -in clientreq.pem -signkey clientkey.pem -out tmp.pem

   openssl ca -config openssl.cnf -policy policy_anything -out clientcert.pem -
   infiles tmp.pem
   ```

4. Transfer the following certificates to the specific location on the log server.

   `cacerts.pem,servercert.pem,serverkey.pem`

5. Transfer the following certificates to the specific location on the client.

   `cacerts.pem,clientcert.pem,clientkey.pem`

15.5 Archiving and Retrieving Audit Data

Learn how to archive and retrieve audit data.

15.5.1 Enabling Automatic Archival

Oracle Audit Vault and Database Firewall 20.1 supports automatic archival to an NFS configured location.

When the online period of the data on the tablespace expires, it is automatically archived without user's intervention. The data is removed from the online location and is available in the archive location. The data cannot be deleted online manually.

Oracle recommends enabling Automatic Remote Archiving. To enable it, you must configure at least one NFS archive location.

- Oracle AVDF Release 20.1-20.8
- Oracle AVDF Release 20.9 and later

Oracle AVDF Release 20.1-20.8

1. Configure a list of NFS archive locations. Ensure that NFS is configured on the Audit Vault Server as the archive location.
2. Log in to the Audit Vault Server console as an administrator.
3. Click **Settings** tab.
4. In the left navigation menu, select **Archiving**.
5. On the main page, click **Data Retention**.
6. Click **Enable** button, against **Auto Archive Status**.

Oracle AVDF Release 20.9 and later

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Data Retention** tab.
3. Click **Remote Archiving** in the left navigation menu.
4. Click **Enable** Automatic Remote Archiving at the top.

Related Topics

- About Archiving and Retrieving Data in Oracle Audit Vault and Database Firewall
  Learn about archiving and retrieving data in Oracle Audit Vault and Database Firewall.
- Defining Archive Locations
  You need to 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.
- REGISTER REMOTE FILESYSTEM
  Use the `REGISTER REMOTE FILESYSTEM` command to register remote file systems with Oracle Audit Vault Server.
- ORA-12660 Error While Registering Target
  Learn how to resolve the ORA-12660 error.

15.5.2 Starting an Archive Job Manually

To start an archive job, you must have configured at least one archive location.

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. Else copying the data file may fail. Transferring large files using SCP or SMB may take long.

You can register a remote file system by using the `AVCLI` command `REGISTER_REMOTE_FILESYSTEM`.

Oracle AVDF Release 20.1-20.8

1. Log in to the Audit Vault Server console as an administrator.
2. Click **Settings** tab.
3. In the left navigation menu, select **Archiving**.
4. On the main page, click **Data Retention**.
5. Under **Job Name**, enter a name for the archive job.
6. Under **Archive Location**, select the archive location from the list.
7. From the list, select the files you want to archive. The files listed are those for which the *Months Online* period has expired according to the target's retention policy.
8. Click **Archive**.

> **Tip:**
>
> If the archive job fails and you receive error OAV-46599, check your RMAN configuration as autobackup in the controlfile should be set to off.
>
> ```
> rman /RMAN> configure controlfile autobackup off;
> ```

Oracle AVDF Release 20.9 and later

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Data Status** tab.
3. Click **Remote Archiving** in the left navigation menu.
4. Click the **Archived Data** tab.
5. Select one or more archived data files from the list by clicking the box to the right of the target name.
6. Click **Move to Remote**.
7. In the dialog box that appears enter the job name.
8. Select a remote archive location from the drop down list. The selected archived data files will be moved to the remote archive location selection.
9. Click **Save**.

> **Tip:**
>
> If the archive job fails and you receive error OAV-46599, check your RMAN configuration as autobackup in the controlfile should be set to off.
>
> ```
> rman /RMAN> configure controlfile autobackup off;
> ```

Related Topics

- REGISTER REMOTE FILESYSTEM
  Use the `REGISTER REMOTE FILESYSTEM` command to register remote file systems with Oracle Audit Vault Server.
- 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 targets.
- Defining Archive Locations
  You need to 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.
- About Archiving and Retrieving Data in Oracle Audit Vault and Database Firewall
  Learn about archiving and retrieving data in Oracle Audit Vault and Database Firewall.

15.5.3 Retrieving Oracle Audit Vault and Database Firewall Audit Data

You can retrieve data files for a specific target and time range.

The **Months Archived** value in a targets retention (archiving) policy determines how long the target's data is available to retrieve to the Audit Vault Server. When the Months Archived period expires, the data is no longer available to retrieve, however, it continues to reside in the archive location.

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and from the left navigation menu, click **Archiving**.
3. Select **Retrieve** sub tab on the main page.
4. Under **Retrieve Request**, enter the following:
   - **Target** menu: Select the target.
   - **Start Date** field: Enter the start date, optionally using the date icon to select from a calendar. The start and end dates are associated with the event time (the time the event occurred).
   - **End Date** field: Enter the end date, optionally using the date icon to select from a calendar.
5. Click the **Retrieve** button.

Note:

- You can check the status of the retrieve job in the **Jobs** dialog that can be accessed from the **System** tab in the left navigation menu.
- When the retrieved data files are available, they are listed in the **Retrieved Datafiles** section of the **Retrieve** tab, and the data will be visible in reports.
- Starting Oracle AVDF 20.4, the datafiles archived in NFS locations are deleted from the location after the retrieve job completes.

6. To purge retrieved files when no longer needed, from the **Retrieved Datafiles** section. 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.
7. After the retrieved data files are released, they are now eligible to be archived again. If they are not needed anytime soon, then they should be archived to release disk space to the system.

Note:

Alternately, you can view or get the tablespaces archived by following these steps:

a. Connect to the primary Audit Vault Server using *SSH*.
b. Connect to *SQL*Plus* as administrator.
c. Run the following commands:

```
set linesize 100


column TABLESPACE_NAME format a30


column EVENT_MONTH format a15


SELECT * FROM
TABLE(avsys.ilm.get_target_eventmonth_for_tablespaces);
```

d. The above query displays the results with `TABLESPACE_NAME`, `SECURED_TARGET_ID` and `EVENT_MONTH` indicating the month for which the data is stored for the respective target ID for each tablespace. This information can be used to retrieve data.

Related Topics

- About Archiving and Retrieving Data in Oracle Audit Vault and Database Firewall
  Learn about archiving and retrieving data in Oracle Audit Vault and Database Firewall.
- Creating Archive and Retention Policies
  You can create retention policies (also called archive policies) that an Oracle Audit Vault and Database Firewall (Oracle AVDF) auditor can apply to targets.

15.6 Managing Repository Encryption

Managing the repository encryption key includes tasks such as rotating the master encryption key or changing the keystore password.

15.6.1 About Oracle Audit Vault Server Repository Encryption

Learn about repository encryption.

Encryption of the Oracle Audit Vault Server's event repository is enabled on new installations of Oracle Audit Vault and Database Firewall. This feature uses Oracle Database's Transparent Data Encryption (TDE) to encrypt all audit event data stored in the Audit Vault Server, data stored in external SAN storage, and data stored in archive locations.

15.6.2 Rotating the Master Key for Repository Encryption

Rotating encryption keys adds a layer of security to your encrypted data.

You should rotate the master encryption key for the Audit Vault Server's event repository on a regular basis, according to your organization's guidelines. It is also a good practice to rotate the encryption key as needed. For example, when a person who had access to your master key leaves your organization.

> **Note:**
>
> If you restore the Audit Vault Server from a backup, the restore operation restores the system to a point in time. Therefore, restoring the system may reinstate an older encryption key.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **Storage** tab.
4. In the page that appears, click **Repository Encryption** tab.
5. In the **Rotate Master Key** section, in the **Keystore Password** field, enter the keystore password.

   This password is originally set as a required post-installation step.
6. Click the **Re-key** button.

15.6.3 Changing the Keystore Password

For better security, periodically change the keystore password.

The keystore password for repository encryption is originally set as a required post-installation step. It is the same as the Event Repository Encryption password. You only need this password for restore operations, not backup operations. Thereafter, you can change this password in the Audit Vault Server console.

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

2. Select the **Settings** tab.
3. In the left navigation menu, select **Storage**.
4. In the page that appears, click **Repository Encryption** tab.
5. Under **Change Keystore Password** section, enter the following:
   - **Old password**
   - **New password**
   - **Re-enter new password**
6. Click **Change Password** button.

> **See Also:**
>
> Backup and Restore of Audit Vault Server for more information on using the keystore password to restore the Audit Vault Server from backup files.

15.6.4 Backing Up TDE Wallets

You can back up TDE wallets to preserve information.

It is important to perform regular backups of Oracle Audit Vault Server, which include the TDE wallet. However, if you cannot back up Oracle Audit Vault Server, then you should, at a minimum, do regular backups of the TDE wallet at this location:

```
/usr/local/dbfw/etc/wallets/dbfwdb_wallet
```

Oracle Audit Vault and Database Firewall does not provide the ability to back up wallets. You should securely back the wallet up in a remote location.

15.6.5 Data Encryption on Upgraded Instances

Learn about data encryption on upgraded instances in Oracle Audit Vault Server.

Phases of Data Encryption

This topic contains a detailed procedure that can be used to start data encryption process.

> **WARNING:**
>
> Do not run data encryption processes on a newly installed Oracle Audit Vault Server or on a system that has been upgraded from fresh install of release Oracle Database 12.2.x. With versions of Oracle Database 12.2.0 and above, all of the new installations have encryption enabled automatically. Thus, all of the table spaces are encrypted by default.

The data encryption process happens in two phases:

1. **Enabling Data Encryption:**

   This phase is automatic and data encryption is enabled while performing an Audit Vault Server upgrade. The upgrade process prompts for a keystore password on standalone and

primary systems. Upon successful upgrade, data encryption is automatically enabled. The newly created table spaces thereafter are automatically encrypted. However, table spaces created before upgrade continue to be in clear text.

2. **Encrypting existing clear text table spaces:**

   This phase is triggered by the user. To encrypt the existing clear text table spaces, the user must initiate the data encryption process. This process is triggered by running the `/usr/local/dbfw/bin/avdf_data_encryption.sh` script. The detailed steps for encrypting existing clear text table spaces triggered by the user are available in this topic.

Before you begin

- The rate of encryption is approximately 20 to 50 seconds to encrypt 1 GiB of data, depending on the hardware profile of the system.
- To begin the process of encrypting the table spaces, the user must execute the `/usr/local/dbfw/bin/avdf_data_encryption.sh` script as *root*.
- Ensure to take AVDF backup prior to the encryption process.
- The user must have *root* operating system user privileges to execute this procedure. Ensure the proper privileges are obtained.
- The encryption process script must be executed on standalone system or on the primary in a HA set up. Ensure that the standby system is also up and running before running the encryption script. The script may result in an error if the standby system is down. The script encrypts table spaces on both the primary and standby system.
- Ensure that the database is up and running prior to executing the encryption process. To verify the status of the database, log in as *root* user and execute the command `/etc/init.d/dbfwdb status`
- The encryption process script stops all the jobs running in the background. Ensure there is no critical process running that may be impacted.

> **Note:**
>
> Data encryption is not completely enabled on HA system, until the primary is successfully upgraded. After a successful upgrade, all clear text table spaces are in one of the following states:
>
> - online
> - offline local (offline but the data file resides on the AVS)
> - offline remote (offline but the data files reside on the remote archive location)
> - online retrieved by user
> - online retrieved by a trail

To start Data Encryption process:

1. Log in to the system as *root* user.
2. Execute the following command to start encryption:

   ```
   /usr/local/dbfw/bin/avdf_data_encryption.sh start
   ```

3. The following message is displayed on the screen:

```
*************************************************************
* This script will encrypt all online tablespaces and create *
* a background job to encrypt offline tablespaces.           *
* Encrypting online tablespaces could potentially take long  *
* time depending on the size of the online data collected.   *
* Note that during this time                                 *
*   - There will be no access to Web UI console.             *
*   - Event collection will be shutdown.                     *
*   - AV agents will not be able to connect.                 *
*   - AVCLI will not be able to connect.                     *
*                                                            *
*  NOTE: It is recommended to take backup before continuing. *
*************************************************************
Do you want to continue (Y/N):
```

4. Type `Y` to continue with encryption.
5. The following message is displayed:

```
************************************************************
* Do not interrupt this script execution or reboot.        *
* To stop the script execution use                         *
* 'avdf_data_encryption stop' command.                     *
* Check /root/avdf_data_encryption.log to track progress   *
************************************************************
```

> **Note:**
>
> At this point, it is recommended to move the process to background by executing `Ctrl+z` followed by `bg`. Alternately to keep the session alive, the user can execute the command `ssh -o ServerAliveInterval 20`

The following messages are displayed on the screen:

```
Successfully encrypted online table spaces.
System is ready for use.
Offline table space encryption can be managed on the AVS GUI.
```

> **Note:**
>
> Contact My Oracle Support with the printed output in the event of a failure.

6. The following message is displayed in the `/var/log/avdf_data_encryption.log` file:

```
Encrypting <tbsp name> Tablespace : % done
```

7. Once the encryption process is successfully completed, another job to encrypt offline table spaces is created and enabled in the background. All the services appear online and the following message is displayed:

   ```
   System is ready for use
   ```

8. In case the encryption process fails, the `/var/log/avdf_data_encryption.log` file displays the following error message.

   ```
   Failed to encrypt table spaces: Please contact Oracle Support
   ```

9. Execute the following command to stop encryption:

   ```
   /usr/local/dbfw/bin/avdf_data_encryption.sh stop
   ```

> **Note:**
>
> Ensure to execute the stop command only after you see the following message in the `/var/log/avdf_data_encryption.log`:
>
> ```
> You may issue stop command to gracefully stop the encrypting process
> ```

> **Note:**
>
> Once the stop encryption command is executed, the encryption process exits only after encrypting the current table space that is being encrypted. It is always recommended to run the script again to complete the encryption process.

10. In case the user decides to perform a reboot of the system during the encryption process, it stops at the current table space that encryption last accessed. The user can decide to run the script again to complete the encryption process.
11. In case the **dbfwdb** service terminates unexpectedly, contact Oracle Support. The encryption script will not run if this service is down.
12. The encryption process collects all the logs to `/var/log/avdf_data_encryption.log` file securely.
13. After all online table spaces are encrypted, a background job *ENCRYPT_OFFLINE_TBSP* is enabled to perform encryption of offline table spaces. This job encrypts all table spaces for those data files that reside locally on the system. In case the data file is located on the remote location `nfs/scp/smb`, the data file is copied to the local system, encrypted, and setup for re archival. The user must manually perform the re archival process to ensure that the data file in the remote location `scp/smb` is encrypted. The user can navigate to **Settings** and **Repository Encryption** page to view a list of offline table spaces that are not encrypted. If the data file is not available, the message displayed indicates the same.
14. The process of encrypting offline table spaces can be in one of the following states.

Message	Description
`NOT YET STARTED`	The user has not executed the script to encrypt table spaces.
`COMPLETED`	All online and offline table spaces are encrypted. Any new table spaces created will also be encrypted. This is the final state.
`IN PROGRESS`	The background job is currently encrypting offline table spaces.

Message	Description
USER	The background job is waiting for user input. User must visit the **Repository Encryption** page and take appropriate action.
ERROR	There was an error in encrypting one or more table spaces. The user must download the diagnostics and provide that to Oracle Support.
TRAIL	The table space has been retrieved by a trail as it is collecting old data. Wait for the trail to release the table space.

15. In the ERROR state the background job is disabled and hence the user, after fixing the cause of the error must re-enable the job from the **Repository Encryption** page.
16. In the event of system reboot, power failure, switch over, or fail over the user can execute the encryption process again.

15.7 Backup and Restore of Audit Vault Server

Learn about backup and restore of Audit Vault Server.

15.7.1 About Backup and Restore of Audit Vault Server

Learn about the details of backing up and restoring Audit Vault Server.

Audit and network event data that is collected by Oracle AVDF is stored in the embedded Audit Vault Server repository (Oracle Database). This repository also contains reports and configuration data. Audit Vault Sever administrator must take backup of Audit Vault Server on a regular basis. In case of an Audit Vault Server outage, the administrator can install a new Audit Vault Server and restore from the backup taken earlier. This minimizes data loss. For example, if the Audit Vault Server machine faces hardware failure, a new Audit Vault Server can be restored using the most recent backup. This process brings the entire data back to the point when the last backup was taken.

Audit Vault Server backup contains the collected data and the configuration data. The configuration data includes data associated with Agent registration, target registration, wallets, etc. The configuration data is located in the OS files and the embedded repository. Audit Vault Server backup does not take backup of the archived data files. As long as the restored Audit Vault Server has access to these archived files, the data can be retrieved and viewed.

The size of the backup is dependent on the size of the data collected and stored in the embedded repository.

Database Firewall does not require a backup. Audit Vault Server can reapply all existing configuration of the monitoring points to the Database Firewall during the post restore steps.

Types of Backup Supported by Audit Vault Server

Audit Vault Server supports full backups and incremental backups. An incremental backup contains only the new data and configuration changes since the previous backup. For example, a full backup is taken on Sunday, and then incremental backups are taken on Monday, Wednesday, and Friday. A full backup and the subsequent incremental backups together make a backup set. Oracle recommends to test and validate the backup set regularly to determine whether the backup set can be restored. Backup validation can be included as part of the backup cron job. An example is mentioned in the later topics.

Audit Vault Server backup functionality supports both hot (online) and cold (offline) backups. A hot backup is a backup that is taken when the Audit Vault Server is up and running and when the embedded repository is online. This option ensures that the deployment continues to

monitor the targets when backup is in progress. The administrator can access reports and make changes to the configuration in this case. Oracle recommends to setup hot backup as a best practice.

A cold backup requires the Audit Vault Server repository to be offline. In this case, the targets are not protected and the Audit Vault Server console is unavailable until the backup is completed.

Types of Backup Locations Supported by Audit Vault Server

A backup location is a user defined directory path to store the backup files. The location can be on a local disk or on NFS (Network File System). Oracle recommends using NFS for the backup location as a best practice. The location of the backup files should be accessible by the Audit Vault Server as *root* and *oracle* OS user.

Redundancy of Audit Vault Server Backups

Redundancy settings control as to when a backup set is marked as obsolete. For example, if redundancy is set to 2 and the third full backup is taken, the files in the first backup set are marked as obsolete. It is recommended to take more backups than the redundancy setting within a period of 30 days to ensure the obsolete backup files are purged properly. Redundancy is an important setting in managing storage space in the backup location.

Encryption of Audit Vault Server Backup

The Audit Vault Server backup contains information of the OS files and the embedded repository. The embedded repository is encrypted using Transparent Data Encryption and the pertaining backup files are also automatically encrypted. However, the OS configuration files are not encrypted and the backup of these files are also not automatically encrypted. Audit Vault Server backup provides a setting to encrypt the backup of the OS configuration files. This allows to restrict access to configuration like wallets present in the backup location.

Tasks Involved in Audit Vault Server Backup and Restore

The following are the backup tasks:

1. Planning for Audit Vault Server backup
2. Configuring Audit Vault Server for backup
3. Performing Audit Vault Sever backup
4. Monitoring Audit Vault Server backup

The following are the restore tasks:

1. Planning for restoring Audit Vault Sever
2. Performing necessary checks for restore
3. Restoring Audit Vault Server from backup taken earlier

15.7.2 Audit Vault Server Backup and Restore in High Availability Environment

Learn about backup and restore of Audit Vault Server in a high availability environment.

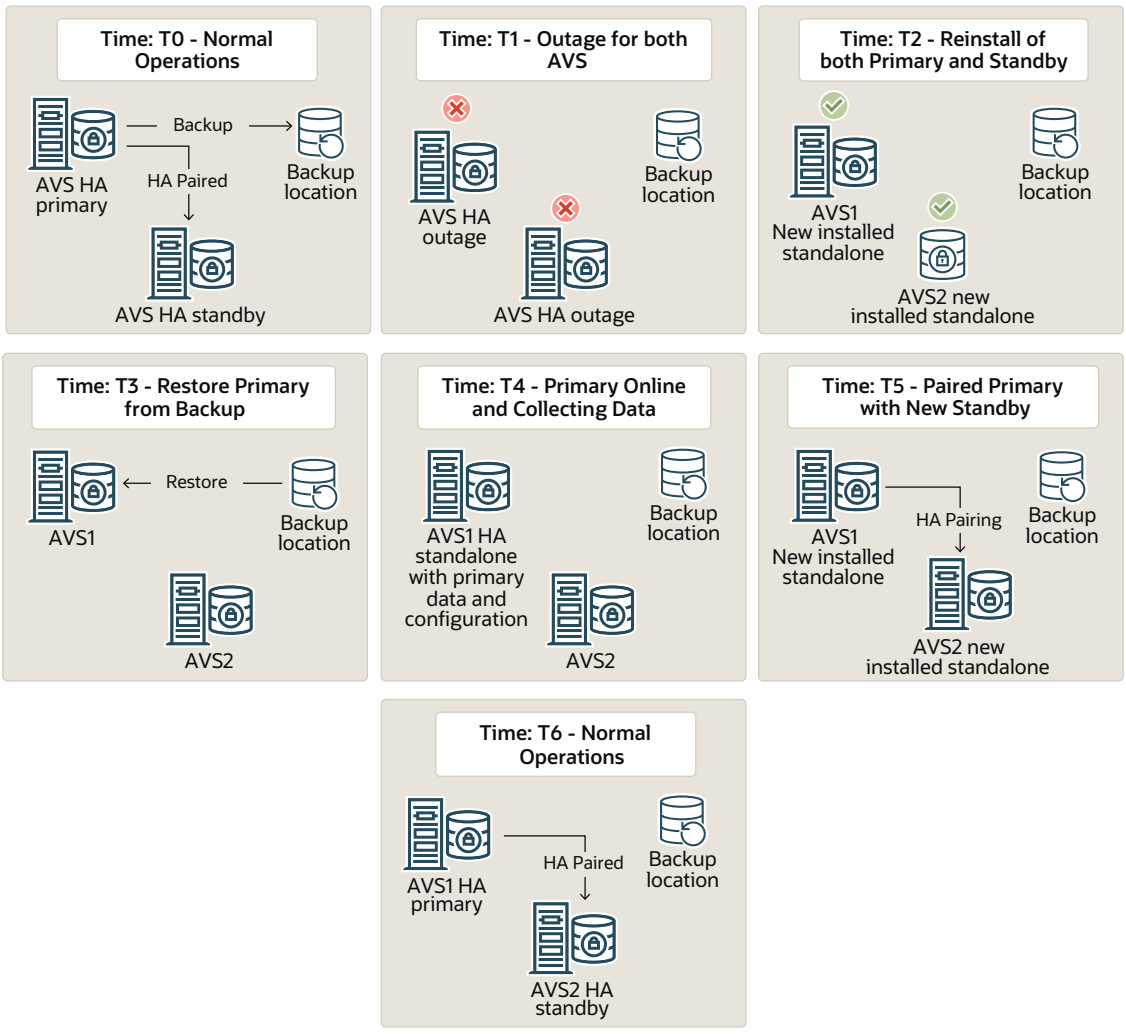
In a high availability environment, there are two Audit Vault Servers paired (primary and standby). The primary Audit Vault Server is the active server that provides the Audit Vault Server functionality. The standby is automatically synchronized (audit data and network event data) and has a consistent copy of the primary. The backup operation must be performed on

the primary Audit Vault Server and not on the standby Audit Vault Server. When Audit Vault Server is restored from a backup taken on primary Audit Vault Server, the restored Audit Vault Server is configured in standalone mode. It must be paired again with another Audit Vault Server to achieve high availability.

> **See Also:**
>
> Configuring High Availability for Audit Vault Servers

The following diagram illustrates different aspects involved in backup and restore functionality of Audit Vault Server configuration in a high availability environment.

Figure 15-1 Audit Vault Server Backup and Restore in High Availability Environment



15.7.3 About Audit Vault Server Backup and Restore Utility

Learn how the Audit Vault Server backup and restore utility works.

Audit Vault Server backup and restore utility provides all the necessary functionality to perform backup and restore related operations on the Audit Vault Server. This utility `avbackup` must be run as the *root* OS user. It is located in `/var/lib/oracle/dbfw/bin`.

The backup utility supports:

- full backup and incremental backup
- hot and cold backup
- local and NFS backup locations
- restore of data and configuration to a new Audit Vault Server from backup taken earlier
- validation of the backup taken earlier

Audit Vault Server Backup and Restore Commands

The following are the commands used to backup and restore Audit Vault Server:

Command	Task
`avbackup config`	To configure Audit Vault Server backup settings.
`avbackup backup`	To perform backup of Audit Vault Server.
`avbackup validate`	To validate the backup file set.
`avbackup restore`	To restore Audit Vault Server using backup file taken earlier.

Audit Vault Server Backup Settings

Configure the Audit Vault Server backup and restore functionality by running the `avbackup config` command as OS *root* user.

> **Note:**
>
> The following settings must be the same for both backup and restore operations.

Field / Category	Description
MAXPIECESIZE	This setting controls the maximum size of a backup file. A backup can contain multiple backup files, otherwise known as backup pieces. The valid maximum file size depends on the actual file system. Setting MAXPIECESIZE is required only if CHANNEL_PARALLELISM is set to 1. Valid values: 1 - 2048 Kbs/Mbs/Gbs Default value: 2G (2 GB) For example: MAXPIECESIZE[2G]:
BACKUP_DIR	The directory that stores all the backup files. The directory path is limited to 200 characters. Default value: /backup After this directory is specified, do not change this directory path as Oracle Recovery Manager (RMAN) tracks the backup files in this directory. The files are written to this directory and access to this directory is managed by *oracle* user (UID 503) who is part of the oinstall group (GID 504). Oracle AVDF backup utility automatically uses this directory path during the restore operation. When the BACKUP_DIR setting is changed, performing a full backup is a must. This is to ensure the backup set is complete and located in the new BACKUP_DIR location.

Note:

- Do *not* change this setting between full backup and incremental backup, as the incremental backup may fail. Change this setting only to put the new full backup files into a different location. If this rule is not followed, it may cause failure of restore operation.
- The BACKUP_DIR location value must be *different* for online backup and offline backup. If this rule is not followed, it may corrupt the backup file and failure of restore operation.
- Do not change this setting between full backups, as the redundancy setting may not apply correctly. In case REDUNDANCY is set to 2 and BACKUP_DIR is changed before the third full backup is taken, then the first backup set is not purged after taking the third full backup. If BACKUP_DIR is not changed before the third full backup is taken, the first backup set is purged after taking the third full backup.
- The backup directory must be a mounted file system with enough free space to hold the backup files. This can be NFS (Network File System). Tape storage is not supported as a backup location.
- All the backup files are saved in BACKUP_DIR location, except when CHANNEL_PARALLELISM is specified to a value greater than 1. When CHANNEL_PARALLELISM is greater than 1, CHANNEL_LOCATION must be specified for each channel, and the specified locations are used as backup locations.
- The BACKUP_DIR location must have enough free space to hold the backup files. The space requirement depends on REDUNDANCY setting.

See Also: *Backup Location Storage Requirements* in Backup of Audit Vault Server

Field / Category	Description
BACKUP_TYPE	Specifies the type of backup to be performed. Enter HOT or COLD. A HOT backup is an online backup when the Audit Vault Server is fully operational. A COLD backup is an offline backup that requires the embedded repository (Oracle Database) in the Audit Vault Server to be shut down. Default value: HOT Archive log mode must be enabled for hot (or online) backup. Enabling archive log mode is quick and requires a restart of the embedded repository. For a cold (offline) backup, the embedded repository in Audit Vault Server is shut down during the backup process. Shutting down the embedded repository results in downtime of monitoring until the backup operation is completed. **See Also:** *Backup Strategy* in Backup of Audit Vault Server
PASSWD	The password used to encrypt the configuration data stored in the OS files. If this is omitted, then the backup OS files are not encrypted. However, the data backed up from embedded repository is always encrypted by TDE (Transparent Data Encryption). If this password is specified during backup, it must be provided for restore operation later. There is no way to recover if the password is lost for restore operation. Hence, it is recommended to keep the password stored in a safe location. Default value: Not set. Password must be at least 8 characters long and must contain a number, uppercase letter, lowercase letter, and a special character . , _ + :
CHANNEL_PARALLELISM	Specifies the number of channels (processes) used for running the commands. In case there are multiple backup locations and each backup location is mounted on separate physical disks, then this setting can be used to increase the speed of backup operations. Set this parameter to match the number of physical disks used for backup locations. If this parameter is set to 1, then the value for MAXPIECESIZE must be specified. If this setting is greater than 1, then the locations and section size (CHANNEL_LOCATION and SECTION_SIZE) must be specified. Default value: 1 For example: CHANNEL_PARALLELISM[1]:4
CHANNEL_LOCATION	Specifies the location for each channel and is required when CHANNEL_PARALLELISM is greater than 1. Based on the value of the CHANNEL_PARALLELISM, specify the same number of channel locations. If CHANNEL_PARALLELISM is 2, then provide values for CHANNEL_LOCATION_1 and CHANNEL_LOCATION_2. Default value: None As shown in the example below, it is recommended to specify each location in a different physical disk. For example: CHANNEL_LOCATION_1[]:/disk_1 CHANNEL_LOCATION_2[]:/disk_2 CHANNEL_LOCATION_3[]:/disk_3 CHANNEL_LOCATION_4[]:/disk_4 **Note:** The CHANNEL_LOCATION takes precedence of the BACKUP_DIR for backup in case of the embedded repository. However, the backup of the OS files continue to be located in BACKUP_DIR.

Field / Category	Description
SECTION_SIZE	This determines the section size for each channel to backup. This setting is required only if CHANNEL_PARALLELISM is set to greater than 1. If CHANNEL_PARALLELISM is set to more than 1, then the Audit Vault Server backup is performed in parallel. The datafiles in the embedded repository are split into logical sections for which the size is determined by this setting. Each channel performs a backup of one section at a time. Specify this size considering the maximum file size of the channel location and the biggest datafile in the embedded repository. A small value could result in an increase in the number of files created in the channel location and a much larger value may be beyond the maximum file size that the channel location can support. Default value: None For example: SECTION_SIZE[]:32G

> **Note:**
>
> Use CHANNEL_PARALLELISM, CHANNEL_LOCATION, and SECTION_SIZE configuration parameters for a database with a size of 1 TB or more.

The following settings can be different for each backup, validate, or restore operations:

Field / Category	Description
TMP_DIR	It is a temporary working parent directory that stores all temporary files and logs. It must have at least 100 MB of free space. The *oracle* user must have read-write access to this directory. Default value (Oracle AVDF release 20.7 and earlier): Directory path /tmp For example: TMP_DIR[/tmp]: /tmp/BCKTMP Default value (Oracle AVDF release 20.8 and later): Directory path /usr/local/dbfw/tmp For example: TMP_DIR[/usr/local/dbfw/tmp]: /usr/local/dbfw/tmp/BCKTMP
KEEP_LOGS	It determines whether the log files are stored after a successful backup operation. Logs are always kept after a failure. Enter YES to retain logs after backup, validate, or restore operations. Enter NO to automatically delete logs after successful backup or restore operations. The logs are always saved if the backup or restore operation fails irrespective of the KEEP_LOGS setting. Default value: NO For example: KEEP_LOGS[NO]:yes
INCREMENTAL	This setting provides an option to choose from full or incremental backup. Enter 0 for a full backup. Enter 1 for incremental backup. This setting applies only to backup. Default value: 0 (full backup) For example: INCREMENTAL[0]:0

Field / Category	Description
USE_NEW_IP	Specifies whether to use a new or an existing IP address for the restored system. This setting applies only to restore operation. This setting is ignored if the Audit Vault Server is restored on an OCI image. The allowed values are Y or N. Default value: N If USE_NEW_IP is set to N, the restored Audit Vault Server automatically switches to the IP address of the Audit Vault Server when the backup was taken. If USE_NEW_IP is set to Y, the restored Audit Vault Server retains the IP address set during fresh installation of this Audit Vault Server. Case 1 • Backup of Audit Vault Server with IP1 • Audit Vault Server with IP1 goes offline • USE_NEW_IP set to N for restore operation • Restore of Audit Vault Server with IP2 • The IP address of the final restored Audit Vault Server is switched from IP2 to IP1 Case 2 • Backup of Audit Vault Server with IP1 • Audit Vault Server with IP1 goes offline • USE_NEW_IP set to Y for restore operation • Restore of Audit Vault Server with IP2 • The IP address of the final restored Audit Vault Server remains IP2 For example: USE_NEW_IP[N]:Y
REDUNDANCY	Specifies the number of full backups to be kept before purging obsolete backup sets. This setting applies only to backup. This setting impacts the backup storage specified in the BACKUP_DIR parameter. For example: If this value is set to 2, the first backup set is purged when the third full backup has completed successfully. Default value: 1 **See Also:** *Backup Location Storage Requirements* in Backup of Audit Vault Server

Note:

- Audit Vault Server backup and restore operations may take a long time. When you use *SSH* to connect to Audit Vault Server to perform these operations, ensure you have configured *SSH* properly to avoid *SSH* timeouts.
- In this table and throughout this document, 1 GB represents 2 to the 30th power (2^{30}) bytes or in decimal notation 1,073,741,824 bytes.

15.7.4 Setting Up NFS for Audit Vault Server Backup and Restore

Oracle recommends using Network File System (NFS) for the Audit Vault Server backup location. This location must be the same for backup and restore operations..

For example, if BACKUP_DIR for the Audit Vault Server backup is /var/lib/oracle/avs_backup, then configure the same BACKUP_DIR (/var/lib/oracle/avs_backup) for

the Audit Vault Sever restore operation. This location (for example, `/var/lib/oracle/avs_backup`) should be owned by `oracle:oinstall` with `read-write` permission.

For example, to mount `avs_backup` to the NFS server, follow these steps:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run the following command:

```
mount -t nfs <NFS_IP>:<export_path> /var/lib/oracle/avs_backup
```

> **Note:**
>
> - Configure the same mount point on the Audit Vault Server before backup and restore.
> - The exact `mount` command may vary.
> - Make sure that the `oracle` user has `read`, `write`, and `execute` permissions for the directory that you created as the mount point.
> - Ensure that `BACKUP_DIR` is set to `/var/lib/oracle/avs_backup` for both backup and restore.
> - If you updated `/etc/fstab` to add the mount point, it reverts to the original state when the system is restarted.

15.7.5 Backup of Audit Vault Server

Learn how to perform Audit Vault Server backup.

These are the steps involved in the backup of Audit Vault Server:

1. Planning for Audit Vault Server backup.
2. Configuring the Audit Vault Server backup.
3. Performing or automating Audit Vault Server backup.
4. Monitoring the Audit Vault Server backup.

Planning for Backup

Planning for backup of Audit Vault Server involves the following aspects:

Aspects	Description
Backup strategy	Backup strategy involves setting up a backup schedule that meets corporate requirements or guidelines. Frequent backups can minimize data loss but impact system performance. A full backup can take longer than an incremental backup. A good backup strategy aims to minimize both the data loss and the impact on system performance. **Best Practice:** A full online backup once a week and multiple incremental backups during the week is optimal. Consider backup optimization mentioned in this table below to reduce backup times. **Note:** Do not keep both online and offline backup files in the same directory. In such a case, make sure they are stored in two separate backup locations.

Backup location storage requirements	Ensure there is sufficient disk space in the backup location to store the backup files. The backup location contains the OS configuration files (`.tar` file) and the related backup of the repository. There may be multiple backup sets in the backup location depending on the redundancy setting. For example, if redundancy is configured to 3, the backup location keeps up to 4 sets of backups before it begins to purge the obsolete backup files.
	Determining the space requirement for the backup location, depends on the size of the Audit Vault Server repository (Oracle Database). Run the following SQL query as *sysdba* user for an approximate calculation:
	`sqlplus / as sysdba`
	`Enter password: password`
	`SELECT SUM (BYTES)/1024/1024/1024||' GB' FROM DBA_DATA_FILES`
	This calculation is a simple estimation of a full backup file. For each incremental backup, add more disk space in addition to the above specified amount. It is not possible to calculate the specific size for incremental backup in a live system. Use this as a guideline after Audit Vault Server is deployed and is stable.
	To calculate a simple estimate of incremental backup file, find the difference between two full backup files. Divide this by the number of incremental backup specified. This provides an average size of an incremental backup file.
	Note: Ensure *oracle* user and group *oinstall* users have `read`, `write`, and `execute` permission to the backup directory.

Backup type	Oracle AVDF supports online and offline backup. Offline backup requires Audit Vault Server downtime. Offline backup does not have data loss up to the time the backup is taken. Online backup allows taking backup when Audit Vault Server is online. There is a potential loss of data involved in online backup. Online backup requires archive log mode to be enabled for the database. Oracle recommends taking online backup.
Retention	The retention of the backup depends on the `REDUNDANCY` setting. Specify an appropriate value based on the organization's policy. In most situations, `REDUNDANCY` is set to a value greater than 1 to keep more than one backup set. For obsolete backup files to be purged properly, schedule more full backups than the retention configuration within a period of 30 days.
Channel parallelism	Setting higher parallelism (`CHANNEL_PARALLELISM`), can improve backup performance. However, it only improves performance if it matches the actual physical number of disks available. If there is only one physical disk, it does not improve the backup performance even if `CHANNEL_PARALLELISM` is set to greater than 1.

Aspects	Description
Backup optimization	It is recommended to increase the channel parallelism to match the physical number of disks. This can improve the backup performance. When channel parallelism is set to a value greater than 1, then set the section size too. Section size defines how the datafile is handled by each channel during backup operation. To improve performance specify different `CHANNEL_LOCATION` on a different physical hard disk. Specifying all the channel locations to the same path, does not utilize the benefits of parallelism. Increasing the maximum piece size can also improve the performance if channel parallelism is set to 1. The maximum piece size depends on the file size supported by the filesystem.

Space Required for Backup Files

Determine the amount of space needed for backup files. The amount of space needed for backup files is determined by the size of Audit Vault Server repository. You can obtain an upper estimate of the backup file size for the database by running the following SQL query on the Audit Vault Server:

```
sqlplus system
Enter password: password
SELECT SUM (BYTES)/1024/1024/1024||' GB' FROM DBA_DATA_FILES
```

Note:

- Ensure the RAM size and disk size in the new system is equal or greater than the original system. This ensures out of memory error is not observed while performing the backup and restore tasks.
- The backup process does not include the SAN configuration. Ensure the new system has sufficient disk space before performing restore. For more information on the disk space needed, refer to the `info.txt` file available in the backup directory.
- The restore system requires at least the same amount of memory and disk space as the backup system. Otherwise, the restore operation fails.

15.7.6 Configuring Audit Vault Server Backup

Learn how to configure the backup utility for Audit Vault Server.

Audit Vault Server must be configured before performing the backup operations. This configuration includes different settings and values that are saved in a backup settings file `/var/lib/oracle/dbfw/av/backup/.backup_restore_config`. This file is used to configure the backup process.

The backup of the OS files can be encrypted with a password that must be specified when configuring the Audit Vault Server backup. The backup of the repository is encrypted using TDE (Transparent Data Encryption). Make sure to store both the password (if specified) for backup of the OS files and the TDE keystore password for repository, in a safe location. These passwords are needed during the restore operation.

Run the following command as *root* user to configure the backup settings, and follow the prompt:

```
/var/lib/oracle/dbfw/bin/avbackup config
```

15.7.7 Performing Audit Vault Server Backup

Learn how to run Audit Vault Server backup tasks.

Prerequisite: Configure the backup utility for Audit Vault Server.

For online (hot) backup, follow these steps before initiating backup:

1. Choose the backup type `HOT` when configuring the backup utility.
2. Ensure that the Audit Vault Server is in archive log mode by following these steps:
   a. Connect through SQL*Plus as the `oracle` OS user, by running the command:

      ```
      sqlplus / as sysdba
      ```

   b. Run the following command:

      ```
      archive log list;
      ```

   c. If the output from the above command displays `No Archive mode`, then Audit Vault Server is not in archive log mode. If the output displayed is `Archive mode`, then skip the next step.
3. To enable archive log mode follow these steps:

- Oracle AVDF 20.12 and later
- Oracle AVDF 20.1 - 20.11

Oracle AVDF 20.12 and later

a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

b. Execute the following:

   ```
   /var/lib/oracle/dbfw/bin/avbackup enable_archinvelog
   ```

c. Enter `Y` to confirm you want to continue with the process which includes restarting the database.
   The process may take several minutes to finish.

Oracle AVDF 20.1 - 20.11

a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

b. Run the following command to stop the monitor process:

```
systemctl stop monitor
```

c. Run the following command to shut down the Audit Vault Server repository (Oracle Database):

```
systemctl stop dbfwdb
```

d. Run the following command to ensure that the Audit Vault Server repository is shut down:

```
/usr/local/dbfw/bin/dbfwdb status
```

The output is `ORACLE instance shut down.`

e. Switch to the `oracle` user.

```
su - oracle
```

f. Start SQL*Plus as `sysdba`.

```
sqlplus / as sysdba
```

g. Run the following commands at the SQL*Plus prompt to enable archive log mode:

```
startup mount

alter database archivelog;

alter database open;

shutdown immediate;
```

h. Exit SQL*Plus.

```
exit
```

4. Switch to `root` OS user.
5. Run the following commands:

```
systemctl start dbfwdb

systemctl start monitor
```

6. As the `root` OS user, run the following command to initiate the backup:

```
/var/lib/oracle/dbfw/bin/avbackup backup
```

7. Enter the required information by following the prompt.
8. A list of files (similar to the following example) appear in the backup location when the backup is complete.

```
DBID_1440353975_09Q7EF7L_1_1
DBID_1440353975_C-1440353975-20150520-00
```

Offline (Cold) Backup

1. Choose the backup type as `COLD` when configuring the backup utility.
2. As *root* OS user, run the following command to initiate backup:

```
/var/lib/oracle/dbfw/bin/avbackup backup
```

3. Enter the required information by following the prompt.

> **Note:**
>
> - For an offline backup the Audit Vault Server repository is shutdown for the entire duration of the backup.
> - Oracle recommends to reboot the system in case there is a failure while performing a cold (offline) backup operation.

15.7.8 Monitoring and Validating the Audit Vault Server Backup

Learn how to validate, monitor, and troubleshoot the Audit Vault Server backup process.

The backup configuration file is release specific. It works on the same release. It is advisable to run the `avbackup config` command and create a new configuration file before performing the backup operation after Oracle AVDF upgrade.

Follow these steps to validate the backup last created:

1. Log in to the Audit Vault Server as `root` OS user.
2. Run the following command:

```
/var/lib/oracle/dbfw/bin/avbackup validate
```

The backup status is displayed, similar to the following:

```
Backup Restore exit status: 0
Status 0 = Success. Status 1 = Failure.
```

3. The backup process records the logs in the `/var/lib/oracle/dbfw/av/log/av.backup*.log` file. Check the log files for any errors. In case there is any issue in the backup process, then the backup process also records the logs in `TMP_DIR/av_backup*` directory. The following logs contain detailed information:
   - `/TMP_DIR/av_backup_<timestamp>/<logs>`
   - `/var/lib/oracle/dbfw/av/log/av.backup_restore-pid-0.log`
   - `/var/lib/oracle/dbfw/av/log/av.backup_restore_error-pid-0.log`

Oracle AVDF administrator must monitor the disk space usage to make sure there is enough space for the new backup files and obsolete backup files that are purged properly based on the retention setting.

> **Note:**
>
> Important aspects involved in troubleshooting of Audit Vault Server backup process:
>
> - The backup directory must be owned by `oracle:oinstall` with permission `770`.
> - Make sure to take more backups than `REDUNDANCY` setting within 30 days and obsolete backup files are purged properly.
> - Check `/var/lib/oracle/dbfw/av/log/av.backup*` log files for any errors. Check `TMP_DIR/av_backup*` for more detailed logs if there are any issues.
> - Check available disk space for backup.
> - The location of offline backup and online backup must be different. Do not use the same `BACKUP_DIR` location. Once this location is specified, it is advisable not to change the directory path until the next full backup.
> - Ensure the `BACKUP_DIR` and `CHANNEL_LOCATION_x` disk has enough space for the backup files.

15.7.9 Automating the Backup Schedule

Learn how to automate the backup schedule of Audit Vault Server.

The backup process can be scheduled and automated by setting up a cron job. For example, set up a cron job to take a full online backup once a week. Set up another cron job to take incremental online backup thrice a week.

The backup operation takes the configuration details from the `/var/lib/oracle/dbfw/av/backup/.backup_restore_config` file. Full backup and incremental backup require different configuration details, and hence need to have two separate configuration files.

Follow these steps to automate both full and incremental backups:

1. Create a settings file for full backup. Run the following command and specify `INCREMENTAL` value to `0`:

```
avbackup config
```

2. Move the `/var/lib/oracle/dbfw/av/backup/.backup_restore_config` file to another location `/var/lib/oracle/dbfw/av/backup/backup_restore_config_full`.
3. Create a settings file for incremental backup. Run the following command and specify `INCREMENTAL` value to `1`:

   ```
   avbackup config
   ```

4. Move `/var/lib/oracle/dbfw/av/backup/.backup_restore_config` file to another location `/var/lib/oracle/dbfw/av/backup/backup_restore_config_incremental`.
5. Create a full backup script (`full_backup_script`), that copies the `/var/lib/oracle/dbfw/av/backup/backup_restore_config_full` to `/var/lib/oracle/dbfw/av/backup/.backup_restore_config` before running the `avbackup backup` command.
6. Set up a cron job to run full backup script as *root* user at a specific time on a specific day of the week. Follow these steps:
   a. Run the following command as *root* user:

      ```
      crontab -e
      ```

   b. Add a line similar to the following example in the editor. The example time specified is for midnight on every Saturday.

      ```
      0 0 * * 6 /<some_directory_path>/<full_backup_script>
      ```

   c. Save the file and exit.
   d. Check the cron job setup by running the following command:

      ```
      crontab -l
      ```

7. Create incremental backup script (`incremental_backup_script`), that copies `/var/lib/oracle/dbfw/av/backup/backup_restore_config_incremental` file to `/var/lib/oracle/dbfw/av/backup/.backup_restore_config` before running the `avbackup backup` command.
8. Set up a cron job to run incremental backup script as *root* user at a specific time thrice a week on specific days. Follow these steps:
   a. Run the following command as *root* user:

      ```
      crontab -e
      ```

   b. Add the lines in the editor similar to the following example for running backup at midnight every Monday, Wednesday, and Friday:

      ```
      0 0 * * 1 /<some_directory_path>/<incremental_backup_script>
      0 0 * * 3 /<some_directory_path>/<incremental_backup_script>
      0 0 * * 5 /<some_directory_path>/<incremental_backup_script>
      ```

   c. Save and exit.

d. Check the cron job setup by running the following command:

```
crontab -l
```

> **Note:**
>
> Use this as a guideline to automate scheduled backups. It is recommended to test out the `full_backup_script`, `incremental_backup_script`, and the cronjob setting before deploying in production. Change the cron job configuration as per your requirement and policy.

15.7.10 Performing Audit Vault Server Backup in High Availability

Learn how to run the Audit Vault Server backup task in a high availability environment.

In a high availability environment, there are two Audit Vault Servers (primary and standby). Backup operation must be performed on the primary Audit Vault Server.

Follow these steps:

1. Disable automatic failover before performing backup operation.
2. Run the backup operation.
3. Enable automatic failover.

> **See Also:**
>
> Disabling or Enabling Failover of the Audit Vault Server

15.7.11 Restoring from Audit Vault Server Backup

Learn how to restore Audit Vault Server from backup taken earlier.

In case of outage or contingency, the Audit Vault Server can be restored from backup taken earlier.

Important aspects involved in restoring of Audit Vault Server:

Aspects	Description
Planning and strategy	• The restore operation can only be performed on the same version of Audit Vault Server. The new system must be a freshly installed system without any data. For example, restore of Oracle AVDF release 20.3 backup can be performed on a newly installed 20.3 Audit Vault Server, but not on a 20.4 Audit Vault Server. • Choose to restore with the original IP address or restore to a new IP address. Restore using the original IP address requires the new system to be on the same subnet as the backup system. Audit Vault Server can be restored on a new system with a new IP address. • The system on which the Audit Vault Server is being restored must have equal (or more) memory and disk space. Audit Vault Server cannot be restored on a system with less memory or disk space. • After the restore operation is initiated, all the information in the restore system is wiped out and replaced by the information from the backup system. • After restore operation, the Audit Vault Server contains data of the backup Audit Vault Server and until the time of the backup taken. **Note:** To perform restore on Audit Vault Server, the administrator must provide: • the repository encryption password of the backup system • the encryption password for backup if that is configured for backup

Space	Ensure the new system has sufficient disk space before performing the restore operation. For more information on the disk space needed, refer to the `info.txt` file available in the backup directory. The lines start with `ASM_TOTAL_EVENTDATA`, `ASM_TOTAL_RECOVER`, and `ASM_TOTAL_SYSTEMDATA`. For example:
	
	`<snip info.txt>`
	`ASM_DG_EVENTDATA 12855`
	`ASM_DG_RECOVERY 5897`
	`ASM_DG_SYSTEMDATA 5793`
	`ASM_TOTAL_EVENTDATA 14475`
	`ASM_TOTAL_RECOVERY 14475`
	`ASM_TOTAL_SYSTEMDATA 14473`
	`</snip info.txt>`
	
	Where `ASM_TOTAL_EVENTDATA 14475` stands for 14,475 MB for `EVEENTDATA` disk group.

Memory	The new system on which the Audit Vault Server is being restored must have equal or more memory available than the backup system.
Storage	The backup files must be in the same backup location or path, as the backup system. In case the local file system is being used, then copy the backup files to the same path similar to the backup system. In case of NFS (Network File System), mount the backup location to the same path as of the backup system.
Configuration	To restore the new Audit Vault Server from backup file taken earlier, configure the backup utility on the new Audit Vault Server. The configuration of the restore system must match the configuration of the backup system. For example, if the backup files are for online backup, you must configure the restore system for online backup. A new IP address can be used if required on the restore system. If a new IP address is used to configure during restore, the new Audit Vault Server stays on the new IP address and does not switch to the original backup Audit Vault Server IP. In this case all the existing Audit Vault Agents and Database Firewall instances must be updated with the new IP address. In case the restore operation is performed with the existing IP address, then make sure the original IP address is available. After the completion of restore operation, the Audit Vault Server is set to the original IP if `NEW_IP` is configured to `N`.

Follow these steps to restore the Audit Vault Server:

1. Verify and make sure the backup files are owned by `oracle:oinstall`.
2. Ensure the OS user *root* on the restore system has access to `BACKUP_DIR` directory.
3. Copy the backup files to the new Audit Vault Server, or mount the NFS placing the files in the `BACKUP_DIR` directory that was specified earlier.
4. Log in to the Audit Vault Server as *root*.
5. Run the following command:

   ```
   /var/lib/oracle/dbfw/bin/avbackup restore
   ```

6. When prompted, enter the keystore password. This password is the same keystore password used for the original system.
7. When restore operation is completed, check the following log files for errors:
   - `/TMP_DIR/av_backup_*_timestamp`
   - `/var/lib/oracle/dbfw/av/log/av.backup_restore-pid-0.log`
   - `/var/lib/oracle/dbfw/av/log/av.backup_restore_error-pid-0.log`

> **Note:**
>
> - Do not initiate the restore process inside the backup directory.
> - Ensure there is no terminal accessing the backup directory. If any terminal is accessing the backup directory, it results in `device busy` error during restore process.
> - Audit Vault Server must be restored from the most recent backup to minimize data loss.

15.7.12 Post Restore Tasks

Perform these tasks after restoring the Audit Vault Server.

1. Update the Audit Vault Agents or the agentless collection service, depending on what you've deployed.
2. Update the Database Firewall instances.
3. Start audit data collection on the restored Audit Vault Server.
4. Configure secondary Network Interface Cards (NICs), if required.

Update Audit Vault Agents

Manually update Audit Vault Agents when restoring the Audit Vault Server with a new IP address so that they connect using the new IP address.

Follow these steps for Oracle AVDF release 20.4 and earlier:

1. Log in to the Agent machine.
2. In case of Audit Vault Agent, update the IP addresses in the `Agent_Home/av/conf/bootstrap.prop` file. In case of Host Monitor Agent, update the IP addresses in the

`Agent_Home/hm/bootstrap.prop` file. Replace all the old IP addresses with the new IP addresses.

3. Restart the Audit Vault Agent. The restart downloads the new `agent.jar` file from the Audit Vault Server with the new IP address. Refer to Stopping, Starting, and Other Agent Operations for more information.

> **Note:**
>
> Perform this operation on all the Audit Vault Agents and restart them.

Follow these steps for Oracle AVDF release 20.5 and later:

1. Log in to the Agent machine.
2. Stop the Audit Vault Agent.
3. Run the following command on the Agent machine:

Platform	Command
Windows	`agentctl.bat update_agent_configuration -ip [new ip address of AVS] -port [new TCP port of AVS ]`
Linux/Unix/AIX/Solaris	`agentctl update_agent_configuration -ip [new ip address of AVS] -port [new TCP port of AVS ]`

> **Note:**
>
> - In case the Audit Vault Server is in high availability configuration, enter the new IP address and port number of the primary Audit Vault Server.
> - In case of multiple network interface cards on Audit Vault Server, enter the new IP address corresponding to the card which is reachable from the Agent machine.

4. Restart the Audit Vault Agent. The restart downloads the new `agent.jar` file from the Audit Vault Server with the new IP address. Refer to Stopping, Starting, and Other Agent Operations for more information.

Update the Agentless Collection Service

If you're using agentless collection (Oracle AVDF 20.9 and later), the agentless collection service will not run on the restored machine if the backup Audit Vault Server and the restored Audit Vault Server are two different machines with different IP address.

If the backup Audit Vault Server and the restored Audit Vault Server are two different machines with different IP address, run the following commands to stop the agentless collection service on the backup Audit Vault Server and deploy and start agentless collection on the restored Audit Vault Server.

1. Enter the following commands to stop the agentless collection service on the backup Audit Vault Server:

```
su root

/usr/bin/systemctl stop monitor_default_agent.service

/usr/bin/systemctl disable monitor_default_agent.service

/usr/bin/systemctl stop monitor_default_agent.timer

/usr/bin/systemctl disable monitor_default_agent.timer

/usr/bin/systemctl stop default_agent.service

/usr/bin/systemctl disable default_agent.service
```

2. Enter the following commands to deploy and start agentless collection on the restored Audit Vault Server:

```
su root

/usr/local/dbfw/bin/deploy_default_agent.py
```

Update Database Firewall Instances

After restoring the Audit Vault Server on a new IP address is completed, the Audit Vault Server console certificate is invalid. The certificate details are pertaining to the backup system which is no longer valid. A new certificate must be generated and uploaded.

Copy the existing certificate to the Database Firewall server to reconnect. Refer to Specifying the Audit Vault Server Certificate and IP Address for more information.

Start Audit Data Collection on Restored Audit Vault Server

The audit trails must be started on the newly restored Audit Vault Server. The trails start collecting audit records from the time stamp when the Audit Vault Server was backed up.

> **Note:**
>
> - If audit trail cleanup is configured on the targets, then the audit data collected after the backup may be purged on the target. This data is not available for collection on a restored Audit Vault Server.
> - If audit trail cleanup is not configured on the targets, then the audit data collected after the backup is still available on the target. This data is available for collection on a restored Audit Vault Server.

Audit Vault Server Networking

The restore process is only restoring the management interface. All the secondary NICs and their associated network configuration has to be manually reconfigured and tested after restoring the Audit Vault Server.

Ensure the network interfaces are connected to the correct networks. Also ensure the new IP addresses and the network masks are correct. After restoring the Audit Vault Server appliance, ensure the following have been reconfigured correctly:

- Secondary NIC IP configuration
- Static routes
- Agent connectivity for secondary NICs
- Access for services (SSH, NTP, etc) previously configured for secondary NICs

> **See Also:**
>
> Multiple Network Interface Cards

15.7.13 Monitor the Restore Process

Learn about monitoring the Audit Vault Server restore process.

The restore process usually takes long time. The output can be monitored by checking the log files in the following locations:

- `/var/lib/oracle/dbfw/av/log/av.backup*`
- `TMP_DIR/av.backup_<timestamp>/*`

> **Note:**
>
> Since the restore operation takes a long time depending on the size of the backup, ensure the session used to run the command does not abruptly terminate. Oracle recommends to use commands like `/usr/bin/screen` to run restore commands.

Additional Information for Restoring Audit Vault Server

Here are some additional pointers for troubleshooting the Audit Vault Server restore process:

- Ensure the access to BACKUP_DIR directory is owned by `oracle:oinstall`.
- Ensure the OS user *root* on the restore system has access to `BACKUP_DIR` directory.
- In case of incorrect password, run the `avbackup config` command again to set the password right. This is applicable to password used to encrypt configuration data and not the keystore password.
- The script must be run as *root* user.
- The backup directory path on the restore system must be the same as the backup system. In case of NFS, it must be mounted on the same path as the backup system.
- In case `device busy` error is observed during restore, then contact Oracle Support for detailed steps for a workaround on the issue.

15.7.14 Restoring Audit Vault Server in High Availability

Learn how to restore Audit Vault Server in a high availability environment.

After restoring Audit Vault Server in a high availability environment, the system is a standalone. The restored system is not automatically configured for high availability. To set up high availability, pair the restored system with another new Audit Vault Server.

> **See Also:**
>
> Backup and Restore of Audit Vault Server in High Availability

15.8 Backing Up and Restoring the Database Firewall

You can back up and restore the Database Firewall instance.

The Database Firewall configuration is backed up automatically when the Audit Vault Server backup is taken. This does not require any additional action.

Restoring the Database Firewall Configuration on an Existing Database Firewall Instance

A copy of the Database Firewall configuration is stored on the Audit Vault Server. If required, it can overwrite the existing settings of the Database Firewall and maintain a copy of the same on the Audit Vault Server.

To restore the Database Firewall configuration from the Audit Vault Server, follow these steps:

1. Ensure the Audit Vault Server's certificate is installed on the Database Firewall. See Specifying the Audit Vault Server Certificate and IP Address for more information.
2. Ensure the IP address of the Database Firewall remains the same.
3. Follow the steps mentioned in section Resetting Database Firewall.

Restoring the Database Firewall Configuration on a New Database Firewall Instance

In case the Database Firewall instance has failed, it is possible to restore the Database Firewall settings on a newly installed system.

To restore the Database Firewall configuration on a new system, follow these steps:

1. Install the Database Firewall. See Configuring Database Firewall for complete information.

2. Configure the same IP address which was used during the previous configuration.
3. Install the Audit Vault Server's certificate on the Database Firewall. See Specifying the Audit Vault Server Certificate and IP Address for more information.
4. Update the Audit Vault Server with the new Database Firewall's certificate by following the instructions mentioned in section Fetching an Updated Certificate from Database Firewall.
5. To restore the Database Firewall configuration, follow the steps mentioned in section Resetting Database Firewall.

15.9 Enabling Oracle Database In-Memory for the Audit Vault Server

After you enable Oracle Database In-Memory, you can monitor it.

15.9.1 About Enabling Oracle Database In-Memory for Oracle Audit Vault Server

You can enable Oracle Database In-Memory for Oracle Audit Vault Server.

You can improve the performance of Oracle Audit Vault and Database Firewall reports and dashboards by enabling Oracle Database In-Memory in Oracle Audit Vault Server. This feature lets you allocate a certain amount of system memory for audit data for a specified period of time. The audit data residing in-memory then becomes available more quickly for use in dashboards and reports.

Based on the amount of system memory you allocate for Oracle Database In-Memory, and the average amount of data collected per day in your environment, Oracle Audit Vault and Database Firewall calculates the number of days of audit data that will fit into that allocated memory. From this calculation, the system displays the in-memory date range to Oracle Audit Vault and Database Firewall auditors, letting them know the time ranges for which they can obtain faster reports. For example, if 1 gigabyte can accommodate 2 days of data, and you have provided 1 gigabyte of memory for Oracle Database In-Memory, then 2 days of the latest data will be put in Oracle Database In-Memory. If you provide 2 gigabytes of memory to Oracle Database In-Memory, then 4 days of data will go to Oracle Database In-Memory.

Before enabling Oracle Database In-Memory, be sure to estimate the amount of memory needed for your current and future targets and Database Firewall monitoring points. You can find some guidelines for calculating RAM requirements in the Oracle Audit Vault and Database Firewall Sizing Advice (My Oracle Support Doc ID 2092683.1). This document can be obtained from Oracle Support. After estimating your normal RAM requirements, if you want to use the Oracle Database In-Memory feature, estimate how much RAM you want to use for in-memory database and add that to your RAM requirement. If you enable this feature, you must allocate at least 1 GB for Oracle Database In-Memory.

15.9.2 Enabling and Allocating Memory for Oracle Database In-Memory

You can enable and allocate memory for Oracle Database In-Memory from the Audit Vault Server console.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select select **System**.

4. Under **Configuration**, select **Oracle Database In-Memory**.
5. In the **Oracle Database In-Memory** dialog, select the **Enable Oracle Database In-Memory** check box.

   The Oracle Database In-Memory window expands to show the total system RAM.
6. If you have sufficient memory on your system, configure the following settings:
   - **Allocated In-Memory** field: Enter (or change) the amount of RAM to allocate in Gigabytes. You must enter a minimum of 1 (default), and up to **Maximum available for Database In-Memory** indicated on this dialog.
   - **Keep latest data** option: Select this option to retain the data that has just been collected. This setting enables the system to automatically select the most recent dates, based on the in-memory size that was configured.
   - **Select a date range** option: Select this option if you want the memory to be available for a specific period of time.
7. Click **Save**.

   After you enable or disable Oracle Database In-Memory, the Audit Vault Server database, Audit Vault Agents, and audit trails shut down for a few minutes, and then restart automatically.

15.9.3 Disabling Oracle Database In-Memory

You can disable Oracle Database In-Memory from the Audit Vault Server console.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **System**.
4. Under **Configuration** section, select **Oracle Database In-Memory**.
5. In the **Oracle Database In-Memory** window, select the **Enable Oracle Database In-Memory** check box to clear it. If enabled, the disable option is available in the dialog.
6. Click **Save**.

   After you enable or disable Oracle Database In-Memory, the Audit Vault Server database, Audit Vault Agents, and audit trails go down for a few minutes, and then restart automatically.

15.9.4 Monitoring Oracle Database In-Memory Usage

You can monitor the Oracle Database In-Memory usage from the Audit Vault Server console.

To see in-memory usage in the Audit Vault Server dashboard:

1. Click the **Settings** tab.
2. In the left navigation menu, select select **System**.
3. Under Configuration, select **Oracle Database In-Memory**.
4. The **Oracle Database In-Memory** dialog contains all the details.

15.10 Managing Plug-ins

You can use plug-ins to deploy additional target types in Oracle Audit Vault and Database Firewall environments.

You can deploy additional plug-ins to support more types of targets, or un-deploy plug-ins that are no longer needed.

> **See Also:**
>
> Deploying Plug-ins and Registering Plug-in Hosts

15.11 Monitoring and Adding Server Tablespace Space Usage

You can monitor and add server table space usage in Oracle Audit Vault Server.

Oracle Audit Vault Server contains the following tablespaces:

- `SYSTEM`
- `SYSAUX`
- `TEMP`
- `USERS`
- `UNDOTBS1`

By default, these tablespaces have one datafile.The tablespaces are locally managed with automatic segment space management.

You should monitor the space usage for the tablespace and create additional data files for storage as needed.

Starting with Oracle AVDF 20.9 the Audit Vault Server console will monitor the space remaining in the `SYSTEM, SYSAUX, and TEMP` tablespaces. You will receive system alerts when the remaining space is low and additional datafiles need to be added.

To add a datafile to any of the above tablespaces:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Switch to the `oracle` user.

   ```
   su - oracle
   ```

3. Connect as a `super administrator` user.

   ```
   sqlplus superadmin/superadmin_password
   ```

4. Run the following to add a 100MB datafile to the provided tablespace.

   ```
   execute avsys.datafile_management.add_datafile(tablespace_name);
   ```

Related Topics

- System Alerts
- Creating Data Files and Adding Data Files to a Tablespace
- Altering a SQL Profile

> **See Also:**
>
> - System Alerts for more information on how to receive notifications when tablespace is low in the Audit Vault Server.
> - Creating Data Files and Adding Data Files to a Tablespace in the *Oracle Database Administrator's Guide* for more information about the `ALTER TABLESPACE` SQL statement, which you can use to add more storage data files.
> - Altering a SQL Profile in the *Oracle Database SQL Tuning Guide* for more information about optimizing a tablespace.

15.12 Monitoring Server Archive Log Disk Space Use

You can monitor archive log disk space use to manage your system.

By default, `ARCHIVELOG` mode is disabled in Oracle Audit Vault Server. The `ARCHIVELOG` mode once enabled, copies the 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.

To change from `No Archive Mode` to `Archive Mode`, follow these steps:

1. Log in as *oracle* user.
2. Connect to SQL*Plus as *sysdba* user.
3. Run the command:

   ```
   SQL> archive log list;
   ```

   Observe the following output:

   ```
   Database log mode No Archive Mode
   Automatic archival Disabled
   Archive destination USE_DB_RECOVERY_FILE_DEST
   ```

4. In case the **Database log mode** is `No Archive Mode`, then run the following commands:

```
SQL> shutdown immediate;

SQL> startup mount;

SQL> alter database archivelog;

SQL> archive log list;
```

5. Observe the following output:

```
Database log mode Archive Mode
Automatic archival Enabled
Archive destination USE_DB_RECOVERY_FILE_DEST
```

6. Run the command:

```
SQL> alter database open;
```

> **Note:**
>
> - If you change the `ARCHIVELOG` mode during the backup configuration process, after the database restarts, then ensure the Java Framework internal tool is running on the Audit Vault Server.
> - Archivelog mode is required for hot backup.

> **See Also:**
>
> - *Oracle Database Administrator's Guide* for more information to set up archive log mode and other general information about Archive logs.
> - Method 1: Using the LOG_ARCHIVE_DEST_n Parameter for more information about changing the `LOG_ARCHIVE_DEST_n` location to relocate these archive log files to larger disks.
> - *Oracle Database Backup and Recovery User's Guide* for information about backing up the archive logs.

15.13 Monitoring Server Flash Recovery Area

Monitoring server flash recovery area is advisable to ensure you have enough space for backups.

By default, Oracle Audit Vault Server 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 your 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 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 increasing 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 Also:

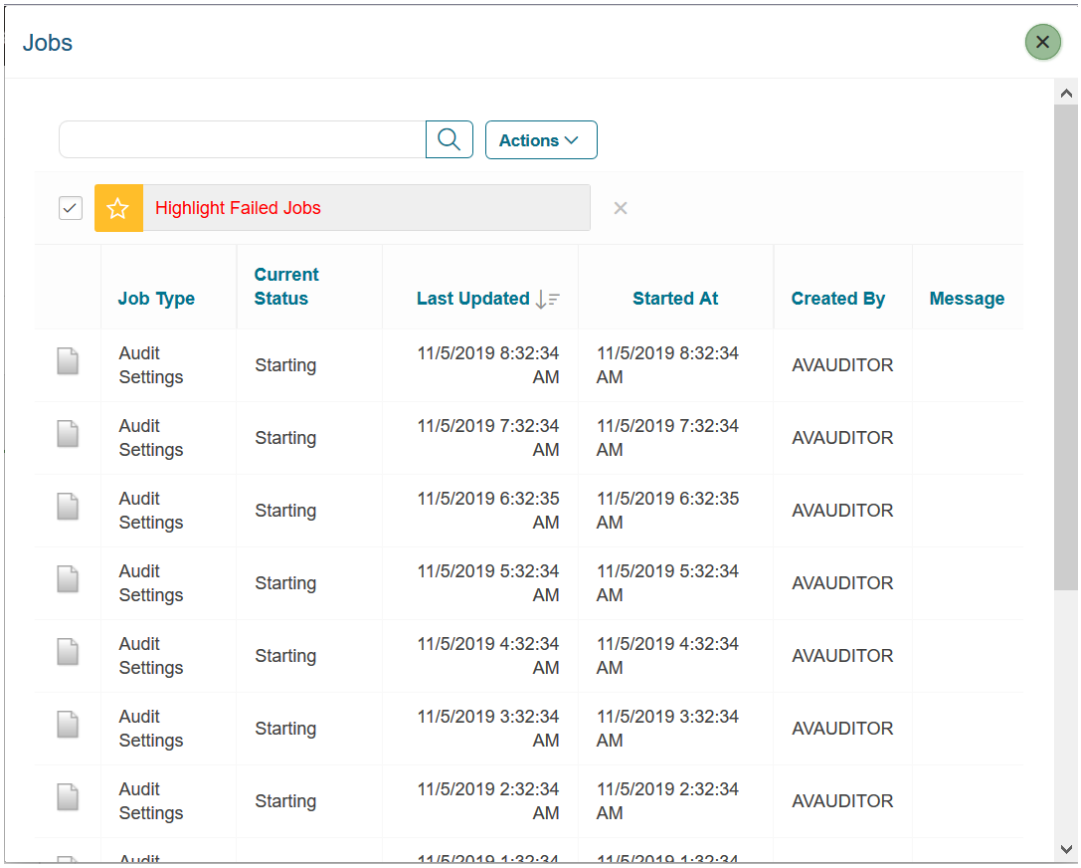
- *Oracle Database Administrator's Guide*
- *Oracle Database Backup and Recovery User's Guide*

15.14 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 targets.

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **System**.
4. In the **Status** page, under **Monitoring** section, click **Jobs**.

   The **Jobs** window appears, listing all the jobs that have been configured. It shows the job type, current status (such as Starting), when last updated, when started, who created the job, and any messages that may result from the job.



5. To see details for an individual job, click the **Job Details** icon to the extreme left of a specific job.

15.15 Schedule Maintenance Jobs

Oracle Audit Vault and Database Firewall (Oracle AVDF) runs some jobs on the Audit Vault Server for proper and effective functioning of the system.

Oracle recommends that you run these jobs during a period when the Audit Vault Server usage is low, such as at night. You can schedule these jobs based on your time zone.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. In the **Configuration** section, click one of the following links, depending on your release:

Oracle AVDF Release	Link
20.1 and 20.2	**Manage**
20.3 and later	**Maintenance**

5. To schedule a new maintenance job, enter the start time in hours and minutes.

   The time that you specify here is the time on the browser.
6. In the **Time Out (In hours)** field, enter the duration of the maintenance job in hours.

   If the job doesn't complete in the specified duration, it times out.

> **Note:**
>
> The job runs at the specified start time daily. You can't change the repeat frequency.

7. Click **Save**.

15.16 Downloading and Using the AVCLI Command Line Interface

You can download the AVCLI command line interface from the Audit Vault Server console.

15.16.1 About the AVCLI Command-Line Interface

Learn about the AVCLI command-line interface.

As an alternative to using the Oracle Audit Vault Server console (Web) UI, you can use the AVCLI command line interface to manage Oracle Audit Vault and Database Firewall, including registering and configuring 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.

> **Note:**
>
> Set the `JAVA_HOME` environment variable to point to JDK installation directory. On Windows, add `%JAVA_HOME%\bin` to the PATH environment variable.

> **See Also:**
>
> AVCLI Commands Reference for details of the available AVCLI commands.

15.16.2 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.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, select **Audit Vault CLI**.

4. Click the **Download AVCLI** button. Save the `avcli.jar` file.
5. Copy the `avcli.jar` file to the computer from which you want to run AVCLI. Run the 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
   ```

6. Set the `JAVA_HOME` environment variable to point to the JDK installation directory. On Windows, add `%JAVA_HOME%\bin` to the PATH environment variable.

15.16.3 Logging in to AVCLI

You can log in to the Audit Vault command line interface by using different methods.

15.16.3.1 About Logging in to AVCLI

You can log in to AVCLI interactively with or without a user name, and with stored credentials.

Before users log in, ensure that the `JAVA_HOME` environment variable in the server points to `JDK` installation directory. The user who logs in to AVCLI must be granted the granted the `AV_ADMIN` role, which you can grant by using the Audit Vault Server console.

The ways to log in are as follows:

- By supplying a user name and password by executing the `avcli` command
- Without supplying a user name and password, but you will be prompted for these credentials after you execute `avcli`
- By using a stored credential, which is useful for situations in which you must run scripts.

15.16.3.2 Logging in to AVCLI Interactively

You can start AVCLI interactively at the command line with or without a user name.

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.

1. Log in to the server where AVCLI is installed as a user who has been granted the `AV_ADMIN` role.
2. Go to the directory where AVCLI has been installed, and open `/bin`.

   ```
   cd ../directory_name/bin/
   ```

3. At the command line, use one of the following methods to log in to AVCLI:
   - **Logging in with a user name:** Use the following syntax:

     ```
     avcli -u username
     Enter password: password
     ```

     For example:

     ```
     avcli -u psmith
     AVCLI : Release 20.1.0.0.0 - Production on timestamp
     Copyright (c) 1996, 2020 Oracle.  All Rights Reserved.
     Enter password for 'psmith': password
     ```

```
Connected to:
Oracle Audit Vault Server 20.1.0.0.0

AVCLI>
```

- **Logging in without a user name:** Use the following syntax:

  ```
  avcli
  AVCLI> CONNECT [username];
  ```

  For example:

  ```
  avcli

  AVCLI : Release 20.1.0.0.0 - Production on timestamp
  Copyright (c) 1996, 2020 Oracle.  All Rights Reserved.

  AVCLI> CONNECT psmith
  Enter password: password;
  Connected.
  ```

  If you do not enter a user name, then you will be prompted for one.

15.16.3.3 Storing or Overwriting Administrative Credentials

If you are the AVCLI owner (that is, you installed the AVCLI utility) you can store the credentials of one Oracle AVDF administrator in the AVCLI wallet.

Thereafter, that administrator can invoke AVCLI without providing credentials, and can also run scripts without intervention.

As a prerequisite for an administrator to be able to invoke AVCLI without credentials (non-interactively), the AVCLI owner must store that administrator's credentials. As the AVCLI owner, you can store credentials for only one administrator.

1. As the AVCLI owner, run `avcli` without connecting to the Audit Vault Server.

   For example:

   ```
   avcli

   AVCLI : Release Release 20.1.0.0.0 - Production on timestamp
   Copyright (c) 1996, 2020 Oracle.  All Rights Reserved.

   AVCLI>
   ```

2. Run the command `STORE CREDENTIALS` and provide the administrator's credentials when prompted.

   For example:

   ```
   AVCLI> STORE CREDENTIALS;
   Enter user name: username
   Enter password:password
   Re-enter password:password
   ```

   Any previously stored credentials will be overwritten. If this administrator's password changes, follow this procedure again to store the new credentials.

15.16.3.4 Logging in to AVCLI Using Stored Credentials

To start AVCLI without having to enter credentials, your credentials must be stored in the Audit Vault Server.

1. Log in to the server where AVCLI is installed as a user who has been granted the `AV_ADMIN` role.
2. Use one of the following methods to log in to AVCLI using stored credentials:
   - **From the shell:** In the Audit Vault Server console, enter the following command, which logs you in to AVCLI and connects to the Audit Vault Server:

     ```
     avcli /@
     ```

   - **From within AVCLI:** If you have invoked AVCLI from the shell without credentials (by typing `avcli`), connect to the Audit Vault Server by entering:

     ```
     AVCLI> CONNECT /@;
     ```

     For example:

     ```
     avcli

     AVCLI : Release 20.1.0.0.0 - Production on timestamp
     Copyright (c) 1996, 2020 Oracle.  All Rights Reserved.

     AVCLI> CONNECT /@;
     Connected.
     ```

Related Topics

- Running AVCLI Scripts
  You can run AVCLI scripts without user intervention or putting credentials inside the script.

15.16.4 Running AVCLI Scripts

You can run AVCLI scripts without user intervention or putting credentials inside the script.

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;
```

1. Log in to the server where AVCLI is installed as a user who has been granted the `AV_ADMIN` role.
2. Use the following syntax to run the script:

   ```
   avcli -u username -f scriptname.av
   ```

   For example:

   ```
   avcli -u psmith -f myscript.av
   AVCLI : Release 20.1.0.0.0 - Production on timestamp
   Copyright (c) 1996, 2020 Oracle.  All Rights Reserved.
   ```

```
Enter password for 'psmith': password

Connected to:
Oracle Audit Vault Server 20.1.0.0.0

AVCLI> the script myscript.av executes
```

If you have stored administrator credentials, to run an AVCLI script, use the appropriate command below:

- `avcli /@ -f sample_script1.av`

  This command uses the stored credentials, connects to the Audit Vault Server, and runs the script.

- `avcli -f sample_script2.av`

  You can use the above command if you include the following command at the beginning of your script:

  ```
  connect /@
  ```

  Then the script runs using the stored credentials, and connecting to the Audit Vault Server.

Related Topics

- Logging in to AVCLI Using Stored Credentials
  To start AVCLI without having to enter credentials, your credentials must be stored in the Audit Vault Server.

15.16.5 Specifying Log Levels for AVCLI

When you run AVCLI, you can specify log levels to capture different categories of information or errors.

Oracle Audit Vault and Database Firewall 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 20.1.0.0.0 - Production on timestamp
Copyright (c) 1996, 2020 Oracle.  All Rights Reserved.
Enter password for 'psmith': password

Connected to:
Oracle Audit Vault Server 20.1.0.0.0

AVCLI>
```

To invoke AVCLI using a script and with the `debug` warning level:

```
avcli -l debug -f myscript.av
```

```
AVCLI : Release 20.1.0.0.0 - Production on timestamp
Copyright (c) 1996, 2020 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.

15.16.6 Displaying Help and the Version Number of AVCLI

You can display help information for various AVCLI commands and find the AVCLI version number from the command line.

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
```

15.17 Downloading the Oracle Audit Vault and Database Firewall SDK

An SDK is available for developing custom Oracle Audit Vault and Database Firewall plug-ins.

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Settings** tab.
3. In the left navigation menu, click **System**.
4. In the **Status** page that appears, under **Monitoring**, click **Plug-ins**.
5. In the **Plug-ins** window, do not select any of the plug-ins.
6. Click **Download SDK**.
7. Select **Save File** and then specify a location.

Related Topics

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

15.18 Managing Database Firewalls

Management tasks for Database Firewalls include tasks such as changing the network or services configuration.

15.18.1 Changing the Database Firewall Network or Services Configuration

Learn how to change the Database Firewall 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 Network Settings for Oracle Database Firewall"

- "Configuring Network Services for Oracle Database Firewall"
- "Configuring Network Settings"
- "Configuring the Database Firewall As a Traffic Proxy"

15.18.2 Viewing Network Traffic for a Database Firewall

You can capture and view network traffic in a `.pcap` file that you can download and analyze for debugging.

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Database Firewalls** tab.
3. In the left navigation menu, click **Database Firewalls**.
4. Click the link for the Database Firewall instance for which you want to capture network traffic.
5. Under **Diagnostics**, click **Network Traffic Capture**.
6. In the **Network Traffic Capture** dialog box, select the network traffic source in the **Network Interface** field.
7. For **Duration (min)**, set the number of minutes for which you want to capture traffic.
8. Click the **Capture** button.

   After the specified duration, a message appears saying that the network files were successfully captured and the captured traffic file appears in the table.

   > **Note:**
   >
   > The maximum file size of the captured network traffic is 1 MB. As soon as the file reaches that size, traffic capture stops, regardless of the specified duration. To capture traffic for longer durations, you can use a network protocol analyzer like Wireshark. For more details, see My Oracle Support Doc ID 2085200.1 and Doc ID 1141588.1.

9. Select the network traffic file, and click **Download**.
10. Specify the location and download the traffic file in `.pcap` format.

15.18.3 Restarting or Powering Off Database Firewall

Use this procedure to restart or power off Database Firewall.

To restart or power off a Database Firewall:

1. Log in to the Audit Vault Server as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Select the specific Database Firewall you want to reboot or power off.
4. Click the **Reboot** or **Power Off** button.

> **See Also:**
>
> Using Audit Vault Server Console

15.18.4 Removing Database Firewall from Audit Vault Server

You can remove Database Firewall from Audit Vault Server.

To remove Database Firewall from Audit Vault Server:

1. Log in to the Audit Vault Server as an *administrator*.
2. Click the **Database Firewalls** tab.
3. Select the specific Database Firewall you want to remove.
4. Click the **Delete** button.

> **See Also:**
>
> Using Audit Vault Server Console

15.18.5 Fetching an Updated Certificate from Database Firewall

Learn how to obtain updated certificates from Database Firewall.

You can update the Database Firewall certificate stored in the Audit Vault Server using the Audit Vault Server console. You must update this certificate when you upgrade the Database Firewall to maintain communication between the Database Firewall and the Audit Vault Server.

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. Select the **Database Firewalls** tab.
3. In the left navigation menu, select **Database Firewalls** tab.
4. Select the specific Database Firewall instance from the list.
5. If the Database Firewall instance is down due to certificate validation error, then the **Update Certificate** button appears on the page. Click this button to update the certificate.

> **See Also:**
>
> Using Audit Vault Server Console

15.18.6 Viewing Diagnostics for Database Firewall

> **See Also:**
>
> Viewing the Status and Diagnostics Report for Database Firewall for viewing Database Firewall diagnostics.

15.18.7 Resetting Database Firewall

Learn how to reset the Database Firewall instance.

This block contains information about the Database Firewall settings and the details of resetting a Database Firewall instance. The **Reset Firewall** button is available in the page that contains details of the specific Database Firewall instance. It performs a reset of the Firewall ID. The Firewall ID is a unique identification number of the Database Firewall. It is derived from the Management Interface card.

Once the reset is performed, it removes the existing monitoring point instances and creates new ones using the configuration information stored in Audit Vault Server. The monitoring point instances not listed on the Audit Vault Server are removed once the reset is performed. The captured data which is not processed is also deleted. The network setting (Management Interface) of the Database Firewall is not altered. This operation restores the network interface card settings other than the Management Interface. It also restores the proxy ports information that was stored in the Audit Vault Server.

> **Note:**
>
> - Whenever the Network Interface Card is replaced, the Database Firewall ID must be reset.
> - The network setting (Management Interface) of the Database Firewall is not altered. Ensure the Database Firewall network is configured appropriately before attempting to reset Firewall ID.

The user must reset the Firewall ID in the following scenarios:

1. After replacing the Management Interface card on the Database Firewall.
2. After replacing an existing and configured Database Firewall instance with a newly installed Database Firewall instance.

15.18.8 Restoring Database Firewall Monitoring Points

Learn how to restore Database Firewall monitoring points.

When you restore the Audit Vault Server from a backup, you must restore the status of the Database Firewall monitoring points that are registered with the Database Firewall.

> **See Also:**
>
> Resetting Database Firewall for more information.

15.19 System Alerts

System Alerts allow administrators to be notified about important system states and possible issues, including, the status of standby servers for high availability, storage availability, certificate expiration, and password expiration through the admin dashboard.

15.19.1 About System Alerts

System alerts allow administrators to be notified of important system statuses and possible issues through the Oracle Audit Vault Server console in Oracle Audit Vault and Database Firewall (Oracle AVDF) 20.9 and later.

System Alerts provide Oracle AVDF administrator users with proactive information necessary for maintaining important Oracle AVDF components. They can help you identify system failures before they happen and improve the stability and reliability of your Oracle AVDF system. The status of different components and processes are checked every six hours. If there are any issues a system alert will be generated for one of the following:

- The status of high availability of Audit Vault Server.
- The utilization of the Audit Vault Server Fast Recovery Area in a high availability environment.
- The Apply Lag on Audit Vault Server. Apply lag is the degree to which the data in Standby Server lags behind the data in the Primary Server.
- The storage availability in the Audit Vault Server file systems, directories, tablespaces, and disk groups.
- The expiration of Audit Vault Server, Audit Vault Agent, and Database Firewall certificates.
- The expiration of Audit Vault Server passwords for administrators, auditors, and operating system users (support and root).

To learn more about the specific system alerts and the recommended resolution, see System Alerts and Recommendations.

15.19.2 Configuring or Modifying System Alert Email Notifications

Starting in Oracle AVDF 20.10, you can configure email notifications for system alerts. This allows you to receive an email whenever a critical or high severity system alert occurs. The email you receive will contain the system alert category and severity in the email subject. The system will check if any email notifications need to be sent out every six hours.

Configuring or Modifying System Alert Email Notifications

Prerequisites:

The connection between your email and Oracle AVDF needs to be configured. See Configuring the Email Notification Service for more information.

To configure or modify email notifications for system alerts:

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. In the System Alerts section,
   - If configuring for the first time, click **Click here**.
   - If modifying, click **Email Notification**.

   A dialog box will appear.
5. In the **To** field, enter the email(s) you would like to receive system alert notifications. Each email address can be comma or semicolon separated.
6. Optionally, in the **Subject** field, enter the Email Subject you want to receive for system alerts. By default, "AVDF System Alerts" will be used as part of the subject. In addition, the email subject will contain the system alert category and severity.
7. Click **Save**.

Example 15-1 Email Notification for One Alert

If the Subject field was left blank and there is one system alert with high severity under Storage category, the email subject will be "AVDF System Alerts: Storage - High".

Example 15-2 Email Notification for Multiple Alerts

If the Subject was set to “Oracle AVDF System Alerts”, and there are multiple system alerts in the system such as:

- A critical severity alert in the High Availability category
- A critical severity alert in the Password category
- A high severity alert in the Storage category

The email subject will be “Oracle AVDF System Alerts: High Availability - Critical, Password - Critical, Storage - High”.

Adjusting the Frequency of the Background Job For System Alert Email Notifications

By default, email notifications are sent out every six hours. This frequency can be adjusting by performing the following steps:

1. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

2. Run the following command on SQL*Plus as the `avsys` user:

```
exec
dbms_scheduler.set_attribute('avsys.avs_email_notification_job','repeat_int
erval','FREQ=<YEARLY
      | MONTHLY | WEEKLY | DAILY | HOURLY | MINUTELY |
SECONDLY>;INTERVAL=<1-99>');
```

3. Lock the `avsys` user.

   See Locking the AVSYS User.

Example 15-3 Adjust the Email Notification Schedule to Daily

```
exec
dbms_scheduler.set_attribute('avsys.avs_email_notification_job','repeat_interv
al','FREQ=DAILY;INTERVAL=1');
```

Example 15-4 Adjust the Email Notification Schedule to Every 30 Minutes

```
exec
dbms_scheduler.set_attribute('avsys.avs_email_notification_job','repeat_interv
al','FREQ=MINUTELY;INTERVAL=30');
```

15.19.3 Viewing System Alerts

System Alerts can be viewed from the admin dashboard, directly from the System tab in the Audit Vault Server console, or in the `syslog`.

Viewing alerts from the dashboard:

1. Log in to the Audit Vault Server Console as an `administrator`.
2. Click on the system alerts chart from the admin dashboard. This will bring you to the **System** page.
3. View the system alerts in the System Alerts section at the bottom of the page.
4. Click on a system alert to view the history of that alert. A pop-up will show a list of alerts based on the selected alert. The alert history will show a maximum history of three months.

Viewing alerts from the System tab:

1. Log in to the Audit Vault Server Console as an `administrator`.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. View the system alerts in the System Alerts section at the bottom of the page.
5. Click on a system alert to view the history of that alert. A pop-up will show a list of alerts based on the selected alert. The alert history will show a maximum history of three months.

Viewing alerts from the `syslog`.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. View system alerts in the `syslog (/var/log/messages)` by filtering for the `AVDF SYSTEM ALERT` tag.

For descriptions of the severity levels, see System Alerts Severity Levels.

For a list of possible alerts and recommendations, see System Alerts and Recommendations.

15.19.4 Closing System Alerts

Once an error condition is fixed, a `super administrator` user can close a system alert.

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click the **Settings** tab.
3. Click **System** in the left navigation menu.
4. In the System Alerts section, select one or more system alerts that you'd like to close.
5. Click **Close System Alerts**.

Once an alert is closed, the same alert will not be displayed within 24 hours, even if the error condition is met again. After 24 hours a new system alert will be generated if the error condition is met.

For descriptions of the severity levels, see System Alerts Severity Levels.

For a list of possible alerts and recommendations, see System Alerts and Recommendations.

15.19.5 System Alerts Severity Levels

System alerts include the following severity levels:

- **Critical**: This severity means that some functionality of the system is not working or will stop working soon. For example, in case of high availability, Fast Recovery Area is more than 80% full or agent certificate is going to expire in five days etc.
- **High**: This severity means that some functionality of the system will stop working in some time. For example, in case of high availability Fast Recovery Area is more than 70% full but less than 80% or agent certificate is going to expire in six weeks.
- **Medium**: This severity means that some functionality of the system may stop in the future or is not performing as expected.
- **Low**: This severity is for information that needs some user attention, but there is no functionality failure expected in near future.

16
Extending Storage

If Oracle AVDF requires more space than was originally allocated, you can extend the storage for the file system and for the collected data.

16.1 Extending File System Storage

If Oracle AVDF requires more space than was originally allocated, you can extend the storage for the file system.

16.1.1 About Extending Storage

You can allocate space in the volume group to extend the storage for a file system. You can add physical storage to extend the storage for the volume group.

You have the following options for extending storage:

- If an Oracle AVDF folder runs out of space, you can allocate more space to the logical volume that holds the file system.

  Oracle AVDF reserves a small amount of space in the volume group so that you can allocate it to any file system that needs more space. The space requirements depend on the workload, so you can evaluate needs and allocate the extra space when and where it's needed.
- If the volume group itself needs more space, you can add more physical storage, like adding an solid state drive (SSD) or allocating space from a storage area network (SAN) repository.

16.1.2 Increasing the Logical Volume Capacity for a File System

If an Oracle AVDF file system runs out of space, you can allocate more space to the logical volume that holds the file system.

Use the `lvextend` command to increase the logical volume capacity. The `vg_root` volume group normally has unallocated space for this purpose.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run `vgs` to check the volume group free space. For example:

   ```
   /usr/sbin/vgs
   VG      #PV #LV #SN   Attr   VSize  VFree
   vg_root   1  13   0 wz--n- 149.84G 10.72G
   ```

   For more detailed volume group information, run `vgdisplay`.
3. Increase the logical volume capacity.

For example, the following command adds 2 GB to the `/tmp` folder from the `VG_ROOT` volume group:

```
/usr/sbin/lvextend -r -L+2G /dev/mapper/vg_root-lv_tmp
```

Related Topics

- Configure Logical Volumes on Oracle Linux

16.1.3 Adding a Disk to a Volume Group

If the `vg_root` volume group needs more space for patching, upgrading, or another purpose, you can add a disk and extend the volume group to the new disk.

> **Caution:**
>
> Each additional physical device that is added to the volume group adds an additional single point of failure, unless the physical devices are hosted on the same back-end storage such as on a SAN or virtual environment. This document does not cover how to make the volume group resilient. To find more information about how to make the volume group resilient through RAID, see Configure RAID Logical Volumes on Oracle Linux

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run `vgs` to check the volume group free space. For example:

```
/usr/sbin/vgs
VG      #PV #LV #SN   Attr   VSize  VFree
vg_root   1  13   0 wz--n- 149.84G 10.72G
```

3. Run `lsblk` to view a list of all the available hard disks. For example:

```
lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 256G 0 disk
        sda1 8:1 0 200M 0 part
        sda2 8:2 0 1G 0 part
        sda3 8:3 0 160.2G 0 part
                vg_root-lv_ol8root 252:0 0 6.6G 0 lvm /
                vg_root-lv_swap 252:1 0 15.3G 0 lvm [SWAP]
                vg_root-lv_images 252:2 0 488M 0 lvm
                vg_root-lv_var_dbfw 252:3 0 2.9G 0 lvm /var/dbfw
                vg_root-lv_oracle 252:4 0 58.6G 0 lvm /var/lib/oracle
                vg_root-lv_tmp 252:5 0 1.9G 0 lvm /tmp
                vg_root-lv_var_log 252:6 0 5.7G 0 lvm /var/log
                vg_root-lv_home 252:7 0 976M 0 lvm /home
                vg_root-lv_opt 252:8 0 976M 0 lvm /opt
                vg_root-lv_var_tmp 252:9 0 5.7G 0 lvm /var/tmp
                vg_root-lv_local_dbfw_tmp 252:10 0 6.6G 0 lvm /usr/local/
dbfw/tmp
                vg_root-lv_local_dbfw 252:11 0 976M 0 lvm /usr/local/dbfw
```

```
        sda4 8:4 0 31.6G 0 part
        sda5 8:5 0 31.6G 0 part
        sda6 8:6 0 31.6G 0 part
sdb 8:16 0 2T 0 disk
sr0 11:0 1 1024M 0 rom
sr1 11:1 1 1024M 0 rom
```

4. From the list, locate a disk with no partitions defined and with the same size that you need.
5. Use the `parted` command to create the partition.
   a. Run `parted /<path of the disk>` using the path of the disk that you identified in step 4. For example:

      ```
      /sbin/parted /dev/sdb

      GNU Parted 3.2
      Using /dev/sdb
      Welcome to GNU Parted! Type 'help' to view a list of commands.
      (parted)
      ```

   b. Run `mklabel gpt` to set the disk label to `GPT`. For example:

      ```
      (parted) mklabel gpt
      (parted) print

      Model: XXX VBOX HARDDISK (scsi)
      Disk /dev/sdb: 2199GB
      Sector size (logical/physical): 512B/512B
      Partition Table: gpt

      Number Start End Size File system Name Flags

      (parted)
      ```

   c. Run the `mkpart primary ext3` command to create the partition.

      When prompted, enter `0GB` as the start point and specify another size of the first partition as the end point.

      For example, to create three partitions and to use `314GB` as the end of partition 1, use the following command:

      ```
      (parted) mkpart primary ext3
      Start? 0GB
      End? -1
      (parted)
      ```

   d. Set the partition type to `LVM`.

      In this example, the partition number is `1`, and you can use the `print` command to verify the change.

      ```
      (parted) set 1 lvm on
      (parted) print
      Model: XXX VBOX HARDDISK (scsi)
      ```

```
Disk /dev/sdb: 2199GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Number Start    End    Size File system Name Flags
1     1049kB 2199GB 2199GB ext3 primary lvm
(parted)
```

e. Run `quit` to exit `parted`. The changes are automatically saved.

6. Run `pvcreate` to create the physical volume using the added disk. For example:

```
/usr/sbin/pvcreate /dev/sdb1
Writing physical volume data to disk "/dev/sdb1"
Physical volume "/dev/sdb1" successfully created
```

7. Verify the creation with `pvdisplay`.

   You should now have two physical volumes: `vg_root` and the one you just created. For example:

```
/usr/sbin/pvdisplay
--- Physical volume ---
PV Name               /dev/sda3
VG Name               vg_root
PV Size               <160.16 GiB / not usable 4.00 MiB
Allocatable           yes
PE Size        4.00 MiB
Total PE              40999
Free PE               13724
Allocated PE          27275
PV UUID               4Fup6c-ruea-0B20-s9Sn-66on-4sVf-fDON2D

"/dev/sdb1" is a new physical volume of "<2.00 TiB"
--- NEW Physical volume ---
PV Name               /dev/sdb1
VG Name
PV Size               <2.00 TiB
Allocatable           NO
PE Size (KByte)       0
Total PE              0
Free PE               0
Allocated PE          0
PV UUID               uDgKdm-LawO-4cXB-Bjog-pZ48-gNHD-fQE1IE
```

8. Run `vgextend` to extend the `vg_root` volume group to the added disk. For example:

```
/usr/sbin/vgextend vg_root /dev/sdb1
Volume group "vg_root" successfully extended
```

9. Run `vgs` again and compare it to the output from step 2.

   You should see more free space available for the `vg_root` volume group. For example:

```
/usr/sbin/vgs
VG      #PV #LV #SN   Attr   VSize  VFree
vg_root   2  13   0 wz--n- 199.81G 60.69G
```

In the examples throughout this procedure, you can see that the `VSize` has increased from 149.84 G to 199.81 G.

Related Topics

- Configure Logical Volumes on Oracle Linux
- Monitoring and Adding Server Tablespace Space Usage
  You can monitor and add server table space usage in Oracle Audit Vault Server.

16.2 Extending Storage for Collected Data

If Oracle AVDF requires more space than was originally allocated for the collected data, you can add local disks or configure a storage area network (SAN).

16.2.1 Adding Local Disks to the Audit Vault Server ASM Disk Groups

To increase storage, you can add local disks to the Oracle Automatic Storage Management (ASM) disk groups for the Audit Vault Server.

This procedure discusses how to add storage to all three ASM disk groups. However, it may not be necessary to increase the storage for all three. Use your discretion to add storage where it's needed.

> **Note:**
>
> For Oracle AVDF installations that are hosted on VMware, don't extend the current virtual disk. Instead, add a new virtual disk device.

Prerequisite

Ensure that any disks that you added to the Oracle AVDF appliance have no preexisting Local Volume Manager (LVM), partition, or other device mapper metadata. If the disks have been used previously, then restore them to a clean state before completing this procedure.

Procedure

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Run `fdisk -l` to view a list of all the available hard disks. For example:

```
/sbin/fdisk -l 2> /dev/null | more
Disk /dev/sda: 322.1 GB, 322122547200 bytes
255 heads, 63 sectors/track, 39162 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot Start   End    Blocks  Id  System
/dev/sda1    *     1    19    152586  83  Linux
/dev/sda2         20 10727  86012010  8e  Linux LVM
/dev/sda3      10728 22914  97892077+ 83  Linux
/dev/sda4      22915 39162 130512060   5  Extended
/dev/sda5      22915 31037  65247966  83  Linux
/dev/sda6      31038 39162  65264031  83  Linux

Disk /dev/sdb: 107.3 GB, 107374182400 bytes
```

```
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

3. From the list, locate a disk with no partitions defined and with the same size that you need. Ignore any entries referring to `/dev/dm-0`, and so on.

   In the example in step 2, a SATA disk of 100 GB was added, so the target in that example would be `/dev/sdb`.

> **Note:**
>
> - Fiber Channel-based storage with multipath is supported starting with Oracle AVDF 20.1.
>
>   Here's an example of the multipath device: `/dev/mpatha`
>
>   To get a list of existing multipath devices, run the `multipath -ll` command.
> - Fiber Channel over Ethernet (FCoE) is currently not supported by Oracle AVDF.

4. Use the `parted` command to create the partitions.

   a. Run `parted /<path of the disk>` using the path of the disk that you identified in step 3. For example:

   ```
   /sbin/parted /dev/sdb

   GNU Parted 1.8.1
   Using /dev/sdb
   Welcome to GNU Parted! Type 'help' to view a list of commands.
   (parted)
   ```

   Oracle recommends that all ASM disks in a disk group should be the same size. For example, if the SYSTEMDATA disk group has a 5 GB disk and you want to add another disk, it should also be 5 GB. This is because Oracle ASM stripes the files in the disk group across each disk. If the disks are mismatched in size, the smallest disk limits the size of the whole disk group. After the smallest disk is 100 percent full, you can't rebalance until space on that disk is freed.

   b. Run `mklabel gpt` to set the disk label to `GPT`. For example:

   ```
   (parted) mklabel gpt
   (parted) print

   Model: ATA VBOX HARDDISK (scsi)
   Disk /dev/sdb: 107GB
   Sector size (logical/physical): 512B/512B
   Partition Table: gpt

   Number Start End Size File system Name Flags

   (parted)
   ```

   c. Run the `mkpart primary ext3` command to create the partition.

When prompted, enter `0GB` as the start point and specify another size of the first partition as the end point.

For example, to create three partitions and to use `35GB` as the end of partition 1, use the following command:

```
(parted) mkpart primary ext3
Start? 0GB
End? 35GB
(parted)
```

d. Run the `mkpart` command to create the second partition. For example:

```
(parted) mkpart primary ext3
Start? 35GB
End? 70GB
(parted)
```

e. Run the `mkpart` command to create the third partition. For example:

```
(parted) mkpart primary ext3
Start? 70GB
End? 107GB
(parted) print
```

The end point GB should match the total GB for the disk that appears in the output of step 4b.

f. Run `quit` to exit `parted`. The changes are automatically saved.

5. Run `oracleasm createdisk` to create the ASM disks. For example:

```
/usr/sbin/oracleasm createdisk -v EVENTDATA2 /dev/sdb1
Disk "EVENTDATA2" does not exist or is not instantiated
Writing disk header: done
Instantiating disk: done
```

> **Note:**
>
> If this command fails, then remove all the data and partitions from the new disk and repeat all the preceding steps.

6. Add the new disks to the existing ASM disk groups.

a. Run the following commands to change to the `grid` user and connect to the grid instance as `sysasm` to manage the existing ASM disk groups:

```
su - grid


id


sqlplus /nolog


sqlplus / as sysasm
```

b. Check the current status of the existing ASM disks and disk groups.

```
select GROUP_NUMBER,NAME,TOTAL_MB,FREE_MB from V$ASM_DISKGROUP;
```

For example:

```
GROUP_NUMBER NAME        TOTAL_MB FREE_MB
------------ ----        -------- -------
1            EVENTDATA   63718    62557
2            RECOVERY    95597    91924
3            SYSTEMDATA  63734    60577


column MOUNT_STATUS format a12
column HEADER_STATUS format a12
column MODE_STATUS format a10
column STATE format a10
column TOTAL_MB format 999999
column FREE_MB format 999999
column NAME format a20
column PATH format a40
column LABEL format a10
column LABEL format a1
set linesize 250

SELECT
MOUNT_STATUS,HEADER_STATUS,MODE_STATUS,STATE,TOTAL_MB,FREE_MB,NAME,PATH,
LABEL FROM V$ASM_DISK;
```

For example:

```
MOUNT_STAT HEADER_STATUS  MODE_STATUS   STATE   TOTAL_MB FREE_MB
NAME             PATH                            LABEL
---------- ------------  -----------   -----   -------- -------
----             ----                            -----
CLOSED     PROVISIONED    ONLINE        NORMAL  0
0                         /dev/oracleasm/disks/RECOVERY2
CLOSED     PROVISIONED    ONLINE        NORMAL  0
0                         /dev/oracleasm/disks/SYSTEMDATA2
CLOSED     PROVISIONED    ONLINE        NORMAL  0
```

```
0                         /dev/oracleasm/disks/EVENTDATA2
CACHED     MEMBER         ONLINE        NORMAL  63734    60577
SYSTEMDATA_0000  /dev/oracleasm/disks/SYSTEMDATA1
CACHED     MEMBER         ONLINE        NORMAL  63718    62557
EVENTDATA_0000   /dev/oracleasm/disks/EVENTDATA1
CACHED     MEMBER         ONLINE        NORMAL  95597    91924
RECOVERY_0000    /dev/oracleasm/disks/RECOVERY1
6 rows selected.
```

c. Use `ALTER DISKGROUP` to add the new disks to the disk groups. For example:

```
SQL> ALTER DISKGROUP EVENTDATA add disk 'ORCL:EVENTDATA2';
Diskgroup altered.
```

d. Verify the increase in storage space. For example:

```
SQL> select GROUP_NUMBER,NAME,TOTAL_MB,FREE_MB from V$ASM_DISKGROUP;

GROUP_NUMBER NAME       TOTAL_MB FREE_MB
------------ ----       -------- -------
1            EVENTDATA  97096    95933
2            RECOVERY   131239   127564
3            SYSTEMDATA 97112    93953
```

Related Topics

- Configuring a SAN Repository
  Learn how to configure, discover targets, and add and drop disks for an Oracle Audit Vault and Database Firewall storage area network.

16.2.2 Configuring a SAN Repository

Learn how to configure, discover targets, and add and drop disks for an Oracle Audit Vault and Database Firewall storage area network.

16.2.2.1 About Configuring a SAN Repository

You can configure an Oracle Audit Vault storage area network (SAN) for event data, system data, recovery data, and for high availability.

You can use storage area networks (SANs) to expand your data storage, and manage high availability.

Types of Data Supported for SANs

You have the option to configure a SAN storage repository for these data types:

- **Event Data** - Data that is kept online in the Oracle 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 Audit Vault and Database Firewall system
- **Recovery** - Recovery data for the Oracle Audit Vault Server repository

During the Oracle Audit Vault Server installation process, your server is 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.

About Configuring a SAN Repository When Federal Information Processing Standards (FIPS) is Enabled on the Audit Vault Server

Challenge-Handshake Authentication Protocol (CHAP) should be disabled on the SAN server when FIPS is enabled.

About Configuring a SAN Repository in High Availability Environments

In a high availability environment, you can configure the storage repository on the secondary Oracle Audit Vault Server from the primary Oracle Audit Vault Server, using either the console UI or AVCLI commands. The primary and secondary Oracle 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.

16.2.2.2 Configuring a SAN Server to Communicate with Oracle Audit Vault and Database Firewall

To configure a storage area network (SAN) for Oracle Audit Vault and Database Firewall, complete this procedure.

Oracle Audit Vault and Database Firewall 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 Audit Vault and Database Firewall 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.

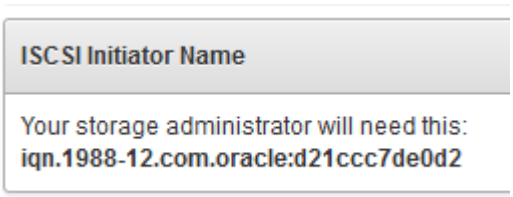
> **Note:**
>
> - Ensure that you do not have more than one target mapped to the same disk on the SAN storage server.
> - Multipath is not supported with ISCSI storage.

Some SAN servers may also require the Oracle Audit Vault Server's IP address.

To find the Oracle Audit Vault Server's iSCSI initiator name and IP address:

1. Log in to the Oracle 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 see two iSCSI initiator names: one for the primary Oracle Audit Vault Server, and one for the secondary.

3. To find the Oracle Audit Vault Server's IP address, click the **Settings** tab, and then click **Network**. The IP address is at the top of this page.

> **Note:**
>
> Do not restart the iSCSI service on either the Oracle Audit Vault Server, or the SAN server that is servicing the Oracle Audit Vault Server. If there is a need to restart either of these services, then contact Oracle Support.

16.2.2.3 Registering or Dropping SAN Servers in the Oracle Audit Vault Server

You can register or drop a storage area network server for Oracle Audit Vault.

16.2.2.3.1 Registering a SAN Server

To register a storage area network (SAN) server to the Oracle Audit Vault server, complete this procedure.

In a high availability environment, you can use this procedure to register a SAN server to the primary or the secondary Oracle Audit Vault Server. Note that while you can register the same SAN server to both the primary and secondary Oracle Audit Vault Servers, they must not share (read or write to) the same SAN disks.

> **Note:**
>
> Multipath is not supported with ISCSI storage.

To register a SAN server in the Audit Vault Server:

1. If you plan to use Internet Small Computer System Interface (iSCSI) as a target, then ensure that it is not shared with other systems. The iSCSI target must be exclusive to the Audit Vault Server.
2. Log in to the Audit Vault Server as a super administrator.
3. Click the **Settings** tab, and then click **SAN**.
4. 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 Oracle Audit Vault Server is authenticated by the SAN server.

5. Click **Submit**.

16.2.2.3.2 Dropping a SAN Server

To drop a storage area network (SAN) server from the Oracle Audit Vault Server, complete this procedure.

You can drop a SAN server if none of its disks are in use for storage in the Oracle Audit Vault Server repository. Otherwise, you must first drop the disks from any disk groups that use this SAN server.

To drop a SAN server from the Audit Vault Server:

1. Log in to the Oracle Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.
3. Select the SAN servers that you want to drop, and then click **Drop**.

Related Topics

- Dropping SAN Disks from the Audit Vault Server Repository
  Learn how to drop a SAN disk from a disk group.

16.2.2.4 Discovering Targets on a SAN Server

Find out how to discover and manage storage area network (SAN) targets for Oracle Audit Vault and Database Firewall.

16.2.2.4.1 About SAN Targets and Disks

To make storage area network disks available to Oracle Audit Vault and Database Firewall, you must discover storage area network servers, and then log in to available targets.

After you have registered SAN servers in the Audit Vault Server, to make SAN disks available for storing Audit Vault Server data, you must discover and log in to the available targets 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.

16.2.2.4.2 Discovering Targets on a SAN Server and Making Disks Available

Discover targets on a storage area network (SAN) server that is registered with the Audit Vault Server.

To make SAN server disks available for storing Audit Vault Server data, you must log in to a target on the SAN server, and then 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, then you can leave those fields empty and click **Log in**.

Related Topics

- Registering a SAN Server
  To register a storage area network (SAN) server to the Oracle Audit Vault server, complete this procedure.

16.2.2.4.3 Logging Out of Targets on SAN Servers

Learn how to log out of SAN server targets.

You can log out of a target if none of its disks are in use for storing Audit Vault Server data. If a disk from a target is in use, then you must first drop the disk and then log out of the target.

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.

> **See Also:**
>
> Dropping SAN Disks from the Audit Vault Server Repository

16.2.2.5 Adding or Dropping SAN Disks in the Audit Vault Server Repository

Find out about storage area network (SAN) disk groups, and how to add or drop them from the Oracle Audit Vault Server repository.

16.2.2.5.1 About Disk Groups in the Oracle Audit Vault Server Repository

You can add disk groups for the three data types to the repository, and you can make these disk groups highly available.

Log in to the Audit Vault Server console as super administrator. Click the **Settings** tab, and then click the **Storage** tab in the left navigation menu. The **Repository** sub tab can be accessed from the main page.

Adding Disk Groups to the Repository sub tab

There are three disk groups used for storing Oracle 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. Else, these data types are stored in disk partitions on the Audit Vault Server.

Adding SAN disks to these disk groups is optional.

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.

The Repository sub tab in a High Availability Environment

In a high availability environment, you see the disk groups in the Repository page for the Primary Oracle Audit Vault Server, followed by the same disk groups for the Secondary Oracle 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.

Related Topics

- About Configuring a SAN Repository
  You can configure an Oracle Audit Vault storage area network (SAN) for event data, system data, recovery data, and for high availability.

16.2.2.5.2 Adding SAN Disks to the Audit Vault Server Repository

To add storage area network (SAN) disks to the Oracle Audit Vault Server repository, use this procedure.

You can add SAN disks that are not already in use to any of the disk groups in the repository.

> **Note:**
>
> Adding an additional disk creates two `VG_ROOT` volume groups. When you have two `VG_ROOT` disks, this results in failure during upgrade. Ensure that any disk added to the appliance has no pre-existing LVM or other device mapper metadata.

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 **Storage** tab in the left navigation menu.
3. Click **Repository** sub tab on the main page.
4. Click the **Add Disk** button against the specific disk group.

   Details for available disks are displayed, including disk capacity and free space.
5. Select the disks that you want to add to this disk group, and then click **Use Disk(s)** button.
6. Click **OK** to confirm.

   The selected disks are displayed under the specified disk group.

16.2.2.5.3 Dropping SAN Disks from the Audit Vault Server Repository

Learn how to drop a SAN disk from a disk group.

The data on the disk being dropped is relocated to the remaining disks in the disk group. Before dropping a disk, the system checks for space on the remaining disks in the disk group

for data to be relocated. If this space check fails, it results in `OAV-47330` error. You cannot drop the only disk in the disk group.

To drop a SAN disk from a disk group in the repository:

1. Log in to the Audit Vault Server console as a *super administrator*.
2. Click the **Settings** tab, and then click **Storage** tab in the left navigation menu.
3. Find the disk you want to drop under one of the disk groups, select the disk, and then click **Drop Disk** button.
4. Click **OK** to confirm.

17
Tuning the Audit Vault Server

With use the Audit Vault Server database might run into performance issues. Adjusting database parameters to tune the Audit Vault Server to your needs will help resolve performance issues.

17.1 Preventing Shutdown of the Listener Due to Too Many Audit Trails

If there are more than 1024 audit trails on a single Audit Vault Server, the database listener might shutdown with errors `TNS-01159: Internal connection limit has been reached; listener has shut down` and `TNS-12540: TNS:internal limit restriction exceeded`. Adjust the `MAX_ALL_CONNECTIONS_LISTENER` parameter to resolve the issue.

Steps to adjust the `MAX_ALL_CONNECTIONS_LISTENER` parameter:

1. Stop all the audit trails running on the Audit Vault Server and the Audit Vault Agent.
2. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
3. Stop the following services by running the following commands:

   ```
   systemctl stop monitor
   systemctl stop javafwk
   systemctl stop controller
   systemctl stop dbfwlistener
   ```
4. Make a backup copy of the `listener.ora` file:

   ```
   cp /var/lib/oracle/dbfw/network/admin/listener.ora /var/lib/oracle/dbfw/
   network/admin/listener.ora.backup
   ```
5. Open the `listener.ora` file for editting:

   ```
   vi listener.ora
   ```
6. Add the following line in the `listener.ora` file:

   ```
   MAX_ALL_CONNECTIONS_LISTENER=Number of trails | Number of trails > 1024
   ```

   For example, if you have 1500 audit trails running:

   ```
   MAX_ALL_CONNECTIONS_LISTENER=1500
   ```

   It will be necessary to adjust this number if you intend to start more audit trails in the future.

7. Start the previously stopped services by running the following commands:

```
systemctl start monitor
systemctl start javafwk
systemctl start controller
systemctl start dbfwlistener
```

8. Start the audit trails that were previously stopped on the Audit Vault Server and the Audit Vault Agent.

Related Topics

- Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server
  Lean about stopping, starting, and setting up autostart of audit trails in Oracle Audit Vault Server.
- Stopping and Starting Audit Vault Agent
  Learn about stopping and starting Audit Vault Agent.

Part III
General Reference

These appendixes provide general reference information for administering the Audit Vault and Database Firewall system.

A

AVCLI Commands Reference

The AVCLI commands enable you to perform tasks such as creating Database Firewall monitoring points and managing audit trails.

A.1 About AVCLI Commands

Learn about AVCLI commands and their uses.

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 Oracle Audit Vault and Database Firewall administrators need to configure target connections.

All AVCLI commands must end in a semi-colon (;).

> **See Also:**
>
> Using the Audit Vault Command Line Interface for general usage information about using the `AVCLI` command line interface.

Setting the JAVA_HOME Environment Variable

In Oracle Audit Vault Server, you must set the `JAVA_HOME` environment variable to point to `JDK` installation directory.

A.2 Agent Host AVCLI Commands

The agent host AVCLI commands enable you to perform agent host-related tasks such as registering hosts.

A.2.1 About the Agent Host AVCLI Commands

The `AVCLI` host commands enable you to configure the host computer on which the Audit Vault Agent will reside.

A.2.2 ACTIVATE HOST

Learn how to use the `ACTIVATE HOST` AVCLI command.

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.

A.2.3 ALTER HOST

Learn how to use the ALTER HOST AVCLI command.

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...]}

ALTER HOST hostname DROP ATTRIBUTE {attribute name}
```

Arguments

Argument	Description
hostname	The name of the host.
key	The attribute being changed. See Table A-1 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-1 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.

Table A-1 (Cont.) Host Attributes (key values)

Parameter	Description
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-2 for descriptions of LOGLEVEL component names, and Table A-3 for LOGLEVEL values. Multiple components log levels can be changed by delimiting them using the | symbol.
AGENT_PHYSICAL_ADDRESS_XX	XX can be any value between 01 and 99. The value for the attribute must be a valid IP address of a node in a UNIX cluster environment or the IP address of a secondary network interface card (NIC) if the host machine where the agent is installed has multiple network cards.
AUTO_RESTART	The value can be either Y on N. Use Y to configure the Agent auto restart service remotely, for an Agent running on a Linux/Unix/AIX/Solaris platforms. Use N to unregister.

Note:

Ensure to understand the Agent's functionality completely before modifying the above mentioned values. They have been set to optimal value by default. Any incorrect value may degrade the performance.

The following are valid values for the LOGLEVEL attribute:

Table A-2 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-3 LOGLEVEL Values

Loglevel Value	Description
INFO	INFO level, loglevel_value of LOGLEVEL value
WARNING	WARNING level, loglevel_value of LOGLEVEL value
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`.

A.2.4 DEACTIVATE HOST

Use the `DEACTIVATE HOST` command to deactivate hosts that are specified by the *hostname* parameter.

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.

A.2.5 DROP HOST

Use the DROP HOST command to drop hosts that are specified by the value of the *host_name* parameter.

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.

> **See Also:**
> - LIST HOST to find the names of currently registered hosts.
> - LIST ATTRIBUTE FOR SECURED TARGET

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.

Oracle AVDF 20.5 and Later

Syntax

```
DROP HOST hostname [FORCE]
```

Arguments

Argument	Description
hostname	The name of the host computer being dropped.

> **See Also:**
> - LIST HOST to find the names of currently registered hosts.
> - LIST ATTRIBUTE FOR SECURED TARGET

FORCE	This is an optional parameter. Use this argument to forcefully drop the host and all the associated trails, when the hosts or trails are in stopped state or in unreachable state for more than two hours.

A.2.6 LIST HOST

Use the LIST HOST command to see the names of registered Agent host computers.

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.

Oracle AVDF 20.3 and later

This command lists the various active hosts registered with the Audit Vault Server.

Syntax

```
LIST HOST [hostname]
```

This command lists the various active hosts registered with the Audit Vault Server.

Argument

Argument	Description
host name	The hostname parameter is optional and can be specified to list a particular active host.

Example

```
list host testhost1;
```

Lists the details of `testhost1` registered with the Audit Vault Server.

A.2.7 REGISTER HOST

Learn about the REGISTER HOST AVCLI command.

The `REGISTER HOST` command adds the host to Audit Vault Server and identifies it as a host machine 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. **See Also:** • LIST HOST to find the names of currently registered hosts. • LIST ATTRIBUTE FOR SECURED TARGET
ip_address	The IP address associated with the host. If the IP address is not specified, then the IP address for the host is deduced by doing a host name lookup on the host name specified. It is possible to override this behavior to associate with a different IP address, by specifying the IP address.

Result

The host is successfully registered with the Audit Vault Server.

If the IP address is not specified, then the host name lookup fails with the following error. Retry registering the host with an IP address.

```
OAV:-46594: unable to resolve host <host_name>
```

Usage Notes

To change the IP address associated with a host, use the ALTER HOST command.

Example

```
avcli> REGISTER HOST sample_host.example.net with ip 192.0.2.1;
```

Registers the host machine, `sample_host.example.net`, and associates it with the IP address 192.0.2.1.

A.2.8 UPLOAD AGENT LOG FILE TO SERVER FOR HOST

This command uploads Audit Vault Agent log files as a `.zip` file to the Audit Vault Server.

Syntax

```
UPLOAD AGENT LOG FILE TO SERVER FOR HOST <hostname>
```

Arguments

Argument	Description
hostname	Name of the agent for which you need to download the log from the Audit Vault Server. For agentless collection of Oracle Database table trails and Microsoft SQL Server directory trails, use `'agentless collection'` as the host name.

Example

```
Upload agent log file to server for host myhost.mycompany.com
```

- Uploads the agent log files as a `.zip` file to the Audit Vault Server for the `myhost.mycompany.com` host.
- If the total agent log size is less than 300 MB, then all agent log files are uploaded.
- If the total agent log size is greater than 300 MB, then only the latest log file for each agent component is uploaded if the latest log file is less than 50 MB.

A.2.9 DOWNLOAD AGENT LOG FILE FROM SERVER FOR HOST

This command downloads Audit Vault Agent log files as a `.zip` file from the Audit Vault Server and saves the `.zip` file in the `<AVCLI installation path>/av/log` directory.

> **Note:**
>
> Oracle highly recommends that you delete the agent logs from the AVCLI log location after you upload the agent logs to the relevant service request.

Syntax

```
DOWNLOAD AGENT LOG FILE FROM SERVER FOR HOST <hostname>
```

Arguments

Argument	Description
hostname	Name of the agent for which you need to download the log from the Audit Vault Server. For agentless collection of Oracle Database table trails and Microsoft SQL Server directory trails, use `'agentless collection'` as the host name.

Example

```
download agent log file from server for host myhost.mycompany.com
```

- Downloads the agent log files as a `.zip` file from the Audit Vault Server for the `myhost.mycompany.com` host and saves the `.zip` in the `<AVCLI installation path>/av/log` directory.

- If the total agent log size is less than 300 MB, then all agent log files are downloaded.
- If the total agent log size is greater than 300 MB, then only the latest log file for each agent component is downloaded if the latest log file is less than 50 MB.

A.3 Database Firewall AVCLI Commands

The `AVCLI` Database Firewall commands enable you to configure the Database Firewall.

A.3.1 About the Database Firewall AVCLI Commands

The `AVCLI` database firewall commands enable you to perform tasks such as registering or altering a database firewall.

A.3.2 ALTER FIREWALL

Use the `ALTER FIREWALL` command to alter Oracle Database Firewall attributes.

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-4 for a list of attributes.

Usage Notes

Table A-4 lists Database Firewall attributes that you can specify for the attribute=value argument.

Table A-4 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.

A.3.3 CREATE RESILIENT PAIR

Use the `CREATE RESILIENT PAIR` command to create a resilient pair with two Oracle Database Firewall installations for high availability.

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
  STANDBY standby_firewall
```

Arguments

Argument	Descriptions
primary_firewall	The name of the primary Database Firewall. Only this Firewall can generate syslog alerts
standby_firewall	The name of the standby Database Firewall. This argument is available starting Oracle AVDF release 20.6.

Starting Oracle AVDF 20.6, the pairing process of the Database Firewall instances is a background job. See the **Jobs** dialog in the Audit Vault Server console to check the status of high availability pairing. Locate for the job against the entry `Create DBFW resilient pair`. After completion of the pairing process, navigate to the **Database Firewalls** tab and then to **High Availability** tab in left navigation menu to verify the resilient pair.

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 standby Database Firewall `sample_fw2`.

A.3.4 DROP FIREWALL

Use the `DROP FIREWALL` command to drop a registered Oracle Database Firewall from Oracle Audit Vault Server.

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.

A.3.5 DROP RESILIENT PAIR

Learn to use the `DROP RESILIENT PAIR` command to drop a resilient pair that contains the specified Oracle Database Firewall.

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.

A.3.6 LIST FIREWALL

Use the `LIST FIREWALL` command to list all of the Oracle Database Firewall installations that are registered with an Oracle Audit Vault Server.

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 Oracle Database Firewalls that are registered with Oracle Audit Vault Server appears.

A.3.7 POWEROFF FIREWALL

You can use the `POWEROFF FIREWALL` command to turn off the power for a named Oracle Database Firewall that is registered with Oracle Audit Vault Server.

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.

A.3.8 REBOOT FIREWALL

Use the `REBOOT FIREWALL` comment to reboot a named Oracle Database Firewall that is registered with Oracle Audit Vault Server.

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.

A.3.9 REGISTER FIREWALL

Use the `REGISTER FIREWALL` command to register an Oracle Database Firewall that has a specific IP address with Oracle Audit Vault Server.

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 a 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`.

A.3.10 SWAP RESILIENT PAIR

Learn how to use the `SWAP RESILIENT PAIR` command to swap Oracle Database Firewall installations that are part of a resilient pair that includes a named Oracle Database Firewall.

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.

A.3.11 SHOW STATUS FOR FIREWALL

Learn how to use the `SHOW STATUS FOR FIREWALL` command to show the status for an Oracle Database Firewall installation.

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 Oracle Database Firewall `sample_fw1` appears.

A.4 Database Firewall Monitors AVCLI Commands

The Database Firewall monitoring points related `AVCLI` commands enable you to configure the Database Firewall.

A.4.1 About Database Firewall Monitors AVCLI Commands

The Database Firewall monitoring points related `AVCLI` commands enable you to configure the host computer on which the Audit Vault Agent resides.

A.4.2 ALTER DATABASE FIREWALL MONITOR

Use the `ALTER DATABASE FIREWALL MONITOR` command to alter monitoring points and their attributes.

The `ALTER DATABASE FIREWALL MONITOR` command alters the monitoring point and the related attributes.

Syntax

```
ALTER DATABASE FIREWALL MONITOR FOR TARGET <target name> USING FIREWALL
<firewall name> SET <options>
```

Arguments

Argument	Description
`firewall name`	The name of the Database Firewall which is associated with the monitoring point.
`target name`	The name of the target which is associated with the Database Firewall monitoring point.

Argument	Description
options	Every option must be in <attribute=value> format. The following attributes can be included in options: MODE=Monitoring_Blocking_Proxy / Monitoring_Out_Of_Band / Monitoring_Host_Monitor PRESERVE_CONNECTION=TRUE/FALSE NETWORK_INTERFACE_CARD=new_network_interface_card DATABASE_RESPONSE=TRUE/FALSE FULL_ERROR_MESSAGE=TRUE/FALSE DATABASE_INTERROGATION=TRUE/FALSE DDI_DB_ADDRESS = <database_address> DDI_DB_PORT = <port> DDI_DB_NAME = <database_name> DDI_DB_CREDENTIAL = <credential> ADD_ADDRESS=<ip:port[:service name | SID]> REMOVE_ADDRESS=<ip:port[:service name | SID]>
ADD_ADDRESS	The address of the target which needs to be monitored by the Database Firewall. The address needs to be in the following format: ip:port:[service]
REMOVE_ADDRESS	The address of the target which needs to be removed from being monitored by the Database Firewall.
NETWORK_INTERFACE_CARD	The new network interface card (or traffic source) for the Database Firewall monitoring point. Starting in Oracle AVDF 20.3, for Monitoring_Host_Monitor deployment mode, provide the name of the network interface card which has an IP address configured. Starting in Oracle AVDF 20.10, for Monitoring_Out_Of_Band deployment mode, you can specify multiple network interface cards in a space separated list.
MODE	The Database Firewall deployment mode. Valid modes are: • Monitoring (Out-of-Band) • Monitoring (Host Monitor) • Monitoring / Blocking (Proxy)
PRESERVE_CONNECTION	True or False where True indicates that when the Database Firewall starts operating in monitoring and blocking mode (either because it had been changed from monitoring only mode, 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 pre-existing connections are broken. The Database Firewall can then enforce the policy when clients reconnect. This is the default behavior.
DATABASE_RESPONSE	True or False indicates whether or not to activate database response monitoring function for the monitoring point.
FULL_ERROR_MESSAGE	True or False enables this option. This starts logging the error message associated with the error code.

Arguments in Release Oracle AVDF 20.5 and Earlier

Argument	Description
DDI_DB_ADDRESS	The address of the database for which the native network encrypted traffic monitoring needs to be enabled.
DDI_DB_PORT	The port number of the database for which the native network encrypted traffic monitoring needs to be enabled.
DDI_DB_NAME	The name of the database for which the native network encrypted traffic monitoring needs to be enabled.
DDI_DB_CREDENTIAL	The credentials used to connect to the database for which the native network encrypted traffic monitoring option needs to be enabled. The credentials must be specified in the format <user name>/<password>.
DATABASE_INTERROGATION	True or False enables this option. This starts the native network encrypted traffic monitoring feature.

Arguments in Release Oracle AVDF 20.6 and Later

Argument	Description
DB_ADDRESS_FOR_DECRYPTION	The address of the database for which the native network encrypted traffic monitoring needs to be enabled.
DB_PORT_FOR_DECRYPTION	The port number of the database for which the native network encrypted traffic monitoring needs to be enabled.
DB_NAME_FOR_DECRYPTION	The name of the database for which the native network encrypted traffic monitoring needs to be enabled.
DB_CREDENTIAL_FOR_DECRYPTION	The credentials used to connect to the database for which the native network encrypted traffic monitoring option needs to be enabled. The credentials must be specified in the format <user name>/<password>.
DECRYPT_WITH_NNE_KEY	True or False enables this option. This starts the native network encrypted traffic monitoring feature.

Arguments in Release Oracle AVDF 20.8 and Later

Argument	Description
BLOCK_UNMATCHED_OSN	True or False enables this option. This blocks the connection with service names other than the ones that are mentioned in the target connection details.

Usage Notes

Attributes are specified by a comma separated list of key=value/pairs. The following key values are supported:

> **Note:**
>
> - The `ADD_ADDRESS` and `REMOVE_ADDRESS` attributes are applicable for a single target only. It is not applicable for a RAC monitoring point.
> - Starting in AVDF 20.10 and only for monitoring (out-of-band) mode, you can specify multiple network interfaces cards. Otherwise, only one network interface card or traffic source can be used.

Examples

```
avcli> ALTER DATABASE FIREWALL MONITOR FOR TARGET target1 USING FIREWALL fw1
SET MODE=monitoring_out_of_band;
```

```
avcli> ALTER DATABASE FIREWALL MONITOR FOR TARGET target1 USING FIREWALL fw1
SET database_response=true, full_error_message=true;
```

```
avcli> ALTER DATABASE FIREWALL MONITOR FOR TARGET target1 USING FIREWALL fw1
SET add_address=1.2.3.4:1234:dbfwfb;
```

Specify multiple network interface cards starting in 20.10 when deploying in Monitoring (Out of Band) mode:

```
avcli> ALTER DATABASE FIREWALL MONITOR FOR TARGET mysource USING FIREWALL
myfwset network_interface_card=enp0s3 enp0s10, database_response=true,
full_error_message=true;
```

A.4.3 CREATE DATABASE FIREWALL MONITOR

The `CREATE DATABASE FIREWALL MONITOR` command creates Database Firewall monitoring points to protect the targets.

The `CREATE DATABASE FIREWALL MONITOR` command creates a Database Firewall monitoring point with the specified name and protects the target with monitoring only, or monitoring and blocking mode.

Syntax

```
CREATE DATABASE FIREWALL MONITOR FOR TARGET <target name> USING FIREWALL <firewall name>
WITH MODE <mode name> NETWORK INTERFACE CARD <network interface card> [PROXY PORT <proxy
port number>] [ADD ADDRESS <ip:port[:service name | SID]>] [FOR TARGET MODE RAC]
```

Arguments

Argument	Descriptions
`target name`	The name of the target.
`firewall name`	The name of the Database Firewall.

Argument	Descriptions
`network interface card name`	The name of the network interface card (NIC). You may specify a bonded NIC. Only one NIC is allowed except in `Monitoring_Out_Of_Band` mode starting in Oracle AVDF 20.10. Starting in Oracle AVDF 20.10, for `Monitoring_Out_Of_Band` deployment mode, you can specify multiple network interface cards in a comma separated list. Starting in Oracle AVDF 20.3, for `Monitoring_Host_Monitor` deployment mode, provide the name of the network interface card which has an IP address configured.
`proxy port number`	Proxy port number required only for `Monitoring_Blocking_Proxy` deployment mode.
`mode name`	The available deployment modes are: • `Monitoring_Blocking_Proxy` • `Monitoring_Out_Of_Band` • `Monitoring_Host_Monitor` For `Monitoring_Blocking_Proxy` mode, both the network interface card and the proxy port must be specified and only one address can be added. For `Monitoring_Out_Of_Band` and `Monitoring_Host_Monitor` mode, the network interface card needs to be set and proxy port cannot be applied. One or more addresses can be added.
`address`	Ip address for the first Database Firewall monitoring point. It is mandatory for the first Database Firewall monitoring point for the specific target and Database Firewall. It is not allowed for the subsequent monitoring points being created. Format: `<ip:port[:service name | SID]>`
`Ip`	Ip address.
`port`	The port number
`service name`	The service name or SID of the Oracle Database.

Note:

If you plan to monitor more than one OSN on a target database:

- Oracle AVDF 20.1-20.9: You need to configure a proxy target for each OSN. This is because a single proxy port cannot service multiple OSN's on the same target database. Add more traffic proxy ports as required.
- Oracle AVDF 20.10 and later: You can use one proxy port and specify multiple OSN's on the target database that are going to be processed. Specify the OSN's in a list delimited by the "|" character. For example, target1|target2|target 3.

Argument	Descriptions
FOR TARGET MODE RAC	Can be set only for Oracle Databases and if proxy port is set.

Examples

```
create database firewall monitor for target mysource using firewall myfw with
mode Monitoring_Blocking_Proxy network interface card eth1 proxy port 1 add
address 192.0.2.0:24:srcdb for target mode rac;
```

Creates a Database Firewall monitoring point for the Database Firewall instance `myfw` using the network interface card `eth1` with port 1 and protects the target `mysource` with the mode `Monitoring_Blocking_Proxy`, adds address (`host=192.0.2.0, port=24 and service=srcdb`) as an Oracle RAC instance.

```
create database firewall monitor for target mysource using firewall myfw with
mode Monitoring_Host_Monitor network interface card eth0 add address
192.0.2.1:dbfwdb
```

Creates a Database Firewall monitoring point and monitors the target `mysource` for the Database Firewall instance `myfw` using network interface card `eth0` in mode `Monitoring_Host_Monitor`; adds address (`host=192.0.2.1, port=80, service=dbfwdb`).

```
create database firewall monitor for target mysource using firewall myfw with
mode Monitoring_Out_Of_Band network interface card eth0
```

Creates a Database Firewall monitoring point and monitors the target `mysource` for the Database Firewall instance `myfw` using network interface card `eth0` in the mode `Monitoring_Out_Of_Band`; assuming addresses have been added before in the first Database Firewall monitoring point for this target and the Database Firewall pair.

```
create database firewall monitor for target mysource using firewall myfw with
mode Monitoring_Out_Of_Band network interface card enp0s3,enp0s10,enp0s9 add
address 192.0.2.0:24:srcdb
```

Creates a Database Firewall monitoring point on Database Firewall `myfw` using network interface cards `enp0s3, enp0s10, and enp0s9` and protects the target `mysource` in mode `Monitoring_Out_Of_Band`, adds `address host = 192.0.2.0, port=24 and service = srcdb`. Specifying multiple network interface cards in `Monitoring_Out_Of_Band` mode is available starting in Oracle AVDF 20.10.

Result

In case the command is run successfully, the following output is displayed:

```
The command completed successfully.
```

In case the command is not successfully run, then it displays error. Here are some of the possible errors that are seen in Oracle AVDF release 20.8 and later:

Error	Description
`OAV-46501: invalid target: <target name provided>`	The target name specified is invalid. Check for the correct name of the target, by running `LIST SECURED TARGET` command.
`OAV-46501: invalid firewall: <firewall name provided>`	The name of the Database Firewall instance specified is invalid. Check for the correct name of the Database Firewall instance by running `LIST FIREWALL` command.
`OAV-46501: invalid monitor mode: <provided monitor mode name>. Monitor mode must be one of: Monitoring_Blocking_Proxy, Monitoring_Host_Monitor, Monitoring_Out_Of_Band.`	The Database Firewall mode specified is invalid. The valid modes are: `Monitoring_Blocking_Proxy`, `Monitoring_Host_Monitor`, `Monitoring_Out_Of_Band`.
`OAV-46501: invalid network interface card: <network interface card provided>`	The name of the network interface card specified is invalid. Check for the correct name of the network interface card by running `SHOW STATUS FOR FIREWALL` command.
`OAV-46501: invalid proxy port number: <proxy port number provided>`	The proxy port number specified is invalid. Check for the correct proxy port number.
`OAV-46991: Invalid option 'proxy port' for mode 'Monitoring (Out-of-Band) OAV-46991: Invalid option 'proxy port' for mode 'Monitoring (Host Monitor)`	The proxy port number is specified for `Monitoring_Out_Of_Band` or `Monitoring_Host_Monitor` mode. Remove the proxy port number.
`OAV-46648: Invalid value for 'proxy port'`	The proxy port number is not specified for `Monitoring_Blocking_Proxy` mode.
`OAV-47501: Traffic proxy <proxy name> is in use.`	The proxy port number specified is being used by another Database Firewall monitoring point.
`OAV-46504: duplicate proxy port numbers: <proxy port number provided as part of network interface card> and <proxy port number provided>`	The proxy port is specified for the `NETWORK INTERFACE CARD` and `PROXY PORT` does not match. Provide a single proxy port number.

Error	Description
`OAV-46995: At least one connection details required for the database firewall monitor`	The address or connection detail is not specified for the first Database Firewall monitoring point for the specific target and pair of Database Firewall instances.
`OAV-47709: Connection details cannot be changed if there is more than one database firewall monitor`	The address or connection detail is specified before and cannot be changed again for the subsequent Database Firewall monitoring point for the specific target and pair of Database Firewall instances. Check the existing connection detail by running the `LIST DATABASE FIREWALL MONITOR` command.
`OAV-47707: Invalid option 'FOR TARGET MODE RAC' for mode 'Monitoring (Out-of-Band)'` `OAV-47707: Invalid option 'FOR TARGET MODE RAC' for mode 'Monitoring (Host Monitor)'`	Attempt to configure `Monitoring_Out_Of_Band` or `Monitoring_Host_Monitor` for Oracle RAC target instance which is not supported. Remove the option `FOR TARGET MODE RAC` or change the mode to `Monitoring_Blocking_Proxy`.
`OAV-46535: failed to add secured target address:` `address <address provided> is used by Secured Target <another target name>`	The address or connection detail is already specified for another target being monitored.

See Also:

- LIST SECURED TARGET
- LIST FIREWALL
- SHOW STATUS FOR FIREWALL
- LIST DATABASE FIREWALL MONITOR

A.4.4 DROP DATABASE FIREWALL MONITOR

Use the `DROP DATABASE FIREWALL MONITOR` command to drop monitoring points.

The `DROP DATABASE FIREWALL MONITOR` command drops the monitoring point.

Syntax

```
DROP DATABASE FIREWALL MONITOR FOR TARGET <target name> USING FIREWALL <firewall name>
```

Arguments

Argument	Descriptions
`firewall name`	The name of the Database Firewall.

Argument	Descriptions
`target name`	The name of the target.

Examples

```
avcli> DROP DATABASE FIREWALL MONITOR FOR TARGET sample_source USING FIREWALL sample_fw;
```

```
avcli> DROP DATABASE FIREWALL MONITOR FOR TARGET target1 USING FIREWALL fw1;
```

The monitoring point is dropped.

A.4.5 LIST DATABASE FIREWALL MONITOR

Use the `LIST DATABASE FIREWALL MONITOR` command to list all of the monitoring points associated with either the Database Firewall or the target.

The `LIST DATABASE FIREWALL MONITOR` command lists the monitoring points associated with either the Database Firewall or the target.

Syntax

```
LIST DATABASE FIREWALL MONITOR FOR FIREWALL <firewall_name>
```

```
LIST DATABASE FIREWALL MONITOR FOR TARGET <target_name>
```

Arguments

Argument	Descriptions
`firewall_name`	The name of the Database Firewall.
`target_name`	The name of the target.

Example

```
avcli> LIST DATABASE FIREWALL MONITOR FOR FIREWALL sample_fw;
```

A list of all the monitoring points associated with the Database Firewall `sample_fw` appears.

```
avcli> LIST DATABASE FIREWALL MONITOR FOR TARGET sample_source;
```

A list all the monitoring points associated with the target `sample_source` appears.

A.4.6 START DATABASE FIREWALL MONITOR

Learn how to use the `START DATABASE FIREWALL MONITOR` command to start a monitoring point that was previously suspended.

The `START DATABASE FIREWALL MONITOR` command starts a monitoring point that was previously suspended.

Syntax

```
START DATABASE FIREWALL MONITOR FOR TARGET <target name> USING FIREWALL <firewall name>
```

Arguments

Argument	Descriptions
`firewall name`	The name of the Database Firewall.
`target name`	The name of the target.

Examples

```
avcli> START DATABASE FIREWALL MONITOR FOR TARGET sample_source USING FIREWALL sample_fw;

avcli> START DATABASE FIREWALL MONITOR FOR TARGET target1 USING FIREWALL fw1;
```

The monitoring point is started.

A.4.7 STOP DATABASE FIREWALL MONITOR

Use the `STOP DATABASE FIREWALL MONITOR` command to stop monitoring point.

The `STOP DATABASE FIREWALL MONITOR` command stops the monitoring point of the target.

Syntax

```
STOP DATABASE FIREWALL MONITOR FOR TARGET <target name> USING FIREWALL <firewall name>
```

Arguments

Argument	Descriptions
`firewall name`	The name of the Database Firewall.
`target name`	The name of the target.

Examples

```
avcli> STOP DATABASE FIREWALL MONITOR FOR TARGET sample_source USING FIREWALL sample_fw;

avcli> STOP DATABASE FIREWALL MONITOR FOR TARGET target1 USING FIREWALL fw1;
```

The monitoring point is stopped.

A.5 Target AVCLI Commands

The `AVCLI` target commands enable you to configure both database and nondatabase targets for Audit Vault Server.

The terms `TARGET` and `SECURED TARGET` are generally synonymous in this release of Oracle Audit Vault and Database Firewall.

A.5.1 About the Target AVCLI Commands

The target `AVCLI` commands enable you to perform tasks such as registering or altering a target.

A.5.2 ALTER SECURED TARGET

Use the `ALTER SECURED TARGET` command to modify the attributes of targets.

The `ALTER SECURED TARGET` command modifies the attributes of a target.

Syntax

```
ALTER SECURED TARGET secured_target_name
   SET attribute=value [, attribute=value]
```

Arguments

Argument	Description
attribute=value	The key/value pair for the target attributes of the target to be modified. You can modify one or more target attributes at a time using a space on the command line. **See Also:** • Table A-5 for target attributes. • Audit Collection Attributes as some types of targets also require collection attributes. • LIST ATTRIBUTE FOR SECURED TARGET to find a list of attribute values for a target.
service	**REQUIRED FOR ORACLE DATABASE ONLY:** The service name or SID

Table A-5 lists target attributes that you can specify,

Table A-5 Target Attributes

Attribute	Description
NAME	The name of the target database to be modified. The name is case-sensitive. This must not be defined already in the Audit Vault Server for another target. Special characters (`&<>"/;,*|=% --`) cannot be used for target names. **See Also:** LIST SECURED TARGET to find a list of existing targets.
LOCATION	The location of the target. **Note:** In case the target location was not specified during registration and if credentials are required to connect to the target, then the credentials must be specified along with the target location.
CREDENTIALS	The new username used to connect to the target. Audit Vault Server prompts for the new password. Credentials in `<new username>/<new password>` format is accepted through a `.av` file.
DESCRIPTION	The description for this target database instance
MAXIMUM_ENFORCEMENT_POINT_THREADS	The maximum number of monitoring point threads for the 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 target name of `sample_source` changed to `sample_source2`.

```
avcli> ALTER SECURED TARGET sample_source SET credentials=scott;
```

The credentials used to connect to the target, `sample_source`, are changed.

```
avcli> ALTER SECURED TARGET sample_source SET description='This is a new description';
```

Number of monitoring point threads is set for target, `sample_source`.

```
avcli> ALTER SECURED TARGET sample_source SET maximum_enforcement_point_threads=14;
```

The description for the target, `sample_source`, is changed.

```
avcli> ALTER SECURED TARGET sample_source set maximum_enforcement_point_threads = 10;
```

Sets the maximum number of monitoring point threads for 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 target, `sample_source`, changes.

A.5.3 DROP SECURED TARGET

Learn how to use the `DROP SECURED TARGET` command to remove the registration of a specified target from Oracle Audit Vault Server.

The `DROP SECURED TARGET` command removes the registration of the specified target from Audit Vault Server.

Syntax

```
DROP SECURED TARGET secured_target_name
```

Arguments

Argument	Description
secured_target_name	The name of the target. To find all registered targets, see "LIST SECURED TARGET".

Usage Notes

Ensure that all trails associated with this target are in stopped state before dropping the target. Otherwise, the `DROP SECURED TARGET` command fails. See `HELP STOP COLLECTION` for an explanation of how to stop active trails.

Dropping a 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` target.

A.5.4 LIST ATTRIBUTE FOR SECURED TARGET

Use the `LIST ATTRIBUTE FOR SECURED TARGET` command to list the attributes of targets.

The `LIST ATTRIBUTE FOR SECURED TARGET` command lists the attributes of a given target.

Syntax

```
LIST ATTRIBUTE FOR SECURED TARGET secured target name;
```

Arguments

Argument	Description
secured target name	The name of the target. To find all registered targets, see "LIST SECURED TARGET".

A.5.5 LIST METRICS

Use the `LIST METRICS` command to list the metrics of a given target, such as various trails.

The `LIST METRICS` command lists the metrics of a given target, such as various trails.

Syntax

```
LIST METRICS FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Description
secured_target_name	The name of the target To find all registered targets, see "LIST SECURED TARGET".

Usage Notes

The `LIST METRICS` command has the same usage for all target types.

Examples

```
avcli> LIST METRICS FOR SECURED TARGET sample_source;
```

Metrics available for the target, `sample_source`, are listed.

A.5.6 LIST SECURED TARGET

Use the `LIST SECURED TARGET` command to list various active targets that are registered with Audit Vault Server.

The `LIST SECURED TARGET` command lists the active targets registered with the Audit Vault Server.

Syntax

```
LIST SECURED TARGET;
```

Lists the active target names registered with Audit Vault Server.

A.5.7 LIST SECURED TARGET TYPE

Use the `LIST SECURED TARGET TYPE` command to list various target types that are registered with Audit Vault Server.

The `LIST SECURED TARGET TYPE` command lists various target types currently registered in the Audit Vault Server.

Syntax

```
LIST SECURED TARGET TYPE
```

Example

```
avcli> list secured target type;
```

Lists various target type names currently registered with the Audit Vault Server.

A.5.8 REGISTER SECURED TARGET

Use the `REGISTER SECURED TARGET` command to register targets to be monitored by Audit Vault Server.

The `REGISTER SECURED TARGET` command registers a 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] [DEPLOYMENT MODE
deployment mode]
```

Arguments

Argument	Description
secured_target_name	Name of target. Must be unique. Special characters (`&<>"/;,*|=% --`) cannot be used for target names.
secured_target_type	A valid target type, for example `"Oracle"`. **See Also:** LIST SECURED TARGET TYPE to find a list of supported target types.
location	The target database connection information. **See Also:** ALTER SECURED TARGET This is optional. It can be added later. The location is an opaque string that specifies how to connect to the target, typically a JDBC connect string. The syntax that you use depends on the 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 target type.

Argument	Description
user_name	Optional. Credentials to connect to the target. After you enter the `username` argument, Audit Vault Server prompts you for the password of the target user account. For target databases, this account must exist on the target database. Optional. See the database specific usage notes in the following sections.
DEPLOYMENT MODE	Optional. Deployment mode of target. This argument is available starting with release Oracle AVDF 20.7. For Oracle Database having Active Data Guard with Unified Auditing, specify the `DEPLOYMENT MODE` as `ADG`. For additional information, refer to Additional Information for Audit Collection from Oracle Active Data Guard.

General Examples

```
avcli> HELP REGISTER SECURED TARGET;
```

Displays detailed help for the `REGISTER SECURED TARGET` command.

Oracle Database Usage Notes and Examples

- Authentication credentials must be specified along with the target location if credentials are required to connect to the target.
- 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
  ```

- JDBC connect string format for different target types are specified below. For example:

  Oracle Database: `jdbc:oracle:thin:@//<host>:<port>/<service name | SID>`

  Sybase ASE and Sybase SQL Anywhere: `jdbc:av:sybase://<host>:<port>`

  > **Note:**
  >
  > Sybase SQL Anywhere was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

  Microsoft SQL Server: `jdbc:av:sqlserver://<host>:<port>`

  > **Note:**
  >
  > Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

  IBM DB2 DBARS and IBM DB2 LUW: `jdbc:av:db2://<host>:<port>/<database name>`

  MySQL: `jdbc:av:mysql://<host>:<port>/mysql`

- If you are unsure of this connection information, then run the `lsnrctl status listener_name` command on the computer where you installed the target database.
- For the `AUTHENTICATED BY` command, enter the user name, and Audit Vault Server prompts you for the password. `AUTHENTICATED BY <username>/<password>` is accepted from file input through `.av` file. This user account must exist in the target database.

  To find this user, query the `SESSION_PRIVS` and `SESSION_ROLES` data dictionary views.
- For Oracle Database having Active Data Guard with Unified Auditing, specify the `DEPLOYMENT MODE` as `ADG`.

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 DEPLOYMENT MODE ADG;
```

Registers an Oracle target, `sample_source`, of target type `Oracle Database`, reachable using connect string `jdbc:oracle:thin:@//anymachinename: 1521/example.com` using credentials `system` and deployment mode ADG.

SQL Server Example With DB

```
avcli > REGISTER SECURED TARGET sample_mssqldb OF SECURED TARGET TYPE "Microsoft
SQL Server" AT jdbc:av:sqlserver://hostname:port authenticated by <user>;
```

SQL Server Example with Windows Authentication

```
avcli > REGISTER SECURED TARGET sample_mssqldb OF SECURED TARGET TYPE
"Microsoft SQL Server" AT "jdbc:av:sqlserver://<Host
Name>:<Port>;authenticationMethod=ntlmjava;domain=<domain name>"
authenticated by <windows user>;
```

IBM DB2 Example

```
avcli> REGISTER SECURED TARGET sample_db2db OF SECURED TARGET TYPE "IBM DB2
LUW" AT jdbc:av:db2://host:port authenticated by sa;
```

Registers a DB2 target, `sample_db2db`, of target type `"IBM DB2 LUW"`, reachable using connect string `jdbc:av:db2://host:port` using credentials authenticated by *sa*.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

A.5.9 UPLOAD OR DELETE WALLET FILE

Use the `UPLOAD OR DELETE WALLET FILE` to upload or delete target wallet files.

This command is used to upload and delete a target wallet file.

Syntax

```
ALTER SECURED TARGET <Secured target name> SET WALLET_FILE=<Path of the wallet
file>

ALTER SECURED TARGET <Secured target name> DROP ATTRIBUTE WALLET_FILE
```

Arguments

Argument	Description
`<Secured target name>`	Name of the target.
`WALLET_FILE`	Name of wallet attribute (Key).
`<Path of the wallet file>`	Path to wallet file (Value).

Examples

```
alter secured target mysource set wallet_file=/dir1/dir2/wallet.sso;
```

Uploads the target wallet file to the specified location of the Audit Vault Server using a TCPS connection.

```
alter secured target mysource drop attribute wallet_file;
```

Deletes the target wallet from the location using a TCPS connection.

A.6 Target Group AVCLI Commands

The `AVCLI` target group commands enable you to alter a target group.

Table A-6

Table A-6 AVCLI Target Group Commands

Command	Description
ADD TARGET	Adds a specific target to a target group.
DELETE TARGET	Deletes a specific target from a target group.

A.6.1 ADD TARGET

Use this command to add a specific target to a target group.

Syntax

```
ALTER TARGETGROUP <target group name> ADD TARGET <target name>


HELP ALTER TARGETGROUP
```

Arguments

Argument	Description
`help`	To seek help on available options.
`target name`	The name of the specific target that needs to be added.

Argument	Description
`target group name`	The name of the specific target group.

Example

```
alter targetgroup tg1 add target t1
```

A.6.2 ALTER TARGET GROUP

Use the `ALTER TARGET GROUP` command to modify the specified target group.

To add or delete targets from the specified target group. To modify the description of the target group.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
ALTER TARGET GROUP <target group name> ADD TARGET <target name>
```

To add a target to an existing target group.

```
ALTER TARGET GROUP <target group name> DELETE TARGET <target name>
```

To remove the target from an existing target group.

```
ALTER TARGET GROUP <target group name> MODIFY DESCRIPTION <description>
```

To modify the description of an existing target group.

```
HELP ALTER TARGET GROUP
```

To seek help on available options.

Arguments

Argument	Description
`target group name`	The name of the specified target group that needs to be modified.
target name	The name of the specified target that needs to be added or deleted from the target group.
description	The new description of the specified target group.

Examples

```
alter target group tg1 add target t1;
```

This command adds target `t1` to the target group `tg1`.

```
alter target group tg1 delete target t1;
```

This command deletes target `t1` from the target group `tg1`.

```
alter target group tg1 modify description 'new description';
```

The description of the specified target group is modified to the specified one.

A.6.3 CREATE TARGET GROUP

Use the `CREATE TARGET GROUP` command to create a target group with the specified name.

To create a target group with the given name. A target group can be created only by a super administrator or superauditor.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
CREATE TARGET GROUP <target group name>
```

Creates a target group with the specified name.

```
CREATE TARGET GROUP <target group name> DESCRIPTION <description>
```

Optionally add a description while creating the new target group.

Arguments

Argument	Description
target group name	The name of the target group being created. Special characters (`&<>"/;,*|=% --`) cannot be used for target names.

Examples

```
CREATE TARGET GROUP test22
```

A new target group with the name `test22` is created.

```
create target group my_group2 description 'new group for new reports';
```

Creates a target group `my_group2` with description `new group for new reports`.

A.6.4 DELETE TARGET

Use this command to delete a specific target from a target group.

Syntax

```
ALTER TARGETGROUP <target group name> DELETE TARGET <target name>
```

```
HELP ALTER TARGETGROUP
```

Arguments

Argument	Description
`help`	To seek help on available options.
`target name`	The name of the specific target that needs to be deleted.
`target group name`	The name of the specific target group.

Example

```
alter targetgroup tg1 delete target t1
```

A.6.5 DROP TARGET GROUP

Use the `DROP TARGET GROUP` command to remove the registration of the specified target group from Audit Vault Server.

To drop the specified target group from Audit Vault Server.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
DROP TARGET GROUP <target group name>
```

Arguments

Argument	Description
`target group name`	The name of the specified target group being dropped.

Example

```
DROP TARGET GROUP test22
```

The target group with the name `test22` is dropped.

A.6.6 LIST TARGET GROUPS

Use the `LIST TARGET GROUPS` command to view a list of all target groups for a user.

To view a list of all target groups for a user.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
LIST TARGET GROUPS
```

This command lists all the target groups for the current user.

Example

```
list target groups;
```

Lists all the target groups.

A.6.7 LIST TARGETS OF TARGET GROUP

Use the `LIST TARGETS OF TARGET GROUP` command to view a list of active targets in a specific target group.

To view a list of active targets in a specific target group.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
LIST TARGETS OF TARGET GROUP <target group name>
```

This command lists various active targets in a specific target group. The output contains the name, location, and description for each target.

Arguments

Argument	Description
target group name	The name of the target group for which the active targets are being listed.

Example

```
list targets of target group tg1;
```

Lists various active targets of the target group `tg1`.

A.7 Audit Trail Collection AVCLI Commands

The audit trail collection AVCLI commands enable you to perform tasks such as starting and stopping audit trail collections.

A.7.1 About Oracle Audit Trail AVCLI Commands

The `AVCLI` target audit trial collection commands enable you to manage the audit trail collections for the targets.

A.7.2 DROP TRAIL FOR SECURED TARGET

This command 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
[WITH CONNECTION <connection_name>]
```

Arguments

Argument	Description
secured_target_name	The name of the target whose audit trail you want to drop.
hostname	The name of the host where the target agent resides. For agentless collection of Oracle Database table trails and Microsoft SQL Server directory trails, use `'agentless collection'` as the host name.
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` directory name / mask • `CUSTOM` *name*
connection_name	Optional. Connection name. Applicable for Oracle AVDF release 20.7 and later. For Oracle Database having Active Data Guard with Unified Auditing, the trails can connect to the current primary database using failover connection string. Or trails can connect to individual databases in Active Data Guard using connection name, specified using `WITH CONNECTION` directive. The `WITH CONNECTION` directive should be used only for Oracle Database having Active Data Guard with Unified Auditing. The `WITH CONNECTION` directive should not be used for non Active Data Guard databases. The `WITH CONNECTION` directive should not be used for Active Data Guard databases with Traditional Auditing. The connection name can be either `failover_connection` or it can be audit collection attribute name in the format `av.target.connection.<name>` specified during target creation. For additional information, refer to Additional Information for Audit Collection from Oracle Active Data Guard.

> **See Also:**
>
> - LIST SECURED TARGET to find all registered targets.
> - LIST HOST to find a list of configured agent hosts.
> - LIST ATTRIBUTE FOR SECURED TARGET for detailed information about a target.

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 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 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 target `sample_source` is dropped.

```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo FROM TRANSACTION LOG /
extract;
```

The transaction log trail from the directory /extract for target `sample_source` is dropped.

```
avcli> DROP TRAIL FOR SECURED TARGET mysource USING HOST foo FROM TABLE
unified_audit_trail WITH CONNECTION failover_connection;
```

Deletes table trail `unified_audit_trail` for target `mysource` using failover connection specified during target registration. This is applicable only for Oracle Database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7.

```
avcli> DROP TRAIL FOR SECURED TARGET mysource USING HOST foo FROM TABLE
unified_audit_trail WITH CONNECTION av.target.connection.<name>;
```

Deletes table trail `unified_audit_trail` for target `mysource` using connection name in the format `av.target.connection.<name>` specified during target registration. This is applicable only for Oracle Database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7.

A.7.3 LIST TRAIL FOR SECURED TARGET

Use the `LIST TRAIL FOR SECURED TARGET` command to list audit trails that have been started with the `START COLLECTION` command or stopped with the `STOP COLLECTION` command,

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 target. To find a list of existing targets, see "LIST SECURED TARGET".

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 target `sample_souce` are listed.

A.7.4 START COLLECTION FOR SECURED TARGET

This command starts the collection of specified audit trail data from a given target, optionally using the specified collection plug-in.

> **Note:**
>
> If the audit trail does not already exist, then it is created and started.

Syntax

```
START COLLECTION FOR SECURED TARGET secured_target_name USING HOST host FROM location
   [USING PLUGIN plugin id] [WITH CONNECTION <connection_name>]
```

Arguments

Argument	Description
secured_target_name	The name of the target whose audit trail collection you want to begin.
host	The name of the host where the target agent resides. For agentless collection of Oracle Database table trails and Microsoft SQL Server directory trails, use `'agentless collection'` as the host name.

Argument	Description
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 directory name / mask • 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.
connection_name	Optional. Connection name. For Oracle Database having Active Data Guard with Unified Auditing, the trails can connect to the current primary database using failover connection string. Or trails can connect to individual databases in Active Data Guard using the connection name specified using WITH CONNECTION directive. The WITH CONNECTION directive should be used only for Oracle Database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7. The WITH CONNECTION directive should not be used for non Active Data Guard databases. The WITH CONNECTION directive should not be used for Active Data Guard databases with Traditional Auditing. The connection name can be either failover_connection or it can be audit collection attribute name in the format av.target.connection.<name> specified during target creation. For additional information, refer to Additional Information for Audit Collection from Oracle Active Data Guard.

See Also:

- LIST SECURED TARGET to find all registered targets.
- LIST HOST to find a list of configured agent hosts.
- LIST ATTRIBUTE FOR SECURED TARGET for detailed information about a target.
- LIST PLUGIN FOR SECURED TARGET TYPE to find a list of existing plug-ins for the type.

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 target, the target must up and running. When multiple plug-ins can process audit data from a 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.

After you run the `START COLLECTION` command, the Audit Vault Server begins to collect audit data from the configured targets. If you want to stop the collection, then run the `STOP COLLECTION` command.

> **See Also:**
>
> - REGISTER SECURED TARGET
> - STOP COLLECTION FOR SECURED TARGET

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 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 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 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 target `sample_source` starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM transaction
log /extract;
```

Audit data collection from trail /extract for target `sample_source`.

Collecting transaction log data from trail location `/extract` for 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 target `sample_source`, using the `com.sample_plugin`, plug-in starts.

```
avcli> START COLLECTION FOR SECURED TARGET mysource USING HOST foo FROM TABLE
unified_audit_trail WITH CONNECTION failover_connection;
```

Starts collecting audit data from table trail `unified_audit_trail` for target `mysource` using failover connection specified during target registration. This is applicable only for Oracle Database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7.

```
avcli> START COLLECTION FOR SECURED TARGET mysource USING HOST foo FROM TABLE
unified_audit_trail WITH CONNECTION av.target.connection.<name>;
```

Starts collecting audit data from table trail `unified_audit_trail` for target `mysource` using connection name in the format `av.target.connection.<name>` specified during target registration. This is applicable only for Oracle database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7.

Oracle Database 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 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`*

Best Practice:

The user must have admin privileges to access the security event log collector system. The user has an option to choose the following properties as the maximum event log size.

Event Log Properties	To Accomplish
Overwrite event as needed	To delete the oldest event first. It automatically clears events.
Do not overwrite events	To avoid overwriting of existing events. In this case the user has to manually clear the event log.

Sybase ASE 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 Also:

Running the XML Transformation Utility for MySQL Audit Formats

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 Target Usage Notes

For an Oracle Solaris target, the trail *location* used in this command must be in the format:

hostname:*path_to_trail*

where *hostname* matches the host name in the audit log names, which look like this:

```
timestamp1.timestamp2.hostname
```

Windows Target Usage Notes

For a Windows 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`.

Best Practice:

The user must have *admin* privileges to access the security event log collector system. The user has an option to choose the following properties as the maximum event log size.

Event Log Properties	To Accomplish
Overwrite event as needed	To delete the oldest event first. It automatically clears events.
Do not overwrite events	To avoid overwriting of existing events. In this case the user has to manually clear the event log.

Active Directory Target Usage Notes

For *Active Directory* target, the event log audit trail type collects data from the security and directory service. The trail location used in this command must be security or directory service.

Best Practice:

Event Log Properties When Maximum Event Log Size Is Reached	To Accomplish
Overwrite event as needed	It is recommended to select `Overwrite event as needed (Oldest event first)` or `Do not overwrite events`. To delete the oldest event first. It automatically clears events.
Do not overwrite events	To avoid overwriting of existing events. In this case the user has to manually clear the event log.

A.7.5 Create Audit Trail for a Secured Target

Learn how to create and start an audit trail.

To create a new audit trail, use the command syntax mentioned in START COLLECTION FOR SECURED TARGET. In case the audit trail does not already exist, then it is created and started.

A.7.6 STOP COLLECTION FOR SECURED TARGET

This command stops audit trail collection.

Syntax

```
STOP COLLECTION FOR SECURED TARGET secured_target_name USING HOST hostname FROM
location
 [USING PLUGIN plugin_id]] [WITH CONNECTION <connection_name>]
```

Arguments

Argument	Description
secured_target_name	The name of the target for the trail collection you want to stop.
hostname	The name of the host where the target agent resides. For agentless collection of Oracle Database table trails and Microsoft SQL Server directory trails, use `'agentless collection'` as the host name.
location	The *location* is one of following: • `DIRECTORY` *directory name* / *mask* • `TABLE` *tablename* • `SYSLOGDEFAULT` | *filename* / *file mask* • `NETWORK` • `EVENT LOG` *[eventlog name]* • `TRANSACTION LOG directory name / mask` • `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.
connection_name	Optional. Connection name. For Oracle Database having Active Data Guard with Unified Auditing, the trails can connect to the current primary database using failover connection string. Or trails can connect to individual databases in Active Data Guard using connection name, specified using `WITH CONNECTION` directive. The `WITH CONNECTION` directive should be used only for Oracle Database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7. The `WITH CONNECTION` directive should not be used for non Active Data Guard databases. The `WITH CONNECTION` directive should not be used for Active Data Guard databases with Traditional Auditing. The connection name can be either `failover_connection` or it can be audit collection attribute name in the format `av.target.connection.<name>` specified during target creation. For additional information, refer to Additional Information for Audit Collection from Oracle Active Data Guard.

> **See Also:**
>
> - LIST SECURED TARGET to find a list of all registered targets.
> - LIST HOST to find a list of configured agent hosts.
> - LIST ATTRIBUTE FOR SECURED TARGET for detailed information about a target.
> - LIST PLUGIN FOR SECURED TARGET TYPE to find a list of existing plug-ins for the type.
> - LIST TRAIL FOR SECURED TARGET to view the current state of target.

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 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.

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 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 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 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 target `sample_source` stops

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host FROM
transaction log /extract;
```

Collecting transaction log data from trail location /extract for 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 target, `sample_source`, using the `com.sample_plugin`, plug-in stops

```
avcli> STOP COLLECTION FOR SECURED TARGET mysource USING HOST foo FROM TABLE
unified_audit_trail WITH CONNECTION failover_connection;
```

Stops collecting audit data from table trail `unified_audit_trail` for target `mysource` using failover connection specified during target registration. This is applicable only for Oracle Database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7.

```
avcli> STOP COLLECTION FOR SECURED TARGET mysource USING HOST foo FROM TABLE
unified_audit_trail WITH CONNECTION av.target.connection.<name>;
```

Stops collecting audit data from table trail `unified_audit_trail` for target `mysource` using connection name in the format `av.target.connection.<name>` specified during target registration. This is applicable only for Oracle Database having Active Data Guard with Unified Auditing starting with Oracle AVDF release 20.7.

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$;
```

TRANSACTION LOG example:

```
avcli> START COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com FROM
TRANSACTION LOG /extract;
```

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 Also:**
>
> Running the XML Transformation Utility for MySQL Audit Formats

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 host name in the audit log names, which look like this:

```
timestamp1.timestamp2.hostname
```

Windows Target Usage Notes

For a Windows 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`.

A.7.7 MOVE COLLECTION FOR SECURED TARGET

Starting in Oracle AVDF 20.11, this command moves the audit collection for the specified trail from one audit agent to another.

Syntax

```
MOVE COLLECTION FOR SECURED TARGET <secured target name> ON <location> [WITH
CONNECTION <connection name>] FROM AGENT <current agent> TO AGENT <another
agent>
```

The <location> can be either: `DIRECTORY <directory name/mask>` or `TABLE <table name>`.

Usage Notes

- The audit collection for the specified trail can be moved from current agent to another agent only if the trail is in `STOPPED` state.
- Move the audit collection command is only supported for Oracle table trails and Microsoft SQL Server - sqlaudit and XEL directory trails.
- For Oracle Database having Active Data Guard(ADG) with Unified Auditing, the trails can connect to current primary database using failover connection string or trails can connect to individual databases in ADG using connection name, specified using `WITH CONNECTION` directive.
- The `WITH CONNECTION` directive should only be used for Oracle database having Active Data Guard with Unified Auditing.
  - The `WITH CONNECTION` directive should not be used for non-Active Data Guard databases.
  - The `WITH CONNECTION` directive should not be used for Active Data Guard databases with Traditional Auditing.
- The connection name can be either `failover_connection` or it can be audit collection attribute name in the format `av.target.connection.<name>` specified during target creation.
- The `FROM AGENT` directive is used to specify the current agent on which the audit collection is currently configured. The `TO AGENT` directive is used to specify the agent to which the audit collection needs to be moved.
- The audit collections present on an agent can be viewed using the `LIST COLLECTION FOR AGENT` command.

Examples

Move audit collection of directory trail `/opt/audit_trail` for secured target `mysource` from `agent1` to `agent2`.

```
MOVE COLLECTION FOR SECURED TARGET mysource ON DIRECTORY /opt/audit_trail
FROM AGENT agent1 TO AGENT agent2
```

Move audit collection of table `trail sys.aud$` for secured target `mysource` from `agent1` to `agent2`.

```
MOVE COLLECTION FOR SECURED TARGET mysource ON TABLE sys.aud$ FROM AGENT
agent1 TO AGENT agent2
```

Move audit collection of table trail `unified_audit_trail` for secured target `mysource` using failover connection from `agent1` to `agent2`. This is applicable only for Oracle database having Active Data Guard with Unified Auditing. Failover connection string is specified during Active Data Guard target registration.

```
MOVE COLLECTION FOR SECURED TARGET mysource ON TABLE unified_audit_trail WITH
CONNECTION failover_connection FROM AGENT agent1 TO AGENT agent2
```

Move audit collection of table trail `unified_audit_trail` for secured target `mysource` using connection `av.target.connection.<name>` from `agent1` to `agent2`. This is applicable only for Oracle database having Active Data Guard with Unified Auditing. Connection `av.target.connection.<name>` is specified using audit collection attribute during target registration.

```
MOVE COLLECTION FOR SECURED TARGET mysource ON TABLE unified_audit_trail WITH
CONNECTION  av.target.connection.<name> FROM AGENT agent1 TO AGENT agent2
```

Related Topics

- List Collection for Agent

A.7.8 LIST COLLECTION

Starting in Oracle AVDF 20.11, this command lists the audit collections present on a given agent.

Syntax

```
LIST COLLECTION FOR AGENT <agent name>
```

Example

List the audit collections present on `agent1`.

```
LIST COLLECTION FOR AGENT agent1
```

A.8 SMTP Connection AVCLI Commands

The AVCLI SMTP commands enable you to manage SMTP email notifications for Audit Vault Server reports and alert.

A.8.1 About the SMTP Connection AVCLI Commands

The AVCLI SMTP connection commands enable you to perform tasks such as registering and modifying SMTP connections.

A.8.2 ALTER SMTP SERVER

Use the ALTER SMTP SERVER command to modify SMTP server configurations and states.

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]
```

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	Optional. The authentication credentials for the recipient user. If the SMTP server runs in authenticated mode and needs a valid user name to connect to send emails, use the AUTHENTICATED BY clause to specify those credentials. Audit Vault Server prompts for the password. AUTHENTICATED BY username/password is accepted from file input through .av file.

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 after you run REGISTER SMTP SERVER.
- To test the configuration, run the TEST SMTP SERVER command.
- If you omit an argument, then Audit Vault Server uses the previously configured setting.

> **See Also:**
>
> - ALTER SMTP SERVER SECURE MODE ON
> - TEST SMTP SERVER

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.

A.8.3 ALTER SMTP SERVER DISABLE

Use the `ALTER SMTP SERVER DISABLE COMMAND` to disable SMTP server configurations.

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".
- 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.

A.8.4 ALTER SMTP SERVER ENABLE

Use the `ALTER SMTP SERVER ENABLE` command to enable SMTP server configurations for servers that you have registered with the `REGISTER SMTP SERVER` command or that you modified with the `ALTER SMTP SERVER` command.

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".

Example

```
avcli> ALTER SMTP SERVER ENABLE;

SMTP integration is enabled.
```

Enables the integration between the Audit Vault and SMTP server.

A.8.5 ALTER SMTP SERVER SECURE MODE OFF

Use the `ALTER SMTP SERVER SECURE MODE OFF` command to disable the secure mode in secure SMTP servers.

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 or ALTER SMTP SERVER 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.

A.8.6 ALTER SMTP SERVER SECURE MODE ON

Use the `ALTER SMTP SERVER SECURE MODE ON` command to enable SMTP server configurations and specify the secure protocol mode that is in use.

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` or `ALTER SMTP SERVER` command.

Only run this command if the SMTP server that you are configuring is a secure server.

> **See Also:**
>
> - REGISTER SMTP SERVER
> - ALTER SMTP 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.

A.8.7 DROP SMTP SERVER

Use the `DROP SMTP SERVER` command to unregister the SMTP server that is registered with Oracle Audit Vault Server and remove associated configuration metadata.

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.

A.8.8 LIST ATTRIBUTE OF SMTP SERVER

Use the `LIST ATTRIBUTE OF SMTP SERVER` command to dislay the current SMTP configuration details the Oracle Audit Vault Server uses.

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") command.

Example

```
avcli> LIST ATTRIBUTE OF SMTP SERVER;
```

The configuration data/attributes for the SMTP server appear.

A.8.9 REGISTER SMTP SERVER

Use the `REGISTER SMTP SERVER` command to register SMTP server configurations with Audit Vault 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]
```

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`).

Argument	Description
sender_email	The email address of the person whose ID you entered for the `SENDER ID`, in Request For Comments (RFC) 822 format.
username	Optional. The authentication credentials for the recipient user. If the SMTP server runs in authenticated mode and needs a valid *username* and *password* to connect to send emails, use the `AUTHENTICATED BY` clause to specify those credentials. Audit Vault Server prompts for the password. `AUTHENTICATED BY username/password` is accepted from file input through `.av` file.

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 after you run `REGISTER SMTP SERVER`.
- To test the configuration, run the `TEST SMTP SERVER` command.
- 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*.

> **See Also:**
>
> - ALTER SMTP SERVER SECURE MODE ON
> - TEST SMTP SERVER

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
```

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` connect to this server to send emails. The password has to be entered in the next step by following the prompt.

A.8.10 TEST SMTP SERVER

Use the `TEST SMTP SERVER` command to test the SMTP integration with Oracle Audit Vault Server by sending a test email.

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` command.
- You can recreate the configuration by running the `ALTER_SMTP SERVER` command.
- 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 Also:**
>
> - ALTER SMTP SERVER
> - REGISTER SMTP SERVER
> - LIST ATTRIBUTE OF SMTP SERVER

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`.

A.9 Security Assessment AVCLI Commands

Use the security assessment AVCLI commands to collect security assessment data for Oracle Database targets. Run these commands as an auditor user.

Related Topics

- Assessment Reports

A.9.1 RETRIEVE SECURITY ASSESSMENT FROM TARGET

Use the `RETRIEVE SECURITY ASSESSMENT FROM TARGET` command to submit security assessment jobs for Oracle Database targets.

Syntax

```
RETRIEVE SECURITY ASSESSMENT FROM TARGET target_name
```

Arguments

Argument	Description
target_name	Name of the Oracle Database target for which want to run the security assessment job.

Example

The following command retrieves security assessment data for the Oracle Database target named `t1`.

```
RETRIEVE SECURITY ASSESSMENT FROM TARGET t1
```

Related Topics

- LIST SECURED TARGET
  Use the `LIST SECURED TARGET` command to list various active targets that are registered with Audit Vault Server.

A.10 Security Management AVCLI Commands

The AVCLI security management commands enable you to manage various administrator and super administrator privileges.

A.10.1 About the Security Management AVCLI Commands

The security management `AVCLI` commands enable you to perform tasks such as registering and modifying SMTP connections.

A.10.2 ALTER DATA ENCRYPTION

Use the `ALTER DATA ENCRYPTION` command to change Transparent Data Encryption (TDE) configuration to rekey or to reset the repository encryption password.

The `ALTER DATA ENCRYPTION` command enables super administrators to change the Transparent Data Encryption (TDE) configuration in an Oracle Audit Vault Server repository. A super administrator can use this command to rekey the master encryption key, or to reset the repository encryption (wallet) password.

Syntax

```
ALTER DATA ENCRYPTION REKEY

ALTER DATA ENCRYPTION CHANGE WALLET PASSWORD
```

Examples

```
avcli> ALTER DATA ENCRYPTION REKEY;
```

This command rekeys the master encryption key for the Audit Vault Server repository.

```
avcli> ALTER DATA ENCRYPTION CHANGE WALLET PASSWORD;
```

This commands gives prompts to change the repository encryption (wallet) password.

A.10.3 ALTER USER

Use the `ALTER USER` command to unlock user accounts.

The `ALTER USER` command unlocks a user account. Only super administrators can run this command.

Syntax:

```
ALTER USER username ACCOUNT UNLOCK
```

Example:

```
avcli> ALTER USER scott ACCOUNT UNLOCK;
```

The account for user `scott` is unlocked.

> **Note:**
>
> To unlock *super administrator* or *super auditor*, follow these steps:
>
> 1. Connect to the Audit Vault Server as *root* user.
> 2. Switch user to dvaccountmgr: `su dvaccountmgr`
> 3. Run `sqlplus /`.
> 4. Run the command: `ALTER USER <super administrator/auditor username> ACCOUNT UNLOCK`

A.10.4 GRANT ACCESS

Use the `GRANT ACCESS` command to grant access to target names or target group names for specified users.

The `GRANT ACCESS` command grants access to a target name or 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 target.
secured_target_group_name	The name of the target group.

Example

```
avcli> GRANT ACCESS ON SECURED TARGET sample_source TO scott;
```

User `scott` granted access to target `sample_source`.

```
avcli> GRANT ACCESS ON SECURED TARGET GROUP hr_db_group TO hr;
```

User `hr` granted access to group of targets specified by the group `hr_db_group`.

A.10.5 GRANT ADMIN

Use the GRANT ADMIN command to grant administrator privileges to specified users.

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`.

A.10.6 GRANT AUDITOR

Use the GRANT AUDITOR command to grant auditor privileges to the specified user.

The `GRANT AUDITOR` command grants auditor privileges to the specified user.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax

```
GRANT AUDITOR TO <username>
```

Arguments

Argument	Description
username	The specified user.

Example

```
avcli> GRANT AUDITOR TO scott;
```

Auditor privileges granted to user `scott`.

A.10.7 GRANT SUPERADMIN

Use the `GRANT SUPERADMIN` command to grant super administrator privileges to users who are specified by username.

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`.

A.10.8 GRANT SUPERAUDITOR

Use the `GRANT SUPERAUDITOR` command to grant super auditor privileges to a specific user.

The `GRANT SUPERAUDITOR` command grants super auditor privileges to the specified user.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax

```
GRANT SUPERAUDITOR TO <username>
```

Arguments

Argument	Description
username	The specified user.

Usage Notes

This user automatically receives regular auditor rights as well.

Example

```
avcli> GRANT SUPERAUDITOR TO scott;
```

Super auditor (and auditor) privileges granted to user `scott`.

A.10.9 REVOKE ACCESS

Use the REVOKE ACCESS command to revoke access to targets or target group names for specified users.

The `REVOKE ACCESS` command revokes access to a target or 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 target.
secured_target_group_name	The name of the target group.

Example

```
avcli> REVOKE ACCESS ON SECURED TARGET sample_source FROM scott;
```

Access to target `sample_source` revoked from user `scott`.

```
avcli> REVOKE ACCESS ON SECURED TARGET GROUP hr_db_group FROM hr;
```

Access to a group of targets specified by the group `hr_db_group` revoked from user `hr`.

A.10.10 REVOKE ADMIN

Use the REVOKE ADMIN command to revoke administrator privileges from specified users.

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`.

A.10.11 REVOKE AUDITOR

Use the REVOKE AUDITOR command to revoke auditor privileges from specified users.

The `REVOKE AUDITOR` command revokes auditor privileges from specified user.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax:

```
REVOKE AUDITOR FROM <username>
```

Arguments

Argument	Description
username	The specified user.

Example

```
avcli> REVOKE AUDITOR FROM scott;
```

Auditor privileges revoked from user `scott`.

A.10.12 REVOKE SUPERADMIN

Use the `REVOKE SUPERADMIN` command to revoke super administrator privileges from users who are specified by username.

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`.

A.10.13 REVOKE SUPERAUDITOR

Use the `REVOKE SUPERAUDITOR` command to revoke super auditor privileges from a specific user.

The `REVOKE SUPERAUDITOR` command revokes super auditor privileges from a specific user.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax

```
REVOKE SUPERAUDITOR FROM <username>
```

Arguments

Argument	Description
`username`	The specified user.

Usage Notes

The user continues to retain regular auditor rights.

Example

```
avcli> REVOKE SUPERAUDITOR FROM scott;
```

Super auditor privileges are revoked from user `scott`. User `scott` continues to be a normal auditor.

A.10.14 SHOW DATA ENCRYPTION STATUS

Use the `SHOW DATA ENCRYPTION STATUS` command to show whether data encryption is enabled for Oracle Audit Vault Server repositories.

The `SHOW DATA ENCRYPTION STATUS` command shows whether encryption is enabled or disabled. Encryption is automatically enabled on new installations.

Syntax

```
SHOW DATA ENCRYPTION STATUS
```

Example

```
avcli> SHOW DATA ENCRYPTION STATUS;
```

This command shows the encryption status (enabled or disabled).

A.11 SAN Storage AVCLI Commands

You can manage SAN servers with SAN storage AVCLI commands.

A.11.1 About the SAN Storage AVCLI Commands

The `AVCLI` SAN storage commands enable you to perform tasks such as registering and altering SAN servers.

A.11.2 ALTER DISKGROUP

Use the `ALTER DISK GROUP` command to alter a diskgroup by adding or dropping disks.

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".

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.

A.11.3 ALTER SAN SERVER

Use the `ALTER SAN SERVER` command to alter SAN servers that are registered with Audit Vault Server by logging into or logging out of a target that is available on the SAN server.

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] [ON SECONDARY]


ALTER SAN SERVER server_name LOGOUT target_name ADDRESS address  [PORT port]
[AUTHENTICATED BY username] [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".
address	IP address or hostname of the target on the SAN server
port	Optional. Default is 3260.
username	If needed, credential used to log in to the target. The user name and password is accepted from file input through `.av` file.

Example

```
avcli> ALTER SAN SERVER testServer1 LOGIN target1 ADDRESS sample_target.example.com
AUTHENTICATED BY username1;
```

Alter the SAN server `testServer1` by logging into `target1` at address `sample_target.example.com` using credentials `username1`. 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`.

A.11.4 DROP SAN SERVER

Use the `DROP SAN SERVER` command to drop SAN servers that are registered with Oracle Audit Vault Server.

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.

A.11.5 LIST DISK

Use the `LIST DISK` commant to see details of disks that are available on your system.

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.

A.11.6 LIST DISKGROUP

Use the `LIST DISKGROUP` command to see the details of all disk groups in your system.

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".

A.11.7 LIST SAN SERVER

Use the `LIST SAN SERVER` command to display the details of SAN servers that are registered with Oracle Audit Vault Server.

The `LIST SAN SERVER` command displays details of SAN servers registered with Oracle 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.

A.11.8 LIST TARGET FOR SAN SERVER

Use the `LIST TARGET FOR SAN SERVER` command to alter SAN servers that are registered with Oracle Audit Vault Server by logging into or logging out of a target that is available on the SAN server

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`.

A.11.9 REGISTER SAN SERVER

Use the `REGISTER SAN SERVER` to register SAN servers of a specified storage type with Audit Vault Server.

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>]`
	`ISNS`
	
	`AUTHENTICATED BY <username>/<password>` is accepted from file input through `.av` file.
	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;
```

Registers a SAN server `testServer2` of storage type `iSCSI` at address `192.0.2.1` using the discover method `sendtargets` with credentials `username2`.

A.11.10 SHOW iSCSI INITIATOR DETAILS FOR SERVER

Use the `SHOW iSCSI INITIATOR DETAILS FOR SERVER` command to see the iSCSI initiator details for Oracle Audit Vault Server.

The `SHOW ISCSI INITIATOR DETAILS FOR SERVER` command displays iSCSI initiator details for Oracle 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.

A.12 Remote File System AVCLI Commands

Use the remote file system AVCLI commands to mange remote file systems. These commands support registering and managing connections to NFS file systems that are used as archive locations.

A.12.1 About the Remote File System AVCLI Commands

Use the remote file system `AVCLI` commands to configure remote file systems to work with Oracle Audit Vault and Database Firewall.

A.12.2 ALTER REMOTE FILESYSTEM

Use the `ALTER REMOTE FILESYSTEM` command to alter remote file systems that are registered with Oracle Audit Vault Server.

The `ALTER REMOTE FILESYSTEM` command alters a remote filesystem registered with Oracle 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.

A.12.3 DROP REMOTE FILESYSTEM

Use the `DROP REMOTE FILESYSTEM` command to drop remote file sytems that are registered with Oracle Audit Vault Server.

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`.

A.12.4 LIST EXPORT

Use the `LIST EXPORT` command to display the list of exports that are available on an NFS server.

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.

A.12.5 LIST REMOTE FILESYSTEM

Use the `LIST REMOTE FILESYSTEM` command to list all of the remote file systems that are registered with Oracle Audit Vault Server.

The `LIST REMOTE FILESYSTEM` command lists all of the remote file systems that are registered with Oracle Audit Vault Server.

Syntax:

```
LIST REMOTE FILESYSTEM
```

Example:

```
avcli> LIST REMOTE FILESYSTEM;
```

Lists all remote filesystems registered with Oracle Audit Vault Server.

A.12.6 REGISTER REMOTE FILESYSTEM

Use the `REGISTER REMOTE FILESYSTEM` command to register remote file systems with Oracle Audit Vault Server.

The `REGISTER REMOTE FILESYSTEM` command registers a remote file system with the Audit Vault Server. This command currently supports registering an NFS file system. After registering a remote file system, an administrator can select it when specifying an archive location.

Syntax:

```
REGISTER REMOTE FILESYSTEM <remote filesystem name> OF TYPE NFS ON HOST <IP address or
host name of NFS server> USING EXPORT export [ON STANDBY HOST <IP address or host name
of NFS server> USING STANDBY EXPORT <export>][MOUNT]
```

Arguments

Argument	Description
filesystem_name	A unique name for the remote file system. Special characters (&<>"/;,*|=% and --) cannot be used for remote file system names.
NFS_server_address	Host name or IP address of the NFS server

Argument	Description
export	Name of the export directory on the NFS server. This directory must be created in `etc/exports` file of the NFS server. **Note:** Special characters (such as $, #, and !) are not allowed in export directory names.

Note:

1. Log in as *Oracle* user `503` to register the remote file system. Use the same user name on the NFS Server and the Audit Vault Server.
2. If this is any different, then edit the `/etc/passwd/` file in the NFS Server and change the USER ID of *Oracle* user to `503`.

Examples:

```
avcli> REGISTER REMOTE FILESYSTEM haFileSystem OF TYPE NFS ON HOST 10.0.0.1 USING
EXPORT /export/home1 AND ON STANDBY HOST 10.0.0.2 USING STANDBY EXPORT /export/home2;
```

Registers a remote NFS file system named `haFileSystem` on the host `10.0.0.1` using the export directory `/export/home1` on standby host `10.0.0.2` using standby export `/export/home2`. This will mount the registered remote file system.

```
avcli> REGISTER REMOTE FILESYSTEM sample_Filesystem OF TYPE NFS ON HOST
example_host.example.com USING EXPORT /export/home1 MOUNT;
```

Registers a remote NFS file system named `sample_Filesystem` on the host `example_host.example.com` using the export directory `/export/home1`. This will also mount the registered remote file system.

```
register remote filesystem haFileSystem of type nfs on host 10.0.0.1 using
export /export/home1 and on standby host 10.0.0.2 using standby export/export/
home2;
```

Registers a remote file system named `haFileSystem` of type NFS on the host `10.0.0.1` using the export directory `/export/home1` on standby host `10.0.0.2` using standby export `/export/home2`.

A.12.7 SHOW STATUS OF REMOTE FILESYSTEM

Use the `SHOW STATUS OF REMOTE FILESYSTEM` command to show the status of remote file systems that are registered with Oracle Audit Vault Server.

The `SHOW STATUS OF REMOTE FILESYSTEM` command shows the status of a specified remote file system.

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`.

A.13 Server Management AVCLI Commands

The server management AVCLI commands enable you to manage the server, such as checking certificates and downloading log files.

A.13.1 About the Server Management AVCLI Commands

The `AVCLI` server management commands manage aspects of Oracle Audit Vault and Database Firewall such as altering the system set.

A.13.2 ALTER SYSTEM SET

Use the `ALTER SYSTEM SET` command to modify system configuration data.

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-7.

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 in the *$Oracle_Home*`/av/log` directory in the Audit Vault Server.

The following *attributes* are supported:

Table A-7 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* See Table A-8 for 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.
SYS.AUTOSTART_INTERVAL	The interval in seconds before the system will try to restart failed audit trails. Default: 1800
SYS.AUTOSTART_RETRY_COUNT	The number of times the system attempts to start failed audit trails. Oracle AVDF release 20.1 to 20.6: 5 times (default) Oracle AVDF release 20.7 and onwards: 20 times (default)

Table A-8 shows valid values for *component_name* and *loglevel_value* for the LOGLEVEL attribute:

Table A-8 Logging component names and values

Logging component name	Values
AlertLog	Alert
AgentLog	Agent
ARLog	Archive and Retrieve
DWLog	Data Warehouse
FWLog	Database Firewall
GUIlog	Web Concole UI
JfwkLog	Java Server Process
NotifyLog	Notification
PfwkLog	Plug-in Management
PolicyLog	Policy Management
ReportLog	Report Generation
SanLog	SAN Storage
TransLog	Transaction Log Trail
All	All components. Valid only with ERROR and WARNING log level values.

Table A-9 Logging level and values

Parameter	Description
ERROR	The ERROR log level
WARNING	The WARNING log level (not supported for GUIlog)

Table A-9 (Cont.) Logging level and values

Parameter	Description
INFO	The INFO log level
DEBUG	The DEBUG log level Be aware that DEBUG generates many files and that this can affect the performance of your system. Only use it when you are trying to diagnose problems.

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;
```

The log levels of the JfwkLog and PfwkLog components running on the system change.

```
avcli> ALTER SYSTEM SET SYS.AUTOSTART_INTERVAL=900;
```

The system will restart failed audit trails after 900 seconds.

> **See Also:**
>
> Downloading Detailed Diagnostics Reports for Oracle Audit Vault Server for information about generating a diagnostics report that captures Audit Vault Server appliance information.

A.13.3 DOWNLOAD LOG FILE

Use the DOWNLOAD LOG FILE to download Oracle Audit Vault Server log files to perform diagnostics,

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.

A.13.4 SHOW CERTIFICATE

Use the `SHOW CERTIFICATE` command to display Oracle Audit Vault Server certificates.

The `SHOW CERTIFICATE` command displays the certificate for the Audit Vault Server.

Syntax

```
SHOW CERTIFICATE FOR SERVER
```

Example

```
avcli> SHOW CERTIFICATE FOR SERVER;
```

The Oracle Audit Vault Server certificate appears.

A.14 Collection Plug-In AVCLI Commands

Use the `AVCLI` collection plug-in commands to manage the deployment of collection plug-ins.

A.14.1 About the Collection Plug-In AVCLI Commands

Use the `AVCLI` collection plug-in commands to work with plug-ins, such as downloading and listing plug-ins.

A.14.2 DEPLOY PLUGIN

Use the `DEPLOY PLUGIN` command to deploy plug-ins into Oracle Audit Vault Server homes from a given archive file.

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 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.

A.14.3 LIST PLUGIN FOR SECURED TARGET TYPE

Use the `LIST PLUGIN FOR SECURED TARGET TYPE` command to list all of the plug-ins in Audit Vault Server installations.

The `LIST PLUGIN FOR SECURED TARGET TYPE` command lists all the plug-ins that support a particular target type.

Syntax

```
LIST PLUGIN FOR SECURED TARGET TYPE secured target type name
```

Arguments

Argument	Description
secured target type name	The name of the target type

Usage Notes

To find a list of available target types, see "LIST SECURED TARGET TYPE".

Examples

```
avcli> LIST PLUGINS FOR SECURED TARGET TYPE "Oracle Database";
```

The plug-ins that support the target type "Oracle Database" are listed.

A.14.4 UNDEPLOY PLUGIN

Use the `UNDEPLOY PLUGIN` command to undeploy plug-ins from Oracle Audit Vault Server homes.

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.

A.15 General Usage AVCLI Commands

You can find general information, such as help, from the general usage AVCLI commands.

A.15.1 About the General Usage AVCLI Commands

The `AVCLI` general usage commands enable you to perform tasks such as connecting to servers or identifying users.

A.15.2 CLEAR LOG

Use the `CLEAR LOG` command to clear a system's diagnostic logs.

The `CLEAR LOG` command deletes all log files in the directory `$ORACLE_HOME/av/log` on the Audit Vault Server.

Syntax

```
CLEAR LOG
```

Example

```
avcli> CLEAR LOG;
```

A.15.3 CONNECT

Use the `CONNECT` command to connect the current AVCLI user as a different user.

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 Audit Vault Command Line Interface".

Example 1

```
avcli> CONNECT psmith;
Enter password: password
```

```
Connected.
```

Example 2

```
avcli> CONNECT;
Enter user name: username
Enter password: password

Connected.
```

A.15.4 HELP

Use the HELP command to list the AVCLI commands with their categories.

The HELP command lists all available AVCLI commands and their categories.

Syntax

```
HELP
```

Example

```
avcli> HELP;
```

A.15.5 -HELP

Use the -HELP command to display help information for all of the AVCLI utility commands.

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 12.2.0.0.0 - Production on Thu Nov 8 00:53:54 UTC 2012


Copyright (c) 1996, 2015 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)
```

A.15.6 QUIT

Use the `QUIT` command to exit AVCLI.

The `QUIT` command exits `AVCLI`.

Syntax

```
QUIT
```

Example

```
avcli> QUIT;
```

A.15.7 SHOW USER

Use the `SHOW USER` command to display the currently logged in AVCLI user.

The `SHOW USER` command displays the currently logged in AVCLI user.

Syntax

```
SHOW USER
```

Example

```
avcli> SHOW USER;
```

A.15.8 STORE CREDENTIALS

Use the `STORE CREDENTIALS` command to store administrator credentials in AVCLI wallet, or to overwrite previously stored credentials.

The `STORE CREDENTIALS` command lets you store credentials for one Oracle Audit Vault and Database Firewall administrator in the Oracle AVCLI wallet, or update existing credentials in the wallet.

Syntax

```
STORE CREDENTIALS [FOR USER username]
```

Example 1

```
avcli> STORE CREDENTIALS FOR USER admin1;
Enter password: password
Re-enter password: password
```

Example 2

```
avcli> STORE CREDENTIALS;
Enter user name: admin1
Enter password: password
Re-enter password: password
```

A.15.9 -VERSION

Use the `-VERSION` command to display the AVCLI version number.

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 12.2.0.0.0 - Production on Tue Apr 26 14:25:31 PDT 2011

Copyright (c) 2014, Oracle.  All Rights Reserved.
```

A.16 Retention Policy AVCLI Commands

You can find general information on retention policy (or Information Lifecycle Management) related AVCLI commands.

A.16.1 APPLY RETENTION POLICY

Use the `APPLY RETENTION POLICY` command to apply a retention policy to a target. This can be applied only by a super auditor.

To apply a retention policy to a target.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
APPLY RETENTION POLICY <policy name> TO TARGET <target name>
```

This command applies a specific retention policy to a specified target.

Arguments

Argument	Description
policy name	The name of the policy on which the retention policy needs to be applied.
target name	The name of specified target for which the policy needs to be applied.

Example

```
apply retention policy test_policy1 to target test_target1;
```

Applies policy `test_policy1` to target `test_target1`.

A.16.2 CREATE RETENTION POLICY

Use the `CREATE RETENTION POLICY` command to create a retention (or lifecycle) policy. This can be created only by a super administrator.

To create a retention policy.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
CREATE RETENTION POLICY <policy name> ONLINE MONTHS <month number> ARCHIVED MONTHS
<month number>
```

This command creates a retention policy with the specified name and specifies the number of online months and archived months. A policy name cannot be null, start with reserved name, or be the same as an existing policy name. Only alphanumeric, underscore (_), dollar sign ($), and pound sign (#) are allowed for the policy name.

Arguments

Argument	Description
`policy name`	The name of the policy to be created.
`month number`	The number of months to be online or to be archived. The number of months for online, must be between 1 and 9000. The number of months to be archived, must be between 0 and 9000. **Note:** In case the above guidelines for the number of months (online and to be archived) are not followed, then an error may be observed.

Example

```
create retention policy test_policy1 online months 2 archived months 3;
```

Creates a retention policy with the name `test_policy1` and sets 2 months online and 3 months as the archival period.

A.16.3 DELETE RETENTION POLICY

Use the `DELETE RETENTION POLICY` command to delete a retention policy.

To delete a retention policy.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
DELETE RETENTION POLICY <policy name>
```

This command deletes the specified retention policy.

Arguments

Argument	Description
policy name	The name of the retention policy to be deleted.

Example

```
delete retention policy test_policy1;
```

Deletes `test_policy1`.

A.16.4 LIST RETENTION POLICIES

Use the `LIST RETENTION POLICIES` command to view all the retention policies.

To view all the retention policies.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
LIST RETENTION POLICIES
```

This command lists all retention policies.

Example

```
list retention policies;
```

Lists all the retention policies.

A.16.5 SET RETENTION POLICY AS DEFAULT

Use the `SET RETENTION POLICY` command to set a retention policy as default.

Syntax

```
SET RETENTION POLICY <policy name> AS DEFAULT
```

This command sets the specified retention policy as default.

Arguments

Argument	Description
policy name	The name of the retention policy to be set as default.

Example

```
set retention policy '1 month online, 0 month in archive' as default;
```

Sets the policy `1 month online, 0 month in archive` as the default policy.

A.16.6 SHOW RETENTION POLICY FOR TARGET

Use the `SHOW RETENTION POLICY FOR TARGET` command to display the current retention policy defined for the specified target.

To view the lifecycle policy defined for the specified target.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
SHOW RETENTION POLICY FOR TARGET <target name>
```

This command displays the current retention policy for the specified target.

Arguments

Argument	Description
target name	The name of specified target for which the policy needs to be viewed.

Example

```
show retention policy for target test_target1;
```

Displays the current policy for `test_target1`.

A.17 Alert Policy Management AVCLI Commands

You can find general information on alert policy management related AVCLI commands.

A.17.1 DELETE ALERT POLICY

Use the `DELETE ALERT POLICY` command to delete an alert policy.

To delete an alert policy.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
DELETE ALERT POLICY <alert policy name>
```

This command deletes the alert policy with the specified name.

Arguments

Argument	Description
alert policy name	The name of the alert policy to be deleted.

Example

```
delete alert policy test_alert1;
```

Deletes alert policy with the specified name `test_alert1`.

A.17.2 DISABLE ALERT POLICY

Use the `DISABLE ALERT POLICY` command to disable an alert policy.

To disable an alert policy.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
DISABLE ALERT POLICY <alert policy name>
```

This command disables the alert policy with the specified name.

Arguments

Argument	Description
alert policy name	The name of the alert policy to be disabled.

Example

```
disable alert policy test_alert1;
```

Disables the alert policy with the name `test_alert1`.

A.17.3 ENABLE ALERT POLICY

Use the `ENABLE ALERT POLICY` command to enable an alert policy.

To enable an alert policy.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
ENABLE ALERT POLICY <alert policy name>
```

Arguments

Argument	Description
alert policy name	The name of the alert policy to be enabled.

Example

```
enable alert policy test_alert1;
```

Enables alert policy with the name `test_alert1`.

A.17.4 LIST ALERT POLICIES

Use the `LIST ALERT POLICIES` command to list all the active alert policies.

Lists all the active alert policies.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
LIST ALERT POLICIES
```

This command lists all the active alert policies.

Example

```
list alert policies;
```

A.18 Unified Audit Policy AVCLI Commands

You can find general information on unified audit policy related AVCLI commands.

A.18.1 ENABLE UNIFIED AUDIT POLICY

Use the `ENABLE UNIFIED AUDIT POLICY` command to enable a unified audit policy.

To enable a unified audit policy for a target. This command provisions the unified audit policy specified on the target.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
ENABLE UNIFIED AUDIT POLICY <policy name> [EXCLUDE USERS <user names>] [LIST OF USERS
<user names>] ON TARGET <target name>
```

This command provisions the unified audit policy with the specified policy name on the specific target. The policy name must be specified with the actual name.

Arguments

Argument	Description
policy name	The name of policy to be provisioned or enabled.
user names	A list of users separated by comma. This is optional.
target name	The name of specific target for which the unified audit policies is to be enabled.
EXCLUDE USERS	Optional parameter required for *LOGON EVENTS* and *USER ACTIVITY*. The list of user names must be separated by comma.
LIST OF USERS	Optional parameter required for *LOGON EVENTS* and *USER ACTIVITY*. The list of user names must be separated by comma.

Result

The job to provision audit policy is successfully submitted. The status of the job can be viewed in the Audit Vault Server console. Provisioning audit policy takes at least a minute to complete.

Examples

```
enable unified audit policy tp1 on target t1;
```

Toggles policy `tp1` of target `t1` to ON.

```
enable unified audit policy 'User Activity' list of users 'BOB,JOHN' on target t1;
```

Enables `User Activity` policy for users *BOB* and *JOHN* on target `t1`.

```
enable unified audit policy 'Logon Events' exclude users 'BOB,JOHN' on target t1;
```

Enables *LOGON EVENTS* policy for users `BOB` and `JOHN` on target `t1`.

Edit Unified Audit Policy

Starting Oracle AVDF 20.4, Custom and Oracle Predefined Unified policies can be enforced on users, roles, and on specific event conditions (successful, unsuccessful, or both).

Syntax

```
ENABLE UNIFIED AUDIT POLICY <policy name> ON TARGET <target name> [WHENEVER
SUCCESSFUL | WHENEVER NOT SUCCESSFUL]


ENABLE UNIFIED AUDIT POLICY <policy name> ON TARGET <target name> FOR USERS
EXCEPT <user names> [WHENEVER SUCCESSFUL] [WHENEVER NOT SUCCESSFUL]


ENABLE UNIFIED AUDIT POLICY <policy name> ON TARGET <target name> { [FOR
USERS <user names> WHENEVER SUCCESSFUL] [FOR USERS <user names> WHENEVER NOT
SUCCESSFUL] [FOR USERS <user names>] [FOR USERS WITH ROLES <role names>
WHENEVER SUCCESSFUL] [FOR USERS WITH ROLES <role names> WHENEVER NOT
SUCCESSFUL] [FOR USERS WITH ROLES <role names>]}
```

Arguments

Argument	Description
policy name	The name of policy to be provisioned or enabled.
target name	The name of the specific target for which the unified audit policies have to be enabled.
FOR USERS EXCEPT	Optional parameter. The list of user names must be separated by comma.
FOR USERS	Optional parameter. The list of user names must be separated by comma.
FOR USERS WITH ROLES	Optional parameter. The list of roles must be separated by comma.
WHENEVER SUCCESSFUL	Optional parameter. The policy is enabled for success events.
WHENEVER NOT SUCCESSFUL	Optional parameter. The policy is enabled for fail events.

Examples

```
enable unified audit policy tp1 on target t1;
```

Toggles policy `tp1` of target `t1` to ON.

```
enable unified audit policy on target t1 'User Activity' for users 'BOB,JOHN';
```

Enables 'User Activity' policy for users *BOB* and *JOHN* on target `t1`.

```
enable unified audit policy on target t1 'Logon Events' for users except
'BOB,JOHN';
```

Enables 'Logon Events' policy for users *BOB* and *JOHN* on target `t1`.

```
enable unified audit policy tp2 on target t1 for users 'SCOTT' whenever
successful for users with roles 'DBA' whenever not successful;
```

Enables policy `tp2` for users *SCOTT* whenever it is successful and for users with granted roles `dba` whenever is not successful on target `t1`.

```
enable unified audit policy tp3 on target t1 for users 'HR';
```

Enables policy `tp2` for users *HR* for both success/failure events on target `t1`.

Enabling Security Technical Implementation Guidelines (STIG) Compliance

Starting Oracle AVDF 20.5, a new category **Security Technical Implementation Guidelines (STIG)** is available for Unified audit policy. Security Technical Implementation Guidelines (STIG) category can be enabled on Oracle Database targets to make the target STIG compliant. Security Technical Implementation Guidelines (STIG) category is available for Oracle Database target starting with version 21.

Syntax

```
ENABLE UNIFIED AUDIT POLICY "Security Technical Implementation Guidelines
(STIG)" ON TARGET <target name>;
```

This command enables the following predefined policies available in Oracle Database version starting with 21.

Predefined Audit Policies Name	Can be enabled for users	Event Condition
`ORA_STIG_RECOMMENDATIONS`	All users	• Success • Failure
`ORA_LOGON_LOGOFF`	All users	• Success • Failure
`ORA_ALL_TOPLEVEL_ACTIONS`	Privileged users	• Success • Failure

Privileged users are users retrieved from the user entitlement job.

In case the user entitlement job was never retrieved, then the audit provisioning job will retrieve the user entitlement first to get the privileged users before enabling the above policies in target database.

```
ENABLE UNIFIED AUDIT POLICY "Security Technical Implementation Guidelines
(STIG)" ON TARGET <target name> FOR USERS <user names>;
```

This command enables following Oracle Predefined policies available in Oracle Database version starting with 21:

- `ORA_STIG_RECOMMENDATIONS` audit policy will be enabled for all users for both successful and failed events.
- `ORA_LOGON_LOGOFF` audit policy will be enabled for all users for both successful and failed events.
- `ORA_ALL_TOPLEVEL_ACTIONS` will be enabled for users provided in the enable statement for both successful and failed events.

Arguments

Argument	Description
target name	The name of the specific target for which the unified audit policies have to be enabled.
FOR USERS	Optional parameter. The list of user names must be separated by comma.

A.18.2 LIST UNIFIED AUDIT POLICIES

Use the `LIST UNIFIED AUDIT POLICIES` command to list all the various unified core, oracle pre-defined, custom, and all the unified policies of a specific target.

To view all the various unified core, Oracle pre-defined, custom, and all the unified policies of a specific target. The output is displayed in the format `|Unified Policy Name|Enabled (Yes/No)|`.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
LIST UNIFIED AUDIT CORE POLICIES FOR TARGET <target name>
```

This command lists all the core policies for the specified target.

```
LIST UNIFIED AUDIT ORACLE PREDEFINED POLICIES FOR TARGET <target name>
```

This command lists all the Oracle pre-defined policies for the specified target.

```
LIST UNIFIED AUDIT CUSTOM POLICIES FOR TARGET <target name>
```

This command lists all the custom policies for the specified target.

```
LIST UNIFIED AUDIT POLICIES FOR TARGET <target name>
```

This command lists all the unified policies for the specified target.

Arguments

Argument	Description
target name	The name of specified target for which the unified audit policies need to be viewed.

Examples

```
list unified audit policies for target tg1;
```

Lists all the unified audit policies (for example core, custom, and others) for `tg1`.

```
list unified audit oracle predefined policies for target tg1;
```

Lists all the Oracle pre-defined policies for `tg1`.

```
list unified audit custom policies for target tg1;
```

Lists all the custom policies for `tg1`.

```
list unified audit policies for target tg1;
```

Lists all the unified policies for `tg1`.

A.18.3 DISABLE UNIFIED AUDIT POLICY

Use the `DISABLE UNIFIED AUDIT POLICY` command to disable a unified audit policy.

To disable a unified audit policy. This command provisions the unified audit policy specified on the target and turns it off. The policy name must be specified properly.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.3.

Syntax

```
DISABLE UNIFIED AUDIT POLICY <policy name> ON TARGET <target name>
```

Arguments

Argument	Description
policy name	The name of policy to be disabled.
target name	The name of specific target for which the unified audit policies is to be disabled.

Result

The job to provision audit policy is successfully submitted. The status of the job can be viewed in the Audit Vault Server console. Provisioning audit policy takes at least a minute to complete.

Examples

```
disable unified audit policy tp1 on target t1;
```

Disables the policy `tp1` on `t1`.

A.18.4 RETRIEVE AUDIT POLICIES

Use the `RETRIEVE AUDIT POLICIES` command to retrieve audit policies configured on the target.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.8.

Syntax

```
RETRIEVE AUDIT POLICIES FROM TARGET <target name>
```

This command retrieves audit policies configured on the specified target.

Arguments

Argument	Description
target name	The name of the specific target for which the audit policies have to be retrieved. The name is case-sensitive and must be one of the registered targets. See LIST SECURED TARGET for a list of registered targets. Special characters (`&<>"/;,*|=% --`) cannot be used for target names.

Result

The job to retrieve audit settings is submitted successfully. The status of the job can be viewed in the Audit Vault Server console.

In case the audit setting retrieval job fails due to connection issues, then check the connection details of the specified target.

A.19 AVCLI User Commands

You can run AVCLI user commands to create users, assign roles, reset passwords, and delete users.

A.19.1 About the User AVCLI Commands

The `AVCLI` general user commands enable you to perform tasks such as creating and dropping Oracle Audit Vault users.

A.19.2 ALTER ADMIN

Use the `ALTER ADMIN` command to reset the password for an admin or superadmin user. Only a superadmin can reset the password for an admin or superadmin user.

The `ALTER ADMIN` command resets the password of the user with admin role. A superadmin can modify the password of the user with admin role.

Syntax

```
ALTER ADMIN <user name>
```

Arguments

Argument	Description
user name	The existing user with *admin* role who requires a password reset.
password	The command prompts a password for modifying the password of the user with *admin* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.

Example

```
alter admin myadmin
```

This command resets the password of the existing user *myadmin*. The password for *myadmin* is taken from the prompt.

Oracle AVDF 20.3 and later

This command is used to modify an *ADMIN* user type or reset an *ADMIN* user's password. This command can be run only by a *SUPERADMIN* user.

Syntax

```
ALTER ADMIN <username> ADMIN TYPE <type>
```

This command changes the *ADMIN* user's type.

```
ALTER ADMIN <username> CHANGE PASSWORD
```

This command resets the password of the specified user name. The user password is taken from the prompt.

Arguments

Argument	Description
user name	The existing user with *ADMIN* role who requires a password reset.
type	Type specifies the particular type of *ADMIN* role being created. The type can only be either *ADMIN* or *SUPERADMIN*.
password	The command prompts a password for modifying the password of the user with *ADMIN* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.

Examples

```
alter admin myadmin admin type admin;
```

Changes the type of user `myadmin` to *ADMIN* role.

```
alter admin myadmin change password;
```

Resets the password of user `myadmin`. The password for `myadmin` is taken from the prompt.

A.19.3 ALTER AUDITOR

Use the `ALTER AUDITOR` command to reset the password for existing auditors or superauditor users. Only a superauditor can reset the password for auditors or superauditor users.

The `ALTER AUDITOR` command resets the password of the user with auditor role. A superauditor can modify the password of the user with auditor role.

Syntax

```
ALTER AUDITOR <user name>
```

Arguments

Argument	Description
user name	The existing user with *auditor* role who requires a password reset.
password	The command prompts a password for modifying the password of the user with *auditor* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.

Example

```
alter auditor myauditor
```

This command resets the password of the existing user *myauditor*. The password for *myauditor* is taken from the prompt.

Oracle AVDF 20.3 and later

This command is used to modify an *AUDITOR* user type or reset an *AUDITOR* user's password. This command can be run only by a *SUPERAUDITOR* user.

Syntax

```
ALTER AUDITOR <username> AUDITOR TYPE <type>
```

This command changes the *AUDITOR* user's type.

```
ALTER AUDITOR <username> CHANGE PASSWORD
```

This command resets the password of the specified user name. The user password is taken from the prompt.

Arguments

Argument	Description
user name	The existing user with *AUDITOR* role who requires a password reset.
type	Type specifies the particular type of *AUDITOR* role being created. The type can only be either *AUDITOR* or *SUPERAUDITOR*.
password	The command prompts a password for modifying the password of the user with *AUDITOR* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.

Examples

```
alter auditor myauditor auditor type superauditor;
```

Modify the type of user `myauditor` to *SUPERAUDITOR* role.

```
alter auditor myauditor change password;
```

Resets the password of user `myauditor`. The password for `myauditor` is taken from the prompt.

A.19.4 CREATE ADMIN

Use the `CREATE ADMIN` command to create users with the admin role. Only a superadmin can create a user with admin role.

The `CREATE ADMIN` command creates a user with admin role. A superadmin can create a user with admin role.

Syntax

```
CREATE ADMIN user name
```

Arguments

Argument	Description
user name	The name of the user being created with *admin* role. The *user name* cannot be null, start with any reserved user name, or be the same as any of the existing user role. It must be alphanumeric only and can contain underscore (_), dollar sign ($), and pound sign (#).
password	The command prompts a password before creating a user with *admin* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.

Example

```
create admin myadmin
```

This command creates a user *myadmin* with *admin* role. The user password is taken from the prompt.

Oracle AVDF 20.3 and later

This command creates a user with administrator privileges. A super administrator can create a user with admin role.

Syntax

```
CREATE ADMIN <user name> ADMIN TYPE <type>
```

This command prompts a password and creates a user with the specified user name and assigns *ADMIN* or *SUPERADMIN* privileges.

Arguments

Argument	Description
user name	The name of the user being created with *ADMIN* role. The *user name* cannot be null, start with any reserved user name, or be the same as any of the existing user role. It must be alphanumeric only and can contain underscore (_), dollar sign ($), and pound sign (#). It can have a maximum of 30 characters in length.
password	The command prompts a password before creating a user with *ADMIN* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.
type	Type specifies the particular type of administrator role being created. The type can only be either *ADMIN* or *SUPERADMIN*. *ADMIN* gives administrator privileges, while *SUPERADMIN* gives super administrator privileges.

Example

```
create admin myadmin admin type superadmin
```

Creates user `myadmin` with *SUPERADMIN* type. The user password is taken from the prompt.

A.19.5 CREATE AUDITOR

Use the `CREATE AUDITOR` command to create users with the auditor role. Only superauditors can create users with the auditor role.

The `CREATE AUDITOR` command creates a user with the auditor role. A superauditor can create a user with auditor role.

Syntax

```
CREATE AUDITOR user name
```

Arguments

Argument	Description
user name	The name of the user being created with *auditor* role. The *user name* cannot be null, start with any reserved user name, or the same as any of the existing user role. It must be alphanumeric only and can contain underscore (_), dollar sign ($), and pound sign (#).
password	The command prompts a password before creating a user with *auditor* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.

Example

```
create auditor myauditor
```

This command creates a user *myauditor* with *auditor* role. The user password is taken from the prompt.

Oracle AVDF 20.3 and later

This command creates a user with *AUDITOR* privileges. A super auditor can create a user with auditor role.

Syntax

```
CREATE AUDITOR <username> AUDITOR TYPE <type>
```

This command prompts a password and creates a user with the specified user name and assigns *AUDITOR* privileges.

Arguments

Argument	Description
user name	The name of the user being created with *auditor* role. The *user name* cannot be null, start with any reserved user name, or the same as any of the existing user role. It must be alphanumeric only and can contain underscore (_), dollar sign ($), and pound sign (#). It can have a maximum of 30 characters in length.
password	The command prompts a password before creating a user with *auditor* role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). A password must be at least 8 characters and at most 30 bytes in length.
type	Type specifies the particular type of auditor role being created. The type can only be either *AUDITOR* or *SUPERAUDITOR*. *AUDITOR* gives auditor privileges, while *SUPERAUDITOR* gives super auditor privileges.

Example

```
create auditor myauditor auditor type superauditor;
```

Creates user `myauditor` with *SUPERAUDITOR* type. The user password is taken from the prompt.

A.19.6 DROP ADMIN

Use the `DROP ADMIN` command to drop or delete admin or superadmin users. Only a superadmin can drop an admin or superadmin user.

The `DROP ADMIN` command drops or deletes a user with admin role. A superadmin can drop a user with admin role.

Syntax

```
DROP ADMIN user name
```

Arguments

Argument	Description
user name	The existing user with *admin* role who needs to be dropped or deleted.

Example

```
drop admin myadmin
```

This command drops the existing user *myadmin*. The command performs a cleanup, expire the password, lock the account, terminate any existing sessions for the user, and drop the user completely from the database.

A.19.7 DROP AUDITOR

Use the `DROP AUDITOR` command to drop or delete auditors or superauditor users. Only superauditors can drop an auditor or superauditor user.

The `DROP AUDITOR` command drops or deletes a user with auditor role. A superauditor can drop a user with auditor role.

Syntax

```
DROP AUDITOR user name
```

Arguments

Argument	Description
user name	The existing user with *auditor* role who needs to be dropped or deleted.

Example

```
drop auditor myauditor
```

This command drops the existing user *myauditor*. The command performs a cleanup, expire the password, lock the account, terminate any existing sessions for the user, and drop the user completely from the database.

A.19.8 LIST ADMIN

Use the LIST ADMIN command to see administrator privileges for a specific user.

The `LIST ADMIN` command lists administrator privileges for a specific user.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax

```
LIST ADMIN <username>
```

This command lists the administrator privileges for a specific user.

Argument

Argument	Description
username	The specified user.

Example

```
list admin scott;
```

Lists the administrator privileges of a specific user `scott`.

A.19.9 LIST ADMINS

Use the LIST ADMINS command to view or get a list of all users with administrator privileges.

The `LIST ADMINS` command lists all users with administrator privileges.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax

```
LIST ADMINS
```

Example

```
list admins;
```

List all users with administrator privileges.

A.19.10 LIST AUDITOR

Use the LIST AUDITOR command to see auditor privileges for a specific user.

The `LIST AUDITOR` command lists auditor privileges for a specific user.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax

```
LIST AUDITOR <username>
```

This command lists the auditor privileges for a specific user.

Argument

Argument	Description
username	The specified user.

Example

```
list auditor scott;
```

Lists the auditor privileges of a specific user `scott`.

A.19.11 LIST AUDITORS

Use the LIST AUDITORS command to view or get a list of all users with auditor privileges.

The `LIST AUDITORS` command lists all users with auditor privileges.

> **Note:**
>
> This command is available starting Oracle AVDF release 20.4.

Syntax

```
LIST AUDITORS
```

Example

```
list auditors;
```

List all users with auditor privileges.

A.20 User Entitlement AVCLI Commands

You can find general information on user entitlement related AVCLI commands.

A.20.1 RETRIEVE USER ENTITLEMENT

Use the `RETRIEVE USER ENTITLEMENT` command to retrieve user entitlement configured on the target.

Syntax

```
RETRIEVE USER ENTITLEMENT FROM TARGET <target name>
```

This command retrieves user entitlement data on the specified target.

Arguments

Argument	Description
target name	The name of specified target for which the user entitlement have to be retrieved. The name is case-sensitive and must be one of the registered targets. See LIST SECURED TARGET for a list of registered targets. Special characters (&<>"/;,*|=% --) cannot be used for target names.

Result

The job to retrieve user entitlement is submitted successfully. The status of the job can be viewed in the Audit Vault Server console.

In case the user entitlement retrieval job fails due to connection issues, then check the connection details of the specified target.

B

System Configuration Utilities

Run these commands as `root` user to manage system configuration and CLI utilities.

B.1 CONFIG-ASO

Use this command to display the public certificate that is presented to the target for decoding Oracle native encryption (Transparent Data Encryption) on the Database Firewall appliance.

This command is available after installing the Database Firewall diagnostics package.

Syntax

```
/opt/avdf/config-utils/bin/config-aso help
```

```
/opt/avdf/config-utils/bin/config-aso show
```

Arguments

Argument	Description
help	To seek help on displaying the public certificate used to present to the target.
show	To display the existing public certificate used to present to the target.

Attributes

Attributes	Key Values
certificate	The actual certificate details.

Example

```
/opt/avdf/config-utils/bin/config-aso show
```

B.2 CONFIG-AVS

Use this command to establish the communication channel between Database Firewall and Audit Vault Server.

This command is available with the Database Firewall installation.

Syntax

```
/opt/avdf/config-utils/bin/config-avs help
```

```
/opt/avdf/config-utils/bin/config-avs set
```

```
/opt/avdf/config-utils/bin/config-avs show
```

Arguments

Argument	Description
help	To seek help on establishing the communication channel between Database Firewall and Audit Vault Server.
show	To display the existing communication channel between Database Firewall and Audit Vault Server.
set	To modify the communication channel between Database Firewall and Audit Vault Server.

Attributes

Attributes	Key Values
address	IP address of the Audit Vault Server instance.
avs	`primary` `secondary`
certificate	The CA certificate of the Audit Vault Server.

Example

```
/opt/avdf/config-utils/bin/config-avs set avs=primary address=192.0.2.12
certificate=/root/avscert.crt
```

B.3 CONFIG-BOND

Use this command to configure bonding between two Network Interface Cards (NIC). The bonding functionality increases the bandwidth and supports redundancy of the network connections on the appliance.

This command is available with the Database Firewall installation.

> **Note:**
>
> The Database Firewall command-line interface (CLI) creates a bond interface with the default configuration for the operating system. To configure specific bonding controls, use the operating system. See the Create Network Bonds using Network Manager CLI documentation or Configuring Network Bonding in the Oracle Linux 8 documentation for details on creating network bonds in Oracle Linux.

Syntax

```
/opt/avdf/config-utils/bin/config-bond help

/opt/avdf/config-utils/bin/config-bond add

/opt/avdf/config-utils/bin/config-bond delete

/opt/avdf/config-utils/bin/config-bond set

/opt/avdf/config-utils/bin/config-bond show
```

Arguments

Argument	Description
help	To seek help on configuring bonding between two Network Interface Cards.
add	To configure bonding between two Network Interface Cards.
delete	To delete the existing bonding between two Network Interface Cards.
show	To display the existing bonding between two Network Interface Cards.
set	To modify the existing bonding functionality between two Network Interface Cards.

Attributes

Attributes	Key Values
description	A short description of the network or service this bond provides.
device	User defined name of the bonded device.
enabled	This attribute confirms if the bonding between two Network Interface Cards exists. The allowed values are `Yes` or `No`.
gateway	IP address of the gateway.
ip_address	IP address of the bond.
network_mask	The network mask of the device.
components	The names of the component devices.

Example

```
/opt/avdf/config-utils/bin/config-bond add device=bond0
components=enp0s18,enp0s19 ip_address=192.168.10.10
network_mask=255.255.255.0 gateway=192.168.10.1 enabled=yes
```

B.4 CONFIG-CAPTURE

Use this command to monitor the network traffic on the Database Firewall and create packet capture files (PCAP) for Database Firewall configuration.

This command is available with the Database Firewall installation.

Syntax

```
/opt/avdf/config-utils/bin/config-capture help
```

```
/opt/avdf/config-utils/bin/config-capture add
```

```
/opt/avdf/config-utils/bin/config-capture delete
```

```
/opt/avdf/config-utils/bin/config-capture show
```

Arguments

Argument	Description
help	To seek help on configuring traffic capture facility on the Database Firewall appliance.
add	To capture traffic using a NIC on the Database Firewall appliance.
delete	To delete the results of the traffic captured using a NIC on the Database Firewall appliance.
show	To display the list of the recorded traffic captured on the Database Firewall appliance.

Attributes

Attributes	Key Values
duration	The amount of time (in seconds) to capture the traffic.
interface	The name of the interface.
size	The maximum allowed size (in kilobytes) of the traffic capture file.

Example

```
/opt/avdf/config-utils/bin/config-capture add interface=enp0s3 duration=300
size=9999
```

B.5 CONFIG-DIAGNOSTICS

Use this command to run the system diagnostics status which displays current information about a range of processes monitored on the appliance.

This command is available after installing the Database Firewall diagnostics package.

Syntax

```
/opt/avdf/config-utils/bin/config-diagnostics help
```

```
/opt/avdf/config-utils/bin/config-diagnostics show
```

Arguments

Argument	Description
help	To seek help on system diagnostic processes monitored on the appliance.
show	To display the existing system diagnostic capturing process on the appliance.

Example

```
/opt/avdf/config-utils/bin/config-diagnostics show
```

B.6 CONFIG-DNS

Use this command to get and set the DNS server addresses on the appliance.

This command is available after installing the Audit Vault Server and Database Firewall diagnostics packages.

Syntax

```
/opt/avdf/config-utils/bin/config-dns help
```

```
/opt/avdf/config-utils/bin/config-dns set
```

```
/opt/avdf/config-utils/bin/config-dns show
```

Arguments

Argument	Description
help	To seek help on configuring DNS server addresses on the appliance.
set	To configure the DNS server address on the appliance.
show	To display the existing DNS server configuration on the appliance.

Attributes

Attributes	Key Values
servers	Up to three DNS server IP addresses separated by comma.

Example

```
/opt/avdf/config-utils/bin/config-dns set servers="192.0.2.1 192.0.2.2
192.0.2.3"
```

B.7 CONFIG-KEYTABLE

Use this command to configure keyboard locale on the appliance.

This command is available after installing the Audit Vault Server and Database Firewall diagnostics packages.

Syntax

```
/opt/avdf/config-utils/bin/config-keytable help
```

```
/opt/avdf/config-utils/bin/config-keytable set
```

```
/opt/avdf/config-utils/bin/config-keytable show
```

Arguments

Argument	Description
help	To seek help on configuring keyboard locale on the appliance.
set	To configure the keyboard locale on the appliance.
show	To display the existing keyboard locale settings on the appliance.

Attributes

Attributes	Key Values
layout	Any value from `/lib/kbd/keymaps/xkb/` and `/lib/kbd/keymaps/legacy/`

Example

```
/opt/avdf/config-utils/bin/config-keytable set layout=us
```

B.8 CONFIG-NIC

Use this command to configure secondary network interfaces on the appliance.

This command is available with the Audit Vault Server and the Database Firewall installation.

Syntax

```
/opt/avdf/config-utils/bin/config-nic help
```

```
/opt/avdf/config-utils/bin/config-nic set
```

```
/opt/avdf/config-utils/bin/config-nic show
```

> **Note:**
>
> This command should be used for debugging purpose only. It is advisable to use the Audit Vault Server console to perform the NIC configuration.

Arguments

Argument	Description
help	To seek help on configuring secondary network interfaces on the appliance.
set	To configure secondary network interfaces on the appliance.
show	To display the current settings of secondary network interfaces on the appliance.
delete	To delete a configured secondary network interface on the appliance.

Attributes

Attributes	Key Values
description	User defined name of the interface.
device	Device name of the interface on the appliance.
enabled	`Yes` `No`
gateway	IP address of the gateway.
hostname	User defined hostname for all the NICs.
info	System level information about the NIC.
ip_address	IP address of the secondary NIC.
network_mask	The network mask of the NIC.

Example

```
/opt/avdf/config-utils/bin/config-nic set device=enp0s3 ip_address=192.0.2.22
network_mask=255.255.255.0 gateway=192.0.2.1 enabled=true
```

B.9 CONFIG-NTP

Use this command to configure up to 3 NTP server addresses on the appliance.

This command is available with the Database Firewall installation. This command is also available after installing the Audit Vault Server diagnostics package.

Syntax

```
/opt/avdf/config-utils/bin/config-ntp help
```

```
/opt/avdf/config-utils/bin/config-ntp set
```

```
/opt/avdf/config-utils/bin/config-ntp show
```

Arguments

Argument	Description
help	To seek help on setting NTP server address on the appliance.
set	To set NTP server address on the appliance.
show	To display the current NTP server settings on the appliance.

Attributes

Attributes	Key Values
enabled	`Yes` `No`
panic	The amount of time drift that the NTP synchronization ends. It can be an integer.
servers	Comma separated IP addresses or hostnames of NTP servers on the appliance.
sync_on_save	To synchronize the time when settings are saved.
time_differences	To get the time difference of different NTP servers on the appliance.

Example

```
/opt/avdf/config-utils/bin/config-ntp set
servers=192.0.2.0,192.0.2.2,192.0.2.22
```

B.10 CONFIG-PROXY

Use this command to configure traffic proxy ports on the Database Firwewall appliance.

This command is available after installing the Database Firewall diagnostics package.

Syntax

```
/opt/avdf/config-utils/bin/config-proxy help

/opt/avdf/config-utils/bin/config-proxy add

/opt/avdf/config-utils/bin/config-proxy delete

/opt/avdf/config-utils/bin/config-proxy set

/opt/avdf/config-utils/bin/config-proxy show
```

> **Note:**
>
> This command should be used for debugging purpose only. It is advisable to use the Audit Vault Server console to configure proxy ports.

Arguments

Argument	Description
add	To add a proxy port on the Database Firewall appliance.
delete	To delete an existing proxy port on the Database Firewall appliance.
help	To seek help on proxy port configuration for the Database Firewall appliance.
set	To modify a proxy port on the Database Firewall appliance.
show	To display the existing traffic proxy ports on the Database Firewall appliance.

Attributes

Attributes	Key Values
description	User defined name of the port.
enabled	`Yes` `No`
id	A unique ID has to be set for the proxy port on the Database Firewall appliance.
network_id	To set the network interface used for the proxy port on the Database Firewall appliance.
port	To set a specific port as a proxy for the Database Firewall appliance.

Example

```
/opt/avdf/config-utils/bin/config-proxy set id=1 network_id=enp0s8 port=9999
enabled=true description='Sales proxy port'
```

B.11 CONFIG-SNMP

Use this command to configure SNMP access on the appliance.

This command is available after installing the Audit Vault Server and Database Firewall diagnostics packages.

Syntax

```
/opt/avdf/config-utils/bin/config-snmp help
```

```
/opt/avdf/config-utils/bin/config-snmp set
```

```
/opt/avdf/config-utils/bin/config-snmp show
```

Arguments

Argument	Description
set	To set SNMP access on the appliance.
show	To display the current SNMP access settings on the appliance.
help	To get help on setting SNMP access on the appliance.

Attributes

Attributes	Key Values
access	To set SNMP access to the appliance, provide a list of IP addresses separated by comma.
community	To set SNMP community string on the appliance.

Example

```
/opt/avdf/config-utils/bin/config-snmp set
access=192.0.2.0,192.0.2.2,192.0.2.22,192.0.2.24
```

B.12 CONFIG-SSH

Use this command to configure SSH access on the appliance.

This command is available with the Database Firewall installation. This command is also available after installing the Audit Vault Server diagnostics package.

Syntax

```
/opt/avdf/config-utils/bin/config-ssh help
```

```
/opt/avdf/config-utils/bin/config-ssh set
```

```
/opt/avdf/config-utils/bin/config-ssh show
```

Arguments

Argument	Description
set	To set SSH access on the appliance.
show	To display the current SSH access settings on the appliance.
help	To get help on setting SSH access on the appliance.

Attributes

Attributes	Key Values
access	To set SSH access to the appliance, provide a list of IP addresses separated by comma.

Example

```
/opt/avdf/config-utils/bin/config-ssh set
access=192.0.2.0,192.0.2.2,192.0.2.22,192.0.2.24
```

B.13 CONFIG-STATUS

Use this command to display the current status of updates on various Database Firewall components.

This command is available after installing the Database Firewall diagnostics package.

Syntax

```
/opt/avdf/config-utils/bin/config-status show
```

```
/opt/avdf/config-utils/bin/config-status help
```

Arguments

Argument	Description
show	To display the current status of updates on various Database Firewall components.

Argument	Description
help	To get help on the commands for retrieving the status of updates on various Database Firewall components.

Attributes

Attributes	Key Values
component_version	Defines the version of the Database Firewall component, like 20.1.0.0.0.
diagnostic_status	Defines the diagnostic status of the Database Firewall component, like `OK`, `Fail`, `Warn`.
free_space	Defines the free available space on the Database Firewall component.
grammar_versions	Defines the SQL grammar version on the Database Firewall component.
software_version	Defines the software version of the Database Firewall component.

Examples

```
/opt/avdf/config-utils/bin/config-status show
```

```
/opt/avdf/config-utils/bin/config-status show component_version
```

```
/opt/avdf/config-utils/bin/config-status show diagnostic_status
```

```
/opt/avdf/config-utils/bin/config-status show free_space
```

```
/opt/avdf/config-utils/bin/config-status set grammar_versions
```

```
/opt/avdf/config-utils/bin/config-status set software_version
```

B.14 CONFIG-SYSLOG

Use this command to configure syslog destinations on the appliance. It can also be used to set the active syslog categories and the maximum message length.

This command is available after installing the Database Firewall diagnostics package.

Syntax

```
/opt/avdf/config-utils/bin/config-syslog set
```

```
/opt/avdf/config-utils/bin/config-syslog show
```

```
/opt/avdf/config-utils/bin/config-syslog help
```

Arguments

Argument	Description
set	To set syslog destinations on the appliance.
show	To display the current syslog destinations on the appliance.
help	To get help of the available commands and supported attributes.

Attributes

Attributes	Key Values

categories	`system`
	`alerts`
	`info`
	`debug`
	`heartbeat`

max_message_length	Defines the maximum length of the syslog messages. It can be any integer between 1024 and 1048576.
tcp_destinations	The TCP destinations on the appliance includes IP address, or the hostname, and the port number. For example, `my.host:1234`
udp_destinations	The UDP destinations on the appliance includes IP address or the hostname. For example, `my.host` The default port number is 514.

Example

```
/opt/avdf/config-utils/bin/config-syslog set
categories=system,alerts,info,debug,hearbeat max_message_length=2000
tcp_destinations=my.host:1234,second.host:4321 udp_destinations=my.host
```

B.15 CONFIG-TIME

Use this command to configure the time on the appliance.

This command is available after installing the Audit Vault Server and Database Firewall diagnostics packages.

Syntax

```
/opt/avdf/config-utils/bin/config-time set
```

```
/opt/avdf/config-utils/bin/config-time show
```

```
/opt/avdf/config-utils/bin/config-time help
```

Arguments

Argument	Description
set	To set the time on the appliance.
show	To display the current time on the appliance.
help	To get help of the available commands and supported attributes.

Attributes

Attribute	Key Values
time	Define the date and time in *ISO8601* format: `yyyy-mm-ddThh:mm:ss`

Example

```
/opt/avdf/config-utils/bin/config-time set time=2020-02-15T14:31:01
```

B.16 CONFIG-PKI_IDENTITY

Use this command to list, add, delete, and validate TLS identities (keys, certificates, Certificate Signing Requests) for Database Firewall.

> **Note:**
>
> This command is available starting with Oracle AVDF 20.7.

Syntax

```
/opt/avdf/config-utils/bin/config-pki_identity show
```

```
/opt/avdf/config-utils/bin/config-pki_identity help
```

Arguments

Argument	Description
show	To display the list of certificates and Certificate Signing Requests.
add	To create a Certificate Signing Request with specified attributes.
set	To self sign or import external signed certificates to a specified path.
delete	To delete a certificate with the specified `common_name`.
help	To get help of the available commands and supported attributes.

Attributes

Attribute	Key Values
common_name	Common name of the certificate.
alt_dns	Generic certificate attributes used for creating a CSR (`add`).
alt_email	
alt_ip	
alt_uri	
common_name	
country	
email	
locality	
organisation	
organisational_unit	
state	
cert_gid	File system setting for the generated CSR.
cert_mode	
cert_path	
cert_uid	
key_gid	File system setting for the generated key.
key_mode	
key_path	
key_uid	
self_sign	Argument to self sign the CSR with the local CA.

Example

```
/opt/avdf/config-utils/bin/config-pki_identity show
common_name=foobar.example.com


/opt/avdf/config-utils/bin/config-pki_identity set cert_path=/usr/local/dbfw/
certificate.crt


/opt/avdf/config-utils/bin/config-pki_identity delete
common_name=foobar.example.com



/opt/avdf/config-utils/bin/config-pki_identity add \
  common_name=foobar.example.com \
  country=US \
  email=first.last@example.invalid \
  locality=city \
  organisation=company \
  organisational_unit=group \
  state=area \
  cert_uid=user \
  cert_gid=group \
```

```
cert_mode=444 \
key_uid=root \
key_gid=privilegedgroup \
key_mode=440 \
key_path=/usr/local/dbfw/private.key \
cert_path=/usr/local/dbfw/certificate.csr
```

C

Plug-In Reference

This appendix contains high-level data for each plug-in that is shipped with Oracle Audit Vault and Database Firewall (Oracle AVDF). It also contains lookup information to complete the procedures for registering targets and configuring audit trails. These procedures link directly to the relevant sections of this appendix.

C.1 About Oracle Audit Vault and Database Firewall Plug-ins

Learn about the plug-ins supported by Oracle Audit Vault and Database Firewall.

Oracle Audit Vault and Database Firewall supports different types of targets by providing a plug-in for each target type. Oracle Audit Vault and Database Firewall 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 Audit Vault and Database Firewall installation.

> **See Also:**
>
> Deploying Plug-ins and Registering Plug-in Hosts

C.2 Plug-ins That are Shipped with Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall supports plug-ins for a variety of different platforms, such as Oracle Solaris, Linux, and Microsoft Windows.

C.2.1 About Plug-ins

Oracle Audit Vault and Database Firewall supports plug-ins for many platforms and third-party products.

Oracle Audit Vault and Database Firewall plug-ins support the target versions listed in Table C-1. Click the link for each target to get detailed information.

Table C-1 Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall

Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor Agent	Native Network Encrypted Traffic Monitoring / Retrieve Session Information
Oracle Database Plug-in for Oracle Audit Vault and Database Firewall 11.2.0.4	Yes	Yes (except Unified Audit Policies)	Yes	Yes	Yes	Yes	Yes
Oracle Database Plug-in for Oracle Audit Vault and Database Firewall 12.1, 12.2, 18c, 19c 21c (Starting with Oracle AVDF 20.4) 23ai (Starting with Oracle AVDF 20.13)	Yes	Yes (including Unified Audit Policies)	Yes	Yes	Yes	Yes	Yes
Microsoft SQL Server Plug-in for Oracle Audit Vault and Database Firewall (Windows) Enterprise Edition 2012*, 2014, 2016, 2017 Enterprise Edition 2019 (Starting with Oracle AVDF 20.3) Enterprise Edition 2022 (Starting with Oracle ADVF 20.10) Standard Edition 2019 (Starting with Oracle AVDF 20.6) Standard Edition 2022 (Starting with Oracle ADVF 20.10)	Yes	No	Yes (Versions 2000, 2005, 2008, 2008 R2)	Yes	Yes	Yes (on Microsoft Windows 2008 and onwards)	Yes (Microsoft SQL Server 2005, 2008, 2008 R2) (Retrieving session information only)
Microsoft SQL Server Plug-in for Oracle Audit Vault and Database Firewall* (Windows Clustered) 2012 R2	Yes	No	Yes (Versions 2012 R2)	Yes	No	No	No

Table C-1 (Cont.) Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall

Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor Agent	Native Network Encrypted Traffic Monitoring / Retrieve Session Information
PostgreSQL Plug-in for Oracle Audit Vault and Database Firewall Open source versions: 9.6 to 11.8 12, 13 (Starting with Oracle AVDF release 20.8) 14, 15 (Starting with Oracle AVDF release 20.10)	Yes	No	No	No	No	No	No
SAP Sybase ASE Plug-in for Oracle Audit Vault and Database Firewall* 15.7, 16	Yes	No	Yes	No	Yes	Yes	No
IBM DB2 Plug-in for Oracle Audit Vault and Database Firewall for LUW 10.5, 11.1, 11.5	Yes	No	No	Yes	Yes Versions 9.1 - 10.5	Yes	No
Quick JSON Target Type for Oracle Audit Vault and Database Firewall	Yes	No	No	No	No	No	No
MySQL Plug-in for Oracle Audit Vault and Database Firewall 5.6, 5.7, 8.0	Yes	No	No	Yes	Yes	Yes	No
Oracle Solaris Plug-in for Oracle Audit Vault and Database Firewall 11.3, 11.4 on x86-64 platforms*	Yes	No	No	No	No	Yes Versions 11, 11.1, 11.2	No
Oracle Solaris Plug-in for Oracle Audit Vault and Database Firewall 11.3, 11.4 on SPARC64 platforms	Yes	No	No	No	No	Yes Versions 11, 11.1, 11.2	No

Table C-1 (Cont.) Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall

Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor Agent	Native Network Encrypted Traffic Monitoring / Retrieve Session Information
Oracle Linux 6.0 to 6.9 7.0 to 7.5 7.6 to 7.8 (Starting with Oracle AVDF 20.2) 7.9 (Starting with Oracle AVDF 20.4) 8 (Starting with Oracle AVDF 20.3) 8.2, 8.3 (Starting with Oracle AVDF 20.4) 9 (Starting with Oracle AVDF 20.9)	Yes	No	No	No	No	Yes	No
Red Hat Enterprise Linux 6.7 to 6.10 7.0 to 7.5 7.6 to 7.8 (Starting with Oracle AVDF 20.2) 7.9 (Starting with Oracle AVDF 20.4) 8 (Starting with Oracle AVDF 20.3) 8.2, 8.3 (Starting with Oracle AVDF 20.4) 9 (Starting with Oracle AVDF 20.9)	Yes	No	No	No	No	Yes	No

Table C-1 (Cont.) Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall

Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor Agent	Native Network Encrypted Traffic Monitoring / Retrieve Session Information
IBM AIX Plug-in for Oracle Audit Vault and Database Firewall on Power Systems (64-bit) 7.1 (TL5) 7.2 (TL2 and above) 7.3 (TL0) (Starting with Oracle AVDF 20.10) 7.3 (TL2) (Starting with Oracle AVDF 20.13)	Yes	No	No	No	No	Yes	No
Microsoft Windows Plug-in for Oracle Audit Vault and Database Firewall Microsoft Windows Server 2012*, 2012 R2, 2016 on x86-64 2019 on x86-64 (Starting with Oracle AVDF 20.2)	Yes	No	No	No	No	No	No
Microsoft Active Directory Plug-in for Oracle Audit Vault and Database Firewall 2012 to 2016 on 64 bit	Yes	No	No	No	No	No	No
Oracle ACFS Plug-in for Oracle Audit Vault and Database Firewall* 12c	Yes	No	No	No	No	No	No

*

- Microsoft Windows 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.
- Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

- Solaris - x86-64 was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.
- Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was desupported in Oracle AVDF release 20.8
- Sybase SQL Anywhere was desupported in Oracle AVDF release 20.8

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.2.2 Oracle Database Plug-in for Oracle Audit Vault and Database Firewall

Learn about the Oracle Database plug-in for Oracle Audit Vault and Database Firewall.

Table C-2 lists features of the Oracle Database Plug-in.

Table C-2 Oracle Database Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.oracle
Target Versions	Oracle 11.2.0.4 Oracle 12*c* Release 1 (12.1) Oracle 12*c* Release 2 (12.2) Oracle 18c Oracle 19c 21c (Starting with Oracle AVDF 20.4) 23ai (Starting with Oracle AVDF 20.13)
Target Platforms	Linux/x86-64 Solaris /x86-64 Solaris /SPARC64 AIX/Power64 Windows /x86-64 HP-UX Itanium See Platform Support Matrix in Oracle Audit Vault and Database Firewall Installation Guide for complete details on supported target platforms and versions.
Setup Script(s)	Yes. See "Oracle Database Setup Scripts" for instructions.
Target Location (Connect String)	jdbc:oracle:thin:@//*hostname*:*port*/*service*
Collection Attributes	None. ORCLCOLL.NLS_LANGUAGE, ORCLCOLL.NLS_TERRITORY and ORCLCOLL.NLS_CHARSET: These will be deprecated in the future. ORCLCOLL.NLS_CHARSET attribute is replaced by AV.COLLECTOR.DATABASECHARSET. See Table C-24 for details. AV.COLLECTOR.TIMEZONEOFFSET **Note:** This attribute must be set to timezone offset of Oracle Database. It is mandatory if Transaction Log audit trail is going to be configured for the target.

Table C-2 (Cont.) Oracle Database Plug-in

Plug-in Specification	Description

AVDF Audit Trail Types	`TABLE`
	`DIRECTORY`
	`TRANSACTION LOG`
	`SYSLOG` (Linux only)
	`EVENT LOG` (Windows only)
	`NETWORK`
	See Table C-22 for descriptions of audit trail types.

Audit Trail Location	For `TABLE` audit trails: `SYS.AUD$`, `SYS.FGA_LOG$`, `DVSYS.AUDIT_TRAIL$`, `UNIFIED_AUDIT_TRAIL`, `CDB_UNIFIED_AUDIT_TRAIL`, `SYS.DBA_SQL_FIREWALL_VIOLATIONS` (Oracle Database 23ai and later). For `DIRECTORY` audit trails: Full path to directory containing `AUD` or `XML` files. For `SYSLOG` audit trails: Use `DEFAULT` or the full path to directory containing the syslog file. For `EVENT LOG` and `NETWORK` audit trails: no trail location required. For `TRANSACTION LOG`: Full path to directory containing Golden Gate Integrated Extract file. **Note:** Oracle Audit Vault and Database Firewall queries and collects records from Unified Audit trail which fetches unified audit records from operating system spillover audit files. The Database Audit Management manages the clean up of Unified Audit trail and the underlying operating system spillover audit files.
Audit Trail Cleanup Support	Yes. See Oracle Database Audit Trail Cleanup for instructions.
OS user running the Agent	For Oracle Database Directory Audit Trail: Any user who has *read* permission on audit files, i.e *oracle* user, or user in DBA group. For Table Trail: Any database user (preferably not a DBA). See Oracle Database Setup Scripts for instructions. For Transaction Log trail : Any user who has read permission on Golden Gate Integrated Extract XML files. For any other directory audit trail: Any user who has *read* permission on audit files.
Supported Character Sets for `DIRECTORY` and `SYSLOG` audit trails	The `DIRECTORY` and `SYSLOG` audit trails use Java character set to open audit files based on the database character sets. This ensures the audit files are processed using the right character sets and to avoid data loss. The database character set is read from the following sources in the same order: 1. Target attribute `AV.COLLECTOR.DATABASECHARSET` 2. Target attribute `ORCLCOLL.NLS_CHARSET` (deprecated) 3. The target Oracle database **Note:** An exception to the above process is XML audit files with Java character set specified in XML declaration. Refer to the known issues for a list of character sets that are not supported.

Table C-2 (Cont.) Oracle Database Plug-in

Plug-in Specification	Description
Cluster support (Oracle Real Application Clusters)	Yes When configuring a Oracle RAC as a target for audit collection, enter the port number of the SCAN Listener.
Oracle Active Data Guard	Additional Information for Audit Collection from Oracle Active Data Guard

C.2.3 MySQL Plug-in for Oracle Audit Vault and Database Firewall

Learn how to use the MySQL plug-in for Oracle Audit Vault and Database Firewall.

Table C-3 lists the features of the MySQL plug-in.

Table C-3 MySQL Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.mysql
Target Versions	Enterprise Edition 5.6, 5.7, 8.0
Target Platforms	Linux (x86-64): OL 5.x, 6.x, 7.x and RHEL 6.x, 7.x Microsoft Windows (x86-64): 8 Microsoft Windows Server (x86-64): 2012, 2012R2, 2016
Target Location (Connect String)	jdbc:av:mysql://*hostname*:*port*/mysql
Collection Attribute(s)	av.collector.securedTargetVersion - (Required) Specifies the MySQL version. Default is 8.0. 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 C-22 for descriptions of audit trail types.
Audit Trail Cleanup Support	Yes.

Audit Trail Location

The path to the directory where the converted files are created.

The default audit format for MySQL 5.5 and 5.6 is old. The default audit format for MySQL 5.7 is new. The audit format can be changed by modifying the configuration on MySQL Server.

The Audit Trail Location is as follows:

1. For old audit format, the path to the directory is where the converted XML files are created when you run the MySQL XML transformation utility.
2. For new audit format, the path to the directory is where the audit.log files are generated by MySQL Server.

Table C-4 Old Audit Format

Audit Trail Location	Value
Input path format before MySQL 5.7.21	`<Path of the converted XML location.>` For example: `\ConvertedXML`
Input path format of MySQL 5.7.21 onwards	`<Path of the converted XML location.>` For example: `\ConvertedXML`

Table C-5 New Audit Format

Audit Trail Location	Value
Input path format before MySQL 5.7.21	`<Path of the audit.log location.>` For example: `\MySQLLog`
Input path format for MySQL 5.7.21 onwards	`<Path of the audit log file>/<log file name>.*.log` Where `*` is the time stamp in `YYYYMMDDThhmmss` format. For example: `MySQLLog/audit*.log`

Note:

- In the old format audit data is collected from converted XML files. In the new format audit data is collected from both active log and rotated logs.
- Audit collection from MySQL Community Edition is not supported by this plug-in of Oracle AVDF.

Best Practice:

Enable automatic size-based audit log file rotation, by setting `audit_log_rotate_on_size` property. See Audit Log File Space Management and Name Rotation in MySQL Reference Manual for further details.

See Also:

- Running the XML Transformation Utility for MySQL Audit Formats
- MySQL Audit Trail Cleanup

C.2.4 Microsoft SQL Server Plug-in for Oracle Audit Vault and Database Firewall

The following table lists the features of the Microsoft SQL Server plug-in for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

Table C-6 Microsoft SQL Server Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.mssql
Target versions	Enterprise Edition 2012, 2014, 2016, 2017, 2019 (Starting with Oracle AVDF 20.3), 2022 (Starting with Oracle ADVF 20.10) Standard Edition 2019 (starting with Oracle AVDF 20.6), 2022 (Starting with Oracle ADVF 20.10) Starting with Oracle AVDF 20.10, agentless and remote collection are supported as follows: • `.sqlaudt` audit events are supported for all supported Microsoft SQL Server versions. • `.xel` audit events are supported for Microsoft SQL Server 2017 and later.
Target platforms	Windows/x86-64 See Platform Support Matrix in *Oracle Audit Vault and Database Firewall Installation Guide* for complete details on supported target platforms and versions.
Setup scripts	Yes. See Microsoft SQL Server Setup Scripts for instructions. **Note:** After upgrading to Oracle AVDF 20.3 or later, rerun the server setup script for all targets to continue with audit collection.
Target location (Connect string for SQL server authentication)	`jdbc:av:sqlserver://`*hostname*`:`*port*
Target location (Connect string for Windows authentication)	`jdbc:av:sqlserver://` *hostname*`:`*port*`;authenticationMethod=ntlmjava` Use Windows user credentials along with the domain. For example: *domain*`\`*username* and password
Collection attributes	None

AVDF audit trail types	`DIRECTORY`
	`TRANSACTION LOG` (starting with Oracle AVDF 20.9)
	`EVENT LOG`
	`NETWORK`
	See Table C-22 for descriptions of the audit trail types.

Table C-6 (Cont.) Microsoft SQL Server Plug-in

Plug-in Specification	Description
Audit trail location for `DIRECTORY` audit trails	• `*.sqlaudit` • `*.trc` (trace) • `*.xel` (extended events) • `#C2_DYNAMIC` • `#TRACE_DYNAMIC` Examples: • *`directory_path`*`\*.sqlaudit` • *`directory_path`*`\`*`prefix`*`*.sqlaudit` • *`directory_path`*`\`*`prefix`*`*.trc` • *`directory_path`*`\*.xel` • *`directory_path`*`\`*`prefix`*`*.xel` • `#C2_DYNAMIC` • `#TRACE_DYNAMIC` **Note:** • For *`prefix`*, you can use any prefix for the `.trc`, `*.xel`, or `*.sqlaudit` files. • Support for extended events (`*.xel` files) is included for `DIRECTORY` audit trails starting with Oracle AVDF 20.3.
Audit trail location for `EVENT LOG` audit trails	• `application` • `security`
Audit trail location for `TRANSACTION LOG` audit trails (Oracle AVDF 20.9 and later)	Full path to the directory containing the Oracle GoldenGate CDC Extract file
Audit trail cleanup support	Yes (not supported for agentless or remote collection) See Microsoft SQL Server Audit Trail Cleanup for instructions.
Cluster support	Yes (not supported for agentless or remote collection)
Target platform for clusters	Windows 2012 R2 Enterprise Edition for audit collection
Cluster collection attribute	Attribute name: `av.collector.clusterEnabled` Attribute value: `1`

Table C-6 (Cont.) Microsoft SQL Server Plug-in

Plug-in Specification	Description
Support for the AlwaysOn availability group	Yes (starting with Oracle AVDF 20.3) **Note:** • Register one target in the Audit Vault Server for every Microsoft SQL Server that is part of the AlwaysOn availability group. • The Oracle AVDF audit report provides a view of audit records that are generated by individual Microsoft SQL Servers in the availability group. It is not a consolidated view of audit records that are generated by all servers in the availability group.
Collection attributes (optional)	`av.collector.validateConnectionOnBorrow` Setting this attribute to `False` eliminates unnecessary logging of records or events due to test queries in the target database. This attribute is available starting with Oracle AVDF 20.6.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.2.5 PostgreSQL Plug-in for Oracle Audit Vault and Database Firewall

Learn about using the PostgreSQL plug-in for Oracle Audit Vault and Database Firewall.

Table C-7 specifies the values or details required for the configuration.

Prerequisite: Ensure to enable `pgaudit` extension. The audit collection is incomplete and operational details are missed out from the reports in case this extension is not enabled.

Table C-7 PostgreSQL

Specification	Description
Plug-in directory	`AGENT_HOME/av/plugins/com.oracle.av.plugin.postgresql`
Target Versions	Open source versions: 9.6 to 11.8 12 and 13 (Starting with Oracle AVDF 20.8) 14 and 15 (Starting with Oracle AVDF 20.10)
Target Platforms	Linux/x86-64
Setup Scripts	None
Target Location (Connect String)	None

Table C-7 (Cont.) PostgreSQL

Specification	Description
Collection Attributes (Required)	`av.collector.securedTargetVersion` Specifies the target version. Default is 11.0.
Collection Attributes (Optional)	`AV.COLLECTOR.DATABASECHARSET` The NLS character set of the audit trail file. This is available starting Oracle AVDF 20.4. The PostgreSQL `DIRECTORY` audit trails use Java character set to open audit files based on the database character sets. This ensures the audit files are processed using the right character sets and avoid data loss.
Audit Trail Types	`DIRECTORY`
Audit Trail Location	The path to the directory containing `CSV` audit files.
Audit Trail Cleanup Support	No

C.2.6 IBM DB2 Plug-in for Oracle Audit Vault and Database Firewall

Learn about how to use the IBM DB2 plug-in for Oracle Audit Vault and Database Firewall.

Table C-8 lists the features of the IBM DB2 plug-in.

Table C-8 IBM DB2 Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*`/av/plugins/com.oracle.av.plugin.db2`
Target Versions	10.5, 11.1, 11.5
Target Platforms	Linux (x86-64): OL 5.x, 6.x, 7.x and RHEL 6.x, 7.x Microsoft Windows (x86-64): 8 Microsoft Windows Server (x86-64): 2012, 2012R2, 2016 IBM AIX on Power Systems (64-bit): 7.1
Setup Script(s)	Yes. See "IBM DB2 for LUW Setup Scripts" for instructions.
Target Location (Connect String)	`jdbc:av:db2://`*hostname*`:`*port*`/dbname` **Note:** • Connect string is not required for Oracle AVDF release 20. • Connect string is not required for IBM DB2 cluster.
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 C-22 for descriptions of audit trail types.

Audit Trail Location	Path to a directory, for example: `d:\temp\trace`
Audit Trail Cleanup Support	Yes
Cluster Support	Yes HADR (High Availability and Disaster Recovery)
Target Platform for Cluster	HADR on OL 7.x

Table C-8 (Cont.) IBM DB2 Plug-in

Plug-in Specification	Description
DB2 Multiple Instances Support	Yes

Multiple Instances Environment

In case of multiple instances environment, create an Audit Vault Agent user and then the Agent group. Install the Agent as the newly created Agent user belonging to the Agent group. Add all the users of the instance to the Agent group and then add the Agent user to the instance group. This functionality is supported from Oracle AVDF 20.2 (RU2) and later.

Perform the following steps from every instance to extract the audit files:

1. Navigate to the extraction utility location using `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/bin`.
2. Set the environment variables `agent_home`, `db2audit_command`, and `lslk_cmd`.
3. Run the extraction utility using `./DB295ExtractionUtil -archivepath <archive path> -extractionpath <extraction path> -audittrailcleanup <yes/no>`.
4. The extracted files are generated in the directory at the instance level.
5. Start the audit trail for every instance as the extraction path is different for each instance.

C.2.7 SAP Sybase ASE Plug-in for Oracle Audit Vault and Database Firewall

Learn how to use the SAP Sybase ASE plug-in for Oracle Audit Vault and Database Firewall.

Table C-9 lists the features of the SAP Sybase ASE plug-in.

Table C-9 SAP Sybase ASE Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.sybase
Target Versions	15.7 16.0
Target Platforms	All platforms
Setup Script(s)	Yes. See "Sybase ASE Setup Scripts for Oracle Audit Vault and Database Firewall " for instructions.
Target Location (Connect String)	jdbc:av:sybase://*hostname*:*port*
Collection Attribute(s)	None
AVDF Audit Trail Types	TABLE NETWORK See Table C-22 for descriptions of audit trail types.
Audit Trail Location	SYSAUDITS
Audit Trail Cleanup Support	No

Table C-9 (Cont.) SAP Sybase ASE Plug-in

Plug-in Specification	Description
Cluster support	No

SAP Sybase Password Encryption

In case you are using password encryption on SAP Sybase database, incorporate the following changes on Oracle Audit Vault and Database Firewall:

1. Use the following connection string in Audit Vault Server console while setting up the audit trail for SAP Sybase database:

   ```
   jdbc:sybase:Tds:<host>:<port>/sybsecurity?
   ENCRYPT_PASSWORD=TRUE&JCE_PROVIDER_CLASS=com.sun.crypto.provider.SunJCE
   ```

2. Copy the `jconn4.jar` file from `/opt/sybase/jConnect-16_0/classes` in Sybase server to `Agent_Home/av/jlib`.

   > **Note:**
   >
   > If you are using Sybase 15.7, then fetch the `jconn4.jar` file from the latest SAP Sybase server version 16.0.

3. Restart the Audit Vault Agent.
4. Start the collection.

C.2.8 Quick JSON Target Type for Oracle Audit Vault and Database Firewall

Learn how to configure and use the Quick JSON target type for Oracle Audit Vault and Database Firewall.

Quick JSON target type can be used to collect audit data from targets that store audit records in JSON format, by mapping few collection attributes.

Table C-10 specifies the values or details required for the configuration.

Table C-10 Quick JSON

Specification	Description
Plug-in directory	`AGENT_HOME/av/plugins/com.oracle.av.plugin.quickjson`
Target Platforms	Linux/x86-64 Windows /x86-64
Setup Scripts	None
Target Location (Connect String)	None
Collection Attributes (Required)	`av.collector.securedTargetVersion` Specifies the target version.

Table C-10 (Cont.) Quick JSON

Specification	Description
Collection Attributes (Optional)	`AV.COLLECTOR.DATABASECHARSET` The NLS character set of the audit trail file. This is available starting Oracle AVDF 20.4. The Quick JSON `DIRECTORY` audit trails use Java character set to open audit files based on the database character sets. This ensures the audit files are processed using the right character sets and avoid data loss.
Audit Trail Types	`DIRECTORY`
Audit Trail Location	The path to the directory containing `JSON` audit files.
Audit Trail Cleanup Support	No

QuickJSON collector relies on collection attributes to map JSON audit data to Oracle AVDF audit record fields. These collection attributes point to data within JSON audit file using JSON Path expressions. Following table lists the QuickJSON collection attributes.

Table C-11 Quick JSON Collection Attributes

Quick JSON Collection Attribute Name	Description	Attribute Value Type
`av.collector.qck.starttag`	Should be set to the first key of JSON audit record. This is not JSON Path expression. It is the name of the required key.	Static String
`av.collector.qck.eventtime`	Time when the event occurred.	JSON Path Expression
`av.collector.qck.username`	The user of the target who executed the event.	JSON Path Expression
`av.collector.qck.os.username`	Operating system login name of the target user who executed the event.	JSON Path Expression
`av.collector.qck.eventname`	Name of the event as recognized by the target.	JSON Path Expression
`av.collector.qck.commandclass`	Class of command issued by the target user who executed the event.	JSON Path Expression
`av.collector.qck.client.ip`	IP address of the client host.	JSON Path Expression
`av.collector.qck.targetobject`	Object affected by the event.	JSON Path Expression
`av.collector.qck.targettype`	Type of the target object. For example: Package, Type, or Table.	JSON Path Expression
`av.collector.qck.eventstatus`	Completion status of the event.	JSON Path Expression
`av.collector.qck.errorid`	Error number in case of event failure.	JSON Path Expression
`av.collector.qck.errormessage`	Error message in case of event failure.	JSON Path Expression
`av.collector.qck.target.entity`	Name of target entity.	JSON Path Expression
`av.collector.qck.target.user`	Name of target user.	JSON Path Expression
`av.collector.qck.target.role`	Name of target role.	JSON Path Expression

> **Note:**
>
> The attributes `av.collector.qck.target.entity`, `av.collector.qck.target.user`, and `av.collector.qck.target.role` are only applicable if Quick JSON target is used to collect audit data from Mongo DB.

> **See Also:**
>
> - Configuring Quick JSON Target Type to Collect Audit Data from MongoDB
> - Audit Record Fields for more information on other collection attributes and corresponding audit record field definitions.

C.2.9 QuickCSV Collector for Oracle Audit Vault and Database Firewall

Learn how to configure and use the QuickCSV target type for Oracle Audit Vault and Database Firewall.

A QuickCSV target type can be used to collect audit data from most targets that store audit records in CSV format through a one-to-one mapping of collection attributes to fields in the log file. If a database stores some data across multiple fields, it cannot be captured in a single field.

The Specifications for QuickCSV Collector table below specifies the values or details required for the configuration.

Table C-12 Specifications for QuickCSV Collector

Specification	Description
Plug-in directory	<agent_home>/av/plugins/com.oracle.av.plugin.quickcsv
Target platforms	All supported OS
Setup scripts	None
Target Location (Connect String)	None
Collection attributes	(See table below)
Audit trail types	Directory
Audit trail location	Path to directory containing the .csv files
Audit trail cleanup support	No

The below table describes the attributes which are mapped to fields within the .csv audit file. Against the attribute, the value to be entered is the field number. The field numbers can be entered as 1, 2, 3, etc. or as $1, $2, $3, etc.

Table C-13 Attributes for QuickCSV Collector

Attribute	Description
av.collector.map.client.hostname	Target hostname
av.collector.map.client.id	Target ID

Table C-13 (Cont.) Attributes for QuickCSV Collector

Attribute	Description
av.collector.map.client.ip	Target IP address
av.collector.map.client.program.name	Program running on target which executed the event
av.collector.map.command.class	Class of command issued by the target user who executed the event
av.collector.map.command.param	Parameters given to command while executing the event
av.collector.map.command.text	Command statement for the event
av.collector.map.database.name	Name of the target database
av.collector.map.error.id	Error number in case of event failure
av.collector.map.error.message	Error message in case of event failure
av.collector.map.event.name (Required)	Name of the event as recognized by the target
av.collector.map.event.status	Completion status of the event
av.collector.map.event.time (Required)	Time when the event occurred
av.collector.map.instance.name	Name of database instance
av.collector.map.os.username	Operating system login name of the target user who executed the event
av.collector.map.repository.name	Name of the database repository
av.collector.map.target.object	Object affected by the event
av.collector.map.target.owner	Name of the user who owns the target
av.collector.map.target.type	Type of target object
av.collector.map.username	The user of the target who executed the event

Other than the predefined attributes mentioned above, you can also add more attributes to specify fields to be collected from. These attributes must begin with the prefix `av.collector.map.extension`. The data collected from the field specified against the user-defined attribute will be added to the extension field along with the name given to the attribute.

The below table describes the attributes that specify the format of the .csv file.

Table C-14 Format Attributes for QuickCSV Collector

Format Attribute	Description	Default value
av.collector.format.delimiter	Specifies the delimiter string used in the .csv file. For example, comma (,) semicolon (;) etc.	, (comma)
av.collector.format.escape	Specifies the escape character within a quoted field	NA
av.collector.format.quote	Specifies the character used to put a field between quotes	" (double-quote)
av.collector.pattern.timestamp	Specifies the timestamp format string	yyyy-MM-dd HH:mm:ss.SSS z
av.collector.timezoneoffset	Specifies the timezone offset for the timestamp	NA

C.2.10 SAP Sybase SQL Anywhere Plug-in for Oracle Audit Vault and Database Firewall

Learn about using the SAP Sybase SQL Anywhere plug-in for Oracle Audit Vault and Database Firewall.

> **Note:**
>
> SAP Sybase SQL Anywhere was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

Table C-15 lists the features of the SAP Sybase SQL Anywhere plug-in.

Table C-15 SAP Sybase SQL Anywhere Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.sqlanywhere
Target Versions	10.0.1
Target Platforms	All platforms
Setup Script(s)	Yes. See "Sybase SQL Anywhere Setup Scripts" for instructions.
Target Location (Connect String)	jdbc:av:sybase://*hostname*:*port*
Collection Attributes	None
AVDF Audit Trail Types	NETWORK (used for host monitoring only) See Table C-22 for descriptions of audit trail types.
Audit Trail Location	Not required
Audit Trail Cleanup Support	No

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.2.11 Oracle Solaris Plug-in for Oracle Audit Vault and Database Firewall

Learn to use the Oracle Solaris plug-in for Oracle Audit Vault and Database Firewall.

Table C-16 lists the features of the Oracle Solaris plug-in.

Table C-16 Oracle Solaris Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.solaris
Target Versions	Versions 11.3 and 11.4 on SPARC64 and x86-64 platforms

Table C-16 (Cont.) Oracle Solaris Plug-in

Plug-in Specification	Description
Target Platforms	Solaris/x86-64 Solaris/SPARC64 Solaris - x86-64 was deprecated in Oracle AVDF 20.9, and it will be desupported in one of the future releases.
Setup Script(s)	No
Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY See Table C-22 for descriptions of audit trail types.
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

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.2.12 Linux Plug-in for Oracle Audit Vault and Database Firewall

Learn how to benefit from using the Linux plug-in for Oracle Audit Vault and Database Firewall.

Table C-17 lists the features of the Linux plug-in that collects audit data from Oracle Linux (OL) and Red Hat Enterprise Linux (RHEL).

Table C-17 Linux Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.linux

Table C-17 (Cont.) Linux Plug-in

Plug-in Specification	Description
Target Versions	**Oracle Linux (OL):** Oracle Linux 6 was deprecated in Oracle AVDF 20.10, and it will be desupported in one of the future releases. • OL 6.0 (with `auditd` package 2.0) • OL 6.1 - 6.5 (with `auditd` package 2.2.2) • OL 6.6 - 6.7 (with `auditd` package 2.3.7) • OL 6.8 - 6.9 (with `auditd` package 2.4.5) • OL 7.0 (with `auditd` package 2.3.3) • OL 7.1 - 7.2 (with `auditd` package 2.4.1) • OL 7.3 (with `auditd` package 2.6.5) • OL 7.4 - 7.5 (with `auditd` package 2.7.6) • OL 7.6 (with `auditd` 2.8) (Oracle AVDF 20.2 and later) • OL 7.7 (with `auditd` 2.8.5) (Oracle AVDF 20.2 and later) • OL 7.8 (with `auditd` 2.8) (Oracle AVDF 20.2 and later) • OL 7.9 (with `auditd` 2.8) (Oracle AVDF 20.4 and later) • OL 8 (with `auditd` 3.0) (Oracle AVDF 20.3 and later) • OL 8.2 and 8.3 (with `auditd` 3.0) (Oracle AVDF 20.4 and later) • OL 9 (Oracle AVDF 20.9 and later) **Red Hat Enterprise Linux (RHEL):** • RHEL 6.7 (with `auditd` 2.3.7) • RHEL 6.8 (with `auditd` 2.4.5) • RHEL 6.9 (with `auditd` 2.4.5) • RHEL 6.10 (with `auditd` 2.4.5) • RHEL 7.0 (with `auditd` 2.3.3) • RHEL 7.1 (with `auditd` 2.4.1) • RHEL 7.2 (with `auditd` 2.4.1) • RHEL 7.3 (with `auditd` 2.6.5) • RHEL 7.4 (with `auditd` 2.7.6) • RHEL 7.5 (with `auditd` 2.7.6) • RHEL 7.6 (with `auditd` 2.8) (Oracle AVDF 20.2 and later) • RHEL 7.7 (with `auditd` 2.8.5) (Oracle AVDF 20.2 and later) • RHEL 7.8 (with `auditd` 2.8) (Oracle AVDF 20.2 and later) • RHEL 7.9 (with `auditd` 2.8) (Oracle AVDF 20.4 and later) • RHEL 8 (with `auditd` 3.0) (Oracle AVDF 20.3 and later) • RHEL 8.2 and 8.3 (with `auditd` 3.0) (Oracle AVDF 20.4 and later) • RHEL 9 (Oracle AVDF 20.9 and later) Run `rpm -q audit` to get the audit package version.
Target Platforms	Linux/x86-64

Table C-17 (Cont.) Linux Plug-in

Plug-in Specification	Description
Setup Script(s)	No. However, the following user/group access rights are needed to start a 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.
Target Location (Connect String)	*`hostname`* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	`DIRECTORY` See Table C-22 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

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.2.13 IBM AIX Plug-in for Oracle Audit Vault and Database Firewall

Learn about the IBM AIX plug-in for Oracle Audit Vault and Database Firewall.

Table C-18 lists the features of the IBM AIX plug-in.

Table C-18 IBM AIX Plug-in

Plug-in Specification	Description
Plug-in directory	*`AGENT_HOME`*`/av/plugins/com.oracle.av.plugin.aixos`
Target Versions	AIX versions: • 7.3 (TL2) (Starting with Oracle AVDF 20.13) • 7.3 (TL0) (Starting with Oracle AVDF 20.10) • 7.2 (TL2 and above) • 7.1 (TL5)
Supported JRE Version	1.8.0_241 (minimum) **Note:** JRE version 11 is not supported on AIX platform.
Target Platforms	Power Systems (64-bit)

Table C-18 (Cont.) IBM AIX Plug-in

Plug-in Specification	Description

Setup Script(s)	No. However, the following user and group access rights are needed to start an AIX audit trail:
	If the Agent process is started by the `root` user, then no changes to access rights are needed.
	If the Agent process is started with a user other than `root`, then run the following commands in the AIX system as `root` to authorize another user:
	1. Create a new role and grant it the `aix.security.audit` authorization:
	`mkrole authorizations= (aix.security.audit) (role_name)`
	2. Alter the Agent user to assign the newly created role:
	`chuser roles=role_name agent_user_name`
	3. Update the kernel table with the newly created role by running the command: `setkst`
	4. Add the Agent user to the same group as that of the AIX audit files.
	5. Ensure you have set read permission on the `/audit` directory where the audit trail files are located.
	6. To start the Agent with the Agent user, log in to the AIX terminal with *agent_user_name* and switch to the role created in this procedure:
	`swrole role_name`

Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY See Table C-22 for descriptions of audit trail types.
Audit Trail Location	Default location of trail (`/audit/trail`) or any custom location configured in the `/etc/security/audit/config` file
Audit Trail Cleanup Support	Yes. The AIX plug-in will create a `.atc` file at: *AGENT_HOME*`/av/atc/`*SecuredTargetName_TrailId.atc* The `.atc` file contains the following information: *trail_location end_time_of_audit_event_collection*

C.2.14 Microsoft Windows Plug-in for Oracle Audit Vault and Database Firewall

Learn about the Microsoft Windows plug-in for Oracle Audit Vault and Database Firewall.

Table C-19 lists the features of the Microsoft Windows plug-in.

Table C-19 Microsoft Windows Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.winos
Target Versions	Microsoft Windows Server 2012, 2012 R2, 2016 2019 (Starting with Oracle AVDF 20.2)
Target Platforms	Windows/x86-64
Setup Script(s)	No
Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	EVENT LOG See Table C-22 for descriptions of audit trail types.
Audit Trail Location	security (case-sensitive)
Audit Trail Cleanup Support	No

C.2.15 Microsoft Active Directory Plug-in for Oracle Audit Vault and Database Firewall

Learn about how to use the Microsoft Active Directory plug-in for Oracle Audit Vault and Database Firewall.

Table C-20 lists the features of the Microsoft Active Directory plug-in.

Table C-20 Microsoft Active Directory Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.msad
Target Versions	2012 to 2016 on 64 bit
Target Platforms	Windows/x86-64
Setup Script(s)	No
Target Location (Connect String)	*hostname* (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	EVENT LOG See Table C-22 for descriptions of audit trail types.
Audit Trail Location	directory service or security (case-sensitive)
Audit Trail Cleanup Support	No

C.2.16 Oracle ACFS Plug-in for Oracle Audit Vault and Database Firewall

Use the Oracle ACFS plug-in for Oracle Audit Vault and Database Firewall to implement Oracle ACFS in Oracle AVDF.

> **Note:**
>
> Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

Table C-21 lists the features of the Oracle ACFS plug-in.

Table C-21 Oracle ACFS Plug-in

Plug-in Specification	Description
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.acfs
Target Versions	12*c* Release 1 (12.1)
Target Platforms	Linux/x86-64 Solaris/x86-64 Solaris/SPARC64 Windows 2008, 2008 R2 64-bit
Setup Script(s)	No
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 C-22 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

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.2.17 Summary of Data Collected for Each Audit Trail Type

Explore the types of data that Oracle Audit Vault and Database Firewall (Oracle AVDF) collects for each audit trail type.

When you configure an audit trail for a target, you select the type of audit trail in the **Audit Trail Type** field. The audit trail type depends on your target type. Table C-22 describes the types of audit trails that you can configure for each target type.

Refer to the product documentation for your target type for details on its auditing features and functionality. See 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
- Oracle Solaris 10.6
- Oracle ACFS: *Oracle Advanced Cluster File System Administrator's Guide*

> **Note:**
>
> Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

Table C-22 Summary of Audit Trail Types Supported for Each Target Type

Target Type	Trail Type	Description
Oracle Database	TABLE Releases supported: 11.2.0.4; 12.1; 12.2; 18c; 19c. Release 21 (Starting Oracle AVDF 20.4)	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$` dictionary table • Oracle database 12.*x* unified audit trail, where audit events are written to the `UNIFIED_AUDIT_TRAIL` data dictionary view **Note:** The `SYS.AUD$` and `SYS.FGA_LOG$` tables have an additional column, `RLS$INFO`. The unified audit trail table has a `RLS_INFO` column. This column describes row-level security policies that are configured. This is mapped to the extension field in Oracle AVDF. To populate this column, set the `AUDIT_TRAIL` parameter of the target to `DB EXTENDED`.

Table C-22 (Cont.) Summary of Audit Trail Types Supported for Each Target Type

Target Type	Trail Type	Description
Oracle Database	DIRECTORY Releases 11.2.0.4, 12c, 18c; 19c.	Collects data from the following audit trails: • **On Linux and UNIX platforms:** Oracle database audit files that are written to the operating system (AUD and XML) files • **On Windows platforms:** Operating system XML files **Note:** Oracle recommends that you use unified audit table trails because directory trails are deprecated.
Oracle Database	TRANSACTION LOG 11.2.0.4 onwards for TRANSACTION LOG collection	Collects audit data from GoldenGate Integrated Extract files. If you plan to use this audit trail type, you can define the GoldenGate Integrated Extract rules to audit the tables from which GoldenGate Integrated Extract will capture audit information. The GoldenGate Integrated Extract files, in turn, are read by transaction log audit trail. For versions before 12.2, Oracle GoldenGate Downstream Mining must be configured. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for more information.
Oracle Database	SYSLOG	Collects Oracle audit records from either `syslog` or `rsyslog` audit files on Linux and Unix platforms only. If the system has both `syslog` and `rsyslog` installed, the exact `rsyslog` audit file location must be specified to collect data from `rsyslog` files. The following `rsyslog` formats are supported: • `RSYSLOG_TraditionalFileFormat` (has low-precision time stamps) • `RSYSLOG_FileFormat` (has high-precision time stamps and time zone information) Events from both formats appear the same on reports. However, with `RSYSLOG_FileFormat`, the `AVSYS.EVENT_LOG` table shows `EVENT_TIME` with microsecond precision. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for details on this table and Audit Vault Server schema documentation.
Oracle Database	EVENT LOG	Collects Oracle audit records from Microsoft Windows event logs on Windows platforms only.
Oracle Database	NETWORK	Collects network traffic (all database operations that use a TCP connection). Used for the Host Monitor Agent.

Table C-22 (Cont.) Summary of Audit Trail Types Supported for Each Target Type

Target Type	Trail Type	Description
Microsoft SQL Server	DIRECTORY	Collects audit data from the following: • `sqlaudit` • `trace` • `extended events` • `C2_DYNAMIC` • `TRACE_DYNAMIC`
Microsoft SQL Server	TRANSACTION LOG	In Oracle AVDF 20.9 and later, collects audit data from Oracle GoldenGate CDC Extract files. If you plan to use this audit trail type, you can define the GoldenGate CDC Extract rules to audit the tables from which GoldenGate CDC Extract will capture audit information. The GoldenGate CDC Extract files, in turn, are read by transaction log audit trail.
Microsoft SQL Server	EVENT LOG	Collects audit data from Windows application and security event logs.
Microsoft SQL Server	NETWORK	Collects network traffic (all database operations that use a TCP connection). Used for the Host Monitor Agent.
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 Agent.
Sybase SQL Anywhere	NETWORK	(For host monitoring only) Collects network traffic (all database operations using a TCP connection). **Note:** Sybase SQL Anywhere was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.
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 Agent.
MySQL	DIRECTORY	Collects XML-based audit data from a specified location
MySQL	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for Host Monitor Agent.
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. **Note:** Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.
Oracle Linux	DIRECTORY	Collects audit data from `audit.log`

Table C-22 (Cont.) Summary of Audit Trail Types Supported for Each Target Type

Target Type	Trail Type	Description
IBM AIX	DIRECTORY	Collects audit data from the binary audit log (`/audit/trail`). Only BIN auditing mode is supported. Any custom location of the audit log is configured in the `/etc/security/audit/config` file.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.3 Scripts for Oracle AVDF Account Privileges on Targets

Oracle Audit Vault and Database Firewall provides scripts for Oracle Database, Sybase, Microsoft, IBM DB2 for LUW, and MySQL plug-ins.

C.3.1 About Scripts for Setting up Oracle Audit Vault and Database Firewall Account Privileges

You can use scripts to set up accounts and privileges for Oracle Audit Vault and Database Firewall.

You must set up a user account with the correct privileges on each target for Oracle Audit Vault and Database Firewall to use to perform functions that are related to monitoring and collecting audit data. Oracle Audit Vault and Database Firewall provides setup scripts for this purpose so that you can configure your database targets. Depending on the type of target, the scripts set up user privileges that enable Oracle Audit Vault and Database Firewall to do the following functions:

- Audit data collection
- Audit policy management
- Stored procedure auditing
- User entitlement auditing
- Native Network Encrypted Traffic monitoring
- Audit trail cleanup (for some targets)
- Sensitive Data Discovery (for Oracle Database targets only)

When you deploy the Audit Vault Agent on a host computer (usually the same computer as the target), the setup scripts for creating the user permissions for Oracle Audit Vault and Database Firewall are in the following directory (Linux example below):

`$AGENT_HOME/av/plugins/com.oracle.av.plugin.`*`secured_target_type`*`/config/`

C.3.2 Oracle Database Setup Scripts

Download and use these scripts to set up user account privileges for Oracle Audit Vault and Database Firewall (Oracle AVDF) to audit Oracle Database targets.

Use these scripts to set up or revoke user privileges on Oracle Database so that Oracle AVDF can perform the following functions:

- Audit data collection
- Audit policy management
- Stored procedure auditing (SPA)
- User entitlement auditing
- Sensitive Data Discovery

Downloading Oracle Database Setup Scripts

To download the scripts from the Audit Vault Server console:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Targets** tab.
3. Click the **Target Setup Script** button.

Download and run the target setup scripts for auditing Oracle Database targets. The scripts aren't required for Database Firewall monitoring.

You can also access the scripts in the following directory (Linux example):

```
/opt/avdf/defaultagent/av/plugins/com.oracle.av.plugin.oracle/config/
```

Setting Up and Revoking User Privileges on Oracle Database Targets

To set up or revoke Oracle Audit Vault and Database Firewall user privileges on an Oracle Database target:

1. Create a user account for Oracle Audit Vault and Database Firewall on the Oracle Database. For example:

   ```
   SQL> CREATE USER username IDENTIFIED BY password
   ```

   You will use this user name and password when registering this Oracle Database as a target in the Audit Vault Server.
2. Connect as the `SYS` user with the `SYSDBA` privilege. For example:

   ```
   SQL> CONNECT SYS / AS SYSDBA
   ```

3. To set up Oracle Audit Vault and Database Firewall user privileges, run the following setup script and then enter the user name and mode at the prompts:

   ```
   SQL> @oracle_user_setup.sql
   ```

   Alternatively, you can enter the script, user name, and mode on one line:

   ```
   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 Audit Vault and Database Firewall, and for collecting data from any audit trail type. For example, use this mode for a TABLE audit trail in Oracle Audit Vault and Database Firewall.

- SPA: To enable stored procedure auditing for this database
- ENTITLEMENT: To enable user entitlement auditing for this database
- DBSAT_DISCOVERY: To enable sensitive data discovery for this database
- SQL_FIREWALL: To grant the AVDF user the SQL_FIREWALL_ADMIN role on the database, allowing AVDF to collect SQL Firewall violation logs and, if enabled, purge the violation logs as well.

> **Note:**
>
> - For audit collection from CDB, create a user in the CDB and run the oracle_user_setup.sql script for this user.
> - For audit collection from individual PDB, first alter the session to switch to the PDB, create the user on the PDB and then run the oracle_user_setup.sql script for this user.

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:

   Grant the Oracle Audit Vault and Database Firewall 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 Audit Vault and Database Firewall to monitor and collect audit trail data for Oracle Database Vault, and run Oracle Database Vault reports.

5. To revoke Oracle Audit Vault and Database Firewall user privileges, follow these steps:

   a. Connect to the database as the SYS user with the SYSDBA privilege.

   b. Run the following script and then enter the user name and mode at the prompts:

   ```
   SQL> @oracle_drop_db_permissions.sql
   ```

   Alternatively, you can enter the script, user name, and mode on one line:

   ```
   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 Audit Vault and Database Firewall, and for collecting data from any audit trail type.
     - SPA: To disable stored procedure auditing for this database
     - ENTITLEMENT: To disable user entitlement auditing for this database
     - DBSAT_DISCOVERY: To disable sensitive data discovery for this database

– SQL_FIREWALL: To revoke the AVDF user the SQL_FIREWALL_ADMIN role on the database, preventing AVDF from collecting and purging SQL Firewall violation logs.

Identifying Users with Audit Report Access in Oracle Audit Vault Server

To find out which users are able to check reports in AVDF, you need to connect to the AVDF server using SSH and run the following query:

```
select * from dba_role_privs where granted_role='AV_AUDITOR';
```

The output will return the users that have the AUDITOR privilege. Users such as SYS, AVREPORTUSER, OPS$DBFW_LOCAL_REPORT, AVSYS can be excluded since they are predefined (system) users. The rest of the listed users are able to connect as AUDITORS to the AVDF.

> **See Also::**
>
> Configuring Audit Trail Collection for CDBs and PDBs

C.3.3 Sybase ASE Setup Scripts for Oracle Audit Vault and Database Firewall

The Sybase ASE setup scripts configure audit data collection privileges and auditing privileges for Sybase ASE targets.

C.3.3.1 About Sybase ASE Setup Scripts

Learn about Sybase ASE setup scripts for Oracle Audit Vault and Database Firewall.

The following scripts are provided for configuring necessary user privileges for Oracle Audit Vault and Database Firewall in a Sybase ASE 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 Audit Vault and Database Firewall to perform the following functions for Sybase ASE:

- Audit data collection
- Stored procedure auditing (SPA)

C.3.3.2 Setting Up Audit Data Collection Privileges for Sybase ASE Targets

Set up audit data collection privileges for Sybase ASE targets to enable you to analyze audit data.

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

1. Create a user account for Oracle Audit Vault and Database Firewall 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 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 Audit Vault and Database Firewall 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.

C.3.3.3 Setting Up Stored Procedure Auditing Privileges for Sybase ASE Targets

You can configure stored procedure auditing privileges for Sybase ASE Targets.

To set up or revoke stored procedure auditing privileges on a Sybase ASE target:

1. If you have not already done so, then 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 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.

C.3.4 Sybase SQL Anywhere Setup Scripts

Learn how to use the Sybase SQL Anywhere setup scripts.

> **Note:**
>
> Sybase SQL Anywhere was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

The Oracle AVDF setup scripts for a Sybase SQL Anywhere 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 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.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.3.5 Microsoft SQL Server Setup Scripts

The Microsoft SQL Server setup scripts manage audit data collection and auditing privileges for Microsoft SQL Server targets.

C.3.5.1 About the SQL Server Setup Script

Use the Microsoft SQL Server setup script to set up or revoke user privileges for Oracle AVDF.

Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

The Oracle AVDF setup and drop scripts for a Microsoft SQL Server target are `mssql_user_setup.sql` and `mssql_drop_db_permissions.sql` for SQL Server 2014 and later (or `mssql_user_setup_pre2014.sql` and `mssql_drop_db_permissions_pre2014.sql` for releases prior to 2014).

Starting with Oracle AVDF 20.10, to download the scripts from the Audit Vault Server console:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Targets** tab.
3. Click the **Target Setup Script** button.

You can also access the scripts in the following directory:

AGENT_HOME`\av\plugins\com.oracle.av.plugin.mssql\config\`

These 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)

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.3.5.2 Setting Up Audit Data Collection Privileges for SQL Server Targets

You can set up audit data collection privileges for Microsoft SQL Server targets.

Prerequisites

Assign the following required privileges to run the commands in this topic:

Version and Usage	Command
To assign the required privileges in SQL Server 2014 and later	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.mssql\config\mssql_user_setup.sql
To revoke the assigned privileges in SQL Server 2014 and later	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.mssql\config\mssql_drop_db_permissions.sql
To assign the required privileges in SQL Server versions prior to 2014	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.mssql\config\mssql_user_setup_pre2014.sql
To revoke the assigned privileges in SQL Server versions prior to 2014	*AGENT_HOME*\av\plugins\com.oracle.av.plugin.mssql\config\mssql_drop_db_permissions_pre2014.sql

To set up or revoke Oracle AVDF user privileges for audit data collection:

1. Create a user account for Oracle AVDF in SQL Server or use a Windows authenticated user. For example:

   ```
   exec sp_executesql N'create login username with password = ''password'', check_policy= off'

   exec sp_executesql N'create user username for login username'
   ```

   Use this user name and password when registering this SQL Server database as a target in the Audit Vault Server.

2. Run the `mssql_user_setup.sql` or `mssql_user_setup_pre2014.sql` script with one of the following commands:

   For SQL Server authentication (SQL Server 2014 and later):

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

   For Windows authentication (SQL Server 2014 and later):

   ```
   sqlcmd -S localhost -U sa -i mssql_user_setup.sql -v username="[domain_name\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're 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 that 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` or `mssql_drop_db_permissions_pre2014.sql` script with one of the following commands:

   For SQL Server authentication (SQL Server 2014 and later):

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

   For Windows authentication (SQL Server 2014 and later):

   a. `sqlcmd -S server_name -U sa -i mssql_drop_db_permissions.sql -v username="[domain_name\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're 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 that you created in step 1.

   b. When prompted for a password, enter the system administrator password.

C.3.5.3 Setting Up Stored Procedure Auditing Privileges for SQL Server Targets

You can set up stored procedure auditing privileges for SQL Server targets.

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:

   ```
   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 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.

C.3.6 IBM DB2 for LUW Setup Scripts

The IBM DB2 for LUW setup scripts manage privileges for audit data collection and stored procedure auditing (SPA) privileges for IBM DB2 for LUW targets.

C.3.6.1 About the IBM DB2 for LUW Setup Scripts

Learn how to use the IBM DB2 for LUW setup scripts.

The Oracle Audit Vault and Database Firewall setup scripts for a DB2 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/
```

> **Note:**
>
> Connect string is not required from release 12.2.0.11.0 and onwards.

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)

C.3.6.2 Setting Up Audit Data Collection Privileges for IBM DB2 for LUW

You can configure audit data collection privileges for IBM DB2 for LUW to control access to the audit data.

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 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
      ```

C.4 Audit Collection Consideration

Considerations for audit collection on other target types.

C.4.1 Additional Information for Audit Collection from Oracle Active Data Guard

Learn about additional information required to collect audit data from Oracle Active Data Guard.

Oracle Active Data Guard is a high availability solution which consists of one primary database and multiple standby databases. This section contains some additional information for configuring different audit trails.

> **Note:**
>
> Oracle AVDF release 20.6 and prior:
>
> - When Traditional Auditing is enabled, Oracle AVDF supports audit collection from both the primary and standby databases of Oracle Active Data Guard. For Oracle Active Data Guard target, Traditional Auditing is recommended for Oracle AVDF release 20.6 and prior.
> - When Unified Auditing is enabled for Oracle Active Dataguard, audit collection is supported only from the primary database and not from the standby database. The audit data generated in the standby database is not collected.
>
> Oracle AVDF release 20.7 and later: When Unified Auditing is enabled, audit collection is supported from both the primary and standby databases of Oracle Active Data Guard. For Oracle Active Data Guard target, Unified Auditing is recommended for Oracle AVDF release 20.7 and later.

Traditional Auditing

Follow these steps for collecting audit data from databases in Oracle Active Data Guard with traditional auditing:

1. Set `AUDIT_TRAIL` parameter to `DB, EXTENDED` on all target databases.
2. Create a target in Oracle AVDF with a single connection string that contains the connection details of all the databases. This ensures that Oracle AVDF trail can read from `sys.aud$` table of the current primary database even when failover or switchover occurs.
3. For the above mentioned target configure Oracle Database table trail in Oracle AVDF to read the records from `sys.aud$`.
4. Create one target in Oracle AVDF for every database in Oracle Active Data Guard with a connection string that contains connection details of only the specific database.
5. Configure one directory trail in Oracle AVDF for every target to collect data from `*.aud` log file for the specific target database in Oracle Active Data Guard.

Unified Auditing (Oracle AVDF 20.6 and Earlier)

Audit data can be collected only from the primary database in Oracle Active Data Guard with unified auditing in releases Oracle AVDF 20.6 and prior. Follow these steps:

1. Create a target in Oracle AVDF with single connection string that contains the connection details of all the databases. This ensures that Oracle AVDF trail can read from `unified_audit_trail` table of the primary database even when failover or switchover occurs.
2. Create Oracle Database table trail in Oracle AVDF to read the records from `unified_audit_trail` of the primary database.

Unified Auditing (Oracle AVDF 20.7 and Later)

Audit data can be collected from both the primary and standby databases in Oracle Active Data Guard with unified auditing. This is applicable starting with Oracle AVDF release 20.7. Follow these steps:

1. Ensure to apply patch (33568223 and 33420490) on all the databases in the Oracle Active Data Guard setup.
2. Create a failover connection string which always connects to the current primary database in Oracle Active Data Guard.
3. Registration of a single target database is required in Oracle AVDF to collect audit data from all the databases in Oracle Active Data Guard.
4. Select **Active Data Guard** checkbox during target registration.
5. In the **Failover Connection String** text box, enter the failover connection string which always connects to current primary database.
6. Create an attribute in the **Audit Collection Attributes** tab for every database in the Oracle Active Data Guard configuration as follows:
   - Each attribute should be in the format `av.target.connection.<name>` where `<name>` can be any identifier defined by the user to identify the database.
   - The value corresponding to each attribute should be specified as the connection string of that specific database. For example, if there are three databases in Oracle Active Data Guard configuration, then the user can create these attributes:

Attribute Name	Attribute Value
`av.target.connection.first_db`	Dedicated connection string of the first database.
`av.target.connection.second_db`	Dedicated connection string of the second database.
`av.target.connection.third_db`	Dedicated connection string of the third database.

7. For audit collection create one trail for every database in the Oracle Active Data Guard configuration. Create an additional trail that uses the failover connection string. The remaining trails must use the connection string specified in the **Audit Collection Attributes**.
8. Click **Add** to create an audit trail and specify the following. This step has to be performed only once. There will be only one trail which uses the failover connection.

Field	Select or enter the value
Audit Trail Type	`TABLE`
Trail Location	`UNIFIED_AUDIT_TRAIL`
Connection	`FAILOVER_CONNECTION`

9. Click the **Add** button to create the trails and select the following options. This step has to be performed for every database in the Oracle Active Data Guard.

Field	Select or enter the value
Audit Trail Type	`TABLE`

Trail Location	UNIFIED_AUDIT_TRAIL
Connection	av.target.connection.<name>

For cleanup of file based audit data on standby database, use DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL with AUDIT_TRAIL_TYPE as DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED_FILES.

For cleanup of file based audit data on primary database, use DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL with AUDIT_TRAIL_TYPE as DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED_FILES.

For cleanup of table based audit data on primary database, use DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL with AUDIT_TRAIL_TYPE as DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED_TABLE. Since the databases are in Active Data Guard configuration, this will also cleanup table based audit data from all the standby databases.

C.4.2 Additional Information for Audit Collection from Oracle Data Guard

Learn about additional information required to collect audit data from Oracle Data Guard.

Oracle Data Guard is a high availability solution which consists of one primary database and multiple standby databases. This section contains some additional information for configuring different audit trails.

Traditional Auditing

Audit data can be collected from the current primary database in Oracle Data Guard with traditional auditing. Follow these steps:

1. Set AUDIT_TRAIL parameter to DB, EXTENDED, on all target databases.
2. Create a target in Oracle AVDF with a single connection string that contains the connection details of all the databases. This ensures that Oracle AVDF trail can read from sys.aud$ table of the current primary database after failover or switchover occurs.
3. Create Oracle Database table trail in Oracle AVDF to read the records from sys.aud$. of the current primary database.

Unified Auditing

Audit data can be collected from the current primary database in Oracle Data Guard with unified auditing. Follow these steps:

1. Create a target in Oracle AVDF with single connection string that contains the connection details of all the databases. This ensures that Oracle AVDF trail can read from unified_audit_trail table of the current primary database after failover or switchover occurs.
2. Create Oracle Database table trail in Oracle AVDF to read the records from unified_audit_trail of the current primary database.

> **Note:**
>
> Oracle AVDF supports audit collection from the traditional audit trail and unified audit trail for the current primary database only. In case of switchover or failover, audit collection starts on the new primary database, from the point at which the collection had stopped on the old primary database. Audit collection is not supported from the standby database.

C.5 Audit Trail Cleanup

Some Oracle Audit Vault and Database Firewall plug-ins include audit trail cleanup utilities.

C.5.1 Oracle Database Audit Trail Cleanup

Oracle Database provides the ability to purge audit trails both manually and with scheduled jobs.

C.5.1.1 About Purging the Oracle Database 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. The target database user must have the EXECUTE privilege on DBMS_AUDIT_MGMT to use it.

Oracle Database 11g release 2 (11.2) or later includes the `DBMS_AUDIT_MGMT` package and its associated data dictionary views installed by default. If your target database does not have this package installed, then you can download the package and data dictionary views from My Oracle Support.

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 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

C.5.1.2 Scheduling Automated Purge Jobs

Simplify maintenance by scheduling automated jobs to purge unneeded audit data.

Oracle Audit Vault and Database Firewall is integrated with the `DBMS_AUDIT_MGMT` package on an Oracle Database. This integration automates the purging of audit records from the `UNIFIED_AUDIT_TRAIL`, `AUD$`, and `FGA_LOG$` tables, 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 target:

1. Log in to SQL*Plus on the 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;
   /
   ```

   > **Note:**
   >
   > - In case you are collecting audit data from CDB, then execute this step every time there is any change in the PDB instance.
   > - In case you are using a CDB unified audit trail, then use `CONTAINER_ALL` parameter in the above command.

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;
/
```

C.5.1.3 How to Prevent Duplication Collection of Audit Trail Data From a Secure Target

Learn how to configure audit trails on Audit Vault Server to collect audit data from registered secure targets while avoiding duplicate collection of data.

`AVSYS.CHECKPOINT` table stores `CHECKPOINT_TIME` for each audit trail. It indicates time stamp, up to which, audit records are collected from secure targets audit trail and inserted/committed to `AVSYS.EVENT_LOG` table.

`LAST_ARCHIVE_TS` column of `DBA_AUDIT_MGMT_LAST_ARCH_TS` view is also updated to indicate time stamp, up to which, the audit data has been collected by audit trail. This helps in deciding the purge operation to prevent deleting those records which are yet to be collected by Audit Trails.

However `LAST_ARCHIVE_TS` column value does not play any role for an Audit trail to decide from where it has to read audit data during next read operation. As Audit Trail will always refer `AVSYS.CHECKPOINT` table when collector restarts, it will resume collection from `CHECKPOINT_TIME`. So Audit Trail will not read any record which has a time stamp lesser than `CHECKPOINT_TIME`.

So it clarifies that Audit Trail is not dependent on value stored in database last archive time stamp at secure target side to decide the point from which it had to collect. Rather it is just an indication for secure target to know that till this time stamp audit data has been collected hence it can be purged.

> **Note:**
>
> As it is evident that `LAST_ARCHIVE_TS` column can be modified manually whereas `CHECKPOINT_TIME` column `AVSYS.CHECKPOINT` table in Audit Vault server is manged automatically and not supposed to be modified manually. Therefore these two columns need not necessarily be in sync with each other.

C.5.1.4 Oracle GoldenGate Extract Cleanup

Learn how to use Oracle GoldenGate extract cleanup and simply maintenance.

Use the Oracle GoldenGate extract cleanup utility to simplify maintenance. This utility is available starting Oracle AVDF 20.4.

To run the Oracle GoldenGate extract cleanup utility:

1. Navigate to the following directory on the host machine:

   ```
   AGENT_HOME\av\plugins\com.oracle.av.plugin.oracle\bin
   ```

2. Run the following command:

```
OracleGoldenGateExtractCleanupHandler <target name> <Agent deployed
location>
```

The above command has the following variables:

`<target name>` is the name of the registered target.

`<Agent deployed location>` is the full path of the directory where the Agent is deployed.

> **Note:**
>
> Ensure to specify the timezone offset when creating the target, using the target attribute `av.collector.timezoneoffset`. Also ensure the Agent machine and Oracle Database target are in the same timezone.

C.5.2 Microsoft SQL Server Audit Trail Cleanup

Learn about cleaning up your Microsoft SQL Server audit trail.

Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

If the SQL Server audit trail has collected data from a trace, extended events, 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.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.5.2.1 Cleaning Up Oracle GoldenGate Extracts

Use the Oracle GoldenGate Extract cleanup utility to simplify maintenance.

> **Note:**
>
> To purge collected audit data from a remote collection, you need to set the rollover file number and size. These values are set on the Microsoft SQL Server.

1. Navigate to the following directory on the host machine:

   ```
   AGENT_HOME\av\plugins\com.oracle.av.plugin.mssql\bin
   ```

2. Run the following command:

   ```
   SQLServerGoldenGateExtractCleanupHandler.bat <target name> <agent deployed location>
   ```

   <target name> is the name of the registered target.

   <agent deployed location> is the full path of the directory where the Audit Vault Agent is deployed.

C.5.3 MySQL Audit Trail Cleanup

Use the MySQL audit trail cleanup utility to simplify maintenance.

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 target
   - *AGENT_HOME* - the path to the directory where the Audit Vault Agent is deployed.

C.5.3.1 Cleaning Up Oracle GoldenGate Extracts

Use the Oracle GoldenGate Extract cleanup utility to simplify maintenance.

1. Navigate to the following directory on the host machine:
AGENT_HOME\av\plugins\com.oracle.av.plugin.mysql\bin
2. Run the following command:

   ```
   MySQLGoldenGateCleanupHandler <target name> <Agent deployed location>
   ```

   <target name> is the name of the registered target.

   <Agent deployed location> is the full path of the directory where the Audit Vault Agent is deployed.

C.5.4 IBM DB2 Audit Trail Cleanup

Learn about using the IBM DB2 scripts to cleanup records.

Refer to Converting Binary Audit Files to ASCII Format for IBM DB2 for information regarding DB2 records cleanup.

C.6 Procedure Look-Ups: Connect Strings, Collection Attributes, Audit Trail Locations

Procedure lookups enable you to fine tune and customize audit records generation.

C.6.1 Target Locations (Connect Strings)

Use connect strings to register target locations in the Audit Vault Server console.

When registering a target in the Audit Vault Server console, you enter a connect string in the **Target Location** field. Use a connect string format from Table C-23 depending on the target type.

> **Note:**
>
> The connection string is mandatory for audit collection. However, it's not required for Database Firewall monitoring.

Table C-23 Target Connect Strings (for Target Location Field)

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` **Note:** Sybase SQL Anywhere was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

Microsoft SQL Server (SQL Server Authentication)	`jdbc:av:sqlserver://hostname:port`
	When SSL Encryption is used with MSSQL sever and the server certificate validation is required. Ensure that agent TLS level is set to *Level 4*.
	`jdbc:av:sqlserver://<MSSQL Host name>:<Port number>;encryptionMethod=SSL;validateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;trustStore=<key store jks path>;trustStorePassword=<keystore password>;extendedOptions=enableCipherSuites=SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA`
	When SSL Encryption is used with MSSQL sever and the server certificate validation is not required.
	`jdbc:av:sqlserver://<MSSQL Host name>:<Port number>;encryptionMethod=SSL;validateServerCertificate=false;CryptoProtocolVersion=TLSv1.2;`

Microsoft SQL Server (Windows Authentication)	`jdbc:av:sqlserver://<Host Name>:<Port>;authenticationMethod=ntlmjava`
	`(Use Windows user credentials along with domain. For example, <domain name>\<user name > and password.)`
	OR
	`jdbc:av:sqlserver://<Host Name>:<Port>;authenticationMethod=ntlmjava;domain=<domain name>`
	`Use Windows user credentials without domain. For example, <user name > and password.`

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) **Note:** Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.
IBM AIX	*hostname* (fully qualified machine name or IP address)

Related Topics

- Registering or Removing Targets in Audit Vault Server
  Learn about registering and removing targets in Audit Vault Server.
- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.6.2 Audit Collection Attributes

Oracle Audit Vault and Database Firewall (Oracle AVDF) provides audit collection attributes that are specific to the target platform, such as Oracle Database or MySQL.

C.6.2.1 About Audit Collection Attributes

Specify audit collection attributes when configuring targets.

Some types of targets have optional or required audit trail collection attributes. You can specify audit collection attributes when registering or modifying targets in the **Audit Collection Attributes** fields.

The following target types do not require audit collection attributes:

- Microsoft SQL Server
- Sybase ASE
- Oracle Solaris
- Windows
- Linux
- Microsoft Active Directory Server

> **See Also:**
>
> Registering or Removing Targets in Audit Vault Server

C.6.2.2 Oracle Database Audit Collection Attributes

Specify audit collection attributes to control the types of data that Audit Vault collects.

You can specify audit collection attributes for a DIRECTORY audit trail for Oracle Database. Table C-24 describes the audit collection attributes you can use if you select DIRECTORY as the **Audit Trail Type** when registering an Oracle Database target in Oracle Audit Vault and Database Firewall.

Table C-24 Audit 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 target (for example, target is not running) **No:** If the started audit trail is able to connect to the Oracle target and get these parameter values from the target (for example, the target is running when the trail is started)	NA	The value is not case sensitive.

Table C-24 (Cont.) Audit Collection Attributes for DIRECTORY Audit Trail for Oracle Database

Attribute Name and Description	Required?	Default	Comments
ORCLCOLL.NLS_TERRITORY The NLS territory of the data source	**Yes:** If the started audit trail cannot establish a connection to the Oracle target (for example, target is not running) **No:** If the started audit trail is able to connect to the Oracle target and get these parameter values from the target (for example, the 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 target (for example, target is not running) **No:** If the started audit trail is able to connect to the Oracle target and get these parameter values from the target (for example, the target is running when the trail is started)	NA	The value is not case sensitive.
ORCLCOLL.RAC_INSTANCE_ID The instance ID in an Oracle RAC environment	No	1	None.
AV.COLLECTOR.DATABASECHARSET The NLS character set of the data source.	Yes: If the audit trail started cannot establish a connection to the target Oracle Database. For example, the target is not running. No: If the audit trail started is able to connect to the target Oracle Database and get these parameter values from the target. For example, the target is running when the trail is started.	NA	None.
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.

Table C-24 (Cont.) Audit Collection Attributes for DIRECTORY Audit Trail for Oracle Database

Attribute Name and Description	Required?	Default	Comments
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 target.
AV.COLLECTOR.TIMEZONEOFFSET Timezone offset of Oracle Database target	Optional. **Note:** For Oracle AVDF release 20.1 only, it is a mandatory target attribute for Transaction Log audit collection. This attribute is not required from Oracle AVDF release 20.2 and onwards, as the Transaction Log audit trail fetches the time zone offset from the target database.	NA	None.

C.6.2.3 IBM DB2 for LUW Audit Collection Attribute

Learn about the IBM DB2 for LUW audit collection attribute.

Table C-25 describes the audit collection attribute required when you register an IBM DB2 for LUW target in Oracle AVDF.

Table C-25 Audit 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. **Note:** The audit collection attribute is not required from release 12.2.0.11.0 and onwards.

C.6.2.4 MySQL Audit Collection Attributes

Learn about the MySQL audit collection attributes.

Table C-26 describes the required and optional audit collection attributes when you register a MySQL target in Oracle Audit Vault and Database Firewall.

Table C-26 Audit Collection Attributes for MySQL Database

Attribute Name and Description	Required?	Default	Comments
av.collector.securedTargetVersion The MySQL database version	**Yes**	8.0	NA

Table C-26 (Cont.) Audit Collection Attributes for MySQL Database

Attribute Name and Description	Required?	Default	Comments
`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 in the ATC file. Audit log files that have a time stamp older than 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

C.6.2.5 Oracle ACFS Audit Collection Attribute

Learn about the Oracle ACFS target audit collection attribute.

> **Note:**
>
> Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

Table C-27 describes the audit collection attribute required when you register an Oracle ACFS target in Oracle Audit Vault and Database Firewall.

Table C-27 Audit 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`.

C.6.3 Audit Trail Locations

When you configure an audit trail for a target in the Audit Vault Server, you specify a trail location. The trail location depends on the type of target.

> **Note:**
>
> Trail locations are case sensitive. To avoid duplicate data collection, Oracle recommends that you provide the entire trail location either in all capital letters or all lowercase letters.

> **Note:**
>
> If you select DIRECTORY for the audit trail type, the trail location must be a directory mask.

Table C-28 Supported Trail Locations for Targets

Target Type	Trail Type	Supported Trail Locations
Oracle Database	Table	`SYS.AUD$`, `SYS.FGA_LOG$`, `DVSYS.AUDIT_TRAIL$`, `UNIFIED_AUDIT_TRAIL`, `CDB_UNIFIED_AUDIT_TRAIL` `SYS.DBA_SQL_FIREWALL_VIOLATIONS` on Oracle Database 23ai
Oracle Database	Directory	Full path to the directory that contains the AUD or XML files
Oracle Database	syslog	Full path to the directory that contains the `syslog` or `rsyslog` file Include the `syslog` or `rsyslog` file prefix in the path. For example, if the file names are `messages.0`, `messages.1`, and so on, you might use the following path: `/scratch/user1/rsyslogbug/dbrecord/messages` You can also enter `Default` and the system will search for either the `syslog` or the `rsyslog` location. If both are present, entering `Default` causes the audit trail to collect data from the `syslog` files.
Oracle Database	Event log	No trail location required
Oracle Database	Transaction Log	Full path to the directory that contains the Oracle GoldenGate Integrated Extract XML trail file
Oracle Database	Network*	`NETWORK/<network interface name>`, `LOCAL/<loopback adapter name>` and `LOCAL/Bequeath` `LOCAL/Bequeath` trail is supported only for Linux and Solaris platform.
Microsoft SQL Server	Directory	`*.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, 2014, and 2016. Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.
Microsoft SQL Server	Event log	`application` or `security` (SQL Server 2008, 2012, 2014, and 2016) Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

Table C-28 (Cont.) Supported Trail Locations for Targets

Target Type	Trail Type	Supported Trail Locations
Microsoft SQL Server	Transaction Log (Oracle AVDF 20.9 and later)	Full path to the directory that contains the Oracle GoldenGate CDC Extract XML trail file
Microsoft SQL Server, MySQL and all types supported for Firewall monitoring	Network*	`NETWORK/<network interface name>` and `LOCAL/<loopback adapter name>`
IBM DB2 for LUW	Directory	Path to a directory, for example: `d:\temp\trace`
Sybase ASE	Table	`SYSAUDITS`
PostgreSQL	Directory	Path to the directory that contains the CSV audit files
MySQL	Directory	Path to the directory where converted XML files are created when you run the MySQL XML transformation utility
Linux	Directory	Default location of the `audit.log` (`/var/log/audit/audit*.log`) or any custom location that is configured in the `/etc/audit/auditd.conf` file
Microsoft Windows	Event log	`security` (case-insensitive) You can use any case combination in the word `security`. However, after you start collecting a trail with 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 Solaris	Directory	*`hostname`*`:`*`path_to_trail`* The *`hostname`* matches the host name in the audit log names, which look like this: *`timestamp1.timestamp2.hostname`*
AIX	Directory	`/audit/trail`
Oracle ACFS	Directory	Path to the directory that contains XML audit files For example, a file system that is mounted at *`$MOUNT_POINT`* has the following audit trail location: *`$MOUNT_POINT`*`/.Security/audit/`

Note:

Oracle Automatic Storage Management Cluster File System (Oracle ACFS) or Oracle Advanced Cluster File System was deprecated in Oracle AVDF release 20.7 and is desupported in 20.8.

Table C-28 (Cont.) Supported Trail Locations for Targets

Target Type	Trail Type	Supported Trail Locations
Microsoft Active Directory Server	Event log	`directory service` or `security` (case-insensitive) You can use any case combination in the words `directory service` or `security`. However, after you start collecting a trail with 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.

*For Oracle AVDF 20.12 and earlier, the trail location will be empty, and you will need to set the attribute `network_device_name_for_hostmonitor`.

Starting in Oracle AVDF 20.13, the trail location drop-down lists available network interface cards. If multiple interfaces are involved, create separate trail for each.

Related Topics

- Adding Audit Trails with Agent-Based Collection
  To begin collecting audit data with the Audit Vault Agent, configure an audit trail for each target that's registered on the Audit Vault Server and then start the audit trail collection.
- Running the XML Transformation Utility for MySQL Audit Formats
  Learn how to run the XML transformation utility for MySQL audit formats.
- Behavior Changes, Deprecated, and Desupported Platforms and Features

C.7 Installing the Audit Vault Agent Under Its Own OS User Account

For environments that require more separation of duties, you can install the Audit Vault Agent under it's own OS user account instead of under the OS user account that owns the Oracle software installation.

You have two options:

- Traditional Unix permissions
- POSIX access control lists (ACLs)

Traditional Unix Permissions

This is the simplest option. It involves adding the Audit Vault Agent user `avagentosuser` to the same primary group (usually `oinstall`) as the Oracle software owner. Sometimes the database does write out an audit file without group read access. This is easy to maintain with the `chmod g:rx` command.

POSIX ACLs

POSIX ACLs let you set privileges on files and directories that override traditional UNIX permissions.

Here are some points to consider before choosing this approach:

- If you're using Oracle Exadata, when a quarterly bundle patch is applied, the file access control list (FACL) packages are removed (or have to be removed to avoid bundle patch

conflicts). When FACL packages are removed, the existing FACLs that are set stay in effect.

- If the DBAs move any directory in the `audit_file_dest` path, the FACLs break. A simple action like `mv audit audit.old; mkdir audit` would break the FACL on that directory.
- The FACL command to `setFACL` can only be run by `root`.

  If the FACLs are broken (or FACL binaries or packages are missing after a bundle patch is applied) and the DBA or Audit Vault Server administrator must work with a system administrator with `root` access to resolve the issue, then audit collection may no longer be in near real time.
- The `/etc/fstab` mount point must have `acl` set so the ACLs will be applied to that file system and remounted.

You can apply FACLs to the directory to allow access for a specific user. Any new file that's created in that directory (like a new audit record) will have the FACL permissions. Any audit file that exists in the directory before you apply the FACL will not have the FACL permissions, so you need to apply the `setFACL` command to each file individually.

Each directory in the fully qualified path to the audit directory must have the FACL set so that the dedicated user can traverse the path to the audit files.

Example C-1 Applying FACLs

This example uses the `root` user and an OS user named `avagent`.

Between running the UNIX commands as `root`, you can user your OS user account to see the results.

1. Run the following commands as `root`:

```
mkdir -p /tmp/dir1/dir2/audit


mkdir -p /tmp/dir1/dir2/audit2


touch /tmp/dir1/dir2/audit/file1


touch /tmp/dir1/dir2/audit2/file2


chmod -R 750 /tmp/dir1
```

2. Grant access to the `/tmp/dir1/dir2/audit` directory only for the `avagent` OS user. You have to do this for every directory (just like you would with `chmod 750`, for example).

```
setfacl -m u:avagent:rx /tmp/

setfacl -m u:avagent:rx /tmp/dir1

setfacl -m u:avagent:rx /tmp/dir1/dir2

setfacl -m u:avagent:rx /tmp/dir1/dir2/audit
```

   The `avagent` OS user can now access the `/tmp/dir1/dir2/audit` directory but not the `/tmp/dir1/dir2/audit2` directory, because no FACL is applied there.

3. To see whether an FACL is applied on a file or directory, use the following command:

```
getfacl <file/directory>
```

4. Specify that any new files that are created in the `/tmp/dir1/dir2/audit` directory will have the `rx` access for the `avagent` OS user.

```
setfacl -dm u:avagent:rx /tmp/dir1/dir2/audit
```

5. To verify that the default information is set up correctly, use the following command:

```
getfacl /tmp/dir1/dir2/audit
```

6. To test the preceding settings, create a new file in `/tmp/dir1/dir2/audit`.

```
echo "test" > /tmp/dir1/dir2/audit/file3
```

   The `avagent` OS user can access `file3` but not `file1`.

7. Use `getfacl` to check the differences between the files.

```
getfacl /tmp/dir1/dir2/audit/file1

getfacl /tmp/dir1/dir2/audit/file3
```

8. To resolve files that didn't have a FACL applied before `setfacl -d [default]` was set up to apply to any new file in the directory, apply the FACL to the files.

```
setfacl -m u:avagent:rx /tmp/dir1/dir2/audit/file1
```

   You can also use wildcards. For example:

```
setfacl -m u:avagent:rx /tmp/dir1/dir2/audit/*
```

9. To test moving files into the `/tmp/dir1/dir2/audit` directory, run the following commands:

```
mv /tmp/dir1/dir2/audit2/file2 /tmp/dir1/dir2/audit/
```

```
getfacl /tmp/dir1/dir2/audit/file2
```

The moved file doesn't have the FACL applied because it wasn't created in the directory when the `setfacl -d [default]` was set up, so you have to apply the FACL to the moved file.

```
setfacl -m u:avagent:rx /tmp/dir1/dir2/audit/file2
```

D

Transaction Log Audit Data Collection for Oracle Database

You can fine-tune audit data collection by setting REDO log parameters for Oracle Database targets.

D.1 Introduction to Transaction Log Audit Trails for Oracle Database Using Oracle GoldenGate

Learn about the recommended collection from REDO logs settings using Oracle GoldenGate.

REDO log files also known as transaction logs are files used by Oracle Database to maintain logs of all the transactions that have occurred in the database. This chapter contains the recommendations for setting initialization parameters to use the *TRANSACTION LOG* audit trail type to collect audit data from the REDO logs of Oracle Database target.

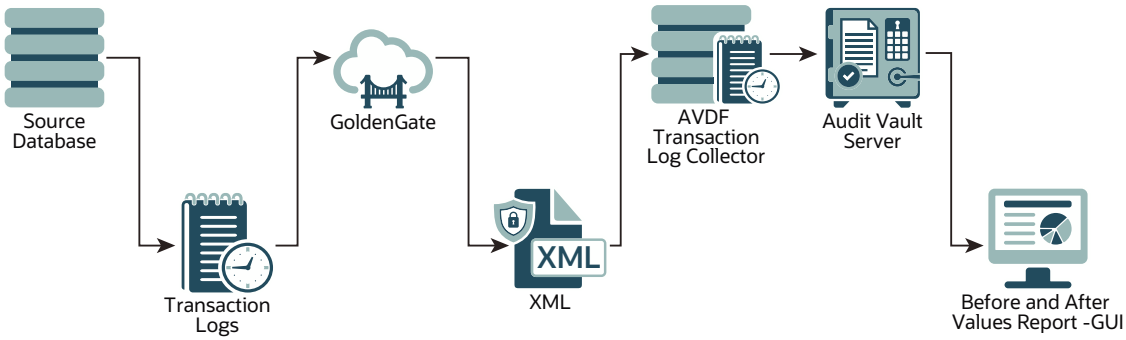
These log files allow Oracle Database to recover the changes made to the database in case of a failure. For example, if a user updates a salary value in a table that contains employee related data, a REDO record is generated. It contains the value before this change (old value) and the new changed value. REDO records are used to guarantee ACID (Atomicity, Consistency, Isolation, and Durability) properties over crash or hardware failure. In case of a database crash, the system performs redo (re-process) of all the changes on data files that takes the database data back to the state it was when the last REDO record was written.

REDO log records contain *Before and After values* for every DML (Data Manipulation Language) and DDL (Data Definition Language) operations. Oracle Audit Vault and Database Firewall provides the ability to monitor the changed values from REDO logs using Transaction Log collector.

Transaction Log collector takes advantage of *Oracle GoldenGate's Integrated Extract* process to move the REDO log data from database to XML files. The extract process is configured to run against the source database or it is configured to run on a Downstream Mining database (Oracle only). It captures DML and DDL operations that are performed on the configured objects. The captured operations from transaction logs are transferred to GoldenGate XML trail files. Oracle AVDF's Transaction Log collector collects transaction log records from generated XML files. These logs are forwarded to the Audit Vault Server to show the before and after values that were changed in the **Data Modification Before-After Values** report. The DDL changes are available in the **All Activity** report. The DML changes are available in the **Data Modification Before-After Values** report.

Starting with Oracle AVDF 20.10, the **Data Modification Before-After Values** report has additional information about key columns. GoldenGate, by default, uses the primary key columns of the table as key columns. If no primary keys are defined for the table, or if you want to use some other columns as key columns, then GoldenGate provides an option to specify key columns in the parameter file.

Figure D-1 Transaction Log Collection Process



> **See Also:**
>
> Oracle Database Setup Scripts for instructions on setting up privileges in the Oracle Database for collecting audit data from the REDO logs.

D.2 Sizing Guidelines

Learn and follow the sizing guidelines outlined in this topic.

Prerequisites

Adhere to the system and sizing requirements outlined in System Requirements and Operating System Requirements of Oracle GoldenGate documentation.

General sizing guidelines

1. General recommendation for memory and CPU is to start with 32G memory and 2 CPUs per Integrated Extract as it is a multi threaded process and uses large memory when processing large transaction. Depending on the transaction volume and transaction pattern, scale up the resources appropriately following the guidelines in Oracle GoldenGate documentation.
2. General recommendation for disk space is to start with 2T, and vary based on the volume of data the Integrated Extract captures from the source databases. Extract uses storage for trail files and temporary disk space for cache files in case there is big transaction to buffer for processing.

There are multiple database dictionary views in the computation formulae referred in the guidelines. They provide information on transaction log size. For example, `v$log` gives detailed information of each online log. Similarly number of log switches per day can be estimated from `v$log_history/gv$log_history`.

Temporary disk space requirements on account of large transactions may fill up cache and spill over to the transaction cached data or temporary files. Configure an archive policy and define the retention period of the files, so they can be recycled accordingly.

Maintain enough physical memory to handle large transactions. As per the guidelines, have at least 32 GB of memory available for Extract to use. For a more accurate estimation, collect the statistics from the database server history run and check for the size of the biggest transaction.

Oracle GoldenGate provides `send <extract> cachemgr, cachestats` command that displays the statistics of the transaction, that is helpful to determine the base line for estimation.

In general, the sizing, storage, and memory for Oracle GoldenGate Integrated Extract process is highly dependent on the transaction volume and transaction pattern. Collect these statistics from every single database server to estimate as there is no standard value.

The number of databases that can be supported by a single GoldenGate instance or Integrated Extract process, depends on the system resources that support multiple extracts. Ensure to configure one extract for every database.

> **Note:**
>
> - Other Disk Space Considerations
> - Temporary Disk Requirements

D.3 Restricted Use License for Oracle GoldenGate

Learn about restricted license of Oracle GoldenGate.

A restricted use license for Oracle GoldenGate is included with Oracle Audit Vault and Database Firewall release 20. This license permits you to install Oracle GoldenGate and use the Integrated Extract process to capture transactional changes in database systems monitored by Oracle AVDF. The extracted data from Oracle GoldenGate is consumed only by Oracle AVDF. Deploy Oracle GoldenGate Microservices Architecture on a separate server other than the server on which the Oracle AVDF appliance is deployed. Later configure the Integrated Extract feature of Oracle GoldenGate. Oracle GoldenGate version 19.1.0.0.4 is the minimum version supported with Oracle Audit Vault and Database Firewall 20.9 and earlier, and Oracle GoldenGate 21.9.0.0.0 is the minimum version supported with Oracle Audit Vault and Database Firewall 20.10 and later. To support Oracle Databases prior to 12.2, Downstream Mining needs to be configured. It requires the deployment of Oracle Database Enterprise Edition and has to be licensed separately.

D.4 Installing Oracle GoldenGate on Oracle Databases

Follow these instructions to install Oracle GoldenGate for Oracle Databases.

Deploy Oracle GoldenGate on a separate server other than the server on which the Oracle AVDF appliance is deployed. Then configure the Oracle GoldenGate Integrated Extract feature.

Oracle AVDF 20.9 and Earlier

Download and install Oracle GoldenGate 19.1.0.0.0 Microservices architecture from Oracle Software Delivery Cloud.

Follow the instructions for Installing Oracle GoldenGate for Oracle Databases in the Oracle GoldenGate 19c documentation. After installing Oracle GoldenGate, apply the Oracle GoldenGate 19.1.0.0.4 Microservices architecture patch from My Oracle Support.

> **Note:**
>
> After installing Oracle GoldenGate, contact Oracle Support to create a Merge Label Request for applying the patch 32063871, 32175609, 33701099, 34014874, and 36684067. This patch needs to be applied on Oracle GoldenGate installation.

Oracle AVDF 20.10 and Later

Download and install Oracle GoldenGate 21.9.0.0.0 Microservices architecture from My Oracle Support (patch 34958369 complete install).

Follow the instructions for Installing Oracle GoldenGate in the Oracle GoldenGate Microservices documentation for Oracle GoldenGate 21c.

D.5 Capturing Transaction Log Data from Oracle Database 12.2.0.1 and Later

Learn how to capture Transaction Log data from Oracle Database versions 12.2.0.1 and later.

Oracle GoldenGate Integrated Extract process is supported only for Oracle Database versions 12.2.0.1 and later. In this case Oracle GoldenGate Integrated Extract is configured on the source database. To capture Transaction Log data from Oracle Database 12.2.0.1 or later, run the steps in the following sections and in the same order:

1. Create User and Grant Relevant Privileges
2. Configure Oracle GoldenGate Parameters for Oracle Database
3. Create a New Credential in the GoldenGate Administration Server
4. Create a New Integrated Extract in Oracle GoldenGate Administration Server

D.6 Downstream Mining to Capture Transaction Log Data from Oracle Database Prior to 12.2.0.1

Learn how to capture Transaction Log data from Oracle Database versions prior to 12.2.0.1.

Oracle GoldenGate Integrated Extract process is supported only for Oracle Database versions 12.2.0.1 and later. In this case Oracle GoldenGate Integrated Extract is configured on the source database.

For capturing Transaction Log data from Oracle Database versions prior to 12.2.0.1, Downstream Mining must be used. In this case there are 2 databases, the source database and the Downstream Mining database. The source database (Oracle Database prior to 12.2.0.1) is configured to ship the online REDO logs to a Downstream database (Oracle Database version 12.2.0.1 or later). Integrated Extract is then configured on the Downstream database.

> **Note:**
>
> - Before configuring Downstream Mining, execute the steps in sections Create User and Grant Relevant Privileges and Configure Oracle GoldenGate Parameters for Oracle Database on both the source database and the Downstream Mining database.
> - Configure Downstream Mining by referring to section Configure GoldenGate Downstream Mining.

D.7 Migrating Transaction Log Audit Trail from Oracle AVDF 12.2 to 20

Learn how to migrate transaction log audit trail from Oracle AVDF 12.2 to 20.

Transaction log audit trail data can be migrated from Oracle AVDF 12.2 to 20. Follow this procedure before upgrading to Oracle AVDF 20:

1. Install and deploy Oracle GoldenGate.
2. Run the below procedure for every transaction log audit trail in Oracle AVDF 12.2:
   a. Ensure Oracle AVDF 12.2 transaction log audit trail is running on the Oracle source database. Create Oracle Goldengate integrated extract. If Oracle source database is older than 12.2.0.1, then configure Downstream Mining and create Integrated Extract for Downstream Mining database. If Oracle source database is version 12.2.0.1 or later, then create Integrated Extract for the source database.
   b. Configure Integrated Extract XML file for each source database instance in a unique location.
   c. Wait for five minutes after creating the Integrated Extract, to ensure it is running successfully. In case the Integrated Extract fails, then check the logs in the **Reports** tab and fix the issue.
   d. After confirming that the Integrated Extract is running successfully, wait till DDL/DML statements run. Ensure that the Integrated Extract file contains XML data in it.
   e. Stop the 12.2 transaction log audit trail. Before Oracle AVDF 12.2 transaction log audit trail is stopped, for a brief duration both the GoldenGate Integrated Extract and Oracle AVDF 12.2 transaction log audit trail are running concurrently. Hence duplicate records are observed only for this brief duration. Safely ignore the duplicate records observed for this short duration.
   f. Ensure these steps run successfully for all the 12.2 transaction log audit trails.
3. If the current version of Oracle AVDF is prior to 12.2.0.9.0, then first upgrade to 12.2.0.9.0 and then upgrade to Oracle AVDF 20.
4. After upgrading to Oracle AVDF 20, perform these steps for each target database which has transaction log audit trail:
   a. Delete the old transaction log audit trail.
   b. Create a new transaction log audit trail.
   c. Make sure the trail location is the full path of the directory containing Integrated Extract XML files.

D.8 Create User and Grant Relevant Privileges

Learn how to create a user and grant the required privileges.

Create a new user depending on the type of the database:

- In case of standalone database, create a new user and grant relevant privileges to the user. This new user can fetch REDO log data from the Oracle Database using Oracle GoldenGate Integrated Extract.
- In case of multitenant database, create a new user in the CDB and grant relevant privileges to the user. This new CDB user can fetch REDO log data from individual PDBs in Oracle Database using Oracle GoldenGate Integrated Extract.

Follow this procedure for the standalone database:

1. Log in to the database as *sysdba*.
2. Execute the following command to create an example user *avggadmin*:

```
create user avggadmin identified by avggadmin;
```

3. Execute the following commands to grant privileges to the newly created user:

```
grant create session, resource, alter system to avggadmin;


grant unlimited tablespace to avggadmin;
```

4. Execute the following commands to grant GoldenGate *admin* privilege to the example user *avggadmin*:

```
begin
DBMS_GOLDENGATE_AUTH.GRANT_ADMIN_PRIVILEGE(
'avggadmin',
'*',
TRUE,
TRUE,
NULL,
NULL,
NULL,
'CURRENT');
end;
/
```

Follow this procedure for multitenant database:

1. Log in to `CDB$ROOT` as *sysdba*.
2. Execute the following command to create an example user *c##avggadmin*:

```
create user c##avggadmin identified by c##avggadmin container=all;
```

3. Execute the following commands to grant privileges to the newly created user:

```
grant create session, resource, alter system to c##avggadmin container=all;


grant unlimited tablespace to c##avggadmin container=all;
```

4. Execute the following commands to grant GoldenGate admin privilege to the example user *c##avggadmin*:

```
begin
DBMS_GOLDENGATE_AUTH.GRANT_ADMIN_PRIVILEGE(
'c##avggadmin',
'*',
TRUE,
TRUE,
NULL,
NULL,
NULL,
'ALL');
end;
/
```

> **See Also:**
>
> - Granting the Appropriate User Privileges
> - GRANT_ADMIN_PRIVILEGE Procedure

D.9 Configure Oracle GoldenGate Parameters for Oracle Database

Follow this procedure to configure Oracle GoldenGate parameters for Oracle Database.

1. For multitenant database, log in to `CDB$ROOT` as *sysdba*. For standalone database, log in as *sysdba*.
2. Execute the following command to enable GoldenGate replication:

```
alter system set enable_goldengate_replication=true scope=spfile;
```

3. Execute the following commands to enable Archive Log:

```
shutdown immediate


startup mount


alter database archivelog;


alter database open;


alter pluggable database all open  /*Applicable only for multitenant
database*/;


select name,log_mode from v$database;
```

4. Enabling *Forced Logging* is recommended by Oracle GoldenGate. Execute the following command to enable *Forced Logging*:

```
alter database force logging;
```

5. Execute the following commands to enable *Supplemental Logging*:

```
alter database add supplemental log data;


select force_logging, supplemental_log_data_min from v$database;
```

6. Change database compatibility only if the version is prior to 12.2.0.1.0. Execute the following command to see database compatibility:

```
show parameter compatible;
```

7. The database compatibility parameter needs to be changed only for the database, on which Integrated Extract will be configured. Execute the following command to set database compatibility to version 12.2.0.1.0 or higher. In case of normal integrated extract, execute the following command on the source database. In case of Downstream Mining configuration, execute the following command only on the Downstream Mining database and not on the source database.

```
alter system set compatible = '12.2.0.1.0' scope=spfile;
```

8. Set the appropriate `streams_pool_size` depending on the number of integrated extracts on the database. Refer to *Oracle GoldenGate Performance Best Practices* guide for complete information on sizing.
9. Execute the following command to check the current parameter values:

```
show parameter streams;
```

10. In case the `streams_pool_size` is not as per above sizing document, then set the relevant `streams_pool_size`, by executing the following commands:

```
alter system set streams_pool_size=1250M scope=spfile;


shutdown immediate;


startup;


alter pluggable database all open /*Applicable only for multitenant
database*/;


show parameter streams;
```

> **See Also:**
>
> - Enabling Minimum Database-level Supplemental Logging
> - Oracle GoldenGate Performance Best Practices

D.10 Create a New Credential in the GoldenGate Administration Server

Create a new credential for the target database in the Oracle GoldenGate Administration Server.

1. Log in to the Oracle GoldenGate Administration Server.
2. Click **Configuration** in the left navigation menu.
3. Click the plus button next to **Credentials** on the main page.
4. Enter the domain name in the **Credential Domain** field. For example, `inst1`.
5. Enter the alias in the **Credential Alias** field. For example, `avggadmin_inst1`.
6. In the **User ID** field, enter the user name in the following format: *<username>*`@`*<connect string>*. For example:

```
avggadmin@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST= foobar.example.com)
(PORT=1234))(CONNECT_DATA=(SERVICE_NAME= foobar.example.com)))
```

7. Enter the password.
8. Re-enter the password in the **Verify Password** field.
9. Click **Submit**.
10. After creating the credential, click the **Log in database** icon to verify that the newly created credential can connect to the target database.
11. Complete the **TRANDATA Information** section.

After you test the database connection, the **TRANDATA Information** section appears below the table of credentials. (In 19c, it's the **Transaction Information** section.)

The following steps are for 21c, as an example:

a. Click the plus button next to **TRANDATA Information**.

b. Select **Table** and add the table name in the **Table Name** field.

c. Edit the columns as needed.

d. Select **nowait** in the **Prepare CSN Mode** drop-down list.

e. Click **Submit**.

D.11 Create a New Integrated Extract in Oracle GoldenGate Administration Server

Follow this procedure to create new Integrated Extract in Oracle GoldenGate Administration Server for the target database.

1. Log in to the Oracle GoldenGate Administration Server.
2. Click the **Overview** tab in left navigation menu.
3. Click the plus button next to **Extract** on the main page.
4. In the **Add Extract** section and **Extract Type** sub section, select the **Integrated Extract** radio button.
5. Click **Next**.
6. In the **Extract Options** sub section, enter the **Process Name**.
7. Optionally, enter the **Description**.
8. Select **Unidirectional** in the **Intent** field.
9. Select the **Credential Domain** from the drop down.
10. Select the **Credential Alias** from the drop down.
11. Select **Now** in the **Begin** field.
12. Enter a two character trail name in the **Trail Name** field.
13. Enter the **Trail Subdirectory**.

> **Note:**
>
> Trail subdirectory can be full path of any directory. This directory must already exist on the file system.

14. Enter the **Trail Size** (in MB).

> **Note:**
>
> In case the record generation rate of GoldenGate is low (less than 50 records per second), then it is recommended to set the **Trail Size** to lower values. For example, 100MB.

15. Select the PDB container in the **Register to PDBs** field.
16. The maximum size of the XML file can be configured using the **Trail Size** field. After the XML file reaches this size, rotation happens and integrated extract starts writing into a new XML file.
17. The other fields can be left unchanged as they are optional.
18. Click **Next**.
19. In the **Parameter File** sub section, enter the below parameters:

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG <pdb_name>
DDL <ddl options to include or exclude schemas and tables>
TABLE <schema>.<table>;
```

Example parameter file:

```
extract int_ex_1
useridalias tkggadmin_inst1 domain inst1
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail subdirectory/aa
SOURCECATALOG cdb1_pdb1
DDL INCLUDE ALL
TABLE scott.*;
```

Note:

- The `SOURCECATALOG` parameter is applicable only for the multi tenant database and is not required for the standalone database.
- There is space between `XML` and `_AUDIT_VAULT` in the `OUTPUTFORMAT` parameter.
- The `OUTPUTFORMAT` parameter must be mentioned before the `exttrail` parameter in the parameter file. Else, the XML files are not generated.
- Ensure the `TABLE` command always ends with a semicolon (;).
- Ensure the sequence of all the parameters are in the exact order as mentioned above.
- The `DDL INCLUDE` command is used to specify the tables for which DDL changes need to be captured.
- The `TABLE` command is used to specify the tables for which DML changes need to be captured.
- Refer to the following sections in *Oracle® GoldenGate Reference for Oracle GoldenGate for Windows and UNIX* for more information about the `DDL`, `TABLE` and `TABLEEXCLUDE` commands.

20. After entering the values in the **Parameter File** field, click **Create and Run** button to start the integrated extract process.
21. In the **Extracts** panel, the newly created Integrated Extract is displayed. To view the status of the Integrated Extract follow these steps:
    a. Click **Actions** drop down next to the **Integrated Extract** icon.
    b. Select **Details**.
    c. Click **Report** tab to view the diagnostic messages. In case the extract process fails, then the relevant errors are displayed in the report.

> **See Also:**
>
> - DDL
> - TABLE | MAP
> - TABLEEXCLUDE

D.12 Periodic Backup of LogMiner Dictionary

Learn when to take backup of the LogMiner dictionary.

Oracle GoldenGate highly recommends periodic backup (preferably every day) of the LogMiner dictionary. It can be performed by extracting the LogMiner dictionary to the redo log files. Database jobs can be created to perform periodic backup.

> **See Also:**
>
> Extracting a LogMiner Dictionary to the Redo Log Files

D.13 Sample Oracle GoldenGate Integrated Extract Parameter Files

Use these Oracle GoldenGate Integrated Extract parameter files as samples.

Audit DML and DDL in the schema excluding some tables

The following parameter file configures Integrated Extract to capture the following:

- DDL operations on all objects, except the objects in `accounts` schema
- DML operations on all tables in `scott` schema, except the `emp` table in the `scott` schema

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
DDL INCLUDE ALL, EXCLUDE OBJNAME accounts.*
```

```
TABLE scott.*;
TABLEEXCLUDE scott.emp
```

Audit all DDL and DML in a schema

The following parameter file configures Integrated Extract to capture the following:

- DDL operations on all objects in the `scott` schema
- DML operations on all tables in the `scott` schema

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
DDL INCLUDE OBJNAME scott.*
TABLE scott.*;
```

Audit only DDL in a schema

The following parameter file configures Integrated Extract to capture DDL operations on all objects in the `scott` schema.

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
DDL INCLUDE OBJNAME scott.*
```

Audit only DML in a schema

The following parameter file configures Integrated Extract to capture DML operations on all tables in the `scott` schema.

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
TABLE scott.*;
```

Audit all DDL in all schema

The following parameter file configures Integrated Extract to capture DDL operations on all objects.

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
```

```
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
DDL INCLUDE ALL
```

Audit DML for a table and set the columns to be used as key columns

The following parameter file configures Integrated Extract to do the following:

- Capture DML operations on the `emp` table in the `scott` schema
- Set `empno` and `ename` as key columns

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
TABLE scott.emp, KEYCOLS (empno, ename);
```

Audit DML for a table with `GETBEFORECOLS` and `KEYCOLS` option

The following parameter file configures Integrated Extract to do the following:

- Capture DML operations on the `emp` table in the `scott` schema
- Set `empno` and `ename` as key columns

The following sample parameter file has GETBEFORECOLS options. The Oracle AVDF is supporting display of key columns from AVDF 20.10.0.0.0. To show key columns in the report for update and delete operations, key column should appear in the before image of audit file generated by the Oracle GoldenGate. If key columns are absent in the before images then, user can use GETBEFORECOLS option.

```
extract <extract_name>
useridalias <credential_userid_alias> domain <credential_domain>
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <sub_directory>/<trail_name>
SOURCECATALOG cdb1_pdb1
TABLE scott.emp, KEYCOLS (empno, ename), GETBEFORECOLS (ON UPDATE ALL, ON
DELETE ALL);
```

Related Topics

- Adding Audit Trails with Agent-Based Collection
  To begin collecting audit data with the Audit Vault Agent, configure an audit trail for each target that's registered on the Audit Vault Server and then start the audit trail collection.

D.14 Audit Trail Creation in Audit Vault Console

Learn how to create a mandatory target attribute before creating audit trail.

Ensure the mandatory target attribute `AV.COLLECTOR.TIMEZONEOFFSET` is set on the Oracle Database target in Audit Vault Server console before audit trail creation. This attribute must be set to timezone offset of Oracle Database. For example, `+03:00` for positive offset, `-03:00` for negative offset.

Create audit trail by specifying the following details or guidelines:

- Trail Type: TRANSACTION LOG
- Trail Location: Full path of directory containing integrated extract XML files
- Agent should be running on the host machine which has access to the trail location
- Agent user should have read permission on the trail location

D.15 Audit Trail Cleanup

Learn how to delete the files that are read by Audit Vault Agent.

Oracle Golden Gate Collector writes the checkpoint information into the Audit Trail Cleanup (ATC) file. This file is present in `<Agent_Home>/av/atc` directory. The ATC file contains information of the target type, target name, trail type, trail directory, and the checkpoint timestamp. The ATC file has extension `.atc`. All the records with event timestamp older than the checkpoint timestamp are read by Audit Vault Agent and written into the `event_log` table in Audit Vault Server.

> **Note:**
>
> The timestamp in ATC file is in UTC (Coordinated Universal Time) time zone.

Here is an example ATC file:

```
securedTargetType=Oracle Database
SecuredTargetName=secured_target_oracle_one
TrailType=TRANSACTION LOG
TrailName=/foo/bar/trail_files
2020-06-30 07:11:46.0
```

For Oracle AVDF 20.3 and Earlier

To delete the files that are read by the Audit Vault Agent, create a script which deletes the files. These are the files where the last modified timestamp is older than the checkpoint timestamp present in ATC file. This script can be scheduled to run periodically.

For Oracle AVDF 20.4 and Later

To delete the files that are read by the Audit Vault Agent use the Oracle GoldenGate Extract Cleanup utility. This is available starting Oracle AVDF 20.4.

D.16 Configure GoldenGate Downstream Mining

Learn how to configure GoldenGate downstream mining.

Oracle GoldenGate Integrated Extract process is supported only for Oracle Database versions 12.2.0.1 and later. In this case Oracle GoldenGate Integrated Extract is configured on the source database. For capturing transaction log data from Oracle Database versions prior to 12.2.0.1, downstream mining is used. In this case there are 2 databases, the source database and the Downstream Mining database. The source database (Oracle Database versions prior to 12.2.0.1) is configured to send the online REDO logs to a Downstream database (Oracle Database version 12.2.0.1 or later). Integrated Extract is then configured on the Downstream database to generate XML files in *_AUDIT_VAULT* format.

Prerequisite

Execute the steps in Create User and Grant Relevant Privileges and Configure Oracle GoldenGate Parameters for Oracle Database on both the source database and the Downstream Mining database.

Configuring the Password File

1. Execute the follow command on the source database to see database compatibility:

   ```
   show parameter compatible;
   ```

2. If the version of the source database is 12.1.0.2.0, then execute below command:

   ```
   alter system set compatible = '12.1.0.2.0' scope=spfile;


   shutdown immediate


   startup
   ```

3. Execute the following command and check if the compatibility has changed to 12.1.0.2.0:

   ```
   show parameter compatible;
   ```

4. Execute the following query to find the *global_name* on both the source database and the Downstream Mining database:

   ```
   select * from global_name;
   ```

5. Ensure the source database and the Downstream Mining database do not have the same *global_name*.
6. If a source database has a remote login password file, copy it to the appropriate directory of the mining database system. The password file must be the same as the source database and the mining database. If the source database and the Downstream Mining database do not have the same password file, then execute the following commands in the source database and then copy over the source password file to the Downstream Mining database:

   ```
   alter system set remote_login_passwordfile = 'shared' scope = spfile;


   shutdown immediate


   startup
   ```

7. In the source database, the password file is `$ORACLE_HOME/dbs/orapw<$ORACLE_SID>`.

   The example source password file is `/foo/bar/orapwsource`.

8. Execute the following command on the Downstream Mining database to find the downstream password file:

   ```
   select file_name from v$passwordfile_info;
   ```

   The example downstream password file is `/foo/bar/orapwdownstream`.

9. Execute the following command to take backup of the existing downstream password file:

   ```
   cp /foo/bar/orapwdownstream /foo/bar/orapwdownstream_orig
   ```

10. Execute the following command to copy the source password file to downstream password file location:

    ```
    cp /foo/bar/orapwsource /foo/bar/orapwdownstream
    ```

Configuring the Source Database

In this example, the database unique name for source database is `source_db_unique_name` and for the Downstream Mining database is `downstream_db_unique_name`.

Execute the following command to find the database unique name:

```
select db_unique_name from v$database;
```

Execute the following commands on the source database, to configure the source database to transmit redo data to the Downstream Mining database. While setting the `LOG_ARCHIVE_DEST_2` parameter, the connection details of the Downstream Mining database needs to be provided.

```
ALTER SYSTEM SET
LOG_ARCHIVE_CONFIG='DG_CONFIG=(source_db_unique_name,downstream_db_unique_name
)';


ALTER SYSTEM SET
LOG_ARCHIVE_DEST_2='SERVICE="(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=foo.bar.com)(PORT=1234))(CONNECT_DATA=(SERVICE_NAME=foo.bar.com)))"
ASYNC OPTIONAL NOREGISTER VALID_FOR=(ONLINE_LOGFILE,PRIMARY_ROLE)
DB_UNIQUE_NAME=downstream_db_unique_name';


ALTER SYSTEM SET LOG_ARCHIVE_DEST_STATE_2=ENABLE;
```

Configuring the Downstream Mining Database

1. Archiving must be enabled in the Downstream Mining database to run Integrated Extract in real time integrated capture mode. Execute the following commands on the Downstream Mining database to archive local redo log files:

   ```
   ALTER SYSTEM SET LOG_ARCHIVE_DEST_1='LOCATION=/foo/bar/arc_dest/local
   valid_for=(ONLINE_LOGFILE,PRIMARY_ROLE)';


   ALTER SYSTEM SET LOG_ARCHIVE_DEST_STATE_1=ENABLE;
   ```

2. Downstream Mining database must be configured to archive the standby redo logs that receive redo data from the online redo logs of the source database. The foreign archived logs should not be archived in the recovery area of the Downstream Mining database. Execute the following commands on the Downstream Mining database to archive standby redo logs locally:

```
ALTER SYSTEM SET
LOG_ARCHIVE_CONFIG='DG_CONFIG=(source_db_unique_name,downstream_db_unique_n
ame)';


ALTER SYSTEM SET LOG_ARCHIVE_DEST_2='LOCATION=/foo/bar/arc_dest/
standbyredo VALID_FOR=(STANDBY_LOGFILE,PRIMARY_ROLE)';


ALTER SYSTEM SET LOG_ARCHIVE_DEST_STATE_2=ENABLE ;
```

3. Execute the following command on the source database and make a note of the results:

```
select group#, thread#, bytes from v$log;
```

4. Add the standby log file groups to the mining database. The standby log file size must be at least the size of the source log file. The number of standby log file groups must be at least one more than the number of source online log file groups. This applies to each instance (thread) in case of Oracle RAC installation. If you have `n` threads in the source database, each having `m` redo log groups, then you should configure `n*(m+1)` redo log groups in the Downstream Mining database.

   For example, let us assume the following is the result of the query `select group#, thread#, bytes from v$log;`:

GROUP#	THREAD#	BYTES
1	1	26214400
2	1	26214400

   Number of threads (n) is 1.

   Number of groups per thread (m) is 2.

   Hence `n*(m+1) = 3` redo logs groups are required in the Downstream Mining database, where the size of each log group should be at least 26214400 bytes.

5. For this example, execute the following query on the Downstream Mining database:

```
ALTER DATABASE ADD STANDBY LOGFILE GROUP 3
('/foo/bar/arc_dest/standbyloggroups/slog3a.rdo', '/foo/bar/arc_dest/
standbyloggroups/slog3b.rdo') SIZE 500M;

ALTER DATABASE ADD STANDBY LOGFILE GROUP 4
('/foo/bar/arc_dest/standbyloggroups/slog4a.rdo', '/foo/bar/arc_dest/
standbyloggroups/slog4b.rdo') SIZE 500M;

ALTER DATABASE ADD STANDBY LOGFILE GROUP 5
('/foo/bar/arc_dest/standbyloggroups/slog5a.rdo', '/foo/bar/arc_dest/
standbyloggroups/slog5b.rdo') SIZE 500M;
```

```
SELECT * FROM V$STANDBY_LOG;
```

Registering Integrated Extract

1. Create credentials for both the source database and the Downstream Mining database on Oracle GoldenGate administration server by following the steps in Create a New Credential in the GoldenGate Administration Server.
2. Launch the *adminclient* command line interface:

   ```
   $GG_HOME/bin/adminclient
   ```

3. Execute the command to connect to the GoldenGate Service Manager. If SSL is configured, then execute the command:

   ```
   connect https://<hostname>:<port> as <username> password <password> !
   ```

   If SSL is not configured, then execute the command:

   ```
   connect http://<hostname>:<port> as <username> password <password> !
   ```

   Example command if SSL is configured:

   ```
   connect https://localhost:1234 as ggadminuser password ggadminpassword !
   ```

   Example command if SSL is not configured:

   ```
   connect https://localhost:1234 as ggadminuser password ggadminpassword !
   ```

4. Execute the following command to log in to the source database in *adminclient*:

   ```
   dblogin useridalias <source db user id> domain <source db domain>
   ```

   For example:

   ```
   dblogin useridalias avggadmin_remotesourceinst1 domain remotesourceinst1
   ```

5. Execute the following command to log in to the Downstream Mining database in *adminclient*:

   ```
   miningdblogin useridalias <downstream db user id> domain <downstream db
   domain>
   ```

   For example:

   ```
   miningdblogin useridalias avggadmin_remotedowninst1 domain remotedowninst1
   ```

6. Execute the following commands to add and register the Integratd Extract. Before executing these steps, manually create the subdirectory, where the Integrated Extract XML files need to be stored.

```
ADD EXTRACT <extract name> INTEGRATED TRANLOG BEGIN NOW


REGISTER EXTRACT <extract name> DATABASE


ADD EXTTRAIL <subdirectory>/<trail name>, EXTRACT <extract name>
```

After executing this command, you may see the message `OGG-12029 The file with name '<extract name>.prm' does not exist.` Ignore this message.

For example:

```
ADD EXTRACT ext1 INTEGRATED TRANLOG BEGIN NOW
REGISTER EXTRACT ext1 DATABASE
ADD EXTTRAIL e1/e1, EXTRACT ext1
```

7. Log in to the Oracle GoldenGate administration server.
8. In the **Extracts** panel, the newly created Integrated Extract is displayed. To update the parameter file of the Integrated Extract follow these steps:
   a. Click **Actions** drop down next to the Integrated Extract icon.
   b. Select **Details**.
   c. In the **Parameters** tab, enter the below parameters:

```
extract <extract name>
useridalias <source db user id> domain <source db domain>
TRANLOGOPTIONS MININGUSERALIAS <downstream db user id> domain
<downstream db domain>
TRANLOGOPTIONS INTEGRATEDPARAMS (downstream_real_time_mine Y)
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail <subdirectory>/<trail name>
DDL INCLUDE ALL
TABLE <schema>.<table>;
```

For example:

```
extract ext1
useridalias avggadmin_remotesourceinst1 domain remotesourceinst1
TRANLOGOPTIONS MININGUSERALIAS avggadmin_remotedowninst1 domain
remotedowninst1
TRANLOGOPTIONS INTEGRATEDPARAMS (downstream_real_time_mine Y)
OUTPUTFORMAT XML _AUDIT_VAULT
exttrail e1/e1
DDL INCLUDE ALL
TABLE scott.*;
```

9. After updating the parameters, click the **Apply** button.
10. Click **Actions** drop down next to the Integrated Extract icon.
11. Click **Start** button to start the Integrated Extract. Wait for 5 minutes for the Integrated Extract to start successfully and create the background log mining process. Log Mining process runs in the background and is not visible to the user.
12. Execute the following commands on the source database to switch the log files on the source database:

```
select * from v$log;


alter system switch logfile;


select * from v$log;
```

13. Wait for 5 minutes after performing the log switch. The Integrated Extract needs few minutes to start creating the XML files.

Checking the status of Downstream Mining

Execute the following commands on both the source database and the Downstream Mining database:

```
select * from V$archive_dest_status;


select * from V$archive_dest;
```

In the row having `dest_name` column with values `LOG_ARCHIVE_DEST_1` and `LOG_ARCHIVE_DEST_2`, ensure the status column has a value `VALID` and the `gap_status` column has a value `NO GAP` or `null`.

If the status column has a value `ERROR`, then the error column shows the relevant error message.

Checking the status of Integrated Extract

1. Log in to the Oracle GoldenGate administration server.
2. View the **Extracts** panel. The Integrated Extract is displayed.
3. Check the status of the Integrated Extract. Click **Actions** drop down next to the Integrated Extract icon.
4. Select **Details**.
5. Click **Report** tab to view the diagnostic messages. In case the extract process fails, then the relevant errors are displayed in the report.

> **See Also:**
>
> Understand the downstream mining process available in Configuring a Downstream Mining Database and Example Downstream Mining Configuration.

E

Transaction Log Audit Data Collection for Microsoft SQL Server

This chapter explains how to configure Oracle GoldenGate for Microsoft SQL Server databases (Oracle AVDF 20.9 and later) and how to create transaction log audit trails in the Audit Vault Server console.

Microsoft SQL Server 2012 was deprecated in Oracle AVDF 20.12, and it will be desupported in one of the future releases.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

E.1 Introduction to the Transaction Log Audit Trail Using Oracle GoldenGate for Microsoft SQL Server

Change Data Capture (CDC) in Microsoft SQL Server records the insert, update, and delete operations that are performed on the data in the tables of the SQL Server.

It captures the data with the help of the SQL Server agent. The first five columns of the CDC table contain the metadata. These columns provide additional information related to the changes that are captured. For each insert, delete, and update operation that is applied to the table, a single row appears in the table. The data columns of the row that results from an insert operation contain the column values after the insert. The data columns of the row that results from a delete operation have the column values before the delete. An update operation requires a one-row entry to identify the column values before the update and a second-row entry to specify the column values after the update.

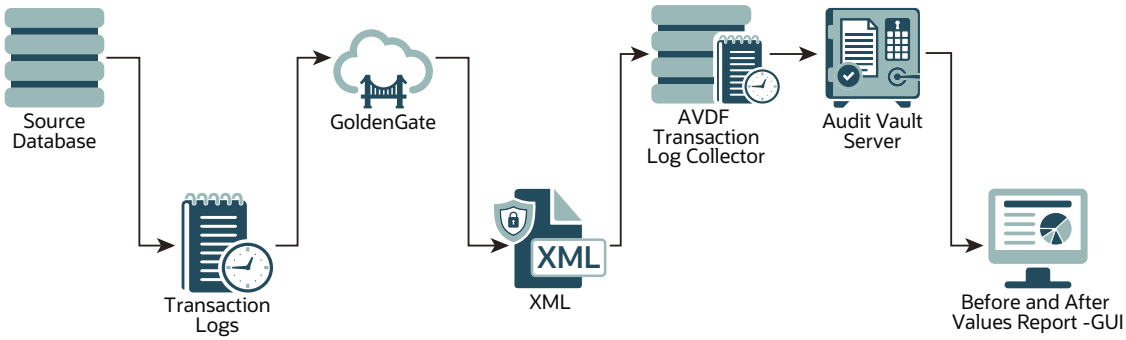
The Transaction Log collector takes advantage of Oracle GoldenGate's Extract process (CDC Capture) to pull CDC table data into XML files.

> **Note:**
>
> This Extract process captures only data manipulation language (DML) operations that are performed on the configured objects.

Oracle AVDF's Transaction Log collector for SQL Server collects transaction log records from generated XML files. These logs are forwarded to the Audit Vault Server to show the before and after values that are changed in the **Data Modification Before-After Values** report. The DML changes are available in the **Data Modification Before-After Values** report.

Starting with Oracle AVDF 20.10, the **Data Modification Before-After Values** report has additional information about key columns. GoldenGate, by default, uses the primary key columns of the table as key columns. If no primary keys are defined for the table, or if you want to use some other columns as key columns, then GoldenGate provides an option to specify key columns in the parameter file.

Figure E-1 Transaction Log Collection Process



> **Note:**
>
> Oracle GoldenGate for Microsoft SQL Server does not capture certain details, such as the program name, database username, OS username, OS terminal, client host name, client ID, process ID, and proxy session ID for transactions committed in the database. As a result, this limitation will cause the Oracle AVDF's Data Modification Before-After Values report to display empty values for these fields.

E.2 Sizing Guidelines

Follow these sizing guidelines to configuring Oracle GoldenGate for Microsoft SQL Server.

Prerequisites

Follow the system and sizing requirements in What is Required? in the Oracle GoldenGate documentation.

General Sizing Guidelines

- For memory and CPU, start with 32 GB of memory and 2 CPUs per Extract, because it's a multithreaded process and uses a large amount of memory when processing large transactions. Depending on the transaction volume and pattern, scale up the resources appropriately following the guidelines in the Oracle GoldenGate documentation.
- For disk space, start with 2 TB, and vary it based on the volume of data that the Extract captures from the source databases. The Extract uses storage for trail files and temporary disk space for cache files if there's a big transaction to buffer for processing.

Temporary disk space requirements due to large transactions may fill up the cache and spill over to the transaction-cached data or temporary files. Configure an archive policy and define the retention period of the files so they can be recycled accordingly.

Maintain enough physical memory to handle large transactions. According to the guidelines, have at least 32 GB of memory available for the Extract to use. For a more accurate estimation, collect the statistics from the database server history run and check for the size of the biggest transaction. Oracle GoldenGate provides the `send <extract> cachemgr, cachestats` command that displays the statistics of the transaction, which is helpful to determine the baseline for estimation.

In general, the sizing, storage, and memory for the Oracle GoldenGate Extract process is highly dependent on the transaction volume and transaction pattern. Collect these statistics

from every single database server to estimate, because there's no standard value. The number of databases that can be supported by a single GoldenGate instance or Extract process depends on the system resources that support multiple Extracts. Configure one Extract for every database.

See Also:

- Other Disk Space Considerations
- Temporary Disk Requirements

E.3 Restricted Use License for Oracle GoldenGate

A restricted-use license for Oracle GoldenGate is included with Oracle AVDF release 20.

This license permits you to install Oracle GoldenGate and use the Extract process to capture transactional changes in database systems that are monitored by Oracle AVDF. The extracted data from Oracle GoldenGate is consumed only by Oracle AVDF. Deploy Oracle GoldenGate Classic Architecture or Microservices Architecture on a separate server other than the server on which the Oracle AVDF appliance is deployed. Then configure the Oracle GoldenGate Extract feature. Oracle AVDF 20.9 supports Oracle GoldenGate Classic Architecture 19.1.0.0.200414 for Microsoft SQL Server versions 2012, 2014, 2016, 2017, and 2019 and Microservices Architecture version 21.4.0.0.0 for Microsoft SQL Server versions 2017 and 2019 for Oracle AVDF 20.10.

E.4 Installing Oracle GoldenGate for Microsoft SQL Server Databases

Follow these instructions to install Oracle GoldenGate for Microsoft SQL Server.

Deploy Oracle GoldenGate on a separate server other than the server on which the Oracle AVDF appliance is deployed. Then configure the Oracle GoldenGate Integrated Extract feature.

Oracle AVDF 20.9 and Earlier

Install Oracle GoldenGate 19.1.0.0.0 classic architecture from Oracle Software Delivery Cloud.

Follow the instructions for Installing GoldenGate for Heterogeneous Databases in the Oracle GoldenGate 19c documentation. After installing Oracle GoldenGate classic architecture, apply patch 31050939 from My Oracle Support.

Oracle AVDF 20.10 and Later

Install Oracle GoldenGate 21.4.0.0.0 Microservices architecture from Oracle GoldenGate Downloads.

Follow the instructions for Installing Oracle GoldenGate in the Oracle GoldenGate Microservices documentation for Oracle GoldenGate 21c.

E.5 Capturing Transaction Log Data from Microsoft SQL Server 2012 (Through Version 2019)

You capture transaction log data from Microsoft SQL Server by using Oracle GoldenGate's change data capture (CDC) Capture (Extract) process.

E.5.1 Capturing Transaction Log Data from Microsoft SQL Server (Classic Architecture)

Use this process to configure Microsoft SQL Server and the CDC Extract process for the Oracle GoldenGate Classic Architecture.

1. Creating Users and Privileges
2. Creating the Manager Process
3. Preparing the System for Oracle GoldenGate
4. Preparing the System for the CDC Capture
5. Creating the GoldenGate CDC Extract

The Oracle GoldenGate CDC Extract process in version 19.1.0.0.200414+ supports capturing transaction log data from Microsoft SQL Server versions 2012 through 2019. For SQL Server 2014, 2016, and 2017, Microsoft has identified and fixed several important issues that directly affect the SQL Server CDC feature. This situation impacts the ability of Oracle GoldenGate to capture data correctly. The current known issues that require Microsoft patches include KB3030352, KB3166120, and KB4073684. If you're using SQL Server 2014, 2016, or 2017 as a source database, Oracle highly recommends that you apply the latest service pack or cumulative update for your version of SQL Server. See SQL Server Supported Versions in the Oracle GoldenGate documentation for information.

E.5.1.1 Creating Users and Privileges

The user that is used for the Oracle GoldenGate Extract process and the user that is used to enable supplemental login need different sets of privileges.

See the following topics in the Oracle GoldenGate documentation for instructions:

- For the Extract user for Microsoft SQL Server, see *only the Extract user section* in Extract and Replicat Users for SQL Server.
- For the user that enables supplemental login, see User that Enables Supplemental Logging and Other Features.

E.5.1.2 Creating the Manager Process

The Manager process can run as a Microsoft Windows service, or it can run interactively as the current user.

The Manager process requires the following:

- Full control permissions over the files and folders within the Oracle GoldenGate directories.
- Full control permissions over the trail files, if they're stored in a location other than the Oracle GoldenGate directory.

- Membership in the server's local administrators group (on all nodes in a cluster).
- If you're running the Manager process as a Windows service with an Extract that is connected to a remote database using Windows Authentication, the process attempts to log in to the database with the account that the Manager process is running under. Ensure that the Manager's service account has the correct access to the remote SQL Server instance.

The programs that capture data for the Extract run under the Manager account and inherit the Manager's operating system privileges.

Create a file named `GLOBALS.txt` in the root folder of Oracle GoldenGate.

Add a new schema in the database to be used by Oracle GoldenGate objects that may get created in the database. Open the `GLOBALS.txt` file and write `GGSCHEMA <schema_name>`. Use the `GGSCHEMA` parameter to specify the name of the schema that contains the database objects that are owned by Oracle GoldenGate, such as those that support data definition language (DDL) replication for trigger-based replication, those that are a part of the heartbeat table implementation, and those that are part of the SQL Server CDC Capture and Cleanup implementation. After creating the `GLOBALS` file, remove the `.txt` extension. The schema name mentioned under `GGSCHEMA` is treated as a system object, and table names with wildcards under `GGSCHEMA` are excluded from the Extract. If you need to capture in `GGSCHEMA`, don't use wildcards and make sure that you explicitly map the respective table names.

Open the command prompt in the location of the GoldenGate folder and run `ggsci.exe` in the command prompt, or you can directly run this as an administrator.

After running `ggsci.exe`, the GoldenGate command prompt appears.

Run the following command at the GGSCI command prompt:

```
create subdirs
```

To create a Manager process, use the following steps:

1. Enter the following command in GGSCI:

   ```
   edit params mgr
   ```

   Notepad or a similar editor opens the parameter file.

2. In the parameter file, enter the port number for the Manager process. It can be any port number except the well-known port numbers. Use the following format: `port <port_number>`

   For example: `port 3456`

3. Enter the following command:

   ```
   start mgr
   ```

   This starts the Manager process and *only* enables communication between the Manager process and the local Oracle GoldenGate instance. For more information about the parameters and configuring other types of network communications for the Manager, see Configuring Manager and Network Communications in the Oracle GoldenGate documentation.

To see if the manager process is running, enter the following command:

```
info all
```

(Optional) To add a Manager process as a Windows service, run the following commands. You'll receive a warning or error message if the Manager process is already running as a Windows service. In that case, you don't need to add the Manager process as a Windows service.

```
stop mgr


shell install addservice


start mgr
```

E.5.1.3 Preparing the System for Oracle GoldenGate

The Extract connects to a source SQL Server database through an Open Database Connectivity (ODBC) connection.

To create this connection, set up a data source name (DSN) through the Data Sources (ODBC) control panel. For instructions, see Configuring an Extract Database Connection in the Oracle GoldenGate documentation.

E.5.1.4 Preparing the System for the CDC Capture

To create a CDC Capture process, you enable supplemental logging and create an Oracle GoldenGate CDC cleanup job.

See the following instructions:

- Enabling CDC Supplemental Logging
- Purging the CDC Staging Data

E.5.1.5 Creating the GoldenGate CDC Extract

This section discusses the steps to initiate the CDC Extract process.

Before creating a parameter file for CDC Extract, make sure that you're already logged in to the database through GGSCI, supplemental logging and Oracle GoldenGate's CDC Cleanup job are enabled, and the Manager process is running. The following file is a sample parameter file for the CDC Extract process. For more detailed information on the fields in the parameter file, see Valid and Invalid Parameters for CDC Capture in the Oracle GoldenGate documentation.

To create and save a new Extract parameter file, enter the following command in GGSCI:

```
edit params <extract_name>
```

For example:

```
edit params exta
```

Notepad or a similar editor opens for you to add the required parameters. The following example parameter file has the minimum required parameters:

```
EXTRACT <extract_name>
SOURCEDB <dsn> USERID <username> PASSWORD <password>
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL .\dirdat\{Any combination of two alphabets indicating prefix of
trail file e.g. ab, bc, ea, sn.....etc}
TABLE owner.table_name;
```

> **Note:**
>
> The `OUTPUTFORMAT` must appear before the `EXTTRAIL`.

The following example parameter file is for a single table. Here the `dirdat` folder will contain the trail files that Oracle GoldenGate generates.

```
EXTRACT exta
SOURCEDB GGDB USERID sa PASSWORD passwd
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL .\dirdat\ea
TABLE dbo.employee;
```

> **Note:**
>
> The following examples and commands continue to use `exta` as the Extract name.

To add the Extract process, run the following commands in GGSCI:

```
add extract exta, tranlog, begin now


add exttrail .\dirdat\ea, extract exta
```

Make sure that the Manager process is already running, and then start the Extract with the following commands in GGSCI:

```
start extract exta


info all
```

This starts the Extract process. From this point onward, every DML operation on the tables that are monitored by the Extract will be captured and entered in the trail file in the `dirdat` folder. To learn more about the Extract process, the naming conventions, creating trail, and so on, see Configuring Online Change Synchronization.

To stop the Extract process, enter the following command:

```
stop exta
```

E.5.2 Capturing Transaction Log Data from Microsoft SQL Server (Microservices Architecture)

Use this process to configure Microsoft SQL Server and the CDC Extract process for the Oracle GoldenGate Microservices Architecture.

1. Creating Users and Privileges
2. Preparing the System for Oracle GoldenGate
3. Configuring the Database for Oracle GoldenGate
4. Preparing the System for the CDC Capture
5. Creating the GoldenGate CDC Extract

E.5.2.1 Creating Users and Privileges

The user that is used for the Oracle GoldenGate Extract process and the user that is used to enable supplemental login need different sets of privileges.

See the following topics in the Oracle GoldenGate documentation for instructions:

- For the Extract user for Microsoft SQL Server, see *only the Extract user section* in Extract and Replicat Users for SQL Server.
- For the user that enables supplemental login, see User that Enables Supplemental Logging and Other Features.

E.5.2.2 Preparing the System for Oracle GoldenGate

The Extract connects to a source SQL Server database through an Open Database Connectivity (ODBC) connection.

To create this connection, set up a data source name (DSN) through the Data Sources (ODBC) control panel. For instructions, see Configuring an Extract Database Connection in the Oracle GoldenGate documentation.

E.5.2.3 Configuring the Database for Oracle GoldenGate

Configure the database credentials and TRANDATA information for Oracle GoldenGate.

1. Open the **Administration Service** page in the Oracle GoldenGate Service Manager console.
2. In the navigation menu for the Administration Service, click **Configuration**.
3. Click the **Database** tab.
4. Click the plus button next to **Credentials** to add the database credentials.
5. Enter the domain name in the **Credential Domain** field.
6. Enter the alias in the **Credential Alias** field.
7. Enter the data source name (DSN) (which you created in Preparing the System for Oracle GoldenGate) in the **DSN** field.

8. Enter the user ID and password.
9. Click **Submit**.
10. Click the **Connect to database** icon for the new credential to ensure that the newly created credential can connect to the target database.

    After you test the database connection, the **TRANDATA Information** section appears below the table of credentials.
11. Click the plus button next to **TRANDATA Information**.
12. Select **Table** and add the table name in the **Table Name** field.
13. Edit the columns as needed.
14. Select **nowait** in the **Prepare CSN Mode** drop-down list.
15. Click **Submit**.

E.5.2.4 Preparing the System for the CDC Capture

To create a CDC Capture process, you enable supplemental logging and create an Oracle GoldenGate CDC cleanup job.

See the following instructions:

- Enabling CDC Supplemental Logging
- Purging the CDC Staging Data

E.5.2.5 Creating the GoldenGate CDC Extract

Use these steps to create and run the CDC capture for Microsoft SQL Server.

1. Open the **Administration Service** page in the Oracle GoldenGate Service Manager console.
2. Click the plus button next to **Extracts**.
3. Select **Change Data Capture Extract** for the extract type and click **Next**.
4. Enter the process name in the **Process Name** field.
5. Select **Unidirectional** in the **Intent** field.
6. In the **Credential Alias** drop-down list, select the credential alias that you created in Configuring the Database for Oracle GoldenGate.
7. In the **Begin** drop-down list, select **Now**.
8. Enter a two-character **Trail Name**.
9. If you need to customize the trail subdirectory, enter the full path of the directory in the **Trail Subdirectory** field.

    This can be any directory, and it must already exist in the file system.
10. Enter the trail size in MB in the **Trail Size** field.

    If the record generation rate of GoldenGate is low (less than 50 records per second), then Oracle recommends that you set the trail size to a lower value, such as 100 MB.

> **Note:**
>
> You can leave all other fields unchanged because they're optional.

11. Click **Next**.
12. In the **Parameter File** section, enter the following parameters:

```
EXTRACT <extract_name>
SOURCEDB <DSN_name> USERIDALIAS <user_alias>, DOMAIN <domain_name>
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL <subdirectory>/<trail_name>
TABLE <schema>.<trail_name>;
```

For example:

```
EXTRACT exta
SOURCEDB odbc1 USERIDALIAS sql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL dirdat/ea
TABLE dbo.employee;
```

Note the following parameter guidelines:

- Include a space between `XML` and `_AUDIT_VAULT` in the `OUTPUTFORMAT` parameter.
- Include the `OUTPUTFORMAT` parameter before the `EXTTRAIL` parameter in the parameter file. Otherwise, the XML files are not generated.
- Ensure that the `TABLE` command always ends with a semicolon (`;`).
- Ensure that the sequence of all the parameters is in the exact same order as the preceding example.
- For the `TABLE` command, specify the tables for which DML changes need to be captured.
- For more information about Oracle GoldenGate parameters, see Oracle GoldenGate Parameters.

13. Click **Create and Run** to start the CDC Extract process.

    The newly created CDC Extract appears in the **Extracts** section on the **Administration Service** page.
14. To view the status of the CDC Extract:
    a. Click the **Actions** button for the extract.
    b. Select **Details**.
    c. Click **Report** tab to view the diagnostic messages.

       If the extract process fails, this report displays the relevant errors.

E.5.2.6 Sample Oracle GoldenGate CDC Extract Parameter Files

Use these Oracle GoldenGate CDC Extract parameter files as samples.

Audit DML for a table and set the columns to be used as key columns

The following parameter file configures CDC Extract to do the following:

- Capture DML operations on the `emp` table in the `dbo` schema.
- Set `empno` and `ename` as key columns.

```
EXTRACT <extract name>
SOURCEDB <Database Name@Database Server:port> USERIDALIAS <useralias>, DOMAIN
<Domain name>
OUTFORMAT XML _AUDIT_VAULT
EXTTRAIL <subdirectory>/<trail name>
TABLE dbo.emp, KEYCOLS (empno, ename);
```

Audit DML in table

The following parameter file audits DML operations on the required tables:

- The parameter file provided is for a single table.
- Additional table names can be added by the user.

```
EXTRACT <extract_name>
SOURCEDB <Database Name@Database Server:port> USERIDALIAS <useralias>, DOMAIN
<Domain name>
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL <subdirectory> {Any combination of two alphabets indicating prefix
of trail file e.g. ab, bc, ea, sn.....etc}
TABLE owner.table_name;
```

Example: The following parameter file audits DML operations on the `dbo.employee` table. The audit data will be stored in the `\dirdat\ea` location:

```
EXTRACT exta
SOURCEDB HR@10.245.102.35:3306 USERIDALIAS mysql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL \dirdat\ea
TABLE dbo.employee;
```

- `exta` is the name of the CDC Extract.
- `HR` is the name of the database.
- `10.245.102.35` is the IP of the host on which database is installed.
- `3306` is the port number of the MySQL database.
- `mysql` is the `USERIDALIAS`.
- `OracleGoldenGate` is the DOMAIN.
- In `dbo.employee`, `dbo` is the schema name that owns the `employee` table.

Audit DML with GETBEFORECOLS option

The following parameter file configures the Extract process to capture DML operations on a specific table with the GETBEFORECOLS option enabled. This option ensures that key columns appear in the before image of the audit file generated by Oracle GoldenGate, which is essential for displaying key columns in reports for update and delete operations.

```
EXTRACT exta
SOURCEDB HR@10.245.102.35:3306 USERIDALIAS mysql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL ea
TABLE dbo.employee, GETBEFORECOLS(ON UPDATE ALL, ON DELETE ALL);
```

Use GETBEFORECOLS to specify the columns to be captured and written to the before image of the trail. In the above example, the ALL keyword indicated that all columns should be included in the before image for update and delete operations.

Audit DML with KEYCOLS option

The following parameter file configures the Extract process to capture DML operations on a specific table using the KEYCOLS option. This option is used to define a substitute primary key when a primary key or an appropriate unique index is not available for the table.

```
EXTRACT exta
SOURCEDB HR@10.245.102.35:3306 USERIDALIAS mysql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL ea
TABLE dbo.emp3, KEYCOLS(id,name), GETBEFORECOLS(ON DELETE ALL);
```

The above parameter file audits DML operations on the dbo.emp3 table. The KEYCOLS option is used to treat the id and name columns together as a unique primary key or substitute index (KEYCOLS(id, name). The audit data will be stored in the ea trail. The format for KEYCOLS is KEYCOLs(column1, column1, …).

Related Topics

- Adding Audit Trails with Agent-Based Collection
  To begin collecting audit data with the Audit Vault Agent, configure an audit trail for each target that's registered on the Audit Vault Server and then start the audit trail collection.

E.6 Creating Audit Trails in the Audit Vault Console

Follow these guidelines for creating transaction log audit trails for Microsoft SQL Server database targets in the Audit Vault console.

> **Note:**
>
> Before creating the audit trails, Oracle recommends (although it's not mandatory) that you set the `AV.COLLECTOR.TIMEZONEOFFSET` attribute for the Microsoft SQL Server database target in the Audit Vault Server console, because the transaction log audit trail gets the timezones of audit records from the target.
>
> Set `AV.COLLECTOR.TIMEZONEOFFSET` to the timezone offset of the Microsoft SQL Server database. For example: +03:00 for positive offset and -03:00 for negative offset.
>
> See Registering Targets for the full instructions.

Use the following guidelines when you create audit trails according to the steps in Adding Audit Trails with Agent-Based Collection:

• For **Trail Type**, select **TRANSACTION LOG**.

• For **Trail Location**, enter the full path of the directory that contains the CDC Extract XML files.

• Ensure that the Audit Vault Agent is running on the host machine that has access to the trail location.

• Ensure that the Audit Vault Agent user has read permission for the trail location.

E.7 Cleaning Up Audit Trails

Audit trail cleanup involves deleting the files that are read by the Audit Vault Agent.

See Cleaning Up Oracle GoldenGate Extracts.

F

Transaction Log Audit Data Collection for MySQL

This chapter explains how to configure Oracle GoldenGate for MySQL databases (Oracle AVDF 20.11 and later) and how to create transaction log audit trails in the Audit Vault Server console.

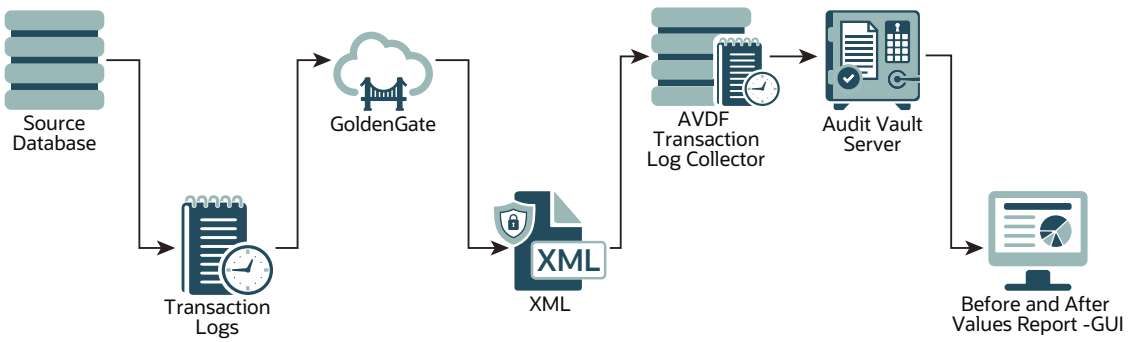
F.1 Introduction to the Transaction Audit Log Trail Using Oracle GoldenGate for MySQL

Change Data Capture (CDC) in MySQL records the insert, update, and delete operations that are performed on the data in the tables of the MySQL server.

The Transaction Log collector takes advantage of Oracle GoldenGate's Extract process (CDC Capture) to pull CDC table data into XML files. Oracle AVDF's Transaction Log collector for MySQL collects transaction log records from generated XML files. These logs are forwarded to the Audit Vault Server to show the before and after values that are changed in the **Data Modification Before-After Values** report. The DML changes are available in the **Data Modification Before-After Values** report.

Starting with Oracle AVDF 20.10, the **Data Modification Before-After Values** report has additional information about key columns. GoldenGate, by default, uses the primary key columns of the table as key columns. If no primary keys are defined for the table, or if you want to use some other columns as key columns, then GoldenGate provides an option to specify key columns in the parameter file.

Figure F-1 Transaction Log Collection Process



> **Note:**
>
> Oracle GoldenGate for MySQL does not capture certain details, such as the program name, database username, OS username, OS terminal, client host name, client ID, process ID, and proxy session ID for transactions committed in the database. As a result, this limitation will cause the Oracle AVDF's Data Modification Before-After Values report to display empty values for these fields.

F.2 Sizing Guidelines

Follow these sizing guidelines to configuring Oracle GoldenGate for MySQL.

Prerequisites

Follow the system and sizing requirements in What is Required? in the Oracle GoldenGate documentation.

General Sizing Guidelines

- For memory and CPU, start with 32 GB of memory and 2 CPUs per Extract, because it's a multithreaded process and uses a large amount of memory when processing large transactions. Depending on the transaction volume and pattern, scale up the resources appropriately following the guidelines in the Oracle GoldenGate documentation.
- For disk space, start with 2 TB, and vary it based on the volume of data that the Extract captures from the source databases. The Extract uses storage for trail files and temporary disk space for cache files if there's a big transaction to buffer for processing.

Temporary disk space requirements due to large transactions may fill up the cache and spill over to the transaction-cached data or temporary files. Configure an archive policy and define the retention period of the files so they can be recycled accordingly.

Maintain enough physical memory to handle large transactions. According to the guidelines, have at least 32 GB of memory available for the Extract to use. For a more accurate estimation, collect the statistics from the database server history run and check for the size of the biggest transaction. Oracle GoldenGate provides the `send <extract> cachemgr, cachestats` command that displays the statistics of the transaction, which is helpful to determine the baseline for estimation.

In general, the sizing, storage, and memory for the Oracle GoldenGate Extract process is highly dependent on the transaction volume and transaction pattern. Collect these statistics from every single database server to estimate, because there's no standard value. The number of databases that can be supported by a single GoldenGate instance or Extract process depends on the system resources that support multiple Extracts. Configure one Extract for every database.

> **See Also:**
>
> - Other Disk Space Considerations
> - Temporary Disk Requirements

F.3 Restricted Use License for Oracle GoldenGate

A restricted-use license for Oracle GoldenGate is included with Oracle AVDF release 20.

This license permits you to install Oracle GoldenGate and use the Extract process to capture transactional changes in database systems that are monitored by Oracle AVDF. The extracted data from Oracle GoldenGate is consumed only by Oracle AVDF. Deploy Oracle GoldenGate Microservices Architecture on a separate server other than the server on which the Oracle AVDF appliance is deployed. Then configure the Oracle GoldenGate Extract feature. Oracle AVDF 20.11 and later supports Oracle GoldenGate Microservices Architecture version 21.3.0.0.0 for MySQL version 8.0.

F.4 Installing Oracle GoldenGate for MySQL Database

Follow these instructions to install Oracle GoldenGate on MySQL Server.

For MySQL-compatible databases on Linux platform

1. Follow the instructions for Installing Oracle GoldenGate in the *Oracle GoldenGate MicroServices Documentation*.
2. Verify the requirements to install Oracle GoldenGate for MySQL in the *Oracle GoldenGate MicroServices Documentation*.
3. Download and install Oracle GoldenGate 21.3 Microservices for MySQL-compatible Databases on Linux x86-64 from Oracle Software Delivery Cloud.

F.5 Capturing Transaction Log Data from MySQL Server

To configure the database and CDC extract process on Oracle GoldenGate for a MySQL database, follow the below steps.

1. Creating Users and Privileges
2. Preparing Database Connection, System, Parameter, and Transaction Log Settings
3. Configuring the Database for Oracle GoldenGate
4. Creating the GoldenGate CDC Extract

F.5.1 Creating Users and Privileges

Oracle GoldenGate recommends having a separate user for it. This can be the same user for all Oracle GoldenGate processes that must connect to a database. For more information, see Prepare Database Users and Privileges in the *Oracle GoldenGate Microservices Documentation*.

F.5.2 Preparing Database Connection, System, Parameter, and Transaction Log Settings

To configure the database and its connection, see Prepare Database Connection, System, and Parameter Settings in *Oracle GoldenGate Microservices Documentation*.

To configure the transaction log settings, see Transaction Log Settings and Requirements in *Oracle GoldenGate Microservices Documentation*.

F.5.3 Configuring the Database for Oracle GoldenGate

Following the installation of Oracle GoldenGate, you will need to configure the MySQL database.

1. Open the console page of the Administration Service.
2. Click on the **Application Navigation** menu.
3. Click the **Configuration** tab.
4. Select the **Database** option.
5. Click on the **+** in front of **Credentials** to add the database credentials.
6. Enter the credential domain.
7. Enter any credential aliases.
8. Enter the database server address.
9. Enter the database port number.
10. Enter the database name.
11. Enter the user ID.
12. Enter the password.
13. Click **Submit**.
14. After creating the credential, click the **Log in** database icon. This ensures that the newly created credential is able to connect to the target database.

F.5.4 Creating the GoldenGate CDC Extract

Create and execute the CDC capture for MySQL.

1. Open the Console page of **Administration Service**.
2. Click on the **Administration Service** tab.
3. Click on the **+** of the **Extracts** tab.
4. Select the extract type as **Change Data Capture Extract**
5. Click **Next**.
6. Enter the process name in the **Process Name** field.
7. Select **Unidirectional** in the **Intent** field.
8. If the extract is going to do remote capture, click on **Remote**.
9. Choose the appropriate **Credential Domain** from the drop-down list.
10. Choose the appropriate **Credential Alias** created in Configuring the Database for Oracle GoldenGate from the drop-down list.
11. Select **Now** from the drop-down list in the **Begin** field.
12. Enter the **Trail Name**. It can be a combination of any two alphabetic characters.
13. Enter the **Trail Subdirectory** if customization of the Trail Subdirectory is needed.
    The trail subdirectory can be the full path of any directory. This directory must already exist in the file system.
14. Set the **Trail Size** (in MB).

> **Note:**
>
> In case the record generation rate of GoldenGate is low (less than 50 records per second), then it is recommended to set the Trail Size to lower values. For example, 100MB.

15. Click **Next**.
16. In the **Parameter File** subsection, enter the below parameters:

```
EXTRACT <extract name>
SOURCEDB <Database Name@Database Server:port> USERIDALIAS <useralias>,
DOMAIN <Domain name>
OUTFORMAT XML _AUDIT_VAULT
TRANLOGOPTIONS ALTLOGDEST REMOTE
EXTTRAIL <subdirectory>/<trail name>
TABLE <schema>.<table name>,GETBEFORECOLS (ON UPDATE ALL, ON DELETE ALL);
```

For example:

```
EXTRACT exta
SOURCEDB HR@10.245.102.35:3306 USERIDALIAS  mysql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
TRANLOGOPTIONS ALTLOGDEST REMOTE
EXTTRAIL xy
TABLE HR.*,KEYCOLS(id,gid),GETBEFORECOLS (ON UPDATE ALL, ON DELETE ALL);
```

Note the following parameter guidelines:

- There is space between `XML` and `_AUDIT_VAULT` in the `OUTPUTFORMAT` parameter.
- The `OUTPUTFORMAT` parameter must be mentioned before the `exttrail` parameter in the parameter file. Otherwise, the XML files are not generated.
- Ensure the `TABLE` command always ends with a semicolon (;).
- Ensure the sequence of all the parameters is in the exact order as mentioned above.
- The `TABLE` command is used to specify the tables for which DML changes need to be captured.
- The `REMOTE` keyword should be used only in case of remote capture, where Oracle GoldenGate and MySQL are installed on different machines.
- To get more information about Oracle GoldenGate parameters, see Oracle GoldenGate Parameters in the *Reference for Oracle GoldenGate* guide.

17. Click **Create and Run** to start the CDC Extract process.
The newly created CDC Extract appears in the **Extracts** section on the **Administration Service** page.
18. To view the status of the CDC Extract:
    a. Click the **Actions** button for the extract.
    b. Select **Details**.
    c. Click **Report** tab to view the diagnostic messages.
    If the extract process fails, this report displays the relevant errors.

F.5.5 Sample Oracle GoldenGate CDC Extract Parameter Files

Use these Oracle GoldenGate CDC Extract parameter files as samples.

Audit DML for a table and set the columns to be used as key columns

The following parameter file configures CDC Extract to do the following:

- Capture DML operations on the `emp` table in the `dbo` schema.
- Set `empno` and `ename` as key columns.

```
EXTRACT <extract name>
SOURCEDB <Database Name@Database Server:port> USERIDALIAS <useralias>, DOMAIN
<Domain name>
OUTFORMAT XML _AUDIT_VAULT
EXTTRAIL <subdirectory>/<trail name>
TABLE dbo.emp, KEYCOLS (empno, ename);
```

Audit DML in table

The following parameter file audits DML operations on the required tables:

- The parameter file provided is for a single table.
- Additional table names can be added by the user.

```
EXTRACT <extract_name>
SOURCEDB <Database Name@Database Server:port> USERIDALIAS <useralias>, DOMAIN
<Domain name>
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL <subdirectory> {Any combination of two alphabets indicating prefix
of trail file e.g. ab, bc, ea, sn.....etc}
TABLE owner.table_name;
```

Example: The following parameter file audits DML operations on the `dbo.employee` table. The audit data will be stored in the `\dirdat\ea` location:

```
EXTRACT exta
SOURCEDB HR@10.245.102.35:3306 USERIDALIAS mysql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL \dirdat\ea
TABLE dbo.employee;
```

- `exta` is the name of the CDC Extract.
- In `dbo.employee`, `dbo` is the schema name that owns the `employee` table.
- `HR` is the name of the database.
- `10.245.102.35` is the IP of the host on which database is installed.
- `3306` is the port number of the MySQL database.
- `mysql` is the `USERIDALIAS`
- `OracleGoldenGate` is the DOMAIN.

Audit DML with GETBEFORECOLS option

The following parameter file configures the Extract process to capture DML operations on a specific table with the GETBEFORECOLS option enabled. This option ensures that key columns appear in the before image of the audit file generated by Oracle GoldenGate, which is essential for displaying key columns in reports for update and delete operations.

```
EXTRACT exta
SOURCEDB HR@10.245.102.35:3306 USERIDALIAS mysql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL ea
TABLE dbo.employee, GETBEFORECOLS(ON UPDATE ALL, ON DELETE ALL);
```

Use GETBEFORECOLS to specify the columns to be captured and written to the before image of the trail. In the above example, the ALL keyword indicated that all columns should be included in the before image for update and delete operations.

Audit DML with KEYCOLS option

The following parameter file configures the Extract process to capture DML operations on a specific table using the KEYCOLS option. This option is used to define a substitute primary key when a primary key or an appropriate unique index is not available for the table.

```
EXTRACT exta
SOURCEDB HR@10.245.102.35:3306 USERIDALIAS mysql, DOMAIN OracleGoldenGate
OUTPUTFORMAT XML _AUDIT_VAULT
EXTTRAIL ea
TABLE dbo.emp3, KEYCOLS(id.name), GETBEFORECOLS(ON DELETE ALL);
```

The above parameter file audits DML operations on the dbo.employee table. The KEYCOLS option is used to treat the id and name columns together as a unique primary key or substitute index (KEYCOLS(id, name). The audit data will be stored in the ea trail. The format for KEYCOLS is KEYCOLS(column1, column1, …).

Related Topics

- Adding Audit Trails with Agent-Based Collection
  To begin collecting audit data with the Audit Vault Agent, configure an audit trail for each target that's registered on the Audit Vault Server and then start the audit trail collection.

F.6 Guidelines for Creating Audit Trails in the Audit Vault Server Console

Follow these guidelines for creating transaction log audit trails for MySQL database targets in the Audit Vault Server console.

Recommendations

1. Before creating the audit trails, Oracle recommends that you set the AV.COLLECTOR.TIMEZONEOFFSET attribute for the MySQL database target in the Audit Vault Server console, because the transaction log audit trail gets the timezones of audit records from the target. Set AV.COLLECTOR.TIMEZONEOFFSET to the timezone offset of the MySQL database. For example: +03:00 for positive offset and -03:00 for negative offset.

See Registering Targets for more information.

2. Oracle also recommends, that you set the `AV.COLLECTOR.securedTargetVersion` attribute for the MySQL database target in the Audit Vault Server Console. This attribute specifies the version of the MySQL database. If this attribute is not set, by default MySQL will be treated as version 8.0.

Guidelines

Use the following guidelines when you create audit trails according to the steps in Adding Audit Trails with Agent-Based Collection:

- For **Trail Type**, select **TRANSACTION LOG**.
- For **Trail Location**, enter the full path of the directory that contains the CDC Extract XML files.
- Ensure that the Audit Vault Agent is running on the host machine that has access to the trail location.
- Ensure that the Audit Vault Agent user has read permission for the trail location.

F.7 Cleaning Up Audit Trails

Audit trail cleanup involves deleting the files that are read by the Audit Vault Agent.

See Cleaning up Oracle GoldenGate Extracts.

G

PostgreSQL Audit Data Collection Reference

Learn how to collect audit data from PostgreSQL.

G.1 Introduction to PostgreSQL Audit Data Collection

Learn how to collect audit data from PostgreSQL.

PostgreSQL is a open source object relational database system that uses and extends the SQL language combined with many features. It safely stores and scales the most complicated data workload. The origin of PostgreSQL dates back to 1986 as part of the POSTGRES project at the University of California in Berkeley, and has more than 30 years of active development on the core platform.

PostgreSQL must be configured to generate audit data in CSV format. The PostgreSQL audit extension (or `pgaudit`) provides detailed session and object audit logging through the standard logging facility provided by PostgreSQL.

Installing `pgaudit` extension on the PostgreSQL database is a must for audit collection. Audit Vault Agent supports collection of PostgreSQL audit events only if the `pgaudit` extension is installed and PostgreSQL is configured to generate audit data in CSV format.

G.2 Installing PostgreSQL

Learn how to install PostgreSQL.

1. Refer to the documentation in the following link:

   https://www.postgresql.org/download/linux/redhat/
2. Install the relevant PostgreSQL version.

G.3 Steps After Installing PostgreSQL

Run post PostgreSQL installation steps.

Update PostgreSQL Super User Password

A default super user *postgres* is created during PostgreSQL installation. Run the following command to change the password for *postgres* user:

```
sudo passwd postgres
```

Create PostgreSQL Non Super User

Create a new user with necessary permission to create databases, and set the password. Run the following command to create the new user:

```
sudo -u postgres createuser <new user name> -d -P
```

Create root Permission on PostgreSQL Database

The role *root* is required for installing `pgaudit` extension on PostgreSQL database. Perform these steps:

1. Run the following command to log in as user *postgres*:

   ```
   sudo -u postgres psql
   ```

2. Run the following commands in the `postgres` command prompt:

   ```
   create role root superuser;


   alter user root with password <new password>;


   alter role root with login;
   ```

3. Find the PostgreSQL configuration file location by running the following commands, and then exit the `postgres` command prompt. Make a note of the configuration file details, as it is updated in the later part of this topic.

   ```
   show config_file;


   exit;
   ```

Create a Sample Database

1. Log in using the newly created PostgreSQL non super user.
2. Create a sample database by running the following commands:

   ```
   createdb <new database name>
   ```

3. Log in to the newly created database with the newly created PostgreSQL non super user by running the following command:

   ```
   psql <new database name>
   ```

4. Exit the database prompt by running `exit` or `\q` command.

Install the pgaudit Extension on PostgreSQL Database

1. Log in as *root* user and run the below commands to install PostgreSQL developer libraries. The commands used in this section are for installing PostgreSQL 11 developer libraries as example only.

   ```
   yum install postgresql11-devel
   ```

2. Follow the steps provided in *Compile and Install* section in the below link, to install `pgaudit` extension.

   https://github.com/pgaudit/pgaudit

3. Log in as *root* user. In the PostgreSQL configuration file, update the `shared_preload_libraries` parameter to include `pgaudit`, and save the file.

   ```
   shared_preload_libraries = 'pgaudit'
   ```

4. Log in as *root* user. Restart the PostgreSQL service by running these commands:

   ```
   /sbin/service postgresql-11 stop


   /sbin/service postgresql-11 start
   ```

Enable pgaudit Audit Logging in PostgreSQL Database

> **Note:**
>
> For complete information on all the PGAUDIT settings, refer to the respective documentation.

1. Log in as *postgres* user:

   ```
   sudo -u postgres psql
   ```

2. Run the following commands in `postgres` command prompt, for enabling auditing for the newly created database:

```
CREATE EXTENSION pgaudit;

alter database <database name> set pgaudit.log = 'all';

SET pgaudit.log = 'ALL';

SET pgaudit.log_level = 'notice';

SET pgaudit.log_client = ON;

SET pgaudit.log_relation = ON;

SET pgaudit.log_parameter = ON;

SET pgaudit.log_catalog = ON;

alter system set log_connections=on;

alter system set log_disconnections=on;

alter system set log_statement='all';

alter system set pgaudit.log_parameter TO 'on';

SELECT pg_reload_conf();
```

Update Audit Logging Parameters in PostgreSQL Configuration File

> **Note:**
>
> For complete information on all the PostgresSQL logging related parameters, refer to the respective documentation.

Log in as *root* user. Edit the PostgreSQL configuration file and update below parameters as follows:

```
log_destination = 'csvlog'
log_filename = 'postgresql-%Y-%m-%d_%H%M%S.log'
```

```
log_min_messages = info
log_checkpoints = on
log_connections = on
log_disconnections = on
log_duration = on
log_error_verbosity = verbose
log_hostname = on
log_statement = 'all'
log_directory = '<full path of directory where log files need to be stored>'
log_file_mode = 0640
```

Log in as *root* user and restart the PostgreSQL service. The following example commands are for PosgreSQL 11:

```
/sbin/service postgresql-11 stop


/sbin/service postgresql-11 start
```

Generate Audit Log

1. Log in as the newly created PostgreSQL non super user. Now, log in to the newly created database using below command:

   ```
   psql <database name>
   ```

2. Run commands to create tables, insert data into the tables, and query the data from the tables.
3. The logs are present in the following location for PostgreSQL 11 (example) installation on Oracle Linux 6.

   ```
   /var/lib/pgsql/11/data/log/
   ```

H

Ports Used by Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall uses specific TCP and UDP ports.

H.1 Ports for Deploying Database Firewall for Targets

You must configure two classes of ports when deploying Database Firewall for targets.

These following two classes of ports must be open in external network firewalls for the following types of Database Firewall deployments:

- When you configure Database Firewall to protect a target database, traffic directed to that database must be able to pass through external network firewalls to Database Firewall. The ports required are configured in the target's page in Audit Vault Server.
- You can configure Database Firewall to accept proxy connections which are passed on to the database. The ports required for proxy connections are configured in the Network Configuration page on Database Firewall.

> **Note:**
>
> It is recommend that you do not change these ports.

> **See Also:**
>
> - Registering or Removing Targets in Audit Vault Server
> - Configuring the Database Firewall As a Traffic Proxy

H.2 Ports for Services Provided by Audit Vault Server

Learn about the ports for services that are provided by Audit Vault Server.

Table H-1 lists the ports for services that are provided by Audit Vault Server. These services are used by external users of the system. Access to most of these ports can be controlled within Oracle AVDF. If you use external network firewalls, then these ports must be open to enable connections from the users, or clients, of these services to Audit Vault Server.

Table H-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)	None
1521	TCP	Oracle Database	Access for Audit Vault agents, and access to Oracle Database for reporting	Audit Vault Agents use native Oracle Net Services data encryption
1522	TCPS	Oracle Database	Access for Audit Vault agents, and access to Oracle Database for reporting	Uses TCPS
7443	TCP	HTTPS	Starting with Oracle AVDF 20.10, the Audit Vault Agent uses this port to connect to the Audit Vault Server. Audit Vault Servers in high availability mode.	This is between primary and secondary Audit Vault Servers when high availability is configured. The Audit Vault Agent uses HTTPS for agent activation.

H.3 Ports for Services Provided by Database Firewall

Learn about the ports for services that are provided by Database Firewall.

Table H-2 lists ports for general services provided by Database Firewall. These services are used by outside users of the system, and access to all them can be controlled within Oracle Audit Vault and Database Firewall. If you use external network firewalls, then these ports must be open to enable connections from the users, or clients, of these services to the Database Firewall configurations in Oracle Audit Vault and Database Firewall.

Table H-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

Table H-2 (Cont.) Ports for Services Provided by Database Firewall

Port	Protocol Family	Protocol	Purpose	Notes
2050 - 5100	TCP	Audit Vault and Database Firewall Internal Protocol	Incoming traffic captured from Host Monitor Agent. The Host Monitor Agent forwards the data securely to Database Firewall.	This applies when deployed in Host Monitor mode and ports need not be open during out-of-band or proxy mode. For each monitoring point, a unique port is created in the given range. The exact port for each monitoring point can be found by: 1. Log in to the Database Firewall through SSH and switch to the `root` user. See Logging In to Oracle AVDF Appliances Through SSH. 2. Change to `/var/dbfw/va` directory. 3. Identify the Database Firewall monitoring point by searching for the target name configured in the Audit Vault Server. Run the following command: `grep -lr <TARGET NAME> *` 4. Find the monitoring point number from the output which contains the name and path of the configuration file. For example: `1/etc/appliance.conf`. In this example, `1` is the monitoring point number. `REMOTE_AGENT_LISTEN_PORT` is the key in `appliance.conf` file that represents the port Database Firewall is listening for data from Host Monitor Agent.
2050 - 5100	TCP	Syslog	Incoming WAF (F5) violation alerts	The exact port number used by a monitoring point can be found in the **Advanced** settings. **See Also:** Finding the Port Number Used by a Database Firewall Monitoring Point

H.4 Ports for External Network Access by Audit Vault Server

You must configure the correct external network firewall ports to enable Audit Vault Server to access them as a client.

Table H-3 lists ports for external services that Audit Vault Server can use. If you use external network firewalls, then the correct ports must be open so that Audit Vault Server can use these services as a client.

Table H-3 Ports for External Network Access by the Audit Vault Server

Port	Protocol Family	Protocol	Purpose	Notes
25	TCP	SMTP	Email delivery	None
53	UDP	DNS	Domain name service	None
123	UDP and TCP	NTP	Time Synchronization	None
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 Also:** Configuring Audit Vault Server Syslog Destinations
3260	TCP	Software iSCSI	SAN server communication	This port can be configured on Audit Vault Server console when registering a SAN server. **See Also:** Registering a SAN Server
Target listener port. It is the same as the port provided in target location.	Oracle Database	TCP or TCPS	User Entitlement Reporting Stored Procedure Auditing Audit Policy Retrieval Security Assessment and Sensitive Objects	The direct connection between Audit Vault Server and the target. The connection details is provided with the target location used.

> **See Also:**
>
> About Plug-ins for a complete list of supported target types.

H.5 Ports for External Network Access by Database Firewall

Learn about the ports that you must configure for access by Database Firewall.

Table H-4 lists ports for external services that Database Firewall can use. If you use external network firewall, then the relevant ports must be open so that Database Firewall can use these services as a client.

Table H-4 Ports for External Network Access by Database Firewall

Port	Protocol Family	Protocol	Purpose	Notes
53	UDP	DNS	Domain name service	None
123	UDP and TCP	NTP	Time Synchronization	None
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.
514	TCP	WAF (F5) alerts	WAF (F5) alerts	The port can be changed from the Audit Vault Server console.

See Also:

Configuring Audit Vault Server Syslog Destinations

H.6 Ports for Internal TCP Communication

Learn about ports for internal TCP communication between Database Firewall and Audit Vault Server.

Table H-5 lists ports for services that are used between Database Firewall and Audit Vault Server. If you configure an external network firewall between these systems, then you must open the relevant ports.

Table H-5 Ports for Internal TCP Communication

Port	Protocol Family	Protocol	Direction	Notes
7443	TCP	HTTPS	• Database Firewall accepts connections from Audit Vault Server • Database Firewall accepts connections from Audit Vault Server in high availability.	It is the default port for inter appliance communication. It applies to both the Audit Vault Server and the Database Firewall. It also handles traffic log transfer from the Database Firewall.
1514	TCP	SSL	Audit Vault Server accepts connections from Database Firewall	Event reporting and monitoring

Message Code Dictionary for Oracle Audit Vault and Database Firewall

Learn about the different messages that Oracle Audit Vault and Database Firewall can generate.

I.1 Audit Vault Messages

Learn about Audit Vault messages.

This table lists the Audit Vault 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 plugins are registered that can collect from this audit trail.

Action: Explicitly specify the plugin 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 plugin to handle the trail.

Action: Deploy the plugin on the server that can handle this trail and deploy the agent with this plugin 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 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 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 target
Cause: Target specified had trails which were active.

Action: Stop all the active trails for the given Target.

46525: Sourcetype-specific extension for Category already exists
Cause: Event Category was specified which already has a Format extension for the given Sourcetype.

Action: Provide an Event Category which does not have a Sourcetype-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: Sourcetype specified had active Sources.

Action: Drop the active Sources before dropping this Sourcetype.

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 Sourcetype.

46532: Attribute '*string*' is not set for target '*string*'.
Cause: The specified attribute was not set for the target.

Action: Set the specified attribute for the target.

46533: Invalid lock type '*string*' specified.
Cause: An invalid plugin lock type was specified.

Action: Valid plugin lock types are 'DEPLOY' and 'UNDEPLOY'.

46534: Plug-in deployment/undeployment operation already in progress.
Cause: A plug-in deployment/undeployment operation is already in progress and a corresponding lock already exists.

Action: Wait for the current operation to end before attempting another plug-in deployment/undeployment operation.

46535: failed to add target address: address '*string*' is used by Target '*string*'.
Cause: The user tried to add a duplicate address for a target.

Action: Check existing address for the 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: Target Name is too long.
Cause: Target Name failed length validation checks.

Action: Provide valid Target Name.

46540: Target Description is too long.
Cause: Target Description failed length validation checks.

Action: Provide valid 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. Audit Trail will continue to auto-start.
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 Target Location requires setting User Name and Password; please specify User Name and Password along with the Target Location.
Cause: The user tried to set target location without setting user name and password.

Action: Set user name and password along with the target location.

46548: Failed to generate target location string.
Cause: User did not specify the correct components of target location string.

Action: Specify the correct components of 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: Target Location is required for registering this target.
Cause: User tried to register a target without providing target location, which is required to connect to the target.

Action: Provide 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: Target Location is too long.
Cause: Target Location failed length validation checks.

Action: Provide valid 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 bytes.
Cause: Password failed length validation checks.

Action: Provide valid Password.

46558: Target Attribute Name is too long.
Cause: Target Attribute Name failed length validation checks.

Action: Provide valid Target Attribute Name.

46559: Target Attribute Value is too long.
Cause: Target Attribute Value failed length validation checks.

Action: Provide valid Target Attribute Value.

46560: Setting User Name and Password requires enabling Target Location; please specify Target Location along with User Name and Password.
Cause: The user tried to set user name and password without enabling target location.

Action: Set 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 Catetory 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).

46569: no agent running on host "*string*". Audit trail no longer eligible for auto-start.
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.

46570: no agent running on host "*string*". Audit trail is now eligible for auto start and will auto-start when the agent is started.
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.

46571: Agent is running on host "*string*". Host name or host IP can not be changed.
Cause: Agent at the specified host is running.

Action: Stop the agent and then change host name and IP.

46572: Agent is UNREACHABLE on host "*string*". Please try after some time. Audit trail no longer eligible for auto-start.
Cause: Agent at the specified host is in UNREACHABLE state.

Action: Please check the agent log files for details.

46573: Agent is UNREACHABLE on host "*string*". Please try after some time. Audit trail is now eligible for auto start.
Cause: Agent at the specified host is in UNREACHABLE state.

Action: Please check the agent log files for details.

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 Target.
Cause: User tried to start a collection of type network for a target which has no enforcement point configured.

Action: Configure an enforcement point for the 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: target address does not exist. cannot drop target address.
Cause: User tries to drop a target address which does not exist.

Action: Check the 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 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 Target; Stored Procedure Auditing collection is in progress.
Cause: User tried to drop 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.

46627: error in aquiring the global lock for target *string*
Cause: Internal error occurred while acquiring the global lock.

Action: Contact Oracle Support Services.

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 Target *string*.
Cause: User tried to drop a 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 Target(s) and try again.

46652: Cannot delete built-in Retention Policies.
Cause: Cannot delete built-in Retention Policies.

Action: n/a

46653: Retention Policy Name is too long.
Cause: Retention Policy Name failed length validation checks.

Action: Provide valid Retention Policy Name.

46654: Invalid Retention Policy Name.
Cause: Retention Policy Name contains illegal characters.

Action: Provide a valid Retention Policy Name.

46655: Invalid Retention Policy Month specified. Online Month must be between 0 and 9996. Offline Month must be between 1 and 9996.
Cause: Retention Policy Month is invalid.

Action: Provide a valid Retention Policy Month.

46656: Unable to release tablespace used by audit trails.
Cause: There is one or more audit trails writing data into the selected tablespace.

Action: n/a

46657: Datafile associated with tablespace *string* is inaccessible at this archive location *string*.
Cause: The datafile for the tablespace needed by a trail is not accessible.

Action: n/a

46658: Unable to stage datafile *string* for archiving.
Cause: Insufficient space on /var/lib/oracle.

Action: Add space and try again.

46661: Service Name is too long.
Cause: Service Name failed length validation checks.

Action: Provide valid Service Name.

46662: Service Name/SID is not supported for Target of type "*string*".
Cause: User entered service name as part of target address for a target which does not support service name.

Action: Do not provide service name when providing target address.

46663: Target Address is not supported for Target of type "*string*".
Cause: User tried to add a target address for a target which cannot be monitored by the firewall.

Action: Users are not allowed to add target address for a target which cannot be monitored by the firewall.

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 control characters, delete character, non-spacebar space, or double-quote (") character
Cause: Illegal characters were supplied in password.

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 invalid. User name cannot be null, or start with reserved user name. Only alphanumeric, underscore (_), dollar sign ($), and pound sign (#) are allowed for user name.
Cause: Illegal user name is provided.

Action: Please specify a different user name and try again.

46678: User account *string* is locked or has expired. Please contact your administrator.
Cause: User account with specified name is locked or has expired.

Action: Contact your administrator.

46679: Password cannot have leading, or trailing space. ASCII only password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(.,+:_!). Password must be at least 8 characters and at most 30 bytes in length.
Cause: Password does not satisfy the password rule.

Action: Specify valid characters and try again.

46680: User account *string* is locked. Please contact your administrator.
Cause: User account with specified name is locked.

Action: Contact your administrator.

46681: Failed to remove AVS log files. [*string*]
Cause: Files does not exist, or no privilege to access the files.

Action: Make sure directory `/var/lib/oracle/dbfw/av/log` and log files exist and OS user oracle has privilege to access and remove those files.

46682: Failed to set trace level for AVS event 46600
Cause: Null value is passed for trace level.

Action: Contact Oracle Support Services.

46683: Old and new passwords should not be the same.
Cause: Old and new password are the same.

Action: Specify different passwords and try again.

46684: The password cannot be reused.
Cause: Old password is reused.

Action: Specify different new password and try again. User can reuse the password after 365 days if the password has already been changed 1 time.

46685: Failed to generate diagnostic file for download
Cause: Operation failed while generating diagnostics file for download.

Action: Check information in `/var/log/messages` and `/var/log/debug`.

46686: Empty diagnostics file name.
Cause: Operation failed while generating diagnostics file without a file name.

Action: Check information in /var/log/messages and /var/log/debug.

46687: Invalid diagnostics file name format: "*string*" for generation.
Cause: Operation failed while generating diagnostics file with invalid file name format.

Action: Check information in /var/log/messages, /var/log/debug, and trace file for "Admin API::Diagnostics".

46688: Diagnostics file is missing after generation opertion.
Cause: Operation failed while generating diagnostics file for download.

Action: Check information in /var/log/messages and /var/log/debug, and trace file for "Admin API::Diagnostics".

46689: Invalid diagnostics file name format: "*string*" for download.
Cause: Operation failed while downloading diagnostics file with invalid file name format.

Action: Check information in /var/log/messages and /var/log/debug, and trace file for "Admin API::Diagnostics".

46690: Diagnostics file "*string*" is missing for downloading.
Cause: Operation failed while downloading diagnostics file.

Action: Check information in /var/log/messages, /var/log/debug, and trace file for "Admin API::Diagnostics".

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: Eventid 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 of 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 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.

46865: Firewall *string* is offline.
Cause: User tried to create an enforcement point using a firewall which is offline.

Action: Bring the firewall online and try again.

46866: An Enforcement Point with the same configuration already exists.
Cause: User tried to create two EPs with the same target and firewall.

Action: Two EPs with the same firewall and target are not allowed.

46867: *string* is not a valid global name.
Cause: Global name contains invalid character [()@=].

Action: Correct Audit Vault Server global name.

46868: Alert syslog template name is too long.
Cause: Alert syslog template name failed length validation check (255B is the limit).

Action: Provide a valid alert syslog template name.

46869: Alert syslog template description is too long.
Cause: Alert syslog template description failed length validation check (4000B is the limit).

Action: Provide a valid alert syslog template description.

46870: Alert syslog template "*string*" already exists
Cause: Alert syslog template already exists.

Action: Please try creating the alert syslog template with another name.

46871: Dropping the default alert syslog template is not allowed.
Cause: User attempts to drop the default alert syslog template.

Action: Users are not supposed to drop the default alert syslog template.

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 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.

46979: Firewall *string* (with IP address *string*) has the same IP address as the Audit Vault Server
Cause: User tried to register a firewall which has the same IP address as Audit Vault Server.

Action: Check the name and/or IP of the firewall then try again.

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 configuration of the secondary Firewall does not match that of the primary Firewall.
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 in monitoring and blocking mode, 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 monitoring and blocking mode, only one proxy interface must be specified.

Action: Specify one proxy most and retry the operation.

46991: Invalid monitoring only mode for proxy interface.
Cause: Use monitoring and blocking mode when proxy interface is specified.

Action: Specify monitoring only mode.

46992: Enforcement Point mode cannot be in monitoring and blocking mode when the Firewall is in a resilient pair configuration.
Cause: Monitoring only mode must be set when Firewall is in a resilient configuration.

Action: Specify monitoring only 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: Target Address cannot be deleted.
Cause: There must be at least one address defined when there are active Enforcement Points.

Action: Add a new 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 timeout must be at least 30 minutes and no more than a day.

Action: Please specify a valid timeout value and try again.

46999: IP address, port number, service name, and credentials must be specified in order to decrypt with Native Network Encryption Key.
Cause: User tried to decrypt with native network encryption key without specifying IP address, port number, service name, or credentials.

Action: Specify IP address, port number, service name, or credentials appropriately 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.

47004: Host Monitor is not installed on host '*string*'.
Cause: Host Monitor is not installed for the Host.

Action: Install Host Monitor at the host

47005: Upgrade of Host Monitor on host '*string*' failed.
Cause: Host Monitor auto upgrade failed for the Host.

Action: Reinstall Host Monitor at the host

47006: Host Monitor on host '*string*' is being upgraded.
Cause: Host Monitor auto upgrade is running for the Host.

Action: Try later once upgrade finishes.

47007: Host Monitor is being installed on host '*string*'.
Cause: Host Monitor installation is running for the Host.

Action: Try later once installation finishes.

47008: Host Monitor is being uninstalled on host '*string*'.
Cause: Host Monitor uninstallation is running for the Host.

Action: Try after Installing Host Monitor once uninstallation finishes.

47009: Host '*string*' is not active.
Cause: The host is deactivated.

Action: Activate the host and install Host Monitor on the host.

47010: Host Monitor is not supported for host '*string*' (*string*).
Cause: Host Monitor is not supported for the platform type

Action: Contact Oracle Support

47011: Host Monitor needs to be upgraded to a newer version for host '*string*'.
Cause: Host Monitor version is lower than the version available at the server.

Action: Download new Host Monitor zip from Audit Vault Server and update Host Monitor.

47012: Host Monitor state is unknown for host '*string*'.
Cause: Host Monitor state is Unkown.

Action: Download new Host Monitor zip from Audit Vault Server and install Host Monitor.

47101: Invalid job name specified. Job name must be at most 18 chars and must be a valid SQL identifier.
Cause: Job name validation failed.

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 diskgroup does not exist.
Cause: ARCHIVE diskgroup must exist.

Action: Please create ARCHIVE diskgroup 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' diskgroup with archived data.
Cause: Archived data is present in the diskgroup.

Action: Add another disk to diskgroup or wait untill 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 untill the archive period expires.

47113: Tablespace is being encrypted. Please try again
Cause: Specified tablespace has been encrypted already.

Action: Encrypt again with another tablespace name.

47114: Job is currently running. Re submit after the job finishes
Cause: Retrieve job for encryption has already been running.

Action: Wait and resubmit.

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: n/a

47206: Operation not permitted. User is neither admin nor auditor.
Cause: The user passed in is neither admin nor auditor.

Action: Specify an admin or auditor and retry.

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 diskgroup *string*.
Cause: Disk specified is not part of an existing diskgroup.

Action: Specify a disk that is a memeber of a diskgroup 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 diskgroup *string* specified.
Cause: Diskgroup must be one of 'SYSTEMDATA', 'RECOVERY', 'EVENTDATA' or 'ARCHIVE'.

Action: Please try again with a valid diskgroup.

47312: Disk *string* already member of a diskgroup.
Cause: Disk already part of diskgroup

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 diskgroup.

Action: Drop the disk from the diskgroup 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* diskgroup. This operation requires *number* MB of free space in the diskgroup
Cause: Disgkroup rebalance operation will fail.

Action: Add more disks to the diskgroup and try again.

47331: User requested to stop the encryption process.
Cause: User requested to stop the encryption process.

Action: Try again.

47332: Encryption process has not started yet. Execute /usr/local/dbfw/bin/avdf_data_encryption.sh as root and try again.
Cause: Encryption process not started yet. Execute /usr/local/dbfw/bin/avdf_data_encryption.sh as root

Action: Try again.

47333: All tablespaces are encrypted.
Cause: All tablespaces are encrypted.

Action: n/a

47401: The remote filesystem is busy.
Cause: There are open file(s) on the filesystem.

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 filesystem mount point still exists.
Cause: Remote filesystem was not unmounted before delete operation.

Action: Unmount the remote filesystem (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: Filesystem name *string* is not unique.
Cause: A duplicate filesytem name is already in use.

Action: Pick a different filesystem 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 filesystem
Cause: The constructed path is missing or outside of the remote filesystem.

Action: Make sure remote location resolves to a valid directory on the remote filesystem.

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.

47411: Export *string* does not exist on remote filesystem.
Cause: The user attempts to mount a non-existing export on the remote filesystem.

Action: Make sure the export exists on the remote filesystem.

47481: Unable to load the generated certificate request.
Cause: Certificate request could not be loaded.

Action: Once again generate certificate request and try.

47482: Certificate requst is not compatible with server.
Cause: Certificate siging request and private key mismatch.

Action: Retry with a valid certificate signing request.

47483: Common Name(*string*) of the certificate request does not match with the host name(*string*).
Cause: Common Name of the certificate request has to be the same as the host name.

Action: Generate certificate request once again.

47484: IP address(*string*) of the certificate request does not match with the host IP address(*string*).
Cause: IP address of the certificate request has to be same as the host.

Action: Generate certificate request once again.

47485: Unable to validate *string* field of the certificate request.
Cause: Validation of the Specified field of certificate request failed.

Action: Generate certificate request once again.

47486: Common Name(*string*) of the certificate does not match with the host name(*string*).
Cause: Common Name of the certificate has to be the same as the host name.

Action: Modify the host name to match with Common Name of the certificate and retry.

47487: Certificate is not compatible with server.
Cause: Certificate and private key mismatch.

Action: Please upload certificate whose certificate signing request file was generated.

47488: Cannot restore the user uploaded certificate for UI.
Cause: The user uploaded certificate is not present.

Action: Please upload a new certificate.

47489: User uploaded certificate is already in use for UI.
Cause: The user uploaded certificate is already in use for UI.

Action: No action required.

47490: Certificate restore failed: Certificate is no longer valid.
Cause: The earlier uploaded certificate is not valid for UI.

Action: Please upload a new certificate.

47491: UI certificate management operation already in progress.
Cause: Another AVS UI certificate management operation is already in progress.

Action: Wait for the current operation to end before attempting another management operation.

47492: IP address(*string*) of the certificate does not match with the host IP address(*string*).
Cause: IP address of the certificate has to be same as the host.

Action: Modify the host IP address to match with IP address of the certificate and retry.

47493: The certificate has expired.
Cause: End date of certificate is more than system time.

Action: Try uploading another valid certificate.

47494: *string* is too long. Maximum allowed length is *string*.
Cause: Length validation check failed.

Action: Provide value with valid length.

47495: Invalid certificate. The certificate can't be null and the size of certificate should be less than 32KB
Cause: Certificate is more than 32767 bytes.

Action: Please provide a certificate with 1 to 32767 bytes.

47496: *string* cannot be a multi-byte character string.
Cause: Given string is multi-byte character string.

Action: Please use only ASCII characters.

47497: Issuer certificate of Firewall console with common name(*string*) is not part of AVS trusted certification authorities.
Cause: Issuer certificate of Firewall console certificate is not imported to AVS oracle wallet

Action: Please import the issuer certificate of Firewall console certificate to AVS oracle wallet

47498: Invalid Certificate. Issuer should use SHA-2 algorithm for signing.
Cause: Issuer should use a stronger algorithm for signing the CSR

Action: Please upload a certificate where the issuer have signed it using SHA-2 algorithm

47501: Traffic proxy '*string*' is in use.
Cause: Traffic proxy port is in use by another Enforcement Point.

Action: Please specify a different proxy port and try again.

47502: Enforcement Point with the specified name already exists.
Cause: Duplicate Enforcement Point name.

Action: Please specify a different name and try again.

47503: Cannot stop trail of type "*string*" at "*string*" for 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 target "*string*"; audit trail is already stopped. Audit trail no longer eligible for auto-start.
Cause: User attempted to stop a trail which is already stopped

Action: User cannot stop an audit trail which is already stopped

47505: Trail auto start invocation failed. Invoker unknown.
Cause: Unknown invoker

Action: Provide valid invoker e.g. 'AGENT' or 'DBJOB'.

47506: Error while setting up redo collector during start trail. Additional Info |*string*|
Cause: Internal Error.

Action: Check additional information to solve the problem or Contact Oracle Support Services.

47551: Invalid user name *string*. User name should be between 1 and 30 bytes long.
Cause: The user name spcified is 0 byte long, or more than 30 bytes.

Action: Provide a simple SQL name as user name between 1 and 30 bytes long.

47553: User name *string* is already in use. Please provide a different user name.
Cause: The user name already exists in the database.

Action: Provide a different simple SQL name as user name.

47571: Invalid host name *string*. Host name should be between 1 and 255 bytes long.
Cause: Host name is more than 255 byte.

Action: Please provide a host name with 1 to 255 bytes.

47572: Invalid host name *string*. The first and last characters of a host name cannnot be dots(.).
Cause: There is a leading and/or trailing dot in the host name.

Action: Please remove the leading and/or trailing dot.

47573: Invalid host name *string*. Host name can only contain the characters a-z, A-Z and dot(.).
Cause: Invalid characters in host name.

Action: Please provide a host name with characters from a-z, A-Z, 0-9, and dot(.).

47581: Invalid certificate. Certificate should be between 1 and 2048 bytes long.
Cause: Certificate is more than 2048 bytes.

Action: Please provide a certificate with 1 to 2048 bytes.

47582: Certificate has invalid format or contains illegal characters.
Cause: Certificate has invalid format or contains illegal characters.

Action: Please provide a valid certificate.

47583: Invalid certificate: *string*.
Cause: Certificate could not be verified.

Action: Please provide a valid certificate.

47584: Unable to load certificate
Cause: Certificate could not be loaded.

Action: Please provide a valid certificate.

47591: Remote system *string* is not accessible.
Cause: Remote system is not accessible.

Action: Please check the IP address or hostname.

47596: Failed to get the HA status of the remote AVS.
Cause: The HA status could not be verified.

Action: Please check the system log files for details.

47597: The primary and the standby system cannot have the same IP address.
Cause: The HA peer IP address is the same as the IP address of the current system.

Action: Please check the provided IP address.

47598: The system cannot use its own certificate.
Cause: The HA peer certificate is the same as the certificate of the current system.

Action: Please check the provided certificate.

47599: Data Encryption status is not compatible between primary and secondary.
Cause: When configuration HA, the encryption status must be the same.

Action: Please enable encryption and try again.

47621: The interval in UE retrieval has invalid value.
Cause: The interval value for retrieval of UE is invalid.

Action: Please input a valid interval value and submit again.

47622: The first run time in UE retrieval should not be in the past.
Cause: The start time for retrieval of UE is in the past.

Action: Please input a future start time and submit again.

47651: The interval in Audit Setting retrieval has invalid value.
Cause: The interval value for retrieval of audit setting is invalid.

Action: Please input a valid interval value and submit again.

47652: The first run time in Audit Setting retrieval should not be in the past.
Cause: The start time for retrieval of audit setting is in the past.

Action: Please input a future start time and submit again.

47671: The interval in SPA has invalid value.
Cause: The interval value for SPA is invalid.

Action: Please input a valid interval value and submit again.

47672: The first run time in SPA should not be in the past.
Cause: The start time for SPA is in the past.

Action: Please input a future start time and submit again.

47681: Oracle Database In-Memory is already enabled on the Audit Vault Server.
Cause: User is trying to enable Oracle Database In-Memory on an Audit Vault Server where Oracle Database In-Memory is already enabled.

Action: No action required.

47682: Oracle Database In-Memory is already disabled on the Audit Vault Server.
Cause: User is trying to disable Oracle Database In-Memory on an Audit Vault Server where Oracle Database In-Memory is already disabled.

Action: No action required.

47683: Value entered is higher than the maximum available for Database In-Memory, or less than 1 GB.
Cause: User entered an invalid memory size for Oracle Database In-Memory".

Action: Provide memory to Oracle Database In-Memory within allowable limit. Memory should be more than 1 GB and less than min((total system memory - 8GB), 90% of total system memory)).

47684: Oracle Database In-Memory: Internal error in *string*. Additional info |*string*|.
Cause: Internal error.

Action: Contact Oracle Support Services.

47685: Oracle Database In-Memory is not enabled on Audit Vault Server. Enable Oracle Database In-Memory on the Audit Vault Server before changing the In-Memory allocation.
Cause: User is trying to change memory for Oracle Database In-Memory while Oracle Database In-Memory is not enabled on Audit Vault Server."

Action: Enable Oracle Database In-Memory on Audit Vault Server before changing memory for Oracle Database In-Memory.

47686: The value entered (*string* GB) is the same as the current memory allocation for Oracle Database In-Memory. Enter a different value to change the allocation.
Cause: User is trying to change the memory allocation to Oracle Database In-Memory by entering a value that is the same as current value allocated.

Action: Provide a value for Oracle Database In-Memory allocation that is different from the current value allocated.

47687: Date range is not valid for Oracle Database In-Memory. Additional information: *string*.
Cause: User has provided an invalid date range for Oracle Database In-Memory.

Action: Provide a valid date range for Oracle Database In-Memory.

47688: Provided Oracle Database In-Memory size is not sufficient for date range. Increase the size of Oracle Database In-Memory or reduce the date range.
Cause: User has not provided enough memory to accommodate all the data into Oracle Database In-Memory for specified date range.

Action: Increase the size of memory provided to Oracle Database In-Memory or reduce the date range size.

47689: Error in *string* . Some other user is performing the same operation. Try *string* after some time
Cause: More than one user is trying to perform the same operation for Oracle Database In-memory.

Action: Try to perform the Oracle Database In-memory operations after some time.

47701: Invalid policy name: *string* ... Policy name should be between 1 and 255 bytes long.
Cause: Policy name is more than 255 bytes.

Action: Please provide a policy name with 1 to 255 bytes.

47702: Policy name cannot be null or the length is 0.
Cause: Policy name is null or the length of the policy name is 0 byte.

Action: Please provide a policy name with 1 to 255 bytes.

47751: The SNMP string is invalid. SNMP string must contain at least 8 characters and at most 30 characters, at least one uppercase letter(A-Z), one lowercase letter(a-z), one digit(0-9), and one special character(.,+:_!). SNMP string must not contain characters outside of a-z, A-Z, 0-9, and . , + : _ !.
Cause: SNMP string does not meet the policy.

Action: Please input a valid string and submit again.

47755: Built-in report *string* cannot be deleted.
Cause: User attempted to delete a built-in report.

Action: Built-in reports cannot be deleted.

47756: Report *string* cannot be deleted as you are not the owner of the report.
Cause: User attempted to delete a report uploaded by a different auditor.

Action: Users can only delete reports owned by them.

I.2 Database Firewall Messages

Learn about Database Firewall messages.

This table lists Database Firewall messages. These messages are captured in the `/var/log/messages` file.

ODF Code	Cause	Action
10000	Minimum number for the DBFW message codes	This message should never be seen. Please contact Oracle Support.
10001	Internal error	Please contact Oracle Support.
10100	The operation has completed successfully	No action required.
10101	Configuration change	A configuration change is being applied. No action required.
10102	Startup complete	The process has completed its initialization and is ready to perform work. No action required.
10103	Engine informational	Informational message only. No action required.
10104	ACE informational	Informational message only. No action required.
10105	Decoder informational	Informational message only. No action required.
10106	Connected to AVS	A connection has been successfully established to the Audit Vault Server. No action is required.
10107	TrafficTrace starting	The TrafficTrace logging system has started. No action is required.
10108	TrafficTrace data	The TrafficTrace logging system is logging data. No action is required.
10109	TrafficTrace stopping	The TrafficTrace logging system has stopped. No action is required.
10110	Process Metrics	Information about the performance of the process. No action is required.
10111	Traffic capture is enabled	Network traffic is being captured for diagnostic purposes. You should only see this message under the direction of Oracle support.
10112	Buffered Traffic written successfully	Buffered network traffic has been written to file for diagnostic purposes. No action is required.
10113	TCP connection successfully disrupted	A client TCP connection to the database has been successfully disrupted. This action was taken as the Database Firewall Monitoring Point is in monitoring and blocking mode, and the option to "Maintain Existing Connections" was not selected. No action is required.
10114	Stopped receiving heartbeat data	Information about the Database Firewall Monitoring Point. No action is required.

ODF Code	Cause	Action
10115	Nsi library version	Informational message about the Nsi library version. No action is required.
10116	Traffic capture initiated	Informational message only. No action is required.
10117	Logging of Process Metrics is enabled	Informational message only. No action is required.
10118	Session cache serialisation	Informational message only. No action is required.
10119	Successfully loaded the Diffie-Hellman parameters	Informational message only. No action is required.
10120	Additional memory allocation permitted	Informational message only. No action is required.
10121	Incrementing the maximum size the IPC buffer can grow up to.	Informational message only. No action is required.
10200	Internal error	None
10201	Internal error	None
10202	Internal error	None
10203	Internal error	None
10204	Internal error	None
10205	Internal error	None
10206	Internal error	None
10207	Internal error	None
10208	Internal error	None
10209	Internal error	None
10210	Internal error	None
10211	Internal error	None
10300	Host Monitor connected	A remote Host Monitor process has established a connection to the Database Firewall. No action required.
10301	Host Monitor disconnected	A remote Host Monitor process has disconnected from the Database Firewall. This is normal behavior if the Host Monitor has been stopped.
10302	Host Monitor not authorized	A Host Monitor has attempted to connect to the Database Firewall from an unauthorized source. Please investigate the source of this unexpected connection attempt.
10303	Authentication not enabled for HostMonitor connections - No certificate provided	No certificate has been provided to authenticate incoming connections from HostMonitor. Please see the documentation related to "Enabling and Using Host Monitoring" for information as to how to resolve this issue.
10400	No ASO records found	Check that database has been configured for ASO as per the instructions in the Administrator's Guide.
10401	ASO traffic will not be decrypted	ASO (encrypted) traffic to the database will not be decrypted. If you wish this traffic to be decrypted, follow the instructions in the Administrator's Guide.
10402	Delayed response to ASO request	The response to the ASO request was so delayed that the request was purged from the queue before the response was received. Verify that the Target is configured for ASO and is functioning correctly.

ODF Code	Cause	Action
10403	ASO is using unsupported encryption algorithm	ASO processing found the session is using unsupported encryption algorithm. If the Database Firewall Monitoring Point is configured in monitoring and blocking mode, the session is terminted. The message is decoded and SQL statements extracted when Database Firewall is in monitoring only mode.
10500	Unable to connect to AVS	A connection could not be established to the Audit Vault Server. This message will be seen in normal operation when the DBFW is first associated with the Audit Vault Server. If the message persists, or is seen under different circumstances then check the settings for the DBFW on the Audit Vault Server GUI.
10501	Failed connecting to the Target	Check the Target configuration. Check the Target host is running and prepared to accept connections.
10502	Failed connecting to remote database	Check the configuration for the remote database in question, and that it is running and prepared to accept connections.
10503	No connection to remote database	Check the connection configuration, and that the remote database is running and prepared to accept connections. Note that this may be due to temporary unavailability of the remote database.
10504	Network device error	Check the configuration of the network devices on the DBFW.
10505	Failed to resolve hostname	Check the DNS settings on your Appliance, and that the hostname is specified correctly.
10506	IP packet fragmented	An IP packet intercepted with Database Firewall in monitoring only mode was marked as fragmented. Check your network infrastructure to determine the cause of the fragmentation.
10507	TCP session re-use	A closed TCP session to the database has been re-opened. This could lead to state from the previous session being applied to the new session. No action required.
10508	Detected connection failure to AVS	A notification of message delivery has not been received for certain period of time. If the message persists then check the network connection between the Audit Vault Server and the Database Firewall (including router or firewall settings).
10509	Failed to find MAC address	Failed to find database MAC address. MAC address substitution will not work. Possible causes: database server is down or unreachable through specified traffic source; database server is connected to client port. Connect the database and firewall correctly, then reboot the firewall.
10510	The TCP connection to the AVS has been lost	Please check the network path between the DBFW and the AVS. Note that this problem may be seen when the AVS is restarted.
10511	IPC Communication Disrupted	Please see other messages in log file for more information.

ODF Code	Cause	Action
10512	A badly formed TCP URG packet was received	This problem has been seen in 'Fuzz-Testing' of the DBFW where bad TCP packets are transmitted. Please verify that the clients using the DBFW are behaving correcly.
10513	SSL handshake failed	An SSL client has failed to connect to the DBFW due to a failure in the initial handshake. Please examine the additional information in this message, and confirm that the client is correctly configured.
10514	Peer has reset the connection	The remote peer of this TCP session has reset the connection. Please ensure that the remote peer is behaving correctly. Note that although resetting a TCP connection is a hard close of the TCP session, it does not necessarily indicate that there is an error in the peer.
10515	TCP connection attempt has failed	An attempt to establish a TCP connection has failed. Please examine other related error messages to determine the context of this failure.
10516	Failed opening socket	An attempt to open a socket has failed. Please examine other related error messages to determine the context of this failure.
10517	DDI request failed	An attempt to query a protected database has failed. Please examine the details given in this message, as the problem may be as a result of mis-configuration. Are the confirured IP address and TCP port of the protected database correct? Have the correct username and password been supplied?
10518	Connection attempt to RAC failed	An attempt to conenct to a RAC database has failed. Please examine other related error messages to determine the context of this failure.
10519	Operation failed - Network is down	A network operartion has failed as the network is currently down. Please examine recent messages to see if a restart is in progress.
10520	A request was received from an unknown client	A client request was received from an unexpected source. If this message persists the source of the request must be verified. It may be an attempt to gain access to the data on this appliance.
10521	Inter-process communication failure	A local IPC communication attempt has failed. This is occasionally seen while the Database Firewall monitoring point processes are restarted. If this message persists, contact Oracle Support.
10522	No data received in TNS connection	A connection to an Oracle RAC node target on the Database Firewall did not send any data. This has been observed when a load balancer in front of the Database Firewall is checking the status of the Database Firewall by pings. A TCP connection which is closed immediately with no data being sent. If this is the case in the current environment, this message may be safely ignored. If your environment is not so configured, please contact Oracle support.

ODF Code	Cause	Action
10523	TCP Connection closed	A TCP connection has been closed. Examine the rest of the message to determine the cause. Note that if the cause is `Timeout`, the socket may have been closed due to the TCP keep alive mechanism detecting a dead peer.
10600	Invalid Target IP address	Ensure the Target IP address has been specified correctly in the GUI.
10601	Target clash	Two Targets with the same connection information (IP:port[:OSN]) have been specified in the GUI. Resolve this clash with the GUI, otherwise data may not be examined as expected.
10602	No MySql database name	The name of the MySql database has not been provided. Check the relevant configuration on the GUI and add the database name.
10603	Reboot now to apply new configuration (cannot apply configuration to running system)	The system management software failed to apply configuration to the running system. A reboot should apply the new settings. More information may be available in the debug log.
10604	Cannot generate new configuration file.	The system management software failed to generate the new configuration. Please contact Oracle Support.
10605	Cannot generate new configuration, please retry the operation	The system management software failed to generate the new configuration. Workaround given.
10606	Internal error, invalid configuration	Please contact Oracle Support.
10607	Value of system configuration rmem_max may be excessive	The value of the system setting rmem_max is unexpectedly high. On some hardware, it has been observed that this can lead to traffic not being intercepted as expected when Database Firewall is in monitoring only mode. Please verify that your system can support this value successfully.
10608	Invalid argument for certificate operation	Please check the parameters or files you have provided.
10609	Invalid certificate key pair	The uploaded certificate was not generated from the correct certificate signing request.
10610	Certificate Signing Request common name mismatch	The uploaded certificate does not match the original common name. Please verify your signing process.
10611	Error processing certificate	The uploaded certificate was not valid. Please check the uploaded certificate.
10612	Proxy-mode Database Firewall Monitoring Points clash	More than one Database Firewall Monitoring Point is configured to use the same proxy port. Please examine the Database Firewall Monitoring Points configured for this DBFW and resolve the conflict.
10613	LVM out of space, add more storage and try again	There is not enough storage available for the requested LVM operation. Please add more storage and try again.
10614	No TrafficTrace SQL statement provided in configuration file	Edit the configuration file and add the SQL against key TRACE_SQL
10615	Unable to parse the expiry time in configuration file	Edit the configuration file and enter the expiry time against key EXPIRES_AT in the format "yyyy-mm-dd hh:mm:ss". Example: "2015-11-23 12:13:14".

ODF Code	Cause	Action
10616	Expiry time has already passed	Edit the configuration file and alter the EXRIRES_AT time as desired
10617	TrafficTrace period set for greater than the permitted value	Edit the configuration file and alter the EXRIRES_AT time as desired
10618	Secure Transport string unrecognised	Edit the configuration file and alter the secure transport protocol string
10619	Insecure Transport protocol	Edit the configuration file and alter the secure transport protocol string to a more secure version
10620	There are public security vulnerabilities in this protocol version	Edit the configuration file and alter the secure transport protocol string to a more secure version, if that option is available in your deployment
10621	Secure Transport Protocols configured	This is an informational message. No action required.
10622	Database dialect does not support Oracle RAC	The selected dialect does not support Oracle RAC connections. Please correct the configuration by disabling RAC for this dialect.
10623	Oracle RAC is only supported for Database Firewall Monitoring Points in Proxy mode	The mode that the Database Firewall Monitoring Point is configured in does not support Oracle RAC. Please change the mode of the Database Firewall Monitoring Point, or turn off RAC support.
10624	Traffic from local IP address is not excluded from capture when Database Firewall is in monitoring only mode	Network traffic associated with IP addresses local to this machine are captured for analysis when Database Firewall is in monitoring only mode. Please note that this message should not be seen in real time deployments.
10625	Secure Transport configured	This is an informational message. No action required.
10626	Secure Transport Ciphers configured	This is an informational message. No action required.
10627	The agent could not be recompiled from the current configuration	The recompilation of the Agent software failed for an unspecified reason. There may be a problem with the Database, the Database Listener or the Java Framework. Contact Oracle Support if this message is seen on a Primary or Standalone server.
10628	The agent could not be recompiled from the current configuration because the database is down	The recompilation of the Agent software failed because the database is down. Contact Oracle Support if this message is seen on a Primary or Standalone server.
10629	Diffie-Hellman Named Group is not known	Please check the configuration to ensure the Diffie-Hellman Named Group is correct.
10630	The agent upgrade signal could not be sent because the database is down	The agents could not be signaled for upgrade at this time because the database was not available. The agent upgrade signal will need to be issued manually. Contact Oracle Support if this message is seen.
10631	The agent upgrade signal could not be sent because the command failed	The agents could not be signaled for upgrade at this time for an unknown reason. The agent upgrade signal will need to be issued manually. Contact Oracle Support if this message is seen.

ODF Code	Cause	Action
10632	The agent upgrade signal could not be disabled	The agents were signaled for upgrade but the target could not be disabled. The agent upgrade signal must be disabled manually. Run 'systemctl agent-signal-upgrade.service disable'.
10633	File missing from Certificate/ private key pair	Ensure that both the required certificate and private key have been provided.
10634	Device name not found on system	The supplied device name could not be found in the list of devices available on this appliance. Check the network device listings to ensure that all expected devices are present.
10635	Dhclient config file missing	The required configuration file could not be found. This may happen during install but should not happen during general runtime activities. If this message persists, contact Oracle Support.
10636	NTP query failed	Confirm that the configured NTP server (echoed in the message) is correct, and if required check the DNS is configured correctly.
10637	Data for stream not processed	Traffic has been observed destined for a database that is not configured for processing by this target, and the traffic is ignored. Alter your configuration so that stream can be processed.
10700	Internal cache full	Check the status of the Audit Vault Server associated with this DBFW, and that the AV Server and DBFW are correctly paired.
10701	Capture capacity exceeded for Database Firewall in monitoring only mode	Some network packets were not captured because the system was overloaded when Database Firewall is in monitoring only mode.
10702	Capacity exceeded	The system is not able to capture all the requested traffic with Database Firewall in monitoring only mode.
10703	Database Firewall in monitoring only mode capture capacity no longer exceeded	The system is now capturing all the requested traffic again when Database Firewall is in monitoring only mode. No action required.
10704	Internal capacity exceeded	Internal system capacity has been exceeded for the protected database. Please contact Oracle Support.
10705	SQL call failed	Check that database is running, that the configured user has permission to execute the statement and has access to the required resources.
10706	Syslog message too big	A message being processed for forwarding to the Audit Vault Server is too large to send. Please contact Oracle Support.
10707	Data truncation	The size of an item of data exceeded a limit and has been truncated.
10708	Failed sending StartMonitoring command to Arbiter	Unable to start the Arbiter process. Please examine the log file for other errors to determine the cause of this failure.
10709	Failed To Start Monitoring Processes	Please examine the debug log file for other errors to determine the cause of this failure.
10710	Internal capacity no longer exceeded	The system is now transferring all the requested traffic again when Database Firewall is in monitoring only mode. No action required.

ODF Code	Cause	Action
10711	Could not find service name information in connection string	The Oracle connection string did not contain recognizable service name information ("SERVICE_NAME" or "SID"). This means that such information will not be logged for display in any reports. If you require this information in reprorts, please alter the client's connection string appropriately.
10712	Syslog Fifo Closed	Informational message only. No action required.
10713	Failed connecting to the Policy Server	This message is sometimes seen in heavily loaded systems during the shutdown or restart of a Database Firewall Monitoring Point. No action required, unless this error is seen repeatedly.
10714	Failure in proxying to Oracle RAC database	There was a failure trying to establish a connection to a protected Oracle RAC database. Please examine recent previous messages to determine the cause of this failure.
10715	Failed sending Stitcher Count Object	This message is sometimes seen in heavily loaded systems during the shutdown or restart of a Database Firewall Monitoring Point. Please contact Oracle support if this error occurs repeatedly during routine operartion.
10716	Bad response to control command from Arbiter	This message is sometimes seen in heavily loaded systems during the shutdown or restart of a Database Firewall Monitoring Point. Please contact Oracle support if this error occurs repeatedly during routine operartion.
10717	Zero packets processed for Database Firewall in monitoring only mode	This message may be seen with Database Firewall in monitoring only mode when zero packets are processed in the event loop. This message is informational only, and has no effect of the performance of the system.
10718	Internal cache full. Possible slow transfer rate between the Database Firewall and the AVS	Check the network throughput between the Audit Vault Server associated with this Database Firewall, and that the number of alerts or syslog messages generated by this Database Firewall does not exceed the network capacity.
10719	Unable to load Session information from file	We were unable to load the cached Session information from file. In DAM mode, this may mean that some fields associated with long lived client connections may not be populated in reports.
10720	Unable to save Session information to file	This may be seen at startup. If it is seen continuously, please call Oracle support.
10721	Update of the Audit Vault Server connectivity flag intterrupted by a reload signal.	Informational message only. No action required.
10722	Failed determining policy	This may be seen at startup. If it is seen continuously, call Oracle support.
10723	Cache at capacity, evicting items	An internal cache has reached its maximum capacity, and entries are being evicted. This message should not be seen during normal functioning of the system. If this message is seen continuously, call Oracle support.

ODF Code	Cause	Action
10724	Potential alert not generated as policy not yet determined.	Under some circumstances the Database Firwall may want to test if an alert is to be issued for a SQL statement before the policy for that SQL statement has been determined. This can happen for the initial SQL statements involved in establishing connection to Oracle databases when the connection is encrypted with ASO.
10725	Unable to retrieve relevant session information.	This message may be emitted when the database session we are inquiring about has already been terminated, or is for other reasons not available from the protected database.
10726	RAC Proxy object present	An internal object was unexpectedly still in existance when it was expected that it should have been released by now. If this message is seen as part of a warning, look for previously logged warnings for an explanation. If this message is seen as part of an error, contact Oracle Support.
10727	Additional memory allocation denied	Informational message only. No action is required.
10728	Items being evicted from cache	Items are being evicted from internal cache. Examine the rest of the message for full details. If this message is seen continuously, call Oracle Support.

ODF Code	Cause	Action
10729	Platform certificates may expire soon. Refer to the required action against the specific ODF code mentioned in Oracle AVDF Administrators Guide.	Perform the following action for uninterrupted Oracle AVDF services. Regenerate the platform certificates on Audit Vault Server and Database Firewall by following these steps: 1. Log in to the appliance as *support* user. 2. Switch to root user using the command: `su root` 3. Run the following command to regenerate the certificate: `/usr/local/bin/gensslcert create-certs` 4. Run the following commands to restart the services on the Database Firewall appliance: • `systemctl stop httpd` • `systemctl start httpd` • `/usr/local/dbfw/bin/dbfwctl restart` • `systemctl stop stund` • `systemctl start stund` Run the following commands to restart the services on the Audit Vault Server appliance: • `systemctl stop httpd` • `systemctl start httpd` • `systemctl stop controller` • `systemctl start controller` • `systemctl stop dbfwlistener` • `systemctl start dbfwlistener` The platform certificates of Audit Vault Server or Database Firewall appliances are rotated or renewed for another year.
10800	Generic GUI information	Generic informational message. No action required.
10801	Generic GUI warning	Generic warning message. No action required.
10900	Invalid user credentials	The system does not recognize the account credentials (username, password)
10901	Failed to set password	The system has failed to set the password.
11000	Migration file result: success	This message is for audit trail and no specific action is required.
11001	Migration file invocation	This message is for audit trail and no specific action is required.
11002	Migration group invocation	This message is for audit trail and no specific action is required.
11003	Migration stanza invocation	This message is for audit trail and no specific action is required.
11004	Migration stanza result: success	This message is for audit trail and no specific action is required.
11005	Migration group result: success	This message is for audit trail and no specific action is required.

ODF Code	Cause	Action
11006	Migration file result: success	This message is for audit trail and no specific action is required.
11007	Migration stanza result: skipped	This message is for audit trail and no specific action is required.
11008	Please confirm you wish to start upgrade	Please read the following messages, and re-run this utility as follows to begin upgrade: /usr/bin/avdf-upgrade --confirm
11009	Please check before continuing	Power loss during upgrade may cause data loss. Do not power off during upgrade.
11010	Please check before continuing	This upgrade will erase /root and /images.
11011	Please check before continuing	Please review Note ID 2235931.1 for a current list of known issues.
11012	The install or upgrade has completed successfully	This message is for audit trail and no specific action is required.
11013	Last migration: success	No further action needed.
11014	Last migration: started	The upgrade is in progress or was interrupted. Please wait until the upgrade completes or contact support.
11015	Last migration: failed	Please fix the failure cause. Migration is rerunnable and can be executed again.
11016	Last migration: failed	Please review /var/log/messages and /var/log/debug for more information. Perform the actions necessary to get the system to the expected final state of migration.
11017	Attempt to resume upgrade without confirmation	Confirm that you have fixed the original error cause by running the tool again with --confirm option.
11018	Attempt to resume upgrade without confirmation	Confirm that you have fixed the original error cause by running the tool again with --confirm option. WARNING: resuming upgrade on an unfixed system may further corrupt it.
11019	Attempt to resume upgrade when not in recovery mode	The system is not in recovery mode. There is nothing to resume.
11030	Migration file result: completed with warnings	Please download the diagnostics package and contact Oracle support. Please review /var/log/messages and /var/log/debug for more information. To download the diagnostics package please follow the instructions from the documentation.
11031	Cannot resume upgrade or install: migration file does not match hash	The migration index does not validate with the given hash, so it is not possible to resume the install or upgrade. Please generate a new hash if you are using a new migration index.
11060	Migration file result: FATAL ERROR - TERMINATED	Please do not use this system in a production environment. Please download the diagnostics package and contact Oracle support. Please review /var/log/messages and /var/log/debug for more information. To download the diagnostics package please follow the instructions from the documentation.

ODF Code	Cause	Action
11061	Migration group result: failed	Please do not use this system in a production environment. Please download the diagnostics package and contact Oracle support. Please review /var/log/messages and /var/log/debug for more information. To download the diagnostics package please follow the instructions from the documentation.
11062	Migration stanza result: failed to start because its preconditions were not met	Please do not use this system in a production environment. Please download the diagnostics package and contact Oracle support. Please review /var/log/messages and /var/log/debug for more information. To download the diagnostics package please follow the instructions from the documentation.
11063	Migration file result: incomplete	Please download the diagnostics package and contact Oracle support. Please review /var/log/messages and /var/log/debug for more information. To download the diagnostics package please follow the instructions from the documentation.
11064	The install or upgrade is incomplete	Please download the diagnostics package and contact Oracle support. Please review /var/log/messages and /var/log/debug for more information. To download the diagnostics package please follow the instructions from the documentation.
11065	Failed to execute migrations	Please review /var/log/messages and /var/log/debug for more information.
19999	Maximum number for the DBFW message codes	This message should never be seen. Please contact Oracle Support.
99999	The code for this message is the maximum permitted number	This message should never be seen. Please contact Oracle Support.

I.3 Agent Messages

Learn about Audit Vault Agent messages.

OAV Message Code	Message Description
6001	Activation request failed.
6002	Error reading the bootstrap configuration file: "string".
6011	Error while reading Agent configuration from server.
6012	Activation key validation failed. Check Audit Vault Server console for activation key.
6013	Agent status update failed.
6014	Agent host is invalid. Register the Agent host.
6016	Agent host is not registered with IP "string". Register the Agent host.
6021	Error validating activation key. Check Audit Vault Server console for activation key.
6022	Agent started successfully.
6024	Activation key required. Check Audit Vault Server console for activation key.

OAV Message Code	Message Description
6025	Agent is already activated.
6026	An instance of the Agent is already running.
6027	Stopping Agent...
6028	Internal Error. See logs for more details.
6029	Agent stop was already requested. Wait for the Agent to stop.
6030	Agent is not running.
6031	Agent is unable to connect to database server. Make sure the database server is up and the Agent is activated.
6032	Invalid activation key. Check Audit Vault Server console for activation key.
6033	Agent is unable to access the Agent home directory. Check if the Agent home directory exists and if the Agent user has relevant permissions to the directory.
6035	Invalid activation key. Maximum allowed attempts reached. Reactivate Agent in Audit Vault Server console.
6036	Agent is unable to determine the platform.
6037	Agent updated successfully.
6038	Plugin file validation failed.
6040	Error: There is more than one plugin with the same ID. Undeploy duplicate plugin in Audit Vault Server console.
6041	Error occurred while fetching plugin from server. See logs for more details.
6042	Error occurred while updating Agent generation timestamp. See logs for more details.
6043	Error occurred while updating plugin inventory for plugin : "string".
6044	Error occurred while resetting plugin inventory.
6045	Error occurred while updating Agent version.
6046	Checking for updates...
6047	Agent is updating. This operation may take a few minutes. Please wait...
6052	The Agent must be started with an activation key. Check Audit Vault Server console for activation key.
6053	Agent setup validation failed. Check logs for more details.
6054	A newer version of the Agent is available on the Audit Vault Server. Update the Agent manually.
6055	The activate command has been deprecated.
6056	Host Monitor upgrade failed.
6057	Agent integrity check failed. Upgrade the Agent manually.
6058	Failed to update Host Monitor state on the Audit Vault Server.
6059	Host Monitor update failed. See logs for more details.
6060	Trail auto start failed. See server trace logs for more details.
6061	Error while reading host attributes from server.
6062	Potential insecure PATH "string". Ensure directories in PATH are not modifiable by others and PATH does not have more than 5 levels of symbolic links.
6063	Invalid PATH "string".

OAV Message Code	Message Description
6064	Agent has connected to standby Audit Vault Server. Purging the old connection pool and trying to connect to primary Audit Vault Server.
6065	Execution of command "string" failed with error code "string".
6066	Execution of command "string" failed.
6067	Error while unzipping file "string".
6068	Error while updating bootstrap file "string".
6070	Error while checking if Host Monitor is supported on current platform.
6071	Error while retrieving Host Monitor state.
6072	Agent username is not present in wallet. Unable to update wallet.
6073	Error while copying new wallet to wallet location.
6074	Error while deleting directory "string".
6075	Error updating Agent certificate expiry date.
6076	Agent update failed after "string" retries.
6077	Error while calculating hash for file "string".
6078	Error while getting plugin updates.
6079	Invalid IP address "string" in bootstrap file.
6080	Invalid port "string" in bootstrap file.
6081	Error while downloading bootstrap file from Audit Vault Server.
6082	Error occurred during install/upgrade. Check log files for more information.
6083	Agent home directory contains invalid characters "string".
6084	Error occured during upgrade. Uninstall Host Monitor and retry.
6085	Error occurred while creating "string". Check log files for more information.
6086	Agent upgrade failed.
6087	Agent host must be registered before an agent can be installed or upgraded. Agent deployment failed.
6088	Error while uploading agent logs to AV Server. Please see agent logs for more details.
6089	Host name returned by AV Server is null.
11300	The activation key cannot be entered in the Agent start command. Enter 'agentctl start -k'.
8002	Internal Collector "string":"string" Error .
8004	Failed to start collector "string":"string".
8005	Failed to establish connection to target for "string". Check if you can connect to target using connection string.
8006	Failed to disconnect from "string".
8008	Failed to establish connection to Audit Vault Server for "string".
8009	Invalid arguments.
8010	Query not found "string".
8012	Error creating AuditEventCollector instance.
8013	Collector class not found "string".
8014	Could not cast the Collector class to AuditEventCollector "string".
8015	Error initializing AuditEventCollector instance.
8016	Error loading SQL properties file "string".

OAV Message Code	Message Description
8017	Illegal arguments in start trail command "string".
8018	Error sending records to server.
8019	Error setting checkpoint.
8020	Error fetching data from server.
8021	Error fetching information from plugin manifest file "string".
8023	Failed to get valid template file from template directory: "string". Check if valid template file exists.
8025	Mapping not specified for mandatory field: "string" in template file. Refer "string" for more information.
8026	Invalid target field name: "string" in template file. Check if field exists on the target.
8027	Trail name is NULL from collector context. Specify valid trail name during trail creation.
8028	Target name is NULL from collector context. Specify valid target name during trail creation.
8030	Source version is NULL. Specify valid target version in Targets tab - Audit Collection Attributes tab for the key AV.COLLECTOR.SECUREDTARGETVERSION.
8031	Invalid attribute name: "string". Check if valid attribute is present in Targets tab - Audit Collection Attributes tab.
8032	Error setting attribute: "string". Check if attribute key and value are valid.
8033	Source Field: "string" has incompatible datatype: "string". Check if target field has valid data type.
8034	Error getting data from target.
8036	Source Type is NULL. Check securedTargetType in template file.
8037	Invalid Trail name. Specify valid trail name during trail creation.
8038	Invalid Document object. Check if valid template file exists.
8039	Failed to parse audit file: "string". Check if the audit file is valid and if Agent user has read permissions on the audit file.
8040	Failed to read audit file: "string". Check if the audit file is valid and if Agent user has read permissions on the audit file.
8041	No Template files present in directory: "string".
8042	No read permission on directory: "string". Provide read permission to Agent user on the directory.
8043	Invalid Template File: "string".
8044	Invalid directory path: "string". Check if directory exists and if Agent user has relevant permissions on the directory.
8046	Value transformation rules not specified for mandatory Audit Vault Server field: "string" in template file. Refer "string" for more information.
8047	Invalid Source version format : "string". Check target version in template file.
8048	SQL Server version "string" not supported.
8049	NULL event time timezone offset from collector context. Specify valid timezone offset in Targets tab - Audit Collection Attributes tab for the key AV.COLLECTOR.TIMEZONEOFFSET.
8051	This Auditing system is not supported by the collector. Specify supported trail type during trail creation.

OAV Message Code	Message Description
8052	Error writing checkpoint to collector ATC file: "string". Check if ATC file exists and if Agent user has write permission on ATC file.
8054	Invalid Target Version: "string". Check if target version is supported by template file.
8055	Invalid Target Platform: "string". Check documentation to see if target operating system is supported.
8057	Unauthorized user to access service : "string".
8058	Invalid Audit Service : "string".
8059	Invalid OAuth 2.0 "string".
8060	Invalid REST Authentication setup.
8061	Invalid Trail Extension. Supported extension is "string".
8062	Registered target is not a CDB container. Provide connection details of CDB container in Targets tab in Audit Vault console.
8064	Could not find Java charset for database charset "string".
8065	Unable to get database charset information either from source or collection attribute. Specify valid java character set in Targets tab - Audit Collection Attributes tab for attribute AV.COLLECTOR.DATABASECHARSET.
8066	Unable to read database charset from database.
8067	Template file "string" has no document element.
8068	Invalid audit trail location format : The format should be <hostname>:<location of OS log files>.
9001	Sybsecurity database not configured.
9003	Error getting active table position.
9004	Error getting list of configured audit tables.
9005	Error constructing marker due to unknown hashing algorithm.
9006	Active table "string" is not present in configured audit table list.
9008	Configured Audit table list is empty.
11000	Cannot read the directory. Check if directory exists and if Agent user has relevant permissions on the directory.
11200	Audit Package Version is not supported.

J

Security Technical Implementation Guides

Oracle Audit Vault and Database Firewall follows the Security Technical Implementation Guides (STIG)-based compliance standards.

J.1 About Security Technical Implementation Guides

Learn about Security Technical Implementation Guides.

A Security Technical Implementation Guide (STIG) is a methodology followed by the U.S. Department of Defense (DOD) to reduce the attack surface of computer systems and networks, thereby ensuring a lockdown of highly confidential information stored within the DOD network. STIGs provide secure configuration standards for the DOD's Information Assurance (IA) and IA-enabled devices and systems. STIGs are created by the Defense Information Systems Agency (DISA).

For over a decade, Oracle has worked closely with the DOD to develop, publish, and maintain a growing list of STIGs for a variety of core Oracle products and technologies including:

- Oracle Database
- Oracle Solaris
- Oracle Linux
- Oracle WebLogic

When STIGs are updated, Oracle analyzes the latest recommendations in order to identify new ways to improve the security of its products by:

- Implementing new and innovative security capabilities that are then added to future STIG updates
- Delivering functionality to automate the assessment and implementation of STIG recommendations

After you enable the STIG guidelines in Oracle Audit Vault and Database Firewall, the settings are preserved when you perform any upgrades.

Improving "out of the box" security configuration settings based upon STIG recommendations

STIG recommendations

Oracle Audit Vault Server is a highly tuned and tested software appliance. Any additional software installed on this server can cause unstable behavior. Hence Oracle does not recommend the installation of any software on Oracle Audit Vault Server. If there are requirements for virus scan, then utilize external scanners as much as possible.

The following are some cases where external scanners cannot be utilized and an Anti-virus is installed on the Audit Vault Server:

- If there is an issue, then Oracle support may request that the user uninstall the Anti-virus software to enable troubleshooting.
- If there are no issues and there is a new Bundle Patch to be applied for Oracle Audit Vault and Database Firewall, then Oracle support may request that you uninstall the anti-virus

software, apply the patch, and then re-install the anti-virus software on Oracle Audit Vault Server. This reduces some of the issues after applying the patch.

- If there are no issues but the anti-virus scanner has detected a virus or malware, then you should contact the anti-virus scanner vendor to verify the validity of the finding.
- If the anti-virus software was not removed in advance and the Bundle Patch upgrade has failed, then Oracle may recommend a fresh installation of Oracle Audit Vault and Database Firewall and a consequent Bundle Patch upgrade. Only after this the anti-virus scanner can be re-installed.
- If the customer followed the instructions from Oracle, the anti-virus scanner does not uninstall completely, and the Bundle Patch upgrade fails, contact the anti-virus vendor for instructions on how to remove their software completely. Once this is completed Oracle Audit Vault and Database Firewall Bundle Patch should be installed. If the install fails, then a clean install may be warranted.

See Also:

- Oracle Database STIG
- Oracle Linux STIG
- DISA STIG Home

J.2 Enabling and Disabling STIG Guidelines on Oracle Audit Vault and Database Firewall

You can enable STIG guidelines on Oracle Audit Vault and Database Firewall by enabling Strict mode.

J.2.1 Enabling STIG Guidelines on Oracle Audit Vault and Database Firewall

Learn how to enable STIG guidelines on Oracle Audit Vault and Database Firewall.

To enable strict mode:

1. Log in to the operating system of Oracle Audit Vault Server as the root user.
2. Run the following command as `root`:

```
/usr/local/dbfw/bin/stig --enable
```

J.2.2 Disabling STIG Guidelines on Oracle Audit Vault and Database Firewall

Learn how to disable STIG guidelines on Oracle Audit Vault and Database Firewall.

To disable strict mode:

1. Log in to the operating system of Oracle Audit Vault Server as the root user.

2. Run the following command as root:

```
/usr/local/dbfw/bin/stig --disable
```

J.3 Current Implementation of STIG Guidelines on Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall is security-hardened because the configurations follow Security Technical Implementation Guide (STIG) recommendations.

Oracle has developed a security-hardened configuration of Oracle Audit Vault and Database Firewall that supports U.S. Department of Defense Security Technical Implementation Guide (STIG) recommendations.

Table J-1 lists the three vulnerability categories of the STIG.

Table J-1 Vulnerability Categories

Category	Description
CAT I	Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

J.4 Current Implementation of Database STIG Guidelines

Learn about the current implementation of database STIG guidelines on Oracle Audit Vault and Database Firewall.

Table J-2 shows the current implementation of Database STIG guidelines on Oracle Audit Vault and Database Firewall.

Table J-2 Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
DG0004-ORACLE11	DBMS application object owner accounts	CAT II	No	No	None	No	Application object owner accounts `AVSYS`, `MANAGEMENT`, `SECURELOG` are locked after the installation of Oracle Audit Vault and Database Firewall.

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
DG0008-ORACLE11	DBMS application object ownership	No	No	Yes	No	No	For more information, see DG0008-ORACLE11 STIG Guideline.
DG0014-ORACLE11	DBMS demonstration and sample databases	CAT II	No	No	None	No	All default demonstration and sample database objects have been removed.
DG0071-ORACLE11	DBMS password change variance	CAT II	No	No	No	No	Currently not supported
DG0073-ORACLE11	DBMS failed login account lock	CAT II	Yes	No	No	No	`MONITORING_PROFILE` no longer exists in Oracle Audit Vault and Database Firewall 12.2. For other profiles, `FAILED_LOGIN_ATTEMPTS` is set to the required limit in the script. Setting `FAILED_LOGIN_ATTEMPTS` to 3 will expose the AVS system to denial of service (DoS) attack.
DG0075-ORACLE11	DBMS links to external databases	CAT II	No	Yes	No	No	For more information, see DG0075-ORACLE11 and DO0250-ORACLE11 STIG Guidelines.
DG0077-ORACLE11	Production data protection on a shared system	CAT II	No	No	None	No	No
DG0116-ORACLE11	DBMS privileged role assignments	CAT II	Yes	Yes	No	No	Revoked `DBFS_ROLE` from `AV_ADMIN`. For more information, see DG0116-ORACLE11 STIG Guideline.
DG0117-ORACLE11	DBMS administrative privilege assignment	CAT II	No	No	No	No	Currently not supported
DG0121-ORACLE11	DBMS application user privilege assignment	CAT II	No	No	No	No	Currently not supported
DG0123-ORACLE11	DBMS Administrative data access	CAT II	No	No	No	No	Currently not supported

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
DG0125-ORACLE11	DBMS account password expiration	CAT II	Yes	No	No	No	`MONITORING_PROFILE` no longer exists in Oracle Audit Vault and Database Firewall 12.2. For other profiles, `PASSWORD_LIFE_TIME` is set to the required limit in the script.
DG0126-ORACLE11	DBMS account password reuse	CAT II	No	No	None	No (Oracle AVDF 20.1 - 20.12) Yes (Oracle AVDF 20.13 and later)	Password reuse is not allowed on Oracle Audit Vault and Database Firewall.
DG0128-ORACLE11	DBMS default passwords	CAT I	Yes	No	No	No	Account `OWBSYS_AUDIT` no longer exists in Oracle Audit Vault and Database Firewall 12.2. Accounts such as `CTXSYS` , `AUDSYS`, `DBSNMP`, and `ORDSYS` are assigned a random password in the script.
DG0133-ORACLE11	DBMS Account lock time	CAT II	Yes	No	No	No	No

DG0141-ORACLE11	DBMS access control bypass	CAT II	Yes	No	No	No	Users can use a script to audit the following events:
							`DROP ANY SYNONYM`
							`DROP ANY INDEXTYPE`

DG0142-ORACLE11	DBMS Privileged action audit	CAT II	No	No	None	No	No

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
DG0192-ORACLE11	DBMS fully-qualified name for remote access	CAT II	Yes	No	No	No	Currently not supported
DO0231-ORACLE11	Oracle application object owner tablespaces	CAT II	No	No	No	No	Currently not supported
DO0250-ORACLE11	Oracle database link usage	CAT II	No	Yes	No	No	For more information, see DG0075-ORACLE11 and DO0250-ORACLE11 STIG Guidelines.
DO0270-ORACLE11	Oracle redo log file availability	CAT II	No	No	No	No	Currently not supported
DO0350-ORACLE11	Oracle system privilege assignment	CAT II	No	No	No	No	Currently not supported
DO3475-ORACLE11	Oracle `PUBLIC` access to restricted packages	CAT II	No	No	No	No	Currently not supported
DO3536-ORACLE11	Oracle `IDLE_TIME` profile parameter	CAT II	Yes	No	No	No	No
DO3540-ORACLE11	Oracle `SQL92_SECURITY` parameter	CAT II	No	No	None	No	Parameter `SQL92_SECURITY` is already set to `TRUE`.
DO3609-ORACLE11	System privileges granted WITH ADMIN OPTION	CAT II	No	No	No	No	Currently not supported
DO3610-ORACLE11	Oracle minimum object auditing	CAT II	No	No	No	No	Currently not supported
DO3689-ORACLE11	Oracle object permission assignment to PUBLIC	CAT II	No	No	No	No	Currently not supported
DO3696-ORACLE11	Oracle RESOURCE_LIMIT parameter	CAT II	No	No	No	No	Currently not supported
O121-BP-021900	The Oracle `REMOTE_OS_AUTHENT` parameter must be set to *FALSE*.	CAT I	No	No	No	Yes	None
O121-BP-022000	The Oracle `REMOTE_OS_ROLES` parameter must be set to *FALSE*.	CAT I	No	No	No	Yes	None
O121-BP-022700	The `Oracle Listener` must be configured to require administration authentication.	CAT I	No	No	No	Yes	None

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
O121-C1-004500	DBA OS accounts must be granted only those host system privileges necessary for the administration of the DBMS.	CAT I	No	No	No	Yes	In Audit Vault and Database Firewall, only Oracle user can connect to the database as *SYSDBA*. Oracle user is granted only necessary privileges.
O121-C1-011100	Oracle software must be evaluated and patched against newly found vulnerabilities.	CAT I	No	No	No	No	Apply Audit Vault and Database Firewall release quarterly bundle patch which patches OS, DB, and Java on the Audit Vault Server and Database Firewall.
O121-C1-015000	DBMS default accounts must be assigned custom passwords.	CAT I	Yes	No	No	Yes	*DVSYS* is assigned custom password in product. Other users are assigned passwords through the STIG script.
O121-C1-015400	The DBMS, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	CAT I	No	No	No	Yes	None
O121-C1-019700	The DBMS must employ cryptographic mechanisms preventing the unauthorized disclosure of information during transmission unless the transmitted data is otherwise protected by alternative physical measures.	CAT I	No	No	No	Yes	On Audit Vault Server, the following list of encryption algorithms is set in *sqlnet.ora: SQLNET.ENCRYPTION_TYPES_SERVER = (AES256,AES192,AES128)*. The communication between agent and the Audit Vault Server is encrypted.
O121-N1-015601	Applications must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.	CAT I	No	No	No	Yes	All passwords in Audit Vault and Database Firewall are either stored in Oracle Wallet or encrypted in the database. All passwords are sent through encrypted channel.

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
O121-N1-015602	When using command-line tools such as Oracle SQL*Plus, which can accept a plain-text password, users must use an alternative login method that does not expose the password.	CAT I	No	No	No	Cannot completely comply.	Audit Vault and Database Firewall has a command line interface AVCLI. The password can be typed clearly without any issue. However AVCLI also provides an alternative login method which does not expose the password as clear text.
O121-OS-004600	Use of the DBMS software installation account must be restricted to DBMS software installation.	CAT I	No	No	No	Yes	None
O121-BP-021300	Oracle instance names must not contain Oracle version numbers.	CAT II	No	No	No	Yes	None
O121-BP-021400	Fixed user and public database links must be authorized for use.	CAT II	No	See Note.	No	No	See note
O121-BP-022100	The Oracle *SQL92_SECURITY* parameter must be set to *TRUE*.	CAT II	No	No	No	Yes	None
O121-BP-022200	The Oracle `REMOTE_LOGIN_PASSWORDFILE` parameter must be set to *EXCLUSIVE* or *NONE*.	CAT II	No	No	No	Yes	None
O121-BP-022300	System privileges granted using the `WITH ADMIN OPTION` must not be granted to unauthorized user.	CAT II	No	No	No	Yes	None
O121-BP-022400	System privileges must not be granted to `PUBLIC` role.	CAT II	No	No	No	Yes	None
O121-BP-022500	Oracle roles granted using the `WITH ADMIN OPTION` must not be granted to unauthorized accounts.	CAT II	No	No	No	Yes	None
O121-BP-022600	Object permissions granted to `PUBLIC` role must be restricted.	CAT II	No	No	No	Yes	None
O121-BP-022800	Application role permissions must not be assigned to the Oracle `PUBLIC` role.	CAT II	No	No	No	Yes	None

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
O121-BP-023000	Connections by mid-tier web and application systems to the Oracle DBMS must be protected, encrypted, and authenticated according to database, web, application, enclave, and network requirements.	CAT II	No	No	No	Yes	None
O121-BP-023200	Unauthorized database links must not be defined and left active.	CAT II	No	See Note.	No	No	See note
O121-BP-023600	Only authorized system accounts must have the `SYSTEM` table space specified as the default table space.	CAT II	No	No	No	Yes	None
O121-BP-023900	The Oracle `_TRACE_FILES_PUBLIC` parameter if present must be set to *FALSE*.	CAT II	No	No	No	Yes	None
O121-BP-025200	Credentials stored and used by the DBMS to access remote databases or applications must be authorized and restricted to authorized users.	CAT II	No	See Note.	No	No	See note
O121-BP-025700	DBMS data files must be dedicated to support individual applications.	CAT II	No	No	No	Yes	None
O121-BP-025800	Changes to configuration options must be audited.	CAT II	No	No	No	Yes	None
O121-BP-026600	Network client connections must be restricted to supported versions.	CAT II	No	No	No	Yes	The following parameter in *sqlnet.ora* on the Audit Vault Server is set to `SQLNET.ALLOWED_LOGON_VERSION_SERVER = 11`
O121-C2-002100	The DBMS must automatically disable accounts after a period of 35 days of account inactivity.	CAT II	Yes	No	No	No	None
O121-C2-003000	The DBMS must enforce Discretionary Access Control (DAC) policy allowing users to specify and control sharing by named individuals, groups of individuals, or by both, limiting propagation of access rights and including or excluding access to the granularity of a single user.	CAT II	No	No	No	Yes	None

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
O121-C2-003400	DBMS processes or services must run under custom and dedicated OS accounts.	CAT II	No	No	No	Yes	None
O121-C2-003600	A single database connection configuration file must not be used to configure all database clients.	CAT II	No	No	No	Yes	None
O121-C2-004900	The DBMS must verify account lockouts and persist until reset by an administrator.	CAT II	Addressed in Audit Vault and Database Firewall 12.2.0.1.0 STIG script.	No	No	No	None
O121-C2-006700	A DBMS utilizing Discretionary Access Control (DAC) must enforce a policy that includes or excludes access to the granularity of a single user.	CAT II	No	No	No	Yes	None
O121-C2-006900	The DBMS must allow designated organizational personnel to select specific events that can be audited by the database.	CAT II	No	No	No	Yes	None
O121-C2-011500	Default demonstration, sample databases, database objects, and applications must be removed.	CAT II	No	No	No	Yes	None
O121-C2-011600	Unused database components, DBMS software, and database objects must be removed.	CAT II	No	No	No	Yes	None
O121-C2-011700	Unused database components that are integrated in the DBMS and cannot be uninstalled must be disabled.	CAT II	No	No	No	Yes	None
O121-C2-013800	The DBMS must support organizational requirements to disable user accounts after a defined time period of inactivity set by the organization.	CAT II	Yes	No	No	No	None
O121-C2-014600	The DBMS must support organizational requirements to enforce password encryption for storage.	CAT II	No	No	No	Yes	None

Table J-2 (Cont.) Current Implementation of Database STIG Guidelines

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
O121-C2-015100	DBMS passwords must not be stored in compiled, encoded, or encrypted batch jobs or compiled, encoded, or encrypted application source code.	CAT II	No	No	No	Yes	None.
O121-C2-015200	The DBMS must enforce password maximum lifetime restrictions.	CAT II	Yes	No	No	No	None

> **Note:**
>
> The use of the DB link has already been documented in Audit Vault and Database Firewall 12.2.0.1.0 STIG documentation.

J.5 Additional STIG Guideline Notes

Learn about additional advice regarding STIG guidelines.

Related Topics

- Current Implementation of Database STIG Guidelines
  Learn about the current implementation of database STIG guidelines on Oracle Audit Vault and Database Firewall.

J.5.1 DG0008-ORACLE11 STIG Guideline

Learn about STIG guideline DG0008-ORACLE11.

Object owner accounts in Audit Vault Server:

- `APEX`
  - `APEX_180200 (Oracle AVDF 20.1 to 20.3)`
  - `APEX_200100 (Oracle AVDF 20.4 to 20.5)`
  - `APEX_210100 (Oracle AVDF 20.6 and later)`
- `MANAGEMENT`
- `AVRULEOWNER`
- `SECURELOG`
- `AVREPORTUSER`
- `AVSYS`

Object owner accounts in Database Firewall:

- MANAGEMENT
- SECURELOG

J.5.2 DG0075-ORACLE11 and DO0250-ORACLE11 STIG Guidelines

Learn about STIG guidelines DG0075-ORACLE11 and DO0250-ORACLE11.

Database links used on Oracle Audit Vault Server:

```
AVRPTUSR_LINK.DBFWDB:
 (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=127.0.0.1)(PORT=1521))
 (CONNECT_DATA=(SERVICE_NAME=dbfwdb)))
```

The database link is created during installation of Oracle Audit Vault Server and is used by the REDO collector.

J.5.3 DG0116-ORACLE11 STIG Guideline

Learn about STIG guideline DG0116-ORACLE11.

Table J-3 lists accounts and role assignments in Audit Vault Server.

Table J-3 Accounts and Role Assignments in Audit Vault Server

Account	Role Assignment
AV_ADMIN	AQ_ADMINISTRATOR_ROLE SELECT_CATALOG_ROLE XDBADMIN
AV_AUDITOR	SELECT_CATALOG_ROLE
AV_MONITOR	SELECT_CATALOG_ROLE
AV_SOURCE	AQ_USER_ROLE
HS_ADMIN_ROLE	HS_ADMIN_EXECUTE_ROLE HS_ADMIN_SELECT_ROLE
OEM_MONITOR	SELECT_CATALOG_ROLE

Table J-4 lists accounts and role assignments in Database Firewall.

Table J-4 Accounts and Role Assignments in Database Firewall

Account	Role Assignment
HS_ADMIN_ROLE	HS_ADMIN_EXECUTE_ROLE HS_ADMIN_SELECT_ROLE
OEM_MONITOR	SELECT_CATALOG_ROLE

J.6 Current Implementation of Operating System STIG Guidelines

This topic contains information on the current implementation of operating system STIG guidelines for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Table J-5 Operating System STIG Guideline Set Reference

Reference	Detail
Document	Oracle Linux 8 Security Technical Implementation Guide
Version	1
Release	5
Release date	January 13, 2023
Document link	Oracle Linux Security Technical Implementation Guide

Table J-6 User Action - Definition and Guidelines

User Action	Description of the Guideline
None	The guideline is implemented by default and no user action is required.
Enable *strict* mode	The guideline can be implemented by switching the appliance to *strict* mode.

> **See Also:**
>
> Enabling and Disabling STIG Guidelines on Oracle Audit Vault and Database Firewall

Site policy	The guideline can be implemented depending on local policy and it requires administrator action. See the **Notes** column for additional information on implementation.
Administrative task	The guideline implementation is an administrator configuration action after installation or upgrade. It can also be a regularly used and defined administrative procedure.

Table J-7 Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-010000	CAT I	-	OL 8 must be a vendor-supported release.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-010140	CAT I	-	OL 8 operating systems booted with United Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user mode and maintenance.	Implemented by default
OL08-00-010150	CAT I	-	OL 8 operating systems booted with a BIOS must require authentication upon booting into single-user and maintenance modes.	Implemented by default
OL08-00-010370	CAT I	-	YUM must be configured to prevent the installation of patches, service packs, device drivers, or OL 8 system components that have not been digitally signed using a certificate that is recognized and approved by the organization.	Implemented by default
OL08-00-010460	CAT I	-	There must be no "shosts.equiv" files on the OL 8 operating system.	Implemented by default
OL08-00-010470	CAT I	-	There must be no ".shosts" files on the OL 8 operating system.	Implemented by default
OL08-00-010820	CAT I	-	Unattended or automatic logon via the OL 8 graphical user interface must not be allowed.	Implemented by default
OL08-00-010830	CAT I	-	OL 8 must not allow users to override SSH environment variables.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-020330	CAT I	-	OL 8 must not allow accounts configured with blank or null passwords.	Implemented by default
OL08-00-020331	CAT I	-	OL 8 must not allow blank or null passwords in the system-auth file.	Implemented by default
OL08-00-020332	CAT I	-	OL 8 must not allow blank or null passwords in the password-auth file.	Implemented by default
OL08-00-040000	CAT I	-	OL 8 must not have the telnet-server package installed.	Implemented by default
OL08-00-040010	CAT I	-	OL 8 must not have the rsh-server package installed.	Implemented by default
OL08-00-040171	CAT I	-	The x86 Ctrl-Alt-Delete key sequence in OL 8 must be disabled if a graphical user interface is installed.	Implemented by default
OL08-00-040190	CAT I	-	The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for OL 8 operational support.	Implemented by default
OL08-00-040200	CAT I	-	The root account must be the only account having unrestricted access to the OL 8 system.	Implemented by default
OL08-00-040360	CAT I	-	A File Transfer Protocol (FTP) server package must not be installed unless mission essential on OL 8.	Implemented by default
OL08-00-010049	CAT II	-	OL 8 must display a banner before granting local or remote access to the system via a graphical user logon.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-010110	CAT II	-	OL 8 must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.	Implemented by default
OL08-00-010120	CAT II	-	OL 8 must employ FIPS 140-2 approved cryptographic hashing algorithms for all stored passwords.	Implemented by default
OL08-00-010130	CAT II	-	The OL 8 shadow password suite must be configured to use a sufficient number of hashing rounds.	Implemented by default
OL08-00-010151	CAT II	-	OL 8 operating systems must require authentication upon booting into rescue mode.	Implemented by default
OL08-00-010152	CAT II	-	OL 8 operating systems must require authentication upon booting into emergency mode.	Implemented by default
OL08-00-010159	CAT II	-	The OL 8 "pam_unix.so" module must be configured in the system-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.	Implemented by default
OL08-00-010160	CAT II	-	The OL 8 "pam_unix.so" module must be configured in the password-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-010161	CAT II	-	OL 8 must prevent system daemons from using Kerberos for authentication.	Implemented by default
OL08-00-010162	CAT II	-	The krb5-workstation package must not be installed on OL 8.	Implemented by default
OL08-00-010163	CAT II	-	The krb5-server package must not be installed on OL 8.	Implemented by default
OL08-00-010200	CAT II	-	OL 8 must be configured so that all network connections associated with SSH traffic are terminate after a period of inactivity.	Implemented by default
OL08-00-010210	CAT II	-	The OL 8 "/var/log/messages" file must have mode 0640 or less permissive.	Implemented by default
OL08-00-010220	CAT II	-	The OL 8 "/var/log/messages" file must be owned by root.	Implemented by default
OL08-00-010230	CAT II	-	The OL 8 "/var/log/messages" file must be group-owned by root.	Implemented by default
OL08-00-010240	CAT II	-	The OL 8 "/var/log" directory must have mode 0755 or less permissive.	Implemented by default
OL08-00-010250	CAT II	-	The OL 8 "/var/log" directory must be owned by root.	Implemented by default
OL08-00-010260	CAT II	-	The OL 8 "/var/log" directory must be group-owned by root.	Implemented by default
OL08-00-010294	CAT II	-	The OL 8 operating system must implement DoD-approved TLS encryption in the OpenSSL package.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-010372	CAT II	-	OL 8 must prevent the loading of a new kernel for later execution.	Implemented by default
OL08-00-010373	CAT II	-	OL 8 must enable kernel parameters to enforce Discretionary Access Control (DAC) on symlinks.	Implemented by default
OL08-00-010374	CAT II	-	OL 8 must enable kernel parameters to enforce Discretionary Access Control (DAC) on hardlinks.	Implemented by default
OL08-00-010381	CAT II	-	OL 8 must require users to reauthenticate for privilege escalation and changing roles.	Implemented by default
OL08-00-010382	CAT II	-	OL 8 must restrict privilege elevation to authorized personnel.	Implemented by default
OL08-00-010480	CAT II	-	The OL 8 SSH public host key files must have mode "0644" or less permissive.	Implemented by default
OL08-00-010500	CAT II	-	The OL 8 SSH daemon must perform strict mode checking of home directory configuration files.	Implemented by default
OL08-00-010520	CAT II	-	The OL 8 SSH daemon must not allow authentication using known host's authentication.	Implemented by default
OL08-00-010521	CAT II	-	The OL 8 SSH daemon must not allow Kerberos authentication, except to fulfill documented and validated mission requirements.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-010522	CAT II	-	The OL 8 SSH daemon must not allow GSSAPI authentication, except to fulfill documented and validated mission requirements.	Implemented by default
OL08-00-010543	CAT II	-	OL 8 must use a separate file system for "/tmp".	Implemented by default
OL08-00-010550	CAT II	-	OL 8 must not permit direct logons to the root account using remote access via SSH.	Implemented by default
OL08-00-010561	CAT II	-	OL 8 must have the rsyslog service enabled and active.	Implemented by default
OL08-00-010571	CAT II	-	OL 8 must prevent files with the setuid and setgid bit set from being executed on the / boot directory.	Implemented by default
OL08-00-010630	CAT II	-	OL 8 file systems must not execute binary files that are imported via Network File System (NFS).	Implemented by default
OL08-00-010640	CAT II	-	OL 8 file systems must not interpret character or block special devices that are imported via NFS.	Implemented by default
OL08-00-010650	CAT II	-	OL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that are imported via Network File System (NFS).	Implemented by default
OL08-00-010760	CAT II	-	All OL 8 local interactive user accounts must be assigned a home directory upon creation.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-020010	CAT II	-	OL 8 systems below version 8.2 must automatically lock an account when three unsuccessful logon attempts occur.	Implemented by default
OL08-00-020011	CAT II	-	OL 8 systems, versions 8.2 and above, must automatically lock an account when three unsuccessful logon attempts occur.	Implemented by default
OL08-00-020012	CAT II	-	OL 8 systems below version 8.2 must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.	Implemented by default
OL08-00-020013	CAT II	-	OL 8 systems, versions 8.2 and above, must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.	Implemented by default
OL08-00-020014	CAT II	-	OL 8 systems below version 8.2 must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.	Implemented by default
OL08-00-020018	CAT II	-	OL 8 systems below version 8.2 must prevent system messages from being presented when three unsuccessful logon attempts occur.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-020019	CAT II	-	OL 8 systems, versions 8.2 and above, must prevent system messages from being presented when three unsuccessful logon attempts occur.	Implemented by default
OL08-00-020020	CAT II	-	OL 8 systems below version 8.2 must log user name information when unsuccessful logon attempts occur.	Implemented by default
OL08-00-020021	CAT II	-	OL 8 systems, versions 8.2 and above, must log user name information when unsuccessful logon attempts occur.	Implemented by default
OL08-00-020022	CAT II	-	OL 8 systems below version 8.2 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.	Implemented by default
OL08-00-020039	CAT II	-	OL 8 must have the tmux package installed.	Implemented by default
OL08-00-020100	CAT II	-	OL 8 must ensure the password complexity module is enabled in the password-auth file.	Implemented by default
OL08-00-020140	CAT II	-	OL 8 must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-020150	CAT II	-	OL 8 must require the maximum number of repeating characters be limited to three when passwords are changed.	Implemented by default
OL08-00-020160	CAT II	-	OL 8 must require the change of at least four character classes when passwords are changed.	Implemented by default
OL08-00-020180	CAT II	-	OL 8 passwords for new users or password changes must have a 24 hours/1 day minimum password lifetime restriction in "/etc/shadow".	Implemented by default
OL08-00-020190	CAT II	-	OL 8 passwords for new users or password changes must have a 24 hours/1 day minimum password lifetime restriction in "/etc/login.defs".	Implemented by default
OL08-00-020200	CAT II	enable strict mode	OL 8 user account passwords must have a 60-day maximum password lifetime restriction.	Implemented in strict mode
OL08-00-020210	CAT II	enable strict mode	OL 8 user account passwords must be configured so that existing passwords are restricted to a 60-day maximum lifetime.	Implemented in strict mode
OL08-00-020230	CAT II	enable strict mode	OL 8 passwords must have a minimum of 15 characters.	Implemented in strict mode
OL08-00-020231	CAT II	enable strict mode	OL 8 passwords for new users must have a minimum of 15 characters.	Implemented in strict mode

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-020263	CAT II	-	The OL 8 lastlog command must be owned by root.	Implemented by default
OL08-00-020264	CAT II	-	The OL 8 lastlog command must be group-owned by root.	Implemented by default
OL08-00-020300	CAT II	-	OL 8 must prevent the use of dictionary words for passwords.	Implemented by default
OL08-00-020310	CAT II	-	OL 8 must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.	Implemented by default
OL08-00-020350	CAT II	-	OL 8 must display the date and time of the last successful account logon upon an SSH logon.	Implemented by default
OL08-00-020351	CAT II	-	OL 8 default permissions must be defined in such a way that all authenticated users can read and modify only their own files.	Implemented by default
OL08-00-030000	CAT II	-	The OL 8 audit system must be configured to audit the execution of privileged functions and prevent all software from executing at higher privilege levels than users executing the software.	Implemented by default
OL08-00-030020	CAT II	-	The OL 8 System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted of an audit processing failure event.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030040	CAT II	-	The OL 8 System must take appropriate action when an audit processing failure occurs.	Implemented by default
OL08-00-030060	CAT II	-	The OL 8 audit system must take appropriate action when the audit storage volume is full.	Implemented by default
OL08-00-030061	CAT II	-	The OL 8 audit system must audit local events.	Implemented by default
OL08-00-030062	CAT II	-	OL 8 must label all offloaded audit logs before sending them to the central log server.	Implemented by default
OL08-00-030063	CAT II	-	OL 8 must resolve audit information before writing to disk.	Implemented by default
OL08-00-030080	CAT II	-	OL 8 audit logs must be owned by root to prevent unauthorized read access.	Implemented by default
OL08-00-030100	CAT II	-	The OL 8 audit log directory must be owned by root to prevent unauthorized read access.	Implemented by default
OL08-00-030121	CAT II	-	The OL 8 audit system must protect auditing rules from unauthorized change.	Implemented by default
OL08-00-030122	CAT II	-	The OL 8 audit system must protect logon UIDs from unauthorized change.	Implemented by default
OL08-00-030130	CAT II	-	OL 8 must generate audit records for all account creation events that affect "/etc/shadow".	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030140	CAT II	-	OL 8 must generate audit records for all account creation events that affect "/etc/security/opasswd".	Implemented by default
OL08-00-030150	CAT II	-	OL 8 must generate audit records for all account creation events that affect "/etc/passwd".	Implemented by default
OL08-00-030160	CAT II	-	OL 8 must generate audit records for all account creation events that affect "/etc/gshadow".	Implemented by default
OL08-00-030170	CAT II	-	OL 8 must generate audit records for all account creation events that affect "/etc/group".	Implemented by default
OL08-00-030171	CAT II	-	OL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers".	Implemented by default
OL08-00-030172	CAT II	-	OL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/".	Implemented by default
OL08-00-030180	CAT II	-	The OL 8 audit package must be installed.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030181	CAT II	-	OL 8 audit records must contain information to establish what type of events occurred, the source of events, where events occurred, and the outcome of events.	Implemented by default
OL08-00-030190	CAT II	-	OL 8 must generate audit records for any use of the "su" command.	Implemented by default
OL08-00-030200	CAT II	-	The OL 8 audit system must be configured to audit any use of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls.	Implemented by default
OL08-00-030250	CAT II	-	OL 8 must generate audit records for any use of the "chage" command.	Implemented by default
OL08-00-030260	CAT II	-	OL 8 must generate audit records for any uses of the "chcon" command.	Implemented by default
OL08-00-030280	CAT II	-	OL 8 must generate audit records for any use of the "ssh-agent" command.	Implemented by default
OL08-00-030290	CAT II	-	OL 8 must generate audit records for any use of the "passwd" command.	Implemented by default
OL08-00-030300	CAT II	-	OL 8 must generate audit records for any use of the "mount" command.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030301	CAT II	-	OL 8 must generate audit records for any use of the "umount" command.	Implemented by default
OL08-00-030302	CAT II	-	OL 8 must generate audit records for any use of the "mount" syscall.	Implemented by default
OL08-00-030310	CAT II	-	OL 8 must generate audit records for any use of the "unix_update" command.	Implemented by default
OL08-00-030311	CAT II	-	OL 8 must generate audit records for any use of the "postdrop" command.	Implemented by default
OL08-00-030312	CAT II	-	OL 8 must generate audit records for any use of the "postqueue" command.	Implemented by default
OL08-00-030313	CAT II	-	OL 8 must generate audit records for any use of the "semanage" command.	Implemented by default
OL08-00-030314	CAT II	-	OL 8 must generate audit records for any use of the "setfiles" command.	Implemented by default
OL08-00-030315	CAT II	-	OL 8 must generate audit records for any use of the "userhelper" command.	Implemented by default
OL08-00-030316	CAT II	-	OL 8 must generate audit records for any use of the "setsebool" command.	Implemented by default
OL08-00-030317	CAT II	-	OL 8 must generate audit records for any use of the "unix_chkpwd" command.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030320	CAT II	-	OL 8 must generate audit records for any use of the "ssh-keysign" command.	Implemented by default
OL08-00-030330	CAT II	-	OL 8 must generate audit records for any use of the "setfacl" command.	Implemented by default
OL08-00-030340	CAT II	-	OL 8 must generate audit records for any use of the "pam_timestamp_check" command.	Implemented by default
OL08-00-030350	CAT II	-	OL 8 must generate audit records for any use of the "newgrp" command.	Implemented by default
OL08-00-030360	CAT II	-	OL 8 must generate audit records for any use of the "init_module" and "finit_module" system calls.	Implemented by default
OL08-00-030361	CAT II	-	OL 8 must generate audit records for any use of the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls.	Implemented by default
OL08-00-030370	CAT II	-	OL 8 must generate audit records for any use of the "gpasswd" command.	Implemented by default
OL08-00-030390	CAT II	-	OL 8 must generate audit records for any use of the delete_module syscall.	Implemented by default
OL08-00-030400	CAT II	-	OL 8 must generate audit records for any use of the "crontab" command.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030410	CAT II	-	OL 8 must generate audit records for any use of the "chsh" command.	Implemented by default
OL08-00-030420	CAT II	-	OL 8 must generate audit records for any use of the "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" system calls.	Implemented by default
OL08-00-030480	CAT II	-	OL 8 must generate audit records for any use of the "chown", "fchown", "fchownat", and "lchown" system calls.	Implemented by default
OL08-00-030490	CAT II	-	OL 8 must generate audit records for any use of the "chmod", "fchmod", and "fchmodat" system calls.	Implemented by default
OL08-00-030550	CAT II	-	OL 8 must generate audit records for any use of the "sudo" command.	Implemented by default
OL08-00-030560	CAT II	-	OL 8 must generate audit records for any use of the "usermod" command.	Implemented by default
OL08-00-030570	CAT II	-	OL 8 must generate audit records for any use of the "chacl" command.	Implemented by default
OL08-00-030580	CAT II	-	OL 8 must generate audit records for any use of the "kmod" command.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030600	CAT II	-	OL 8 must generate audit records for any attempted modifications to the "lastlog" file.	Implemented by default
OL08-00-030610	CAT II	-	OL 8 must allow only the Information System Security Manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.	Implemented by default
OL08-00-030620	CAT II	-	OL 8 audit tools must have a mode of "0755" or less permissive.	Implemented by default
OL08-00-030630	CAT II	-	OL 8 audit tools must be owned by root.	Implemented by default
OL08-00-030640	CAT II	-	OL 8 audit tools must be group-owned by root.	Implemented by default
OL08-00-030670	CAT II	-	OL 8 must have the packages required for offloading audit logs installed.	Implemented by default
OL08-00-030700	CAT II	-	OL 8 must take appropriate action when the internal event queue is full.	Implemented by default
OL08-00-040001	CAT II	-	OL 8 must not have any automated bug reporting tools installed.	Implemented by default
OL08-00-040002	CAT II	-	OL 8 must not have the sendmail package installed.	Implemented by default
OL08-00-040021	CAT II	-	OL 8 must not have the asynchronous transfer mode (ATM) kernel module installed if not required for operational support.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-040022	CAT II	-	OL 8 must not have the Controller Area Network (CAN) kernel module installed if not required for operational support.	Implemented by default
OL08-00-040023	CAT II	-	OL 8 must not have the stream control transmission protocol (SCTP) kernel module installed if not required for operational support.	Implemented by default
OL08-00-040080	CAT II	-	OL 8 must be configured to disable the ability to use USB mass storage devices.	Implemented by default
OL08-00-040111	CAT II	-	OL 8 Bluetooth must be disabled.	Implemented by default
OL08-00-040129	CAT II	-	OL 8 must mount "/var/log/audit" with the "nodev" option.	Implemented by default
OL08-00-040130	CAT II	-	OL 8 must mount "/var/log/audit" with the "nosuid" option.	Implemented by default
OL08-00-040131	CAT II	-	OL 8 must mount "/var/log/audit" with the "noexec" option.	Implemented by default
OL08-00-040160	CAT II	-	All OL 8 networked systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.	Implemented by default
OL08-00-040161	CAT II	-	OL 8 must force a frequent session key renegotiation for SSH connections to the server.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-040209	CAT II	-	OL 8 must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted.	Implemented by default
OL08-00-040210	CAT II	-	OL 8 must prevent IPv6 Internet Control Message Protocol (ICMP) redirect messages from being accepted.	Implemented by default
OL08-00-040220	CAT II	-	OL 8 must not send Internet Control Message Protocol (ICMP) redirects.	Implemented by default
OL08-00-040230	CAT II	-	OL 8 must not respond to Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.	Implemented by default
OL08-00-040239	CAT II	-	OL 8 must not forward IPv4 source-routed packets.	Implemented by default
OL08-00-040240	CAT II	-	OL 8 must not forward IPv6 source-routed packets.	Implemented by default
OL08-00-040249	CAT II	-	OL 8 must not forward IPv4 source-routed packets by default.	Implemented by default
OL08-00-040250	CAT II	-	OL 8 must not forward IPv6 source-routed packets by default.	Implemented by default
OL08-00-040260	CAT II	-	OL 8 must not enable IPv6 packet forwarding unless the system is a router.	Implemented by default
OL08-00-040261	CAT II	-	OL 8 must not accept router advertisements on all IPv6 interfaces.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-040262	CAT II	-	OL 8 must not accept router advertisements on all IPv6 interfaces by default.	Implemented by default
OL08-00-040270	CAT II	-	OL 8 must not allow interfaces to perform Internet Control Message Protocol (ICMP) redirects by default.	Implemented by default
OL08-00-040279	CAT II	-	OL 8 must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.	Implemented by default
OL08-00-040280	CAT II	-	OL 8 must ignore IPv6 Internet Control Message Protocol (ICMP) redirect messages.	Implemented by default
OL08-00-040281	CAT II	-	OL 8 must disable access to the network "bpf" syscall from unprivileged processes.	Implemented by default
OL08-00-040283	CAT II	-	OL 8 must restrict exposed kernel pointer addresses access.	Implemented by default
OL08-00-040284	CAT II	-	OL 8 must disable the use of user namespaces.	Implemented by default
OL08-00-040285	CAT II	-	OL 8 must use reverse path filtering on all IPv4 interfaces.	Implemented by default
OL08-00-040286	CAT II	-	OL 8 must enable hardening for the Berkeley Packet Filter Just-in-time compiler.	Implemented by default
OL08-00-040290	CAT II	-	OL 8 must be configured to prevent unrestricted mail relaying.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-040340	CAT II	-	OL 8 remote X connections for interactive users must be disabled unless to fulfill documented and validated mission requirements.	Implemented by default
OL08-00-040341	CAT II	-	The OL 8 SSH daemon must prevent remote hosts from connecting to the proxy display.	Implemented by default
OL08-00-040350	CAT II	-	If the Trivial File Transfer Protocol (TFTP) server is required, the OL 8 TFTP daemon must be configured to operate in secure mode.	Implemented by default
OL08-00-040390	CAT II	-	OL 8 must not have the "tuned" package installed if not required for operational support.	Implemented by default
OL08-00-010171	CAT III	-	OL 8 must have the "policycoreutils" package installed.	Implemented by default
OL08-00-010292	CAT III	-	The OL 8 SSH server must be configured to use strong entropy.	Implemented by default
OL08-00-010375	CAT III	-	OL 8 must restrict access to the kernel message buffer.	Implemented by default
OL08-00-010376	CAT III	-	OL 8 must prevent kernel profiling by unprivileged users.	Implemented by default
OL08-00-010390	CAT III	-	OL 8 must have the package required for multifactor authentication installed.	Implemented by default
OL08-00-010440	CAT III	-	YUM must remove all software components after updated versions have been installed on OL 8.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-010541	CAT III	-	OL 8 must use a separate file system for "/var/log".	Implemented by default
OL08-00-020024	CAT III	-	OL 8 must limit the number of concurrent sessions to 10 for all accounts and/or account types.	Implemented by default
OL08-00-020110	CAT III	-	OL 8 must enforce password complexity by requiring that at least one uppercase character be used.	Implemented by default
OL08-00-020120	CAT III	-	OL 8 must enforce password complexity by requiring that at least one lowercase character be used.	Implemented by default
OL08-00-020130	CAT III	-	OL 8 must enforce password complexity by requiring that at least one numeric character be used.	Implemented by default
OL08-00-020170	CAT III	-	OL 8 must require the change of at least 8 characters when passwords are changed.	Implemented by default
OL08-00-020220	CAT III	-	OL 8 must be configured in the password-auth file to prohibit password reuse for a minimum of five generations.	Implemented by default
OL08-00-020280	CAT III	-	All OL 8 passwords must contain at least one special character.	Implemented by default
OL08-00-030741	CAT III	-	OL 8 must disable the chrony daemon from acting as a server.	Implemented by default

Table J-7 (Cont.) Current Implementation of Operating System STIG Guidelines for Oracle AVDF

STIG ID	Severity	User Action	Title	Notes
OL08-00-030742	CAT III	-	OL 8 must disable network management of the chrony daemon.	Implemented by default
OL08-00-040024	CAT III	-	OL 8 must disable the transparent inter-process communication (TIPC) protocol.	Implemented by default
OL08-00-040025	CAT III	-	OL 8 must disable mounting of cramfs.	Implemented by default
OL08-00-040026	CAT III	-	OL 8 must disable IEEE 1394 (FireWire) Support.	Implemented by default

K

Enabling FIPS 140-2 in Oracle AVDF

Learn about enabling FIPS 140-2 in Oracle AVDF.

K.1 About FIPS and Oracle AVDF

FIPS (Federal Information Processing Standards) is a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, by government contractors, and vendors who work with these agencies.

FIPS publications are issued by the National Institute of Standards and Technology (NIST). The publication entitled *Security Requirements for Cryptographic Modules* (FIPS 140-2) specifies the security requirements over several key areas that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information.

You can enable FIPS 140-2 for the following Oracle AVDF components only:

- Audit Vault Server: Enabling FIPS on the Audit Vault Server turns on FIPS mode in the embedded Oracle Linux operating system and Oracle Database.
- Database Firewall: Enabling FIPS 140-2 on the Database Firewall turns on FIPS mode in the embedded Oracle Linux operating system.

> **Tip:**
>
> Before enabling FIPS 140-2, ensure that your SSH keys are compliant with FIPS. If your SSH keys are not compliant with FIPS, the SSH connection with the appliance might be lost after enabling FIPS.

Related Topics

- FIPS 140-2 Compliance in Oracle Linux 7
- FIPS 140-2 Compliance in Oracle Linux 8
- Oracle Database FIPS 140-2 Settings

K.2 Enabling FIPS 140-2 on the Audit Vault Server

Enable FIPS on the Audit Vault Server to turn on FIPS mode in the embedded Oracle Linux operating system and Oracle Database.

> **Note:**
>
> For Oracle AVDF on Oracle Cloud Infrastructure (OCI), before enabling FIPS mode, ensure that the `opc` user has FIPS-compliant keys registered to `/home/opc/.ssh/authorized_keys`.

1. Log in to Audit Vault Server console as a `super administrator`.
2. Click the **Settings** tab.
   The **Security** tab in the left navigation menu is selected by default.
3. Click the **FIPS** subtab on the main page.
4. Click the toggle switch to enable FIPS 140-2. The toggle switch is green when it's on.
5. Click **Save**.
   A message says that the Audit Vault Server will reboot and prompts you to continue or cancel.
6. Click **OK** to continue to enable FIPS 140-2 for Audit Vault Server. Otherwise, click **Cancel**.

The Audit Vault Server restarts and is unavailable for several minutes. Don't attempt to access the Audit Vault Server console during this period. Close the browser and open a new tab or window to log in to the Audit Vault Server console.

> **Note:**
>
> - To disable FIPS 140-2 mode for the Audit Vault Server, click the toggle switch on the FIPS subtab.
> - For Oracle AVDF on OCI, if SSH access becomes disabled after enabling FIPS mode, log into the Audit Vault Server console and disable FIPS mode. Then log back into the appliance through SSH and update the user keys for `opc` in `/home/opc/.ssh/authorized_keys` to be compliant with FIPS. It can take several minutes for the console to become available after enabling or disabling FIPS mode.
> - In a high availability configuration, enabling FIPS 140-2 mode for the primary Audit Vault Server also enables FIPS 140-2 mode for the standby Audit Vault Server. Similarly, disabling FIPS mode for the primary Audit Vault Server also disables it for the standby Audit Vault Server.

K.3 Enabling FIPS 140-2 in Database Firewall

Learn how to enable FIPS 140-2 in Database Firewall.

1. Log in to Audit Vault Server console as `super administrator`.
2. Click **Database Firewalls** tab. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Click the name of the specific Database Firewall instance for which you want to enable FIPS 140-2.
4. Click **FIPS** under the **Configuration** section. A dialog is displayed.

5. In the dialog, turn on the toggle switch to enable FIPS 140-2. The toggle switch turns green when it is turned on.
6. Click **Save**. A message pops that Database Firewall will reboot and prompts you to continue or cancel.
7. Click **OK** to continue to enable FIPS 140-2 for the Database Firewall instance. Else, click **Cancel**.
   The Database Firewall instance is restarted and is unavailable for some time.
8. Wait for a while, and navigate back to the **Database Firewalls** tab in the left navigation menu.
9. Check the status of FIPS 140-2 mode under the column **FIPS Mode** against the specific Database Firewall instance.

K.4 Enabling FIPS 140-2 for Database Firewall Instances in High Availability

Learn how to enable FIPS 140-2 for Database Firewall instances in high availability configuration.

Prerequisites

- At least two instances of Database Firewall must be configured for high availability.
- The FIPS 140-2 status of both the Database Firewall instances must either be `Off` or `On`. FIPS 140-2 mode can be disabled or enabled on both the Database Firewall instances. In case, these two instances have different FIPS mode, then an error message is displayed on the screen.

1. Log in to Audit Vault Server console as `super administrator`.
2. Click **Database Firewalls** tab. The **Database Firewalls** tab in the left navigation menu is selected by default.
3. Click **High Availability** tab in the left navigation menu. All the Database Firewall instances that are configured in high availability are listed in the main page.
4. The names of paired Database Firewall instances are listed under the **Primary** and **Secondary** columns on the main page. Select the specific pair of Database Firewall instances for which you want to enable FIPS.
5. Click **FIPS** in the top right corner of the page. A dialog is displayed.
6. Turn on the toggle switch to enable FIPS 140-2. The toggle switch turns green when it is turned on.
7. Click **Save** button. A message pops that the Database Firewall instances will reboot and prompts you to continue or cancel.
8. Click **OK** to continue to enable FIPS 140-2 for the Database Firewall instances. Else, click **Cancel**.
   The Database Firewall instances are restarted and are unavailable for some time.
9. Wait for a while and check the status of FIPS 140-2 mode under the column **FIPS Mode** against the paired Database Firewall instances.

> **See Also:**
>
> Configuring High Availabilty for Database Firewalls

K.5 Verify the Status After Enabling FIPS 140-2 for Database Firewall Instances in High Availability

Learn how to verify or check the status after enabling or disabling FIPS 140-2 for the Database Firewall instances configured in high availability.

1. Log in to Audit Vault Server console as *super administrator*.
2. Click **Settings** tab.
3. Click **System** tab in the left navigation menu.
4. Click **Jobs** under the **Monitoring** section. The **Jobs** dialog is displayed.
5. The recent jobs are listed on the top. Else, rearrange to locate the job that is specific to enabling or disabling the FIPS 140-2 mode for the Database Firewall instances configured in high availability.
6. Verify the status is `Completed`. Else, click the **Job Details** icon to the extreme left of the specific job.
7. The **Job Status Details** dialog is displayed. It contains detailed information on the list of events pertaining to the job triggered.

K.6 Enabling FIPS 140-2 for Database Firewall Instances in High Availability Deployed in Proxy Mode

Learn how to enable FIPS 140-2 for Database Firewall instances in high availability deployed in proxy mode.

Prerequisite

At least two instances of Database Firewall must be configured for high availability in proxy mode.

Steps to be followed for enabling or disabling FIPS 140-2 for all Database Firewall instances that are part of high availability and deployed in **Monitoring / Blocking (Proxy)** mode:

1. All the Database Firewall instances that are part of high availability must have the same FIPS 140-2 mode. They should either be enabled for FIPS 140-2 or disabled (`On` or `Off`).
2. To enable or disable FIPS 140-2 for every Database Firewall instance follow the procedure in section Enabling FIPS 140-2 in Database Firewall.
3. After following the previous step, ensure all the Database Firewall instances that are part of high availability should have the same FIPS 140-2 mode (either `On` or `Off`).

Note:

Inconsistent behavior is expected if Database Firewall instances are in different FIPS 140-2 modes (some of them having FIPS 140-2 enabled and some of them disabled).

See Also:

Configuring High Availability for Database Firewalls in Proxy Mode

L

Troubleshooting Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall provides troubleshooting advice for a range of scenarios.

L.1 Information to Provide Support When Filing a Service Request

Review this list of information to provide support when filing a service request.

> **Note:**
>
> Diagnostics data, especially trace files, often contains sensitive information. Protect it accordingly and only gather and send the information that's required.

- Oracle AVDF version, including any installed bundle patches
- If virtualization is being used? If so, which one?
- How much physical memory is available to Audit Vault Server and Database Firewall appliances?
- How much disk space was available with the initial installation?
- Did you add any SAN storage and in that case how much disk space?
- Provide any relevant details about the brand and model of the hardware being used. This is relevant if you have specific issues relating to booting from the installation media.
- Host OS for the secured target database and version, this is relevant for checking agent compatibility issues.
- Brand of the secured target database, such as Oracle, MySQL, SQL Server, etc.
- Version of the secured target database, including PSU and other one-off patches.
- Upload the alert.log file of the secured target database.
- From any Oracle secured target database provide the output of:
  - `show parameter audit`
  - `opatch lsinventory -patch -detail`
  - If unified auditing was configured (for some versions of Oracle database only)
  - Audit Trail type that is being configured and all relevant attributes
- Detailed diagnostic information for Audit Vault Server, see Downloading Detailed Diagnostics Reports for Oracle Audit Vault Server
- If requested by Oracle Support, diagnostic information from Oracle Trace File Analyzer. See Using Oracle Trace File Analyzer (TFA).

- Information about Database Firewall:
  - Detailed diagnostic info for Database Firewall, see Viewing the Status and Diagnostics Report for Database Firewall
  - How many Network Interface Cards are installed in the database firewall appliance?
  - Is the enforcement point using default password enumeration (DPE) or database activity monitoring (DAM)? If so is it bridge, span, or proxy?
  - Do you use VLAN tagging? There are restrictions for support of VLANs.
- For installation issues, diagnostic files related to the installation. See Collecting Logs to Debug Installation Failures.

Before contacting support, the Audit Trail Transaction Log should follow these guidelines:

- The user setup script must be run with the argument `REDO_COLL`
- The secured target database must be configured with `ARCHIVELOG`
- The streams recommended patches must be applied to the secured target db: Streams Recommended Patches (Doc ID 437838.1)
- `global_name` must be fully qualified (select global_name from global_name;)
- Parameter `global_names = true` is recommended
- If errors happen on capture or apply side please check respective alert.logfiles as you would do with any Streams related issue (av log will show only limited information for this audit trail type)

Related Topics

- Configure and Download the Diagnostics Report File

L.2 Using Oracle Trace File Analyzer (Oracle AVDF 20.1 - 20.11)

If you request support from Oracle Support, they may ask you to install and run Oracle Trace File Analyzer on the Audit Vault Server to collect diagnostic information.

> **Note:**
>
> Install Oracle Trace File Analyzer only when requested by Oracle Support, and uninstall it when you're done to maintain a high level of security. Make sure that it's uninstalled before patching or upgrading to the latest version of Oracle AVDF.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Enter the following command to install Oracle Trace File Analyzer:

   ```
   /usr/local/dbfw/bin/setup_TraceFileAnalyzer.py --install
   ```
3. Run any `tfactl` command to collect diagnostics, as needed. For example:

   ```
   tfactl diagcollect <options>
   ```

4. Securely copy the collected diagnostic file to a location from which you can upload the file to the service request. For example:

   ```
   scp /opt/ahf_installation/oracle.ahf/data/repository/<diagnostic_zip_file>
   <new_location>
   ```

5. Run the following command to uninstall Oracle Trace File Analyzer:

   ```
   /usr/local/dbfw/bin/setup_TraceFileAnalyzer.py --uninstall
   ```

If you have modified the IP address of the Audit Vault Server and are encountering the `TFA-00104 Cannot establish connection with TFA Server. Please check TFA Certificates` error when running TFA commands, follow these steps to resolve the error:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. `tfactl syncnodes -regenerate`

L.3 Using Oracle Trace File Analyzer (Oracle AVDF 20.12 and later)

If you request support from Oracle Support, they may ask you to run Oracle Trace File Analyzer on the Audit Vault Server to collect diagnostic information. Oracle Trace File Analyzer is already installed on the Audit Vault Server starting with Oracle AVDF 20.12.

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run `tfactl` command to collect diagnostics, as needed. For example:

   ```
   tfactl diagcollect -avs -noclassify  -noinsight
   ```

   The `avs` parameter should be used to ensure the Audit Vault Server application layer logs will also get collected.

3. Securely copy the collected diagnostic file to a location from which you can upload the file to the service request. For example:

   ```
   scp /var/opt/oracle/ahf/oracle.ahf/data/repository/<diagnostic_zip_file>
   <new_location>
   ```

   Oracle Trace File Analyzer on the Audit Vault Server will automatically collect logs in `/var/opt/oracle/ahf/oracle.ahf/data`.

If you have modified the IP address of the Audit Vault Server and are encountering the `TFA-00104 Cannot establish connection with TFA Server. Please check TFA Certificates` error when running TFA commands, follow these steps to resolve the error:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. `tfactl syncnodes -regenerate`

Related Topics

- Oracle Trace File Analyzer Installer, Command-Line and Shell Options

L.4 Ability to Boot Into Rescue Mode When Troubleshooting

Starting in Oracle AVDF 20.10 you can boot directly into rescue mode from the grub menu on both the Audit Vault Server and the Database Firewall. Booting into the rescue mode does not run AVDF processes and allows for easier troubleshooting. Running rescue mode is intended for use by and under the direction of Oracle Support.

Once the system has booted you can switch to rescue mode by running the following command:

```
- systemctl isolate avdf-minimal.target
```

You can switch back to usual runtime by running the following command:

```
- systemctl isolate avdf-runtime.target
```

> **Note:**
>
> Switching from rescue mode on the Audit Vault Server to the usual runtime mode can take a long time, around 15 minutes.

L.5 Audit Vault Agent or Host Monitor Agent Is Not Upgraded to the New Release

Learn how to upgrade the Audit Vault Agent or Host Monitor Agent manually.

Problem

After upgrading to Oracle AVDF 20.1 or later, some of the Audit Vault Agents or Host Monitor Agents are not upgraded.

Symptom - 1

Audit Vault Agent is in `STOPPED` state after Audit Vault Server upgrade.

Symptom - 2

Host Monitor Agent is in `NEEDS UPGRADE` or `UPDATE FAILED` state after Audit Vault Server upgrade.

Solution - 1

The symptom indicates that the Audit Vault Agent has failed to auto upgrade during the Audit Vault Server upgrade. Execute the following steps as the user who installed Agent previously:

1. Check for any Agent processes on the host machine. Ensure there are no Agent related processes currently running.
2. Remove the existing `agent.jar` file and the Agent folder from the host machine.
3. Download the new `agent.jar` file from the upgraded Audit Vault Server.
4. Execute the following command:

```
java -jar agent.jar [-d <AgentHome>]
```

5. Verify the Agent is in `RUNNING` state.

Solution - 2

The symptom indicates that the Host Monitor Agent has failed to auto upgrade during the Audit Vault Server upgrade. Execute the following steps as *root* user:

1. Check for any Host Monitor Agent related processes on the host machine. Ensure there are no `hostmonitor`, `hmdeployer`, or `hostmonmanager` processes currently running.
2. Navigate to the directory outside of `hm` where the Host Monitor Agent is installed.
3. Execute the following command to uninstall the Host Monitor Agent:

```
./hm/hostmonsetup uninstall
```

4. Download the new Host Monitor Agent installable bundle from the Audit Vault Server console, for the specific platform on which it will be reinstalled.
5. Extract the Host Monitor Agent bundle inside the `hm` directory.
6. Execute the following command to reinstall the Host Monitor Agent in a *root* owned location:

```
./hostmonsetup install
```

L.6 Failure While Building a Host Monitor Agent or Collecting Oracle Database Trails

Learn what to do when you experience a failure while building Host Monitor Agents or collecting Oracle Database trails.

Problem

This problem may manifest with various symptoms:

- When I try to build a Host Monitor Agent, the operation fails or the operation cannot locate the correct binaries.
- When I try to collect audit data from an Oracle Database 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.

> **See Also:**
>
> Deploying the Audit Vault Agent

2. If you deployed the Audit Vault Agent in a Linux environment, then ensure that the host machine name appears in the `/etc/hosts` file.

L.7 Error When Running Host Monitor Agent Setup

Review the resolutions for errors that occur when running Host Monitor Agent setup.

Problem

I am setting up a Host Monitor Agent. When I run the command `$HOSTMON_HOME/hm/hostmonsetup install`, the following error is displayed:

```
Failed to generate executables for Host monitor
```

This means the host computer does not have the required libraries for the Host Monitor Agent. Install the required libraries mentioned in Host Monitor Agent Requirements.

Symptom 1

Even after installing the required libraries, if the Host Monitor Agent installation fails with above error message, then examine the `makelogerror` file which is available in the Host Monitor Agent installation directory. The following errors, may appear in the file:

```
/bin/ld: cannot find -laio
/bin/ld: cannot find -lssl
/bin/ld: cannot find -lcrypto
/bin/ld: cannot find -lnsl
/bin/ld: cannot find -lpcap
/bin/ld: cannot find -lcap
```

Solution 1

To resolve the issue on Linux (64 bit) systems, follow these steps:

1. Search where the actual binaries (not symlinks) are present – `libssl, libnsl,libaio, libpcap, libcap`. In most scenarios it should be present either in `/lib64` or `/usr/lib`

2. Create below symlinks if not already present in `/lib64` or `/usr/lib`
   a. libcap binary
      - ln -s *<location from step 1>*/libcap.so.<version> /lib64/libcap.so.1
      - ln -s *<location from step 1>*/libcap.so.1 /lib64/libcap.so
   b. libaio binary
      - ln -s *<location from step 1>*/libaio.so.<version> /lib64/libaio.so.1
      - ln -s /lib64/libaio.so.1 /lib64/libaio.so
   c. libnsl binary
      - ln -s *<location from step 1>*/libnsl.so.<version> /lib64/libnsl.so.1
      - ln -s /lib64/libnsl.so.1 /lib64/libnsl.so
   d. libpcap binary
      - ln -s *<location from step 1>*/libpcap.so.<version> /lib64/libpcap.so.1
      - ln -s /lib64/libpcap.so.1 /lib64/libpcap.so
   e. libssl binary
      - ln -s *<location from step 1>*/libssl.so.*<version>* /lib64/libssl.so.1
      - ln -s /lib64/libssl.so.1 /lib64/libssl.so
   f. libcrypto binary
      - ln -s *<location from step 1>*/libcrypto.so.*<version>* /lib64/libcrypto.so.1
      - ln -s /lib64/libcrypto.so.1 /lib64/libcrypto.so

Symptom 2

The following error is observed in the `HOSTMON_HOME/makelogerror` file:

```
Undefined first referenced symbol in file
__1cG__CrunKex_dealloc6Fpv_v_       ./libhostmon19.a(Class.o)
ld: fatal: symbol referencing errors
make: Fatal error: Command failed for target `hostmonitor'
```

Solution 2

This error is observed when attempting to install Host Monitor Agent on Solaris 11.3 host machine. Some of the Solaris OS libraries are corrupt. Upgrade the operating system to Solaris 11.4 or contact the Solaris team for further assistance.

L.8 Host Monitor Agent Fails to Start

Learn what to do when the Host Monitor Agent fails to start.

Problem

The Host Monitor Agent network trail does not start after installation. The collection framework (`collfwk`) log file contains one of the following errors:

- `java.io.IOException: Cannot run program "<AgentHome>/hm/hostmonmanager" (in directory "<AgentHome>/hm"): error=13, The file access permissions do not allow the specified action.`

- `HMCommandExecutor : startTrail : binary is not found here: <AgentHome>/hm/hostmonmanager`

Solution

This issue may arise due to insufficient privileges while starting Host Monitor Agent. Ensure the Audit Vault Agent user belongs to the group that owns `hm` (Host Monitor Agent installation) directory. Ensure that the following permissions are given:

- The group that owns the Host Monitor Agent installation (`hm`) directory has `read` and `execute` permission on the `hm` directory.
- The group that owns the Host Monitor Agent installation (`hm`) directory has `execute` permission on `hostmonmanager` binary.

In the event that assigning the above permissions to the group did not work, use Access Control Lists (ACL) to ensure that the following permissions are given:

- The Audit Vault Agent user has `read` and `execute` permissions on the `hm` directory.
- The Audit Vault Agent user has `execute` permissions on `hmdeployer`, `hostmonitor` and `hostmonmanager` binaries.
- The Audit Vault Agent user has `read` permissions on `libnnz*.so` and `libociicus.so` libraries.

> **Note:**
>
> - `AgentHome` is the Audit Vault Agent installation directory.
> - `hm` is the Host Monitor Agent installation directory.

L.9 Host Monitor Agent Network Trail is in STOPPED State

Learn how to fix the issue when Host Monitor Agent network trail is in STOPPED state.

Problem

After starting the Host Monitor Agent network trail it goes into a `STOPPED` state.

Symptom

The following error is observed in the `HOSTMON_HOME/log/av.hostmonitor*.log` file:

```
[2022-01-27 13:40:57,061] [PID: <ID>, TName: main] [WARNING]
- Failed to perform SSL handshake using TLS protocol TLS 1.2 Error Msg: SSL
error:
Error in system call. Details: error:00000000:lib(0):func(0):reason(0)
Retrying with lower protocol
```

Solution

The Host Monitor Agent certificate is corrupt. Follow the steps in the topic Using Mutual Authentication for Communication Between the Database Firewall and the Host Monitor Agent to regenerate the certificate.

L.10 Network Audit Trail Does Not Start on Unix Platforms

Learn the resolution when the network audit trail fails to start on Unix platforms.

Problem

The network audit trail does not start on Unix platforms.

Symptoms

- The Oracle Audit Vault Server console displays the following error:

  ```
  Unable to start Host Monitor process
  ```

- The collection framework log displays the following error:

  ```
  <Host Monitor home>/hostmonmanager binary is not found here
  ```

Solution

1. Connect to the host machine on which the Audit Vault Agent and Host Monitor Agent are installed.
2. In the Agent Home location there is an `hm` symlink pointing to Host Monitor Agent installation location.
3. Run the following command from the Agent Home as the user who installed Audit Vault Agent:

   ```
   ls -lrt hm
   ```

4. Verify that it's possible to list the contents of the Host Monitor Agent installation directory.
5. Check the permissions of all directories in the hierarchy of the path under which the Host Monitor Agent is installed.

   > **Note:**
   >
   > The entire directory hierarchy must be owned by the `root` user. All of the directories in this hierarchy must have `read` and `execute` permission for other users or groups, but not `write` permission.
   >
   > In addition, the `hostmonitor` and `hostmonmanager` binaries should have `execute` access for the user who owns the Host Monitor Agent. These permissions should be granted by using an access control list (ACL).

6. Grant the necessary permissions according to the preceding note.
7. Restart the network audit trail.

L.11 Partial or No Traffic Seen for an Oracle Database Monitored by Oracle Database Firewall

Review the troubleshooting advice for when you see limited or no traffic for an Oracle Database that is monitored by Oracle 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 target system.
3. Check that the target's network traffic is visible to the Database Firewall using the Live Capture utility on the firewall.
4. Check that the Oracle Database service name or SID is used correctly. If you specified an Oracle Database service name in the monitoring point settings for this target, you will only see traffic for that service name. To see all traffic, remove the service name from the monitoring point settings.

   If you have entered a service name in the monitoring point, and see no traffic, check to see that the service name is entered correctly in the monitoring point settings.

   For monitoring points set to use monitoring only 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 monitoring point. In this case, restart the client connections to the database.
5. Check that the correct Database Firewall policy is deployed.

See Also:

- *Oracle Audit Vault and Database Firewall Auditor's Guide* for information on editing and deploying firewall policies.
- Configuring Database Firewall Monitoring Points
- Viewing Network Traffic for a Database Firewall

L.12 Incomplete or Missing SQL Statements or Network Traffic in Oracle AVDF Reports

Learn about the probable causes that may result in missing SQL statements in Oracle AVDF Reports.

Problem

Sometime there may be SQL statements missing or incomplete network traffic information in Oracle AVDF Reports. This topic contains the probable causes and some tips to troubleshoot.

Symptoms

Although there may be multiple reasons that may cause this issue, the following are some of the probable causes:

- The database client is unable to connect to the Database Firewall instance
- The Database Firewall is unable to connect to the target database
- The Audit Vault Server may be down
- The Database Firewall is unable to connect to the Audit Vault Server
- The Audit Vault Server may not be collecting data

Solution

Take necessary steps to resolve depending on the issue and diagnostic information. The following table contains some of the probable issues and some measures for the resolution:

Issue	Resolution
The database client is unable to connect to the Database Firewall proxy port.	1. Check the IP address and TCP port used by the database client to connect to the Database Firewall. Does that belong to the specific Database Firewall instance or monitoring point? 2. Ping the Database Firewall server from the database client's host machine. In case there is a failed response, then contact the network administrator. 3. Is there any other firewall between the database client and Oracle Database Firewall which may block the connection? 4. Is the Database Firewall listening to the expected or configured port? Log in to the Database Firewall instance through SSH as *support* user and then switch to *root* user. Run the command `netstat -alnpt | grep LISTEN | grep nnnnn` where `nnnnn` is the port number the database client is attempting to connect. If there is no port displayed in the output, then check

	the proxy port settings for the configured target.
The Database Firewall deployed in **Monitoring / Blocking (Proxy)** mode is unable to connect to the target database.	1. Check the IP address and TCP port of the target database. Verify if this information is properly entered when registering the target in the Audit Vault Server console. 2. Is there any other firewall between the database client and Oracle Database Firewall which may block the connection? 3. Ping the target database from the Database Firewall server. In case there is a failed response, then contact the network administrator. 4. Log in to the Database Firewall instance through SSH as *support* user and then switch to *root* user. Access and examine the contents of the `/var/log/messages` file. Check if the string `com.oracle.dbfw.fw ERROR - ODF-10501: Failed connecting to the Target` exists. See Database Firewall Messages for more information on the error message. The message also contains additional information for the failure. For example: `No route to host`.
Missing SQL statements that were expected to be captured by the Database Firewall.	1. Check if the Database Firewall monitoring point is running. In the Audit Vault Server console, check the status of the specific Database Firewall monitoring point. 2. Check if the Database Firewall instance is generating the required log files. There are two ways of doing this: a. Check the Database Firewall policy applied to the specific target. See if the option `Pass-All` is selected. This does not log any traffic. In case of a custom policy, analyze and revert to `Log-All` policy option and check if the expected traffic data is reflecting in the Oracle AVDF reports. If records are present, then examine the details of the custom policy and redefine as per the requirements. b. Log in to the Database Firewall instance through SSH as *support* user and then switch to *root* user. Run the following command `watch ls -`

`ltr /usr/local/dbfw/va/*/log/`. Examine the logs displayed and search for the log files named `kernel.nnnnnnnnnn.nnn.n.nnnn.dat.gz`. In case the traffic is being logged, then these files are displayed. Later these files disappear in a few minutes as their contents are transferred to the Audit Vault Server.

3. Check if the Audit Vault Server is requesting the transfer of the traffic log files from the Database Firewall. Follow these steps:
   a. The network traffic is being logged in Database Firewall and the log files are not removed after a while. Audit Vault Server may not be requesting the transfer of the traffic log files from the Database Firewall. Log in to the Database Firewall instance through SSH as *support* user and then switch to *root* user.
   b. Run the following command `tail -f /var/log/httpd/ssl_request_log`.
   c. Examine the output of the command. Some of the regular entries that end as follows exist:

      ```
      GET /logs/2/list HTTP/1.0" 78
      ```

      ```
      GET /logs/2/
      kernel.1655297472.734.0.0000.dat.
      gz HTTP/1.0" 1321
      ```

   d. If these entries are not displayed, then further troubleshooting in the Audit Vault Server is required. Raise a bug and attach the diagnostics of both Audit Vault Server and Database Firewall.

L.13 Agent Activation Request Returns 'host is not registered' Error

Read the troubleshooting advice if you receive a 'host is not registered' error.

Problem

I used the following two commands to register the Oracle 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:

Start *SQL*Plus* connection as `sqlplus /nolog` without the username or password.

In *SQL*Plus* execute the command: `connect <user>`. Enter the password when prompted.

```
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.

L.14 Unable to Deploy Agent on the Secondary Audit Vault Server

Learn the resolution if you are unable to deploy an agent on a secondary Oracle 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.

L.15 'java -jar agent.jar' Failed on Windows Machine

Review the resolution procedures when the `java -jar agent.jar` command fails on Windows machines.

Problem

The command `java -jar agent.jar` failed on my Windows 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 and Unregistering the Audit Vault Agent as a Windows Service.

   If Method 1 fails, then try Method 2.
2. Run the `java -jar agent.jar` command again.

L.16 Unable to Install the Agent or Generate the `agent.jar` File

Determine the steps to perform if you are unable to install the agent or generate the `agent.jar` file.

Problem

Unable to install the Audit Vault Agent. Attempts to regenerate the `agent.jar` file are also unsuccessful.

Solution

Follow these steps to regenerate the `agent.jar` file:

1. Log in to the Audit Vault Server through SSH as user `oracle`.
2. Go to the directory `/var/lib/oracle/dbfw/av/conf/` location.
3. Delete the `bootstrap.prop` file.
4. Execute the following command:

   ```
   /var/lib/oracle/dbfw/bin/avca configure_bootstrap
   ```
5. Check the `avca.log` file that is available at `/var/lib/oracle/dbfw/av/log/` to check if the above command was executed successfully.
6. Switch the user (`su`) to `avsys`.
7. Run the following query:

   ```
   select agent_gen_ts from file_repos where file_name='agent.jar';
   ```
8. The above query displays the current time in case the `agent.jar` file is generated successfully.

L.17 Unable to Un-install the Oracle Audit Vault Agent Windows Service

Review the troubleshooting advice if you are unable to un-install the Oracle Audit Vault Agent Windows Service.

Follow the instructions for unregistering the Agent inRegistering and Unregistering the Audit Vault Agent as a Windows Service.

If Method 1 fails, then try Method 2.

L.18 Access Denied Error While Installing Agent as a Windows Service

Learn how to resolve access denied errors when installing Oracle Audit Vault agent as a Windows service.

Problem

I got an error during installation of Oracle 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.

L.19 Unable to Start the Agent Through the Services Applet on the Control Panel

Review how to resolve being 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.

L.20 Error When Starting the Agent

Resolved errors that occur 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.

L.21 Alerts on Oracle Database Targets Are Not Triggered for Extended Periods of Time

Learn what to do when alerts on targets are not triggered for a long time.

Problem

I configured an Oracle Database 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 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*.

L.22 Error When Creating an Audit Policy

Resolve errors that can occur when you create an audit policy.

Problem

I received this error message when I tried to create a new audit policy setting for Oracle Database:

```
-ORA-01400: cannot insert NULL into
("AVSYS"."AUDIT_SETTING_ARCHIVE_MAP"."ARCHIVE_ID")
```

Cause

The Oracle Database must have at least one audit policy setting before you can create and provision new audit settings using Oracle Audit Vault and Database Firewall. Oracle Database comes with a predefined set of audit policy settings. You must not manually remove these settings. If the audit settings have been removed, then you can manually create at least one audit setting in the Oracle Database. Then try again to create new audit settings using Oracle Audit Vault and Database Firewall.

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

L.23 Connection Problems When Using Oracle Database Firewall Monitoring and Blocking

Resolve the connection problems that might occur when using Oracle Database Firewall monitoring and blocking.

Problem

In monitoring and blocking mode, my client application cannot connect to the target database.

Solution

1. Log in as `root` on the Database Firewall server.
2. Run this command using the target database IP address or host name:

   ```
   ping -I secured_target_ip_address_or_hostname
   ```

   If you do not receive a response, then ensure that the DNS is configured on Oracle Database Firewall.

   If a response is received, check:

   - The firewall policy to ensure that it is not blocking the connection attempt.
   - The client connection settings to ensure that the client is attempting to connect to the correct target database.

> **See Also:**
>
> - Configuring the Database Firewall and Its Traffic Sources on Your Network
> - Configuring Network Services for Oracle Database Firewall

L.24 Audit Trail Does Not Start

Learn the resolution to use when the audit trail does not start.

Problem

An audit trail does not start. For example, in the Audit Vault Server console, in the Audit Trails page, the **Collection Status** column indicates that the trail is **Stopped** or **Unreachable**.

Solution

When a trail does not start, you can show the associated error in two ways:

- In the Audit Vault Server console:
  1. Click the **Targets** tab, and then from the **Monitoring** menu, click **Audit Trails**.
  2. Click the Actions button, and then click Select Columns.
  3. From the left-hand box, double-click **Error Message** so that it moves into the **Display in Report** box on the right.

4. Click **Apply**.

   The **Error Message** column is displayed on the Audit Trails page and contains the error message for the stopped trail.

- On the Audit Vault Agent host computer:

  1. Go to the `logs` directory:

     ```
     cd %agenthome%/av/logs
     ```

  2. Run the following:

     ```
     grep -i 'error|warning|fail' *
     ```

     The error messages should indicate the cause of the problem.

If the cause is still unclear, or the grep command returns no results, raise an SR with Oracle Support and include Audit Vault Agent log files.

L.25 Cannot See Data for Targets

Learn what to do when you cannot see the data for a target.

Problem

Data for my Target does not appear on reports.

Solution

If you cannot see the data you expect to see in the Audit Vault Server, you can troubleshoot by trying one or more of the following:

- Confirm that Audit Vault Agent hosts are up and that the Audit Vault Agents are running.
- Confirm that audit trails are running and that the audit trail settings match the audit configuration of the Target database

  For example, the audit trail configuration in Oracle Audit Vault and Database Firewall should have the correct trail type and location.

  > **See Also:**
  >
  > Configuring and Managing Audit Trail Collection

- Check the audit policy on the target to ensure you are auditing the activity that you are expecting to see in the reports.
- Check the firewall policy to ensure you are logging the activity you are expecting to see in reports.
- Clear any time filters on reports, and then check time settings on the target and on the AVS. If the time is incorrect, the time recorded against audit events will not be accurate. As a result, the audit events may not be displayed in the time window you expect.
- Check the `/var/log/messages` file on Audit Vault Server and on the Database Firewall for errors.
- Check that the Database Firewall monitoring point is created and running.
- Check that the Database Firewall monitoring point traffic source is correct.

- If the Database Firewall is in monitoring only mode, use the Database Firewall Live Capture utility to verify that traffic is being seen on the relevant traffic source. If necessary, use the File Capture utility to capture traffic to a file and verify (using Wireshark or a similar product) that the traffic being captured is consistent with the settings in the Target Addresses section of your Target configuration.

  > **See Also:**
  >
  > Viewing Network Traffic for a Database Firewall

- Check that you have used the correct Oracle Database service name when configuring the Target Address in your Target configuration.

  Also, have you included all available Oracle Service names in the Target Addresses section of the Target configuration? Unless you intend to define a different firewall policy for each service name, Oracle recommends you omit service name and use only IP address and TCP ports in Target Addresses.
- On the Database Firewall, check the `/var/log/httpd/ssl_access_log` file to confirm that the Audit Vault Server is collecting logs.
- On the Audit Vault Server, check the `/var/dbfw/tmp/processing*` directories and make sure `kernel*.dat` files are arriving in the directory, and then being deleted once the Audit Vault Server has processed them.
- On the Audit Vault Server, check that the `mwecsvc` process is running. For example, run the command:

  ```
  ps -ef | grep mwecsvc
  ```

  If the process is not running, use this command to restart it:

  ```
  service controller start
  ```

L.26 Problems Pairing Oracle Database Firewall and Oracle Audit Vault Server

Review the procedure to follow when you have problems pairing Oracle Database Firewall with Oracle Audit Vault Server.

Problem

I encounter errors when I try to associate a Database Firewall with the Audit Vault Server.

Solution

Check the following:

- Ensure that you have entered the correct Audit Vault Server IP address in the Database Firewall **Certificate** page.

  Log in to the Audit Vault Server console, and click the **Settings** tab. Then click the **Certificate** tab on the main page.
- Ensure that both the Database Firewall server and the Audit Vault Server are configured to use NTP and that each machine is synced to the NTP time server.

> **See Also:**
>
> - Specifying the Server Date, Time, and Keyboard Settings
> - Setting the Date and Time in Database Firewall

L.27 User Names Do Not Appear on Database Firewall Reports

Learn what to do when names do not appear on Database Firewall reports.

Problem

When I generate a Database Firewall report, I do not see user names.

Solution

Check the following possibilities:

- If this is occurring for a Microsoft SQL Server database target, check to make sure that retrieve session information is turned on.
- This problem may be caused by bad network traffic arriving at the Database Firewall. Check for duplicate or missing network packets. You can use the Database Firewall's Live Capture utility to capture network traffic to a file and analyze it.

> **Note:**
>
> Sometimes `unknown_username` is displayed in the **User** field of Database Firewall reports for SQL server. This can be resolved by enabling **Retrieve session information from target DB** option under the **Advanced** tab for the Database Firewall monitoring point. The report may also display `unknown_osusername` in the **OS User** field of Database Firewall reports for SQL server. This information is available to Database Firewall only if the client uses Windows authentication or a trusted connection.

> **See Also:**
>
> - Configuring Advanced Settings for Database Firewall
> - Viewing Network Traffic for a Database Firewall

L.28 Alerts Are Not Generated

Review the resolution to use when alerts that you created are not generated.

Problem

Alerts I have created are not being generated.

Solution

Try the following:

- Examine the alert condition to make sure it is written correctly:

  Log in to the Audit Vault Server console as an auditor, click the **Policy** tab, click **Alerts**, and then click the name of the alert in question.

  > **See Also:**
  >
  > – *Oracle Audit Vault and Database Firewall Auditor's Guide* for help in writing alert conditions.
  >
  > – Using Audit Vault Server Console for more information about logging in to the Audit Vault Server console.

- Restart the job framework on the Audit Vault Server. See My Oracle Support Doc ID 1592181.1.

L.29 Problems Retrieving or Provisioning Audit Settings on Oracle Target

Learn what to do when you encounter problems while retrieving or provisioning Oracle target audit settings.

Problem

I have a problem either retrieving audit settings form an Oracle Database target, or provisioning audit settings to an Oracle Database target.

Solution

If you have problems retrieving audit settings, try the following:

- Check the job status of the retrieval job for errors:

  Log in to the Audit Vault Server console as an auditor, click **Settings**, and then click **Jobs** in the System menu.

- Ensure you have entered the correct connect string in the Oracle Database's target configuration:

  Log in to the Audit Vault Server as an administrator, click the **Targets** tab, and then click the name of this Oracle target. Check the **Target Location** field for the connect string.

  > **See Also:**
  >
  > Target Locations (Connect Strings)

If you have problems provisioning audit settings, and the Oracle Database target has Database Vault enabled, confirm that the Oracle Audit Vault and Database Firewall user you created on this database has the `AUDIT SYSTEM` and `AUDIT ANY` privileges.

L.30 Operation Failed Message Appears When Attempting to Enable Oracle Audit Vault and Database Firewall Policies

Learn how to resolve operation failures when you try to enable Oracle Audit Vault and Database Firewall policies.

Problem

I configured Oracle Audit Vault and Database Firewall for a backup and restore operation. After I completed the procedure, I could not enable an Oracle Audit Vault and Database Firewall policy. The error message `Operation failed. Please contact Oracle Support` appeared.

Solution

During the backup and restore process, Oracle Audit Vault and Database Firewall must perform a restart of the Oracle Audit Vault Server database. The internal tool Java Framework may need to be restarted. To remedy this problem:

1. Log in to Oracle Audit Vault Server.
2. At the command line, run the following command to check the status of the Java Framework:

   ```
   /usr/local/dbfw/bin/javafwk status
   ```

3. If the output says `Java framework process is stopped`, then restart it as follows:

   ```
   /usr/local/dbfw/bin/javafwk start
   ```

L.31 Out of Memory Error Message During Restore

Learn the resolution when you receive an out of memory error message during a restore.

Problem

Encounter `out of memory` error while performing restore task.

Solution

Prior to initiating the restore task, ensure that the RAM size and Disk size in the new system is equal or bigger than the original system. This ensures that the `out of memory` error is not encountered while performing the restore task.

L.32 JAVA.IO.IOEXCEPTION Error

Learn how to resolve a `JAVA.IO.IOEXCEPTION` error.

Problem

SSL peer shuts down incorrectly with the following error:

```
JAVA.IO.IOEXCEPTION: IO ERROR:SSL PEER SHUT DOWN INCORRECTLY
```

Solution

1. Access the target through **SSH**.
2. Change to the following location using the command:

   ```
   cd $ORACLE_HOME/network/admin
   ```

3. Edit the `sqlnet.ora` file. Add parameter *sqlnet.recv_timeout=100000* in the file.
4. Restart the target listener.
5. Once the target listener is started, start the agent, and the audit trail.

L.33 Failed to Start ASM Instance Error

Learn what to do when you receive a `Failed to start ASM instance` error.

Problem

The `avdf-upgrade --confirm` command stops and results in an error. The command may fail for many reasons. The error mainly occurs due to failure in starting or stopping of a service.

The following is an example of `Failed to start ASM instance` error:

```
{{{
[support@avs00161e637973 ~]$ su - root
Password:
[root@avs00161e637973 ~]# /usr/bin/avdf-upgrade --confirm
Please wait while validating SHA256 checksum for
/var/dbfw/upgrade/avdf-upgrade-12.2.0.3.0.iso
Checksum validation successfull for
/var/dbfw/upgrade/avdf-upgrade-12.2.0.3.0.iso
Mounting /var/dbfw/upgrade/avdf-upgrade-12.2.0.3.0.iso on /images
Successfuly mounted /var/dbfw/upgrade/avdf-upgrade-12.2.0.3.0.iso on /images
Starting Oracle High Availability Service
2016-08-05 15:32:09.097:
CLSD: Failed to generate a fullname. Additional diagnostics: ftype: 2
(:CLSD00167:)
CRS-4639: Could not contact Oracle High Availability Services
CRS-4000: Command Start failed, or completed with errors.
Starting ASM instance
Error: Failed to start ASM Instance
Unmounted /var/dbfw/upgrade/avdf-upgrade-12.2.0.3.0.iso on /images
Failed to start ASM Instance
}}}
```

Solution

Rerun the command `avdf-upgrade --confirm`

Executing this command again will get past the `Failed to start ASM instance` error.

L.34 Internal Capacity Exceeded Messages Seen in the /var/log/messages file

Learn how to resolve `Internal capacity exceeded` messages that appear in the `/var/log/messages` file.

Problem

Not all the expected traffic is being captured or logged by the Database Firewall, 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 target on which the issue is observed through the setting of the *MAXIMUM_ENFORCEMENT_POINT_THREADS* collection attribute.

> **See Also:**
>
> Registering Targets

Solution - 2

The size of the buffer used for inter-process communication on the Database Firewall 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 Audit Vault Server 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 Database Firewall processes so that the new setting is used with the command line `/usr/local/dbfw/bin/dbfwctl 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 Audit Vault Server console as the *root* user.
2. Edit the file `/var/dbfw/va/N/etc/appliance.conf`, where *N* is the number of the Database Firewall monitoring points 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 Database Firewall processes so that the new setting is used with the command line `/usr/local/dbfw/bin/dbfwctl 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 Audit Vault Server 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 Database Firewall processes so that the new setting is used with the command line `/usr/local/dbfw/bin/dbfwctl restart`
6. Leave the Database Firewall 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 Database Firewall 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.

L.35 First Archive Or Retrieve Job After Upgrade

Learn what to do if after an upgrade, the first archive or rervireve job submission displays the status of `Starting`.

Problem

After upgrade the first archive or retrieve job submission may display the status as `Starting`.

Solution

Submit the job again. This is a known issue and subsequent submission of job succeeds.

L.36 Audit Vault Agent Installation Fails After HA Pairing Or Separation

Learn what to do after the Oracle Audit Vault installation fails after an HA pairing or separation.

Problem

Installation of Audit Vault agent fails after performing pairing or separation (un-pairing) of Oracle Audit Vault server.

The following command generates agent debug logs during agent installations.

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

Symptoms

The following errors may be found during agent installation in the agent log file:

```
PKIX path validation failed
```

```
signature check failed
```

Solution

After the pairing or separating of Oracle Audit Vault servers, you must download the Audit Vault agent from the GUI and install the agent again after removing the existing Audit Vault Agent.

> **See Also:**
>
> Post High Availability Pairing Steps

If the Audit Vault agent fails to install after pairing or separating of Audit Vault server, then install the Audit Vault agent using `-v` option.

To resolve the above errors, follow the steps mentioned below:

1. Log in to the Audit Vault server as user `root`.
2. Run the following script to generate a new `agent.jar` file.

   ```
   /usr/local/dbfw/bin/priv/update_connect_string_ip.sh
   ```
3. Download the new `agent.jar` file from the GUI.
4. Install the newly downloaded `agent.jar` file.

L.37 Error in Restoring Files

Learn what to do when you encounter errors while restoring files.

Problem

An attempt to restore the data files results in a failure. The restore job completes successfully, however the data files are not restored. There is no information in the restore job log file.

Solution

Check for the following to troubleshoot the issue:

- The restore policy must follow the guidelines listed under the section Configuring Archive Locations and Retention Policies.
- Check the tablespace that needs to be archived and the corresponding tablespace that needs to be purged as per the policy defined.
- Restoring data into empty tablespaces is not possible. Check accordingly.
- In case the tablespace enters the delete period, it is deleted automatically from Oracle Audit Vault Server.
- Every tablespace is uniquely identified by the month it moves offline and the month during which it is purged. They are created automatically based on the policies that you create.
- When the retention policy is changed, the new policy is applied to the incoming data immediately. It does not affect existing tablespaces that adhere to the old policy.
- You can archive the tablespace when it enters the offline period.
- After restoring the tablespace, it is online. Once it is released, it goes offline. The tablespace must be rearchived once released.

L.38 DB2 Collector Fails Due to Source Version NULL Errors

If the DB2 collector fails due to source version NULL errors, then follow these steps.

Problem

The following error or trace is displayed in the collector log file.

```
Caused by: java.lang.ClassNotFoundException:

sun.io.MalformedInputException

at java.net.URLClassLoader.findClass(Unknown Source)

at java.lang.ClassLoader.loadClass(Unknown Source)
```

Solution

Check the Java version on the host system This failure is due to Java SE version 8. Attempt to use Java SE 7.

> **Note:**
>
> This issue may be encountered in releases prior to `12.2.0.11.0`.

L.39 DB2 Collector Fails Due to Database Connection or Permission Issues

If the DB2 collector fails due to database connection or persmission issues, then follow these steps.

Problem

The following error or trace is displayed in the collector log file.

```
Caused by: oracle.ucp.UniversalConnectionPoolException: Cannot get Connection
from Datasource: java.sql.SQLSyntaxErrorException: [Audit Vault][DB2 JDBC Driver]
[DB2]<User> DOES NOT HAVE PRIVILEGE TO PERFORM OPERATION EXECUTE ON THIS OBJECT
NULLID.DDJC360B
```

Solution

Run the following command for successful execution of DB2 collector:

```
grant execute on package NULLID.DDJC360B to <User> (user while registering
the target)
```

L.40 ORA-12660 Error While Registering Target

Learn how to resolve the ORA-12660 error.

Problem

Audit Vault agent fails with *ORA-12660* error.

Solution

The server encryption is set to `REQUIRED` in on-premises by default. Set the server encryption to `ACCEPTED` or `REQUESTED` or `REJECTED`.

> **Note:**
>
> `REJECTED` is not a recommended option. The following table describes these options in detail.

Table L-1 Server Encryption Types

Option	Description
`ACCEPTED`	The server does not enable both encrypted and non-encrypted connections. This is the default value in case the parameter is not set.
`REJECTED`	The server does not enable encrypted traffic.
`REQUESTED`	The server requests encrypted traffic if it is possible, but accepts non-encrypted traffic if encryption is not possible.
`REQUIRED`	The server accepts only encrypted traffic.

L.41 Audit Trail Performance Issues Occur After Audit Vault Server Upgrade

Learn what to do when audit trail performance issues occur after upgrading Oracle Audit Vault Server.

Problem

You might experience audit trail performance issues after upgrading Oracle Audit Vault Server.

Solution

The `audit_trail_id_idx` index that is created resolves the performance issues encountered. However, you must retain sufficient disk space if there is large amount of event data for the period prior to upgrading Oracle Audit Vault Server. The amount of disk space required is about 5% of the total event log data size.

L.42 Failures Due to Dropping Users

Learn how to resolve failures that occur when dropping users.

Problem

Failed to drop the user with an error message and the user was not listed in the Audit Vault Server GUI.

Solution

Contact Oracle Support for the best workaround and to drop the user manually using **SQL*Plus**.

L.43 Failure of Agent Automatic Upgrades

Learn what to do when agent automatic upgrades fail.

Problem

The automatic upgrade of the Agent fails with the following error. This is because the Agent is unable to connect to the Audit Vault Database.

```
Message: Exception occurred while updating Agent.
Cause: Unable to connect to AV Server.
Note: Agent will try to re-connect automatically in 10 seconds.
```

Solution

The Agent attempts to connect to the Audit Vault Database and auto upgrade after 10 seconds. Check the Oracle Audit Vault Database connection or contact Oracle Support.

L.44 Some Services May Not Start After Backup

Learn what to do when services fail to start after a backup.

Problem

The system may not be stable after a cold backup operation failed to complete.

Solution

Oracle recommends that you reboot the system if there is a failure while performing a cold backup operation.

L.45 Data Overflow Issues in the Oracle Audit Vault UI

Learn how to resolve data overflow issues in the Oracle Audit Vault UI.

Problem

The **Recently Raised Alerts Report** region appears on your dashboard and displays the list of alerts with data overflowing in the **Audit Vault GUI**. This may occur when you launch the GUI using Internet Explorer and the Microsoft Windows Server operating system.

Solution

To fix this issue and to display the data properly on the **Audit Vault GUI**, you should make minor changes to the Internet Explorer browser settings. Press **F12** and click the **Emulation** tab.

Change the **Document mode** and **Browser profile** fields from the default settings. For example, change the **Document mode** value to `10` from the drop down menu and change the **Browser profile** field to `Desktop`.

L.46 Oracle Audit Vault Agent is Unreachable and the Transaction Log Audit Trail is Frozen in Starting Status

Learn what to do when the Oracle Audit Vault Agent is unreachable and the transaction log audit trail is frozen in `Starting` status.

Problem

The status of Oracle Audit Vault Agent is unreachable from the **AV GUI**. The status of the `Transaction Log` audit trail persistently remains in the `Starting` status.

This may be due to a user application that is blocking the creation of streams by `ORAAUDIT` user.

Symptom

The `Transaction Log` audit trail does not start. The following information may be found in the thread dump that is taken using `jstack` tool:

```
oracle.av.platform.agent.collfwk.impl.redo.RedoCollector.sourceSetup(RedoColle
ctor.java:634)
```

Solution

Terminate the user application that is blocking the creation of streams. Restart the `Transaction Log` audit trail.

L.47 Scheduled PDF or XLS Reports Result in a Hung State

To resolve a hung state that occurs for scheduled PDF or XLS reports, follow these recommendations.

Problem

Scheduled PDF or XLS reports remain incomplete for an extended period of time or ramin in q `RUNNING` state.

Solution

You can schedule reports to be sent to other users in PDF or XLS formats. Avoid triggering or scheduling concurrent long-running reports at the same time. Producing PDF and XLS reports occupies a lot of system resources because there is a significant amount of data involved. Scheduled concurrent long-running reports can remain in a hung state indefinitely. The reports

must be scheduled with staggered intervals in between. For example, run the reports at intervals of `5`, `10`, or `20` minutes.

L.48 Pending Reports Remain in Scheduled Status

To resolve pending reports that remain in scheduled status, follow these steps.

Problem

Many reports are stuck in `scheduled` or `pending` status. These reports may never be completed and may be stopped.

Solution

This may be due to an issue with the Java Framework process in the background. Use these steps to check and resolve this issue:

1. Log in to the CLI as `support` user.
2. Switch to `root` user using the command:

   ```
   su root
   ```

3. Run the following command to check the status of the Java Framework:

   ```
   systemctl status javafwk
   ```

4. Stop the Java Framework even if it is running. Run the following command:

   ```
   systemctl stop javafwk
   ```

5. Run the following command to start the Java Framework:

   ```
   systemctl start javafwk
   ```

6. Run the following command to restart the Java Framework:

   ```
   systemctl restart javafwk
   ```

Use the following procedure to check the status of the reports from the operating system logs after running one of the procedures mentioned above and restarting the Java Framework:

1. Log in to AVCLI as *admin* user.
2. Run the following command to enable diagnostics for the reports:

   ```
   ALTER SYSTEM SET loglevel=ReportLog:DEBUG|JfwkLog:DEBUG;
   ```

3. The diagnostics can also be enabled using the Oracle Audit Vault Server console by following these steps:
   a. Log in to the console as `admin` user.
   b. Click **Settings** tab.
   c. Click on **Diagnostics** on the left navigation menu.
   d. Select **Debug** against **Report Generation**.
   e. Click **Save**.
4. Run a PDF report. For example, **Activity Overview**.
   a. Log in to the Oracle Audit Vault Server console as `auditor`.
   b. Click **Reports** tab.
   c. Click **Activity Reports** under **Built-in Reports**.

d. In the **Activity Reports** tab on the screen, you can schedule a report and view the generated report.

5. After a while, check on the `/var/lib/oracle/dbfw/av/log` file. For example, **av.report*** file. It contains the PDF/XLS report generation debug logs.

L.49 Audit Vault Log Displays a Message to Install WinPcap and OpenSSL

To resolve the Audit Vault log message to install WinPcap and OpenSSL, follow these steps.

Problem

The Host Monitor Agent can collect audit data from Windows 2016 servers. A message displays alerting you to install `WinPcap` and `OpenSSL`.

Solution

A set of `DLL` files may be causing issues. Run the following procedure to resolve this problem:

1. Search for the following files in the system:
   - `ssleay32.dll`
   - `libeay32.dll`
   - `wpcap.dll`
   - `packet.dll`
2. Append the file names with the `.bk` format notation.
3. Go to **Control Panel** then to **Uninstall Programs** and uninstall `OpenSSL` and `WinPcap`.
4. Reinstall `WinPcap` and `OpenSSL 1.0.2.q (64-bit)`. The `DLL` files are restored to Windows system folder.
5. Check the **Control Panel** to verify that these two programs are installed.
6. Go to `C:\Windows\System32` or `C:\Windows\SysWOW64` folders and search for the above four *DLL* files. At least one file for each *DLL* must be present without the `.bk` extension.
7. Go to the OpenSSL installation location and search for `libssl-1_1-x64.dll` and `libcrypto-1_1-x64.dll` files. One for each type is available.
8. Upon confirmation, add the `C:\Windows\System32` or `C:\Windows\SysWOW64` to the path variable.
9. Restart the trail.
10. If the network audit does not start, then check the `collfwk` logs present at `<AgentHome>\av\log` location. If the following message is available in the `collfwk` log, then check the Host Monitor Agent logs present at `<AgentHome>\hm\log` location.

    `<AgentHome>` refers to the Audit Vault Agent installation directory.

> **Note:**
>
> Continue with the remaining steps if your installation is 12.2.0.10.0 or before. The steps are not required for release 12.2.0.11.0 and later.

11. If the following message is available in the Host Monitor Agent log, then execute the remaining procedure:

    ```
    Invalid AVS Credentials provided
    ```

12. Open the `av/conf/bootstrap.prop` file.
13. Copy the following line:

    ```
    CONNECT_STRING_PARAM_POSTFIX=9999
    ```

14. Paste this line in the `hm/bootstrap.prop` file.
15. Restart the trail.
16. In case the network audit trail starts without any errors, then the collection status on the Audit Vault Server console confirms the same.
17. Navigate to **AVAUDIT** then to **Target** then **Firewall Policies** and, finally, **Log All**.
18. Connect to the target database instance using SQL Developer, or any other tool.
19. Generate the traffic for collecting data.
20. It must be recorded in the reports of the `event_log` table.

L.50 Error OAV-47409 While Managing Archive Locations

Learn what to do when you receive the `OAV-47409` error while managing archive locations.

Problem

The following error message displays in the **Auto Archive Message** column under **Manage NFS Locations** tab:

```
OAV-47409: Absolute path does not exist on remote filesystem
ORA-06510: PL/SQL: unhandled user-defined exception
```

The configured path of the archive location is either missing or outside of the remote filesystem.

Cause

The NFS export directory configured on the AVDF server did not have read/write permissions assigned to the Oracle user.

Solution-1

The value under **Auto Archive Order** column is set to 0 [zero]. The system has set this value as the archive location is problematic. You must ensure that the NFS location issue is resolved to a valid directory on the remote filesystem. Upon resolving this issue, set the value under

Auto Archive Order column to `1` or higher. This sets the appropriate priority for the auto archive order.

Solution-2

Check if the owner of the NFS archive location is `oracle:oinstall`.

1. If not, run the following commands:

```
# chown oracle:oinstall /archive/archive
```

2. Change the directory to the archive location:

```
# cd /archive
```

3. On the AV server, execute the following command to check the existence and the permissions:

```
# ls -lrth


drwxrwxrwx. 2 root   root      16K Jan  2 15:54 lost+found
drwxrwxr-x. 2 oracle oinstall 4.0K Jan  4 11:30 archive
```

4. Use the `pwd` command to know the present working directory and change to `/archive/archive` directory by using the following command:

```
# cd archive
```

Now try to configure the NFS, it is expected to function correctly.

L.51 Error OAV-47402 While Defining Archive Locations Using NFS Mount Point

Learn what to do when you receive the `OAV-47402` error while defining archive locations.

Problem

An error is observed after registering the archive location using NFS mount point through *AVCLI*. The created remote file system shows inaccessible when running the `SHOW STATUS` command. The following error is observed when running `ALTER REMOTE FILESYSTEM <file system name> MOUNT` command. However, the process of defining or creating the archive location is successful.

```
OAV-47402: Unable to mount export /exabackup from host <host Ip address>
```

Solution

This issue is observed when using NFS version v3 only. Reach out to the NAS storage support or NFS administrator support team to verify if the mount point in the NFS server is properly configured. It must support both v3 and v4 to integrate with Oracle AVDF.

> **Note:**
>
> NFS version v3 only is not supported for Oracle AVDF releases 20.3 and prior. It is supported starting Oracle AVDF release 20.4.

Follow the steps documented in My Oracle Support Doc ID 2232033.1 to verify if the mount point in the NFS server is properly configured.

See Defining Archive Locations for complete information.

L.52 Audit Trail Stopped After Relocating Windows Event Log Files

Use this procedure when the audit trail stops after you relocate the Windows event log files.

Problem

Windows event log relocation causes audit trail to be stopped.

Solution

Follow this procedure to resolve this problem:

1. Stop the audit trail.
2. Drop the audit trail.
3. Restart the audit trail. The new trail recognizes the new location for event logs.

L.53 Missing or Incomplete Client Information in Oracle Database Firewall Logs

Learn how to resolve missing or incomplete client information in Oracle Database Firewall logs.

Problem

Empty client information in the Oracle Database Firewall logs after upgrading Oracle Audit Vault and Database Firewall. The logs that are generated are missing some of the client information such as the user name.

> **Note:**
>
> This issue occurs only when you are in `DAM` mode deployment of Oracle Database Firewall. You will not experience this issue in the `Proxy` mode deployment.

Cause

Oracle Database Firewall records information that is related to the TCP sessions during inspection and it saves this data to disk. This recorded information includes client user names and other metadata about the connection. When Oracle Database Firewall processes are restarted after a configuration change or an upgrade, Oracle Database Firewall continues to generate logs accurately by re-reading this cached information.

The format of the cache file has changed in the recent releases. Oracle Database Firewall may not be able to read the file in the old format. Therefore, existing client connections to the database that were established before performing the upgrade may not retain certain information such as client user names. This can lead to logs missing information such as the client username.

Solution

Restart the database clients.

L.54 Issues with Retrieving Session Information Through Clients Connecting to Microsoft SQL Server

Learn what to do when you have issues retrieving session information through clients that connect through Microsoft SQL Server.

Problem

Database Firewall is unable to retrieve session information through some clients (for example, MS SQL Server Management Studio) as the information is encrypted. You can retrieve session information for non Oracle databases to obtain the name of the database user, operating system, and client program that originated a SQL statement.

Symptom

Audit Reports show unknown user names and unknown program names where the target is Microsoft SQL Server.

Solution

Ensure the following steps are accurate while registering Microsoft SQL Server as a target.

1. In the **User Name** field, enter the user name of the system administrator.
2. In the **Password** field, enter the password of the system administrator.
3. In the **Host Name / IP Address** field, enter the IP address of the SQL Server.
4. In the **Port** field, enter the port of the SQL server listening port.
5. In the **Service Name** field, enter a valid database service name on SQL Server. In case the database service name is not correct, then SQL server DDI requests fail on the SQL Server with invalid request error.

> **Note:**
>
> If the secured type is not Oracle, then the **Service Name** field must be empty. This field is designated for a specific Oracle Service Name (OSN) and is not applicable to any other database type. If this field is not blank, then no traffic will be recorded, as per the reported symptoms.

See Also:

- Registering Targets
- Setting Permissions to Retrieve Session Information in Microsoft SQL Server

L.55 Performance Issues Due to High Memory Usage

Learn how to address performance issues in Oracle AVDF with very large deployments.

Problem

Audit Vault Server in large deployments may have performance issues due to increased memory usage.

Solution

- Ensure the Audit Vault Server is sized as per the sizing guidelines documented in *Audit Vault and Database Firewall Best Practices and Sizing Calculator for AVDF 12.2 and AVDF 20.1 (Doc ID 2092683.1)*.
- Audit Vault Server has Transparent Huge Pages set by default which should work in most cases. However, in some cases it has to be disabled by setting `transparent_hugepages` to never. This helps in improving the performance. For detailed the steps, refer to *Oracle Linux 7 - How to disable Transparent HugePages for RHCK kernel? (Doc ID 2066217.1)*.
- If you still face performance issues after applying the above mentioned solution, contact Oracle Support.

L.56 httpd Crash Issue on Database Firewall

Learn how to fix `httpd` crash issue in Database Firewall.

Problem

The `httpd` process in Database Firewall may crash under some circumstances.

Symptom

The status of the Database Firewall instance appears `Down` in the Audit Vault Server console. The Database Firewall logs are not transferred to the Audit Vault Server.

The following is observed in the log files of the impacted Database Firewall instance. The `httpd.service` file in `/etc` is symlinked to the file in `/usr` path.

```
# ls -l /etc/systemd/system/multi-user.target.wants/httpd.service

lrwxrwxrwx. 1 root root 37 Nov 27 09:26 /etc/systemd/system/multi-
user.target.wants/httpd.service -> /usr/lib/systemd/system/httpd.service

# ls -lL /etc/systemd/system/multi-user.target.wants/httpd.service

-rw-r--r--. 1 root root 752 Nov 10 20:33 /etc/systemd/system/multi-
user.target.wants/httpd.service

#
```

Solution

Follow these steps to change the configuration of the system and restart the `httpd` process:

1. Log in to the Database Firewall instance as *root* user.
2. Check and confirm that the above mentioned symptom exists.
3. Copy the base file from `/usr` to `/etc` by running the following command:

```
# install -m 0644 -o root -g root /usr/lib/systemd/system/httpd.service /etc/
systemd/system/httpd.service
```

4. Edit the file in `/etc` and find the below mentioned `Service` block:

```
# vi /etc/systemd/system/httpd.service

...

[Service]

Type=notify

EnvironmentFile=/etc/sysconfig/httpd

ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND

...
```

5. Modify the file and add the following code to include the restart failure directive. The file looks like the folllowing:

```
...
[Service]
Restart=on-failure
Type=notify
EnvironmentFile=/etc/sysconfig/httpd
ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND
...
```

6. Save the file.
7. Disable and re-enable the service to fully apply the following changes:

```
# systemctl disable httpd
Removed symlink /etc/systemd/system/multi-user.target.wants/httpd.service.
# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/
httpd.service to /etc/systemd/system/httpd.service.
#
```

8. Verify the following changes:

```
# sha256sum -c - <<EOF
eac607c17f2c122619b3e1459eafdfef6bde003d24964891aa506735df4f55c2  /etc/
systemd/system/multi-user.target.wants/httpd.service
EOF
```

```
/etc/systemd/system/multi-user.target.wants/httpd.service: OK
#
```

9. Reload the `systemd` configuration and restart `httpd` by running the following commands:

```
# systemctl daemon-reload


# systemctl restart httpd
```

10. Verifying the service is enabled by running the following command:

```
# systemctl list-unit-files | grep http
```

11. Observe the following output:

```
httpd.service enabled
#
```

12. If the daemon subsequently fails, the `systemd` will restart it, and write the following example audit trail to the system log:

```
Nov 27 08:38:09 example systemd: httpd.service: main process exited,
code=killed, status=11/SEGV
Nov 27 08:39:40 example systemd: httpd.service stop-sigterm timed out.
Killing.
Nov 27 08:39:40 example systemd: Unit httpd.service entered failed state.
Nov 27 08:39:40 example systemd: httpd.service failed.
Nov 27 08:39:40 example systemd: httpd.service holdoff time over, scheduling
restart.
Nov 27 08:39:40 example systemd: Stopped The Apache HTTP Server.
Nov 27 08:39:40 example systemd: Starting The Apache HTTP Server...
Nov 27 08:39:40 example systemd: Started The Apache HTTP Server.
```

L.57 Issue with Retrieval of Return Row Count

Learn how to fix the issue related to retrieval of return row count.

Problem

Database Firewall captures the number of rows returned by a `SELECT` query and display them in reports under the column **Row Count**.

If the database takes a while to generate response result set, then return row count may not be extracted due to timeout configuration.

Workaround

Follow these steps to adjust the timeout interval:

1. Log in to the Database Firewall through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Change to `/var/dbfw/va` directory.

3. Identify the Database Firewall monitoring point by searching for the target name configured in the Audit Vault Server. Run the following command:

   ```
   grep -lr <TARGET NAME> *
   ```

4. Find the monitoring point number from the output which contains the name and path of the configuration file. For example: `1/etc/appliance.conf`. In this example, `1` is the monitoring point number.
5. Change the directory to the identified monitoring point and open configuration file of the appliance.
6. Search for the following entry in the file:

   ```
   MAX_LOG_FILE_TIMERANGE
   ```

7. Modify the `MAX_LOG_FILE_TIMERANGE` line to reflect the required time range in seconds. For example, if you wish to change the time range to 5 minutes, then the configuration line should be `MAX_LOG_FILE_TIMERANGE=="300"`.
8. Save the changes.
9. Run the following command to restart the Database Firewall processes so that the new setting takes effect:

   ```
   /usr/local/dbfw/bin/dbfwctl restart <monitoring point number>
   ```

   In this case the monitoring point number was `1`.

   Hence, the command should be:

   ```
   /usr/local/dbfw/bin/dbfwctl restart 1
   ```

> **Note:**
>
> Increasing the timeout configuration delays the availability of captured SQL statements in the reports and any alerts configured for the same. Use your discretion while configuring the above value close to the actual query completion time.

L.58 Unable to Log in to the Oracle AVDF Appliance through SSH

Learn how to fix log in issue to Oracle AVDF appliance.

Problem

The user is unable to log in to the Oracle AVDF appliance through SSH. This may be because of using old SSH clients to log in to the Oracle AVDF appliance.

Workaround

Log in to ARU (Automated Release Updates). Apply the patch number 32287150 that solves the problem.

> **Note:**
>
> This patch must be applied on Oracle AVDF 20.3 and later only.

L.59 Error When Changing IP Address of Management Interface

Learn how to resolve the error encountered when changing the IP address of the Management Interface.

Problem

The Management Interface IP address is the IP address of the Database Firewall which was used to register the Database Firewall in the Audit Vault Server console.

In Oracle AVDF 20.1, the following error may be encountered while attempting to change the IP address of the Management Interface:

```
Operation failed OAV-46981: Unable to connect to Database Firewall with IP
<ipaddress>
```

Solution

This error may come up because the IP Address of the Database Firewall is changed successfully. However, there may be a delay in the response from Database Firewall. It may take a few seconds for the network update on the Database Firewall and for the system to settle.

Click **Save** and **Close** buttons to exit the dialog. Do not click on the cross (X) mark in the top right corner of the dialog.

L.60 Unable to Configure Microsoft SQL Server XEL Audit Trail After Upgrade

Problem

The following error is observed while configuring Microsoft SQL Server XEL audit trail on Audit Vault Server after upgrading to Oracle AVDF 20.3:

```
[oracle][SQLServer JDBC Driver][SQLServer]VIEW SERVER STATE permission was denied
on object 'server', database 'master'
```

Solution

Follow these steps to resolve this issue in Oracle AVDF 20.3:

1. Create a new user on Microsoft SQL Server target database.
2. Grant the necessary privileges. See *Oracle AVDF Administrators Guide* for complete information.
3. Modify the registered target with the newly created user credentials.
4. Configure the Microsoft SQL Server XEL audit trail.

This issue is resolved in Oracle AVDF 20.4. Follow these steps after upgrading to Oracle AVDF 20.4 (or later):

1. Revoke audit data collection privileges by running 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"
   ```

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"
   ```

3. Configure the Microsoft SQL Server XEL audit trail.

L.61 Transaction Log Audit Trail Stops Due to an Error While Parsing XML File Containing Emoji

Problem

Transaction Log audit trail stops while parsing a file that contains emoji. The following error is observed in the Agent logs:

```
javax.xml.stream.XMLStreamException: ParseError at [row,col]
```

Solution

Follow these steps to resolve this error:

1. Run the following command to stop the Audit Vault Agent:

   ```
   AGENT_HOME/bin/agentctl stop
   ```

   .

2. Delete the *sjsxp.jar* file present in the `AGENT_HOME/av/jlib` directory.
3. Run the following command to start the Audit Vault Agent:

   ```
   AGENT_HOME/bin/agentctl start
   ```

   .

L.62 Unable to Find the FIPS Status for Database Firewall Instance

Learn how to fix the error when the FIPS status for a Database Firewall instance is not displayed in the Audit Vault Server console.

Problem

The FIPS status for the Database Firewall instance could not be determined from the Audit Vault Server console.

Solution

Perform the following checks to determine the root cause of the problem:

- The Database Firewall version is 20.4 or later.
- Check the network connectivity between the Audit Vault Server and the two Database Firewall instances.
- Ensure the Audit Vault Server's certificate is correctly copied or installed on the Database Firewall instance.
- Check if the Audit Vault Server can connect to the Database Firewall by confirming that the status of the Database Firewall instance is `online`.

If none of the above points are helpful in identifying the cause of the problem, then contact Oracle Support.

L.63 Unable to Modify the Database Firewall FIPS Mode Through Audit Vault Server Console

Learn how to fix the error when the FIPS mode cannot be modified through the Audit Vault Server console.

Problem

This could be caused due to a communication issue between the Audit Vault Server and the Database Firewall instances.

Solution

Perform the following checks to determine the root cause of the problem:

- The Database Firewall version is 20.4 or later.
- Check the network connectivity between the Audit Vault Server and the two Database Firewall instances.
- Ensure the Audit Vault Server's certificate is correctly copied or installed on the Database Firewall instance.
- Check if the Audit Vault Server can connect to the Database Firewall by confirming that the status of the Database Firewall instance is `online`.

If none of the above points are helpful in identifying the cause of the problem, then contact Oracle Support.

L.64 The FIPS Status on Both the Database Firewall Instances is Different

Learn how to fix the error when the FIPS mode is different on both the Database Firewall instances.

Problem

The FIPS mode is different on both the Database Firewall instances. This could be caused when FIPS mode is manually changed on one of the Database Firewall instances. It can also be caused when such an attempt to manually change the FIPS mode failed.

Solution

All the Database Firewall instances that are part of high availability must have the same FIPS 140-2 mode. The FIPS 140-2 status of the Database Firewall instances must either be `Off` or `On`.

FIPS 140-2 mode can be disabled or enabled on both the Database Firewall instances. In case, these two instances have different FIPS mode, then an error message is displayed on the screen.

Verify the high availability status of the Database Firewall instances, and change the FIPS mode again.

L.65 After Restarting Secondary Audit Vault Server, the Primary Instance Fails to Switchover

Learn how to fix a switchover issue on the primary Audit Vault Server, after the secondary instance is restarted.

Problem

After restarting the secondary Audit Vault Server, the switchover status of the primary Audit Vault Server shows `NOT ALLOWED` state.

This status of the primary Audit Vault Server is not recoverable and the following error messages appear and are repeated every 50 seconds on the secondary Audit Vault Server:

```
<Date> <avs-instance-name> observerctl: com.oracle.avs.observerctl DEBUG -
DGMGRL:[W000 <date and timestamp>] The primary database has requested a
transition to the UNSYNC/LAGGING state with the standby database DBFWDB_HA2.
<Date> <avs-instance-name> observerctl: com.oracle.avs.observerctl DEBUG -
DGMGRL:[W000 <date and timestamp>] Permission granted to the primary database
to transition to LAGGING state with the standby database DBFWDB_HA2.
<Date> <avs-instance-name> observerctl: com.oracle.avs.observerctl DEBUG -
DGMGRL:[W000 <date and timestamp>] Reconnect interval expired, create new
connection to primary database.
<Date> <avs-instance-name> observerctl: com.oracle.avs.observerctl DEBUG -
DGMGRL:[W000 <date and timestamp>] The primary database has been in LAGGING
state for 7138 seconds.
```

Solution

In case the primary Audit Vault Server's switchover status goes into `NOT ALLOWED` status after restarting the secondary instance, then follow the steps mentioned in *MOS Note (Doc ID 1258074.1)* to restart the standby Audit Vault Server.

L.66 Incorrect Syntax Near Connectivity Entry in Audit Logs

Learn how to fix incorrect syntax error entry in audit logs.

Problem

When attempting to add an audit trail for Microsoft SQL Server, the Audit Vault Agent attempts to acquire a target connection using JDBC driver. After the connection is established, a test query is sent to validate the connection by the JDBC driver.

This test query may generate the following error:

```
Incorrect syntax near 'Connectivity'
```

This error is visible in the database audit records.

Solution

Starting Oracle AVDF release 20.6, to avoid unnecessary logging of records or events due test queries in the target database, define the collection attribute as follows:

```
av.collector.validateConnectionOnBorrow = false
```

> **See Also:**
>
> Microsoft SQL Server Plug-in for Oracle Audit Vault and Database Firewall

L.67 Certificate Regenerate Failure Error

Learn how to fix a certificate regenerate failure error.

Problem

In case the certificate regenerate operation fails, then one of the possible reasons can be the incorrect date and time of the appliance (Audit Vault Server or Database Firewall).

Solution

Specify the correct time, and then run the following command to regenerate the certificate:

```
/usr/local/bin/gensslcert create-certs
```

To retrieve the details about certificate expiry date, run the following command:

```
openssl x509 -enddate  -startdate -noout -in {certificate path}
```

For example:

```
openssl x509 -enddate  -startdate -noout -in /usr/local/dbfw/etc/cert.crt
notAfter=Oct 17 17:44:53 2022 GMT
notBefore=Sep 14 17:44:53 2021 GMT
```

> **Note:**
>
> The audit trails go to `UNREACHABLE` state for about 45 minutes after the certificates are rotated and all the relevant services are restarted. The trails continue to work normally after that. This behavior is observed in Oracle AVDF release 20.6 only.

L.68 User Entitlement or Audit Policy Job Stuck in Running State

Learn how to manage the user entitlement or audit policy job stuck in `RUNNING` state.

Problem

The user entitlement job or audit policy job is stuck in `RUNNING` state for a long time. This job is stuck and has to be manually stopped.

Workaround

This issue may be due to an issue with the Java Framework process in the background. Follow these steps and submit the job again:

1. Log in to the Audit Vault Server as *support* user through SSH.
2. Switch to *root* user by running the following command:

   ```
   su root
   ```

3. Restart the Java Framework by running the following command:

   ```
   systemctl restart javafwk
   ```

L.69 Audit Trails are Toggling Between COLLECTING and UNREACHABLE Status

Learn how to fix the incorrect audit trail status issue.

Problem

The **Audit Trails** tab in the Audit Vault Server console displays the status of all the audit trails. Some audit trails are continuously toggling between the status `COLLECTING` and `UNREACHABLE`.

The trails go to `UNREACHABLE` state if they take more than 120 seconds (2 heartbeat intervals) to update the trail status. This can happen if either the target or Audit Vault Server is temporarily loaded, causing the trails to take more time to update the trail status.

Solution

Consider increasing the heartbeat interval to 120 seconds. Currently, the default value is 60 seconds. Run the following command as *avsys* user:

```
exec avsys.adm.add_config_param('SYS.HEARTBEAT_INTERVAL', 120);
```

> **Note:**
>
> This scenario is applicable for Oracle AVDF releases 20.5 and earlier, where the default value is 60 seconds. Starting with Oracle AVDF 20.6, the default value is 120 seconds.

L.70 Displaying Job Status Takes Lot of Time in the Audit Vault Server Console

Learn how to resolve the **Jobs** dialog issue.

Problem

The **Jobs** dialog in the **System** tab takes lot of time to load and to display the jobs and their current status.

Solution

Delete unwanted or old data from the Status column. This resolves the issue and the Jobs dialog displays the required information.

For example: Delete unwanted or old data from the `avsys.job_status` table that is more than 30 days old using the following SQL query:

```
Delete from job_status
where status = 'Completed'
and status_time < sysdate - 30;
```

L.71 Microsoft SQL Server Database Audit Trails are in Stopped State After Upgrading Java

Learn how to fix issue when audit trails belonging to Microsoft SQL Server database go to stopped state after upgrading Java version u291 or greater.

Problem

Audit trails that belong to Microsoft SQL Server database are not collecting audit data. This issue is observed after upgrading the Java version to u291 or greater and when Microsoft SQL Server target's connect string is one of the following:

- `jdbc:av:sqlserver://<MSSQL Host name>:<Port number>;encryptionMethod=SSL; validateServerCertificate=false;`

- `jdbc:av:sqlserver://<MSSQL Host name>:<Port number>;encryptionMethod=SSL;validateServerCertificate=true; trustStore=<key store jks path>;trustStorePassword=<keystore password>;extendedOptions=enableCipherSuites=SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA`

Solution

Modify the connect string for Microsoft SQL Server database (in Audit Vault Server console or AVCLI) to one of the following:

- `jdbc:av:sqlserver://<MSSQL Host name>:<Port number>;encryptionMethod=SSL;validateServerCertificate=false;CryptoProtocolVersion=TLSv1.2;`
- `jdbc:av:sqlserver://<MSSQL Host name>:<Port number>;encryptionMethod=SSL;validateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;trustStore=<key store jks path>;trustStorePassword=<keystore password>;extendedOptions=enableCipherSuites=SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA`

L.72 Unable to Delete Database Firewall

Learn how to fix an issue observed when attempting to delete Database Firewall.

Problem

An error `OAV-47704` is observed when attempting to delete Database Firewall. This issue is observed in the following scenario:

- Oracle AVDF releases 20.1 to 20.5
- Audit Vault Server is upgraded to Oracle AVDF 20, but Database Firewall is not upgraded to Oracle AVDF 20
- Error observed in the Audit Vault Server console or in AVCLI

Solution

This issue is fixed in Oracle AVDF release 20.6. In case the installed version is Oracle AVDF releases 20.5 and earlier, then follow these steps:

1. Log in to the Audit Vault Server through SSH.
2. Switch user to root:

   ```
   su root
   ```

3. Switch user to dvaccountmgr:

   ```
   su dvaccountmgr
   ```

4. Start *SQL*Plus* connection without the username or password:

   ```
   sqlplus /nolog
   ```

5. Unlock *avsys* user and assign a password by running the command:

   ```
   alter user avsys identified by <pwd> profile default account unlock;
   ```

6. Run the command:

   ```
   exit
   ```

7. Start *SQL*Plus* connection without the username or password:

   ```
   sqlplus /nolog
   ```

8. In *SQL*Plus* run the command:

   ```
   connect avsys
   ```

9. Enter the password when prompted. Alternatively, run the command:

   ```
   connect <avsys/password>
   ```

10. Run the following SQL query:

    ```
    select id from avsys.firewall where name= '<firewall_name> ' and
    deleted_at is null;
    ```

11. Make a note of the Database Firewall ID.
12. Run the command:

    ```
    update avsys.firewall set software_version='<avs_version>' where
    id=<firewall_id>;
    ```

    For example: `update avsys.firewall set software_version='20.5.0.0.0' where id=<firewall_id>;`

13. Run the command:

    ```
    commit;
    ```

14. Repeat the process for any other Database Firewall instance that needs to be deleted.
15. Run the command:

    ```
    exit
    ```

16. Attempt to delete the Database Firewall instance from the Audit Vault Server console or through AVCLI.

L.73 Issue in Language Setting of the Audit Vault Agent

Learn how to fix the language setting in Audit Vault Agent.

Problem

Unable to change or set the language in Audit Vault Agent. Audit Vault Agent supports languages other than English.

Audit Vault Agent uses the language specified in the locale settings of the host machine (Agent machine), provided the language is supported. In case the specific language is already set on the system, then there is no need to change the settings for the Agent to use the specific language.

Solution

The locale settings for the Windows platform can be changed through the **Control Panel** on the Windows host machine.

To change the locale settings on Linux/Unix/AIX/Solaris platform, set the `LC_ALL` and `LANG` environment variables.

For example:

```
export LC_ALL=fr_FR.iso88591


export LANG=fr_FR.iso88591
```

L.74 Unable to Create a Database Firewall Monitoring Point

Learn how to fix an error while creating a Database Firewall monitoring point.

Problem

An attempt to create a Database Firewall monitoring point using the target host name does not succeed.

Symptom

- Failure to create a Database Firewall monitoring point using the target host name displays the status as `Starting`. The status changes to `Unreachable` after a while.
- The `/var/log/messages` file in Database Firewall contains an error similar to the following:

```
May 10 11:06:02 dbfw08002718dd46 hostname_lookup.rb[19691]:
foobar.example.com.oracle.dbfw.hostname-lookup WARN - ODF-10505: Failed to
resolve hostname:
Unable to resolve the hostname ["hostname1.foobar.example.com"].
Verify DNS settings. Hostname resolution will be tried every minute.
```

Solution

DNS is not configured and hence the above error is observed. Configure the DNS and attempt to create the Database Firewall monitoring point again.

In case DNS is configured, verify the DNS settings. Attempt to resolve the host name is made once every minute.

L.75 Issue with Configuring or Managing Oracle AVDF through Oracle Enterprise Manager Cloud Control

Learn how to solve an issue with configuring or managing Oracle AVDF through Oracle Enterprise Manager Cloud Control.

Problem

Unable to configure or manage Oracle AVDF through Oracle Enterprise Manager Cloud Control.

Solution

Oracle AVDF plug-in is an interface within Oracle Enterprise Manager Cloud Control for administrators to manage and monitor Oracle AVDF components. Refer to System Monitoring Plug-in User's Guide for Audit Vault and Database Firewall in case of any issues when configuring the Oracle EM plug-in.

Refer to Compatibility with Oracle Enterprise Manager to check the supported versions of Oracle Enterprise Manager with Oracle AVDF 20.

L.76 Unable to Connect to Audit Vault Server through Console or SSH

Learn how to resolve if you are unable to log in to Audit Vault Server through the console or SSH.

Problem

Unable to log in to the Audit Vault Server console or through SSH as *opc* user.

The following error is displayed when attempting to connect through SSH as *opc* user:

```
remote side unexpectedly closed network connection
```

The following error is displayed when attempting to connect through the Audit Vault Server console:

```
internal server error 500
```

Solution

Oracle AVDF OCI Marketplace image has a password expiry setting. Check if the password for the *opc* user has expired. The following message is displayed when attempting to connect through SSH from another Linux VM to the Audit Vault Server instance:

```
ssh -i av_key opc@<IP address>
Audit Vault Server 20.x.0.0.0

DO NOT CHANGE ANY CONFIGURATIONS IN Audit Vault Server APPLIANCE WITHOUT
GUIDANCE FROM ORACLE SUPPORT.
ANY CHANGES SHOULD BE TRACEABLE TO APPROPRIATE SR REFERENCE.
Your account has expired; please contact your system administrator.
Authentication failed.
```

Follow these steps to resolve the issue on the:

- Audit Vault Server
- Audit Vault Server Console 20.11
- Audit Vault Server Console 20.12

Audit Vault Server

1. Boot in single user mode.
2. Remove the password aging for the *opc* user.
3. Log in as usual by connecting to the local Audit Vault Server through VNC.
4. Reboot the Audit Vault Server appliance after connecting successfully.
5. When the boot screen appears, press `e` to edit the command line.
6. Add the following at the end of line starting `linux16`:

   ```
   init=/bin/bash
   ```

7. Press `Ctrl+x` to boot the appliance.
8. Remount the filesystem by running the following command:

   ```
   mount -o rw,remount /
   ```

9. Set the *opc* user to never expire:

   ```
   change -m 0 -M -1 -I -1 -E -1 opc
   ```

10. Reboot the appliance.
11. Log in as usual through SSH.

Audit Vault Server Console 20.11

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `oracle` user.

   ```
   su - oracle
   ```
3. Start SQL*Plus as `sysdba`.

   ```
   sqlplus / as sysdba
   ```
4. Run the following command:

   ```
   alter package APEX_230100.WWV_FLOW_DYNAMIC_EXEC compile body;
   ```

Audit Vault Server Console 20.12

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Switch to the `oracle` user.

   ```
   su - oracle
   ```
3. Start SQL*Plus as `sysdba`.

   ```
   sqlplus / as sysdba
   ```
4. Run the following command:

   ```
   alter package APEX_230200.WWV_FLOW_DYNAMIC_EXEC compile body;
   ```

Related Topics

- My Oracle Support Doc ID 2693466.1
- My Oracle Support Doc ID 2284110.1

L.77 Audit Vault Agent Fails with the ORA-01745 Error

Learn how to resolve the `ORA-01745` error for Audit Vault Agent.

Problem

Audit Vault Agent fails with the `ORA-01745` error.

Solution

Modify the firewall rules to ensure that communication between Audit Vault Agent and Audit Vault Server is allowed.

L.78 Oracle Directory or Table Audit Trail Stops with Error PLS-00201

Learn how to resolve error `PLS-00201` in the collector logs.

Problem

The Oracle directory or table audit trail stops and the collector logs display the following error:

```
PLS-00201: identifier 'SYS.DBMS_AUDIT_MGMT' must be declared
```

Solution

Grant permissions to the target user and start the trail again. See Oracle Database Setup Scripts.

L.79 Error with Potential Insecure Path

Learn how to solve error `java.lang.IllegalArgumentException:Potential insecure path found : <path>`.

Problem: Audit Vault agent fails with error `java.lang.IllegalArgumentException: Potential insecure path found : <path>`.

Solution:

- Ensure directories in path do not have write permission for other users.
- Ensure path does not have more than 5 levels of symbolic links.

L.80 Error "ORA-28000 the Account Is Locked" After Changing the Admin User Password

Learn what to do when you receive the `ORA-28000` error when changing the admin user password.

Problem

The following error message appears after you change the admin user password:

```
ORA-28000 the account is locked
```

Solution

You might receive this error when the Oracle Enterprise Manager Agent is monitoring Audit Vault Server. Changing the admin password on the Audit Vault Server Console does not automatically update the password that Enterprise Manager Agent uses to connect to Audit Vault Server. Ensure that the Enterprise Manager Agent is connecting with the correct password.

L.81 Error OAV-47112 When Trying to Delete an Existing Archive Location

Learn what to do when you receive the `OAV-47112` error when trying to delete an existing archive location.

Problem

The `OAV-47112` error appears when you try to delete an existing archive location.

Solution

You might receive this error when you try to delete an archive location that is currently in use to store archive tablespaces or data files. Wait until the tablespace or data file archive period expires before deleting the archive location. If needed, you can create a new archive location to use for the tablespace or data file archiving and then retrieve the tablespaces from the previous location and archive them to the new location.

L.82 Transaction Log Audit Trail Stops Due to XML Parsing Error

Learn how to fix issue when Transaction Log Audit Trail goes to stopped state due to XML parsing error.

Problem: Transaction Log Audit Trail stops due to XML parsing error. This is because of invalid XML record generated by Oracle GoldenGate.

Solution: Contact Oracle Support to create a Merge Label Request for applying the patch 32175609, 32063871, 33701099, and 34014874. This patch needs to be applied on Oracle GoldenGate installation.

L.83 "-bash: permission denied" Error When Trying to Run Custom Backup Script from /home/oracle

Scripts in /home/oracle cause permission errors when trying to run the scripts.

Problem: "-bash: permission denied" error when trying to run script from /home/oracle. The reason is executing script under /home/oracle is not allowed.

Solution: Move scripts to a different location.

L.84 Issues Deleting Target Database With Audit Trail Still Running

Secured target could not be deleted as the audit trail had not officially been stopped via the console or command line.

Problem: Unable to delete a target while it's trails are running. This is a safety function to prevent removal of active audit trails by accident.

Solution: Stop all the trails on that target through GUI, or AVCLI before dropping the target.

L.85 Deleting Audit Records Requires Applying Retention Period to Purge Records

Learn how to apply retention periods to audit data so that it can be purged.

Problem: No mechanism to delete audit data.

Solution: Apply small retention period to audit data to be deleted so that it is purged with time. See Configuring Archive Locations and Retention Policies for retention periods.

L.86 Unable to Mount NFS on New AVDF 20.3 Server

Learn how to fix inability to Mount NFS on s System running with Oracle AVDF.

Problem: AVDF Client is unable to mount due to bug or parameter settings on NAS Storage and/or NFS Server.

Symptoms:

- Oracle Linux running with Oracle AVDF (Audit Vault and Database Firewall).
- NFS Archive mount point cannot be mounted on a Oracle Linux system with AVDF.
- Further details are found in the following command:

```
[root@nfs-client01 ~]# mount -t nfs nfs-server01:/avdf_archive_vol01/
avdf_archive_backup
mount.nfs: rpc.statd is not running but is required for remote locking.
mount.nfs: Either use '-o nolock' to keep locks local, or start statd.
mount.nfs: an incorrect mount option was specified
[root@nfs-client01 ~]# service nfslock status
rpc.statd (pid 25042) is running...
```

> **Note:**
>
> `nfs-client01` is the Oracle AVDF system. Oracle AVDF has no mechanism to collect the sosreport.

Solution:

1. Engage Vendor NAS Storage Support or NFS Admin Support Team to verify if the mount point at the NFS Server side is properly set-up. See the output of the command below.

```
[root@nfs-client01 ~]# showmount -e nfs-server01
/avdf_archive_vol01 nfs-client01 <== This is the limited NFS configuration
of the NFS Server, which can be seen from AVDF NFS Client.
[root@nfs-server01 ~]# cat/etc/exports
/avdf_archive_vol01 nfs-client01(rw,no_subtree_check,no_root_squash)
```

2. Test whether the NFS mount point can be mounted properly on NFS client, please use the command below.

```
[root@nfs-client01 ~]# mount -vvvv -t nfs -o nolock nfs-server01:/
avdf_archive_vol01/avdf_archive_backup
mount.nfs: timeout set for Mon Oct 29 14:05:37 2018
mount.nfs: trying text-based options 'nolock,vers=4.1,addr=<IP
ADDR>,clientaddr=<IP ADDR>'
[root@nfs-client01 ~]# df -hP
Filesystem Size Used Avail Use% Mounted on
devtmpfs 412M 0 412M 0% /dev
tmpfs 432M 0 432M 0% /dev/shm
tmpfs 432M 6.0M 426M 2% /run
tmpfs 432M 0 432M 0% /sys/fs/cgroup
/dev/mapper/ol-root 9.8G 7.3G 2.5G 75% /
/dev/sdb1 16G 11G 5.7G 65% /yum
/dev/sda1 1014M 171M 844M 17% /boot
tmpfs 87M 0 87M 0% /run/user/0
nfs-server01:/avdf_archive_vol01 11G 2.2G 7.4G 23% /avdf_archive_backup
<== This the sample AVDF NFS mount point. The one in use might be
different.
```

> **Note:**
>
> `vvvv` – this is the debugging mode in NFS to test which layer of NFS is failing.
> `-o nolock` – to test if the NFS mount can mount using `nolock`.
>
> If the above command is able to mount the ADVF NFS mount point, hence, there is no issue on the NFS at the Linux OS level.

For more information refer to My Oracle Support Doc ID 2466520.1.

L.87 Alert Email Notifications Are Not Received from Oracle AVDF Server

Learn what checks need to be performed when the email alerts are not received from the AVDF server.

Problem: Alert email notifications are not received from Oracle AVDF Server.

Solution:

1. Login with super administrator user in AVCLI and check SMTP server settings.

```
AVCLI> connect avadmin;
Connected.
AVCLI> LIST ATTRIBUTE OF SMTP SERVER;
------------------------------------------------------------------------
----------------------------
| HOST | PORT | SENDER_ID | SENDER_EMAIL | SECURE | TRUSTSTORE | STATE |
========================================================================
============================
| <mail server host> | 25 | user1 | user1@<mail server host> | UNSECURED |
```

```
| ENABLED |
-------------------------------------------------------------------------
----------------------------
1 row(s) selected.
The command completed successfully.
```

2. From AVCLI interface send an email to test if the connection with the SMTP server works:

```
AVCLI> TEST SMTP SERVER SEND EMAIL TO user2@<mail server host>;
Request submitted successfully.
```

3. There are multiple reasons why the connection to the SMTP server might not work including:
   - The SMTP server is configured using DNS name and it cannot be resolved by AVDF server
   - AVDF server cannot communicate with the mail server
   - There are invalid objects in the database
   - Java processes are stuck
   - There are scheduled jobs by auditor user to retrieve audit settings or user entitlements

   View other problem causes and their solutions at My Oracle Support Doc ID 2232033.1

L.88 Audit Vault Agent is Stuck in Starting State: Error OAV-46573

Problem:

Audit Vault agent installed as a service on Windows is stuck in starting state after restarting the agent host.

```
Error OAV-46573: Agent is UNREACHABLE on host "hostname". Please try after some
time. Audit trail is not eligible for auto start.
```

Solution:

Set `JAVA_HOME`. Audit Vault agent needs to find Java Runtime Environment.

L.89 SSH Becomes Disabled After Enabling FIPS Mode

If SSH becomes disabled after enabling FIPS mode, update the SSH keys to be compliant with FIPS.

Problem

In Oracle AVDF 20.9, SSH becomes disabled after enabling FIPS mode.

Solution

Before enabling FIPS 140-2, ensure that your SSH keys are compliant with FIPS. If your SSH keys are not compliant with FIPS, the SSH connection with the appliance might be lost after enabling FIPS.

For Oracle AVDF on Oracle Cloud Infrastructure (OCI), before enabling FIPS mode, ensure that the `opc` user has FIPS-compliant keys registered to `/home/opc/.ssh/authorized_keys`.

Follow these steps to resolve this issue:

1. Log into the Audit Vault Server console and disable FIPS mode.
2. Log back into the appliance through SSH and check or update the user keys for SSH-enabled users in `~/.ssh/authorized_keys` to be compliant with FIPS.

   It can take several minutes for the console to become available after enabling or disabling FIPS mode.
3. Enable FIPS mode.

Related Topics

- Enabling FIPS 140-2 on the Audit Vault Server
  Enable FIPS on the Audit Vault Server to turn on FIPS mode in the embedded Oracle Linux operating system and Oracle Database.

L.90 Audit Vault Agent Is Not Reachable from the Audit Vault Server Console

Problem

The Audit Vault Server console reports an agent as "not reachable." When trying to start the agent, a message similar to the following appears:

```
C:\AUDIT_VAULT_AGENT_3\bin>agentctl.bat start An instance of the agent is
already running.
[2015-08-26T10:51:25.345+03:00] [agent] [ERROR] [] [] [tid: 10] [ecid:
172.xx.1.xxx:69595:1440575485345:0,0] OAV-10: Failed to release connection to
DB[[
Failed to release connection to DB at
oracle.av.platform.common.dao.ConnectionManagerImpl.destroy(ConnectionManagerI

mpl.java:578) at
oracle.av.platform.agent.AgentController.doStop(AgentController.java:1966)
at
oracle.av.platform.agent.AgentController.doProcess(AgentController.java:2037)
at oracle.av.platform.agent.AgentController.main(AgentController.java:2046)
Nested Exception: oracle.ucp.UniversalConnectionPoolException: The Universal
Connection Pool cannot be null at
oracle.ucp.util.UCPErrorHandler.newUniversalConnectionPoolException(UCPErrorHa
ndler.java:368) at
oracle.ucp.util.UCPErrorHandler.newUniversalConnectionPoolException(UCPErrorHa
ndler.java:336) at
oracle.ucp.util.UCPErrorHandler.newUniversalConnectionPoolException(UCPErrorHa
ndler.java:350) at
oracle.ucp.admin.UniversalConnectionPoolManagerBase.destroyConnectionPool
UniversalConnectionPoolManagerBase.java:469) at
oracle.av.platform.common.dao.ConnectionManagerImpl.destroy(ConnectionManagerI
mpl.java:574)
at oracle.av.platform.agent.AgentController.doStop(AgentController.java:1966)
```

```
at
oracle.av.platform.agent.AgentController.doProcess(AgentController.java:2037)
at oracle.av.platform.agent.AgentController.main(AgentController.java:2046)
```

Cause

The lock file is still present. This is a protection mechanism to prevent starting multiple agents from the same host.

Solution

1. Make sure that the `java.exe` processes for the agent are terminated. Use Task Manager to terminate them, if necessary.
2. Remove the `<agent home>\av\conf\agent.lck` file. For example:

   ```
   del C:\AUDIT_VAULT_AGENT_3\av\conf\agent.lck
   ```

3. Start the agent normally. For example:

   ```
   C:\AUDIT_VAULT_AGENT_3\bin> agentctl.bat start
   ```

L.91 Proxy Error When Opening AVDF Console in Web Browser

Problem

While opening the AVDF console in a web browser, the following error is shown:

```
Proxy Error
The proxy server received an invalid response from an upstream server.
The proxy server could not handle the request GET /console/f.
```

Solution

To fix the proxy error:

1. Check if the database and the Automatic Storage Management (ASM) instance is running or not. If not, then reboot the Audit Vault Server once and then check again.
2. If Java framework is not running, then start it by running the following command: `/usr/local/dbfw/bin/javafwk start`

L.92 Prevent a Terminal Login Session from Expiring When Connecting to an Audit Vault Server or a Database Firewall Server

Problem

When performing an Audit Vault Server or Database Firewall Server backup or upgrade, sometimes the connection to the server through the terminal timeouts.

Solution
To prevent a terminal login session from expiring when connecting to an Audit Vault Server or a Database Firewall Server.

1. Connect to the AV Server as root using a terminal session (like putty).
2. Run the following command: `cd /etc/ssh`
3. Run the following command: `vi sshd_config`
4. Run the following command: `/ClientAliveCountMax`
5. Set the value from 0 to 1000
6. Save the file by running the following command: `:wq!`
7. Run the following command at the OS prompt: `service sshd restart`
8. Run the following command: `cd /usr/local/dbfw/templates`
9. Run the following command: `vi template-ssh-sshd-conf`
10. Run the following command: `/ClientAliveCountMax`
11. Set the value from 0 to 1000
12. Save the file by running the following command: `:wq!`
13. Exit out of the terminal session.
14. Connect to the Audit Vault server or Database Firewall server again.

L.93 Microsoft SQL Server Database Audit Trails Are Unreachable

Problem

When you start an audit trail, it fails with the following message:

```
OAV-46573: Agent is UNREACHABLE on host "****.XXX.com". Please try after some
time. Audit trail is now eligible for auto start.
```

This may occur for EVENT LOG and DIRECTORY audit trails for Microsoft SQL Server on Microsoft Windows Server 2012.

Cause

The Audit Vault Agent was stopped. To verify this, use the `agentctl status` command. For example:

```
PS C:\Agent_Home\bin> ./agentctl status
Agent is stopped.
```

Solution

Start the Audit Vault Agent by using the `agentctl start` command. For example:

```
PS C:\Agent_Home\bin> ./agentctl start
Agent started successfully.
```

The audit trails are configured for automatic startup. After you start the Audit Vault Agent, the audit trails should start automatically. Check the status to verify that the audit trails are started and collecting audit data.

> **Note:**
>
> You can also configure the Audit Vault Agent to restart automatically. See Configuring Agent Auto Restart Functionality.

L.94 Database Firewall Error ODF-10507: TCP Session Re-use

Problem

The Database Firewall reports an error similar to the following in `/var/log/messages`:

```
Dec 23 08:41:20 dp-svif-odb-n001 dbfw2.0:
com.oracle.dbfw.dbfw_server WARN - ODF-10507: TCP session re-use:
Session reuse observed for session 10.8.130.107:35699-10.2.129.152:8521
Connection observed 61 seconds since last access
```

Cause

A closed TCP session to the database has been reopened. This could lead to the state from the previous session being applied to the new session.

Solution

No action is required.

L.95 Automate Archivelog Deletion in the Audit Vault Server Repository By Using the `oracle` User

Problem

You can't automate archivelog deletion in the Audit Vault Server repository because crontab is not enabled for the `oracle` user.

Cause

Crontab is disabled by default for the `oracle` user in Oracle AVDF.

Workaround

Use the `root` user to log in as the `oracle` user and issue the required command. For example: `su -l oracle -c bash`.

To enable the `oracle` user's crontab, as the `root` user, update `/etc/cron.allow` and change the command to ensure that the `oracle` user password has not expired. This results in configuration errors for using crontab.)

L.96 OAV-46511: Missing Plug-in for Trail at Agent on Host

Problem

Adding an audit trail fails after unregistering and re-registering a host. The following error appears:

```
OAV-46511: missing plugin for trail at agent on host "<hostname>"
```

Solution

1. Stop the Audit Vault Agent.
2. Make sure that no processes are running from the Audit Vault Agent home.
3. Log into the Audit Vault Server console and stop any audit trails that are using this Audit Vault Agent. These should already have been be stopped when the agent was stopped, but check again.
4. In the Audit Vault Server console, click the **Agents** tab.
5. Select the host name that appears in the error.
6. Click **Deactivate**.
7. Select the same host name, and click **Activate**.

   A new key is created.
8. Click **Downloads** in the left navigation menu.
9. Download the `agent.jar` file to the target host.
10. Create a new home (or remove all files from the old Audit Vault Agent home).
11. Redeploy the Audit Vault Agent.

    ```
    java -jar agent.jar -d <AGENT_HOME>
    ```
12. Start the Audit Vault Agent.

    ```
    cd <AGENT_HOME>/bin ./agentctl start -k
    ```

Related Topics

- Registering Hosts and Deploying the Agent
  If you're deploying the Audit Vault Agent, you register the host computers for the targets for which you want to collect audit data and deploy the Audit Vault Agent on each of them.

L.97 Initiate Pairing for High Availability Fails with OAV-46599: Internal Error

Problem

When setting up high availability, the Initiate Pairing command fails with the following error:

```
OAV-46599: internal error Error: Failed to execute HTTPS request on the
remote Audit Vault Server.
```

The messages log shows errors similar to the following:

```
Jun 4 16:07:10 avs00001702d420 setup_ha.rb[5272]:
com.oracle.avs.high_availability ERROR - ODF-10001: Internal error: Error:
Failed to execute HTTPS request on the remote Audit Vault Server.
Jun 4 16:18:04 avs00001702d420 setup_ha.rb[9959]:
com.oracle.avs.high_availability ERROR - ODF-10001: Internal error: Error:
Failed to execute HTTPS request on the remote Audit Vault Server.
```

Cause

The ports that are required for network connectivity between the primary and secondary Audit Vault servers in high availability mode are not open in the firewall.

Solution

Open port 7443 in the firewall.

Related Topics

- Ports for Services Provided by Audit Vault Server
  Learn about the ports for services that are provided by Audit Vault Server.

L.98 Archive Error OAV-46599 and Internal Error ORA-14400: Partition Key Not Mapped

Problem

When archiving the data, the following errors appear:

```
OAV-46599: Internal error ORA-14400: partition key not mapped to any partition
```

Cause

The `EVENTDATA` disk group doesn't have enough space.

Solution

1. Check the current status of the existing Oracle Automatic Storage Management (Oracle ASM) disks and disk groups.

```
set pagesize 1000
set linesize 1000
COLUMN NAME format A25
COLUMN MOUNT_STATUS format A10
COLUMN HEADER_STATUS format A20
COLUMN MODE_STATUS format A20
COLUMN STATE format A20
COLUMN PATH format A40
COLUMN LABEL format A20
SELECT GROUP_NUMBER,NAME,TOTAL_MB,FREE_MB FROM V$ASM_DISKGROUP;
SELECT
MOUNT_STATUS,HEADER_STATUS,MODE_STATUS,STATE,TOTAL_MB,FREE_MB,NAME,PATH,LAB
EL FROM V$ASM_DISK;
```

2. Add space to the EVENTDATA disk group.

```
ALTER DISKGROUP EVENTDATA add disk 'path';
```

L.99 SYSLOG Forwarding for Alerts Isn't Working

Problem

`SYSLOG` forwarding for alerts isn't working.

Cause

This may happen if the `SYSLOG` forwarding queue has many alerts without the old events backlog.

Solution

1. Bounce the database.
2. Purge the `av_alert queue` table as the `AVSYS` user.

```
DECLARE
po_t dbms_aqadm.aq$_purge_options_t;
BEGINdbms_aqadm.purge_queue_table('AVSYS.AV_ALERT_QT', NULL, po_t);
end;
/
```

L.100 `SYSLOG` Forwarding to SIEM Isn't Working

Problem

`SYSLOG` forwarding to SIEM isn't working.

Cause

`rsyslog.conf` file has incorrect configuration entries.

The `rsyslog.conf` says to forward alerts, while also stating to filter out alerts. Because of this, the alert will never get written to local `/var/log/messages` and can't be forwarded to SIEM.

```
#FORWARDED SYSLOG CATEGORIES:system, alerts, debug, info
*.info;local0.none;local1.none;local2.none;user.crit;user.warn;*.=debug;local1
.info @<SIEM
      server IP address>


# This filters out AVDF alerts, which are either user.crit, or user.warn
user.crit;user.warn ~
```

Solution

1. Modify `/etc/rsyslog.conf` to not filter out alerts. Change `user.crit;user.warn ~` to:

   ```
   user.crit;user.warn /var/log/AVDF_alerts
   ```

   > **Note:**
   >
   > This change to `/etc/rsyslog.conf` will revert after a server reboot.

2. As `root` services rsyslog restart.
3. If there are no alerts being forwarded but the following "logger" command works, then either no alerts are generated or `SYSLOG` forwarding is not setup fully in WebConsole.

   ```
   #Force it something log to rsyslog to process to send to remote @IP (and
   write to the AVDF_alerts file)
   logger -p user.crit AVDF Alert dummy test
   #You should see this dummy test being logged in the /var/log/dbalerts file
   ```

   For more information see, Configuring Audit Vault Server Syslog Destinations.

To monitor what is being sent by `rsyslog` off AVDF server via `rsyslog`, run one of the following commands on port 514:

```
tcpdump -nn -i <eth#> | grep <IP of SIEM>
tcpdump -i eth0 tcp port 514


tcpdump -i lo -A udp and port 514


tcpdump -A dst
tcpdump -nnvvXS dst
```

L.101 Oracle AVDF Reports For Oracle Database Shows UNKNOWN For Session Info If Native Network Encryption Is Enabled On the Database

Problem

If Native Network Encryption is enabled on an Oracle Database the Oracle AVDF reports show `UNKNOWN` for session info. Examples include `unknown_username` and `unknown_client`.

Solution

See Monitor Native Network Encrypted Traffic Through Database Firewall for Oracle Databases for how to resolve this issue.

L.102 Error: Kernel Out of Memory

Problem

The following error appears:

```
kernel: Out of memory: Kill process nnnnn (oracle) score nnn or sacrifice
child
```

The following output is a partial example:

```
<kern.warning> xxxxav01aud kernel: java invoked
      oom-killer: gfp_mask=0x201da, order=0, oom_adj=0,
oom_score_adj=0<kern.info> xxxxav01aud
      kernel: java cpuset=/ mems_allowed=0-1<kern.warning> xxxxav01aud
kernel: Pid: 19085, comm:
      java Not tainted 2.6.39-400.250.6.el5uek #1<kern.warning> xxxxav01aud
kernel: Call
      Trace:<kern.warning> xxxxav01aud kernel: [<ffffffff81113e04>]
      dump_header+0x94/0xe0<kern.warning> xxxxav01aud kernel:
[<ffffffff81113f4d>]
```

After this error occurs once, similar errors are logged intermittently and the audit trail may be stopped or a repository database may be terminated suddenly.

Cause

When this error occurs, the memory usage of `oraagent.bin` becomes very high. When this type of memory usage occurs, the Linux: Out-of-Memory (OOM) Killer may stop some processes. See Doc ID 452000.1 in My Oracle Support for more information about this process.

The root cause of the `oraagent.bin` high memory usage is related to an Oracle Database issue where the dependent listener is removed or renamed. See Doc ID 1640721.1 for more information about this issue.

Solution

Stop the `oraagent.bin` process periodically.

L.103 Increasing the Logical Volume Capacity for a File System

If an Oracle AVDF file system runs out of space, you can allocate more space to the logical volume that holds the file system.

Use the `lvextend` command to increase the logical volume capacity. The `vg_root` volume group normally has unallocated space for this purpose.

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.

2. Run `vgs` to check the volume group free space. For example:

   ```
   /usr/sbin/vgs
   VG      #PV #LV #SN   Attr   VSize  VFree
   vg_root   1  13   0 wz--n- 149.84G 10.72G
   ```

   For more detailed volume group information, run `vgdisplay`.

3. Increase the logical volume capacity.

   For example, the following command adds 2 GB to the `/tmp` folder from the `VG_ROOT` volume group:

   ```
   /usr/sbin/lvextend -r -L+2G /dev/mapper/vg_root-lv_tmp
   ```

Related Topics

- Configure Logical Volumes on Oracle Linux

L.104 Banner Is Incorrect When Logging In as the Support User

Problem

In Oracle AVDF 20.1, when you log in through SSH as the `support` user, the banner is incorrect. For example:

```
login as: support
\S
Kernel \r on an \ms
upport@'s Password:

support@ -] $
```

Solution

> **Note:**
>
> This issue was fixed in Oracle AVDF 20.2.

To resolve the issue, request a backport or apply the latest bundle patch. See bug 31715004 - BANNER WHILE LOGIN AS SUPPORT USER IS NOT CORRECT.

L.105 Can't Install Host Monitor with Error: Failed to Generate Executables for Host Monitor

Problem

When installing the Host Monitor Agent, you receive one of the following errors:

```
[root@hm]# ./hostmonsetup install
/usr/bin/ld: cannot find -lssl
collect2: ld returned 1 exit status
make: *** [hostmonitor] Error 1
Line 751: Failed to generate executables for Host monitor.
```

```
[root@hm]# ./hostmonsetup install
/usr/bin/ld: cannot find -lpcap
collect2: ld returned 1 exit status
make: *** [hostmonitor] Error 1
Line 751: Failed to generate executables for Host monitor.
```

```
[root@hm]# ./hostmonsetup install
/usr/bin/ld: cannot find -lcap
collect2: ld returned 1 exit status
make: *** [hostmonitor] Error 1
Line 751: Failed to generate executables for Host monitor.
```

The `libcap`, `libpcap`, and `openssl` packages are already installed. For example:

```
rpm -qa|grep cap
```

The output lists the following:

```
libcap-2.16-5.5.el6.x86_64
compat-libcap1-1.10-1.x86_64
libcap-ng-0.6.4-3.el6_0.1.x86_64
libpcap-1.0.0-6.20091201git117cb5.el6.x86_64
perl-Pod-Escapes-1.04-119.el6_1.1.x86_64
```

Cause

The `libcap`, `libpcap`, and `openssl` package should be installed.

Also, the `-devel` packages for `libcap`, `libpcap`, and `openssl` packages must be installed.

Solution

Run the following commands to verify whether the packages are installed:

```
rpm -q libcap
```

```
rpm -q libcap-devel
```

```
rpm -q libpcap
```

```
rpm -q libpcap-devel
```

```
rpm -q openssl
```

```
rpm -q openssl-devel
```

The output of each command should display the location where the library is installed. If any package is not installed, you should see a prompt stating that the package is not installed.

If a package isn't installed, then install it by using the following command:

```
yum -y install <package_name>
```

To install the `-devel` packages, use the following commands:

```
yum -y install libpcap libpcap-devel
```

```
yum -y install libcap libcap-devel
```

```
yum -y install openssl openssl-devel
```

L.106 OAV-47704 Error When Dropping a Firewall

Problem

In Oracle AVDF 20.5, when you try to drop (remove) a firewall, you receive ERROR OAV-47704. For example:

```
ERROR: OAV-47704: Database Firewall avdf001 is not on the latest version.
Upgrade to the latest.
```

Cause

Oracle AVDF is not allowing you to configure or remove a older-versioned Database Firewall.

Solution

> **Note:**
>
> This issue was fixed in Oracle AVDF 20.6.

In Oracle AVDF 20.5, try the following workaround:

1. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

2. Start SQL*Plus as the `avsys` user.

   ```
   sqlplus avsys
   ```

3. Enter the password at the prompt.
4. Update the firewall version to `20.5.0.0.0`.
   a. Get the firewall ID.

      ```
      select id from avsys.firewall where name= '<firewall_name>' and
      deleted_at is null;
      ```

   b. Update the version for the firewall ID.

      ```
      update avsys.firewall set software_version='20.5.0.0.0' where
      id=<firewall_id>;
      ```

c. Commit the change.

```
commit;
```

d. Repeat steps a-c for any other firewalls that you want to remove.

5. Exit SQL*Plus.

```
exit
```

6. Try to remove the firewall by using the Audit Vault Server console or AVCLI.
7. If the preceding steps do not resolve the error, try the following additional steps:
   a. Start SQL*Plus as the `avsys` user.

```
sqlplus avsys
```

   b. Enter the password at the prompt.
   c. Get the firewall ID again, if needed.

```
select id from avsys.firewall where name= '<firewall_name>' and
deleted_at is null;
```

   d. Run the following command:

```
update avsys.enforcement_point set deleted_at = systimestamp where
firewall_group_id = (select firewall_group_id from avsys.firewall where
name='<firewall_name>' and deleted_at is null) and deleted_at is null;
```

   e. Run the following command:

```
update avsys.enforcement_point_instance set deleted_at = systimestamp
where firewall_id = (select id from avsys.firewall where
name='<firewall_name>' and deleted_at is null) and deleted_at is null;
```

   f. Commit the changes.

```
commit;
```

   g. Exit SQL*Plus.

```
exit
```

8. Try to remove the firewall by using the Audit Vault Server console or AVCLI.

Related Topics

- Removing Database Firewall from Audit Vault Server
  You can remove Database Firewall from Audit Vault Server.
- DROP FIREWALL
  Use the `DROP FIREWALL` command to drop a registered Oracle Database Firewall from Oracle Audit Vault Server.

L.107 Installing the Oracle Enterprise Manager Management Agent for Oracle AVDF Fails with an Unzip Not Found Error

Problem

In Oracle AVDF release 20, when you install the Oracle Enterprise Manager Management Agent on the Audit Vault Server or Database Firewall server, the installation may fail with an error saying "unzip not found."

Cause

The unzip RPM is not present on the Audit Vault Server or Database Firewall server.

Solution

1. Access https://yum.oracle.com/repo/OracleLinux/OL7/latest/x86_64/index.html from a machine that has internet access.
2. Download `unzip-6.0-21.el7.x86_64.rpm`.
3. Use SCP to transfer the RPM file to the Audit Vault Server or Database Firewall server.
4. Enter the following command to install unzip:

   ```
   rpm -i unzip-6.0-21.el7.x86_64.rpm
   ```

5. Instal the Enterprise Manager Management Agent again. See Installing the Enterprise Manager Management Agent.

L.108 Audit Trail Error: Unable to Connect to Target to Get Timezone Offset

Problem

In Oracle AVD 20.5 and later, audit collection stops with the following error:

```
OAV-8015: Error initializing AuditEventCollector instanceCollectionController :
run : AuditException from process()
```

In the Audit Vault Server console, when you start the audit trail, the state changes to "Stopped" with the following error:

```
Unable to connect to target to get Timezone Offset
```

Cause

The `AV.COLLECTOR.TIMEZONEOFFSET` audit collection attribute for the target is missing.

Solution

1. Run the following SQL query on the target database:

   ```
   select systimestamp from dual;
   ```

The output should look like the following example:

```
SYSTIMESTAMP
---------------------------------------------------------------------------
AV.COLLECTOR.TIMEZONEOFFSET +7:00
```

2. Log in to the Audit Vault Server console and an administrator.
3. Modify the target and add the `AV.COLLECTOR.TIMEZONEOFFSET` audit collection attribute that you identified in the preceding step.

   For instructions, see Modifying Targets.
4. Stop and start the audit trail.

   For instructions, see Stopping, Starting, and Autostart of Audit Trails in Oracle Audit Vault Server.

L.109 Issue with Phusion Passenger Configuration

Problem

In Oracle AVDF 20.1-20.4, you may see communication attempts from Oracle AVDF to an external URL related to Phusion Passenger.

Cause

Oracle AVDF uses third-party open source software called Phusion Passenger. This software may anonymously send usage statistics to an external URL if anonymous telemetry reporting is enabled. For more information about this, see Anonymous Telemetry Reporting on the Phusion Passenger website.

Solution

To disable Passenger anonymous telemetry reporting in Oracle AVDF 20.1-20.4:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Edit the `template-httpd-httpd.conf` platform template.

   ```
   vi /usr/local/dbfw/templates/template-httpd-httpd.conf
   ```
3. Locate the following `mod_passenger` configuration text block:

   ```
   <IfModule mod_passenger.c>
   ...
   </IfModule>
   ```
4. At the end of that text block, add `PassengerDisableAnonymousTelemetry on`.

   ```
   <IfModule mod_passenger.c>
   …
   PassengerDisableAnonymousTelemetry on
   </IfModule>
   ```
5. Save and close the file.

6. To apply the updated configuration and restart Apache, run the following command:

```
/usr/local/dbfw/bin/priv/configure-networking
```

L.110 Diagnostic Report: Checking for Unknown Keys in /usr/local/dbfw/etc/dbfw.conf

Problem

The diagnostic report has the following message:

```
Checking for unknown keys in /usr/local/dbfw/etc/dbfw.conf: ["duplex",
"speed"] - WARN
```

Cause

This warning may appear if the following entries are not configured in `/usr/local/dbfw/etc/dbfw.conf`:

```
speed=""
duplex=""
```

Solution

You can safely ignore this warning.

L.111 ODF-10001: Internal Error: Failure in Read from <IP Address>:<Port>: Connection Timed Out in Firewall Server

Problem

In Oracle AVDF 20.1-20.5, the following error may appear multiple times in `/var/log/messages` on the Database Firewall server:

```
<hostname> fw7: com.oracle.dbfw.fw ERROR - ODF-10001: Internal error: Failure
in  Read from <IP ADDRESS>:<PORT>: Connection timed out
```

Cause

This message may appear if a if TCP connection has been closed due to the TCP keep-alive mechanism detecting a terminated peer.

Solution

In Oracle AVDF 20.1-20.5, treat this message as a warning, rather than an error. It will not cause a loss of functionality.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

L.112 Database Firewall Server /var/log Partition Is Full

Problem

The Database Firewall server `/var/log` partition is full. This issue may occur in Oracle AVDF 20.3 and earlier.

Solution

The issue does not happen in Oracle AVDF 20.4 and later.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

As a workaround until you can patch Oracle AVDF, you can also restart `rsyslog`. For example:

```
systemctl restart rsyslog
```

L.113 The `tuned.service` Status Is Failed in the Database Firewall Health Check

Problem

In Oracle AVDF 20.3 and earlier, the Oracle Linux `tuned-service` process may appear with a `Failed` status in the Database Firewall health check job details.

```
# systemctl status
tuned.service - Dynamic System Tuning Daemon
Loaded: loaded (/usr/lib/systemd/system/tuned.service; enabled; vendor
preset: enabled)
Active: failed (Result: exit-code) since Fri 2021-02-05 06:21:12 UTC; 2min
27s ago
  Docs: man:tuned(8)
      man:tuned.conf(5)
      man:tuned-adm(8)
Process: 16912 ExecStart=/usr/sbin/tuned -l -P (code=exited, status=1/FAILURE)
Main PID: 16912 (code=exited, status=1/FAILURE)
Feb 05 06:21:12 dbfw0000abc00000 tuned[16912]: from tuned import storage,
units, monitors, plugins, profiles, exports, hardware
Feb 05 06:21:12 dbfw0000abc00000 tuned[16912]: File "/usr/lib/python2.7/site-
packages/tuned/exports/__init__.py", line 3, in <module>
Feb 05 06:21:12 dbfw0000abc00000 tuned[16912]: from . import dbus_exporter as
dbus
Feb 05 06:21:12 dbfw0000abc00000 tuned[16912]: File "/usr/lib/python2.7/site-
packages/tuned/exports/dbus_exporter.py", line 3, in <module>
Feb 05 06:21:12 dbfw0000abc00000 tuned[16912]: import dbus.service
Feb 05 06:21:12 dbfw0000abc00000 tuned[16912]: ImportError: No module named
dbus.service
Feb 05 06:21:12 dbfw0000abc00000 systemd[1]: tuned.service: main process
exited, code=exited, status=1/FAILURE
Feb 05 06:21:12 dbfw0000abc00000 systemd[1]: Failed to start Dynamic System
```

```
Tuning Daemon.
Feb 05 06:21:12 dbfw0000abc00000 systemd[1]: Unit tuned.service entered
failed state.
Feb 05 06:21:12 dbfw0000abc00000 systemd[1]: tuned.service failed.
```

You can use the following commands to get more details about this error:

- `systemctl status tuned.service`
- `journalctl -xe`

Cause

The following RPM is missing on the Database Firewall server:

`dbus-python-1.1.1-9.el7.x86_64.rpm`

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

As a workaround until you can patch Oracle AVDF, you can use the following steps:

1. As the `root` user, install `dbus-python-1.1.1-9.el7.x86_64.rpm`.

   Get the RPM from the following public yum (other locations may not be supported):

   ```
   http://public-yum.oracle.com/repo/OracleLinux/OL7/latest/x86_64/getPackage/
   dbus-python-1.1.1-9.el7.x86_64.rpm
   ```

   Use the following command:

   ```
   yum install dbus-python-1.1.1-9.el7.x86_64.rpm

   Plugin "ulninfo" can't be imported
   Installed:  dbus-python.x86_64  0:1.1.1-9.el7
   Complete!
   ```

2. 2) Restart `tuned.service` and then check the status.

   ```
   systemctl restart tuned


   systemctl status tuned

   tuned.service - Dynamic
   System Tuning Daemon
      Loaded: loaded (/usr/lib/systemd/system/tuned.service; enabled; vendor
   preset: enabled)
      Active: active (running) since Tue 2021-03-09 08:22:10 UTC; 12s ago
      Docs: man:tuned(8)
            man:tuned.conf(5)
            man:tuned-adm(8)
   Main PID: 779 (tuned)
      CGroup: /system.slice/tuned.service
              └─779 /usr/bin/python2 -Es /usr/sbin/tuned -l -P
   ```

```
Mar 09 08:22:09 dbfw0000abc00000 systemd[1]: Starting Dynamic System
Tuning Daemon...
Mar 09 08:22:10 dbfw0000abc00000 systemd[1]: Started Dynamic System Tuning
Daemon...
```

3. Check the Database Firewall in the Audit Vault Server console and verify that `tuned.service` is running (green).

L.114 Agent IO Error: Network Adapter Can't Establish Connection

Problem

In Oracle AVDF 20.3 and later, the following error may occur after install when trying to start with this command: `./agentctl start -k`:

```
Internal Error. See log files for detail.
```

Within the `av.agent` log, the following error may appear:

```
[2021-07-29T16:25:36.956+07:00][agent] [ERROR] [] [] [tid: 1] [ecid:
1918831609:74227:1627550704887:0,0] Unable to connect to AV Server after 10
retries
[2021-07-29T16:25:36.959+07:00] [agent] [ERROR] [] [] [tid: 1] [ecid:
1918831609:74227:1627550704887:0,0] Error occurred in Agent.[[Failed to
connect to DB at
oracle.av.platform.common.dao.ConnectionManagerImpl.getConnection(ConnectionMa
nagerImpl.java:548) at
oracle.av.platform.agent.AgentController.doValidateKey(AgentController.java:30
40) at
oracle.av.platform.agent.AgentController.doProcess(AgentController.java:3595)
at oracle.av.platform.agent.AgentController.main(AgentController.java:3614)]]
```

Similarly, within the `av.common` log, the following error may appear:

```
[2021-07-29T16:25:04.879+07:00][common] [ERROR] [] [] [tid: 1] [ecid:
1918831609:74227:1627550704887:0,0] [Thread]:main. Unable to get connection
to the datasource through certificate and without credentials. Unable to
start the Universal Connection Pool:
oracle.ucp.UniversalConnectionPoolException: Cannot get Connection from
Datasource: java.sql.SQLRecoverableException: IO Error: The Network Adapter
could not establish the connection
```

Cause

This error may occur if the external firewall is blocking network traffic from the secure target host to the audit vault server on port 1522.

Solution

To start correctly, you need to open the ports between Oracle AVDF and a secured target on 1521 and 1522. If there is a firewall in between the firewall ports, you must open it. After you open the ports, the error should no longer persist.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

L.115 Error ORA-01403 No Data Found When Adding a Database Firewall Instance to a Target

Problem

In Oracle AVDF 20.3 and later, when configuring Database Firewall monitoring points for a target, you can add the first Database Firewall instance as a monitoring point, but when you try to add the second instance, you may get the following error:

```
ora-01403 no data found
```

If you remove the first Database Firewall instance and try to add the second instance as a new monitoring point, you may get the following error:

```
OAV-46593: secured target address does not exist. cannot drop secured target
address.
```

Cause

This issue may happen when the `ha_role` for one of the Database Firewalls is set to `2` in the database. The `ha_role` needs to be set to `1`.

This could happen if the Database Firewall instances were previously configured as a resilient pair.

Solution

1. Connect to the Audit Vault Server database.
2. Run the following SQL query:

   ```
   select id, name, is_active, ha_role from avsys.firewall where deleted_at
   is null;
   ```

3. Find the row where `ha_role` is set to `2` and make a note of the Database Firewall ID.
4. Run the following query by replacing the *firewall_id* with the ID that you identified in the preceding step.

   ```
   update avsys.firewall set ha_role = 1, is_active = 1, ha_role_changed_at =
   current_timestamp where id in (<firewall_id>);
   ```

For example:

```
update avsys.firewall set ha_role = 1, is_active = 1, ha_role_changed_at =
current_timestamp where id in (2);
```

5. Run the following command:

```
commit;
```

6. Add the second Database Firewall instance for the target by using the Audit Vault Server console.

L.116 The Order of IP Addresses Changes After Setting Up DNS Servers

Problem

After setting up DNS servers, the order of the IP addresses may change.

For example, you might set up the DNS servers in the following order:

1. DNS server 1: xx.xxx.xx.14
2. DNS server 2: xx.xxx.xx.15
3. DNS server 3: xx.xxx.xx.16

After the configuration, the IP addresses might change to the following order:

1. DNS server 1: xx.xxx.xx.14
2. DNS server 2: xx.xxx.xx.16
3. DNS server 3: xx.xxx.xx.15

Cause

The order depends on the behavior of the package that's operating internally when registering the DNS servers.

Solution

No action is required. The IP addresses are not always registered in the order in which they are set.

L.117 NTP Is Unreachable on the Audit Vault Server

Problem

When configuring Network Time Protocol (NTP) on the Audit Vault Server, NTP is unreachable. It may be working fine on a Database Firewall server in the same network.

Cause

This may occur if the browser that you're using to access the Audit Vault Server console is set to a language other than English.

Solution

To resolve this issue, change the browser to English and refresh the Audit Vault Server console.

L.118 Database Firewall Status Is Running but the Status Is Down on the Audit Vault Server Console

Problem

The Audit Vault Server console shows that the Database Firewall is `Down` even though it's up and running.

Cause

This may be caused by an application timeout that's related to a bug that was fixed in Oracle AVDF 20.8.

Solution

To resolve this issue, complete the following steps on the Database Firewall sever:

1. Rename `/usr/local/dbfw/.bash_profile`. For example:

   ```
   mv /usr/local/dbfw/.bash_profile /usr/local/dbfw/.bash_profile_old
   ```

2. Restart Apache.

   ```
   systemctl restart httpd
   ```

   This should make it possible for Apache to spawn the web server APIs and for the system to start working again.

3. Check the status of the Database Firewall in the Audit Vault Server console. The status should be `Up`.

L.119 Network Audit Trail Is Not Collecting Audit Data When Using the Host Monitor Agent

Problem

When using the Host Monitor Agent to capture network traffic, the network audit trail isn't collecting audit data, even though the audit trail is running.

> **Note:**
>
> The following instructions apply only when using the Host Monitor Agent to capture network traffic. Ensure that there are no connection issues between the Host Monitor Agent and the Database Firewall before proceeding.

Solution

1. Log in to the target machine where the Host Monitor Agent is installed.
2. Restart the Audit Vault Agent in debug mode by running the following command:

```
<AVDF AGENT HOME>/bin>./agentctl stop
<AVDF AGENT HOME>/bin>./agentctl start -l debug
```

3. Log in to the Audit Vault Server console as an *administrator*.
4. Start the network audit trail and see if the network audit trail status changes to `Collecting`.
5. Run the following command on the machine where the Host Monitor Agent is installed and ensure that the `hostmonitor` process is running.

```
ps -ef | grep hostmonitor
```

6. Navigate to the folder that contains the `hostmonitor` logs (for example, `AGENT_HOME/hm/log`), and run the following command:

```
grep "Successfully sent data to Firewall machine" *
```

> **Note:**
>
> If "Successfully sent data to Firewall machine" appears in a log file, then the Host Monitor Agent is collecting and sending the network traffic to the Database Firewall successfully.

7. If the preceding text doesn't appear in the entry is not present in the `hostmonitor` log file, run the following command on the secured target machine to see which IP addresses and ports the target database is listening to.

```
lsnrctl status
```

8. Log in to to the Audit Vault Server console as an *administrator* and complete the following steps using the IP addresses and ports that you identified in the preceding step.
   a. Click the **Targets** tab.
   b. Select the target for which the network audit trail configured.
   c. Verify that all the IP addresses and ports that the target database is listening to appear in the **Connection Details** column in the **Database Firewall Monitoring** section.
   d. If an IP address or port doesn't appear, click the link under **Connection Details**.
   e. In the **Database Firewall Monitor** dialog box, click **Add** to add any missing IP addresses and ports.
   f. Click **Save** twice.
9. Run the following command on the target and verify the network interface card (NIC) to which all target database listening IP addresses belong.

```
ifconfig -a
```

10. Navigate to the folder that contains the `hostmonitor` logs (for example, `AGENT_HOME/hm/log`), and run the following command:

    ```
    grep "network_device_name_for_hostmonitor" *
    ```

    The output should be similar to the following example:

    ```
    The selected network device for capturing is: eth0. To change the device
    update the network_device_name_for_hostmonitor attribute at Collection
    Attributes to any one value from the list: eth0, nflog, nfqueue, any, lo
    and restart the trail.
    ```

    In the preceding example, the log shows that `hostmonitor` is listening on the `eth0` NIC.

    Verify that `hostmonitor` is listening on the same NIC to which the target database listening IP addresses belong.

11. If the target database listening IP addresses belong to a different NIC, perform the following steps:
    a. Log in to the Audit Vault Server console as an *administrator*.
    b. Click the **Targets** tab.
    c. Select the target for which the network audit trail is configured.
    d. Click **Modify**.
    e. Click the **Audit Collection Attributes** tab.
    f. Click **Add** and add the following attribute name and value pair:

       Name: `network_device_name_for_hostmonitor`

       Value: Enter the name of the NIC to which the target database listening IP addresses belong.

       Click **Save** twice.
12. Restart the network audit trail from the Audit Vault Server console.
13. Navigate to the folder that contains the `hostmonitor` logs (for example, `AGENT_HOME/hm/log`), and run the following command:

    ```
    grep "Successfully sent data to Firewall machine" *
    ```

    > **Note:**
    >
    > If "Successfully sent data to Firewall machine" appears in a log file, then the Host Monitor Agent is collecting and sending the network traffic to the Database Firewall successfully.

14. Log in to the target machine where the Host Monitor Agent is installed.
15. Restart the Audit Vault Agent in normal mode by running the following command:

    ```
    <AVDF AGENT HOME>/bin>./agentctl stop
    <AVDF AGENT HOME>/bin>./agentctl start
    ```

L.120 Internal Error When Deploying the Audit Vault Agent

Problem

Deploying the Audit Vault Agent fails with the following error:

```
Internal Error
Error occurred during install/upgrade. Check log files for more information.
```

The log file may contain entries similar to the following:

```
Unable to get connection to the datasource through certificate and without
credentials. Exception occurred while getting connection:
oracle.ucp.UniversalConnectionPoolException: Cannot get Connection from
Datasource: java.sql.SQLRecoverableException: IO Error: The Network Adapter
could not establish the connection
```

Cause

The Audit Vault Agent was trying to connect to an incorrect IP address.

Solution

Cross-check the IP address of the Audit Vault Server and the secured target server on which you're installing the Audit Vault Agent.

Related Topics

- Registering Hosts on the Audit Vault Server
  Learn about registering hosts on the Audit Vault Server.
- Deploying the Audit Vault Agent
  Learn about deploying the Audit Vault Agent.

L.121 Agent Host Is Not Registered

Problem

Deploying the Audit Vault Agent fails with the following message, even though the agent was already registered:

```
Agent host is not registered.
Agent host must be registered before an agent can be installed or upgraded.
Agent deployment failed.
```

Cause

This might happen on a multi-homed system when there are multiple routes from the Audit Vault Agent host to the Audit Vault Server. The SQLNet traffic might use an IP address that's different from the one that was used to register the Audit Vault Agent host.

When registering a host in the Audit Vault Server, you have two choices:

- Provide both a host name and an IP address: In this case, the name is treated as a handle with no significance and only the IP address is used.
- Provide only the host name: In this case, when you don't provide an IP address, the Audit Vault Server tries to resolve the host name to an IP address using DNS, if configured. If DNS is not configured, you receive an error. If the name resolves correctly, the IP address is remembered and used. The host name is ignored for normal operations.

This means that you must register the host with the same IP address that you see when using SQL*Plus to connect from the Audit Vault Agent host to the Audit Vault Server.

Solution

To verify the IP address with which the host should be registered, use SQL*Plus and connect using the connect string that's defined in the `<agent_home>/av/conf/bootstrap.prop` file. For convenience, you can also add it to the `tnsnames.ora` file with the designation `AV`.

Use the following steps to determine which IP address to register:

1. Determine which network interface card (NIC) is used for the Audit Vault Agent communication.
   a. Connect to the AV Server Database from the agent host using the following command.

      ```
      sqlplus <username>/<password>@"`cat <agent_home>/av/conf/bootstrap.prop
      | grep "SYS.CONNECT_STRING" | sed -e 's/SYS.CONNECT_STRING=//g' | sed -
      e 's/\\\//g'`"
      ```

      For *<username>*, enter a valid user name in the database, such as `avauditor`.

      For *<agent_home>*, enter the path to the agent directory.

   b. Run the following query:

      ```
      select SYS_CONTEXT('USERENV','IP_ADDRESS') FROM dual;
      ```

2. Use the IP address that was returned by the preceding query to register the Audit Vault Agent in the Audit Vault Server console. See Registering Hosts on the Audit Vault Server.

   Alternative, you can use the following AVCLI command:

   ```
   register host <hostname> with ip <ip address from the query>
   ```

On a multi-homed system, to register with another IP address, contact your network administrator and change the TCP routing configuration.

Related Topics

- Deploying the Audit Vault Agent
  Learn about deploying the Audit Vault Agent.

L.122 A Database Firewall Policy Is Not Blocking Statements Correctly

Problem

After creating a Database Firewall policy to block or substitute all queries from a specific database user, that user may still be able to run the SQL statements freely.

Cause

This could happen if the protected address that's associated with the secured target doesn't have an Oracle service name.

Solution

Make sure that all protected addresses contain an Oracle service name.

Related Topics

- Configuring Targets, Audit Trails, and Database Firewall Monitoring Points
  Learn about configuring targets, audit trails, and Database Firewall monitoring points.

L.123 Having Automatic Archiving Enabled Is Giving `OAV-47116` Error

Problem

`AUTOMATIC ARCHIVING ENABLE` is giving error `OAV-47116`.

Cause

Auto archive order should be greater than 0 (i.e 1 or more) to enable automatic archiving.

Solution

Change auto archive order to be greater than 0 from UI then try to enable automatic archiving.

L.124 Network Trail Fails To Be Started Due To Insufficient Permissions Error

Problem

The following errors are spotted in agent host monitor logs when the network trail is started:

```
startHostMonitor : exception while starting HostMonitor[[
Failed to start collector {0}:{1}
at
oracle.av.platform.agent.collfwk.impl.factory.HMCommandExecutor.execute(HMComm
andExecutor.java:380)
at
oracle.av.platform.agent.collfwk.impl.factory.HMCommandExecutor.execute(HMComm
andExecutor.java:311)
at
```

```
oracle.av.platform.agent.collfwk.impl.factory.HMCommandExecutor.startHostMonit
or(HMCommandExecutor.java:111)
at
oracle.av.platform.agent.collfwk.impl.factory.HMCommandManager.startHostMonito
r(HMCommandManager.java:679)
at
oracle.av.platform.agent.collfwk.impl.factory.HMCommandManager.startTrail(HMCo
mmandManager.java:736)
at
oracle.av.platform.agent.collfwk.impl.factory.CollectionFactory.createCollecti
on(CollectionFactory.java:565)
at
oracle.av.platform.agent.collfwk.impl.factory.CollectionFactory.createCollecti
on(CollectionFactory.java:392)
at
oracle.av.platform.agent.StartTrailCommandHandler.processMessage(StartTrailCom
mandHandler.java:63)
at
oracle.av.platform.agent.AgentController.processMessage(AgentController.java:5
85)
at
oracle.av.platform.agent.AgentController$MessageListenerThread.run(AgentContro
ller.java:3075)
at java.lang.Thread.run(Thread.java:745)
Caused by: java.io.IOException: Cannot run program "/u02/app/oracle/product/
avdf12/av_agent/hm/hostmonmanager" (in directory "/u02/app/oracle/product/
avdf12/av_agent/hm"): error=13,
Permission denied
Caused by: java.io.IOException: error=13, Permission denied
```

Cause

The AVDF agent and the hostmonitor have been deployed as `root` and `oracle` users are not allowed to run the executables due to the binaries' permissions and the hardcoded configuration.

Solution

1. Redeploy the AVDF agent with oracle user using documentation steps: Deactivate and Remove the Audit Vault Agent
2. Copy the zip file for host monitor deployment:

   ```
   cd <Agent Installation Directory>/stage/plugins
   cp agent-linux-x86-64-hmon-one.zip to /usr/local
   ```

3. Unzip the file as `root` user:

   ```
   unzip the agent-linux-x86-64-hmon-one.zip filecd hm
   ```

4. Install host monitor:

   ```
   ./hostmonsetup install agentuser=oracle agentgroup=oinstall
   ```

5. Start the agent

```
cd <agent home>/bin
./agentctl start
```

6. Start the network trail.

L.125 How To Start an Audit Trail for Audit Trail Type `DIRECTORY` if the Database is Down

This document explains how to start audit trail for OS audit files even when the database is down or only in `MOUNT` state.

1. For the collector to start you need to add 3 NLS attributes that the collector needs to parse the OS audit files.Collect the following information from the secured target database while it is running, if this is a standby database you can also collect this information from the primary database:

```
select parameter, value from v$nls_parameters where parameter in
('NLS_LANGUAGE','NLS_TERRITORY','NLS_CHARACTERSET');
```

   For example:

```
PARAMETER VALUE---------------- --------------------
NLS_LANGUAGE AMERICAN
NLS_TERRITORY AMERICA
NLS_CHARACTERSET AL32UTF8
```

2. Add these NLS attributes of the secured target database to the collector:

```
ORCLCOLL.NLS_TERRITORY
ORCLCOLL.NLS_LANGUAGE
ORCLCOLL.NLS_CHARSET
```

   Adding these attributes manually is necessary to be able to start the audit trail and collect audit records from OS files even if the database is in `MOUNT` state or down.

   See more information atOracle Database Audit Collection Attributes in the Plug-In Reference section.

L.126 After Setting the "SSH Acess" Setting, the SSH Connections are Dropped

Symptoms

After setting the "SSH Access" setting from the "Network Services" AVDF configuration page, the SSH connections are dropped.

Cause

When the SSH connection was being created a telnet connection protocol was used.

Solution

Use the SSH protocol to connect to the AVDF server.

L.127 AVDF Directory Audit Trail Stays Up Collecting Audit Data Even When Target Database Is Shutdown

Question

Why does AVDF directory Audit Trail stay up collecting audit data, even when target database is shutdown?

Answer

Directory audit trail collectors does not need target database to be up and running for collection. As long as the directory contains log files or audit files, directory trail collector collects. Hence non-availability of target database does not immediately translate to warning in AVDF UI. This is the inherent nature of directory trail collector.

If the target database is down, directory trail can continue running as long as it has access to directory or audit logs.

This behavior is unlike table audit trails, where non-availability of target database immediately translates to warning in AVDF UI.

L.128 ODF-10717 Is Logged In /var/log/messages File During The Starting Up of Database Firewall

Symptoms

ODF-10717 can be logged in /var/log/messages file during the starting up of database firewall.

```
Example)
Jan 18 00:45:51 <HOST> <EP>: com.oracle.dbfw.fw INFO - ODF-10102: Startup
complete: Ready to process network traffic
Jan 18 00:45:51 <HOST> <EP>: com.oracle.dbfw.fw WARN - ODF-10717: Zero DAM
packets processed: pcap_dispatch() processed zero packets out of 20 requested
Jan 18 00:45:51 <HOST> <EP>: com.oracle.dbfw.fw ERROR - ODF-10701: Network
packets not intercepted: Maximum capacity of the system has been exceeded for
Protected Databases '<SECURE TARGET1>', '<SECURE TARGET2>'
```

Cause

ODF-10717 can be logged when a empty network packet is detected on using DAM mode environment.

Also it is easly detected during the starting-up of database firewall or under heavy networking trafic.

This does not always mean that there are some kinds of crtical errors and it can be safely ignored in usual.

Solution

Safely ignore ODF-10717.

L.129 Error: Net::ReadTimeout occurred when executing Setup_ha.rb --disable_failover

Symptoms

Error: Net::ReadTimeout occurred when executing `Setup_ha.rb --disable_failover`.

```
$ /usr/local/dbfw/bin/setup_ha.rb --disable_ failover
Error: Net::ReadTimeout
```

Cause

After script was changing status to `DISABLE`, the other DBFW will be processed to reflect the settings, but at that point a timeout error has occurred.

Solution

If the result of `/usr/local/dbfw/bin/setup_ha.rb --status` is DISABLE, no other action is needed.

```
[root@avsxxxxx ~]#sudo -u oracle /usr/local/dbfw/bin/setup_ha.rb --status
HA mode: PRIMARYHA server 1: xx.xx.xx.xx
HA server 2: xx.xx.xx.xx
...
Automatic failover: DISABLED <<<<<
```

L.130 Audit Records Being Re-Read After Upgrade to 20.1

Problem

After upgrading to 20.1, audit records for `SYSLOG` that have been read prior to the upgrade are being re-read.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

> **Note:**
>
> This issue is only found in Oracle AVDF 20.1 and is resolved in 20.2 (20 RU2) and subsequent releases.

If you are still encountering this problem, follow these steps to resolve the issue:

1. Stop the audit trail.

2. Unlock the `avsys` user.

   See Unlocking the AVSYS User.

   > **Note:**
   >
   > Remember to relock the `avsys` account when you've completed this task.

3. Execute the provided SQL procedure:

```
DECLARE
   v_count NUMBER;
BEGIN
   FOR i IN (select audit_trail_id from audit_trail where location not
like 'ÞLETED_%' and audit_trail_type like 'SYSLOG' and plugin_guid like
'com.oracle.av.plugin.oracle') LOOP
      select count(*) into v_count from avsys.checkpoint where
audit_trail_id=i.audit_trail_id;
      if v_count = 0 then
         insert into avsys.checkpoint (audit_trail_id,checkpoint_time)
(select i.audit_trail_id,max(event_time) from event_log where
audit_trail_id=i.audit_trail_id);
      end if;
   END LOOP;
   COMMIT;
END;
/
```

4. Lock the `avsys` user.

   See Locking the AVSYS User.

5. Proceed with the upgrade to version 20.1 as intended.

L.131 Audit Records May Be Skipped After Upgrade to 20.1

Problem

Oracle `DIRECTORY` and `SYSLOG` audit trails may skip audit records during successive recoveries for `XML` and `SYSLOG` files. This behavior occurs after upgrading to 20.1.

Solution

This issue is only found in Oracle AVDF 20.1 and is resolved in 20.2 (20 RU2) or later.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

L.132 Processes Still Run After Stopping Audit Trails

Problem

Before upgrading to 20.1, audit trails should stop; however, some of the processes continue to run even after stopping the audit trails. These processes may lead to problems.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

To resolve this issue, begin by identifying and removing the `avorclcoll` processes that might be persisting on the host machine. For each host machine where an Oracle Directory trail is configured, execute the following command:

```
ps -ef | grep avorclcoll
```

If the `avorclcoll` process exists, then terminate the process by executing the following command:

```
kill -9 <pid>
```

Replace `<pid>` with the actual Process ID associated with the `avorclcoll` process.

L.133 Unable to Execute the Oracle User Setup Script

Problem

You may encounter an execution failure when attempting to run the `oracle_user_setup.sql` script. This may be attributed to the presence of an underscore (_) in the username, leading to the unsuccessful execution of the script.

> **Note:**
>
> This issue is only found in Oracle AVDF 20.1 and is resolved in 20.2 (20 RU2) and subsequent releases.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

To fix this issue, you should create a user profile that does not contain an underscore in the name. Proceed with the execution of the `oracle_user_setup.sql` script using the newly created user account.

L.134 Loss of Bonding Between Network Interface Cards Upon Creation of Proxy Port

Problem

When a network interface card (NIC) bonding is established, the creation of a proxy port on one of the NICs through the Audit Vault Server console, performed as a super administrator, leads to the unintended removal of the established NIC bonding.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

After setting the port in the UI and encountering the loss of bonding, follow these steps to reconfigure the bond using the command-line interface (CLI):

1. Configure Bonding via CLI: Use the CLI on the Database Firewall instance to configure the bonding between the relevant devices. See the CONFIG-BOND documentation for more details.
2. Configure Proxy Ports: Set up the necessary proxy ports for the bonded device as required for your configuration. See the CONFIG-PROXY documentation for more details.
3. Re-establish Bonding: Execute the bonding command, as outlined in Step 1, to re-establish the bond between the network interface cards.

L.135 Issue Between Returned Number of Rows and Database Response Monitoring Interaction

Problem

An issue occurs when database response monitoring is active and you have enabled the return number of rows for the Database Objects policy.

> **Note:**
>
> This issue has been eliminated in Oracle AVDF 20.4 and subsequent releases.

Symptoms

The following symptoms may occur when you experience this issue:

1. Successful extraction of returned number of rows for all `SELECT` queries.
2. Marking of returned number of rows as -1 on timeout for `SELECT` queries that match the policy.
3. A substantial influx of Database Firewall alerts is generated in Oracle AVDF 20.3. This occurs when both the **Capture Database Response** and **Capture number of rows returned for** `SELECT` **queries** field are enabled within the Database Firewall monitoring point.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

To resolve this issue, implement the following workarounds:

1. If database response monitoring is not essential, consider turning off this feature to mitigate the encountered issue.
2. Adjust the timeout interval as guided in the solution described under Issue with Retrieval of Return Row Count.

3. Avoid enabling the **Capture Database Response** field while simultaneously activating the **Capture number of rows returned for** `SELECT` **queries** field within the Database Firewall monitoring point. This step helps alleviate the generation of excessive Database Firewall alerts.

L.136 Database Firewall Instance Status "Down" Post-Upgrade to 20.2

Problem

Upon upgrading from Oracle AVDF 20.1 to 20.2, an issue may occur where the status of the Database Firewall instance is incorrectly indicated as "Down" within the Audit Vault Server console. Additionally, the version of the Database Firewall instance is incorrectly displayed as 20.1, despite the upgrade.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

To resolve this issue, implement the following step:

1. Reboot the Database Firewall host.

By performing a host reboot, you can rectify the inaccurately reported "Down" status and the version mismatch for the Database Firewall instance.

L.137 "Failed to Update" Error Encountered During Oracle AVDF 20.2 Upgrade

Problem

When upgrading to Oracle AVDF 20.2, a “Failed to Update Error” may be observed while running the pre-upgrade RPM.

The following error message is displayed:

```
Failed to apply update: Verifying pre-upgrade conditions failed.
Failed to apply update: /images/upgrade/lib/preconditions……
```

> **Note:**
>
> Losing power during an upgrade can result in the loss of data. Do not power off your machine while the upgrade is in progress for best results.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

To address this issue, complete these steps:

1. Execute the following command, where <PID> represents the Process ID and is accessible within the directory path: /tmp/<directory name>/<PID>:

   ```
   kill -9 <PID>
   ```

2. Proceed by applying the pre-upgrade RPM once more.

L.138 Significant Time Delay in Captured Traffic by the Database Firewall For Reporting

There may be a significant time delay from the moment traffic is captured by the Database Firewall to the time it is available for report generation.

Symptoms

There may be a significant time difference between the time when the traffic is captured by the Database Firewall and the time when it is available at Audit Vault Server (AVS) for report generation. For example, if some SQL is captured, it may not be available in AVS for a few hours to generate the reports.

The corresponding time at which the data becomes available to AVS can be checked from the AVSYS.EVENT_LOG table on the AVS server. This can be done by the following SQL command:

```
SELECT MAX(EVENT_TIME) FROM AVSYS.EVENT_LOG;
```

Cause

The possible causes may be one of the following:

1. There could be a time zone mismatch on the UI and the visible time stamp is shifted.
2. There is a significant load on one of the Enforcement Points and the Audit Vault Server is not able to insert the data at the appropriate rate.
3. Some other problem.

Solution

The corresponding solutions to the above mentioned causes are as follows:

1. Connect directly to the Audit Vault Server database and run a query on the AVSYS.EVENT_LOG table. Compare the time stamp with the expected one.
2. To confirm there is a significant load on one of the Enforcement Points, check the number of files in the /usr/local/dbfw/va/*/log directories. If the number of kernel*.gz files is over 10, then this is a plausible cause.
3. Collect the diagnostic package for further investigation.

L.139 ODF-10719 Error Logged In Messages File After Starting Database Firewall

The error code `ODF-10719` is logged in the messages file when starting Database Firewall, indicating difficulties in loading session information from a file.

Problem

When starting Database Firewall, a `ODF-10719` error may be logged into the `/var/log/messages` file.

The following error message is an example of what is displayed:

```
<HOST> auditd[4106]: Audit daemon rotating log files
<HOST> <EP>.24: com.oracle.dbfw.dbfw_server WARN - ODF-10719: Unable to load
Session information from file: Could not acquire lock on file for instance=0
after 120 seconds.
```

Cause

Database Firewall collects the information of a session via a connect packet. Database Firewall manages the information of each session by using the connection information. A `ODF-10719` error can occur when the Database Firewall cannot confirm the connect package information because it is unable to load the session information from its files. This may occur if sessions are already established before starting Database Firewall, which in turn means that Database Firewall cannot collect connect packets of the established session so it is missing this information in the logs.

Another possible cause is if the connection pooling feature is used on a target environment. This may result in an `ODF-10719` error being logged in messages file after starting Database Firewall.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

Please safely ignore the `ODF-10719` error. Restart Database Firewall and then your session.

L.140 "Server Error 500" on Oracle AVDF Server after Setting Network Time Protocol (NTP)

After setting the Network Time Protocol (NTP) option on the Oracle AVDF server, the following error may occur: `Server Error 500`.

Problem

After setting the NTP using the setup page from the GUI, the following error message is observed:

```
Server Error 500
```

Cause

This error is caused by setting the NTP option on the Oracle AVDF server. This causes the server to stop working and show the above error message.

Solution

This issue can be solved by completing the following steps:

1. Disable the NTP setting.
2. Set the time manually.
3. Reboot the Oracle AVDF Server

After completing these steps, the database and all other services should start successfully. After the application starts successfully, the NTP service can be enabled again without issues.

L.141 Audit Vault Agent Logs Report IO Error: The Network Adapter Could Not Establish Connection Due To Inactive Database Listener

Audit Vault Agent logs report IO Error saying the network adapter could not establish connection due to the inactivity of the database listener which leads to the disruption in the audit trail.

Problem

The Audit Vault Agent logs return an IO Error that states `The Network Adapter could not establish the connection`.

Cause

When the database listener is inactive, the audit trail loses its ability to establish communication with the database through the agent, leading it to enter a stopped state. It is crucial to ensure that the database is available and that the connected listener is active. Additionally, you should verify that the database services are correctly registered with the listener. If the listener is down, or in instances where the listener is active, but without any associated database services registered, this situation triggers a shutdown of the audit trails with the above error message.

Solution

To resolve this issue, you must ensure that the database listener is active and the database service is up. Use the command `ps -ef|grep tns` to check the status of the listener. Below is the output of this command when the listener is down:

```
root 10 2 0 Aug30 ? 00:00:00 [netns]
oracle 1673 1245 0 07:47 pts/1 00:00:00 grep tns
```

Next, use the command `ps -ef|grep pmon` to see the status of the database service. Below is the output of this command when the database service is up:

```
oracle 1670 1245 0 07:47 pts/1 00:00:00 grep pmon
oracle 3003 1 0 Aug30 ? 00:00:46 ora_pmon_orcl
```

See Creating and Configuring a Database Firewall Monitoring Point for more information.

Additionally, a `TNSPING` to the database service can verify the availability of the listener. If the listener is found to be inactive, start it using the `LSNRCTL` utility. Once the listener is running, the audit trail collector should initiate, and the status should display a green arrow pointing upwards.

Monitor the agent logs located at `$AGENT_HOME/av/log`. No further error logs should be reported upon successfully starting the collectors. Regularly checking these logs will help ensure the proper functioning of the collectors.

L.142 `oracle_user_setup.sql` Script Does Not Finish

Problem

When using the `oracle_user_setup.sql` script to grant `AVAUDIT SETUP` privilieges to a database user, the gets stuck and never finihses, but does not show any errors on screen.

Cause

In the script a grant select on `SYS.GV_$INSTANCE` to `AVAUDIT` is ran but it never finishes. You can see this from the logs generated on the target database by implementing the below traces:

```
alter session set max_dump_file_size = unlimited;
alter session set tracefile_identifier='&name_for_the_output';
alter session set events '10046 trace name context forever, level 12';
grant select on SYS.GV_$INSTANCE to AVAUDIT;
ALTER SESSION SET EVENTS '10046 trace name context off';
```

Solution

Determine what is preventing the grant on `GV_$INSTANCE` by running the following commands:

```
SQL>SELECT SID, OWNER, OBJECT, TYPE FROM V$ACCESS WHERE OBJECT =
'GV_$INSTANCE'
select * from V$LOCKED_OBJECT where OBJECT_ID in (select object_id from
All_Objects where OBJECT_NAME = 'GV_$INSTANCE');
select distinct to_name object_locked from v$object_dependency where
to_address in (select w.kgllkhdl address from dba_kgllock w, dba_kgllock h,
v$session w1, v$session h1 where ((h.kgllkmod != 0) and (h.kgllkmod != 1) and
((h.kgllkreq = 0) or (h.kgllkreq = 1))) and (((w.kgllkmod = 0) or
(w.kgllkmod= 1)) and ((w.kgllkreq != 0) and (w.kgllkreq != 1))) and
w.kgllktype = h.kgllktype and w.kgllkhdl = h.kgllkhdl and w.kgllkuse =
w1.saddr and h.kgllkuse = h1.saddr);
```

On a Real Application Cluster (RAC) database, run these commands on all nodes.

If no process can be identified, then a restart of the database might solve this issue. This way, any lock on the `GV_$INSTANCE` will be removed.

L.143 Authentication Processing Error When Logging in Due to Excessive Group String Length in Active Directory

An error in authentication processing is triggered by an excessive group string length in the Active Directory, leading to disruptions in user access.

Problem

Users receive an error message prompting them to contact their application administrator after there is an error processing authentication. This error disrupts the user's ability to successfully authenticate and access the AVDF system.

Cause

This issue arises when the group string associated with the AD/LDAP user in the Active Directory is too long. The group string length cannot exceed 8,000 characters; the system encounters an error processing authentication when the length surpasses this amount. See Integrating Oracle Audit Vault and Database Firewall with Microsoft Active Directory or OpenLDAP for more information.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

To resolve this issue and ensure successful authentication, it is important to adhere to the current group string length requirement. Reduce the number of groups for the AD/LDAP users so that the group string length remains within the 8,000 character limit. Additionally, administrators should manage the user group assignments within the Active Directory to ensure that users are only added to necessary groups. After reducing the number of groups, login to AVDF with the AD user as planned.

L.144 Discrepancies When Registering a Target Using Internet Explorer as the Browser

Problem

When using Internet Explorer Audit Vault Server target registration screen is different from the manual.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

You will additionally need to use a different broswer as Audit Vault Server console does not support Microsoft Internet Explorer 11 (and prior), starting with Oracle AVDF release 20.6

L.145 Datafiles Don't Change to Read Only Mode After Entering Archive Period

Problem

A tablespace is not entering `READ ONLY` status even after the archive period has started.

Cause

The definition of `ALERT_EVENT_MAP_TRANS` is incorrect. The definition of `ALERT_EVENT_MAP_TRANS` should be the same as the definition of `ALERT_EVENT_MAP`.

Check the definition of `ALERT_EVENT_MAP_TRANS` and `ALERT_EVENT_MAP` by running the following commands:

```
desc AVSYS.ALERT_EVENT_MAP_TRANS


desc AVSYS.ALERT_EVENT_MAP
```

Solution

Change the definition of the `ALERT_EVENT_MAP_TRANS` table to match that of the `ALERT_EVENT_MAP` table.

L.146 Datafiles Don't Change to Read Only Mode After Entering Archive Period

Problem

A tablespace is in `ONLINE` status even after the archive period has started, because the tablespace is not entering `READ ONLY` status.

Symptoms

You can use the following query to determine the date that the tablespace entered the archive period and it's current status:

```
SQL> select a.tablespace_name, a.status,
to_char(b.bytes,'999,999,999,999')"BYTES",
to_char(add_months(to_date('01-01-1970','MM-
DD,YYYY'),substr(a.tablespace_name,9,3)+1),'DD-MON-YYYY') "WHEN PLACE
OFFLINE",
to_char(add_months(to_date('01-01-1970','MM-
DD,YYYY'),substr(a.tablespace_name,14,3)+1),'DD-MON-YYYY') "WILL BE DELETED",
(-1)*months_between(to_char(add_months(to_date('01-01-1970','MM-
DD,YYYY'),substr(a.tablespace_name,9,3)),'DD-MON-YYYY'),
to_char(add_months(to_date('01-01-1970','MM-
DD,YYYY'),substr(a.tablespace_name,14,3)),'DD-MON-YYYY')) "MONTHNS BETWEEN"
from dba_tablespaces a, dba_data_files b
where a.tablespace_name = b.tablespace_name
```

```
and a.tablespace_name like '%ILM%'
order by a.tablespace_name
```

The output will be in the format: `TABLESPACE_NAME STATUS BYTES DATE PLACED OFFLINE DATE IT WILL BE DELETED MONTHNS BETWEEN`.

For example, if the output is `TABLESPACE_ABC ONLINE 104,857,600 01-OCT-2020 01-APR-2021 6`, then it means that the tablespace "TABLESPACE_ABC" is online, contains 104,857,600 bytes, was placed offline on October 1, 2020, was deleted on April 1, 2021, and was in the archive period for six months between October and April.

Solution

1. Check the following information:
   This should return 0:

   ```
   select count(*) from avsys.JOB_STATUS_TRANS;
   ```

   This should return `AVSPACE`:

   ```
   select tablespace_name from dba_tables where table_name
   ='JOB_STATUS_TRANS';
   ```

2. Disable `AVS_MAINTENANCE_JOB` by running the following:

   ```
   exec dbms_scheduler.disable ('AVSYS.AVS_MAINTENANCE_JOB');
   ```

   Ensure that it is disabled by running the following:

   ```
   SELECT STATE,enabled FROM dba_scheduler_jobs where
   job_name='AVS_MAINTENANCE_JOB';
   ```

3. Set event 14529 at level 512 by running the following:

   ```
   alter session set events '14529 trace name context forever, level 512';
   alter system set events '14529 trace name context forever, level 512';
   ```

4. Run the following on the Audit Vault database as the `AVSYS` user:

   ```
   DROP TABLE AVSYS.JOB_STATUS_TRANS;

   CREATE TABLE AVSYS.JOB_STATUS_TRANS as
       SELECT * FROM AVSYS.JOB_STATUS
           WHERE 1=0;

   ALTER TABLE AVSYS.JOB_STATUS_TRANS
       ADD CONSTRAINT CK_JOB_STATUS_TRANS_STATUS
       CHECK (STATUS IN ('Starting',
                         'Running',
                         'Stopping',
                         'Completed',
                         'Failed',
   ```

```
                    'Waiting'));
commit;
```

Verify this completed successfully by running the following:

This should return 0:

```
select count(*) from avsys.JOB_STATUS_TRANS;
```

This should return 1:

```
 select count(*)from dba_tables where table_name = 'JOB_STATUS_TRANS';
```

This should return `AVSPACE`:

```
select tablespace_name from dba_tables where table_name
='JOB_STATUS_TRANS';
```

5. Disable event 14529 by running the following:

```
alter system set events '14529 trace name context off';
alter session set events '14529 trace name context off';
```

Confirm event 14529 is now disabled by running the following:

```
SET SERVEROUTPUT ON
DECLARE
event_level NUMBER;
BEGIN
DBMS_SYSTEM.READ_EV(14529, event_level);
dbms_output.put_line (' 14529 is set at level '||TO_CHAR (event_level));
END;
```

6. Re-enable the `AVS_MAINTENANCE_JOB` by running the following:

```
exec dbms_scheduler.enable ('AVSYS.AVS_MAINTENANCE_JOB');
```

Ensure that it is enabled by running the following:

```
SELECT STATE,enabled FROM dba_scheduler_jobs where
job_name='AVS_MAINTENANCE_JOB';
```

L.147 OAV-46599 Internal Error: The Data Guard Observer Is Not Present When Performing Manual Switchover of Audit Vault Server

The internal error `OAV-46599` occurs in a High Availability (HA) setup where the data guard observer is found to be absent, preventing the switchover process. To resolve this issue, you should enable automatic failover so that the data guard observer status is set to `YES`.

Problem

When attempting to perform a High Availability switchover, an `OAV-46599 Internal Error` occurs, indicating the absence of the Data Guard observer. The following error message is an example of what is displayed:

```
OAV-46599: Internal Error: The Data Guard Observer is not present
```

When the automatic failover is disabled, both the primary and secondary (standby) servers will display blank Data Guard observer statuses, which inhibits the switchover process. The following is an example of the first several lines of the status:

```
$ /usr/local/dbfw/bin/setup_ha.rb --status
HA mode: PRIMARY
HA server 1: <IP 1>
HA server 2: <IP 2>
Unique database name:
Current database role: PRIMARY
Data guard broker: ENABLED
Data guard observer:
...
```

> **Note:**
>
> Data Guard observer is blank instead of saying `YES`. This occurs in both the primary and secondary (standby) modes.

Cause

This error is caused by the absence of the Data Guard observer, which is necessary for the role switching process in the High Availability setup. The observer statuses are blank because automatic failover must be disabled.

Solution

To resolve this issue, please take the following steps:

1. Enable automatic failover. Please see Disabling or Enabling Failover of the Audit Vault Server for more information.
2. Ensure that the Data Guard observer status is set to `YES`.
3. Now perform the switchover process.

L.148 Mail Notification Fails When Mailing Server is Configured with TLS/SSL

Problem

When the mailing server is configured with TLS/SSL, the mail notifications fail due to a failure during secure handshake.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

L.149 Upgrade To Oracle AVDF 20.5 Fails While Executing Database-Migrations.rb

When attempting to upgrade to Oracle AVDF 20.5, it fails due to executing database-migrations.rb simultaneously. Take the below steps to successfully complete the upgrade.

Problem

Upgrading to Oracle AVDF 20.5 fails due to executing database-migrations.rb simultaneously. First, you should confirm that the upgrade failed due to this issue. Below are the various ways to confirm:

- Check the status within the Oracle AVDF Server.
  1. Log in to the Oracle AVDF server as the root user.
  2. Run the following command: `/opt/avdf/bin/privmigutl -status`
     If the following error was produced, then the upgrade did fail for this reason:

     ```
     System state - recovery
     Migration set 'AVS' - failed
     Last migration 'Updating Oracle Audit Vault and Database Firewall data'
     - failed
     Migrations will be resumed with 'Upgrading apex20'
     ```

- Check the output of this command: `/opt/avdf/bin/privmigutl -history`. The last three lines produced should be similar to below:

  ```
  Migration AVS:35, database-migrations.rb (as root) - failed
  Migration APPLICATION:4, run-application-migrations["avs"] (as root; retry
  permitted) - failed
  Migration TOP:11, run-privileged-migrations["application"] (as root; retry
  permitted) - failed
  ```

- Check the output of this command: `/var/log/messages`. The result should contain the following error message or similar:

  ```
  database-migrations.rb ERROR - ODF-10001: Internal error: Failed to
  execute: ["/usr/bin/sudo", "-u", "oracle", "-E", "-H", "/var/lib/oracle/
  dbfw/bin/sqlplus", "/", "as", "sysdba", "@/usr/local/dbfw/bin/migration/
  ```

```
connector.sql", "/usr/local/dbfw/bin/migration/2021/
changeset_210528_PIGYKICYSE/database.sql"]
database-migrations.rb ERROR - ODF-10001: Internal error: Incremental
migration of the system failed
```

- Check the output of this command: `/var/log/debug`. The result should contain the following error message or similar:

```
database-migrations.rb DEBUG - Command output: alter table
avsys.alert_event_map_arch add policy_name varchar2(4000 char)
database-migrations.rb DEBUG - Command output: *
database-migrations.rb DEBUG - Command output: ERROR at line 1:
database-migrations.rb DEBUG - Command output: ORA-01658: unable to create
INITIAL extent for segment in tablespace
database-migrations.rb DEBUG - Command output: AV_ILM_0615_0621
```

Cause

The upgrade fails because you cannot upgrade the Oracle AVDF server while executing database-migrations.rb.

Solution

To resolve this issue, please take the following steps:

1. Log in to the AVDF server database as `sysdba`
2. Execute the following query:

   ```
   alter table avsys.alert_event_map_arch add policy_name varchar2(4000 char);
   ```

   The query should fail with the error:

   ```
   ERROR at line 1: ORA-01647: tablespace 'AV_ILM_XXXX_XXXX' is read-only,
   cannot allocate space in it
   ```

3. Make the `AV_ILM_XXXX_XXXX` tablespace online/read write by executing the below queries in the AV server database as `sysdba`:

   ```
   alter tablespace AV_ILM_XXXX_XXXX online;
   alter tablespace AV_ILM_XXXX_XXXX read write;
   ```

4. Repeat steps 2-3 until the query in step 2 executes successfully.
5. Open the SQL file: `/usr/local/dbfw/bin/migration/2021/changeset_210528_PIGYKICYSE/database.sql`
6. Comment out the first two `alter` queries by adding `--` at the start of each line.
7. Navigate to `/usr/local/dbfw/etc/privileged-migrations/` as the root user.
8. Execute the `database-migrations.rb` script:

   ```
   cd /usr/local/dbfw/etc/privileged-migrations/
   ./database-migrations.rb
   ```

9. After the script successfully completes, execute the following command: `echo $?`.

If the output is `2`, the `database-migrations.rb` script has completed successfully.

10. Make all tablespaces read only/offline (revert changes from step 3). Do this by executing the following queries in the AV Server Database as `sysdba`:

```
alter tablespace AV_ILM_XXXX_XXXX read only;
alter tablespace AV_ILM_XXXX_XXXX offline normal;
```

11. Log in to Oracle AVDF Server as the root user and resume the upgrade by executing the following command:`/opt/avdf/bin/privmigutl --resume -confirm`

L.150 How to Disable APEX Developer Console After Upgrading to Oracle APEX 20.1 in Oracle AVDF 20.4

Problem

When upgrading to Oracle APEX 20.1 in Oracle AVDF 20.4, the developer console may become available. The developer console should be disabled.

Solution

To disable the APEX developer console:

1. Log in to the Audit Vault Server through SSH as the `support` user.

> **Note:**
>
> If you're using the Oracle Cloud Infrastructure (OCI) marketplace image, connect through SSH as the `OPC` user.

```
ssh support@<audit_vault_server_ip_address>
```

2. Switch to the `root` user.

```
su - root
```

> **Note:**
>
> If you're using the OCI marketplace image, use the `sudo su -` command.

3. Switch to the `oracle` user.

```
su - oracle
```

4. Start SQL*Plus as `sysdba`.

```
sqlplus / as sysdba
```

5. Run the following:

```
 begin
    APEX_INSTANCE_ADMIN.SET_PARAMETER('DISABLE_ADMIN_LOGIN', 'Y');
    APEX_INSTANCE_ADMIN.SET_PARAMETER('DISABLE_WORKSPACE_LOGIN', 'Y');
end;
```

L.151 AVDF Agent Deployment Failure: Unable to Get Connection from Datasource

The AVDF Agent deployment fails due to an error connecting to the datasource; the solution is to increase the init parameter `processes` value to 1000 for the AV repository database.

Problem

AVDF Agent deployment fails with the following error message:

```
Unable to get connection to the datasource through certificate and without
credentials.
Exception occurred while getting connection:
oracle.ucp.UniversalConnectionPoolException:
Cannot get Connection from Datasource: java.sql.SQLRecoverableException:
IO Error: Got minus one from a read call
```

Cause

The init parameter `processes` is set to the default value of 500. This value is too low for the AV repository database.

Solution

To resolve this issue, increase the init parameter `processes` value to 1000 for the AV repository database. You can do this by running the following SQL query:

```
ALTER SYSTEM SET processes = 1000;
```

Once you have increased the value of this parameter, restart the AV repository database. The AVDF Agent deployment should then succeed.

To learn more about the sizing guidelines, review the *Audit Vault and Database Firewall Best Practices and Sizing Calculator for AVDF 12.2 and AVDF 20.1 (Doc ID 2092683.1)*.

L.152 Audit Vault Agent Installation Fails Due To File System Permissions

The Audit Vault agent installation fails when the file system on which the agent is being installed is mounted with the `noexec` option. This option prevents the execution of programs from the mounted file system.

Symptoms

When attempting to install the Audit Vault agent, the following error message appears:

```
Error occurred during install/upgrade. Check log files for more information.
```

The agent deployment log file contains the following error message:

```
java.io.IOException: Cannot run program "/home/audituser/avault/bin/
agentctl":
java.io.IOException: error=13, Permission denied
```

Cause

The error occurs because the file system on which the agent is being installed is mounted with the `noexec` option. This option prevents the execution of programs from the mounted file system.

Solution

To resolve this issue, take the following steps:

1. Check the Java version: Ensure that you have Java SE 6 or later installed on your machine. To check the Java version, run the following command: `java -version`
2. Verify the file system mount options: Check whether the file system on which the agent is being installed is mounted with the `noexec`option. Run the following command to check the mount options: `mount`. Below is sample output of the `mount` command showing the file system mounted with `noexec` option:

   ```
   # mount
   /dev/sda5 on / type ext4 (rw,errors=remount-ro)
   proc on /proc type proc (rw,noexec,nosuid,nodev)
   sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
   ```

3. Remount the file system: If the file system is mounted with the `noexec` option, remount it without this option. The specific command for remounting the file system will depend on the operating system and file system type. For example, to remount an ext4 file system named `/dev/sda5` without the `noexec` option, you would run the following command:

   ```
   mount -o remount,noexec=off /dev/sda5
   ```

4. Deploy the Audit Vault agent: After remounting the file system, deploy the Audit Vault agent. The installation should now proceed without encountering the permission error.

L.153 AVDF Agent Deployment Fails on Target Host with RAC DB Due to Incorrect IP Address Registration

The agent deployment on the target host fails due to an incorrect IP address being used when registering the 'secured host' in the AV server. The outgoing IP address of the cluster should be used instead.

Problem

The agent deployment process fails on the target host, resulting in the following errors:

```
java -jar agent.jar -d <Agent_Home_Path>
Agent host is not registered.
Agent host must be registered before an agent can be installed or upgraded.
Agent deployment failed.
```

Cause

The target host has a RAC DB installed, and the host's physical IP address was used when registering the 'secured host' in the AV server. This causes the agent deployment to fail.

Solution

To resolve this issue, ensure that the outgoing IP address of the cluster, rather than the physical IP address, is specified when registering the 'secured host' in the AV server.

To determine the outgoing IP address of the host:

1. Connect to the AV database using SQLplus.
2. Execute the following query:

   ```
   select sys_context('userenv','ip_address') from dual;
   ```

   The result of this query will display the outgoing IP address of the host. Use this IP address when registering the 'secured host' in the AV server.

L.154 Host Monitoring Agent Installation Fails With Error About Inability to Retrieve Agent Details

Problem

Installation of Host Monitoring Agent fails with the following error:

```
/usr/local/hm# ./hostmonsetup install
Unable to retrieve - 1. Agent User 2. Agent Location 3. Platform Validation
4. HM Install State
Exception occured while creating AVS DB connection. Exception: Error while
trying to retrieve text for error ORA-01804
Contact Oracle support.
:/usr/local/hm# ls -ltrh
```

```
/usr/local/hm/log# cat av.hmdeployer.log
[2023-09-16 11:06:21,784] [PID: 54294, TName: main] [ERROR] - Exception
occured while creating AVS DB connection. Exception: Error while trying to
retrieve text for error ORA-01804

[2023-09-16 11:06:21,784] [PID: 54294, TName: main] [ERROR] - Exception
Occured: Unable to establish bootstrap connection to AV Server Database using
connect string:(DESCRIPTION=(ENABLE=BROKEN)(FAILOVER=on)(R
[2023-09-16 11:06:21,851] [PID: 54300, TName: main] [ERROR] - Exception
occured while creating AVS DB connection. Exception: Error while trying to
retrieve text for error ORA-01804
```

Solution

Set the `LD_LIBRARY_PATH` environment variable as the Host Monitoring Agent installation path:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Change the directory to the location of the Host Monitoring Agent:

   ```
   cd /user/local/hm
   ```
3. Set the `LD_LIBRARY_PATH` environment variable:

   ```
   export LD_LIBRARY_PATH=/usr/local/hm
   ```
4. Run the installation of the Host Monitoring Agent:

   ```
   ./hostmonsetup install -verbose
   ```

L.155 Database Firewall Database Tablespace Growing Quickly in AVDF 20.5

Problem

The tablespace in the database firewall database is continuously growing.

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

L.156 AVDF 20.3 - 20.6: Cron File Message - Parent Directory Has Insecure Permissions

Problem

The cron file has the following messages:

```
<Date and Timestamp> <Server-name> CROND[127134]: (root) CMDOUT (error:
skipping "/var/lib/oracle/dbfw/av/log/av.jfwk-<log-nujmber-0>.log"
```

```
because parent directory has insecure permissions (It's world writable or
writable by group which is not "root")
Set "su" directive in config file to tell logrotate which user/group should
be used for rotation.)
```

The log file rotation cron job fails with: `because parent directory has insecure permissions.`

Cause

The `/var/lib/oracle/dbfw/av/log` directory has `drwxrwx--T 2 oracle dbfw` as the ownership and permissions which causes log file rotation issues and stops the Java framework.

Solution

To fix this issue for AVDF 20.3 - 20.6:

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Execute the following:

```
chown oracle:oinstall /var/lib/oracle/dbfw/av/log
chmod 750 /var/lib/oracle/dbfw/av/log
```

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

L.157 Audit Vault Agent Fails to Start from Windows Service

When trying to start the Audit Vault Agent from the Windows service, an error is returned.

Problem

The following error was logged in `<AVDF AGENT HOME>/av/log/av.agent.prunsvr.YYYY-MM-DD.log`:

```
Unable to find Java Runtime Environment.
The system could not find the environment option that was entered.
reportServiceStatusE: dwCurrentState = 1, dwWin32ExitCode = 0, dwWaitHint =
0, dwServiceSpecificExitCode = 0.
```

This is because the `JAVA_HOME` variable was not set in the environment of the Windows operating system (OS).

Solution

1. In the Windows OS, navigate to **Control Panel**.
2. Click **System**.
3. Click **Advanced system settings**.
4. In the **Advanced** tab, click on **Environment Variables** button.
   The Environment Variables dialog is displayed.

5. Add a new `JAVA_HOME` variable that points to your JDK or JRE installation path. For example, `C:\Program Files\Java\jdk1.8.0_65`
6. Start the Audit Vault Agent.

L.158 Error: "tee" Is Not Recognized When Registering Or Starting an Audit Vault Agent on Windows

When registering or starting AVDF AV Agent on Windows server, users may encounter an error stating "tee" is not recognized as an internal or external command.

Problem

When attempting to register or start an AV Agent on Windows Servers, users may encounter the following error:

```
$agentctl start -k
Agent updated successfully
'tee' is not recognized as an internal or external command, operable program
or batch file
```

Cause

The "tee" command error occurs consistently during AV Agent registration or start-up on Windows Servers due to the absence of the "tee" command in the Windows OS.

Solution

The issue does not occur in Oracle AVDF 20.4 and later.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See Patching Oracle Audit Vault and Database Firewall Release 20.

As a workaround until you can patch Oracle AVDF, follow these steps to modify `agent.jar` and resolve the "tee" command error:

1. Connect to the AV server as the Oracle user:

   ```
   su oracle
   ```

2. Navigate to `$ORACLE_HOME/av/jlib` (`ORACLE_HOME` path is `/var/lib/oracle/dbfw` by default):

   ```
   $cd $ORACLE_HOME/av/jlib
   ```

3. Take a backup of the existing `agent.jar`:

   ```
   $cp agent.jar agent_tee.jar
   ```

4. Create a script named `agent-ch.sh` with the provided entries:

   ```
   $ vi agent-ch.sh
   #!/bin/sh
   cd $ORACLE_HOME
   cd av/jlib/
   ```

```
/var/lib/oracle/dbfw/jdk/bin/jar -xvf agent.jar bin/agentctl.bat
sed -i 's: | tee -a "%OH%\\av\\log\\av.agent.log"::g' bin/agentctl.bat
/var/lib/oracle/dbfw/jdk/bin/jar -uvf agent.jar bin/agentctl.bat
rm /var/lib/oracle/dbfw/av/conf/bootstrap.prop
$ORACLE_HOME/bin/avca configure_bootstrap
```

Save the file.

5. Provide execute privileges on `agent-ch.sh`:

```
$chmod 744 agent-ch.sh
```

6. Execute the script `agent-ch.sh`:

```
$./agent-ch.sh
```

7. Download `agent.jar` from the AVDF console and use it to deploy the agent on the Windows server.

L.159 AVDF Agent Management after OS Upgrade

After an OS upgrade, users may encounter problems with the AVDF Agent; users should restart the agent to prevent problems.

Problem

When using Oracle AVDF 20.1 and later, users may encounter issues with the AVDF Agent after an operating system upgrade. The AVDF Agent may be affected if specific precautions are not followed.

Solution

To mitigate potential issues after an OS upgrade, follow these steps:

1. Stop AVDF Agent before an OS upgrade:

```
<AVDF AGENT HOME>/bin>./agentctl stop
```

2. After an OS upgrade, start the Agent:

```
<AVDF AGENT HOME>/bin>./agentctl start
<AVDF AGENT HOME>/bin>./agentctl status
```

Additionally, ensure that the OS version being upgraded is certified and supported by the AVDF Agent.

L.160 Starting a Monitoring Point Causes Error `OAV-46649`

Problem

After successfully creating a monitoring point, attempting to start it fails. Starting through the AVCLI results in error `OAV-46649: Enforcement point is in resume state.`

Cause

DNS is not properly configured in the Database Firewall.

Solution

1. Log in to the Audit Vault Server Console as a `super administrator`.
2. Click **Settings** tab.
3. Click **System** in the left menu.
4. Under **Status** section, click **System Settings**.
5. Configure DNS settings.
6. Click **Save**.
7. Start the monitoring point.

Related Topics

- Configuring Database Firewall Monitoring Points

L.161 Database Firewall Not Capturing in DAM Mode

Problem

Database Firewall is not capturing in database activity monitoring mode on a VMware installation due to network misconfiguration.

Solution

ESX/VMware virtual switch has a property that does not allow VLAN traffic.

1. The switch needs to be re-configured to allow VLAN traffic.
2. Live capture should start working at this point, test and verify that.
3. Check the reports to ensure they are being populated with data.
4. Check to verify that alerts in the Audit Vault Server console are being generated.

L.162 How to Use Linux to Send E-mails From an AVDF Appliance

Problem

How to use Linux to send e-mails from an AVDF appliance?

Solution

1. Log in to the appliance through SSH and switch to the `root` user.

   See Logging In to Oracle AVDF Appliances Through SSH.
2. Execute the following command:

```
Example: echo TEST | mailx -s "subject " -S smtp=10.10.10.10:25
username@oracle.com
```

L.163 Capture Bind Variables When Running the Database Firewall in DAM Mode

Problem

Is it possible to capture bind variables when running the Database Firewall in database activity monitoring (DAM) mode?

Solution

If the Database Firewall is only used to monitor the secured target through a monitoring point then the All Activity report will not capture bind variables involved in the SQL statement.

L.164 Audit Vault Agent Configuration for a `Table` Audit Trail in a RAC Environment

Problem

Learn how to configure the Audit Vault Agent for a <codeph>table</codeph> type audit trail in a real application cluster (RAC) environment.

Solution

Install the Audit Vault Agent in one of the following ways:

- The Audit Vault Agent is installed on one of the nodes. If one of the servers go down, the collection will stop.
- The Audit Vault Agent is installed on both of the nodes. If you register the same database twice, one on each node, then there will be duplicate records.
- The Audit Vault Agent is installed on a separate server. To do this:
  1. Register a separate server as host and install the Audit Vault Agent on the machine
  2. Register the RAC database as a secured target
  3. Add a `Table` type audit trail for this secured target using the same host.
     Since the `Table` audit trail makes a Java database connectivity (JDBC) connection to the secured target database to fetch the records from the `AUD$` table, the audit trail running on a separate host will work without any issues.

Related Topics

- Configuring and Managing Audit Trail Collection
- Configuring Audit Trail Collection for Oracle Real Application Clusters

L.165 Database Firewall Certificate Validation Failed

If in the Audit Vault Server console the Database Firewall page shows a status of `Certificate Validation Failed`, follow these steps to resolve the issue.

1. Update the certificate of the Database Firewall.
   For more information see Fetching an Updated Certificate from Database Firewall.

2. If updating the certificate does not resolve the issue, rotate the Database Firewall certificate.
   For more information see Rotating Database Firewall Certificates.
3. If the Database Firewall certificate can't be rotated, it may be because the Audit Vault Server certificate authority is no longer valid on the Database Firewall. Follow these steps to resolve the issue:
   a. Log in to the Audit Vault Server through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.
   b. Run the following command:

      ```
      openssl x509 -noout -subject -in /usr/local/dbfw/etc/ca.crt
      ```

      Take note of the output.
   c. Log in to the Database Firewall through SSH and switch to the `root` user.

      See Logging In to Oracle AVDF Appliances Through SSH.
   d. Run the following command:

      ```
      openssl x509 -noout -subject -in /usr/local/dbfw/etc/controller.crt
      ```

   e. If the outputs of the commands are different, then you need to add the Audit Vault Server certificate to the Database Firewall.
      For more information see Specifying the Audit Vault Server Certificate and IP Address.

L.166 Configuring ERSPAN for SQL Traffic Auditing in Monitoring (Out of Band) Mode

If Monitoring (Out of Band) is not collecting any SQL traffic audit, follow these steps to resolve the issue.

Problem

Monitoring (Out of Band) in AVDF 20.7 is not collecting any SQL traffic audit. Even though the network interface cards (NICs) are correctly configured and the traffic is being captured in the pcap files, no SQL traffic audit is displayed on the AVDF web page.

Cause

The Database Firewall does not process ERSPAN traffic by default in Monitoring (Out of Band) mode. This has to be enabled on the Database Firewall monitoring points, otherwise, the SQL traffic audits will not be displayed despite being correctly mirrored and captured.

Solution

To resolve this issue, you need to enable ERSPAN processing by setting `DAM_TRAFFIC_IS_ERSPAN=1`. More information can be found in Configuring Encapsulated Remote Switched Port Analyzer with Database Firewall.

L.167 Recovery Disk Group is Getting Full with Archive Logs

Problem

Archive logs are not deleting and are causing the disk group of the standby Audit Vault Server in a high availability pairing to get full.

Run the following commands to determine if the archivelog has been applied to the standby:

```
select a.thread#, a.sequence#, a.applied
from v$archived_log a, v$database d
where a.activation# = d.activation#
and a.applied='YES'
/
```

Make sure the standby is in sync with the primary.

Solution

Ensure that your retention policies are set as this can help free up space in the fast recovery area. For more information see Creating and Deleting Archive and Retention Policies.

If no files are eligible for deletion based on their retention policy, then manual intervention is required. For more information see Managing Archival and Retrieval in High Availability Environments.

L.168 Cannot View the Updated Maintenance Job Schedule After Making Changes

After changing the maintenance job schedule in AVS, the updated time may incorrectly display as 0:00 due to a display issue, but the changes are correctly applied.

Problem

After changing the start time of the maintenance job schedule in the Audit Vault Server, the schedule displays as 0:00 instead of the updated time upon re-login.

Cause

This is a display issue only found in Oracle AVDF 20.7 and later.

Solution

Although 0:00 is displayed, the schedule changes have been successfully applied. You can verify the updated schedule by running the following SQL query in the AVS repository database:

```
select next_run_date,STATE,enabled FROM dba_scheduler_jobs where
job_name='AVS_MAINTENANCE_JOB';
```

L.169 Oracle AVDF Does Not Failover When Primary Server Is Down

When the network connection to the Primary Oracle AVDF server is down, the system does not failover to the Standby server. The current design only triggers a failover if the Oracle AVDF Database or a critical process crashes.

Symptoms

When the network connection to the Primary setup is down and the Primary Oracle AVDF server becomes inaccessible, Oracle AVDF does not initiate a failover to the standby server. Once the network connection to the primary server is restored, Oracle AVDF becomes accessible again through the primary site.

Cause

Oracle AVDF is currently designed to failover only if the Oracle AVDF Database or a critical process crashes and triggers a failover to the Standby site. However, if the network connection is disabled or down, the Observer cannot determine the status of the processes, and as a result, failover will not occur.

Solution

The current Oracle AVDF failover mechanism does not guarantee High Availability, as failover only occurs during process crashes. In cases of network or system outages, the service may remain down. To maintain continuous availability, Oracle AVDF should be accessible from the Standby site when the Primary server is inaccessible. Implementing a Load Balancer could help by directing traffic to the Standby site in such scenarios. See Handling a Failover Scenario for more information on Failover Scenarios.

L.170 Upgrading AVDF from 20.7 to 20.8 Fails When Rebuilding the Index with `UTLRP.SQL`

When attempting to upgrade to Oracle AVDF 20.8, it fails while rebuilding the index by executing `UTLRP.SQL` after setting `max_string_size` to extended.

Problem

When upgrading Oracle AVDF from 20.7 to 20.8, it fails while rebuilding index with `UTLRP.SQL`. You may receive the following error logged in `/var/log/messages`:

```
HOSTNAME su: (to oracle) root on none
HOSTNAME com.oracle.privilegedMigration.max_string_size_extended: Failed
utlrp.sql to setup MAX_STRING_SIZE to extended.
HOSTNAME run-application-migrations[28910]:
com.oracle.dbfw.privilegedMigration ERROR - ODF-10001: Internal error:
FAILEDmigration: max_string_size_extended (as root) (applied change)
```

Cause

The upgrade fails while rebuilding the index by executing `UTLRP.SQL` after setting `max_string_size` to extended.

Solution

To resolve this issue and resume upgrade, follow the steps below:

1. Connect to AVDF DB as `sys`

   ```
   sqlplus / as sysdba
   @/var/lib/oracle/dbfw/rdbms/admin/utlrp.sql
   DECLARE
   ```

   The query should fail with the following error:

   ```
   ERROR at line 1:
   ORA-01502: index 'SYS.I_WRI$_OPTSTAT_HH_OBJ_ICOL_ST' or partition of such
   index is in unusable state
   Function created.
   PL/SQL procedure successfully completed.
   Function dropped.
   Warning: XDB now invalid
   PL/SQL procedure successfully completed.
   ```

2. Rebuild the package to fix the issue by executing the following query:

   ```
   alter index SYS.I_WRI$_OPTSTAT_HH_OBJ_ICOL_ST rebuild;
   ```

3. Executed the script again:

   ```
   @/var/lib/oracle/dbfw/rdbms/admin/utlrp.sql
   ```

4. Run the following commands:

   ```
   alter package objowner.object compile body;
   grant execute on DBMS_SQL to public;
   ```

5. Check if any other invalid objects are present:

   ```
   SELECT owner, object_type, object_name FROM dba_objects WHERE status !
   ='VALID';
   ```

6. Drop the trigger which failed:

   ```
   drop trigger avsys.start_el_migration;
   ```

7. Resume the upgrade:

   ```
   /opt/avdf/bin/privmigutl --resume --confirm
   ```

L.171 Executing '`AVBACKUP BACKUP`' Command Fails

Problem

When executing the '`/var/lib/oracle/dbfw/bin/avbackup backup`' command after running '`/var/lib/oracle/dbfw/bin/avbackup config`' , the operation fails with the following error "info.txt: No such file or directory."

Solution

The `info.txt` file should be located in the same directory. The user must ensure that the backup directory and its parent directories are owned by oracle:oinstall to prevent this error.

see Backup and Restore of Audit Vault Server for more information.

L.172 `Error OAV-47411` "Export Path" Does Not Exist on Remote File System

Learn what to do when you receive the `OAV-47411` error while registering a Network File System (NFS) export to Oracle AVDF.

Problem

While registering an NFS export by executing the following command:

```
AVCLI> REGISTER REMOTE FILESYSTEM <Remote FS name> OF TYPE NFS ON HOST
<Hostname> USING EXPORT <Export path> MOUNT;
```

This error might be encountered:

```
OAV-47411: Export <Export path> does not exist on remote filesystem.
```

Cause

To identify the root cause, complete the following steps:

1. Run the following AVCLI commands and ensure the outputs are correct:
   - The output should display the export path:

     ```
     AVCLI> LIST EXPORT OF TYPE NFS ON HOST <Hostname>;
     ```

   - The output should display the Remote Filesystem name, along with export path:

     ```
     AVCLI> LIST REMOTE FILESYSTEM;
     ```

   - The output should be ACCESSIBLE:

     ```
     SHOW STATUS OF REMOTE FILESYSTEM "<Name of the Remote Filesystem>";
     ```

2. On the NFS server, execute the following command to check the existence and the permissions on the export path:

   ```
   ls -ld <Export path>
   ```

3. Check if the entry for the NFS location is located in the `/etc/fstab` within the Audit Vault Server:

   ```
   cat /etc/fstab
   ```

4. Check the output of following queries:

   ```
   select * from avsys.remote_filesystem;
   select * from avsys.remote_location;
   select * from avsys.archive_host;
   ```

5. Follow the below steps on the AV Server:
   a. Login to the AV Server as support.
   b. Execute the following commands:

      ```
      su root
      su oracle
      cd $ORACLE_HOME
      ```

   c. The output for the above command should display the export list for <IP address of the NFS server>, as shown below:

      ```
      [oracle@<AV host>]$ /usr/sbin/showmount --export <IP address of NFS
      server>
      clnt_create: RPC: Port mapper failure - Unable to receive: errno 111
      (Connection refused)
      ```

      This means the ports (NFS) and 111 (port map) are blocked by the firewalls on the NFS server OR they are not open.

Solution

To resolve this error, check if the NFS server is reachable and all the required ports are open (no firewall is blocking the request on specific ports).

1. Turn off the firewall on the NFS machine.
2. Register the remote filesystem.
3. Mount and check the status.

L.173 AVDF 20.4 Error Accessing Target Report: " P107_FIRST_RUN_TIME_AUDIT "

While accessing the secured target on the AVDF Console, users receive an error "P107_FIRST_RUN_TIME_AUDIT" in Oracle AVDF 20.4.

Problem

When accessing a secured target in the Oracle AVDF 20.4 console, users encounter the following error message:

```
"Error computing item source value for page item P107_FIRST_RUN_TIME_AUDIT".
```

Cause

The error message indicates an issue in retrieving or calculating the source value for the specified page item.

Solution

This issue is resolved in Oracle AVDF 20.6. For earlier versions, the following workaround can be applied:

1. Schedule Audit Policy/User Entitlement (UE) Retrieval with One Auditor only: If the audit retrieval is already scheduled by multiple auditors, delete one.
2. Steps to perform in AVSYS:
   a. Find the Target ID of the affected target:

      ```
      select secured_Target_id from avsys.secured_Target where
      secured_Target_name='target name';
      ```

   b. Check schedules created for that target by auditors:

      ```
      select * FROM avsys.retrieval_schedule where secured_Target_id = <
      Target Id from first SQL Output>;
      ```

   c. Delete an entry for one auditor:

      ```
      DELETE FROM avsys.retrieval_schedule where secured_Target_id = < Target
      Id from first SQL Output> and user_name = 'username' ;
      ```

After completing these steps, the error should no longer occur when accessing the target report.

L.174 Error OAV-47487: Uploading a Certificate to AVDF Fails

Learn what to do when you receive the OAV-47487 error while uploading the certificates to AVDF.

Problem

Uploading a new certificate generated using a CSR from an external source (such as a third-party application) fails with the following error:

```
OAV-47487: Certificate is not compatible with server
```

Cause

Oracle AVDF 12 does not support CSRs that originate outside of its own system.

Solution

The only supported process is to generate the CSR directly from the AVDF application, signing it with a CA, and then uploading the signed certificate. Follow the steps below:

1. Download the CSR from the AVDF Server.
2. Have the CSR signed by the Certificate Authority (CA).
3. Then, upload only the newly signed certificate (excluding the CSR and any intermediate certificates). A certificate chain is not supported.

L.175 Troubleshooting Server Error 500 in AVDF

Learn how to identify the cause of "Server Error 500" in the Oracle AVDF environment.

Problem

When logging into the AVDF Web Console, users may encounter "Server Error 500." This error typically indicates a failure to connect to the repository database, a critical back-end required for the Web Console. Without this connection, login fails, and a Server Error 500 is triggered.

Cause

There are various possible reasons for the Server 500 Error:

1. User account or password issues: Incorrect password, locked account, or unsupported characters in passphrase.
2. Database unavailability: The repository database may be down or not correctly configured.
3. Service startup issues: The database services may not have started correctly, or other dependencies may be unavailable.
4. Database limitations: Connection may be restricted due to database limitations or session limits.
5. Timeout issues: Long loading times for dashboard or console due to performance delays.
6. File system iNode exhaustion: The iNode count on `/var/lib/oracle` is full, preventing login.
7. Other configuration issues: Other system-level configurations may block access.

Solution

To troubleshoot and resolve Server Error 500 in AVDF, follow these steps based on the potential causes listed above:

1. **User Account or Password Issues:**
   a. Verify login credentials by attempting to connect with `sqlplus`:

```
su - oracle
sqlplus <avadmin_user>/<password>
```

b. If login fails, try changing the password or unlocking the account:

```
su - oracle
sqlplus "/as sysdba"
SQL> ALTER USER <avadmin_user> IDENTIFIED BY <new_password> ACCOUNT
UNLOCK;
```

c. Ensure the passphrase does not contain special characters other than _, as unsupported characters may cause login issues.

2. **Database Unavailability:**
   a. Check `/var/log/messages` for specific errors like `ORA-01034` or `ORA-27101` indicating that the database is not available.
   b. For persistent issues, inspect `alert.log` and diagnostic files. Rebooting the AVS server may help restart the repository database and resolve the error.
3. **Service Startup Issues:**
   a. Verify that required services, including Grid Infrastructure (GI) resources, +ASM instance, and TNS listener, are running.
   b. Restart the AVS server if services are not initialized correctly, especially if running AVDF version 12.2.0.4 or later.
4. **Database Limitations**:
   a. Check for `ORA-20` or `ORA-18` errors, which indicate session limits. Reboot the AVS server if these limitations cause connectivity issues.
   b. If session limits continue to be problematic, contact Oracle Support for further investigation.
5. **Timeout Issues:**
   a. Long loading times for the dashboard or Web Console may result in Server Error 500. This is often cause by performance issues or large alert volumes.
   b. For AVDF versions before 12.2 BP#5, increase the `TIMEOUT` setting in `/usr/local/dbfw/templates/template-httpd-httpd.conf` and restart networking settings.
6. **File System iNode Exhaustion**:
   - Run `df -i` to check if `/var/lib/oracle` has reached 100% inode usage. If so, remove excess audit files.
7. **Other Configuration Issues:**
   - Review recent system or database changes. Incorrect configurations, such as manual host reboots without reconfiguration, may disrupt the database.

Following these steps should help diagnose and resolve the underlying cause of Server Error 500. If issues persist, consult Oracle Support with AVDF diagnostic files for additional assistance.

L.176 User Entitlement Retrieval Job Fails After Twelve Hours

Learn how to manage when a user entitlement job fails after running for twelve hours.

Problem

User Entitlement retrieval jobs consistently fail after running for an extended period. This issue may occur when retrieving data from databases with a large number of accounts, resulting in

job termination before completion. The failure typically occurs with an error message indicating the inability to process privilege user data for the target database.

As a result, entitlement snapshots cannot be generated, which impacts reporting capabilities such as Privileged Users or other entitlement reports.

Cause

This issue is caused by a system-defined timeout setting that limits the maximum runtime for jobs. when the job exceeds this limit, it terminates prematurely. Logs may show errors such as: `java.sql.SQLRecoverableException: IO Error: Socket read interrupted`.

Solution

This issue is caused by a system-defined timeout setting that limits the maximum runtime for jobs. when the job exceeds this limit, it terminates prematurely. Logs may show errors such as: `java.sql.SQLRecoverableException: IO Error: Socket read interrupted`

To resolve this issue, follow the steps below:

1. Modify the job configuration by executing the following commands:

   ```
   su - oracle
   vi /var/lib/oracle/dbfw/bin/avjfwk
   ```

2. Update the relevant Java process line to include the following:

   ```
   /usr/bin/java -ea -Dfile.encoding=UTF-8 -DNLS_LANG="$NLS_LANG"-
   DORACLE_HOME="$OH" -Doracle.jdbc.javaNetNio=false -mx1024m -
   classpath$CLASSPATH oracle.av.platform.server.javafwk.JfwkProcess "$@"
   >/dev/null 2>&1
   ```

3. Restart the `javafwk` Service:

   ```
   restart javafwk
   systemctl stop javafwk
   systemctl status javafwk
   systemctl start javafwk
   ```

4. Increase Timeout Settings:

   ```
   AVCLI>alter system set JFWK.THREAD_TIMEOUT_MINUTES=1440;
   ```

5. Resubmit the job. Once the changes are applied, resubmit the User Entitlement job from the AV UI to ensure it completes successfully.

L.177 Unable to Drop Audit Trail from Unreachable Host

If the error "`OAV-46572`: Agent is unreachable on host" appears during an audit trail drop operation, use the following steps to resolve it.

Symptoms

Attempts to drop an audit trail using the GUI or AVCLI fail with the error message:

```
OAV-46572: Agent is UNREACHABLE on host
```

The system reports that the audit trail from the secured target is still running, even though the host or agent has been removed.

Cause

This issue occurs if the agent and audit trails were removed without properly stopping them first. The Audit Vault server keeps the audit trail in an "UNREACHABLE" status, anticipating that the host or agent might recover. Since the agent is inactive, the audit trail cannot be fully stopped.

Solution

If the host and agent will not be restored, proceed with the following steps to manually update the audit trail status:

1. Connect to Audit Vault Server as the support user, switch to root, then to the `dvaccountmgr`, and access SQL*Plus.
2. Set a temporary password for the `AVSYS` user and unlock the account.
3. Execute the following SQL command to update the audit trail status to "STOPPED":

```
UPDATE AVSYS.AUDIT_TRAIL
SET COLLECTION_STATUS=0
WHERE COLLECTION_STATUS <> 0
AND ACTIVE='Y'
AND HOST_NAME = '&unreachable_host'
AND AUDIT_TRAIL_ID IN(
  SELECT AUDIT_TRAIL_ID
  FROM AVSYS.AUDIT_TRAIL
  WHERE HOST_NAME IN(
    SELECT HOST_NAME
    FROM AVSYS.AGENT_VIEW
    WHERE STATUS='UNREACHABLE'
  )
);


COMMIT;
```

4. After executing this update, attempt to drop the audit trail again using the GUI or AVCLI.

> **Note:**
>
> In Oracle AVDF 20.5 and later, you can use the command `DROP HOST <hostname> FORCE` to force the host and its audit trails to be dropped directly.

L.178 Error OAV-47746: Sensitive Objects Data Upload Fails

Learn what to do when you receive the `OAV-47411` error while uploading sensitive objects data in Oracle AVDF.

Problem

When attempting to upload sensitive object data in AVDF 20.8, users encounter the following error:

```
OAV-47746: "Input file with sensitive data is invalid format."
```

Cause

This error may occur when unsupported, invisible characters are present in the file. These characters can cause the file format to be unrecognized during the upload process.

Solution

To resolve this issue, follow the below steps:

1. Open the file with sensitive data and re-saved it.
2. Convert the file from DOS to Unix format using the following command:

   ```
   dos2unix <example.txt>
   ```

3. After converting the file, attempt to upload it again through the AVDF UI console.

For more information on converting files from DOS to Unix format, refer to "Convert DOS to Unix".

L.179 Status "Certificate Validation Failed" Error Shown in Audit Vault Server GUI

If Database Firewall page shows a status of `Certificate Validation Failed` in the Audit Vault Server GUI with the error `OAV-46981: Unable to connect to Database Firewall with IP <ipaddress>`, follow these steps to resolve the issue.

Problem

The Audit Vault Server GUI displays the status "Certificate Validation Failed" for the Database Firewall. Moreover, the following errors appear in the Host Monitor log:

- `OAV-46981: Unable to connect to Database Firewall with IP <ipaddress>`
- `ORA-29273, ORA-28791, ORA-06512: Various errors indicating HTTP request failure and certificate verification failure.`
- Log errors show that the certificate and key files for Host Monitor could not be loaded, and SSL handshake failed.

Cause

The Database Firewall is down due to failed certificate validation. This may be caused by issues with the existing certificates or keys used for SSL communication.

Solution

To resolve the issue, perform the following steps:

1. Take a backup of `/usr/local/dbfw/etc/avs/` folder.
2. Remove the existing certificates and wallet files:
   On the Audit Vault Server, as the root user, execute the following commands:

   ```
   rm -f /usr/local/dbfw/etc/avs/fwcerts/*
   rm -f /usr/local/dbfw/etc/avs/avswallet/*
   ```

3. Generate new SSL certificates:
   Run the following command to recreate the necessary certificates:

   ```
   /usr/local/bin/gensslcert create-certs
   ```

4. Update certificates in the `AV` Console:
   - Log in to the AV console as an administrator.
   - Go to the Database Firewall tab.
   - Select each Database Firewall and click the "Update Certificate" button.
   - Confirm that the Database Firewall status is now showing up as "Up."

   This solution should resolve the certificate validation issue and restore the connection with the Database Firewall.

L.180 OAV-47804: Invalid Credentials for User While Registering AD With AVDF

Problem:

While Registering AD with AVDF, the following error appears:

```
Error OAV-47804: Invalid Credential for User
```

Cause:

This error arises when the AD user DN, such as `cn=xyz,cn=users,dc=domain,dc=com` is specified instead of the username `xyz`.

Solution:

To resolve this issue, replace the DN with the AD username `xyz` and retry the registration process.

L.181 "Check Health of Audit Vault Server" Is Seen as Failed in the Job Status

Problem

In Oracle AVDF 20.9, the job status of the AVS health check job may fail with the following error message:

```
avsxxxxxxxxxxx oracle: [AVDF SYSTEM ALERT] <Severity:Critical> <Alert
Category:Password> <Alert Subcategory:Audit Vault Server Administrator and
Auditor users password expiry> <Description:Password has expired of Audit
Vault Server user XXXXXXXXX, YYYYYYYYY, ZZZZZZZZ.> <Recommendation:Change the
password for these users.>
```

Solution

To resolve the following error, reset the password for the users shown in the above log.

> **Note:**
>
> User details may vary.

L.182 User Entitlement Job Fails With Error '`Failed to Get User Entitlement Data From Secured Target Targetname`'

Learn how to resolve a User Entitlement job failing when user account privileges are not setup on the secured target database.

Problem

The User Entitlement Job fails with the follwing errors in the AVDF Console:

```
Failed to get user entitlement data from secured target TARGETNAME.
```

or

```
Caused by: Error : 942, Position : 58, Sql = SELECT grantee, privilege,
admin_option, common FROM sys.dba_sys_privs, OriginalSql = SELECT grantee,
privilege, admin_option, common  FROM sys.dba_sys_privs, Error Msg =
ORA-00942: table or view does not exist
```

Cause

The cause of this error is the user account privileges for Oracle AVDF are not setup on the secured target database.

To check this, connect to the secure target TARGETNAME as the avagent user. Then, execute the following query:

```
Sql = SELECT count(*) FROM sys.cdb_pdbs
```

the same error "ORA-00942: table or view does not exist" occurred.

Solution

To resolve this issue, follow the steps below:

1. Refer to Oracle Database Setup Scripts.
2. Execute `@oracle_user_setup.sql` and enter mode as `SETUP`.
3. Execute `@oracle_user_setup.sql` once more and enter the mode as `ENTITLEMENT`.

Once the script completes successfully, rerun the User Entitlement Job, which should now execute successfully.

L.183 Agent Fails To Restart Automatically in Oracle AVDF 20.9

Learn how to resolve issues when the Agent in Oracle AVDF 20.9 does not restart automatically.

Problem

In Oracle AVDF 20.9, Agent fails to start automatically.

Cause

The Agents fails to start automatically due to permission issue on `/etc/cron.allow`.

Solution

To resolve this issue, follow the steps below:

1. Switch to the root user.
2. Check the user list in `cron.allow` to see which users are allowed to access `crontab`:

   ```
   cat /etc/cron.allow
   ```

3. If the OS user who owns the Agent is not listed, modify the `cron.allow` file to add their username.

   ```
   vi /etc/cron.allow
   ```

L.184 All Activity Scheduled Reports Fail with "`Unknown Report Type`" Error

Learn how to address the issue when all scheduled activity reports fail with 'Unknown Report Type'.

Problem

All activity scheduled reports fail with 'Unknown Report Type' error message.

Cause

The directory `/usr/local/dbfw/tmp` may have run out of available space.

Solution

Ensure that sufficient space is available in the `/usr/local/dbfw/tmp` directory. Delete unnecessary files from this location and rerun the Scheduled Report.

L.185 Error Encountered While Executing the DB295ExtractionUtil Utility in Oracle AVDF 20.6

Problem

Error encountered while executing the DB295ExtractionUtil Utility for integrating the DB2 database with the Oracle AVDF 20.6 Server.

Cause

The parameter `LSLK_CMD /bin/lslocks` may not configured.

Solution

Execute the following commands for configuring `LSLK_CMD` to resolve the issue:

```
$ export LSLK_CMD=/bin/lslocks


$ echo $LSLK_CMD/bin/lslocks
```

M

Multiple Network Interface Cards

The Audit Vault Server (AVS) supports network separation through addition and initialization of additional network interfaces.

M.1 About Multiple Network Interface Cards

Oracle Audit Vault and Database Firewall enables additional network interfaces to allow some services to be accessible on networks other than the default management interface.

Oracle Audit Vault and Database Firewall supports multiple network interface cards. The Audit Vault Server console can only be used to modify secondary NICs of the Database Firewall. The `config-nic` command must be used to modify the secondary NICs for the Audit Vault Server only.

> **Note:**
>
> Oracle AVDF appliances support only 1 NIC (Network Interface Card) with an IP address per subnet. This can be a secondary NIC or a NIC used for monitoring traffic. If higher throughput or redundancy is an issue, then see Bonding of Network Interface Cards.

Perform the following steps in the Audit Vault Server console to view and manage the network interface cards for Database Firewall.

1. Log in to the Audit Vault Server console as *administrator*.
2. Click the **Database Firewalls** tab.
3. Select a specific Database Firewall instance.
4. In the main page, under the **Configuration** section, click **Network Settings** link.
5. Starting in Oracle AVDF 20.12, if the **Synchronize NICs** button is disabled, proceed to the next step. If the **Synchronize NICs** is active, click it, as the AVS detects NIC name changes in the Database Firewall which must be synchronized.
   a. Select a NIC name on the Database Firewall for all the devices. If a device is no longer available on the Database Firewall and is no longer required on the AVS, select **not required**.
   b. After mapping each device, select **Save**.
6. In the **Network Settings** dialog, click on a specific network interface card.
7. Select the specific network interface that needs to be modified. The **Network Interface Settings** dialog is displayed. It can be used to view and manage the secondary network interface cards.

> **Note:**
>
> The Database Firewall diagnostics package can be installed. After the installation, the commands executed for the Audit Vault Server can be executed on the Database Firewall.

The secondary network interfaces can be enabled and modified for the Audit Vault Server. Log in to the Audit Vault Server as *support* user and then switch user to *root*, to execute these commands.

Action	Command
To display the current status of the configured NICs on the appliance.	`/opt/avdf/config-utils/bin/config-nic show`
To display the settings of a single network interface on the Audit Vault Server.	`/opt/avdf/config-utils/bin/config-nic show device=enp0s8`
To bring a secondary NIC online. The NIC must be configured with an IP, mask, and gateway (optional and not advisable).	`/opt/avdf/config-utils/bin/config-nic set device=enp0s8 ip_address=192.0.2.9 network_mask=255.255.255.0 enabled=true`
To disable a secondary network interface.	`/opt/avdf/config-utils/bin/config-nic set device=enp0s8 enabled=false`
To delete the setting of a secondary network interface.	`/opt/avdf/config-utils/bin/config-nic delete device=enp0s8`

> **See Also:**
>
> Configure and Download the Diagnostics Report File

M.2 Enabling SSH on a Secondary Network Interface Card

Use this procedure to enable SSH on a secondary network interface card for Audit Vault Server and Database Firewall.

To enable and configure SSH on a secondary network interface card, follow these steps:

1. Execute the command `config-nic` to bring the NIC online.

2. The NIC must be configured with an IP, mask, and gateway (optional). Execute the following command:
3. The *dbfw.conf* file contains the settings of the secondary network interface card. To enable SSH, modify the settings as follows:

```
NET_SERVICE_MAP="{"enp0s8":{"ip4":
{"address":"192.0.2.9/24","gateway":"","enabled":true},"ssh":
{"port":"22","access_list":["192.0.2.1"]}}}"
```

4. The `access_list` field can be used with the following attributes:
   - `"all"`: The IP tables allow any IP address to connect through SSH.
   - `"disabled"`: The IP tables reject all incoming connections for SSH on this NIC.
   - An array of IP addresses separated by comma and a space. These IP addresses are permitted to access the SSH port on the NIC. For example: `["192.0.2.11","192.0.2.12"]`
5. Ensure a valid port number on the appliance is mentioned in the **Port** field.

M.3 Enabling Agent Connectivity on a Secondary NIC for Audit Vault Server 20.7 and Earlier

Use this procedure to enable Agent connectivity on a secondary network interface card for Audit Vault Server version 20.7 and earlier.

After a secondary NIC (network interface card) is online, you can enable it for communication between the Audit Vault Agent and the target database. This topic describes how to enable the Agent connectivity on secondary network interface cards in Oracle AVDF release 20.7 and earlier.

To enable agent connectivity on secondary network interface cards for Audit Vault Server release 20.7 and earlier:

1. Run the command `config-nic` to bring a NIC online.
2. The *dbfw.conf* file contains the settings of the secondary network interface card. To enable access to the Audit Vault Agent, modify the settings as follows:

```
NET_SERVICE_MAP="{"enp0s8":{"ip4":
{"address":"192.0.2.9/24","gateway":"","enabled":true},"agent":
{"port":"1521","tls_port":"1522","access_list":["192.0.2.1"]}}}"
```

3. The `access_list` field can be used with the following attributes:
   - `"all"`: The IP tables allow any IP address for connection to the Audit Vault Agent.
   - `"disabled"`: The IP tables reject all incoming connections for the Audit Vault Agent on this NIC.
   - An array of IP addresses separated by comma and a space. These IP addresses are permitted to access the Agent port on the NIC. For example, ["192.0.2.11","192.0.2.12"]
4. Ensure a valid port number on the appliance is mentioned in the **Port** field.

5. Run the following command to apply the Agent and enable the changes to the network configuration:

```
/usr/local/dbfw/bin/priv/configure-networking
```

> **Note:**
>
> If this command is not run, then the changes made are not applied and the Audit Vault Agent does not work on the secondary NIC.

> **See Also:**
>
> Deploying the Audit Vault Agent

M.4 Enabling Agent Connectivity on a Secondary NIC for Audit Vault Server 20.8 and Later

Use this procedure to enable Agent connectivity on a secondary network interface card for Audit Vault Server version 20.8 and later.

After a secondary NIC (network interface card) is online, you can enable it for communication between the Audit Vault Agent and the target database. This topic describes how to enable the Agent connectivity on secondary network interface cards in Oracle AVDF release 20.8 and later.

To enable agent connectivity on secondary network interface cards for Audit Vault Server release 20.8 and later:

1. Use the following command to activate the specific NIC required for the Audit Vault Agent:

```
config-nic
```

2. Run the following example command to enable device `enp0s9` in the local network:

```
/opt/avdf/config-utils/bin/config-nic set device=enp0s9
ip_address=192.0.2.24 network_mask=255.255.255.0 enabled=true
```

> **Note:**
>
> Do not add a gateway to a secondary NIC if it has already been assigned in the system configuration.

3. Use the following command to add the Audit Vault Agent configuration:

```
config-agent
```

4. Run the following example command to enable Audit Vault Agent connectivity on the specific ports using the device `enp0s9` from the Agent host machine:

```
/opt/avdf/config-utils/bin/config-agent set device=enp0s9 port=12345
tls_port=12346 access_list=all
```

> **Note:**
>
> Enable the Audit Vault Agent for high availability as per the requirement. See Enabling the Agent for High Availability Connection on a Secondary NIC for Audit Vault Server for complete information.

M.5 Enabling the Agent for High Availability Connection on a Secondary NIC for Audit Vault Server

Use this procedure to enable the Audit Vault Agent for high availability connection on a secondary network interface card for Audit Vault Server.

Prerequisite: This procedure must be performed prior to pairing the appliances (Audit Vault Server or Database Firewall) for high availability.

If the Audit Vault Agent is being run on a high availability pair of appliances, the secondary NIC must be enabled on the standby appliance (Audit Vault Server or Database Firewall). High availability involves a pair of Audit Vault Server instances or a pair of Database Firewall instances. Additional entries must also be made to the `dbfw.conf` file of both appliances.

To enable Audit Vault Agent connectivity on secondary network interfaces card for Audit Vault Server in a high availability environment:

1. Enable the Audit Vault Agent for high availability connection. Open the *dbfw.conf* file and scroll to the bottom where you will see automatically generated entries similar to the following:

```
SECONDARY_NIC_1_DEVICE         = enp0s8
SECONDARY_NIC_1_ADDRESS        = enp0s8:ip4:address:192.168.90.9
SECONDARY_NIC_1_AGENT_PORT     = enp0s8:agent:port:1521
SECONDARY_NIC_1_AGENT_PORT_TLS = enp0s8:agent:port:1522
```

> **Note:**
>
> In case these entries are not generated and are missing, refer to the previous topic on how to generate them.

2. Depending on the number of secondary NICs configured for Agent connectivity, there may be more than one block of `SECONDARY_NIC_[N]_` values. Select the block with the correct IP address and add the following field:

```
SECONDARY_NIC_1_ADDRESS_HA="<IP address>"
```

On the primary instance, this value will be the IP address of the NIC on the standby instance. And on the standby instance it is the IP address of the NIC on the primary instance.

3. Apply the Audit Vault Agent high availability configuration. Run the following command to apply the configuration, on both appliances:

```
/usr/local/dbfw/bin/priv/configure-networking
```

M.6 Bonding of Network Interface Cards

This section contains information on bonding of Database Firewall Network Interface cards.

Oracle Audit Vault and Database Firewall 20 supports bonding of Network Interface cards for Database Firewall only. This bonding functionality is used by the Database Firewall monitoring points. Bonding increases bandwidth and supports redundancy of the network connections on the appliance.

> **Note:**
>
> The Database Firewall command-line interface (CLI) creates a bond interface with the default configuration for the operating system. To configure specific bonding controls, use the operating system. See the Create Network Bonds using Network Manager CLI documentation or Configuring Network Bonding in the Oracle Linux 8 documentation for details on creating network bonds in Oracle Linux.

Run the following command to check for bonding between network interface cards:

```
/opt/avdf/config-utils/bin/config-bond
```

The command output displays information about the composite device.

Run the following command to bond multiple network interface cards and give the composite device an IP address:

```
/opt/avdf/config-utils/bin/config-bond add device=bond0
components=enp0s18,enp0s19 ip4addr=192.0.2.10 ip4mask=255.255.255.0
ip4gateway=192.0.2.1 state=true
```

Run the following command to bond multiple network interface cards without an IP address (for use in out-of-band mode):

```
/opt/avdf/config-utils/bin/config-bond add device=bond0
components=enp0s18,enp0s19
      state=true
```

Upon establishing the bonding, the following confirmation message is displayed:

```
config-bond add ...
```

Run the following command to delete a bonded device:

```
/opt/avdf/config-utils/bin/config-bond delete device=bond0
```

The following confirmation message is displayed:

```
config-bond delete ...
```

Run the following command to remove the existing bonding between network interfaces:

```
/opt/avdf/config-utils/bin/config-bond delete device=bond0
```

The following is the output:

```
Notice: Settings deleted.
:device: bond0
:components:
- enp0s9
- enp0s8
:description:
:ip_address: 192.0.2.20
:network_mask: 255.255.255.0
:gateway: ''
:enabled: true
```

Note:

- Run the following command to seek help for the bonding of network interfaces:

  ```
  /opt/avdf/config-utils/bin/config-bond help
  ```

- It is not possible to create bonding of two network interface cards using the interfaces on which the monitoring point already exists. In this case disable the existing monitoring point, create bonding between the network interface cards, and then use the newly created bond name to configure the monitoring point.

M.7 Configuring Routing on Secondary Network Interface Cards

Learn how to configure routing on secondary network interface cards in Oracle AVDF.
The following table contains the necessary information to view and set routing for the secondary network interface cards on Audit Vault Server and Database Firewall. Log in to the terminal as *root* user to run the commands listed in the table.

Task	Command	Output

To view the existing routing configuration on the network interface card.	`/opt/avdf/config-utils/bin/config-route`	`device: enp0s3`
		`gateway: " "`
		`routes: []`

To set the gateway. **Note:** A gateway must be assigned to only one device. However, it is possible to assign a gateway to multiple devices. It introduces system instability. In most cases the gateway must be assigned to only the default management interface device that is configured during installation.	`/opt/avdf/config-utils/bin/config-route set device=enp0s3 gateway=<gateway address>`	`Notice: Success. Settings saved.`

To set a custom static route.	`/opt/avdf/config-utils/bin/config-route set device=enp0s3 routes='<IP address of the network interface card followed by the gateway address separated by space>'`
	
	For example:
	
	`/opt/avdf/config-utils/bin/config-route set device=enp0s3 routes='192.0.2.1 192.0.2.4'`
		`Notice: Success. Settings saved.`

Task	Command	Output
To set multiple route at the same time. **Note:** Although the routes are assigned to a single device, the routing table applies to all devices.	/opt/avdf/config-utils/bin/config-route set device=enp0s3 routes='<IP address of the network interface card and gateway address separated by comma and space>' For example: /opt/avdf/config-utils/bin/config-route set device=enp0s3 routes='192.0.2.1 192.0.2.4, 192.0.2.11 192.0.2.5, 192.0.2.21 192.0.2.6,'	- :device: enp0s3 :gateway: " " :routes: - 192.0.2.1 192.0.2.4 - 192.0.2.11 192.0.2.5 - 192.0.2.21 192.0.2.6
To add a single static route.	/opt/avdf/config-utils/bin/config-route add device=enp0s3 routes='<IP address of the network interface card followed by the gateway address separated by space>' For example: /opt/avdf/config-utils/bin/config-route add device=enp0s3 routes='192.0.2.1 192.0.2.4'	Notice: Success. Settings saved. --- :device: enp0s3 :gateway: " " :routes: - 192.0.2.1 192.0.2.4 - 192.0.2.11 192.0.2.5 - 192.0.2.21 192.0.2.6 - 192.0.2.22 192.0.2.16

Task	Command	Output

To delete a single static route.	`/opt/avdf/config-utils/bin/config-route delete device=enp0s3 routes='<IP address of the network interface card followed by the gateway address separated by space>'`
	
	For example:
	
	`/opt/avdf/config-utils/bin/config-route delete device=enp0s3 routes=192.0.2.1 192.0.2.4`
		`Notice: Settings deleted.`
		`---`
		`:device: enp0s3`
		`:gateway: ''`
		`:routes:`
		`- 192.0.2.1 192.0.2.4`

To delete all static routes.	`/opt/avdf/config-utils/bin/config-route set device=enp0s3 routes=""`	`Notice: Success. Settings saved.`

M.8 Changing a New or Secondary NIC to the Management NIC

You can change a new or secondary network interface card (NIC) to the management NIC.

The management NIC is usually the main NIC of the appliance (Audit Vault Server or Database Firewall). It is attached to the default gateway.

1. Log in to the Audit Vault Server or Database Firewall as an *administrator*.
2. Make sure that the new or secondary NIC is plugged in.
3. Enable SSH on the new or secondary NIC.
4. Change to the `/usr/local/dbfw/etc` folder and open the `dbfw.conf` file, which contains the NIC settings.
5. Edit the value of `DEFAULT_DEVICE` in the `dbfw.conf` file.

   By default, `DEFAULT_DEVICE` is set to `eth0`. Change this value and specify the name of the new or secondary NIC.
6. Run the following command to complete the configuration script:

   ```
   /usr/local/dbfw/bin/priv/configure-networking
   ```

> **Note:**
>
> Alternately, you can change the NIC by turning off the appliance (Audit Vault Server or Database Firewall). Then replace the `eth0` device with the new one in the same slot. The new device is replaced with the new one when the server is restarted.

N

Configuring Quick JSON Target Type to Collect Audit Data from MongoDB

Learn how to collect MongoDB audit data using Oracle AVDF's Quick JSON target type.

MongoDB audit data is available in multiple formats like `BSON`, `JSON`, or `Syslog`. Oracle AVDF supports audit data collection from Enterprise Edition in `JSON` format only.

To register MongoDB as a target, select the target type as `Quick JSON`. Later provide the required collection attributes for the fields in the MongoDB audit trail, as mentioned in the table below. Quick JSON uses this mapping to read the MongoDB audit file and map it to the fields in the Audit Vault Server.

Additionally, when adding audit trail for the MongoDB target, provide the location of MongoDB audit files. Ensure the Audit Vault Agent user can access MongoDB JSON audit file. If required grant read permissions to the file.

Use Quick JSON target type for reading from JSON audit files without any conversion of data. For situations where the JSON data needs to be converted before it is stored in the Audit Vault Server, use the JSON custom collector.

Table N-1 Collection attributes and values required for audit collection from MongoDB audit file

Audit Vault Collection Attribute	MongoDB JSON File Value
av.collector.qck.starttag	atype
av.collector.qck.eventtime	$.ts.$date
av.collector.qck.username	$.users[0].user
av.collector.qck.os.username	$.users[0].user
av.collector.qck.eventname	$.atype
av.collector.qck.commandclass	$.atype
av.collector.qck.client.ip	$.remote.ip
av.collector.qck.targetobject	$.atype
av.collector.qck.targettype	$.atype
av.collector.qck.eventstatus	$.result
av.collector.qck.errorid	$.result
av.collector.qck.errormessage	$.result
av.collector.qck.target.entity	$.param.ns
av.collector.qck.target.user	$.param.user
av.collector.qck.target.role	$.param.role

Note:

Delete the attribute `av.collector.timezoneoffset` during QuickJSON target creation in Oracle AVDF 20.4 and later. This attribute is not required for collecting audit data from MongoDB.

See Also:

- Quick JSON Target Type for Oracle Audit Vault and Database Firewall
- Registering Targets

O

Audit Vault Agent Auto Start Configuration

Learn how to configure Audit Vault Agent to restart automatically when the host machine is restarted.

Audit Vault Agent is installed on a host machine. The Audit Vault Agent is not restarted automatically when the host machine is restarted. The Audit Vault Agent can be configured to restart automatically, whenever the host machine is restarted. The configuration is different for the type of operating system installed on the host machine. This appendix contains the required information.

> **Note:**
>
> - This functionality involves configuring a service to restart the Agent and is available in Oracle AVDF releases 20.3 to 20.6.
> - Starting with Oracle AVDF release 20.7, a new Agent auto start functionality is introduced. This functionality constantly monitors the Agent and also restarts the Agent if it stops unexpectedly. See Configuring Agent Auto Restart Functionality for complete information.

O.1 Configuring Agent Auto Start on Host Machine With OL7 and OL8

Learn to configure Audit Vault Agent auto start functionality on a host machine with OL7 and OL8.

1. Install the Audit Vault Agent and activate using the activation key.
2. Run the following command to manually start the Audit Vault Agent as *agent* user:

   ```
   <AgentHome>/bin/agentctl start
   ```

3. Create a file `/etc/systemd/system/multi-user.target.wants/agentctl.service` as *root* user. Use the sample script provided below. In this sample script replace the `<AgentUser>` and `<AgentHome>` with relevant Agent user name and Agent home directory.

   ```
   [Unit]

   Description=AgentController Service

   After=network.target

   After=syslog.target
   ```

```
[Install]

WantedBy=multi-user.target


[Service]

User=<Agent User>

Type=forking


# Start main service

ExecStart=<AgentHome>/bin/agentctl start


#Stop main service

ExecStop=<AgentHome>/bin/agentctl stop


RemainAfterExit=yes
```

4. Run the following command to enable the service from the directory `/etc/systemd/system/multi-user.target.wants/` as *root* user:

   ```
   systemctl enable agentctl.service
   ```

   > **Note:**
   >
   > This command may throw the following error message. Ignore this message.
   >
   > `Failed to execute operation: Invalid argument`

5. Run the following command as *agent* user to stop the Agent process:

   ```
   <AgentHome>/bin/agentctl stop
   ```

6. Run the following command as *agent* user to restart using `systemctl`:

   ```
   systemctl start agentctl.service
   ```

7. To verify successful configuration of Agent auto start functionality, follow these steps:
   a. Reboot the system.
   b. After the system is up, check the status by running the following command:

      ```
      systemctl status agentctl.service
      ```

   c. Verify the status is `STARTED`.

> **Note:**
>
> Ensure the Agent is started or stopped only using the `systemctl` command. Using the `agentctl` command leads to inconsistencies and must be avoided.

O.2 Configuring Agent Auto Start on Host Machine With OL6

Learn to configure Audit Vault Agent auto start functionality on a host machine with OL6.

1. Install the Audit Vault Agent and activate using the activation key.
2. Create the script as *root* user in the location `/etc/init.d/agentAVDF`. Use the sample script provided below. In this sample script set the `USER` and `AGENT_HOME` with appropriate Agent user and Agent home path.
3. In the script update the `chkconfig` parameter with start priority and stop priority. The parameters `<start priority>` and `<stop priority>` decide the order in which file is executed, in comparison with the rest of files that exist in the location `./etc/init.d` during machine start and shutdown respectively. Smaller priority numbers are executed first. For example, `# chkconfig: 2345 99 95`

```
# chkconfig: 2345 <start priority> <stop priority>

PROGRAM="agentAVDF"

USER=<AgentUser>

AGENT_HOME=<AgentHomeDirectory>


start() {

    su - ${USER} -c "/bin/bash -c '${AGENT_HOME}/bin/agentctl start'"

}


stop() {

    su - ${USER} -c "/bin/bash -c '${AGENT_HOME}/bin/agentctl stop'"

}


case "$1" in

    start)

        start

        ;;
```

```
    stop)
        stop
        ;;

    *)
        echo $"Usage: $0 {start|stop}"
        exit 1
esac
```

4. Run the following command to provide execute permission to the script:

   ```
   chmod +x /etc/init.d/agentAVDF
   ```

5. Run the following command to enable the service:

   ```
   /sbin/chkconfig agentAVDF on
   ```

6. To verify successful configuration of Agent auto start functionality, follow these steps:
   a. Reboot the system.
   b. After the system is up, wait for few minutes and then run the following command:

      ```
      <AgentHome>/bin/agentctl status
      ```

   c. Verify the status is `RUNNING`.

O.3 Configuring Agent Auto Start on Host Machine With Windows x64

Learn to configure Audit Vault Agent auto start functionality on a host machine with Windows x64.

1. Register the Audit Vault Agent as a Windows service, for Windows x64.
2. The Windows Agent service is automatically started when the Windows host machine is restarted.

O.4 Configuring Agent Auto Start on Host Machine With Solaris [SPARC/x64]

Learn to configure Audit Vault Agent auto start functionality on a host machine with Solaris [SPARC/x64].

1. Install the Audit Vault Agent and activate using the activation key.

2. Create the file `/lib/svc/method/agentAVDF` as *root* user. Use the sample script provided below. In this sample script set the `AGENT_USER` and `AGENT_HOME` with appropriate Agent user and Agent home path.

```
#!/bin/sh

################################################
# name: agentAVDF
# purpose: script that will start or stop the AVDF agent daemon.
################################################

case "$1" in
start )
su - <AGENT_USER> -c "/bin/bash -c '<AGENT_HOME>/bin/agentctl start'"
;;
stop )
su - <AGENT_USER> -c "/bin/bash -c '<AGENT_HOME>/bin/agentctl stop'"
;;
* )
echo "Usage: <AGENT_HOME>/bin/agentctl (start | stop)"
exit 1
esac
```

3. Run the following command to provide execute permission to the script:

```
chmod +x /lib/svc/method/agentAVDF
```

4. Create a manifest file `/tmp/agentAVDF.xml` as *root* user, using the below sample manifest file.

```
<?xml version="1.0" ?>
<!DOCTYPE service_bundle
SYSTEM '/usr/share/lib/xml/dtd/service_bundle.dtd.1'>
<service_bundle name="startstopAgent" type="manifest">
<service name="startstopAgent" version="1" type="service">
<dependency name="multi_user_dependency" grouping="require_all"
restart_on="none" type="service">
<service_fmri value="svc:/milestone/multi-user"/>
</dependency>
<exec_method name="start" type="method" timeout_seconds="300"
exec="/lib/svc/method/agentAVDF start"/>
<exec_method name="stop" type="method" timeout_seconds="300"
exec="/lib/svc/method/agentAVDF stop"/>
<!--
The exec attribute below can be changed to a command that SMF
should execute when the service is refreshed. Use svcbundle -s
refresh-method to set the attribute.
-->
<exec_method name="refresh" type="method" timeout_seconds="60"
exec=":true"/>
<!--
A duration property group is not needed.
-->
```

```
<instance name="default" enabled="true"/>
<template>
<common_name>
<loctext xml:lang="start/stop AVDF agent">
startstopAgent
</loctext>
</common_name>
<description>
<loctext xml:lang="The service can start and stop AVDF Agent by agentctl">
The startstopAgent service.
</loctext>
</description>
</template>
</service>
</service_bundle>
```

5. Run the following command as *root* user, to validate the manifest file:

   ```
   /usr/sbin/svccfg validate /tmp/agentAVDF.xml
   ```

6. Run the following command as *root* user, to copy the manifest file to the location `/lib/svc/manifest/site/`:

   ```
   cp /tmp/agentAVDF.xml /lib/svc/manifest/site/
   ```

7. Run the following command as *root* user, to import the manifest file and start the service:

   ```
   /usr/sbin/svcadm restart manifest-import
   ```

8. Run the following command as *root* user, to check the status of the service. The status of the service must be `maintenance` or `online`. If the status is `offline`, then run the below command again after few minutes:

   ```
   svcs | grep startstopAgent
   ```

9. To verify successful configuration of Agent auto start functionality, follow these steps:
   a. Reboot the system.
   b. After the system is up, wait for few minutes and then run the following command as *root* user:

      ```
      # svcs | grep startstopAgent
      ```

      The status of the service must be `online`.

O.5 Configuring Agent Auto Start on Host Machine With IBM AIX

Learn to configure Audit Vault Agent auto start functionality on the host machine with IBM AIX.

1. Install the Audit Vault Agent and activate using the activation key.
2. Create the script as *root* user in the location `/etc/rc.d/init.d/agentAVDF`. Use the sample script provided below. In this sample script set the `AGENT_USER`, `JAVA_HOME`, and

AGENT_HOME with appropriate Agent user, Java home path, and Agent home path respectively.

```
#!/bin/bash

################################################
# Agent start/stop script
################################################


case "$1" in
start )
su - <AGENT_USER> -c "/bin/bash -c 'PATH=<JAVA_HOME>/bin:$PATH;
<AGENT_HOME>/bin/agentctl start;'"
;;
stop )
su - <AGENT_USER> -c "/bin/bash -c 'PATH=<JAVA_HOME>/bin:$PATH;
<AGENT_HOME>/bin/agentctl stop;'"
;;
* )
echo "Usage: <AGENT_HOME>/bin/agentctl (start | stop)"
exit 1
esac
```

3. Run the following command as *root* user to provide execute permission to the script:

```
chmod +x /etc/rc.d/init.d/agentAVDF
```

4. Create symlink S<script name> and K<script name> under the directory /etc/rc.d/rc2.d/. The symlink S file and symlink K is used to start and end the Agent during machine start and shutdown respectively. Create symlinks by running the below commands as *root* user. The parameter <priority_number> decides the order in which the file runs in comparison with the rest of the files that exist in the directory ./etc/rc.d/rc2.d. Smaller priority numbers are run first.

```
ln -s /etc/rc.d/init.d/agentAVDF /etc/rc.d/rc2.d/
S<priority_number>agentAVDF


ln -s /etc/rc.d/init.d/agentAVDF /etc/rc.d/rc2.d/
K<priority_number>agentAVDF
```

For example:

```
ln -s /etc/rc.d/init.d/agentAVDF /etc/rc.d/rc2.d/S99999agentAVDF


ln -s /etc/rc.d/init.d/agentAVDF /etc/rc.d/rc2.d/K99999agentAVDF
```

5. To verify successful configuration of Agent auto start functionality, follow these steps:
   a. Reboot the Agent machine.

b. After the machine is up, wait for few minutes, and then run the following command as *agent* user:

```
<AgentHome>/bin/agentctl status
```

c. Ensure the status is `RUNNING`.

P

Adding User Content To System Configuration Files

Use this procedure to add user specified content to AVDF template files. AVDF allows specific content to persist on the appliance through various procedures such as upgrade and regular system configuration. This is handled by the user interface of the appliance.

Every template configuration file on the appliance allows to add user defined content. An additional file is available that contains such content. Within this file an additional output data file must be added. Any user defined content is added to the end of the final output file.

> **Note:**
>
> Not all template files are written regularly. In some cases files are only updated on upgrade, while some are updated frequently like networking configuration.

To create and include a file for a template generated content follow this procedure:

1. Create a *root-owned* directory where all the files can be stored.

   > **Note:**
   >
   > The directory must be owned by *root* user and must have *write* access.

   The following commands can be executed to create the directory named *include*:

   ```
   mkdir /usr/local/dbfw/templates/include
   ```

   ```
   chown root:root /usr/local/dbfw/templates/include
   ```

   ```
   chmod 755 /usr/local/dbfw/templates/include
   ```

2. Create a new directory to have data automatically inserted into the output of a template file. The name of this new directory can be prefixed with *after-*.
3. The list of files that have user data appended are stored at `/usr/local/dbfw/templates`
4. To add further host names to `/etc/hosts`, add the file named *after-template-hosts* to the directory `/usr/local/dbfw/templates/include`.

   > **Note:**
   >
   > The file *after-template-hosts* must be *read-only* and owned by *root*. It may be world readable also.

5. Execute the following commands to set the required permission after creating the *after-template-hosts* file:

```
touch /usr/local/dbfw/templates/include/after-template-hosts

chmod 444 /usr/local/dbfw/templates/include/after-template-hosts

chown root:root /usr/local/dbfw/templates/include/after-template-hosts
```

6. Modify the file to include new user data. This is used when the template file and the data is appended to the generated file. The newly appended data is found in the end of the generated file.
7. In most cases it is necessary to restart or re-initialize the affected component before the changes are completely applied. Refer to the Oracle Linux documentation for more information about the components and files modified.