

Oracle® Audit Vault and Database Firewall

Administrator's Guide



Release 12.2
E41705-35
June 2022

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Audit Vault and Database Firewall Administrator's Guide, Release 12.2

E41705-35

Copyright © 2012, 2022, Oracle and/or its affiliates.

Primary Authors: Karthik Shetty, Gigi Hanna

Contributing Authors: Siddharth Naidu

Contributors: Andrey Brozhko, Marek Dulko, Nithin Gomez, Paul Hackett, William Howard-Jones, Slawek Kilanowski, Shirley Kumamoto, Ravi Kumar, Paul Laws, Sreedhar Madiraju, Vijay Medi, Sidharth Mishra, Sarma Namuduri, Eric Paapanen, Abdulhusain Rahi, Mahesh Rao, Vipin Samar, Gian Sartar, Lok Sheung, Yan Shi, Rajesh Tammana, Tom Taylor, Graham Thwaites

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	xxv
Documentation Accessibility	xxv
Diversity and Inclusion	xxv
Related Documents	xxv
Conventions	xxvi

What's New

Oracle AVDF Release 12.2.0 Changes	xxvii
Changes In This Document	xxviii

Quick Reference for Common Tasks

About this Quick Reference	xlii
Audit Vault Server	xlii
Database Firewall	xlili
Hosts	xliv
Agent	xliv
Host Monitor	xliv
Secured Targets	xliv
BIG-IP ASM Integration	xlvi
Arcsight Integration	xlvii
Other Administrator Tasks	xlvii
Reference Information	xlvii

Part I Getting Started

1 Introducing Oracle Audit Vault and Database Firewall

1.1 Downloading the Latest Version of This Manual	1-1
1.2 Learning About Oracle AVDF	1-1

1.3	Supported Platforms for Oracle Audit Vault and Database Firewall	1-1
1.4	System Features	1-2
1.4.1	About Audit Vault and Database Firewall	1-2
1.4.2	Security Technical Implementation Guides and Implementation for Oracle Audit Vault and Database Firewall	1-2
1.4.3	System Requirements for Oracle Audit Vault and Database Firewall	1-3
1.4.4	Supported Secured Targets	1-3
1.4.5	Administrative Features	1-3
1.4.6	Oracle Audit Vault and Database Firewall Auditing Features	1-4
1.4.7	Integrating Oracle Audit Vault and Database Firewall with Third-Party Products	1-4
1.4.8	Integrating Oracle Audit Vault and Database Firewall with Oracle Key Vault	1-5
1.5	Understanding the Administrator's Role	1-5
1.6	Summary of Configuration Steps	1-6
1.6.1	Configuring Oracle AVDF and Deploying the Audit Vault Agent	1-6
1.6.2	Configuring Oracle AVDF and Deploying the Database Firewall	1-7
1.7	Planning the System Configuration	1-7
1.7.1	Guidance for Planning Your Oracle Audit Vault and Database Firewall Configuration	1-7
1.7.2	Step 1: Plan Your Oracle Audit Vault Server Configuration	1-8
1.7.3	Step 2: Plan the Database Firewall Configuration	1-8
1.7.4	Step 3: Plan the Audit Vault Agent Deployments	1-8
1.7.5	Step 4: Plan the Audit Trail Configurations	1-9
1.7.6	Step 5: Plan Your Integration Options	1-9
1.7.7	Step 6: Plan for High Availability	1-10
1.7.8	Step 7: Plan User Accounts and Access Rights	1-10
1.8	Logging in to the Audit Vault Server Console UI	1-11
1.8.1	Log in to Oracle Audit Vault Server Console	1-11
1.8.2	Understanding the Tabs and Menus in the Audit Vault Server Console	1-11
1.8.3	Working with Lists of Objects in the UI	1-12
1.9	Logging in to the Database Firewall Console UI	1-13
1.9.1	Log in to the Database Firewall Console UI	1-14
1.9.2	Using the Oracle Database Firewall UI	1-15
1.10	Using the Audit Vault Command-Line Interface	1-15
1.11	Using the Audit Vault and Database Firewall Enterprise Manager Plug-in	1-16

2 General Security Guidelines

2.1	Installing Securely and Protecting Your Data	2-1
2.1.1	Installing Oracle Audit Vault and Database Firewall Securely	2-1
2.1.2	Protecting Your Data	2-1
2.2	General Security Recommendations	2-2
2.3	External Network Dependencies	2-2

2.4	Considerations for Deploying Network-Based Solutions	2-3
2.4.1	Managing Database Firewall Network Encryption	2-3
2.4.2	Handling Server-Side SQL and Context Configurations	2-3
2.5	How Oracle AVDF Works with Various Database Access Paths	2-4
2.6	Security Considerations for Special Configurations	2-4
2.6.1	Database Firewall Configuration for Oracle Database Target Configured in Shared Server Mode	2-4
2.6.2	How TCP Invited Nodes Are Affected by Client IP Addresses	2-5
2.6.3	Additional Behavior to be Aware Of	2-5
2.6.4	Custom Collector Development	2-6
2.7	About Setting Transport Layer Security Levels	2-6
2.8	Certificates	2-12
2.8.1	Renew Audit Vault Server Certificate	2-12
2.8.2	Renew Database Firewall Certificate	2-16

3 Configuring the Audit Vault Server

3.1	About Configuring Oracle Audit Vault Server	3-1
3.2	Changing the UI (Console) Certificate for Oracle Audit Vault Server	3-2
3.3	Specifying Initial System Settings and Options (Required)	3-3
3.3.1	Specifying the Server Date, Time, and Keyboard Settings	3-3
3.3.2	Specifying the Audit Vault Server System Settings	3-5
3.3.2.1	Setting or Changing the Audit Vault Server Network Configuration	3-5
3.3.2.2	Configuring or Changing the Oracle Audit Vault Server Services	3-7
3.3.2.3	Changing IP Address Of An Active And Registered Host	3-8
3.3.3	Configuring Oracle Audit Vault Server Syslog Destinations	3-8
3.4	Configuring the Email Notification Service	3-10
3.4.1	About Email Notifications in Oracle Audit Vault and Database Firewall	3-10
3.4.2	Configuring Email Notification for Oracle Audit Vault and Database Firewall	3-11
3.5	Configuring Archive Locations and Retention Policies	3-11
3.5.1	About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall	3-12
3.5.2	Defining Archive Locations	3-13
3.5.3	Creating or Deleting Archiving Policies	3-17
3.5.3.1	Creating Archiving (Retention) Policies	3-17
3.5.3.2	Deleting Archiving Policies	3-18
3.5.4	Running Archive or Retrieve Jobs	3-18
3.6	Managing Archival and Retrieval in High Availability Environments	3-18
3.7	Defining Resilient Pairs for High Availability	3-20
3.8	Registering Database Firewall in Audit Vault Server	3-20
3.9	Testing Audit Vault Server System Operations	3-21
3.10	Configuring Fiber Channel-Based Storage for Audit Vault Server	3-21

3.11	Adding Network Address Translation IP Addresses to Audit Vault Agent	3-23
------	--	------

4 Configuring the Database Firewall

4.1	About Configuring the Database Firewall	4-1
4.2	Changing the UI (Console) Certificate for the Database Firewall	4-2
4.3	Managing the Database Firewall's Network and Services Configuration	4-3
4.3.1	Configuring Network Settings For A Database Firewall	4-3
4.3.2	Configuring Network Services For A Database Firewall	4-4
4.4	Setting the Date and Time in the Database Firewall	4-5
4.5	Specifying the Audit Vault Server Certificate and IP Address	4-6
4.6	Changing IP Address For A Single Instance Of Database Firewall Server	4-7
4.7	Configuring Database Firewall and its Traffic Sources on Your Network	4-8
4.7.1	About Configuring The Database Firewall And Traffic Sources On Your Network	4-8
4.7.2	Configuring Traffic Sources	4-9
4.7.3	Configuring a Bridge in the Database Firewall	4-9
4.7.4	Configuring Oracle Database Firewall As A Traffic Proxy	4-11
4.8	Configuring an Interface Masters Niagara Server Adapter Card	4-12
4.9	Viewing the Status and Diagnostics Report for a Database Firewall	4-12
4.10	Configure and Download the Diagnostics Report File	4-13

5 Registering Hosts and Deploying the Agent

5.1	Registering Hosts in the Audit Vault Server	5-1
5.1.1	About Registering Hosts	5-1
5.1.2	Registering Hosts in the Audit Vault Server	5-2
5.1.3	Changing Host Names	5-3
5.2	Deploying and Activating the Audit Vault Agent on Host Computers	5-3
5.2.1	About Deploying the Audit Vault Agent	5-3
5.2.2	Steps Required to Deploy and Activate the Audit Vault Agent	5-5
5.2.3	Registering the Host	5-5
5.2.4	Deploying the Audit Vault Agent on the Host Computer	5-5
5.2.5	Activating and Starting the Audit Vault Agent	5-6
5.2.6	Registering and Unregistering the Audit Vault Agent as a Windows Service	5-7
5.2.6.1	About the Audit Vault Agent Windows Service	5-7
5.2.6.2	Registering the Audit Vault Agent as a Windows Service	5-7
5.2.6.3	Unregistering the Audit Vault Agent as a Windows Service	5-8
5.3	Stopping, Starting, and Other Agent Operations	5-9
5.3.1	Stopping and Starting Oracle Audit Vault Agent	5-9
5.3.1.1	Stopping and Starting the Agent on Unix Hosts	5-9
5.3.1.2	Stopping and Starting the Agent on Windows Hosts	5-9

5.3.1.3	Autostarting the Agent on Windows Hosts	5-10
5.3.2	Changing the Logging Level for the Audit Vault Agent	5-11
5.3.3	Viewing the Status and Details of an Audit Vault Agent	5-11
5.3.4	Deactivating and Removing the Audit Vault Agent	5-12
5.4	Updating Oracle Audit Vault Agent	5-12
5.5	Deploying Plug-ins and Registering Plug-in Hosts	5-13
5.5.1	About Plug-ins	5-13
5.5.2	Ensuring that Auditing is Enabled in the Secured Target	5-14
5.5.3	Registering the Plug-in Host in Audit Vault Server	5-14
5.5.4	Deploying and Activating the Plug-in	5-14
5.5.5	Un-Deploying Plug-ins	5-15
5.6	Deleting Hosts from the Audit Vault Server	5-16

6 Configuring Secured Targets, Audit Trails, and Enforcement Points

6.1	About Configuring Secured Targets	6-1
6.2	Registering Secured Targets and Creating Groups	6-2
6.2.1	Registering or Removing Secured Targets in the Audit Vault Server	6-2
6.2.1.1	About Secured Targets in the Audit Vault Server	6-2
6.2.1.2	Registering Secured Targets	6-3
6.2.1.3	Modifying Secured Targets	6-5
6.2.1.4	Removing Secured Targets	6-5
6.2.2	Creating or Modifying Secured Target Groups	6-6
6.2.3	Controlling Access to Secured Targets and Target Groups	6-7
6.3	Preparing Secured Targets for Audit Data Collection	6-7
6.3.1	Using an NTP Service to set Time on Secured Targets	6-7
6.3.2	Ensuring that Auditing is Enabled on the Secured Target	6-8
6.3.3	Setting User Account Privileges on Secured Targets	6-8
6.3.4	Scheduling Audit Trail Cleanup	6-9
6.4	Configuring and Managing Audit Trail Collection	6-9
6.4.1	Adding an Audit Trail in the Audit Vault Server	6-9
6.4.2	Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server	6-11
6.4.3	Checking the Status of Audit Trails in the Audit Vault Server	6-12
6.4.4	Handling new Audit Trails with Expired Audit Records	6-13
6.4.5	Deleting an Audit Trail	6-14
6.4.6	Converting Audit Record Format For Collection	6-14
6.4.7	Configuring Audit Trail Collection for Oracle Real Application Clusters	6-18
6.4.8	Configuring Audit Trail Collection For CDB And PDB	6-19
6.5	Configuring Enforcement Points	6-20
6.5.1	About Configuring Enforcement Points for Secured Targets	6-20
6.5.2	Creating and Configuring an Enforcement Point	6-20

6.5.3	Modifying an Enforcement Point	6-22
6.5.4	Starting, Stopping, or Deleting Enforcement Points	6-23
6.5.5	Viewing the Status of Enforcement Points	6-23
6.5.6	Finding the Port Number Used by an Enforcement Point	6-24
6.6	Configuring Stored Procedure Auditing (SPA)	6-24
6.7	Configuring and Using Database Interrogation	6-24
6.7.1	About Database Interrogation	6-25
6.7.1.1	Using Database Interrogation for SQL Server and SQL Anywhere Databases	6-25
6.7.1.2	Using Database Interrogation for Oracle Databases with Network Encryption	6-25
6.7.2	Configuring Database Interrogation for SQL Server and SQL Anywhere	6-26
6.7.2.1	Setting Database Interrogation Permissions in a Microsoft SQL Server Database	6-26
6.7.2.2	Setting Database Interrogation Permissions in a Sybase SQL Anywhere Database	6-26
6.7.3	Enabling Database Interrogation	6-27
6.7.4	Disabling Database Interrogation	6-28
6.8	Configuring Oracle Database Firewall for Databases That Use Network Encryption	6-29
6.8.1	Step 1: Apply the Specified Patch to Oracle Database	6-29
6.8.2	Step 2: Run the Oracle Advance Security Integration Script	6-29
6.8.3	Step 3: Provide the Database Firewall Public Key to the Oracle Database	6-31
6.8.4	Step 4: Enable Database Interrogation for the Oracle Database	6-32
6.9	Configuring and Using Database Response Monitoring	6-32
6.9.1	About Database Response Monitoring	6-32
6.9.2	Configuring Database Response Monitoring	6-33
6.9.2.1	Enabling Database Response Monitoring	6-33
6.9.2.2	Setting Up Log-in and Log-out Policies in Oracle Database Firewall	6-34
6.10	Securing the Agent and Oracle Database Secure Target Connection	6-34

7 Enabling and Using Host Monitoring

7.1	About Host Monitoring	7-1
7.2	Installing and Enabling Host Monitoring	7-2
7.2.1	Host Monitor Requirements	7-2
7.2.2	Register the Computer that will Run the Host Monitor	7-3
7.2.3	Deploying the Agent and Host Monitor on Microsoft Windows Hosts	7-3
7.2.4	Deploying the Agent and Host Monitor on Unix Hosts	7-6
7.2.5	Create a Secured Target for the Host-Monitored Database	7-7
7.2.6	Create an Enforcement Point for the Host Monitor	7-7
7.2.7	Create a Network Audit Trail	7-7
7.3	Starting, Stopping, and Other Host Monitor Operations	7-9

7.3.1	Starting the Host Monitor	7-9
7.3.2	Stopping the Host Monitor	7-9
7.3.3	Changing the Logging Level for a Host Monitor	7-10
7.3.4	Viewing Host Monitor Status and Details	7-10
7.3.5	Checking the Status of a Host Monitor Audit Trail	7-10
7.3.6	Uninstalling the Host Monitor (Unix Hosts Only)	7-10
7.4	Updating the Host Monitor (Unix Hosts Only)	7-11
7.5	Using Certificate-based Authentication for the Host Monitor	7-11
7.5.1	Requiring a Signed Certificate for Host Monitor Connections to the Firewall	7-11
7.5.2	Getting a Signed Certificate from the Audit Vault Server	7-12

8 Configuring High Availability

8.1	About High Availability Configurations in Oracle Audit Vault and Database Firewall	8-1
8.2	Managing A Resilient Audit Vault Server Pair	8-2
8.2.1	About Pairing Audit Vault Servers	8-3
8.2.2	Prerequisites for Configuring a Resilient Pair of Audit Vault Servers	8-3
8.2.3	Configure the Secondary Audit Vault Server	8-4
8.2.4	Configure the Primary Audit Vault Server	8-5
8.2.5	Checking the High Availability Status of an Audit Vault Server	8-6
8.2.6	Updating Audit Vault Agents and Host Monitor Agents After Pairing Audit Vault Servers	8-6
8.2.7	Swapping Roles Between a Primary and Standby Audit Vault Server	8-7
8.2.8	Handling a Failover of the Audit Vault Server Pair	8-8
8.2.9	Disabling or Enabling Failover of the Audit Vault Server	8-9
8.2.10	Performing a Manual Failover of the Audit Vault Server	8-9
8.3	Managing A Resilient Database Firewall Pair	8-9
8.3.1	About Managing A Resilient Database Firewall Pair	8-9
8.3.2	Configuring A Resilient Database Firewall Pair	8-10
8.3.3	Switching Roles in a Resilient Pair of Database Firewalls	8-10
8.3.4	Breaking (Un-pairing) a Resilient Pair of Database Firewalls	8-11
8.4	High Availability For Database Firewall In Proxy Mode	8-12
8.4.1	Configuring High Availability For Database Firewall In Proxy Mode Through Client Configuration	8-12
8.4.2	Configuring High Availability For Database Firewall In Proxy Mode Through DNS Setup	8-14

9 Configuring Integration with BIG-IP ASM

9.1	System Requirements	9-1
9.2	About the Integration of Oracle Audit Vault and Database Firewall with F5 BIG-IP Application Security Manager (BIG-IP ASM)	9-1

9.3	How the Integration Works	9-3
9.4	Deploying the Oracle AVDF and F5 BIG-IP Application Security Manager Integration	9-4
9.4.1	About the Deployment	9-4
9.4.2	Configuring Oracle Audit Vault and Database Firewall to Work with F5 BIG-IP Application Security Manager	9-4
9.4.3	Configuring F5 BIG-IP Application Security Manager	9-5
9.4.3.1	Logging Profile	9-6
9.4.3.2	Policy Settings	9-7
9.4.4	Developing a F5 BIG-IP Application Security Manager iRule	9-7
9.4.4.1	Required Syslog Message Format	9-9
9.4.4.2	Configuring syslog-ng.conf	9-10
9.5	Viewing F5 Data in Oracle Audit Vault and Database Firewall Reports	9-10

10 Integration with Third Party SIEM and Log-data Analysis Tools

10.1	How Oracle Audit Vault and Database Firewall Integrates with HP ArcSight SIEM	10-2
10.2	Enabling the HP ArcSight SIEM Integration	10-2

11 Using an Oracle Database Firewall with Oracle RAC

11.1	Configuring a Database Firewall with Oracle RAC for DPE Mode	11-1
11.1.1	About Configuring a Database Firewall with Oracle RAC for DPE Proxy Mode	11-1
11.1.2	Step 1: Configure the Listeners for Each Oracle RAC Node	11-3
11.1.3	Step 2: Configure the Proxies in the Oracle Database Firewall Console	11-4
11.1.4	Step 3: Test the Audit Reports to Ensure That They Can Collect Oracle RAC Node Data	11-7
11.2	Configuring a Database Firewall with Oracle RAC for DAM Mode	11-8

12 Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment

12.1	Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment And Prerequisites	12-1
12.2	Opening Ports on DBCS	12-3
12.3	Configuring Hybrid Cloud Secured Target Using TCP	12-4
12.3.1	Step 1: Registering On-premises Host on the Audit Vault Server	12-4
12.3.2	Step 2: Installing Audit Vault Agent on Registered On-premises Hosts	12-5
12.3.3	Step 3: Creating A User Account On The DBCS Target Instance	12-5
12.3.4	Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Database Cloud Service Instances	12-6
12.3.5	Step 5: Creating a Secured Target on Audit Vault Server for the DBCS Instance	12-7
12.3.6	Step 6: Starting Audit Trail On Audit Vault Server For The DBCS Instance	12-7
12.4	Configuring TCPS Connections for DBCS Instances	12-8

12.4.1	Step 1: Creating Server Wallet and Certificate	12-8
12.4.2	Step 2: Creating Client (Agent) Wallet and Certificate	12-10
12.4.3	Step 3: Exchanging Client (Agent) and Server Certificates	12-13
12.4.4	Step 4: Configuring Server Network	12-16
12.4.5	Step 5: Connecting to DBCS instances in TCPS mode	12-18
12.5	Configuring Hybrid Cloud Secured Target Using TCPS	12-19
12.5.1	Step 1: Registering On-premises Host on Oracle Audit Vault Server	12-19
12.5.2	Step 2: Installing Oracle Audit Vault Agent on Registered On-premises Hosts and Configuring TCPS	12-20
12.5.3	Step 3: Creating User Accounts on Oracle Database Cloud Service Target Instances	12-20
12.5.4	Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Database Cloud Service Instances	12-21
12.5.5	Step 5: Creating A Secured Target On Audit Vault Server For The DBCS Instance	12-22
12.5.6	Step 6: Starting Audit Trail On Audit Vault Server For The DBCS Instance	12-23
12.6	Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCPS	12-23
12.6.1	Step 1: Installing Audit Vault Agent on registered on-premises Host and configuring TCPS	12-24
12.6.2	Step 2: Creating User Accounts on Oracle Exadata Express Cloud Service Instances	12-24
12.6.3	Step 3: Creating A Secured Target On Audit Vault Server For Exadata Express Cloud Service Instance	12-25
12.7	Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCP	12-25
12.7.1	Step 1: Registering On Premises Host On The Audit Vault Server	12-25
12.7.2	Step 2: Installing Audit Vault Agent On Registered On Premises Host	12-25
12.7.3	Step 3: Creating User Accounts on Oracle Exadata Express Cloud Target Instances	12-25
12.7.4	Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Exadata Express Cloud Instances	12-26
12.7.5	Step 5: Creating A Secured Target On Audit Vault Server For The Exadata Express Cloud Instance	12-26
12.7.6	Step 6: Starting Audit Trail On Audit Vault Server For The Exadata Express Cloud Instance	12-26
12.8	Configuring Autonomous Data Warehouse and Autonomous Transaction Processing	12-27
12.8.1	Step 1: Install Audit Vault Agent On Registered On-premises Host And Configuring TCPS	12-27
12.8.2	Step 2: Create User Accounts on Oracle Cloud Instances	12-27
12.8.3	Step 3: Create A Secured Target On Audit Vault Server For The Cloud Instance	12-28

Part II General Administration Tasks

13 Managing User Accounts and Access

13.1	About Oracle Audit Vault and Database Firewall Administrative Accounts	13-1
13.2	Security Technical Implementation Guides and Implementation for User Accounts	13-2
13.3	Configuring Administrative Accounts for the Audit Vault Server	13-2
13.3.1	Guidelines for Securing the Oracle Audit Vault and Database Firewall User Accounts	13-3
13.3.2	Creating Administrative Accounts for the Audit Vault Server	13-3
13.3.3	Viewing the Status of Administrator User Accounts	13-4
13.3.4	Changing a User Account Type for the Audit Vault Server	13-4
13.3.5	Unlocking a User Account	13-4
13.3.6	Deleting an Audit Vault Server Administrator Account	13-5
13.4	Configuring sudo Access for Users	13-5
13.4.1	About Configuring sudo Access	13-5
13.4.2	Configuring sudo Access for a User	13-5
13.5	Managing User Access Rights to Secured Targets or Groups	13-7
13.5.1	About Managing User Access Rights	13-7
13.5.2	Controlling Access Rights by User	13-7
13.5.3	Controlling Access Rights by Secured Target or Group	13-7
13.6	Changing User Passwords in Oracle Audit Vault and Database Firewall	13-8
13.6.1	Password Requirements	13-8
13.6.2	Changing the Audit Vault Server Administrator User Password	13-9
13.6.3	Changing the Database Firewall Administrator Password	13-9

14 Managing the Audit Vault Server and Database Firewalls

14.1	Managing Audit Vault Server Settings, Status, and Maintenance Operations	14-1
14.1.1	Checking Server Status and System Operation	14-2
14.1.2	Running Diagnostics Checks for the Audit Vault Server	14-2
14.1.3	Downloading Detailed Diagnostics Reports for the Audit Vault Server	14-3
14.1.4	Accessing the Audit Vault Server Certificate and Public Key	14-4
14.1.4.1	Accessing the Server Certificate	14-4
14.1.4.2	Accessing the Server Public Key	14-4
14.1.5	Changing Logging Levels and Clearing Diagnostic Logs	14-5
14.1.6	Changing the Keyboard Layout	14-6
14.1.7	Rebooting or Powering Off the Audit Vault Server	14-6
14.2	Changing the Audit Vault Server's Network or Services Configuration	14-6
14.3	Managing Server Connectors for Email, Syslog, and Arcsight SIEM	14-6
14.4	Archiving and Retrieving Audit Data	14-7

14.4.1	Starting an Archive Job	14-7
14.4.2	Retrieving Oracle Audit Vault and Database Firewall Audit Data	14-8
14.5	Managing Repository Encryption	14-9
14.5.1	About Oracle Audit Vault Server Repository Encryption	14-9
14.5.2	Rotating the Master Key for Repository Encryption	14-9
14.5.3	Changing the Keystore Password	14-9
14.5.4	Backing Up the TDE Wallet	14-10
14.5.5	Data Encryption on Upgraded Instances	14-10
14.6	Backing Up and Restoring the Audit Vault Server	14-14
14.6.1	About the Backup and Restore Utility	14-14
14.6.2	How Much Space Do I Need for Backup Files?	14-16
14.6.3	Backing Up the Audit Vault Server	14-16
14.6.3.1	Step 1: Configure the Backup Utility	14-16
14.6.3.2	Step 2: Back Up the Audit Vault Server	14-20
14.6.3.3	Step 3: Validate the Backup	14-21
14.6.4	Restoring the Audit Vault Server	14-22
14.6.4.1	About Restoring the Audit Vault Server	14-23
14.6.4.2	Prerequisites for Restoring Audit Vault Server	14-23
14.6.4.3	Step 1: Configure the Backup Utility on the Audit Vault Server	14-24
14.6.4.4	Step 2: Restore Audit Vault Server	14-24
14.6.5	Restoring a Backup to a New System with a New or Different IP Address	14-25
14.7	Enabling Oracle Database In-Memory for the Audit Vault Server	14-26
14.7.1	About Enabling Oracle Database In-Memory for the Audit Vault Server	14-26
14.7.2	Enabling and Allocating Memory for Oracle Database In-Memory	14-27
14.7.3	Setting the Oracle Database In-Memory Options	14-28
14.7.4	Disabling Oracle Database In-Memory	14-28
14.7.5	Monitoring Oracle Database In-Memory Usage	14-28
14.8	Managing Plug-ins	14-29
14.9	Monitoring Server Tablespace Space Usage	14-29
14.10	Monitoring Server Archive Log Disk Space Use	14-29
14.11	Monitoring Server Flash Recovery Area	14-30
14.12	Monitoring Jobs	14-31
14.13	Scheduling Maintenance Job	14-31
14.14	Downloading and Using the AVCLI Command Line Interface	14-32
14.14.1	About the AVCLI Command Line Interface	14-32
14.14.2	Downloading the AVCLI Command Line Utility and Setting JAVA_HOME	14-33
14.14.3	Starting AVCLI	14-33
14.14.3.1	Starting AVCLI Interactively	14-34
14.14.3.2	Starting AVCLI Using Stored Credentials	14-34
14.14.4	Running AVCLI Scripts	14-36
14.14.5	Specifying Log Levels for AVCLI	14-37

14.14.6	Displaying Help and the Version Number of AVCLI	14-37
14.15	Downloading the Oracle Audit Vault and Database Firewall SDK	14-38
14.16	Managing Database Firewalls	14-38
14.16.1	Changing the Database Firewall's Network or Services Configuration	14-38
14.16.2	Viewing Network Traffic in a Database Firewall	14-39
14.16.3	Capturing Network Traffic in Oracle Database Firewall	14-39
14.16.4	Restarting or Powering Off Oracle Database Firewall	14-40
14.16.5	Removing Oracle Database Firewall from Oracle Audit Vault Server	14-40
14.16.6	Fetching an Updated Certificate from Oracle Database Firewall	14-40
14.16.7	Viewing Diagnostics for Oracle Database Firewall	14-41
14.16.8	Resetting Oracle Database Firewall	14-41
14.16.9	Restore Enforcement Points	14-42

15 Configuring a SAN Repository

15.1	About Configuring a SAN Repository	15-1
15.2	Configuring a SAN Server to Communicate with Oracle Audit Vault and Database Firewall	15-2
15.3	Registering or Dropping SAN Servers in the Audit Vault Server	15-3
15.3.1	Registering a SAN Server	15-3
15.3.2	Dropping a SAN Server	15-3
15.4	Discovering Targets on a SAN Server	15-4
15.4.1	About SAN Targets and Disks	15-4
15.4.2	Discovering Targets on a SAN Server and Making Disks Available	15-4
15.4.3	Logging Out of Targets on SAN Servers	15-5
15.5	Adding or Dropping SAN Disks in the Audit Vault Server Repository	15-6
15.5.1	About Disk Groups in the Audit Vault Server Repository	15-6
15.5.2	Adding SAN Disks to the Audit Vault Server Repository	15-7
15.5.3	Dropping SAN Disks from the Audit Vault Server Repository	15-8

Part III General Reference

A AVCLI Commands Reference

A.1	About the AVCLI Commands	A-1
A.2	Agent Host AVCLI Commands	A-2
A.2.1	REGISTER HOST	A-2
A.2.2	ALTER HOST	A-3
A.2.3	LIST HOST	A-5
A.2.4	DROP HOST	A-5
A.2.5	ACTIVATE HOST	A-6

A.2.6	DEACTIVATE HOST	A-6
A.3	Database Firewall AVCLI Commands	A-7
A.3.1	REGISTER FIREWALL	A-7
A.3.2	DROP FIREWALL	A-8
A.3.3	LIST FIREWALL	A-8
A.3.4	REBOOT FIREWALL	A-9
A.3.5	POWEROFF FIREWALL	A-9
A.3.6	CREATE RESILIENT PAIR	A-9
A.3.7	SWAP RESILIENT PAIR	A-10
A.3.8	DROP RESILIENT PAIR	A-10
A.3.9	ALTER FIREWALL	A-11
A.3.10	SHOW STATUS FOR FIREWALL	A-11
A.4	Enforcement Point AVCLI Commands	A-12
A.4.1	CREATE ENFORCEMENT POINT	A-12
A.4.2	DROP ENFORCEMENT POINT	A-13
A.4.3	LIST ENFORCEMENT POINT	A-13
A.4.4	START ENFORCEMENT POINT	A-14
A.4.5	STOP ENFORCEMENT POINT	A-14
A.4.6	ALTER ENFORCEMENT POINT	A-15
A.5	Secured Target AVCLI Commands	A-16
A.5.1	REGISTER SECURED TARGET	A-17
A.5.2	ALTER SECURED TARGET	A-19
A.5.3	UPLOAD OR DELETE WALLET FILE	A-21
A.5.4	LIST ADDRESS FOR SECURED TARGET	A-22
A.5.5	LIST SECURED TARGET	A-22
A.5.6	LIST SECURED TARGET TYPE	A-22
A.5.7	LIST ATTRIBUTE FOR SECURED TARGET	A-23
A.5.8	LIST METRICS	A-23
A.5.9	DROP SECURED TARGET	A-24
A.6	Target Group AVCLI Commands	A-24
A.6.1	ADD TARGET	A-24
A.6.2	DELETE TARGET	A-25
A.7	Audit Trail Collection AVCLI Commands	A-25
A.7.1	START COLLECTION FOR SECURED TARGET	A-26
A.7.2	STOP COLLECTION FOR SECURED TARGET	A-30
A.7.3	LIST TRAIL FOR SECURED TARGET	A-34
A.7.4	DROP TRAIL FOR SECURED TARGET	A-35
A.8	SMTP Connection AVCLI Commands	A-36
A.8.1	REGISTER SMTP SERVER	A-36
A.8.2	ALTER SMTP SERVER	A-38
A.8.3	ALTER SMTP SERVER ENABLE	A-39

A.8.4	ALTER SMTP SERVER DISABLE	A-39
A.8.5	ALTER SMTP SERVER SECURE MODE ON	A-40
A.8.6	ALTER SMTP SERVER SECURE MODE OFF	A-41
A.8.7	TEST SMTP SERVER	A-41
A.8.8	LIST ATTRIBUTE OF SMTP SERVER	A-42
A.8.9	DROP SMTP SERVER	A-43
A.9	Security Management AVCLI Commands	A-43
A.9.1	ALTER DATA ENCRYPTION	A-43
A.9.2	SHOW DATA ENCRYPTION STATUS	A-44
A.9.3	GRANT SUPERADMIN	A-44
A.9.4	REVOKE SUPERADMIN	A-45
A.9.5	GRANT ACCESS	A-45
A.9.6	REVOKE ACCESS	A-46
A.9.7	GRANT ADMIN	A-46
A.9.8	REVOKE ADMIN	A-46
A.9.9	ALTER USER	A-47
A.10	SAN Storage AVCLI Commands	A-47
A.10.1	REGISTER SAN SERVER	A-48
A.10.2	ALTER SAN SERVER	A-49
A.10.3	LIST TARGET FOR SAN SERVER	A-50
A.10.4	DROP SAN SERVER	A-50
A.10.5	LIST DISK	A-50
A.10.6	ALTER DISKGROUP	A-51
A.10.7	LIST DISKGROUP	A-51
A.10.8	LIST SAN SERVER	A-52
A.10.9	SHOW iSCSI INITIATOR DETAILS FOR SERVER	A-52
A.11	Remote File System AVCLI Commands	A-53
A.11.1	REGISTER REMOTE FILESYSTEM	A-53
A.11.2	ALTER REMOTE FILESYSTEM	A-54
A.11.3	DROP REMOTE FILESYSTEM	A-55
A.11.4	LIST EXPORT	A-55
A.11.5	LIST REMOTE FILESYSTEM	A-55
A.11.6	SHOW STATUS OF REMOTE FILESYSTEM	A-56
A.12	Server Management AVCLI Commands	A-56
A.12.1	ALTER SYSTEM SET	A-56
A.12.2	SHOW CERTIFICATE	A-58
A.12.3	DOWNLOAD LOG FILE	A-59
A.13	Collection Plug-In AVCLI Commands	A-59
A.13.1	DEPLOY PLUGIN	A-59
A.13.2	LIST PLUGIN FOR SECURED TARGET TYPE	A-60
A.13.3	UNDEPLOY PLUGIN	A-61

A.14	General Usage AVCLI Commands	A-61
A.14.1	CONNECT	A-62
A.14.2	STORE CREDENTIALS	A-62
A.14.3	SHOW USER	A-63
A.14.4	CLEAR LOG	A-63
A.14.5	HELP	A-63
A.14.6	-HELP	A-63
A.14.7	-VERSION	A-64
A.14.8	QUIT	A-65
A.15	AVCLI User Commands	A-65
A.15.1	CREATE AUDITOR	A-65
A.15.2	ALTER AUDITOR	A-66
A.15.3	DROP AUDITOR	A-67
A.15.4	CREATE ADMIN	A-67
A.15.5	ALTER ADMIN	A-68
A.15.6	DROP ADMIN	A-68

B Plug-in Reference

B.1	About Oracle Audit Vault and Database Firewall Plug-ins	B-1
B.2	Plug-ins Shipped with Oracle Audit Vault and Database Firewall	B-1
B.2.1	Out-of-the Box Plug-ins at a Glance	B-2
B.2.2	Oracle Database	B-4
B.2.3	Microsoft SQL Server	B-6
B.2.4	Sybase ASE	B-8
B.2.5	Sybase SQL Anywhere	B-9
B.2.6	IBM DB2	B-9
B.2.7	MySQL	B-10
B.2.8	Oracle Solaris	B-12
B.2.9	Linux	B-12
B.2.10	IBM AIX	B-14
B.2.11	Microsoft Windows	B-15
B.2.12	Microsoft Active Directory	B-15
B.2.13	Oracle ACFS	B-16
B.2.14	Oracle Big Data Appliance	B-16
B.2.15	Summary of Data Collected for Each Audit Trail Type	B-17
B.3	Scripts for Oracle AVDF Account Privileges on Secured Targets	B-21
B.3.1	About Scripts for Setting up Oracle Audit Vault and Database Firewall Account Privileges	B-22
B.3.2	Oracle Database Setup Scripts	B-22
B.3.3	Sybase ASE Setup Scripts	B-24
B.3.3.1	About the Sybase ASE Setup Scripts	B-24

B.3.3.2	Setting Up Audit Data Collection Privileges for a Sybase ASE Secured Target	B-25
B.3.3.3	Setting Up Stored Procedure Auditing Privileges for a Sybase ASE Secured Target	B-25
B.3.4	Sybase SQL Anywhere Setup Scripts	B-26
B.3.5	Microsoft SQL Server Setup Scripts	B-27
B.3.5.1	About the SQL Server Setup Script	B-27
B.3.5.2	Setting Up Audit Data Collection Privileges for a SQL Server Secured Target	B-27
B.3.5.3	Setting Up Stored Procedure Auditing Privileges for a SQL Server Secured Target	B-28
B.3.6	IBM DB2 for LUW Setup Scripts	B-29
B.3.6.1	About the IBM DB2 for LUW Setup Scripts	B-29
B.3.6.2	Setting Up Audit Data Collection Privileges for IBM DB2 for LUW	B-30
B.3.6.3	Setting Up SPA Privileges for an IBM DB2 for LUW Secured Target	B-30
B.3.7	MySQL Setup Scripts	B-31
B.4	Audit Collection Consideration	B-31
B.4.1	Additional Information for Audit Collection from Oracle Active Data Guard	B-31
B.5	Audit Trail Cleanup	B-32
B.5.1	Oracle Database Audit Trail Cleanup	B-33
B.5.1.1	About Purging the Oracle Database Secured Target Audit Trail	B-33
B.5.1.2	Scheduling an Automated Purge Job	B-33
B.5.2	SQL Server Audit Trail Cleanup	B-34
B.5.3	MySQL Audit Trail Cleanup	B-35
B.6	Procedure Look-ups: Connect Strings, Collection Attributes, Audit Trail Locations	B-36
B.6.1	Secured Target Locations (Connect Strings)	B-36
B.6.2	Collection Attributes	B-38
B.6.2.1	About Collection Attributes	B-38
B.6.2.2	Oracle Database Collection Attributes	B-38
B.6.2.3	IBM DB2 for LUW Collection Attribute	B-41
B.6.2.4	MySQL Collection Attributes	B-41
B.6.2.5	Oracle ACFS Collection Attributes	B-41
B.6.3	Audit Trail Locations	B-42

C REDO Logs Audit Data Collection Reference

C.1	About the Recommended Settings for Collection from REDO Logs	C-1
C.2	Oracle Database 11g Release 2 (11.2) and 12c Secured Target Audit Parameter Recommendations	C-2
C.3	Oracle Database 11g Release 1 (11.1) Secured Target Audit Parameter Recommendations	C-8
C.4	Oracle Database 10g Release 2 (10.2) Secured Target Audit Parameter Recommendations	C-13

C.5	Populating Client ID In Reports for REDO Collector	C-18
-----	--	------

D Ports Used by Audit Vault and Database Firewall

D.1	Ports Required When Database Firewall is Deployed for Secured Targets	D-1
D.2	Ports for Services Provided by Oracle Audit Vault Server	D-2
D.3	Ports for Services Provided by the Database Firewall	D-2
D.4	Ports for External Network Access by the Audit Vault Server	D-3
D.5	Ports for External Network Access by the Database Firewall	D-4
D.6	Ports for Internal TCP Communication	D-5

E Message Code Dictionary

E.1	Audit Vault Messages	E-1
E.2	Database Firewall Messages	E-40

F Security Technical Implementation Guides

F.1	About Security Technical Implementation Guides	F-1
F.2	Enabling and Disabling STIG Rules on Oracle Audit Vault and Database Firewall	F-3
F.2.1	Enabling STIG Rules on Oracle Audit Vault and Database Firewall	F-3
F.2.2	Disabling STIG Rules on Oracle Audit Vault and Database Firewall	F-3
F.3	Current Implementation of STIG Rules on Oracle Audit Vault and Database Firewall	F-3
F.4	Current Implementation of Database STIG Rules	F-4
F.5	Additional Notes	F-12
F.5.1	DG0008-ORACLE11 STIG Rule	F-12
F.5.2	DG0075-ORACLE11, DO0250-ORACLE11 STIG Rules	F-12
F.5.3	DG0116-ORACLE11 STIG Rule	F-13
F.6	Current Implementation of Operating System STIG Rules	F-13

G Troubleshooting Oracle Audit Vault and Database Firewall

G.1	Audit Vault Agent or Host Monitor is not Upgraded to the Latest Bundle Patch	G-1
G.2	Enable Archiving Functionality Post Upgrade From BP11 to Later Releases	G-2
G.3	Partial or No Traffic Seen for an Oracle Database Monitored by Database Firewall	G-4
G.4	RPM Upgrade Failed	G-5
G.5	Agent Activation Request Returns 'host is not registered' Error	G-5
G.6	Unable to Deploy Agent on the Secondary Audit Vault Server	G-6
G.7	Operation Fails When I Try to Build Host Monitor or Collect Oracle Database Trail	G-6
G.8	'java -jar agent.jar' Failed on Windows Machine	G-7
G.9	Unable to Install the Agent or Generate the agent.jar File	G-7
G.10	Unable to Un-install the Oracle Audit Vault Agent Windows Service	G-8

G.11	Access Denied Error While Installing Agent as a Windows Service	G-8
G.12	Unable to Start the Agent Through the Services Applet On The Control Panel	G-9
G.13	Error When Starting the Agent	G-9
G.14	Error When Running Host Monitor Setup	G-10
G.15	Alerts on Oracle Database Secured Target are not Triggered for a Long Time	G-10
G.16	Error When Creating an Audit Policy	G-10
G.17	Connection Problems when Using Database Firewall DPE Mode	G-11
G.18	Audit Trail Does Not Start	G-12
G.19	Cannot Access the Audit Vault Server UI	G-12
G.20	Cannot See Data for My Secured Target	G-13
G.21	Problems Pairing Oracle Database Firewall and Oracle Audit Vault Server	G-14
G.22	User Names Do Not Appear on Database Firewall Reports	G-15
G.23	Alerts Are Not Generated	G-15
G.24	Problems Retrieving or Provisioning Audit Settings on Oracle Secured Target	G-16
G.25	Operation Failed Message Appears When Attempting to Enable Oracle Audit Vault and Database Firewall Policies	G-17
G.26	Failure While Adding Disks	G-17
G.27	Out of Memory Error Message During Restore	G-18
G.28	JAVA.IO.IOEXCEPTION Error	G-18
G.29	Failed to Start ASM Instance Error	G-19
G.30	Internal capacity exceeded messages seen in the /var/log/messages file	G-19
G.31	A Client Is Unable To Connect To The AVS Using SSH With A Secondary Network Interface Card	G-21
G.32	First Archive Or Retrieve Job After Upgrade	G-22
G.33	Audit Vault Agent Installation Fails After HA Pairing Or Separation	G-23
G.34	Error in Restoring Files	G-24
G.35	DB2 Collector Fails Due to Source Version NULL Errors	G-24
G.36	DB2 Collector Fails Due To Connection or Permission Issue From Database	G-25
G.37	ORA-12660 Error While Registering Secured Target	G-25
G.38	Failure During High Availability Pairing in Oracle Audit Vault Server	G-26
G.39	Audit Trail Performance Issues Occur After Audit Vault Server Upgrade	G-26
G.40	Failures Due to Dropping Users	G-27
G.41	Failure of Agent Automatic Upgrades	G-27
G.42	Some Services May Not Start After Backup	G-27
G.43	Data Overflow Issues in the Oracle Audit Vault UI	G-28
G.44	Oracle Audit Vault Agent is Unreachable and the Transaction Log Audit Trail is Frozen in Starting Status	G-28
G.45	Scheduled PDF or XLS Reports Result in a Hung State	G-29
G.46	Pending Reports In Scheduled Status	G-29
G.47	The Audit Vault Logs Display A Message To Install Npcap And OpenSSL	G-30
G.48	Host Monitor Agent Fails to Start	G-31
G.49	Audit Trail Stopped After Relocating Windows Event Log Files	G-32

G.50	Network Audit Trail Does Not Start on Unix Platforms	G-32
G.51	Audit Vault Agent in Unreachable state upon Failover	G-33
G.52	Unable to Reach Gateway Error	G-34

H Multiple Network Interface Cards

H.1	Enabling A Secondary Network Interface For Audit Vault Server	H-2
H.2	Configuring Physical Network Separation For Database Firewall	H-4
H.3	Enabling NFS On Secondary Network Interface Card For Audit Vault Server	H-4
H.4	Enabling SPA On Secondary Network Interface Card For Audit Vault Server	H-5
H.5	Enabling SSH On A Secondary Network Interface Card For Audit Vault Server	H-5
H.6	Applying Static Routing Rules On Network Interfaces For Audit Vault Server And Database Firewall	H-7
H.7	Enabling Agent Connectivity On Secondary NICs for Audit Vault Server	H-8
H.8	Enabling Agent To Operate In High Availability Environment With Secondary Network Interface Card For Audit Vault Server	H-12
H.9	Disabling A Secondary Network Interface For Audit Vault Server	H-14
H.10	Changing The IP Address On A Secondary Network Interface Card For Audit Vault Server	H-14
H.11	Features Of Network Interfaces For Audit Vault Server	H-15

I Adding User Content To System Configuration Files

Index

List of Figures

1-1	Selecting the Time Range for the Dashboard in the Home Tab	1-12
6-1	Database Response Monitoring	6-33
8-1	Pairs of Audit Vault Servers and Database Firewalls in High Availability Mode	8-2
9-1	Oracle Audit Vault and Database Firewall with F5 BIG-IP ASM Data Flow Unit	9-2
11-1	Oracle Database Firewall and Oracle RAC SCAN VIP Architecture	11-2
15-1	The Repository Page	15-7

List of Tables

5-1	OS Permission Required For Installing The Agent	5-4
14-1	Components with Variable Logging Levels	14-5
A-1	AVCLI Agent Host Commands	A-2
A-2	Host Attributes (key values)	A-4
A-3	LOGLEVEL Component Names	A-4
A-4	LOGLEVEL Values	A-4
A-5	Database Firewall Commands	A-7
A-6	Oracle Database Firewall Attributes	A-11
A-7	Enforcement Point Commands	A-12
A-8	Enforcement Point Attributes	A-15
A-9	AVCLI Secured Target Commands	A-16
A-10	Secured Target Attributes	A-21
A-11	AVCLI Target Group Commands	A-24
A-12	AVCLI Secured Target Connection Commands	A-25
A-13	AVCLI SMTP Commands	A-36
A-14	AVCLI Security Management Commands	A-43
A-15	AVCLI SAN Storage Commands	A-47
A-16	AVCLI Remote Filesystem Commands	A-53
A-17	AVCLI Server Management Commands	A-56
A-18	System Attributes	A-57
A-19	Logging component names and values	A-57
A-20	Logging level and values	A-58
A-21	AVCLI Collection Plug-In Commands	A-59
A-22	AVCLI HELP and EXIT Commands	A-61
A-23	AVCLI User Commands	A-65
B-1	Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall	B-2
B-2	Oracle Database Plug-in	B-5
B-3	Microsoft SQL Server Plug-in	B-6
B-4	Sybase ASE Plug-in	B-8
B-5	Sybase SQL Anywhere Plug-in	B-9
B-6	IBM DB2 Plug-in	B-9
B-7	MySQL Plug-in	B-10
B-8	Old Audit Format	B-11
B-9	New Audit Format	B-11
B-10	Oracle Solaris Plug-in	B-12

B-11	Linux Plug-in	B-13
B-12	IBM AIX Plug-in	B-14
B-13	Microsoft Windows Plug-in	B-15
B-14	Microsoft Active Directory Plug-in	B-15
B-15	Oracle ACFS Plug-in	B-16
B-16	Big Data Appliance Plug-in	B-16
B-17	Summary of Audit Trail Types Supported for Each Secured Target Type	B-18
B-18	Secured Target Connect Strings (for Secured Target Location Field)	B-36
B-19	Collection Attributes for DIRECTORY Audit Trail for Oracle Database	B-39
B-20	Collection Attribute for IBM DB2 for LUW Database	B-41
B-21	Collection Attributes for MySQL Database	B-41
B-22	Collection Attribute for Oracle ACFS	B-42
B-23	Supported Trail Locations for Secured Targets	B-42
C-1	Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database	C-2
C-2	Hidden Initialization Parameters for a Release 11.1 Secured Target Database	C-8
C-3	Initialization Parameters for a Release 11.1 Secured Target Database	C-9
C-4	Hidden Initialization Parameters for a Release 10.2 Secured Target Database	C-13
C-5	Initialization Parameters for a Release 10.2 Secured Target Database	C-14
D-1	Ports for Services Provided by Audit Vault Server	D-2
D-2	Ports for Services Provided by Database Firewall	D-2
D-3	Ports for External Network Access by the Audit Vault Server	D-3
D-4	Ports for External Network Access by the Database Firewall	D-4
D-5	Ports for Internal TCP Communication	D-5
F-1	Vulnerability Categories	F-3
F-2	Current Implementation of Database STIG Rules	F-4
F-3	Accounts and Role Assignments in Audit Vault Server	F-13
F-4	Accounts and Role Assignments in Database Firewall	F-13
F-5	Operating System STIG Rule Set Reference	F-14
F-6	User Action – Definition and Guidelines	F-14
F-7	Current Implementation of Operating System STIG Rules	F-14
G-1	Server Encryption Types	G-26

Preface

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

Topics

- [Audience](#) (page xxv)
- [Documentation Accessibility](#) (page xxv)
- [Related Documents](#) (page xxv)
- [Conventions](#) (page xxvi)

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

For more information, see the following documents:

- *Oracle Audit Vault and Database Firewall Release Notes*
Contains release note material for Oracle Audit Vault and Database Firewall.
- *Oracle Audit Vault and Database Firewall Concepts Guide*
Contains conceptual information for Oracle Audit Vault and Database Firewall.
- *Oracle Audit Vault and Database Firewall Auditor's Guide*
Explains how to use Oracle Audit Vault and Database Firewall to create audit and firewall policies, and to generate reports.
- *Oracle Audit Vault and Database Firewall Installation Guide*
Explains how to install or upgrade Oracle Audit Vault and Database Firewall.
- *Oracle Audit Vault and Database Firewall Developer's Guide*
Explains how to create custom Oracle Audit Vault collectors.
- *Oracle Audit Vault and Database Firewall Licensing Information*
Contains licensing requirements for Oracle Audit Vault and Database Firewall.

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.
<i>italic</i>	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.

What's New

This preface describes new features in the most recent, as well as prior, releases of Oracle Audit Vault and Database Firewall (AVDF) version 12.2.

Oracle AVDF Release 12.2.0 Changes

The following are new features in this release:

- A backup and restore utility for the Audit Vault Server has been integrated into the product.
- Audit trails will automatically start when the Audit Vault Agent is restarted or when Oracle AVDF is upgraded.
- The AVCLI command line utility can be used non-interactively by storing an administrator's credentials in the AVCLI wallet.
- You can configure Oracle Database In-Memory to speed up reports.
- New (full) installations of Oracle AVDF 12.2 will have all audit data encrypted using Oracle Database Transparent Data Encryption (TDE). Any upgrade performed thereafter encrypts audit data from that point onwards.
- When new audit trails contain data that is older than limits set in the retention (archiving) policy, that data will be automatically archived according to the policy.
- You can change the certificate for the Audit Vault Server and Database Firewall Web UIs.
- You can register hosts without providing an IP address.
- You can change the logging levels of system components from the Web UI.
- You can unlock user accounts from the Web UI.
- New reports have been added including: summary reports, IRS compliance reports, and reports that correlate database audit events with OS users that used `su` or `sudo` to execute commands.
- In the Administrator's Web UI, the Hosts tab has new Host Monitor details, and added Audit Vault Agent details.
- The Audit Vault Server's high availability pairing UI has been improved for usability.
- Support for IBM AIX secured targets has been added.
- The Oracle AVDF auditor can create an alert syslog template.
- The Oracle AVDF auditor can set a schedule for retrieval of audit data and entitlements from Oracle Database.
- Support for the Interface Niagara Masters Server Adapter card is now available for this release.

- Included *Oracle Audit Vault and Database Firewall Concepts Guide* to the documentation library.
- Introducing Oracle AVDF Hybrid Cloud in release 12.2.0.3.0. In the AVDF Hybrid Cloud deployment model, the Audit Vault server is deployed on-premises and monitors DBCS (Database Cloud Service), Exadata Cloud Service instances, and on-premises databases. See [Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment](#) (page 12-1) for more information.
- Introducing TDE (Transparent Data Encryption) support during Audit Vault Server upgrade. Refer to [Data Encryption on Upgraded Instances](#) (page 14-10) for more information.
- Introducing support for multiple Network Interface Cards (NIC) on Oracle Audit Vault and Database Firewall. The AVDF users can now effectively separate different aspects of the Audit Vault Server network usage by enabling multiple Network Interface Cards on the AVDF appliance. See [Multiple Network Interface Cards](#) (page H-1) for more information.
- Included new release of Oracle database 12.2 as supported secure target version. See sections [UPLOAD OR DELETE WALLET FILE](#) (page A-21) and [Securing the Agent and Oracle Database Secure Target Connection](#) (page 6-34) for more information.
- Introducing a new feature to schedule maintenance jobs. See [Scheduling Maintenance Job](#) (page 14-31) for more information.
- Oracle Database Collector is enhanced to support Oracle DB 12.2. See sections [Oracle Database](#) (page B-4) and [Summary of Data Collected for Each Audit Trail Type](#) (page B-17) for more information.
- Included support for Oracle Database Exadata Express Cloud Service. See sections [Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCPS](#) (page 12-23) and [Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCP](#) (page 12-25) for more information.
- Included support for Autonomous Data Warehouse Cloud. See [Configuring Autonomous Data Warehouse and Autonomous Transaction Processing](#) (page 12-27) for complete information.

Changes In This Document

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

Revision History

The following are the updates and correction in this document.

E41705-35 (June 2022)

Introducing support for renewing or rotating certificates for Database Firewall and Audit Vault Server. See [Certificates](#) (page 2-12) for complete information.

Update or correction to the following topics:

- [Defining Archive Locations](#) (page 3-13)
- [Step 2: Restore Audit Vault Server](#) (page 14-24)

- [REGISTER HOST](#) (page A-2)

E41705-34 (March 2021)

Update to requirements for using Host Monitor functionality on Windows platform. See sections [Deploying the Agent and Host Monitor on Microsoft Windows Hosts](#) (page 7-3) and [Host Monitor Requirements](#) (page 7-2) for complete information, prior to upgrade of Oracle AVDF.

E41705-33 (September 2020)

Updates and correction to the following topics:

- Host Monitor functionality on Windows platform is re-certified in 12.2.0.13.0. For using Host Monitoring on Windows platform install Npcap and update OpenSSL libraries on Windows before upgrading to 12.2.0.13.0. Complete the steps in the following sections:
 - [Host Monitor Requirements](#) (page 7-2)
 - [Deploying the Agent and Host Monitor on Microsoft Windows Hosts](#) (page 7-3)
 - [Create a Network Audit Trail](#) (page 7-7) to set the `network_device_name_for_hostmonitor` collection attribute post installation of Npcap and OpenSSL
- In case the Audit Vault Agents or Host Monitor Agents fail to upgrade automatically to recent bundle patch, then the Agents must be manually upgraded. See [Audit Vault Agent or Host Monitor is not Upgraded to the Latest Bundle Patch](#) (page G-1) for complete information.
- [Step 1: Apply the Specified Patch to Oracle Database](#) (page 6-29)
- Updated the following topics to clarify on archiving functionality in high availability environment:
 - [Defining Archive Locations](#) (page 3-13)
 - [Managing Archival and Retrieval in High Availability Environments](#) (page 3-18)

E41705-31 (March 2020)

- Database Activity Monitoring with Host monitor on Windows platform is not certified in release 12.2.0.11.0 and 12.2.0.12.0. Upgrade to these releases only when you are sure that host monitoring functionality on Windows platform is not required.
- Supporting IBM DB2 audit data collection from IBM AIX on Power Systems (64-bit) starting release 12.2.0.12.0. See [IBM DB2](#) (page B-9) for complete information.
- Supporting audit collection from IBM DB2 (version 11.1) HADR (High Availability and Disaster Recovery) on OL 7.x starting release 12.2.0.12.0.
- Supporting audit collection from Microsoft SQL Server Cluster on Windows 2012 R2 starting release 12.2.0.12.0. See section [Microsoft SQL Server](#) (page B-6) for mandatory collection attribute.
- Introducing DDI enhancement to retrieve session information for Oracle Database targets. This is available for Database Firewall in Monitoring and Blocking, or in Monitoring only mode. See [Step 2: Run the Oracle Advance Security Integration Script](#) (page 6-29) for complete information.
- Included important information in section [About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall](#) (page 3-12).
- Updates to section [About Setting Transport Layer Security Levels](#) (page 2-6).

- Added new [Target Group AVCLI Commands](#) (page A-24) to add or remove targets from target group.

E41705-29 (December 2019)

- Included important information for configuring CDB and PDB instances for audit collection. See following sections:
 - [Oracle Database Setup Scripts](#) (page B-22)
 - [Configuring Audit Trail Collection For CDB And PDB](#) (page 6-19)
 - [Scheduling an Automated Purge Job](#) (page B-33)
- Configuring IBM DB2 for audit collection is now simpler. The connect string `jdbc:av:db2://hostname:port` and collection attribute `av.collector.databasename` is not required from Oracle Audit Vault and Database Firewall release 12.2.0.11.0 and onwards.
- Correction to the command in [Sybase ASE](#) (page B-8).

E41705-28 (November 2019)

- Updates and correction to the entire document.
- Update to section [Defining Archive Locations](#) (page 3-13).

E41705-27 (October 2019)

- Correction to section [Configuring Oracle Audit Vault Server Syslog Destinations](#) (page 3-8).
- Updates and correction to the entire document.

E41705-26 (September 2019)

Caution:

- *Oracle Audit Vault and Database Firewall* release 12.2.0.11.0 does not support Niagara cards. Do not upgrade to this release if you have Niagara cards in your system.
- Host Monitor on Windows platform is not certified in release 12.2.0.11.0. Upgrade or use 12.2.0.11.0 only when you are sure that network trail monitoring functionality on Windows platform is not required. This functionality will be certified in a future release. If your installation is pertaining to any of the older releases before 12.2.0.11.0, then Host Monitor functionality on Windows platform is certified.

- *Oracle Audit Vault and Database Firewall* supports audit collection from SAP Sybase ASE (version 16.0). It also supports Sybase password encryption starting release 12.2.0.11.0. See [Sybase ASE](#) (page B-8) for complete information.
- *Oracle Audit Vault and Database Firewall* release 12.2.0.11.0 and later, enables archiving functionality in high availability environment. See [Managing Archival and Retrieval in High Availability Environments](#) (page 3-18) for complete information.
- *Oracle Audit Vault and Database Firewall* Hybrid Cloud can be configured with Autonomous Data Warehouse and Autonomous Transaction Processing. See

[Configuring Autonomous Data Warehouse and Autonomous Transaction Processing](#) (page 12-27) for complete information.

- *Oracle Audit Vault and Database Firewall* supports high availability configuration for proxy deployment. Refer to the following sections for complete information:
 - [Configuring High Availability For Database Firewall In Proxy Mode Through Client Configuration](#) (page 8-12)
 - [Configuring High Availability For Database Firewall In Proxy Mode Through DNS Setup](#) (page 8-14)
- Minor correction to section [About High Availability Configurations in Oracle Audit Vault and Database Firewall](#) (page 8-1).
- Included workaround for [Audit Trail Stopped After Relocating Windows Event Log Files](#) (page G-32).
- Included workaround for [Network Audit Trail Does Not Start on Unix Platforms](#) (page G-32).
- Included workaround for [Pending Reports In Scheduled Status](#) (page G-29).
- Correction to commands in the following sections:
 - [Enabling STIG Rules on Oracle Audit Vault and Database Firewall](#) (page F-3)
 - [Disabling STIG Rules on Oracle Audit Vault and Database Firewall](#) (page F-3)
- Included information on [External Network Dependencies](#) (page 2-2).
- Updated the connect string for Windows authentication in [Microsoft SQL Server](#) (page B-6).
- Updated *OpenSSL* version for Windows. See [Host Monitor Requirements](#) (page 7-2).

E41705-25 (June 2019)

The `JAVA_HOME` environment variable must be set to point to the JDK installation directory. On Windows, add `%JAVA_HOME%\bin` to the `PATH` environment variable. See section [Downloading the AVCLI Command Line Utility and Setting JAVA_HOME](#) (page 14-33).

E41705-24 (March 2019)

- Included important information on the backup functionality which does not backup archived files as they may be located on a remote file system. See sections [Defining Archive Locations](#) (page 3-13) and [About the Backup and Restore Utility](#) (page 14-14) for complete information.
- Included important information on configuring Host Monitor only. See [Create an Enforcement Point for the Host Monitor](#) (page 7-7) for complete information.
- Included workaround for an issue on Host Monitor. See [The Audit Vault Logs Display A Message To Install Npcap And OpenSSL](#) (page G-30) for complete information.
- Included important information regarding disk space for the restore operation. See section [How Much Space Do I Need for Backup Files?](#) (page 14-16) for complete information.
- Included supported link types for Host Monitor. See [About Host Monitoring](#) (page 7-1) for complete information.
- Included details that a certificate must contain in section [Changing the UI \(Console\) Certificate for Oracle Audit Vault Server](#) (page 3-2).

- Included commands to disable or enable the failover through `AVCLI`. See section [Disabling or Enabling Failover of the Audit Vault Server](#) (page 8-9) for complete information.
- The primary and secondary Audit Vault Servers must have the same specification. See section [Prerequisites for Configuring a Resilient Pair of Audit Vault Servers](#) (page 8-3) for complete information.
- Minor update to section [About Deploying the Audit Vault Agent](#) (page 5-3).
- Minor correction to section [Step 1: Configure the Backup Utility](#) (page 14-16).
- Included important note on changing the IP addresses of Audit Vault Servers in case of high availability configuration. See section [Setting or Changing the Audit Vault Server Network Configuration](#) (page 3-5).
- Included workaround for an issue. See section [Host Monitor Agent Fails to Start](#) (page G-31) for complete information.

E41705-22 (October 2018)

- **Required Action:**
 - If any Agent is using `Java 1.6`, then upgrade the `Java` version to `1.8`.
 - Install the *Mandatory Pre-upgrade Patch* before upgrading to *Oracle Audit Vault and Database Firewall* release `12.2.0.9.0`. See *Oracle Audit Vault and Database Firewall Readme* for release `12.2.0 BP9` for complete information.
- Added support for setting TLS levels across all components of *Oracle Audit Vault and Database Firewall*. See [About Setting Transport Layer Security Levels](#) (page 2-6) for complete information.
- Added an important note on scheduling concurrent long running reports at the same time. See section [Scheduled PDF or XLS Reports Result in a Hung State](#) (page G-29) for complete information.
- **F5 BIG-IP ASM** integration is deprecated in release `12.2.0.7.0`, and will be desupported in `19.1.0.0.0`. This functionality is only supported on **F5 BIG-IP ASM** version `10.2.1`.
- **Micro Focus Security ArcSight SIEM** is deprecated in `12.2.0.8.0` and is desupported in `12.2.0.9.0`. Use the `syslog` integration feature instead.
- See the following sections for updated list of supported systems and components:
 - [Viewing F5 Data in Oracle Audit Vault and Database Firewall Reports](#) (page 9-10)
 - [Integrating Oracle Audit Vault and Database Firewall with Third-Party Products](#) (page 1-4)
 - [Step 5: Plan Your Integration Options](#) (page 1-9)
 - [About Configuring Oracle Audit Vault Server](#) (page 3-1)
 - [Integration with Third Party SIEM and Log-data Analysis Tools](#) (page 10-1)
 - [Managing Server Connectors for Email, Syslog, and Arcsight SIEM](#) (page 14-6)
 - [Host Monitor Requirements](#) (page 7-2)
- Added important information in section [Retrieving Oracle Audit Vault and Database Firewall Audit Data](#) (page 14-8).

- Added important information in section [Ports for Services Provided by the Database Firewall](#) (page D-2).
- Added important information in section [REGISTER REMOTE FILESYSTEM](#) (page A-53).
- Added important information in section [Configure and Download the Diagnostics Report File](#) (page 4-13).
- Added important information on backup in section [Backing Up the Audit Vault Server](#) (page 14-16).
- Added best practice note in section [MySQL](#) (page B-10).
- Minor update to section [Configuring Physical Network Separation For Database Firewall](#) (page H-4).
- Minor update to section [Oracle Database](#) (page B-4).
- Minor update to section [Configuring Physical Network Separation For Database Firewall](#) (page H-4).
- Minor update to section [Managing Database Firewall Network Encryption](#) (page 2-3).
- Fiber Channel based storage with multipath is not supported in Oracle Audit Vault and Database Firewall. Updated this document accordingly.
- Included [Database Firewall Messages](#) (page E-40).
- The syntax of the following commands will be changed in Oracle Audit Vault and Database Firewall release 19.1.0.0.0:
 - [REGISTER SECURED TARGET](#) (page A-17)
 - [ALTER SECURED TARGET](#) (page A-19)
 - [REGISTER SMTP SERVER](#) (page A-36)
 - [ALTER SMTP SERVER](#) (page A-38)
 - [REGISTER SAN SERVER](#) (page A-48)
 - [ALTER SAN SERVER](#) (page A-49)

E41705-21 (June 2018)

- Added important information in section [Failure While Adding Disks](#) (page G-17).
- Minor update to sections [Defining Archive Locations](#) (page 3-13) and [REGISTER REMOTE FILESYSTEM](#) (page A-53).

E41705-20 (June 2018)

- Enhanced audit collection by supporting:
 - Autonomous Data Warehouse Cloud. See [Configuring Autonomous Data Warehouse and Autonomous Transaction Processing](#) (page 12-27) for complete information.
 - MySQL version 5.7.21. See [MySQL](#) (page B-10) for complete information.
- Introduced an option to restore backup to a new system with a new IP address and not retain the old IP address by default. See [Restoring a Backup to a New System with a New or Different IP Address](#) (page 14-25) for complete information.
- Introduced an option to manually add the NAT IP address of the Audit Vault Server into the Audit Vault Agent. See [Adding Network Address Translation IP Addresses to Audit Vault Agent](#) (page 3-23) for complete information.

- Updated the connect string for Microsoft SQL Server (SQL Server Authentication) in section [Secured Target Locations \(Connect Strings\)](#) (page B-36).
- Audit data collection for Oracle Database 12 c Release 2 (12.2) as secured targets is supported on Oracle Audit Vault and Database Firewall release 12.2.0.4.0 and onwards. Updated section [Oracle Database](#) (page B-4).
- Reinstated option to automatically start the Audit Vault Agent as a service on Windows. This functionality was previously removed in release 12.2.0.7.0. It is now restored in release 12.2.0.8.0. See [Registering and Unregistering the Audit Vault Agent as a Windows Service](#) (page 5-7) for complete information.
- Minor updates and correction to ports in sections [Ports for External Network Access by the Audit Vault Server](#) (page D-3), [Ports for Internal TCP Communication](#) (page D-5), and [Ports for Services Provided by Oracle Audit Vault Server](#) (page D-2).
- Added steps to change the IP address of the Database Firewall Server. See [Changing IP Address For A Single Instance Of Database Firewall Server](#) (page 4-7) for complete steps.
- Added some best practices for setting event log properties in section [START COLLECTION FOR SECURED TARGET](#) (page A-26).
- Added an important note on assigning roles to the source user for running the REDO collector with Database Vault. See section [About the Recommended Settings for Collection from REDO Logs](#) (page C-1) for more information.
- Added an important limitation in section [About the Recommended Settings for Collection from REDO Logs](#) (page C-1).
- Added guidelines for [Configuring Audit Trail Collection For CDB And PDB](#) (page 6-19).
- Minor update and correction to the following sections:
 - [Configure and Download the Diagnostics Report File](#) (page 4-13)
 - [Resetting Oracle Database Firewall](#) (page 14-41)
 - [About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall](#) (page 3-12)
 - [Configuring Enforcement Points](#) (page 6-20)
 - [Configuring Oracle Database Firewall for Databases That Use Network Encryption](#) (page 6-29)
 - [Starting an Archive Job](#) (page 14-7)
 - [Managing Database Firewalls](#) (page 14-38)
 - [Setting or Changing the Audit Vault Server Network Configuration](#) (page 3-5)
 - [Multiple Network Interface Cards](#) (page H-1)
- **Micro Focus Security ArcSight SIEM** (previously known as **HP ArcSight SIEM**) is deprecated in 12.2.0.8.0, and will be desupported in 12.2.0.9.0. It is advisable to use the `syslog` integration feature instead.
- In-line bridge mode is deprecated in 12.2.0.8.0, and will be desupported in 19.1.0.0.0. It is advisable to use proxy mode as an alternative.

- See the following sections for an updated list of supported systems and components:
 - [Integrating Oracle Audit Vault and Database Firewall with Third-Party Products](#) (page 1-4)
 - [Integration with Third Party SIEM and Log-data Analysis Tools](#) (page 10-1)
 - [Step 5: Plan Your Integration Options](#) (page 1-9)
 - [About Configuring Oracle Audit Vault Server](#) (page 3-1)
 - [Managing Server Connectors for Email, Syslog, and Arcsight SIEM](#) (page 14-6)
 - [Enabling the HP ArcSight SIEM Integration](#) (page 10-2)
 - [About the Integration of Oracle Audit Vault and Database Firewall with F5 BIG-IP Application Security Manager \(BIG-IP ASM\)](#) (page 9-1)
 - [Configuring a Bridge in the Database Firewall](#) (page 4-9)

E41705-19 (February 2018)

- Included an important note in section [Configure and Download the Diagnostics Report File](#) (page 4-13).
- **F5** is deprecated in release 12.2.0.7.0, and will be desupported in 19.1.0.0.0.

E41705-18 (December 2017)

- Introduced new `AVCLI` commands. See [AVCLI User Commands](#) (page A-65) for complete information.
- Included support for the following versions of Red Hat Enterprise Linux operating system as secured target for audit collection. See [Out-of-the Box Plug-ins at a Glance](#) (page B-2) and [Linux](#) (page B-12) for more information.
 - RHEL 6.7
 - RHEL 6.8
 - RHEL 6.9
 - RHEL 7.1
 - RHEL 7.2
 - RHEL 7.3
- Included support for the following new versions of MySQL with both old and new audit formats. See [Out-of-the Box Plug-ins at a Glance](#) (page B-2), [MySQL](#) (page B-10), and [Converting Audit Record Format For Collection](#) (page 6-14) for more information.
 - 5.5.34 to 5.5.57
 - 5.6.13 to 5.6.37
 - 5.7.0 to 5.7.19
- Included support for AIX 7.2 version as secured target for audit collection. See [Out-of-the Box Plug-ins at a Glance](#) (page B-2) and [IBM AIX](#) (page B-14) for more information.
- Included support of version 12 of SUSE Linux Enterprise Server operating system for Audit Vault Agent and Host Monitor. Updated section [Out-of-the Box Plug-ins at a Glance](#) (page B-2).
- Included support for Microsoft Windows Server (x86-64) 2016 and Active Directory 2016 versions. Updated sections [Microsoft Windows](#) (page B-15), [Microsoft Active Directory](#) (page B-15), and [Out-of-the Box Plug-ins at a Glance](#) (page B-2).

- Starting release 12.2.0.7.0 the *Audit Vault Agent* cannot be registered as a Windows service. You can only unregister the service that was previously registered. See [Unregistering the Audit Vault Agent as a Windows Service](#) (page 5-8) for complete information.
- The user may encounter data overflow issue in the **Audit Vault GUI**. See [Data Overflow Issues in the Oracle Audit Vault UI](#) (page G-28) for detailed information on this problem and for the workaround.
- Included workaround for issue on audit trail stuck in `Starting` status. See section [Oracle Audit Vault Agent is Unreachable and the Transaction Log Audit Trail is Frozen in Starting Status](#) (page G-28) for complete information.
- Included workaround for issue on generating the *agent.jar* file. See [Unable to Install the Agent or Generate the agent.jar File](#) (page G-7) for detailed information.
- Minor updates to section [Configure and Download the Diagnostics Report File](#) (page 4-13).
- Minor correction to supported trail types in section [Summary of Data Collected for Each Audit Trail Type](#) (page B-17).

E41705-16 (September 2017)

Correction to [Resetting Oracle Database Firewall](#) (page 14-41).

E41705-15 (August 2017)

- Included workaround for [Failures Due to Dropping Users](#) (page G-27).
- In case the auto upgrade of the Agent fails due to a connection issue to the Audit Vault Database, it continues to attempt and initiate the auto upgrade process. See [Failure of Agent Automatic Upgrades](#) (page G-27) for more information.
- Included support for collection from DB2 version 11.1. See [Out-of-the Box Plug-ins at a Glance](#) (page B-2) and [IBM DB2](#) (page B-9) for complete information.
- Included important instruction in [Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment And Pre-requisites](#) (page 12-1).
- Update to [Configuring Fiber Channel-Based Storage for Audit Vault Server](#) (page 3-21).
- Update to [Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment](#) (page 12-1).
- Update to [About Setting Transport Layer Security Levels](#) (page 2-6).
- Update to [Deactivating and Removing the Audit Vault Agent](#) (page 5-12).
- Correction to the steps in [Managing A Resilient Audit Vault Server Pair](#) (page 8-2).
- Improved backup and restore process. The user can configure and specify multiple physical disk locations to backup simultaneously. See [Step 1: Configure the Backup Utility](#) (page 14-16) for complete information.
- The user can enable, configure, and modify the way diagnostic report is generated. See [Configure and Download the Diagnostics Report File](#) (page 4-13) for complete information.
- Included important information to [Resetting Oracle Database Firewall](#) (page 14-41) and to [Restore Enforcement Points](#) (page 14-42).

- Included important information in [Step 2: Back Up the Audit Vault Server](#) (page 14-20) and [Some Services May Not Start After Backup](#) (page G-27).
- Included support for the following versions of Oracle Linux operating system as secured targets for audit collection. See [Out-of-the Box Plug-ins at a Glance](#) (page B-2) and [Linux](#) (page B-12) for complete information.
 - OL 6.8
 - OL 6.9
 - OL 7.3
- Included support for Red Hat Enterprise Linux operating system (version 7.0) as secured target for audit collection.
- The user can configure audit trail collection for Oracle Real Application Clusters (Oracle RAC). See the following sections for details:
 - [Configuring Audit Trail Collection for Oracle Real Application Clusters](#) (page 6-18)
 - [About Deploying the Audit Vault Agent](#) (page 5-3)
 - [Registering Secured Targets](#) (page 6-3)

E41705-14 (June 2017)

- Minor update in [Step 4: Configuring Server Network](#) (page 12-16).
- Included workaround for failure of Audit Vault agent installation after performing pairing or separation (un-pairing) of Audit Vault server. See [Audit Vault Agent Installation Fails After HA Pairing Or Separation](#) (page G-23) for more information.
- Included important information on having the same path while performing backup and restore operation. See section [About the Backup and Restore Utility](#) (page 14-14) for more information.
- Included information on rules that must be adhered while archiving and restoring tablespaces. See sections [Configuring Archive Locations and Retention Policies](#) (page 3-11) and [Error in Restoring Files](#) (page G-24).
- Included workaround for DB2 collector failures. See sections [DB2 Collector Fails Due to Source Version NULL Errors](#) (page G-24) and [DB2 Collector Fails Due To Connection or Permission Issue From Database](#) (page G-25) for more information.
- Correction to the procedure in section [Enabling SSH On A Secondary Network Interface Card For Audit Vault Server](#) (page H-5).
- Included workaround for ORA-12660 error. See [ORA-12660 Error While Registering Secured Target](#) (page G-25) for more information. Also updated section [Step 4: Configuring Server Network](#) (page 12-16).
- Including support for **Policy Name** and **Client Program** fields in alerts.
- Updated Oracle Linux versions supported in sections [Out-of-the Box Plug-ins at a Glance](#) (page B-2) and [Linux](#) (page B-12).
- The `SYS.AUD$` and `SYS.FGA_LOG$` tables have an additional column `RLS$INFO`. See sections [Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment And Prerequisites](#) (page 12-1) and [Summary of Data Collected for Each Audit Trail Type](#) (page B-17) for more information.
- Introducing customizable set of cipher levels. See section [About Setting Transport Layer Security Levels](#) (page 2-6) for more information on creating a custom file that defines the cipher levels and to apply the file.

- Introduced `agentctl stop -force` command to forcibly stop the Agent in console mode. See [Stopping and Starting the Agent on Windows Hosts](#) (page 5-9) for more information.
- Introducing Fiber channel based storage. The user can configure this storage during installation. See [Configuring Fiber Channel-Based Storage for Audit Vault Server](#) (page 3-21) for more information.
- Included pointer for [Integrating Oracle Audit Vault and Database Firewall with Oracle Key Vault](#) (page 1-5).
- Updated prerequisites to start Data Encryption process. See [Data Encryption on Upgraded Instances](#) (page 14-10) for more information.
- The AVDF upgrade script provides additional information about the upgrade before prompting the user for confirmation to start.
- Execute high availability pairing prior to archiving of ILM. Else, it may result in an error. See section [Failure During High Availability Pairing in Oracle Audit Vault Server](#) (page G-26) for more information.
- Included important information on updating the Audit Vault Agents. See sections [Updating Audit Vault Agents and Host Monitor Agents After Pairing Audit Vault Servers](#) (page 8-6) and [About Pairing Audit Vault Servers](#) (page 8-3) for more information.
- Included steps to change IP address of an active host. See section [Changing IP Address Of An Active And Registered Host](#) (page 3-8) for more information.
- Introducing `audit_trail_id_idx` index to resolve audit trail performance issues. See [Audit Trail Performance Issues Occur After Audit Vault Server Upgrade](#) (page G-26) for more information on having sufficient disk space while performing Audit Vault Server upgrade if there is huge amount of event data.
- Update to section [Configuring an Interface Masters Niagara Server Adapter Card](#) (page 4-12).
- Windows host monitor is compatible with recent version of *WinPcap*. See [Host Monitor Requirements](#) (page 7-2) for more information.
- The REDO collector can populate `Client_ID` in the **Data Modification Before-After Values Report** or the event log report. See section [Populating Client ID In Reports for REDO Collector](#) (page C-18) for more information.
- Correction to the steps for [Switching Roles in a Resilient Pair of Database Firewalls](#) (page 8-10).
- Included important information for [Configuring A Resilient Database Firewall Pair](#) (page 8-10).
- Update to [Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment](#) (page 12-1).
- MSSQL Server secured target can be used with Windows authentication along with SQL Server authentication. See the following sections for information:
 - [Secured Target Locations \(Connect Strings\)](#) (page B-36)
 - [Setting Up Audit Data Collection Privileges for a SQL Server Secured Target](#) (page B-27)
 - [REGISTER SECURED TARGET](#) (page A-17)
 - [Microsoft SQL Server](#) (page B-6)

E41705-13 (December 2016)

- Included new releases of Oracle Linux OL 7.1 version 2.4.1 and Oracle Linux OL 7.2 version 2.4.1 as supported secured target type. See sections [Out-of-the Box Plug-ins at a Glance](#) (page B-2) and [Linux](#) (page B-12) for details.
- Included host monitoring support for Oracle Linux releases OL 6.0, OL 6.1 to 6.5, and OL 6.6. See section [Out-of-the Box Plug-ins at a Glance](#) (page B-2) for details.
- Update to prerequisites for deploying AVDF Hybrid Cloud in the section [Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment And Pre-requisites](#) (page 12-1). Included *Stored Procedure Auditing* in the table as it is not supported for TCPS connection.
- Update to ARCHIVELOG mode in [Monitoring Server Archive Log Disk Space Use](#) (page 14-29).
- Updated the Audit Vault error messages. See [Message Code Dictionary](#) (page E-1) for more information.
- Minor correction to the procedure in [Step 3: Validate the Backup](#) (page 14-21).
- Included an important note to be followed before performing the upgrade task, if there is a Niagara card in the system. See section [Configuring an Interface Masters Niagara Server Adapter Card](#) (page 4-12) for more information.
- Included an important task that must be completed post upgrading to release 12.2.0.4.0 from 12.2.0.3.0. See [Data Encryption on Upgraded Instances](#) (page 14-10) for more information.
- Included `openssl-devel` as a required package for Linux machines. See [Host Monitor Requirements](#) (page 7-2) for more information.
- Update to the procedure [Updating Audit Vault Agents and Host Monitor Agents After Pairing Audit Vault Servers](#) (page 8-6).
- Included workaround for connection error. See [A Client Is Unable To Connect To The AVS Using SSH With A Secondary Network Interface Card](#) (page G-21) for more information.
- Included workaround for archive or retrieve job submission error. See [First Archive Or Retrieve Job After Upgrade](#) (page G-22) for more information.
- Introducing support for retrieval of data from multiple targets. See the following sections:
 - [Changing Logging Levels and Clearing Diagnostic Logs](#) (page 14-5)
 - [ALTER SYSTEM SET](#) (page A-56)
 - [Running Archive or Retrieve Jobs](#) (page 3-18)
 - [About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall](#) (page 3-12)
 - [Retrieving Oracle Audit Vault and Database Firewall Audit Data](#) (page 14-8)
 - [Creating Archiving \(Retention\) Policies](#) (page 3-17)
 - [Handling new Audit Trails with Expired Audit Records](#) (page 6-13)
 - [Archiving and Retrieving Audit Data](#) (page 14-7)

E41705-12 (August 2016)

- Update to Database STIG rules implemented in Oracle Audit Vault and Database Firewall release 12.2.0.3.0. See [Current Implementation of Database STIG Rules](#) (page F-4) for more information.
- Update to Operating System STIG rules implemented in Oracle Audit Vault and Database Firewall release 12.2.0.3.0. See [Current Implementation of Operating System STIG Rules](#) (page F-13) for more information.
- Included an important pre-requisite for performing restore task. See [Out of Memory Error Message During Restore](#) (page G-18) and [How Much Space Do I Need for Backup Files?](#) (page 14-16) for more information.
- Included workaround for `JAVA.IO.IOEXCEPTION` error. Refer to [JAVA.IO.IOEXCEPTION Error](#) (page G-18) for more information.
- Included workaround for `Failed to start ASM instance` error. Refer to [Failed to Start ASM Instance Error](#) (page G-19) for more information.
- Correction and update to the supported Trail locations for Secured Targets. Refer to [Audit Trail Locations](#) (page B-42) for more information.
- Included workaround for failure while adding a new disk. Refer to [Failure While Adding Disks](#) (page G-17) for more information.
- Included information on STIG recommendations. See [About Security Technical Implementation Guides](#) (page F-1) for more information.
- Ensure the new system has sufficient disk space before performing restore. See [How Much Space Do I Need for Backup Files?](#) (page 14-16) for more information.

Quick Reference for Common Tasks

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

Topics

- [About this Quick Reference](#) (page xlii)
- [Audit Vault Server](#) (page xlii)
 - [System Settings](#) (page xlii)
 - [Archiving and Retrieving](#) (page xlii)
 - [High Availability Pairing of Audit Vault Servers](#) (page xlii)
 - [AVCLI \(Command Line Interface\)](#) (page xliii)
 - [Other Operations](#) (page xliii)
- [Database Firewall](#) (page xliii)
 - [Firewall System Settings](#) (page xliii)
 - [Firewall Network Configuration](#) (page xliii)
 - [Managing Database Firewalls in the Audit Vault Server](#) (page xliv)
 - [High Availability Pairing of Database Firewalls](#) (page xliv)
- [Hosts](#) (page xliv)
- [Agent](#) (page xliv)
 - [Agent Deployment](#) (page xliv)
 - [Updating Agent](#) (page xliv)
- [Host Monitor](#) (page xlv)
 - [Host Monitor Installation](#) (page xlv)
 - [Host Monitor Operations](#) (page xlv)
 - [Updating](#) (page xlv)
 - [Host Monitor Security](#) (page xlv)
- [Secured Targets](#) (page xlv)
 - [Registering and Managing](#) (page xlv)
 - [Auditing](#) (page xlv)
 - [Monitoring with Database Firewall](#) (page xlvi)
- [BIG-IP ASM Integration](#) (page xlvi)
- [Arcsight Integration](#) (page xlvii)

- [Other Administrator Tasks](#) (page xlvii)
- [Reference Information](#) (page xlvii)
 - [Plug-ins](#) (page xlvii)
 - [Other Reference Information](#) (page xlvii)

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](#) (page 1-6) 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](#) (page 3-3)"
- "[Setting or Changing the Audit Vault Server Network Configuration](#) (page 3-5)"
- "[Changing the UI \(Console\) Certificate for Oracle Audit Vault Server](#) (page 3-2)"
- "[Configuring or Changing the Oracle Audit Vault Server Services](#) (page 3-7)"
- "[Configuring Oracle Audit Vault Server Syslog Destinations](#) (page 3-8)"
- "[Configuring Email Notification for Oracle Audit Vault and Database Firewall](#) (page 3-11)"
- "[Testing Audit Vault Server System Operations](#) (page 3-21)"
- "[Data Encryption on Upgraded Instances](#) (page 14-10)"

Archiving and Retrieving

- "[Defining Archive Locations](#) (page 3-13)"
- "[Creating Archiving \(Retention\) Policies](#) (page 3-17)"
- "[Deleting Archiving Policies](#) (page 3-18)"
- "[Starting an Archive Job](#) (page 14-7)"
- "[Retrieving Oracle Audit Vault and Database Firewall Audit Data](#) (page 14-8)"

High Availability Pairing of Audit Vault Servers

- "[Configure the Secondary Audit Vault Server](#) (page 8-4)"
- "[Configure the Primary Audit Vault Server](#) (page 8-5)"
- "[Checking the High Availability Status of an Audit Vault Server](#) (page 8-6)"
- "[Updating Audit Vault Agents and Host Monitor Agents After Pairing Audit Vault Servers](#) (page 8-6)"

["Disabling or Enabling Failover of the Audit Vault Server \(page 8-9\)"](#)

["Performing a Manual Failover of the Audit Vault Server \(page 8-9\)"](#)

AVCLI (Command Line Interface)

["Downloading the AVCLI Command Line Utility and Setting JAVA_HOME \(page 14-33\)"](#)

["Starting AVCLI \(page 14-33\)"](#)

["Displaying Help and the Version Number of AVCLI \(page 14-37\)"](#)

["Running AVCLI Scripts \(page 14-36\)"](#)

["Specifying Log Levels for AVCLI \(page 14-37\)"](#)

["AVCLI Commands Reference \(page A-1\)"](#)

Other Operations

["Backing Up and Restoring the Audit Vault Server \(page 14-14\)"](#)

["Rotating the Master Key for Repository Encryption \(page 14-9\)"](#)

["Changing the Keystore Password \(page 14-9\)"](#)

["Enabling Oracle Database In-Memory for the Audit Vault Server \(page 14-26\)"](#)

["Monitoring Jobs \(page 14-31\)"](#)

["Checking Server Status and System Operation \(page 14-2\)"](#)

["Accessing the Audit Vault Server Certificate and Public Key \(page 14-4\)"](#)

["Rebooting or Powering Off the Audit Vault Server \(page 14-6\)"](#)

["Changing the Keyboard Layout \(page 14-6\)"](#)

["Running Diagnostics Checks for the Audit Vault Server \(page 14-2\)"](#)

Database Firewall

Firewall System Settings

["Configuring Network Settings For A Database Firewall \(page 4-3\)"](#)

["Configuring Network Services For A Database Firewall \(page 4-4\)"](#)

["Setting the Date and Time in the Database Firewall \(page 4-5\)"](#)

["Specifying the Audit Vault Server Certificate and IP Address \(page 4-6\)"](#)

["Viewing the Status and Diagnostics Report for a Database Firewall \(page 4-12\)"](#)

Firewall Network Configuration

["Configuring Traffic Sources \(page 4-9\)"](#)

["Configuring a Bridge in the Database Firewall \(page 4-9\)"](#)

["Configuring Oracle Database Firewall As A Traffic Proxy \(page 4-11\)"](#)

["Viewing Network Traffic in a Database Firewall \(page 14-39\)"](#)

Managing Database Firewalls in the Audit Vault Server

["Registering Database Firewall in Audit Vault Server \(page 3-20\)"](#)

["Restarting or Powering Off Oracle Database Firewall \(page 14-40\)"](#)

["Removing Oracle Database Firewall from Oracle Audit Vault Server \(page 14-40\)"](#)

["Fetching an Updated Certificate from Oracle Database Firewall \(page 14-40\)"](#)

High Availability Pairing of Database Firewalls

["Configuring A Resilient Database Firewall Pair \(page 8-10\)"](#)

["Switching Roles in a Resilient Pair of Database Firewalls \(page 8-10\)"](#)

["Breaking \(Un-pairing\) a Resilient Pair of Database Firewalls \(page 8-11\)"](#)

Hosts

["Registering Hosts in the Audit Vault Server \(page 5-2\)"](#)

["Changing Host Names \(page 5-3\)"](#)

["Deleting Hosts from the Audit Vault Server \(page 5-16\)"](#)

["Deploying Plug-ins and Registering Plug-in Hosts \(page 5-13\)"](#)

["Un-Deploying Plug-ins \(page 5-15\)"](#)

Agent

Agent Deployment

["Steps Required to Deploy and Activate the Audit Vault Agent \(page 5-5\)"](#)

["Deploying the Audit Vault Agent on the Host Computer \(page 5-5\)"](#)

["Activating and Starting the Audit Vault Agent \(page 5-6\)"](#)

["Unregistering the Audit Vault Agent as a Windows Service \(page 5-8\)"](#)

["Stopping and Starting the Agent on Unix Hosts \(page 5-9\)"](#)

["Stopping and Starting the Agent on Windows Hosts \(page 5-9\)"](#)

["Changing the Logging Level for the Audit Vault Agent \(page 5-11\)"](#)

["Deactivating and Removing the Audit Vault Agent \(page 5-12\)"](#)

Updating Agent

["Updating Oracle Audit Vault Agent \(page 5-12\)"](#)

Host Monitor

Host Monitor Installation

- "[Register the Computer that will Run the Host Monitor](#) (page 7-3)"
- "[Deploying the Agent and Host Monitor on Microsoft Windows Hosts](#) (page 7-3)" or "[Deploying the Agent and Host Monitor on Unix Hosts](#) (page 7-6)"
- "[Create a Secured Target for the Host-Monitored Database](#) (page 7-7)"
- "[Create an Enforcement Point for the Host Monitor](#) (page 7-7)"

Host Monitor Operations

- "[Starting the Host Monitor](#) (page 7-9)"
- "[Stopping the Host Monitor](#) (page 7-9)"
- "[Changing the Logging Level for a Host Monitor](#) (page 7-10)"
- "[Checking the Status of a Host Monitor Audit Trail](#) (page 7-10)"
- "[Uninstalling the Host Monitor \(Unix Hosts Only\)](#) (page 7-10)"

Updating

- "[Updating the Host Monitor \(Unix Hosts Only\)](#) (page 7-11)"

Host Monitor Security

- "[Using Certificate-based Authentication for the Host Monitor](#) (page 7-11)"

Secured Targets

Registering and Managing

- "[Registering Secured Targets](#) (page 6-3)"
- "[Removing Secured Targets](#) (page 6-5)"
- "[Creating or Modifying Secured Target Groups](#) (page 6-6)"
- "[Managing User Access Rights to Secured Targets or Groups](#) (page 13-7)"

Auditing

Preparing for Auditing

- "[Preparing Secured Targets for Audit Data Collection](#) (page 6-7)"
- "[Using an NTP Service to set Time on Secured Targets](#) (page 6-7)"
- "[Ensuring that Auditing is Enabled on the Secured Target](#) (page 6-8)"
- "[Setting User Account Privileges on Secured Targets](#) (page 6-8)"

["Scheduling Audit Trail Cleanup \(page 6-9\)"](#)

Audit Trails

["Adding an Audit Trail in the Audit Vault Server \(page 6-9\)"](#)

["Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server \(page 6-11\)"](#)

["Checking the Status of Audit Trails in the Audit Vault Server \(page 6-12\)"](#)

["Deleting an Audit Trail \(page 6-14\)"](#)

["Converting Audit Record Format For Collection \(page 6-14\)"](#)

Monitoring with Database Firewall

Enforcement Points

["Creating and Configuring an Enforcement Point \(page 6-20\)"](#)

["Modifying an Enforcement Point \(page 6-22\)"](#)

["Starting, Stopping, or Deleting Enforcement Points \(page 6-23\)"](#)

["Viewing the Status of Enforcement Points \(page 6-23\)"](#)

["Finding the Port Number Used by an Enforcement Point \(page 6-24\)"](#)

Database Interrogation and Response Monitoring

["Configuring and Using Database Interrogation \(page 6-24\)"](#)

["Configuring Database Interrogation for SQL Server and SQL Anywhere \(page 6-26\)"](#)

["Configuring Oracle Database Firewall for Databases That Use Network Encryption \(page 6-29\)"](#)

["Enabling Database Interrogation \(page 6-27\)"](#)

["Disabling Database Interrogation \(page 6-28\)"](#)

["Configuring Database Response Monitoring \(page 6-33\)"](#)

See also: ["Database Firewall \(page xlili\)"](#)

BIG-IP ASM Integration

[Configuring Oracle Audit Vault and Database Firewall to Work with F5 BIG-IP Application Security Manager \(page 9-4\)](#)

[Configuring F5 BIG-IP Application Security Manager \(page 9-5\)](#)

[Developing a F5 BIG-IP Application Security Manager iRule \(page 9-7\)](#)

 **Note:**

- **F5 BIG-IP ASM** integration is deprecated in release 12.2.0.7.0, and will be desupported in 19.1.0.0.0.
- This functionality is only supported on **F5 BIG-IP ASM** version 10.2.1.

Arcsight Integration

[Enabling the HP ArcSight SIEM Integration](#) (page 10-2)

 **Note:**

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

Other Administrator Tasks

["Downloading the Oracle Audit Vault and Database Firewall SDK](#) (page 14-38)"

["Monitoring Server Tablespace Space Usage](#) (page 14-29)"

["Monitoring Server Archive Log Disk Space Use](#) (page 14-29)"

["Monitoring Server Flash Recovery Area](#) (page 14-30)"

["Backing Up and Restoring the Audit Vault Server](#) (page 14-14)"

Reference Information

Plug-ins

[Out-of-the Box Plug-ins at a Glance](#) (page B-2)

[Summary of Data Collected for Each Audit Trail Type](#) (page B-17)

[Scripts for Oracle AVDF Account Privileges on Secured Targets](#) (page B-21)

[Audit Trail Cleanup](#) (page B-32)

[Secured Target Locations \(Connect Strings\)](#) (page B-36)

[Collection Attributes](#) (page B-38)

[Audit Trail Locations](#) (page B-42)

Other Reference Information

[AVCLI Commands Reference](#) (page A-1)

[REDO Logs Audit Data Collection Reference](#) (page C-1)

[Ports Used by Audit Vault and Database Firewall](#) (page D-1)

[Troubleshooting Oracle Audit Vault and Database Firewall](#) (page G-1)

Part I

Getting Started

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

This part contains the following chapters:

- [Introducing Oracle Audit Vault and Database Firewall](#) (page 1-1)
- [General Security Guidelines](#) (page 2-1)
- [Configuring the Audit Vault Server](#) (page 3-1)
- [Configuring the Database Firewall](#) (page 4-1)
- [Registering Hosts and Deploying the Agent](#) (page 5-1)
- [Configuring Secured Targets, Audit Trails, and Enforcement Points](#) (page 6-1)
- [Enabling and Using Host Monitoring](#) (page 7-1)
- [Configuring High Availability](#) (page 8-1)
- [Configuring Integration with BIG-IP ASM](#) (page 9-1)
- [Integration with Third Party SIEM and Log-data Analysis Tools](#) (page 10-1)

1

Introducing Oracle Audit Vault and Database Firewall

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

Topics

- [Downloading the Latest Version of This Manual](#) (page 1-1)
- [Learning About Oracle AVDF](#) (page 1-1)
- [Supported Platforms for Oracle Audit Vault and Database Firewall](#) (page 1-1)
- [System Features](#) (page 1-2)
- [Understanding the Administrator's Role](#) (page 1-5)
- [Summary of Configuration Steps](#) (page 1-6)
- [Planning the System Configuration](#) (page 1-7)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)
- [Logging in to the Database Firewall Console UI](#) (page 1-13)
- [Using the Audit Vault Command-Line Interface](#) (page 1-15)
- [Using the Audit Vault and Database Firewall Enterprise Manager Plug-in](#) (page 1-16)

1.1 Downloading the Latest Version of This Manual

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

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

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

<http://docs.oracle.com>

1.2 Learning About Oracle AVDF

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

1.3 Supported Platforms for Oracle Audit Vault and Database Firewall

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

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

1.4 System Features

Topics

- [About Audit Vault and Database Firewall](#) (page 1-2)
- [Security Technical Implementation Guides and Implementation for Oracle Audit Vault and Database Firewall](#) (page 1-2)
- [System Requirements for Oracle Audit Vault and Database Firewall](#) (page 1-3)
- [Supported Secured Targets](#) (page 1-3)
- [Administrative Features](#) (page 1-3)
- [Oracle Audit Vault and Database Firewall Auditing Features](#) (page 1-4)
- [Integrating Oracle Audit Vault and Database Firewall with Third-Party Products](#) (page 1-4)

1.4.1 About Audit Vault and Database Firewall

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

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

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

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

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.

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

Learn about Oracle Audit Vault and Database Firewall compliance with Security Technical Implementation Guides (STIG) standards.

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

**See Also:**

[Security Technical Implementation Guides](#) (page F-1)

1.4.3 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*.

1.4.4 Supported Secured Targets

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

Oracle AVDF supports various secured target products out of the box in the form of built-in plug-ins.

**See Also:**

- [About Plug-ins](#) (page 5-13)
- [Plug-in Reference](#) (page B-1) for detailed information on each plug-in.
- [Table B-1](#) (page B-2) for supported secured target products and versions.
- [Table B-17](#) (page B-18) for the data collected and platforms supported for each audit trail type.

**See Also:**

- *Oracle Audit Vault and Database Firewall Developer's Guide* for information on creating custom plug-ins to capture audit trails from more secured target types using the Oracle AVDF SDK.
- *Oracle Big Data Appliance Owner's Guide* for more information on Oracle Big Data Appliance as a secured target on Oracle Audit Vault and Database Firewall.

1.4.5 Administrative Features

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

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

1.4.6 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

See Also:

Oracle Audit Vault and Database Firewall Auditor's Guide for detailed information about these auditing features

1.4.7 Integrating Oracle Audit Vault and Database Firewall with Third-Party Products

Learn about integrating Oracle Audit Vault and Database Firewall with third-party products.

You can integrate Oracle Audit Vault and Database Firewall with the following third-party products:

- **F5 BIG-IP Application Security Manager (ASM):** This product, from F5 Networks, Inc., is an advanced web application firewall that provides comprehensive edge-of-network protection against a wide range of web-based attacks. ASM analyzes each HTTP and HTTPS request and blocks potential attacks before they reach the web application server.

 **Note:**

- This functionality is only supported on F5 BIG-IP ASM version 10.2.1.
 - F5 BIG-IP ASM integration is deprecated in release 12.2.0.7.0, and will be desupported in 19.1.0.0.0.
- Micro Focus Security ArcSight SIEM: This product is a centralized system for logging, analyzing, and managing syslog messages from different sources.

 **Note:**

ArcSight Enterprise Security Manager (ESM) Security Information and Event Management (SIEM) (previously known as HP ArcSight SIEM) is deprecated in 12.2.0.8.0 and is desupported in 12.2.0.9.0. Use the `syslog` integration feature instead.

 **See Also:**

- [Configuring Integration with BIG-IP ASM](#) (page 9-1) for more information on integrating with F5 BIG-IP Application Security Manager.
- [Integration with Third Party SIEM and Log-data Analysis Tools](#) (page 10-1) for more information on integrating with ArcSight Enterprise Security Manager (ESM) Security Information and Event Management (SIEM).

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

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

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

1.5 Understanding the Administrator's Role

Oracle AVDF Administrator Tasks

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

- Configuring system settings on the Audit Vault Server
- Configuring connections to the host computers where the Audit Vault Agent is deployed (usually the same computer as the secured targets)
- Creating secured targets in the Audit Vault Server for each database or operating system you are monitoring

- Deploying and activating the Audit Vault Agent on the secured target host computers
- Configuring audit trails for secured targets that are monitored by the Audit Vault Agent
- Configuring Database Firewalls on your network
- Creating enforcement points for secured targets that are monitored by a Database Firewall.
- Backing up and archiving audit and configuration data
- Creating administrator users and managing access (super administrator only)

Administrator Roles in Oracle AVDF

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

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

1.6 Summary of Configuration Steps

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

- [Configuring Oracle AVDF and Deploying the Audit Vault Agent](#) (page 1-6)
- [Configuring Oracle AVDF and Deploying the Database Firewall](#) (page 1-7)

1.6.1 Configuring Oracle AVDF and Deploying the Audit Vault Agent

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

1. Configure the Audit Vault Server. See "[Configuring the Audit Vault Server](#) (page 3-1)".
2. Register the host computers where you will deploy the Audit Vault Agent. Then deploy and activate the Audit Vault Agent on those hosts. See "[Registering Hosts and Deploying the Agent](#) (page 5-1)".
3. Create user accounts on your secured targets for Oracle AVDF to use. See "[Scripts for Oracle AVDF Account Privileges on Secured Targets](#) (page B-21)".
4. Register the secured targets you are monitoring with the agent in the Audit Vault Server, and configure audit trails for these secured targets. See "[Configuring Secured Targets, Audit Trails, and Enforcement Points](#) (page 6-1)".

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

1.6.2 Configuring Oracle AVDF and Deploying the Database Firewall

The general workflow for configuring Oracle AVDF and deploying the Database Firewall is as follows:

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

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

1.7 Planning the System Configuration

Topics

- [Guidance for Planning Your Oracle Audit Vault and Database Firewall Configuration](#) (page 1-7)
- [Step 1: Plan Your Oracle Audit Vault Server Configuration](#) (page 1-8)
- [Step 2: Plan the Database Firewall Configuration](#) (page 1-8)
- [Step 3: Plan the Audit Vault Agent Deployments](#) (page 1-8)
- [Step 4: Plan the Audit Trail Configurations](#) (page 1-9)
- [Step 5: Plan Your Integration Options](#) (page 1-9)
- [Step 6: Plan for High Availability](#) (page 1-10)
- [Step 7: Plan User Accounts and Access Rights](#) (page 1-10)

1.7.1 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](#) (page 1-7) for guidance on planning deployments of Oracle Audit Vault Server, Oracle Audit Vault Agent, and Oracle Database Firewall.

1.7.2 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 the Audit Vault Server](#) (page 3-1) for information on the Oracle Audit Vault Server configuration settings.
- [Configuring High Availability](#) (page 8-1) for information about setting up resilient pairs of Oracle Audit Vault Servers.

1.7.3 Step 2: Plan the Database Firewall Configuration

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

 **See Also:**

- [Configuring the Database Firewall](#) (page 4-1) for information on the Database Firewall configuration settings.
- [Configuring High Availability](#) (page 8-1) for information on setting up resilient pairs of firewalls.

1.7.4 Step 3: Plan the Audit Vault Agent Deployments

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

 **See Also:**

- [Registering Hosts and Deploying the Agent](#) (page 5-1)
- [Registering Secured Targets and Creating Groups](#) (page 6-2)

1.7.5 Step 4: Plan the Audit Trail Configurations

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

To plan the secured target audit trail configuration:

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

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

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

3. Determine what type of audit trail to collect.

[Table B-17](#) (page B-18) lists the types of audit trails that can be configured for each secured target type and supported platforms.

4. Familiarize yourself with the procedures to register a secured target and configure an audit trail.
5. If you are collecting audit data from MySQL or IBM DB2 secured targets, there are additional steps you need to take.

 **See Also:**

- *Oracle Audit Vault and Database Firewall Auditor's Guide* for more information about the secured target requirements.
- [Deploying and Activating the Audit Vault Agent on Host Computers](#) (page 5-3)
- [Registering Secured Targets and Creating Groups](#) (page 6-2)
- [Configuring and Managing Audit Trail Collection](#) (page 6-9)
- [Converting Audit Record Format For Collection](#) (page 6-14)

1.7.6 Step 5: Plan Your Integration Options

Learn how to plan your integration options.

You can integrate Oracle Audit Vault and Database Firewall with the following third-party products:

- **F5 BIG-IP Application Security Manager (ASM), from F5 Networks, Inc.**

 **Note:**

- This functionality is only supported on **F5 BIG-IP ASM** version 10.2.1.
- **F5 BIG-IP ASM** integration is deprecated in release 12.2.0.7.0, and will be desupported in 19.1.0.0.0.

- **ArcSight Security Information Event Management (SIEM)**

 **Note:**

Micro Focus Security ArcSight SIEM is deprecated in 12.2.0.8.0 and is desupported in 12.2.0.9.0. Use the `syslog` integration feature instead.

 **See Also:**

- [Configuring Integration with BIG-IP ASM](#) (page 9-1)
- [Integration with Third Party SIEM and Log-data Analysis Tools](#) (page 10-1)

1.7.7 Step 6: Plan for High Availability

In this step, consider the high availability options outlined in "[Configuring High Availability](#) (page 8-1)".

1.7.8 Step 7: Plan User Accounts and Access Rights

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

 **See Also:**

[Managing User Accounts and Access](#) (page 13-1)

1.8 Logging in to the Audit Vault Server Console UI

Topics

- [Log in to Oracle Audit Vault Server Console](#) (page 1-11)
- [Understanding the Tabs and Menus in the Audit Vault Server Console](#) (page 1-11)
- [Working with Lists of Objects in the UI](#) (page 1-12)

1.8.1 Log in to Oracle Audit Vault Server Console

Learn how to log in to Oracle Audit Vault Server Console.

When you first log in after installing Oracle Audit Vault Server, you must set up a password.



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 Oracle Audit Vault Server](#) (page 3-2) 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.

1.8.2 Understanding the Tabs and Menus in the Audit Vault Server Console

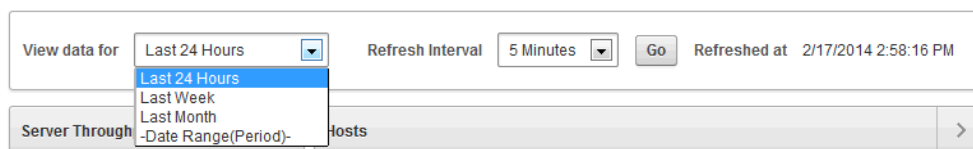
The Audit Vault Server console UI includes the following five tabs:

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

- Server Throughput
- Disks Usage
- CPU
- RAM
- Hosts
- Database Firewalls

At the top of the page, you can select the time range for the data displayed and the refresh interval, as shown in [Figure 1-1](#) (page 1-12).

Figure 1-1 Selecting the Time Range for the Dashboard in the Home Tab



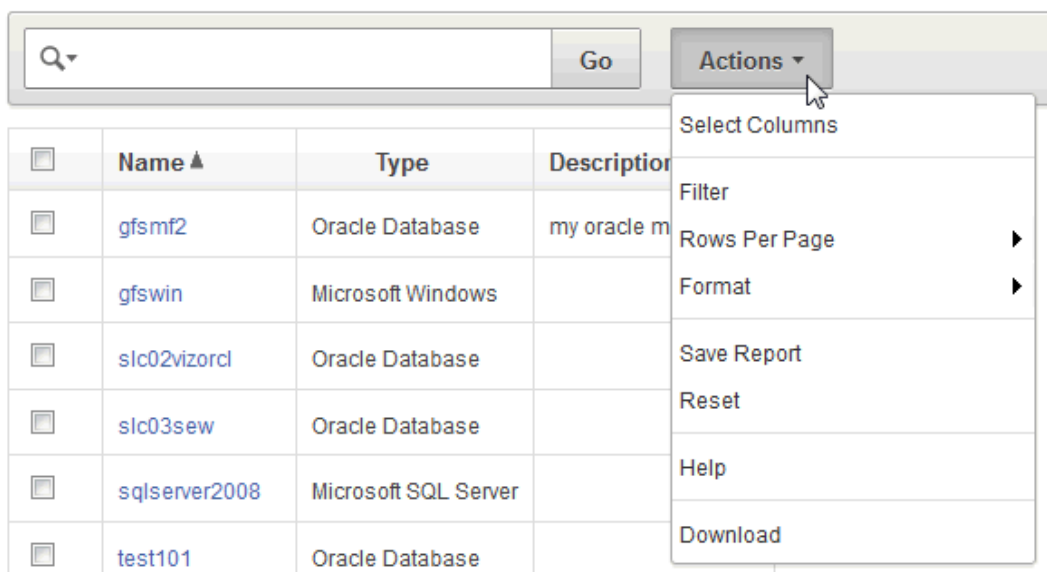
- **Secured Targets** - Provides menus for registering secured targets, managing secured target groups, managing access rights, and monitoring audit trails and enforcement points.
- **Hosts** - Provides menus for registering and managing host computers (where the agent is deployed), and downloading and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

1.8.3 Working with Lists of Objects in the UI

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

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

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



2. To find an item in the list, enter its name in the search box, and then click **Go**.
3. To customize the list, from the **Actions** menu, select any of the following:
 - **Select Columns:** Select which columns to display.
 - **Filter:** Filter the list by column or by row using regular expressions with the available operators. When done, click **Apply**.
 - **Rows Per Page:** - Select the number of rows to display per page.
 - **Format:** Format the list by selecting from the following options:
 - **Sort**
 - **Control Break**
 - **Highlight**
 - **Compute**
 - **Aggregate**
 - **Chart**
 - **Group By**
 Fill in the criteria for each option as needed and click **Apply**.
 - **Save Report:** Save the current view of the list. Enter a name and description and click **Apply**.
 - **Reset:** Reset the list to the default view.
 - **Help:** Display the online help.
 - **Download:** Download the list. Select the download format (CSV or HTML) and click **Apply**.

1.9 Logging in to the Database Firewall Console UI

Topics

- [Log in to the Database Firewall Console UI](#) (page 1-14)

- [Using the Oracle Database Firewall UI](#) (page 1-15)

1.9.1 Log in to the Database Firewall Console UI

When you first log in after installing the Database Firewall, you are required to set up a password.



See Also:

Oracle Audit Vault and Database Firewall Installation Guide for information on post-installation tasks.

To log in to the Database Firewall Console UI:

1. From a browser, enter the following URL:

```
https://host/
```

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

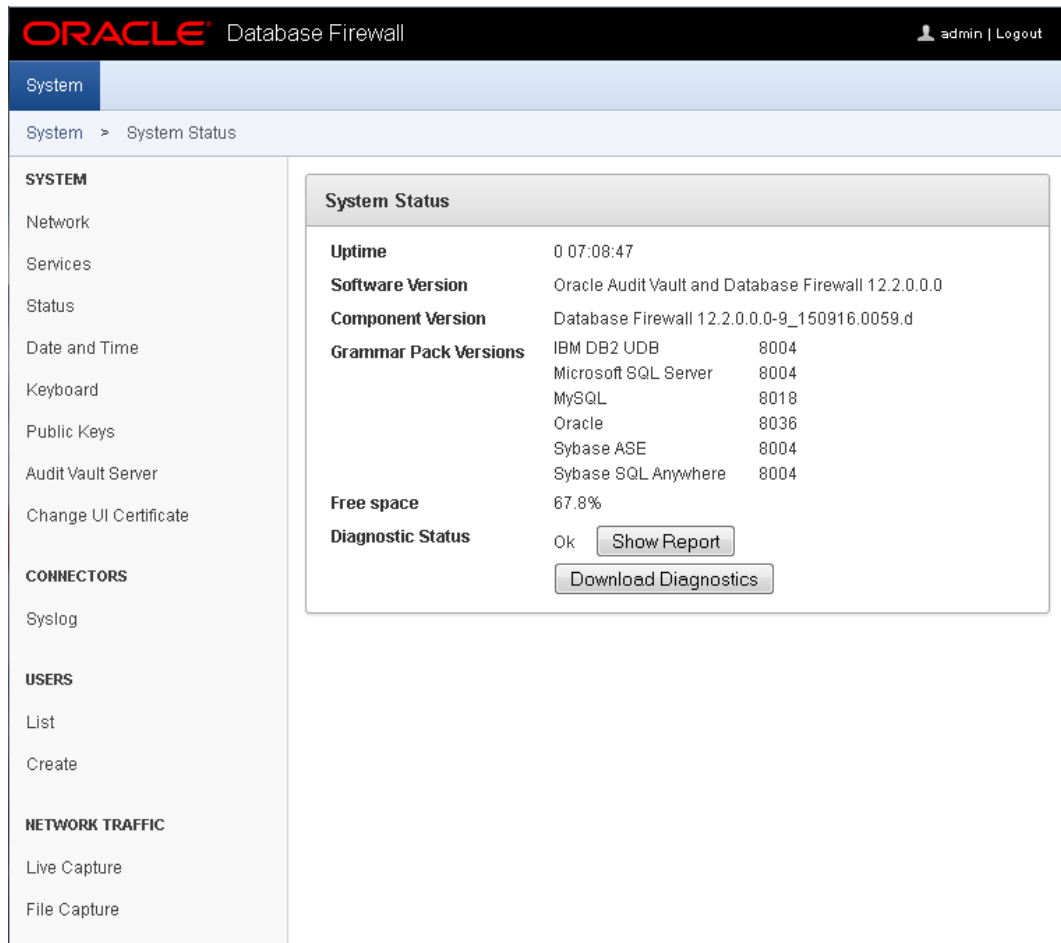
For example:

```
https://192.0.2.2/
```

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

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

The Dashboard page appears, similar to the following:



ORACLE Database Firewall admin | Logout

System > System Status

SYSTEM

- Network
- Services
- Status
- Date and Time
- Keyboard
- Public Keys
- Audit Vault Server
- Change UI Certificate

CONNECTORS

- Syslog

USERS

- List
- Create

NETWORK TRAFFIC

- Live Capture
- File Capture

System Status

Uptime	0 07:08:47
Software Version	Oracle Audit Vault and Database Firewall 12.2.0.0.0
Component Version	Database Firewall 12.2.0.0.0-9_150916.0059.d
Grammar Pack Versions	IBM DB2 UDB 8004
	Microsoft SQL Server 8004
	MySQL 8018
	Oracle 8036
	Sybase ASE 8004
	Sybase SQL Anywhere 8004
Free space	67.8%
Diagnostic Status	Ok <input type="button" value="Show Report"/>
	<input type="button" value="Download Diagnostics"/>

1.9.2 Using the Oracle Database Firewall UI

Learn about using the Oracle Database Firewall UI.

As administrator, use the Oracle Database Firewall UI to configure the network, services, and system settings on Oracle Database Firewall. Also use the Oracle Database Firewall UI to identify the Oracle Audit Vault Server that manages each firewall. Also use it to configure network traffic sources so that the firewall can monitor or block threats to your target databases.

See Also:

[Configuring the Database Firewall](#) (page 4-1) for detailed information on configuring the Oracle Database Firewall using the Database Firewall console UI

1.10 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.

 **See Also:**

- [Downloading and Using the AVCLI Command Line Interface](#) (page 14-32) for information on downloading and using AVCLI
- [AVCLI Commands Reference](#) (page A-1) for details of available commands and syntax

1.11 Using the Audit Vault and Database Firewall Enterprise Manager Plug-in

If you have Oracle Enterprise Manager Cloud Control installed, you can install Oracle Audit Vault and Database Firewall plug-in. This plug-in can be used to manage and monitor Oracle Audit Vault and Database Firewall through the Enterprise Manager.

The following tasks can be performed:

- View Audit Vault and Database Firewall topology
- Monitor availability and performance of Audit Vault components
- Provision Audit Vault Agent on Secured Targets
- Initialize and integrate Audit Vault and Database Firewall with Secured Targets including Oracle Database, Hosts, and Audit Trails for Hosts as well as Oracle Database.
- Perform discovery of sensitive columns on Secured Targets
- Monitor Secured 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	<ul style="list-style-type: none"> • Restart • Delete • Power Off
Audit Vault Agent	<ul style="list-style-type: none"> • Activate • Deactivate • Delete • Start • Stop
Enforcement Point	<ul style="list-style-type: none"> • Start • Stop • Delete
Audit Trail	<ul style="list-style-type: none"> • Start • Stop • Delete
Secure Target	<ul style="list-style-type: none"> • Delete

Related Topics

- [Managing Oracle AVDF in Cloud Control](#)
- [Manually Installing the Enterprise Manager Management Agent](#)

2

General Security Guidelines

Topics

- [Installing Securely and Protecting Your Data](#) (page 2-1)
- [General Security Recommendations](#) (page 2-2)
- [Considerations for Deploying Network-Based Solutions](#) (page 2-3)
- [How Oracle AVDF Works with Various Database Access Paths](#) (page 2-4)
- [Security Considerations for Special Configurations](#) (page 2-4)

2.1 Installing Securely and Protecting Your Data

Topics

- [Installing Oracle Audit Vault and Database Firewall Securely](#) (page 2-1)
- [Protecting Your Data](#) (page 2-1)

2.1.1 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.

2.1.2 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.

2.2 General Security Recommendations

Oracle recommends that you follow these security recommendations:

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

2.3 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

2.4 Considerations for Deploying Network-Based Solutions

Topics

- [Managing Database Firewall Network Encryption](#) (page 2-3)
- [Handling Server-Side SQL and Context Configurations](#) (page 2-3)

2.4.1 Managing Database Firewall Network Encryption

Learn about handling Database Firewall network encryption.

You deploy Database Firewall between the database tier and application tier. Database Firewall can decrypt traffic to and from an Oracle Database when you use Oracle Native Network Encryption. For non-Oracle databases, and for Oracle Databases that use TLS network encryption, if SQL traffic between the database tier and application tier is encrypted, then Database Firewall cannot interpret or enforce protection policies on this SQL traffic.

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

2.4.2 Handling Server-Side SQL and Context Configurations

This section is relevant to the Database Firewall.

The Database Firewall policy enforcement relies on capturing and understanding SQL traffic between the database client and server. Because the Database Firewall only analyzes network traffic between the application tier and the database server, be aware that it cannot see SQL that is directly invoked from the database server itself. Some of the common types of SQL statements that the Database Firewall cannot see are system-provided and user-defined SQL executed from stored procedures and callouts, SQL executed from background jobs such as those that were created by the `DBMS_JOB` or `DBMS_SCHEDULER` PL/SQL packages in Oracle databases, or SQL that is indirectly executed from DDLs or other SQL statements. You can use the auditing features in Oracle AVDF to capture these types of SQL statements.

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

2.5 How Oracle AVDF Works with Various Database Access Paths

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

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

2.6 Security Considerations for Special Configurations

Topics

- [Database Firewall Configuration for Oracle Database Target Configured in Shared Server Mode](#) (page 2-4)
- [How TCP Invited Nodes Are Affected by Client IP Addresses](#) (page 2-5)
- [Additional Behavior to be Aware Of](#) (page 2-5)
- [Custom Collector Development](#) (page 2-6)

2.6.1 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

2.6.2 How TCP Invited Nodes Are Affected by Client IP Addresses

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

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

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

See Also:

- [Configuring a Bridge in the Database Firewall](#) (page 4-9) for more information on Database Firewall's IP address.
- *Oracle Audit Vault and Database Firewall Auditor's Guide* for more information about profiles.

2.6.3 Additional Behavior to be Aware Of

- **Client-side context.** Database Firewall policies can be configured to use client-side context information such as client program name, client OS username, etc. After the client transmits this information to the database server, the Database Firewall captures it

from the network. The Database Firewall does not control or enforce the integrity of the client side or network; the integrity of this information must be considered before using it to define a security policy.

- **Multiple databases and services on a shared listener.** The Database Firewall supports policies based on Oracle Database service names. For non-Oracle databases, the Database Firewall enforces policies that are based on the IP address and port number. In a configuration where a single listener endpoint (*IP_address:port*) is shared among multiple databases, the Database Firewall cannot differentiate traffic directed to each individual database.

2.6.4 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.

2.7 About Setting Transport Layer Security Levels

Learn about setting Transport Layer Security (TLS) levels.

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

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

- Connection between Oracle Audit Vault Server and the Agent or Host Monitor (from release 12.2.0.9.0)
- Connection between Host Monitor and Oracle Database Firewall (from release 12.2.0.9.0)

- Connection between Oracle Audit Vault Server and Database Firewall
- Oracle Audit Vault Server and Database Firewall GUI

 **Note:**

- Ensure that the host machine has `OpenSSL 1.0.1` (or later) installed for Oracle Audit Vault Agent or Host Monitor.
- If any agent is using `Java 1.6`, then upgrade the `Java` version to `1.8`.

Connection Encryption Strength Used On Oracle Audit Vault and Database Firewall 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: If any Audit Vault Agent has to be deployed on <i>IBM AIX</i> , then set the TLS level to <i>Level-3</i> or below.
Level-3	TLSv1.2	This level supports everything that <i>Level-4</i> does.
Level-2 (Default on upgrade)	TLSv1.2 TLSv1.1	This level adds support for legacy and deprecated ciphers. Note: <ul style="list-style-type: none"> • It is recommended to upgrade the TLS level to Level-4 (page 2-7) instead of the default. • The upgrade process does not change the TLS level to default in case the user has changed or set the value of TLS level manually in previous releases.
Level-1 (Custom)	TLSv1.2	This is a customizable cipher set that is configured with <i>Level-4</i> strength by default.

How To Change TLS Levels and Other Tasks

Task	Command	Detailed Information
To check the existing TLS levels for Audit Vault Server and Database Firewall.	<code>cat /usr/local/dbfw/etc/dbfw.conf grep CIPHER_LEVEL</code>	Use this command to check the actual configuration of the Audit Vault Server and Database Firewall.

Task	Command	Detailed Information
To set the TLS level and to find more options.	<code>/usr/local/dbfw/bin/priv/ configure-networking --help</code>	By default, on a new installation the TLS level is set to <i>Level-4</i> . On upgrade it is set to <i>Level-2</i> 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.
To set TLS level for the AVS GUI.	<code>/usr/local/dbfw/bin/priv/ configure-networking --wui- tls-cipher-level [LEVEL]</code>	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.
To set TLS level for communication between Audit Vault Server and Database Firewall.	<code>/usr/local/dbfw/bin/priv/ configure-networking -- internal-tls-cipher-level [LEVEL]</code>	This command sets the desired TLS level and restarts the internal services. The levels can be set to 1, 2, 3, or 4.
To set the TLS level for Audit Vault Agent to Audit Vault Server, and Host Monitor to Database Firewall communication.	<code>/usr/local/dbfw/bin/priv/ configure-networking --agent- tls-cipher-level [LEVEL]</code>	This command sets the TLS level for communication between the Audit Vault Agent to Audit Vault Server, and Host Monitor 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 <code>configure-networking</code> command: 1. Log in to the Audit Vault Server console as <i>root</i> user. 2. Change the directory by using the command: <code>cd /usr/local/dbfw/bin/priv</code> 3. Execute the script using the command: <code>./send_agent_update_signal.sh</code> This command must not be executed more than once in a period of one hour.

Task	Command	Detailed Information
To apply customized cipher set.	<pre>/usr/local/dbfw/bin/priv/ configure-networking --wui- tls-cipher-level 1 -- internal-tls-cipher-level 1 --agent-tls-cipher-level 1</pre>	<p>By default, on a new installation the product is set to <i>Level-4</i>. On upgrade it is set to <i>Level-2</i>. This is appropriate to most of the situations. It is possible to customize.</p> <p>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.</p> <p>Note: Before executing this command verify the error output in the system log file available at <code>/var/log/messages</code> to confirm that there are no errors in the file.</p>
To edit the custom level configuration file.	<pre>/usr/local/dbfw/etc/ platform-configuration/ tls_configuration_custom_g roup.xml /usr/local/dbfw/etc/ platform-configuration/ tls_configuration_custom_g roup_agent.xml /usr/local/dbfw/etc/ platform-configuration/ tls_configuration_custom_g roup_ssl_services.xml</pre>	<p>The customizable set of cipher suites is defined in this file. By default, on a new installation the product is set to <i>Level-4</i>. This file can be modified to further restrict the cipher suite and include ciphers available on the product.</p>
To display the complete list of available cipher suites.	<pre>openssl ciphers -v</pre>	Use this command to display the current set of available cipher suites.

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 <i>Level-4</i> for increased security.
Audit Vault Server GUI	To support old browsers, set the TLS level to match the browser.
Audit Vault Agent / Host Monitor / Audit Vault Server	Oracle recommends to set at <i>Level-4</i> for increased security.
Audit Vault Agent deployed with <i>IBM AIX</i>	On a fresh installation of release <code>12.2.0.9.0</code> , it is set to <i>Level-4</i> . Change the TLS level to <i>Level-3</i> if any of the Audit Vault Agents are deployed on <i>IBM AIX</i> .

Setting Custom Cipher Sets

Use this procedure to set 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
```

2.8 Certificates

Learn about different certificates in Oracle AVDF.

2.8.1 Renew Audit Vault Server Certificate

Learn how to renew or rotate Audit Vault Server certificates.

Audit Vault Server uses certificates for internal communication with various components and services. Oracle AVDF provides the ability to renew Audit Vault Server certificates before they expire.

Follow these steps to renew or rotate the Audit Vault Server certificates:

1. Log in to *MOS (My Oracle Support)*.
2. Search for the patch with *34308451*.
3. Download the `p34308451_1220120_Linux-x86-64.zip`.
4. Extract the contents of the bundle.
5. Copy the `gensslcert.avs.tar.gz` file from the extracted location to the `/tmp` directory in the Audit Vault Server.
6. Follow these steps to complete the installation on the Audit Vault Server:
 - a. Connect to the Audit Vault Server appliance as *support* user through SSH.
 - b. Switch to *root* user by running the command:

```
su - root
```

- c. Create a new directory by running the command:

```
mkdir /root/gensslcert
```

- d. Copy the `gensslcert.avs.tar.gz` by running the command:

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

- e. Change directory by running the command:

```
cd /root/gensslcert
```

- f. Extract the files by running the command:

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

7. The following are the services in the Audit Vault Server appliance that have to be restarted when `[Restart AVS Services]` is mentioned in the later part of the

instructions. This is accomplished by running the commands mentioned in the table below:

```
(root)$ /etc/init.d/httpd reload
```

```
(root)$ /etc/init.d/controller restart
```

8. The following are the services in the Database Firewall appliance that have to be restarted, only when [Restart DBFW Services] is mentioned later in the instructions below. This can be accomplished by running the commands mentioned for reference in the table below:

```
(root)$ /etc/init.d/httpd reload
```

```
(root)$ /etc/init.d/stund restart
```

9. Generate new certificate authority signed certificates on the primary (or standalone) Audit Vault Server by running the following commands. This process updates the central self signed CA certificate on the Audit Vault Server and reload the affected services.

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

10. Restart the services in the primary Audit Vault Server appliance:

```
primary(root)$ [Restart AVS Services]
```

11. In case of high availability environment, transfer the certificate authority signed certificates from the primary Audit Vault Server to the standby Audit Vault Server and reload the services on the standby instance:

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

```
standby(root)$ cp /tmp/ha_partner.crt /usr/local/dbfw/etc/ha_partner.crt
```

12. Restart the services in the standby Audit Vault Server appliance:

```
standby(root)$ [Restart AVS Services]
```

13. In case of high availability environment, regenerate certificate authority signed certificates and all certificates on the standby Audit Vault Server instance. Reload the services by running the following commands:

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

14. Restart the services in the standby Audit Vault Server appliance:

```
standby(root)$ [Restart AVS Services]
```

- 15.** In case of high availability environment, transfer the standby certificate authority signed certificates to the primary instance and reload the services:

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

```
primary(root)$ cp /tmp/ha_partner.crt /usr/local/dbfw/etc/  
ha_partner.crt
```

- 16.** Restart the services in the primary Audit Vault Server appliance:

```
primary(root)$ [Restart AVS Services]
```

- 17.** Update and regenerate the certificate authority signed certificate bundles and services. This needs to be performed on the primary and standby Audit Vault Server instances one at a time.

- a.** Run the following command on the primary Audit Vault Server appliance:

```
primary(root)$ cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/  
dbfw/etc/ca.crt > /etc/pki/tls/certs/dbfw-ca.crt
```

- b.** Restart the services in the primary Audit Vault Server appliance:

```
primary(root)$ [Restart AVS Services]
```

- c.** Run the following command on the standby Audit Vault Server appliance:

```
standby(root)$ cat /usr/local/dbfw/etc/ha_partner.crt /usr/local/  
dbfw/etc/ca.crt > /etc/pki/tls/certs/dbfw-ca.crt
```

- d.** Restart the services in the standby Audit Vault Server appliance:

```
standby(root)$ [Restart AVS Services]
```

- 18.** In case of high availability environment, restart the observer on the primary Audit Vault Server server. Run the following commands:

```
primary(root)$ /etc/init.d/monitor stop
```

```
primary(oracle)$ /usr/local/dbfw/bin/observerctl --stop
```

```
primary(oracle)$ /usr/local/dbfw/bin/observerctl --start
```

- 19.** Wait for two minutes for the observer process to come up.

- 20.** Run the following command:

```
primary(root)$ /etc/init.d/monitor start
```


21. Copy and transfer the new certificate authority signed certificates from primary instance (and standby in case of high availability environment) to each of the linked Database Firewall instances:

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

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

```
dbfw(root) $ cp /tmp/primary.ca /usr/local/dbfw/etc/controller.crt
```

```
dbfw(root) $ cp /tmp/standby.ca /usr/local/dbfw/etc/controller_second.crt
```

22. Update the Database Firewall and Audit Vault Server controllers. Follow the steps mentioned in [Specifying the Audit Vault Server Certificate and IP Address](#) (page 4-6).
23. Restart the services:

```
dbfw(root) $ [Restart DBFW Services]
```

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

Use the `config-diagnostics`, `sappdiag`, or `openssl x509` commands to check the certificate validity. The `openssl x509` command is appropriate for Oracle AVDF release 12.2. Here are some example commands:

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

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

25. Check if the following peer certificates are valid:

- /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

2.8.2 Renew Database Firewall Certificate

Learn how to renew or rotate Database Firewall certificates.

Database Firewall uses certificates for internal communication with various components and services. Oracle AVDF provides the ability to renew Database Firewall certificates before they expire.



Note:

Renew or rotate certificates for each Database Firewall instance including those paired for high availability.

Follow these steps to renew or rotate the Database Firewall certificates:

1. Log in to *MOS (My Oracle Support)*.
2. Search for the patch with *34307693*.
3. Download the `p34307693_1220120_Linux-x86-64.zip`.
4. Extract the contents of the bundle.
5. Copy the `gensslcert.dbfw.tar.gz` file to the `/tmp` directory in the Database Firewall server.
6. Follow these steps to complete the installation on the Database Firewall server:
 - a. Connect to the Database Firewall appliance as *support* user through SSH.
 - b. Switch to *root* user by running the command:

```
su - root
```

- c. Create a new directory by running the command:

```
mkdir /root/gensslcert
```

- d. Copy the `gensslcert.dbfw.tar.gz` by running the command:

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

- e. Change directory by running the command:

```
cd /root/gensslcert
```

- f. Run the following command:

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

7. Generate the new certificate authority signed certificates on the Database Firewall appliance. First regenerate the local certificate authority signed certificates on the Database Firewall appliance by running the following command:

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

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

```
dbfw(root) $ /etc/init.d/httpd restart
```

```
dbfw(root) $ /etc/init.d/stund restart
```

9. Update the Database Firewall certificate on the Audit Vault Server and regain control of the Database Firewall. Refer to [Fetching an Updated Certificate from Oracle Database Firewall](#) (page 14-40) for complete information.

10. Check if 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` commands to check the certificate validity. The `openssl x509` command is appropriate for Oracle AVDF release 12.2. Here are some example commands:

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

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

11. Check if 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

Configuring the Audit Vault Server

Topics

- [About Configuring Oracle Audit Vault Server](#) (page 3-1)
- [Changing the UI \(Console\) Certificate for Oracle Audit Vault Server](#) (page 3-2)
- [Specifying Initial System Settings and Options \(Required\)](#) (page 3-3)
- [Configuring the Email Notification Service](#) (page 3-10)
- [Configuring Archive Locations and Retention Policies](#) (page 3-11)
- [Defining Resilient Pairs for High Availability](#) (page 3-20)
- [Registering Database Firewall in Audit Vault Server](#) (page 3-20)
- [Testing Audit Vault Server System Operations](#) (page 3-21)

3.1 About Configuring Oracle Audit Vault Server

Learn about configuring Oracle Audit Vault Server.

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

Note:

Oracle Audit Vault Server and Oracle Database Firewall server 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. Configure the Audit Vault agents.
3. (Optional) Define resilient pairs of servers for high availability.
4. (Optional) Add each Oracle Database Firewall at Oracle Audit Vault Server.
5. (Optional) Configure Oracle Audit Vault and Database Firewall to work with F5 BIG-IP Application Security Manager (ASM).
6. (Optional) Configure Oracle Audit Vault and Database Firewall to work with the **HP ArcSight Security Information Event Management (SIEM)** system.

 **Note:**

Micro Focus Security ArcSight SIEM (previously known as **HP ArcSight Security Information Event Management (SIEM)**) is deprecated in 12.2.0.8.0 and is desupported in 12.2.0.9.0. Use the `syslog` integration feature instead.

7. Check that the system is functioning correctly.

 **See Also:**

- [Managing A Resilient Audit Vault Server Pair](#) (page 8-2) for more information about configuring a resilient pair of Oracle Audit Vault Servers for high availability. Perform the initial configuration that is described in this chapter for both Oracle Audit Vault Servers
- [Summary of Configuration Steps](#) (page 1-6) to understand the high-level workflow for configuring Oracle Audit Vault and Database Firewall

3.2 Changing the UI (Console) Certificate for Oracle Audit Vault Server

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

When you first access the Oracle 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 Oracle Audit Vault Server console as a super administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information

To change the UI certificate for the Audit Vault Server:

1. Click the **Settings** tab.
2. Under Security, click **Console Certificate**.
3. Click **Generate Certificate Request**.

The certificate request form is displayed with the common name for the certificate.

4. 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 Oracle Audit Vault Server. To suppress the warning when you access Oracle Audit Vault Server console using its IP address instead of the host name, also check **Suppress warnings for IP based URL access**.

5. Complete the form and enter content in the mandatory fields.
6. Click **Submit and Download**.

7. 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`
8. After the certificate authority issues a new certificate, upload it by returning to the Change UI Certificate page and 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.

3.3 Specifying Initial System Settings and Options (Required)

Topics

- [Specifying the Server Date, Time, and Keyboard Settings](#) (page 3-3)
- [Specifying the Audit Vault Server System Settings](#) (page 3-5)
- [Configuring Oracle Audit Vault Server Syslog Destinations](#) (page 3-8)

3.3.1 Specifying the Server Date, Time, and Keyboard Settings

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

Super administrators can change the Oracle Audit Vault Server date, time, and keyboard settings. It is important to ensure that the date and time that you set for Oracle Audit Vault Server are correct. This is because events that the server performs 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 Time Stamps

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

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

 **WARNING:**

Do not change the Oracle Audit Vault Server database time zone or change the time zone through any configuration files. Doing so causes serious problems in Oracle Audit Vault Server.

- If you are looking at the Oracle Database Firewall UI, then all time zones are displayed in UTC.

Prerequisite

Log in to Oracle Audit Vault Server console as super administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To set the server date, time, and keyboard settings

1. Click the **Settings** tab.
2. From the **System** menu, click **Manage**.
3. From the **Timezone Offset** drop-down list, select your local time in relation to Coordinated Universal Time (UTC).
For example, **-5:00** is five hours behind UTC. You must select the correct setting to ensure that the time is set accurately during synchronization.
4. From the **Keyboard** drop-down list, select the keyboard setting.
5. In the **System Time** field, select **Manually Set** or **NTP Synchronization**.
Selecting NTP Synchronization keeps the time synchronized with the average of the time recovered from the time servers specified in the **Server 1/2/3** fields.
6. If you selected **NTP Synchronization**, then select **Enable NTP Time Synchronization** 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.
7. (Optional) Select **Synchronize Time After Save** if you want the time to be synchronized when you click **Save**.
8. In the **Server 1**, **Server 2**, and **Server 3** sections, use the default server addresses, or enter the IP addresses or names of your preferred time servers.
If you specify a name, then the DNS server that is specified in the System Services page is used for name resolution.
9. Click **Test Server** to display the time from the server.
Click **Apply Server** to update the Audit Vault Server time from this NTP server. The update will not take effect until you click **Save**.
10. Click **Save**.

To enable time synchronization, you may also need to specify the IP address of the default gateway and a DNS server.

 **See Also:**

- [Setting or Changing the Audit Vault Server Network Configuration](#) (page 3-5)
- [Configuring or Changing the Oracle Audit Vault Server Services](#) (page 3-7)
- [Setting the Date and Time in the Database Firewall](#) (page 4-5)

3.3.2 Specifying the Audit Vault Server System Settings

Topics

- [Setting or Changing the Audit Vault Server Network Configuration](#) (page 3-5)
- [Configuring or Changing the Oracle Audit Vault Server Services](#) (page 3-7)

3.3.2.1 Setting or Changing the Audit Vault Server Network Configuration

Learn how to change the Audit Vault Server network configuration.

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

 **Note:**

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

1. Restart all audit trails.
2. Reconfigure the resilient pair of Database Firewalls if you previously configured them.
3. If the IP address of Audit Vault Server was changed, then update this information in Database Firewall.

Prerequisite

Log in to the Audit Vault Server console as an administrator or super administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To configure the Audit Vault Server network settings:

1. Click the **Settings** tab.
2. In the **System** menu, click **Network**.
3. Edit the following fields as necessary, then click **Save**.
 - **Host Name:** The host name must be a fully qualified domain name of the Audit Vault Server. The host name must start with a letter, can contain maximum of 24 characters, and cannot contain spaces. For Oracle AVDF release 12.2.0.14.0, the host name can contain a maximum of 64 characters.

 **Note:**

- Changing the host name requires a reboot. After you click **Save**, the system asks you to confirm if you want to reboot or cancel. If you confirm, then the system reboots and Audit Vault Server will be unavailable for a few minutes.
- The host name cannot be changed in a high availability environment. If the host name requires to be changed, unpair the Audit Vault Servers, change the host name, and pair them again.

- **IP Address:** The IP address of Audit Vault Server. An IP address was set during the installation of Audit Vault Server. To use a different address, you can change it now. The IP address is static and must be obtained from your network administrator.

 **Note:**

- Changing the IP address requires a reboot.
- If you have a high availability configuration, then the primary and secondary Audit Vault Servers must be unpaired before changing the IP address. Once the IP address of the primary or secondary Audit Vault Server is changed, pair the two servers again. Once you complete the pairing process, redeploy the Audit Vault Agents to ensure that they are updated with the new IP addresses for both the primary and the secondary Audit Vault Servers.

You may need to add the specified IP Address to routing tables to enable traffic to go between the Audit Vault Server and Database Firewalls.

- **Network Mask:** (Super Administrator only) The subnet mask of the Audit Vault Server.
- **Gateway:** (Super Administrator only) The IP address of the default gateway (for example, to access the management interface from another subnet). The default gateway must be on the same subnet as Audit Vault Server.
- **Link properties:** Do not change the default setting unless your network has been configured to not use auto negotiation.

 **See Also:**

- [Ports Used by Audit Vault and Database Firewall](#) (page D-1) for a list of default Audit Vault Server port numbers.
- [Managing A Resilient Database Firewall Pair](#) (page 8-9) to configure a resilient pair of Database Firewalls.
- [Specifying the Audit Vault Server Certificate and IP Address](#) (page 4-6) to update Audit Vault Server's IP address in the Database Firewall.

3.3.2.2 Configuring or Changing the Oracle Audit Vault Server Services

Learn how to configure and change Oracle Audit Vault Server services.

Prerequisite

Log in to the Oracle Audit Vault Server console as a super administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To configure the Oracle Audit Vault Server services:

1. In the **System** tab, from the **System** menu, click **Services**.
2. Complete the following fields as necessary, then click **Save**.

 **Caution:**

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

- **DNS Servers 1, 2, 3:** (Optional) Select **IP Address(es)** and enter the IP addresses of up to three DNS servers on the network. Oracle 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.
- **Web Access:** If you want to allow only selected computers to access the Audit Vault Server console, select **IP Address(es)** and enter specific IP addresses in the box, separated by spaces. Using the default of **All** allows access from any computer in your site.
- **SSH Access:** You can specify a list of IP addresses that are allowed to access Audit Vault Server from a remote console by selecting **IP Address(es)** and entering them in this field, separated by spaces. Using a value of **All** allows access from any computer in your site. Using a value of **Disabled** prevents console access from any computer.
- **SNMP Access:** You can specify a list of IP addresses that are allowed to access the network configuration of Audit Vault Server through SNMP by selecting **IP Address(es)** and entering them in this field, separated by spaces. Selecting **All** allows access from any computer. Selecting the default value of **Disabled** prevents SNMP access. The SNMP community string is `gT8@fq+E`.

 **See Also:**

[Protecting Your Data](#) (page 2-1) for a list of recommendations and precautions to maintain security

3.3.2.3 Changing IP Address Of An Active And Registered Host

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

Prerequisites

1. Stop Audit Trails. See section [Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server](#) (page 6-11) for more information.
2. Stop the Audit Vault Agent before changing the IP address of the Secured Target Server. See section [Stopping, Starting, and Other Agent Operations](#) (page 5-9) for more information to stop the Audit Vault Agent.

To change the IP address of a live Registered Host

1. Change the IP address of the Secured Target Server.
2. Change the IP address of the previously registered host entity of Audit Vault and Database Firewall using the Audit Vault GUI or AVCLI.
3. Execute the following to start the Audit Vault Agent with `-k` option:

```
agentctl start -k
```
4. Enter Activation Key.
5. Start Audit Trails.

 **See Also:**

[Changing IP Address For A Single Instance Of Database Firewall Server](#) (page 4-7)

3.3.3 Configuring Oracle Audit Vault Server Syslog Destinations

Learn how to configure Oracle Audit Vault Server syslog destinations.

Use the following procedure to configure the types of syslog messages to send from Oracle 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.

Prerequisites

- Log in to the Oracle Audit Vault Server console as an administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

- Ensure that the IP addresses provided for syslog destinations are on a different host than the Oracle Audit Vault Server.
1. Click the **Settings** tab.
 2. From the **System** menu, click **Connectors**, and scroll down to the **Syslog** section.

The screenshot shows a configuration window titled "Syslog". It contains two large text input areas for "Syslog Destinations (UDP)" and "Syslog Destinations (TCP)". At the bottom, there is a "Syslog Categories" section with four checkboxes: "Alert", "Debug", "Info", and "System".

3. Complete the fields, as necessary:
 - **Syslog Destinations (UDP):** Use this box if you are using User Datagram Protocol (UDP) to communicate syslog messages from Oracle 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 Oracle Audit Vault Server. Enter the IP address and port combinations of each server that is permitted to receive the syslog messages, separated by spaces.
 - **Syslog Categories:** You can select the types of syslog messages to generate as follows:
 - **Alert:** 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`.
4. Click **Save**.
5. If you are using two Oracle Audit Vault Servers as a resilient pair, then repeat specifying the initial system settings and options on the second Oracle Audit Vault Server.

 **See Also:**

- [Specifying Initial System Settings and Options \(Required\)](#) (page 3-3)
- *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed instructions and information about Oracle Audit Vault and Database Firewall syslog alert formats

3.4 Configuring the Email Notification Service

Topics

- [About Email Notifications in Oracle Audit Vault and Database Firewall](#) (page 3-10)
- [Configuring Email Notification for Oracle Audit Vault and Database Firewall](#) (page 3-11)

3.4.1 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.

3.4.2 Configuring Email Notification for Oracle Audit Vault and Database Firewall

Learn how to configure email notification for Oracle Audit Vault and Database Firewall.

Prerequisite

Log in to Audit Vault Server console as a super administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To configure the email notification service:

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

3.5 Configuring Archive Locations and Retention Policies

Learn about configuring archive locations and retention policies.

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.

3.5.1 About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall

You can archive data files in Oracle Audit Vault and Database Firewall as part of your information life cycle strategy. To do so, you must create archiving (or retention) policies, and configure archive locations to which data will be transferred according to the policies. We recommend that you archive regularly in accordance with your corporate policy.

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

What is a Retention (or Archiving) Policy?

Retention policies determine how long data is retained in the Audit Vault Server, when data is available for archiving, and for how long archived data can be retrieved to the Audit Vault Server. An administrator creates retention (or archiving) policies and an auditor assigns a specific policy to each secured target, as well as to scheduled reports. The settings in a retention policy are as follows:

- **Months Online:** The audit data is available in the Audit Vault Server for the number of months online specified. During this period, data is available for viewing in reports. When this period expires, 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 the Audit Vault Server.
- **Months Archived:** The archived audit data can be retrieved to the Audit Vault Server for the number of months specified in Months Archived. If the data is retrieved during this period, it will be available again in reports. When the months archived period expires, the data can no longer be retrieved to the Audit Vault Server.

Retention times are based on the time that the audit events occurred in the secured target. If the auditor does not select a retention policy for a secured target or scheduled report, the default retention policy will be used (12 months retention online and 12 months in archives).

Example

Suppose your retention policy is:

- Months Online: 2
- Months Archived: 4

With this retention policy, data that is newer than two months ago is available in the Audit Vault Server. Data that becomes older than two months ago 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 ago but newer than six months ago, and can be retrieved from the archives to the Audit Vault Server. Data that becomes older than six months ago is no longer available.

When new Data Collected is Older than Retention Policy Limits

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

For instance, suppose your retention policy is the same as the above [Example](#) (page 3-12). Now suppose you start collecting audit data from a newly configured secured 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), Oracle Audit Vault and Database Firewall does one of the following:

- If this is an audit trail for a newly configured secured target, 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 secured target, 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](#) (page 6-13) for information to make required data files available.

3.5.2 Defining Archive Locations

Learn about defining archive locations.

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

Oracle recommends that you use NFS to transfer data to an archive location. If you use Secure Copy (SCP) or Windows File Sharing (SMB) to transfer data to an archive location, then your data files are first copied to a staging area in Oracle 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 backup 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.

Prerequisite

Log in to the Audit Vault Server as an administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To create an archive location:

1. Click the **Settings** tab, and under **Archiving**, click **Manage Archive Locations**.
A list of existing archive locations is displayed.
2. Click the **Create** button, and complete the following fields:
 - **Transfer Method:** The method used 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 Storage (NFS):** Select if using a network file share or NAS.
 - **Location Name:** The name of the archiving destination. This name is used to select the archiving destination when starting an archive.
 - **Remote Filesystem:** If you use the Network File System (NFS) transfer method, then you can select an existing filesystem, 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 filesystem. This filesystem can be later selected in the Audit Vault Server console. This is not possible in a high availability environment.

The archive locations must be created using the Audit Vault Server console only in a high availability environment by selecting the **Create New Filesystem** option.

- **Address:** The host name or IP address of the NFS server used by the Audit Vault Server for archiving. If Windows File Sharing is the transfer method, then specify an IP address.
- **Export Directory:** If you use the Network File System (NFS) transfer method, then enter the export directory of the NFS server. For example, this directory can be created in the `/etc/exports` file of the NFS server. Ensure the

`oracle` user (User ID: 503) has appropriate `read` and `write` permissions to this directory.

- **Path:** The path to the archive storage location. Enter a path to a directory (not a file), noting the following for these transfer methods:
 - **Secure Copy (scp):** If there is no leading slash character, the path is relative to the user's home directory. If there is a leading slash, the path is relative to the `root` directory.
 - **Windows File Sharing (SMB):** Enter the sharename, followed by a forward slash and the name of the folder (for example, `/sharename/myfolder`).
 - **Network File System (NFS):** Enter the path relative to the export directory. For example if the export directory is `/export_dir`, and the full path to the directory you want to designate as an archive location is `/export_dir/dir1/dir2`, then enter `/dir1/dir2` in the **Path** field. To put archives directly in the NFS server's export directory, enter `/` (forward slash) for the **Path**.

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

- **Port:** This is the port number that secure copy uses or the Windows fileshare service on the machine that archives the data. You can normally use the default port number. If you selected **Windows File Sharing** as the Transfer Method, then use port 445.
- **Username:** The account name on the machine to which the archive data will be transferred.
- **Authentication Method:** If Secure Copy (scp) is the transfer method, then you can select **Password** and enter the login password. If a Linux machine is used, then you can select **Key Authentication**.
If using Key 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, or if you selected Password as the authentication method, then this is the password to log into the machine that archives the data.
- **Public Key:** This field appears if you selected Key Authentication. Copy this public key and add it to the public keys file on the machine that archives the data. For example, add the key in `~/.ssh/authorized_keys`.

3. Click **Save**.



See Also:

[REGISTER REMOTE FILESYSTEM](#) (page A-53)

Managing NFS locations in high availability environment

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.

Follow these steps to create a new NFS archive location:

1. Log in to the Audit Vault Server console as admin user.
2. Click **Settings**.
3. Under **ARCHIVING**, click **Manage Archive Locations**.
4. The list of existing archive locations is displayed. Click the name of the existing archive location to modify. Make the changes and click **Save**.
5. Click **Create**, to create a new archive location using NFS.
6. The **Network File System (NFS)** is selected by default. Enter the following details to create a new NFS archive location:

Field	Description
Location Name	The name of the archiving destination.
Remote Filesystem	Select an existing filesystem, or one will be created automatically based on the details of this archive location.
Primary Server Address	NFS Server IP address for primary Audit Vault Server.
Secondary Server Address	NFS Server IP address for standby Audit Vault Server.
Primary Server Export Directory	Export directory on the NFS server for primary Audit Vault Server.
Secondary Server Export Directory	Export directory on the NFS server for standby Audit Vault Server.
Primary Server Path	The destination path relative to the export directory on the NFS server for primary Audit Vault Server.
Secondary Server Path	The destination path relative to the export directory on the NFS server for standby Audit Vault Server.

7. Click **Save**.

 **Note:**

- The combination of NFS server host name/IP address, export directory, and the destination path specified for primary and standby Audit Vault Servers must be unique.
- Enable archiving functionality post upgrade from release 12.2.0.10.0 and prior. Follow the steps in section [Enable Archiving Functionality Post Upgrade From Release BP10 and Prior](#). This is required only if the Audit Vault Server is deployed in a high availability environment.
- Enable Archiving functionality post upgrade from 12.2.0.11.0 to later releases (12.2.0.12.0 or 12.2.0.13.0). Follow the steps in section [Enable Archiving Functionality Post Upgrade From BP11 to Later Releases](#).

3.5.3 Creating or Deleting Archiving Policies

Topics

- [Creating Archiving \(Retention\) Policies](#) (page 3-17)
- [Deleting Archiving Policies](#) (page 3-18)

3.5.3.1 Creating Archiving (Retention) Policies

After you create a retention policy, an Oracle AVDF auditor can apply it to secured targets.

Prerequisite

Log in to the Audit Vault Server console as an *administrator*. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To create an archiving (retention) policy:

1. Click the **Settings** tab.
2. Under **Archiving**, select **Manage Policies**, and then click the **Create** button.
3. Enter a **Name** for this policy.
4. In the **Months Online** field, enter the number of months to retain audit data in the Audit Vault Server before it is marked for archiving. The default value is 1.

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

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

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

 **See Also:**

Oracle Audit Vault and Database Firewall Auditor's Guide for instructions on assigning retention policies.

3.5.3.2 Deleting Archiving Policies

Learn how to delete archiving policies.

You can only delete user-defined archiving policies.

Prerequisite

Log in to Oracle Audit Vault Server console as an administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To delete an archiving (retention) policy:

1. Click the **Settings** tab.
2. Under **Archiving**, click **Manage Policies**.
3. Select the user-defined policy to delete and click **Delete**.

3.5.4 Running Archive or Retrieve Jobs

See "[Archiving and Retrieving Audit Data](#) (page 14-7)".

3.6 Managing Archival and Retrieval in High Availability Environments

Learn about managing Oracle Audit Vault and Database Firewall data 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 Oracle Audit Vault Servers have the same number of NFS archive locations. Having the same number of locations is crucial for the effective operation of archiving and file management in high availability environments.

 **Note:**

- Any user with admin privileges can perform archival and retrieval tasks.
- It is recommended that you place the NFS archive locations for the primary and secondary Oracle Audit Vault Servers on separate NFS servers.
- It is also recommended that the primary and secondary NFS servers reside within the same data center as the Oracle Audit Vault Server.
- 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 requirements mentioned in [Prerequisites for Configuring a Resilient Pair of Audit Vault Servers](#) (page 8-3) are satisfied before configuring your high availability environment.

After you successfully pair your high availability servers, the NFS locations pertaining to both the primary and secondary Oracle Audit Vault Servers are displayed under **Manage Archive Locations** on the primary Oracle Audit Vault Server console. These NFS locations include those that you created on both the primary and secondary Oracle Audit Vault Servers before and after configuring high availability. The names of these NFS locations have the primary location name or the name that you specified when you created the location after high availability is configured. The Oracle Audit Vault Server console provides details of the host, export directory, and destination path for both the primary and secondary Oracle Audit Vault Servers.

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.

Updating or Deleting NFS locations

The super admin can update or delete the NFS locations after high availability pairing of primary and secondary Oracle Audit Vault Servers. You can update or delete the NFS locations on both the primary and secondary Oracle Audit Vault Servers. If the datafiles are archived, then you cannot update or delete the locations. The **Location Name** and the **Primary Server Path** or the **Secondary Server Path** can be updated when high availability is enabled.

 **See Also:**

- Enable archiving functionality post upgrade from release 12.2.0.10.0 and prior. Follow the steps in section [Enable Archiving Functionality Post Upgrade From Release BP10 and Prior](#). This is required only if the Audit Vault Server is deployed in a high availability environment.
- Enable Archiving functionality post upgrade from 12.2.0.11.0 to later releases (12.2.0.12.0 or 12.2.0.13.0). Follow the steps in section [Enable Archiving Functionality Post Upgrade From BP11 to Later Releases](#).
- [Monitoring Jobs](#) (page 14-31)
- [Defining Archive Locations](#) (page 3-13)

3.7 Defining Resilient Pairs for High Availability

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

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

 **See Also:**

- [Configuring High Availability](#) (page 8-1)

3.8 Registering Database Firewall in Audit Vault Server

Learn how to register Database Firewall in Audit Vault Server.

Use this procedure to register an Database Firewall in 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 the Database Firewall](#) (page 4-1).
- You must register Database Firewalls in Audit Vault Server before you can pair them for high availability. See [Managing A Resilient Database Firewall Pair](#) (page 8-9) 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](#) (page 4-6).
- Log in to Audit Vault Server as an administrator. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) 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**.

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.

3.9 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 [Logging in to the Audit Vault Server Console UI](#) (page 1-11) 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. In the **System** menu, click **Diagnostics**.
4. 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
 - Statuses of various process 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.
5. Click the **Home** tab, and check the status of **Database Firewalls** and **Hosts**.

3.10 Configuring Fiber Channel-Based Storage for Audit Vault Server

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

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

 **Note:**

- Fiber channel-based storage is supported on Oracle Audit Vault and Database Firewall release 12.2.0.0 and later only.

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.
 - Oracle 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 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 not supported by Oracle Audit Vault and Database Firewall.

3. Log in to Audit Vault Server as root.
4. Stop the Oracle databases by running the following commands:

```
/etc/init.d/dbfwdb stop
```

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

5. Stop the ASMLib driver by running the following command:

```
oracleasm exit
```

6. Modify the values in the `/etc/sysconfig/oracleasm` file as follows:

```
ORACLEASM_SCANORDER="dm /mnt"
```

7. Reboot your system.

3.11 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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

Configuring the Database Firewall

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

Topics

- [About Configuring the Database Firewall](#) (page 4-1)
- [Changing the UI \(Console\) Certificate for the Database Firewall](#) (page 4-2)
- [Managing the Database Firewall's Network and Services Configuration](#) (page 4-3)
- [Setting the Date and Time in the Database Firewall](#) (page 4-5)
- [Specifying the Audit Vault Server Certificate and IP Address](#) (page 4-6)
- [Configuring Database Firewall and its Traffic Sources on Your Network](#) (page 4-8)
- [Configuring an Interface Masters Niagara Server Adapter Card](#) (page 4-12)
- [Viewing the Status and Diagnostics Report for a Database Firewall](#) (page 4-12)

4.1 About Configuring the Database Firewall

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

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.
- Database Firewall introduces very minimal latency overhead of less than 100 microseconds per SQL statement with 4000 transactions per second. This is based on internal performance tests.

Basic firewall configuration consists of these four steps:

1. [Managing the Database Firewall's Network and Services Configuration](#) (page 4-3)
2. [Setting the Date and Time in the Database Firewall](#) (page 4-5)
3. [Specifying the Audit Vault Server Certificate and IP Address](#) (page 4-6)

4. [Configuring Database Firewall and its Traffic Sources on Your Network](#) (page 4-8)

After configuring the Database Firewalls, perform the following tasks:

- Configure enforcement points for each database secured target that the firewall is protecting.
- You can optionally set up resilient pairs of Database Firewalls for a high availability environment.

See Also:

- [Summary of Configuration Steps](#) (page 1-6) to understand the high level workflow for configuring the Oracle Audit Vault and Database Firewall system.
- [Planning the System Configuration](#) (page 1-7) for an overview of the planning steps.
- [Configuring Enforcement Points](#) (page 6-20) to configure enforcement points.
- [Configuring High Availability](#) (page 8-1) to set up resilient pairs of Database Firewalls for a high availability.

4.2 Changing the UI (Console) Certificate for the Database Firewall

When you first access the Database Firewall administration console, you see a certificate warning or message. To avoid this type of message in the future, you can upload a new UI certificate signed by a relevant certificate authority.

Prerequisite

Log in to the Database Firewall administration console as an *administrator*. See [Logging in to the Database Firewall Console UI](#) (page 1-13) for more information.

To change the UI certificate for the Database Firewall:

1. Under System, click **Change UI Certificate**.
2. In the Change UI Certificate page, click **Generate a Certificate Request and download the certificate.csr file**.

The Generate Certificate Signing Request form is displayed, with the common name for the certificate. The certificate warnings are based on the common name used to identify the Audit Vault Server host.

3. If you do not want to see the certificate warning when you access the Audit Vault Server console using its IP address instead of the host (common) name, check the **Suppress warnings for IP based URL access** checkbox.
4. Fill out the form, and then click **Generate**.

A confirmation message appears confirming that the request has been generated.

5. Click **Download**, select **Save File**, and then save the `.csr` file in a selected location.
6. Submit the saved `.csr` file to a certificate authority.
7. Once the certificate authority issues a new certificate, to upload it, return to the UI Certificate page and click **Upload the issued certificate to this Database Firewall**.
8. Browse for the new certificate `.csr` file, 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.

4.3 Managing the Database Firewall's Network and Services Configuration

Topics

- [Configuring Network Settings For A Database Firewall](#) (page 4-3)
- [Configuring Network Services For A Database Firewall](#) (page 4-4)

4.3.1 Configuring Network Settings For A Database Firewall

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

Prerequisite

Log in to the Database Firewall administration console. See [Logging in to the Database Firewall Console UI](#) (page 1-13) for more information.

To change the Database Firewall network settings:

1. In the **System** menu, select **Network**.
2. In the Network Configuration page, click the **Change** button.
3. In the Management Interface section, complete the following fields as necessary.
 - **IP Address:** The IP address of the currently accessed Database Firewall. An IP address was set during installation. If you want to use a different address, then you can change it here. The IP address is static and must be obtained from the network administrator.
 - **Network Mask:** The subnet mask of the Database Firewall.
 - **Gateway:** The IP address of the default gateway (for example, for internet access). The default gateway must be on the same subnet as the host.
 - **Name:** Enter a descriptive name for this Database Firewall. The name must be alphanumeric with no spaces.
4. In the Link Properties section, only change these settings if you are advised to do so by your network administrator.

Auto-negotiation is the most common configuration and is the default.

5. Click **Save**.

4.3.2 Configuring Network Services For A Database Firewall

The network services configuration determines how administrators can access the Database Firewall. See the guidelines to protect data and ensure that you take the appropriate security measures when configuring network services.

Prerequisite

Log in to the Database Firewall administration console. See [Logging in to the Database Firewall Console UI](#) (page 1-13) for more information.

To configure network services for a Database Firewall:

1. In the **System** menu, select **Services**.
2. Click the **Change** button.
3. In the Configure Network Services page, edit the following as necessary:
 - **DNS Server 1, DNS Server 2, and DNS Server 3:** If you require host names to be translated, then you must enter the IP address of at least one DNS server on the network. You can enter IP addresses for up to three DNS servers. Keep the fields blank if there is no DNS server, otherwise system performance may be impaired.

If you want to use DNS, then ensure the servers are reliable. If the DNS servers are unavailable, then many services on the Database Firewall will not work. For example, the Database Firewall may pass traffic that it would otherwise block.
 - **Web Access:** If you want to enable selected computers to have Web access to the Database Firewall administration console, enter their IP addresses separated by spaces. Entering **all** allows access from any computer in your site.
 - **SSH Access:** If you want to allow selected computers to have secure shell access to the Database Firewall, enter their IP addresses separated by spaces. Enter **disabled** to block all SSH access. Enter **all** to allow unrestricted access.
 - **SNMP Access:** If you want to allow access to the network configuration of the Database Firewall through SNMP, enter a list of IP addresses that are allowed to do so, separated by spaces. Enter **disabled** to restrict all SNMP access. Enter **all** to allow unrestricted access.
 - **SNMP Community String:** Enter an SNMP community string (password) that is unique for this Oracle AVDF installation. It must not be the same password as any other password used for authentication. Confirm this string in the **Confirm SNMP Community String** field.
4. Click **Save**.



See Also:

[Protecting Your Data](#) (page 2-1)

4.4 Setting the Date and Time in the Database Firewall

Use this procedure to set the Database Firewall date and time:

Prerequisite

Log in to the Database Firewall administration console. See [Logging in to the Database Firewall Console UI](#) (page 1-13) for more information.

To set the Date and Time in the Database Firewall:

1. In the System menu, select **Date and Time**.
2. In the Date and Time page, select **Change**.
3. After System Time, enter the correct date and time in Coordinated Universal Time (UTC).
4. (Optional) Under NTP Synchronization, select the **Enable NTP Synchronization** check box and then add 1 to 3 NTP server addresses in the fields provided.

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

To enable time synchronization, you also must specify the IP address of the default gateway and a DNS server.

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



WARNING:

In DPE (blocking) mode, changing the time causes all enforcement points to restart, dropping existing connections to protected databases. This causes a temporary disruption to traffic, and will happen when you choose **Synchronize Time After Save** or enter the time directly.

5. Click **Save**.



See Also:

[Managing the Database Firewall's Network and Services Configuration](#) (page 4-3) to specify the IP address of the default gateway and DNS server.

4.5 Specifying the Audit Vault Server Certificate and IP Address

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

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

To specify the Audit Vault Server certificate and IP address:

1. Ensure that the system clocks for each server that you want to use for a Database Firewall and for the Audit Vault Server are synchronized.
2. Log in to the Audit Vault Server administration console.
3. Select **Settings**.
4. In the **Security** menu, click **Server Certificate**.
The server's certificate is displayed.
5. Copy the server's certificate.
6. Log in to the Database Firewall administration console.
7. In the **System** menu, click **Audit Vault Server**.
8. In the **Audit Vault Server 1 IP Address** field, enter the IP address of the Audit Vault Server.
9. Paste the Audit Vault Server's certificate in the **Audit Vault Server 1 Certificate** field.
10. If you are using a resilient pair of Audit Vault Servers, in the Audit Vault Server 2 area, add the IP address and certificate of this secondary Audit Vault server.

 **Tip:**

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

11. Click **Apply**.
12. Register each firewall in the Audit Vault Server console, to complete the association of the Database Firewall to the Audit Vault Server.

 **See Also:**

- [Registering Database Firewall in Audit Vault Server](#) (page 3-20)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)
- [Logging in to the Database Firewall Console UI](#) (page 1-13)

4.6 Changing IP Address For A Single Instance Of Database Firewall Server

Use this procedure to change the IP address of the Database Firewall Server.

Before you begin

Change the IP address of the Database Firewall Server during a safe period as it avoids interruption to collection of logs.

To change the IP address of the Database Firewall Server:

1. Log in to the Database Firewall Web User Interface console as *FWADMIN* user.
2. Click **SYSTEM** and then **Network** in the User Interface on the left navigation bar.
3. The IP Address of the Database Firewall Server is displayed under the tab **Management Interface**.
4. Scroll down to the bottom of the **Network Configuration** page. Click **Change** in order to change the IP address of the Database Firewall Server.
5. Remove the existing IP address and enter the new one provided by your network administrator.
6. Click **Save**.

Result:

Settings saved message is displayed on the screen. The new IP address appears in the **Management Interface** tab confirming the change.

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.

7. Change the IP address on the `/etc/hosts` to the new one as *root* user.
8. Once the IP address of the Database Firewall Server is changed using the UI console, update this information in the Audit Vault Server. Click **Database Firewalls** under the **Database Firewalls** menu.
9. Check the IP Address listed on the UI console.
10. The Database Firewall instance for which the IP address was changed, registers as *Offline*. Click on the link under the **Name** field. This is the name of the Database Firewall and is similar to the one assigned to the Database Firewall System Appliance.
11. The **Modify Database Firewall** screen appears. Enter the new IP address and click **Save**.

12. Once the changes are saved, the certificate validation may fail. Click on the name of the Database Firewall and then click **Update Certificate**.
13. Once the certificate is updated, the **Database Firewalls** tab is displayed. The Database Firewall Server is online.

 **Note:**

Once the Database Firewall Server is back online it begins to download any Enforcement Point log data that is not downloaded while it was offline.

 **See Also:**

[Changing IP Address Of An Active And Registered Host](#) (page 3-8)

4.7 Configuring Database Firewall and its Traffic Sources on Your Network

Topics

- [About Configuring The Database Firewall And Traffic Sources On Your Network](#) (page 4-8)
- [Configuring Traffic Sources](#) (page 4-9)
- [Configuring a Bridge in the Database Firewall](#) (page 4-9)
- [Configuring Oracle Database Firewall As A Traffic Proxy](#) (page 4-11)

4.7.1 About Configuring The Database Firewall And Traffic Sources On Your Network

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

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

You will use traffic and proxy sources of a firewall to configure enforcement points for each secured target database you are monitoring with that firewall.

 **See Also:**

- [Configuring Enforcement Points](#) (page 6-20)
- Introduction to Database Firewall Deployment for more information on Database Firewall modes.

4.7.2 Configuring Traffic Sources

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

Prerequisite

Log in to the Database Firewall administration console. See [Logging in to the Database Firewall Console UI](#) (page 1-13) for more information.

To change the configuration of traffic sources:

1. In the **System** menu, click **Network**.

In the Network Configuration page, the current network settings are displayed. These include a range of detailed information, such as the Database Firewall network settings, proxy ports, traffic sources, network interfaces, and any enabled bridges.

2. Click the **Change** button.
3. Scroll to the **Traffic Sources** section and change the following settings as necessary:
 - To remove a traffic source, click the **Remove** button next to the traffic source name.
 - Edit the **IP address** or **Network Mask** fields as necessary.
 - To enable or disable a bridge, check or uncheck the **Bridge Enabled** check box. You can only enable a bridge if the traffic source has two network interfaces in the Devices area.
 - To remove a network interface (that is, a network card) from the traffic source, in the Device area, click the **Remove** button for the device that you want to remove.
 - To add a network interface to a traffic source, scroll to the **Unallocated Network Devices** section, and from the **Traffic Source** drop-down list, select the name of the traffic source to which you want to add this device.
4. Click **Save**.

 **See Also:**

[Configuring a Bridge in the Database Firewall](#) (page 4-9) to enable or disable a bridge.

4.7.3 Configuring a Bridge in the Database Firewall

Before you configure a bridge in the Database Firewall, ensure that the following is in place:

- Ensure that the Database Firewall is inline with network traffic (or configured as a proxy) if it is to be used in blocking mode (DPE) to block potential SQL attacks.
- If the Database Firewall is not in proxy mode, then allocate an additional IP address that is unique to the database network, to enable a bridge.
- Oracle Audit Vault and Database Firewall uses the bridge IP address to redirect traffic within the Database Firewall. When the Database Firewall is used as a proxy, you do not need to allocate this additional IP address.
- To enable a traffic source as a bridge, ensure that this traffic source has two network interfaces. These network interface ports must connect the Database Firewall in-line between the database and its clients (whether Database Policy Enforcement or Database Activity Monitoring mode is used).

 **Note:**

- The IP address of the bridge must be on the same subnet as all secured target databases when the Database Firewall is in DPE mode using that bridge. This restriction does not apply when the Database Firewall is deployed in DAM mode.
- If the Database Firewall's management interface (specified in the console's **Network** page) and the bridge are connected to physically separate networks that are on the same subnet, the Database Firewall may route responses out of the wrong interface. If physically separate networks are required, use different subnets.
- In-line bridge mode is deprecated in 12.2.0.8.0, and will be desupported in 19.1.0.0.0. It is advisable to use proxy mode as an alternative.

To configure the Database Firewall bridge IP address:

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

This traffic source must have two network interfaces, which are listed in the Devices table. You can add an interface if necessary from the Unallocated Network Interfaces section of the page.

5. Select **Bridge Enabled** for this traffic source.
6. If necessary, edit the **IP Address** or **Network Mask** settings.

The bridge IP address is used to redirect traffic within the Database Firewall.

7. Click **Save**.

 **See Also:**

- [Configuring Oracle Database Firewall As A Traffic Proxy](#) (page 4-11)
- [Configuring Traffic Sources](#) (page 4-9)
- [Logging in to the Database Firewall Console UI](#) (page 1-13)
- [Applying Static Routing Rules On Network Interfaces For Audit Vault Server And Database Firewall](#) (page H-7)

4.7.4 Configuring Oracle Database Firewall As A Traffic Proxy

Learn about configuring a firewall as a traffic proxy.

Depending on your network configuration, you may prefer to configure a traffic proxy in the Database Firewall instead of a bridge inline with network traffic. You can then associate the proxy with an enforcement point. You can also specify multiple ports for a proxy in order to use them for different enforcement points.

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

To configure a traffic proxy:

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

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

5. Click **Add**.
The new traffic proxy appears under the Traffic Proxies area of the page.
6. Under the new proxy, select **Enabled**.
7. In the Proxy Ports section for the new proxy, enter a port number, and then click **Add**.
You can specify more than one proxy port by entering another port number and clicking **Add**.
8. Check **Enabled** next to the port number(s).
9. Click **Save**. The traffic proxy is now available to use in an Enforcement Point.

 **Note:**

- [Configuring Enforcement Points](#) (page 6-20)
- [Logging in to the Database Firewall Console UI](#) (page 1-13)
- [Applying Static Routing Rules On Network Interfaces For Audit Vault Server And Database Firewall](#) (page H-7)

4.8 Configuring an Interface Masters Niagara Server Adapter Card

Learn how to configure an Interface Masters Niagara Server adapter card

 **Caution:**

Oracle Audit Vault and Database Firewall release 12.2.0.11.0 does not support Niagara cards. Do not upgrade to this release if you use Niagara cards.

Use this procedure to configure an Interface Masters Niagara Server Adapter Card. The drivers are available when you install Oracle Audit Vault and Database Firewall.

1. Log in to the Database Firewall command shell as the root user.
2. Edit the `/etc/init.d/dbfw.niagara` file as follows:
 - a. Find the line `INSTALLED_NIAGARA_CARDS=0`.
 - b. Change the `0` to match the number of installed Niagara cards for this Database Firewall.
3. Restart the Database Firewall.

 **See Also:**

- [Oracle Audit Vault and Database Firewall Installation Guide](#) for a complete list of supported Network Interface Cards.
- [Restarting or Powering Off Oracle Database Firewall](#) (page 14-40)

4.9 Viewing the Status and Diagnostics Report for a Database Firewall

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

1. Log in to the Database Firewall administration console.

2. In the **System** menu, click **Status**.

The Status page is displayed by default. The Status page displays the uptime, software version, component versions, grammar pack versions, free space, and diagnostic status for this Database Firewall.

The text next to **Diagnostic Status** indicates `OK` or `Errors`.

3. Next to the **Diagnostic Status** field, select one of the following:
 - **Show Report** to see an overview of diagnostic status.
 - **Download Diagnostics** to download all diagnostics files.

 **See Also:**

[Logging in to the Database Firewall Console UI](#) (page 1-13)

4.10 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.

Starting with release 12.2.0.6.0, 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.

The following file contains instructions about how to install, enable, and run the diagnostic utility:

```
diagnostics-not-enabled.readme
```

 **See Also:**

This file is generated only if you follow the instructions for downloading the diagnostics report. See [Viewing the Status and Diagnostics Report for a Database Firewall](#) (page 4-12) for more information.

Use the following commands to accomplish certain tasks related to diagnostics.

Command	Action
<code>/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb</code>	To capture the enabled diagnostic information for the appliance. The location of the saved zip file is displayed at the end of the command execution. Note: This command must be run from <code>/usr/local/dbfw/tmp</code> when collecting diagnostics information.
<code>/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --install</code>	To enable the system to capture diagnostics report.
<code>/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --enable ALL</code>	To enable capturing the complete diagnostics report.
<code>/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb -enable <Element></code>	To enable individual elements in the diagnostics report.

The following elements can be included while customizing the diagnostics report:

```
SYSTEM
LOG
DATABASE
AVS_ARCHIVE
DBFW_ARCHIVE
PLATFORM_COMMANDS
AVS_HA_COMMANDS
AVS_COMMANDS
DBFW_COMMANDS
```

The content of the diagnostics report is controlled by the file `/usr/local/dbfw/etc/dbfw-diagnostics-package.yml`. The user can modify this file to include and exclude a combination of files in multiple categories. Each section of this file has an option to enable and disable the specific category by setting the value to `true` or `false`.

For example, to add an item to one of the log file collections simply add the file path or glob to the list under the `:files:` element.

```
:log_files:
  :comment: Log files generated by the system runtime, install and
  upgrade.
  :enabled: false
  :platform:
    - AVS
    - DBFW
  :files:
```

- /root/apply.out
- /root/install.log
- /root/install.log.syslog
- /root/install_database_api.log
- /root/migration-stats-*.yaml
- /root/once.log
- /root/pre_firstboot_logs/partition-include
- /root/pre_firstboot_logs/partitions_error
- /root/pre_firstboot_logs/syslog
- /var/lib/avdf/system_history.yaml
- /var/log
- /path/to/new/file
- /path/to/new/*glob

To add a new command output to the log, add the command to the correct group:

```
:all_commands:
  :comment: Command output to include in the diagnostics package.
  :enabled: false
  :platform:
    - AVS
    - DBFW
  :commands:
    :cpuinfo:
      :enabled: true
      :command:
        - :cat
        - /proc/cpuinfo
```

```
:logfile: /proc-cpuinfo.log

:diskuse:

:enabled: true

:command:

- :df

- -kP

:logfile: /disk-usage.log

:new_command

:enabled: true

:command:

- :new_command

- -arg1

- -arg2

:logfile: /new-command.log
```



Note:

To remove the diagnostic package when it is not in use, run the following command:

```
/usr/local/dbfw/bin/priv/dbfw-diagnostics-package.rb --remove
```

5

Registering Hosts and Deploying the Agent

Topics

- [Registering Hosts in the Audit Vault Server](#) (page 5-1)
- [Deploying and Activating the Audit Vault Agent on Host Computers](#) (page 5-3)
- [Stopping, Starting, and Other Agent Operations](#) (page 5-9)
- [Updating Oracle Audit Vault Agent](#) (page 5-12)
- [Deploying Plug-ins and Registering Plug-in Hosts](#) (page 5-13)
- [Deleting Hosts from the Audit Vault Server](#) (page 5-16)

5.1 Registering Hosts in the Audit Vault Server

Topics

- [About Registering Hosts](#) (page 5-1)
- [Registering Hosts in the Audit Vault Server](#) (page 5-2)
- [Changing Host Names](#) (page 5-3)

5.1.1 About Registering Hosts

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

After registering a host, you must then deploy and activate the Audit Vault Agent on that host.

This chapter assumes the Audit Vault Agent is deployed on the secured target host, and describes the procedures for registering hosts using the Audit Vault Server console UI.

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

 **See Also:**

- [Registering Secured Targets](#) (page 6-3)
- [Configuring and Managing Audit Trail Collection](#) (page 6-9)
- [Summary of Configuration Steps](#) (page 1-6) to understand the high-level workflow for configuring the Oracle Audit Vault and Database Firewall system.
- [Using the Audit Vault Command-Line Interface](#) (page 1-15)
- [Deploying and Activating the Audit Vault Agent on Host Computers](#) (page 5-3)

5.1.2 Registering Hosts in the Audit Vault Server

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

To register a host machine in the Audit Vault Server:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Hosts** tab.
A list of the registered hosts, if present, appears in the **Hosts** page.
3. Click **Register**.
4. Enter the **Host Name** which is mandatory. Entering the **Host IP** address is optional.

If you enter a host name only, you must have a DNS server configured.

5. Click **Save**.

An Agent Activation Key is automatically generated when you register the host.

 **See Also:**

- [REGISTER HOST](#) (page A-2) for the command line syntax to register a host.
- [Configuring or Changing the Oracle Audit Vault Server Services](#) (page 3-7) to configure DNS server.
- [Working with Lists of Objects in the UI](#) (page 1-12) to control the view of registered hosts listed in the **Hosts** page.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

5.1.3 Changing Host Names

After you change a host name, the change takes place immediately. You do not need to restart the host Audit Vault Server.

▲ Caution:

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

Prerequisite

Log in to the Audit Vault Server console as an *administrator*. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To change the name of a registered host:

1. Click the **Hosts** tab.
2. Click the name of the host you want to change.
3. In the Modify Host page, change the **Host Name** field, and then click **Save**.
4. Wait for the system to automatically reboot.

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

5.2 Deploying and Activating the Audit Vault Agent on Host Computers

Learn about how to deploy and activate the Audit Vault Agent on host computers.

5.2.1 About Deploying the Audit Vault Agent

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

In addition to deploying the Audit Vault Agent, in order to start audit trail collections you must also register each host, register secured targets, configure audit trails, and start audit trail collections manually (thereafter, audit trails start automatically when the Audit Vault Agent is restarted, or updated due to an Audit Vault Server update).

To deploy the Audit Vault Agent in Oracle RAC environment, follow these guidelines.

Trail Type	Guideline
TABLE	To configure TABLE trail, deploy one Audit Vault Agent on a remote host.

Trail Type	Guideline
DIRECTORY	To configure DIRECTORY trail, deploy one Audit Vault Agent. This is sufficient in case the audit trails are configured as described in section Configuring Audit Trail Collection for Oracle Real Application Clusters (page 6-18).
TRANSACTION LOG (REDO)	To configure TRANSACTION LOG trail, deploy one Audit Vault Agent on a remote host.

Table 5-1 OS Permission Required For Installing The Agent

Operating System	User
Linux/Unix	Any user.
Windows	Any user for running the Agent from the command prompt. <i>admin</i> user for registering as a service.

 **Note:**

- Host Monitor 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 on Windows platform is not certified in release 12.2.0.11.0.
If your installation is 12.2.0.10.0 and prior, then Host Monitor must be installed as *admin* user.
- Ensure that the host machine has *OpenSSL 1.0.1* (or later) installed for Audit Vault Agent

 **See Also:**

- [Registering Hosts in the Audit Vault Server](#) (page 5-1)
- [Registering Secured Targets and Creating Groups](#) (page 6-2)
- [Configuring and Managing Audit Trail Collection](#) (page 6-9)
- [Summary of Configuration Steps](#) (page 1-6) to understand the high-level workflow for configuring the Oracle Audit Vault and Database Firewall system.
- [Adding an Audit Trail in the Audit Vault Server](#) (page 6-9) to configure an audit trail.

5.2.2 Steps Required to Deploy and Activate the Audit Vault Agent

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

1. [Registering the Host](#) (page 5-5)
2. [Deploying the Audit Vault Agent on the Host Computer](#) (page 5-5).
3. [Activating and Starting the Audit Vault Agent](#) (page 5-6).

5.2.3 Registering the Host

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

5.2.4 Deploying the Audit Vault Agent on the Host Computer

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



Note:

Ensure that the host machine has *OpenSSL 1.0.1* (or later) installed for Audit Vault Agent.



See Also:

The Audit Vault Agent is supported on Unix, Windows, and HP-UX Itanium platforms, and requires `Java` version *1.8* to be installed on the host computer. See *Oracle Audit Vault and Database Firewall Installation Guide* for Agent platform support details for the current release and for the supported `Java` versions. For supported platforms in prior releases, see **Article 1536380.1** at the Oracle Support website: <https://support.oracle.com>

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

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Hosts** tab, and then from the **Hosts** menu, click **Agent**.

The Agent and host monitor files are listed.

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

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.

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

 **Best Practice:**

Do not install the Audit Vault Agent as *root* user.

5. On the host machine, set the `JAVA_HOME` environment variable to the installation directory of the `Jdk`, and make sure the `Java` executable corresponds to this `JAVA_HOME` setting.

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

6. Start a command prompt with **Run as Administrator**.
7. In the directory where you placed the `agent.jar` file, extract it by running:

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

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

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

 **Caution:**

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

5.2.5 Activating and Starting the Audit Vault Agent

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

Prerequisites

- Follow and complete the procedure in [Registering Hosts in the Audit Vault Server](#) (page 5-1).
- Log in to the Audit Vault Server console as an *administrator*. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To activate and start the agent:

1. Click on the **Hosts** tab.
2. On the **Hosts** tab, make a note of the Agent Activation Key for this host.
3. On the host machine, change directory as follows:

```
cd Agent_Home/bin
```

`Agent_Home` is the directory created in the step 7 (page 5-6) above.

4. Run one of the following command and provide the Agent Activation Key:

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

Enter the activation key when prompted. This key will not be 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](#) (page 5-7) 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](#) (page A-6) for the command line syntax to activate the Agent.

5.2.6 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.

5.2.6.1 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 on the Host Computer](#) (page 5-5)

5.2.6.2 Registering the 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:

- 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 any of the directories defined in the PATH variable.
- Add the directory path where `msvcr110.dll` is present to the PATH variable. For example: `C:\Windows\System32`
- Copy the `msvcr110.dll` file that is compatible with the Windows target machine to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` folders.

To register the 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 dialogue.
- 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.

5.2.6.3 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
```

5.3 Stopping, Starting, and Other Agent Operations

Topics

- [Stopping and Starting Oracle Audit Vault Agent](#) (page 5-9)
- [Changing the Logging Level for the Audit Vault Agent](#) (page 5-11)
- [Viewing the Status and Details of an Audit Vault Agent](#) (page 5-11)
- [Deactivating and Removing the Audit Vault Agent](#) (page 5-12)

5.3.1 Stopping and Starting Oracle Audit Vault Agent

Learn about stopping and starting Oracle Audit Vault Agent.

Topics



Important:

Stop and start the Audit Vault Agent as the same OS user account that you used during installation.

5.3.1.1 Stopping and Starting the Agent on Unix Hosts

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

```
agentctl stop
```

```
agentctl start
```

5.3.1.2 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 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](#)
(page 5-7)

To stop or start the Agent Windows service

Use one of the methods below:

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

```
agentctl stopsvc
```

```
agentctl startsvc
```

To check that the Windows service is stopped

Run this command:

```
cmd> sc queryex OracleAVAgent
```

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

To stop or start the Agent in console mode

```
start /b agentctl stop
```

```
start /b agentctl start
```

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.

5.3.1.3 Autostarting the Agent on 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 on **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.

5.3.2 Changing the Logging Level for the Audit Vault Agent

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

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

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

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

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 "[Changing Logging Levels and Clearing Diagnostic Logs](#) (page 14-5)".

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`.

5.3.3 Viewing the Status and Details of an 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 [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To view the status and details of an Audit Vault Agent:

1. Click the **Hosts** tab.
2. Check the **Agent Status**, **Agent Activation Key**, and **Agent Details** columns for the host that you are interested in.
3. To see the audit trails for a specific agent host, click **View Audit Trails** in the **Agent Details** column.

5.3.4 Deactivating and Removing the Audit Vault Agent

Use this procedure to deactivate and remove the 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](#) (page 5-7) to unregister the service.

To deactivate and remove the Audit Vault Agent:

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

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

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 secured targets. It sends this data to the specific Audit Vault Server. To configure the audit trail collection from the existing secured 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.

5.4 Updating Oracle Audit Vault Agent

Learn about updating Oracle Audit Vault Agent.

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

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

As of Oracle Audit Vault and Database Firewall 12.2.0, 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 this Audit Vault Agent automatically restart if you have not explicitly stopped them. If you upgrade the Audit Vault Server to 12.2.0 from a prior release, 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.

5.5 Deploying Plug-ins and Registering Plug-in Hosts

Topics

- [About Plug-ins](#) (page 5-13)
- [Ensuring that Auditing is Enabled in the Secured Target](#) (page 5-14)
- [Registering the Plug-in Host in Audit Vault Server](#) (page 5-14)
- [Deploying and Activating the Plug-in](#) (page 5-14)
- [Un-Deploying Plug-ins](#) (page 5-15)

5.5.1 About Plug-ins

Each type of secured target has a corresponding software plug-in in the Audit Vault Server, which enables the Audit Vault Agent to collect audit data. You can deploy more plug-ins, in addition to those shipped with Oracle Audit Vault and Database Firewall, in order to collect audit data from more secured target types. New plug-ins are available from Oracle Technology Network or third parties.

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

To start collecting audit data from the secured target type associated with a plug-in, you must also add the secured target in the Audit Vault Server, then configure and manually start audit trail collection.

 **See Also:**

[Configuring Secured Targets, Audit Trails, and Enforcement Points](#) (page 6-1)

Deploying a plug-in consists of three steps:

1. [Ensuring that Auditing is Enabled in the Secured Target](#) (page 5-14)
2. [Registering the Plug-in Host in Audit Vault Server](#) (page 5-14)
3. [Deploying and Activating the Plug-in](#) (page 5-14)

5.5.2 Ensuring that Auditing is Enabled in the Secured Target

Ensure that auditing has been enabled in the secured target. See the secured target's product documentation for more information.



See Also:

[Ensuring that Auditing is Enabled on the Secured Target](#) (page 6-8) for information on plug-ins for Oracle Database.

5.5.3 Registering the Plug-in Host in Audit Vault Server

To register a host in the Audit Vault Server, see "[Registering Hosts in the Audit Vault Server](#) (page 5-2)".

5.5.4 Deploying and Activating the Plug-in

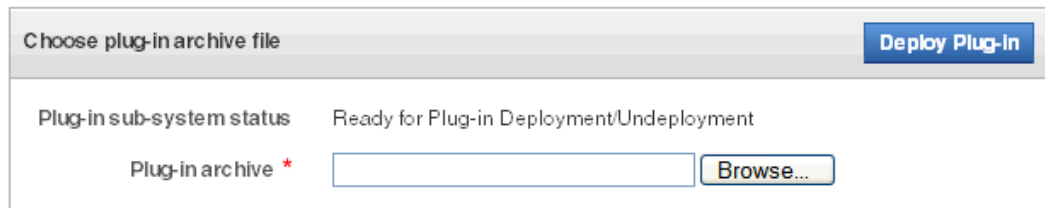
To deploy and activate a plug-in:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Settings** tab, and from the **System** menu, click **Plug-ins**.

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

<input type="checkbox"/>	Plugin Name ▲	Version	Plugin ID	Deployed Time	Secured Target Type
<input type="checkbox"/>	IBM DB2 LUW Plug-in	12.1.1.0.0	com.oracle.avplugin.db2	7/1/2013 10:31:09 AM	IBM DB2 LUW
<input type="checkbox"/>	Linux Plug-in	12.1.1.0.0	com.oracle.avplugin.linuxos	7/1/2013 10:31:09 AM	Linux
<input type="checkbox"/>	Microsoft Active Directory Plug-in	12.1.1.0.0	com.oracle.avplugin.msad	7/1/2013 10:31:09 AM	Microsoft Active Directory Server

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



Choose plug-in archive file Deploy Plug-in

Plug-in sub-system status Ready for Plug-in Deployment/Undeployment

Plug-in archive * Browse...

4. Click **Deploy Plug-in**.

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

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

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

Register the host machine in case it is not registered.

6. On the host machine, extract the agent:

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

 **Note:**

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

 **See Also:**

- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)
- [Registering Hosts in the Audit Vault Server](#) (page 5-2)

5.5.5 Un-Deploying Plug-ins

To un-deploy a plug-in:

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

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

5.6 Deleting Hosts from the Audit Vault Server

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

To delete hosts:

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

A list of the registered hosts, if present, appears in the **Hosts** page.

3. Select the host(s) you want to delete, and then click **Delete**.

See Also:

- [Working with Lists of Objects in the UI](#) (page 1-12) to control the view of registered hosts listed.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6

Configuring Secured Targets, Audit Trails, and Enforcement Points

Topics

- [About Configuring Secured Targets](#) (page 6-1)
- [Registering Secured Targets and Creating Groups](#) (page 6-2)
- [Preparing Secured Targets for Audit Data Collection](#) (page 6-7)
- [Configuring and Managing Audit Trail Collection](#) (page 6-9)
- [Configuring Enforcement Points](#) (page 6-20)
- [Configuring Stored Procedure Auditing \(SPA\)](#) (page 6-24)
- [Configuring and Using Database Interrogation](#) (page 6-24)
- [Configuring Oracle Database Firewall for Databases That Use Network Encryption](#) (page 6-29)
- [Configuring and Using Database Response Monitoring](#) (page 6-32)
- [Securing the Agent and Oracle Database Secure Target Connection](#) (page 6-34)

6.1 About Configuring Secured Targets

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

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

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

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

If you are using the Database Firewall, you can also monitor the secured target database's responses to incoming SQL traffic. The following sections contain the high-level workflow for configuring the Oracle Audit Vault and Database Firewall system.

 **See Also:**

- [Configuring Oracle AVDF and Deploying the Audit Vault Agent](#) (page 1-6)
- [Configuring Oracle AVDF and Deploying the Database Firewall](#) (page 1-7)

6.2 Registering Secured Targets and Creating Groups

Topics

- [Registering or Removing Secured Targets in the Audit Vault Server](#) (page 6-2)
- [Creating or Modifying Secured Target Groups](#) (page 6-6)
- [Controlling Access to Secured Targets and Target Groups](#) (page 6-7)
- [Removing Secured Targets](#) (page 6-5)

6.2.1 Registering or Removing Secured Targets in the Audit Vault Server

Topics

- [About Secured Targets in the Audit Vault Server](#) (page 6-2)
- [Registering Secured Targets](#) (page 6-3)
- [Modifying Secured Targets](#) (page 6-5)
- [Removing Secured Targets](#) (page 6-5)

6.2.1.1 About Secured Targets in the Audit Vault Server

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

Important: In the following procedure, if you specify service names and/or SIDs, then the Database Firewall only captures traffic to the service names and/or SIDs listed. In this case, if a database client connects using a different service name or SID than those listed, the Database Firewall does not monitor that traffic. As a best practice to avoid this problem, follow these guidelines:

- Define the configuration and policies that use Oracle service names for each and every service that runs on a protected Oracle secured target. This ensures that the configuration enables each policy to be applied to the correct Oracle service name.
- Always define a catch-all secured target (and associated enforcement point) to process the database traffic that does not match the Oracle service names that were explicitly configured in the previous secured targets. This new secured target should have the same IP address and TCP port number, but the Oracle service name should be left blank, and should have a "log-all" policy applied. This way,

any traffic that the secured targets with explicitly defined Oracle service names do not capture is logged and can be examined. Based on your findings, you then can tighten the configuration and policies so all traffic that reaches an Oracle service name is captured in an explicit fashion.

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

6.2.1.2 Registering Secured Targets

To register a secured target in the Audit Vault Server:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Secured Targets** tab.
 The **Secured Targets** page lists the configured secured targets to which you have access. You can sort or filter the list of targets.
3. Click **Register** to register a new target.
4. In the **Register Secured Target** page, enter a **New Secured Target Name** and optional **Description** for the new target.
5. In the **Secured Target Type** field, select the secured target type. For example, Oracle Database.
6. Optionally enter the **Secured Target Location (For Auditing)** settings. This is required for the agent to collect audit data, but not required to deploy Database Firewall only.

In the **Secured Target Location (For Auditing)** section, choose the **Basic** option. Enter the **Host Name or IP Address**, **Port**, and for Oracle Databases, the **Service Name** (or SID).

If you know the exact connect string, you can click the **Advanced** radio button instead, and enter the string there.

For example, for Oracle Database, the string might look like the following:

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

When you configure an Oracle RAC secured target for agent data collection, enter the SCAN host name. Oracle RAC secure target can be configured with Oracle Database Firewall for protection.

7. If required by the secured target type, enter the **User Name** and **Password** fields. These are the credentials for the secured target user account you created for Oracle Audit Vault and Database Firewall.

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

- **Host Name / IP Address**
- **Port Number**
- **Service Name** (Optional, for Oracle Database only)

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

If you want to enforce different Database Firewall policies for different service names or SIDs on the same database, then you must create a separate secured target for each service name or SID.

 **Note:**

- In case the secured target is Oracle Real Application Cluster (RAC), the IP (or hostname) is the *SCAN* name of cluster node. The *PORT* is the port on which the remote listener is running. See [How to Configure an Oracle Grid Infrastructure SCAN Listener](#) for detailed steps to configure SCAN name for Oracle RAC environment.
- In case the secured target is Microsoft SQL Server Cluster, a mandatory collection attribute needs to be set. See section [Microsoft SQL Server](#) (page B-6) for complete information.

9. If required, enter values for **Attribute Name** and **Attribute Value** in the **Collection Attributes** section. Click **Add**.

Collection attributes may be required by the Audit Vault Agent depending on the secured target type.

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

Attribute Name: `MAXIMUM_ENFORCEMENT_POINT_THREADS`

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

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

11. Click **Save**.

 **Note:**

TCPS must be configured for registering Hybrid Cloud Oracle Databases. See [Securing the Agent and Oracle Database Secure Target Connection](#) (page 6-34).

 **See Also:**

- [Collection Attributes](#) (page B-38) to look up requirements for a specific secured target type.
- [Using an Oracle Database Firewall with Oracle RAC](#) (page 11-1) to configure Oracle Database Firewall in an Oracle RAC environment.
- [Working with Lists of Objects in the UI](#) (page 1-12) to sort or filter the list of secured targets.
- [Secured Target Locations \(Connect Strings\)](#) (page B-36)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)
- [Setting User Account Privileges on Secured Targets](#) (page 6-8)

6.2.1.3 Modifying Secured Targets

To modify a secured target:

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

The Secured Targets page lists the configured secured targets to which you have access. You can sort or filter the list of targets.

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

 **Note:**

If you change the name of a secured target, the new name does not appear in Oracle Audit Vault and Database Firewall reports until you restart the Audit Vault Agent.

 **See Also:**

- [Registering Secured Targets](#) (page 6-3) for description of the fields in the **Modify Secured Target** page.
- [Working with Lists of Objects in the UI](#) (page 1-12) to sort or filter the list of secured targets.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.2.1.4 Removing Secured Targets

If you no longer need to have a secured target registered with Oracle AVDF, you can use either the console or the command-line utility to remove the secured target. After you have

removed the secured target from Oracle AVDF, its audit data still resides in the data warehouse within its retention period (archiving policy).

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

To remove a secured target:

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

 **See Also:**

- [Creating or Deleting Archiving Policies](#) (page 3-17) for information on archiving (retention) policies.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.2.2 Creating or Modifying Secured Target Groups

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

To create a secured target group:

1. Log into the Oracle Audit Vault and Database Firewall console as a super administrator, and click the **Secured Targets** tab.
2. Click the **Groups** menu on the left.
Preconfigured groups are listed in the top pane, and user defined groups are listed in the bottom pane.
You can adjust the appearance of the list in the bottom pane from the **Actions** menu.
3. Click **Create**, and enter a name and optional description for the group.
4. To add secured targets to the group, select the secured targets, and click **Add Members**.
5. Click **Save**.

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

To modify a secured target group:

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

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

You can adjust the appearance of the list in the bottom pane from the **Actions** menu.

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



See Also:

[Working with Lists of Objects in the UI](#) (page 1-12) to adjust the appearance of the list in the bottom pane from the **Actions** menu.

6.2.3 Controlling Access to Secured Targets and Target Groups

Oracle Audit Vault and Database Firewall super administrators can control which administrators have access to secured targets or secured target groups. You can control access for an individual user, or for an individual secured target or group.



See Also:

[Managing User Access Rights to Secured Targets or Groups](#) (page 13-7)

6.3 Preparing Secured Targets for Audit Data Collection

Topics

- [Using an NTP Service to set Time on Secured Targets](#) (page 6-7)
- [Ensuring that Auditing is Enabled on the Secured Target](#) (page 6-8)
- [Setting User Account Privileges on Secured Targets](#) (page 6-8)
- [Scheduling Audit Trail Cleanup](#) (page 6-9)

6.3.1 Using an NTP Service to set Time on Secured Targets

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

 **See Also:**

[Specifying the Server Date, Time, and Keyboard Settings](#) (page 3-3) for instructions on using an NTP server to set time for the Audit Vault Server.

6.3.2 Ensuring that Auditing is Enabled on the Secured Target

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

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

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

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

2. Run the following command:

```
SHOW PARAMETER AUDIT_TRAIL
```

NAME	TYPE	VALUE
audit_trail	string	DB

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

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

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

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

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

STARTUP
ORACLE instance started.
```

4. Make a note of the audit trail setting.

You will need this information when you configure the audit trail in Oracle Audit Vault and Database Firewall.

6.3.3 Setting User Account Privileges on Secured Targets

Some secured target types require credentials in order for Oracle Audit Vault and Database Firewall to access them. If you plan to collect audit data from a secured

target, do stored procedure auditing (SPA), entitlements auditing, or enable database interrogation, you must create a user account on the secured target with the appropriate privileges to allow Oracle Audit Vault and Database Firewall to access the required data.

Setup scripts for database secured targets: Oracle Audit Vault and Database Firewall provides scripts to configure user account privileges for database secured target types.

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

 **Note:**

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

 **See Also:**

[Scripts for Oracle AVDF Account Privileges on Secured Targets](#) (page B-21) for information on scripts to configure user account privileges for database secured target types.

6.3.4 Scheduling Audit Trail Cleanup

Learn about scheduling audit trail cleanup.

Oracle Audit Vault and Database Firewall supports audit trail cleanup for Oracle Database, Microsoft SQL Server, and MySQL.

 **See Also:**

[Audit Trail Cleanup](#) (page B-32)

6.4 Configuring and Managing Audit Trail Collection

Learn about configuring and managing audit trail collection.

6.4.1 Adding an Audit Trail in the Audit Vault Server

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

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

Prerequisites

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

- Add the secured target in the Audit Vault Server. See [Registering or Removing Secured Targets in the Audit Vault Server](#) (page 6-2) for details.
- Register the host machine. This is usually the machine where both the secured target resides and the Audit Vault Agent is deployed. See [Registering Hosts and Deploying the Agent](#) (page 5-1).
- Deploy and activate the Audit Vault Agent on the host machine. See [Deploying and Activating the Audit Vault Agent on Host Computers](#) (page 5-3).
- For MySQL secured targets, run the XML transformation utility. For IBM DB2 secured targets, ensure that the binary audit file has been converted to ASCII format before starting an audit trail. See [Converting Audit Record Format For Collection](#) (page 6-14).
- Log in to the Audit Vault Server console as an *administrator*. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To configure an audit trail for a secured target:

1. Click the **Secured Targets** tab.
2. Under **Monitoring**, click **Audit Trails**.
The Audit Trails page appears, listing the configured audit trails and their status.
3. In the Audit Trails page, click **Add**.
4. From the **Audit Trail Type** drop-down list, select one of the following:
 - CUSTOM
 - DIRECTORY
 - EVENT LOG
 - NETWORK
 - SYSLOG

This trail type can collect from either `syslog` or `rsyslog` files. If both are present, you must give the exact **Trail Location** (in step 7 (page 6-11)) if you want to collect audit data from `rsyslog` files. See [Table B-23](#) (page B-42) for details.

Important: Be sure that records generated by `rsyslog` have the same timezone information as the Audit Vault Agent running on the **Collection Host**.

 - TABLE
 - TRANSACTION LOG

For this audit trail type, ensure that the secured target database has a fully qualified database name. See the `GLOBAL_NAMES` setting in [Table C-1](#) (page C-2).

See [Table B-17](#) (page B-18) for details on which type(s) of audit trails can be collected for a specific secured target type.
5. In the **Collection Host** field, click the up-arrow icon to display a search box, and then find and select the host computer where the Audit Vault Agent is deployed.

6. In the **Secured Target** field, click the up-arrow icon to display a search box, and then find and select the secured target.
7. In the **Trail Location** field, enter the location of the audit trail on the secured target computer, for example, `sys.aud$`.

The trail location depends on the type of secured target.

Note 1: If you selected DIRECTORY for **Audit Trail Type**, the Trail Location must be a directory mask.

Note 2: If you selected SYSLOG for **Audit Trail Type**, and both `syslog` and `rsyslog` file types are present, enter the exact directory location of either the `syslog` or `rsyslog` files. See [Table B-23](#) (page B-42) for important details.

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

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

See Also:

- [Summary of Data Collected for Each Audit Trail Type](#) (page B-17) for descriptions of data collected.
- [Audit Trail Locations](#) (page B-42) for supported trail locations.
- [About Plug-ins](#) (page 5-13)

6.4.2 Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server

An audit trail starts automatically shortly after you add it. In order to start an audit trail, the Audit Vault Agent must be running on a host computer.

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 secured 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.

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

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

You cannot start an audit trail while the Audit Vault Agent is updating.

 **Note:**

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

 **See Also:**

- [ALTER SYSTEM SET](#) (page A-56) to set parameters on when and how many times the system attempts Autostart using the AVCLI utility.
- [Deploying and Activating the Audit Vault Agent on Host Computers](#) (page 5-3)
- [Updating Oracle Audit Vault Agent](#) (page 5-12)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.4.3 Checking the Status of Audit Trails in the Audit Vault Server

To check the status of audit trails:

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

The Audit Trails page lists audit trails and their status in the **Collection Status** column, along with other details. The status may 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 Secured 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 has collected a batch of audit data and is setting a checkpoint on the Audit Vault Server. This can take a while depending on the server load.
- **Unreachable** - A heartbeat timeout has occurred, indicating that a heartbeat message has not been received from the trail in the last two minutes. This status is temporary unless the trail has crashed.
- **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 secured 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, you can click the **Hosts** tab, and in the **Agent Details** column for that host click **View Audit Trails**.

 **Note:**

If an audit trail fails to start, you can get more information by showing the **Error Message** column:

1. In the Audit Trails page, click the **Actions** button, then click **Select Columns**.
2. Double-click **Error Message** on the left to move it to the Display in Report box, and then click **Apply**.

 **See Also:**

- [Working with Lists of Objects in the UI](#) (page 1-12) to sort and filter the audit trail list.
- [Handling new Audit Trails with Expired Audit Records](#) (page 6-13)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.4.4 Handling new Audit Trails with Expired Audit Records

With established audit trail collection, audit data is retained in the 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 secured target, the audit data collected may contain records that fall into the Months Archived period in the retention policy assigned to this secured 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 secured 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 **Secured 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](#) (page 3-13) 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](#) (page 3-12)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.4.5 Deleting an Audit Trail

Follow these steps to delete an audit trail:

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

 **See Also:**

- [Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server](#) (page 6-11)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.4.6 Converting Audit Record Format For Collection

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.

Running The XML Transformation Utility For MySQL Auditing

For MySQL secured 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.

Prerequisites

- Register the MySQL secured target in the Audit Vault Server. See [Registering or Removing Secured Targets in the Audit Vault Server](#) (page 6-2).
- Deploy the Audit Vault Agent on the MySQL host machine. See [Deploying the Audit Vault Agent on the Host Computer](#) (page 5-5).

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 secured target in the Audit Vault Server, or when starting audit trail collection using the `AVCLI` command line.
- *path_to_AGENT_HOME* - The path to the installation directory of the Audit Vault Agent
- *interval_in_minutes* - (Optional) The waiting time, in minutes, between two transformation operations. If not specified, the default it is 60 minutes. To run the transformation utility once, specify `-ve` for this argument.
- *XSL_file_path* - (Optional) The path to the XSL file to use for the transformation.
- *registered_secured_target_name* - The name of the MySQL secured target registered in the Audit Vault Server.

Example:

```
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
```

Converting Binary Audit Files to ASCII Format

Converting Binary Audit Files to ASCII Format For IBM DB2 Auditing

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

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

Note:

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

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

1. Identify a user who has privileges to run the `db2audit` command.
This user will extract the binary files to the text files.
2. Grant the user you identified in Step 1 execute privileges to run the conversion script from the Oracle AVDF directory. The script name is:
 - **DB2 release 8.2 databases:** `DB282ExtractionUtil` (for Microsoft Windows, this file is called `DB282ExtractionUtil.bat`.)
 - **DB2 9.5 release databases:** `DB295ExtractionUtil` (for Microsoft Windows, this file is called `DB295ExtractionUtil.bat`.)
3. Grant the user you identified in Step 1 read permission for the `$AGENT_HOME/av/atc` directory and its contents.
4. In the server where you installed the IBM DB2 database, open a shell as the `SYSADM DB2` user.
5. Set the following variables:
 - `AGENT_HOME` (this is the Audit Vault Agent installation directory)
 - `DB2AUDIT_HOME` (this directory points to the main directory that contains the `db2audit` command)
6. Ensure that the Oracle AVDF owner of the agent process has read permissions for the audit text files that will be generated by the extraction utility.

7. Log in as the DB2 user that you identified in "IBM DB2 for LUW Setup Scripts (page B-29)".
8. Run one of the following scripts, depending on the version of DB2 that you have installed:

- **For DB2 release 8.2 databases:**

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

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

UNIX: *DB2_HOME*/sqlib/security/auditdata

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

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

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

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

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

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

- **For DB2 release 9.5 databases:**

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

In this specification:

- *archive_path*: This is DB2 archive path configured using the *db2audit* utility.
- *extraction_path*: This is the directory where the DB2 extraction utility places the converted ASCII text file. This file is created in either the *db2audit.instance.log.0.YYYYDDMMHHMMSS.out* or *db2audit.db.database_name.log.0.20111104015353.out* format.
- *yes/no*: Enter *yes* or *no*, to enable or disable the audit trail cleanup. Entering *yes* deletes the archived IBM DB2 audit files that were collected by the Oracle AVDF DB2 audit trail. If you omit this value, then the default is *no*.
- *database_name*: (Optional) This is the name, or names separated by spaces, of the database(s) that contain the audit records.

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

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

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

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

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

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

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

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

6.4.7 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 (REDO)	To configure Transaction Log (REDO) audit data collection from Oracle RAC environment, 1 audit trail is sufficient.



See Also:

[Adding an Audit Trail in the Audit Vault Server](#) (page 6-9) to configure an audit trail.

6.4.8 Configuring Audit Trail Collection For CDB And PDB

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 12c are non-CDB.

The PDB and CDB can be registered as secured 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 you must create a separate secured target for each PDB instance.

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	<ul style="list-style-type: none"> Audit records can be collected from audit tables of CDB. They contain audit details of only CDB activities. Every PDB has its own audit tables for storing audit data that are independent of each other. Hence, separate audit trails are needed for every PDB to collect audit data. CDB level audit collection of PDB audit is not supported.
DIRECTORY	<ul style="list-style-type: none"> 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>. <p>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.</p>
TRANSACTION LOG (REDO)	Transaction log collection is not supported for PDB or CDB.
Audit Policy Retrieval and Provisioning	Audit policies can be provisioned or retrieved by treating every PDB as an independent secured target.



Note:

Audit collection from CDB_UNIFIED_AUDIT_TRAIL is not supported.



See Also:

[Adding an Audit Trail in the Audit Vault Server](#) (page 6-9) to configure an audit trail.

6.5 Configuring Enforcement Points

Learn about configuring enforcement 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.

6.5.1 About Configuring Enforcement Points for Secured Targets

If you are monitoring databases with a Database Firewall, you must configure one enforcement point for every secured target database that you want to monitor with the firewall. The enforcement point configuration lets you specify the firewall monitoring mode (monitoring only or blocking), identify the secured target database being monitored, the network traffic sources to that database, and the Database Firewall used for the enforcement point.

Before configuring enforcement points, configure network traffic sources as part of database firewall configuration.



See Also:

[Configuring Database Firewall and its Traffic Sources on Your Network](#) (page 4-8)

6.5.2 Creating and Configuring an Enforcement Point

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

Prerequisites

- Ensure that you have configured traffic sources on the Database Firewall you plan to use for this enforcement point. See [Configuring Database Firewall and its Traffic Sources on Your Network](#) (page 4-8) for more information.
- Log in to the Audit Vault Server console as an *administrator*. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To configure an enforcement point:

1. Click the **Secured Targets** tab, and from the **Monitoring** menu, click **Enforcement Points**.

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

2. Click **Create**.
3. Enter a **Name** for this enforcement point.
4. Select a **Monitoring Mode**:
 - **Database Policy Enforcement (DPE)** - to block or substitute SQL statements.
 - **Database Activity Monitoring (DAM)** - to log SQL statements and raise alerts only
5. In the **Select Secured Target to monitor** section, select a secured target.

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

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

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

7. Select traffic sources in either the **Bridged Interfaces** or the **Proxy Interfaces** area.
Note: If you select a proxy traffic source, you cannot select any other traffic sources. Also, selecting a proxy forces the Monitoring Mode to DPE.

8. Click **Save**.

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

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

Note:

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

 **See Also:**

- [Configuring High Availability](#) (page 8-1) for details on configuring a resilient pair of servers.
- *Oracle Audit Vault and Database Firewall Concepts Guide* for more information on different modes.
- [Configuring Traffic Sources](#) (page 4-9) for more information on traffic sources.
- [Configuring a Bridge in the Database Firewall](#) (page 4-9)
- [Configuring Oracle Database Firewall As A Traffic Proxy](#) (page 4-11)

6.5.3 Modifying an Enforcement Point

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

Advanced settings in the enforcement point let you configure Oracle Audit Vault and Database Firewall to work with BIG-IP Application Security Manager (ASM).

To modify an enforcement point:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click **Secured Targets** tab.
3. From the **Monitoring** menu, click **Enforcement Points**, and then click the name of the enforcement point you want to modify.
4. In the Modify Enforcement Point page, you can change the following settings:
 - **Secured Target** - Select a different secured target to monitor
 - **Monitoring Mode** - Select the alternate monitoring mode.
Note: If switching from DAM to DPE mode, select whether or not to **Maintain Existing Connections** from clients to your secured target database. If you select this option, existing connections will not be disrupted, but will need to reconnect to the secured target database before they can be monitored in DPE mode.
 - **Traffic Sources** - Enable different traffic sources.
 - **Database Response** - Select to enable database response monitoring.
 - **Database Interrogation** - Select to enable database interrogation.
5. Click **Save**.

 **See Also:**

- [Configuring Oracle Audit Vault and Database Firewall to Work with F5 BIG-IP Application Security Manager](#) (page 9-4) to configure Oracle Audit Vault and Database Firewall to work with BIG-IP Application Security Manager (ASM).
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)
- [Configuring and Using Database Response Monitoring](#) (page 6-32)
- [Configuring and Using Database Interrogation](#) (page 6-24)

6.5.4 Starting, Stopping, or Deleting Enforcement Points

To manage enforcement points:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Secured Targets** tab, and under **Monitoring**, click **Enforcement Points**.
3. Select the enforcement points you want, and click one of the following buttons:
 - **Start** to start the enforcement point
 - **Stop** to stop the enforcement point
 - **Delete** to delete the enforcement point

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.5.5 Viewing the Status of Enforcement Points

To view the status of enforcement points:

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

A list of enforcement points and their status is displayed. Possible status values are:

- **Up** - The enforcement point is up and running, and there are no errors.
- **Suspended** - The user has stopped the enforcement point, and there are no errors.
- **Down** - The enforcement point is not working, probably due to errors.
- **Unreachable** - There are communications errors between the Database Firewall and the Audit Vault Server.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.5.6 Finding the Port Number Used by an Enforcement Point

To find the port number used by an enforcement Point:

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

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

See Also:

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.6 Configuring Stored Procedure Auditing (SPA)

Stored procedure auditing (SPA) enables Oracle Audit Vault and Database Firewall auditors to audit changes to stored procedures on secured 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. SPA is supported for all database secured targets supported by Oracle Audit Vault and Database Firewall.

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 secured target. Oracle Audit Vault and Database Firewall provides scripts for setting up these privileges. Run the scripts specific to the secured 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 Secured Target configuration.

See Also:

- [Scripts for Oracle AVDF Account Privileges on Secured Targets](#) (page B-21)
- [Supported Secured Targets](#) (page 1-3)
- *Oracle Audit Vault and Database Firewall Auditor's Guide*

6.7 Configuring and Using Database Interrogation

Learn about configuring and using database interrogation.

6.7.1 About Database Interrogation

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

- [Using Database Interrogation for SQL Server and SQL Anywhere Databases](#) (page 6-25)
- [Using Database Interrogation for Oracle Databases with Network Encryption](#) (page 6-25)

6.7.1.1 Using Database Interrogation for SQL Server and SQL Anywhere Databases

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

To configure database interrogation for these two databases you must:

- Create a user account for Audit Vault and Database Firewall database interrogation on the database. Grant specific privileges to that user account.
- In Audit Vault and Database Firewall, enable database interrogation in the enforcement point that monitors the secured target database.

See Also:

- [Configuring Database Interrogation for SQL Server and SQL Anywhere](#) (page 6-26)
- [Enabling Database Interrogation](#) (page 6-27)

6.7.1.2 Using Database Interrogation for Oracle Databases with Network Encryption

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

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.



See Also:

[Configuring Oracle Database Firewall for Databases That Use Network Encryption](#) (page 6-29)

6.7.2 Configuring Database Interrogation for SQL Server and SQL Anywhere

Topics

- [Setting Database Interrogation Permissions in a Microsoft SQL Server Database](#) (page 6-26)
- [Setting Database Interrogation Permissions in a Sybase SQL Anywhere Database](#) (page 6-26)

6.7.2.1 Setting Database Interrogation Permissions in a Microsoft SQL Server Database

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

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

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

2. Grant the following permissions to the user account you created in Step 1:
 - `VIEW ANY DEFINITION` and `VIEW SERVER STATE` for SQL Server 2005 and later
 - `SELECT` on the `master.dbo.sysdatabases` table
3. Enable database interrogation in the enforcement point that monitors this secured target database, using the credentials you created in Step 1.



See Also:

[Enabling Database Interrogation](#) (page 6-27)

6.7.2.2 Setting Database Interrogation Permissions in a Sybase SQL Anywhere Database

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

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

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

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

2. Grant the following permissions to the user account you created in Step 1:

- CONNECT
- SELECT on these system tables:

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

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

 **See Also:**

[Enabling Database Interrogation](#) (page 6-27)

6.7.3 Enabling Database Interrogation

Use this procedure to enable Database Interrogation.

Prerequisite

Log in to the Audit Vault Server console as an *administrator*. See [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information.

To enable database interrogation in an enforcement point:

1. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Enforcement Points**.
2. Find the enforcement point that monitors the secured target that will be interrogated, and then click the name of that enforcement point.

The Modify Enforcement Point page appears.

3. In the Database Interrogation section of the page, click the **Enable Database Interrogation** check box.

Additional input fields appear:

Database Interrogation	
Enable Database Interrogation	<input checked="" type="checkbox"/>
Database Address	<input type="text" value="192.0.2.24"/> Port <input type="text" value="1521"/>
Database Name	<input type="text" value="sales_db"/>
User Name	<input type="text" value="jsmith"/>
Password	<input type="password" value="*****"/>
Re-type Password	<input type="password" value="*****"/>

4. Enter values for the following:
 - **Database Address** and **Port** - Enter the IP address and port number of the secured target database that will be interrogated.
 - **Database Name** - Enter the name of the database or database instance.
 - **User Name** - Enter the database interrogation user name that was set up for this secured target.



See Also:

[Configuring Database Interrogation for SQL Server and SQL Anywhere](#) (page 6-26)

- **Password** and **Re-type Password** - Enter the password for the database interrogation user name.
5. Click **Save**.

6.7.4 Disabling Database Interrogation

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

To disable database interrogation:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Enforcement Points**.
The Enforcement Points page appears, listing enforcement points and their status. You can sort or filter the list.
3. Find the enforcement point for which you want to disable database interrogation, and then click the name of that enforcement point.
The Modify Enforcement Point page appears.
4. In the Database Interrogation section of the page, clear the **Enable Database Interrogation** check box.

5. Click **Save**.

 **See Also:**

- [Working with Lists of Objects in the UI](#) (page 1-12) to sort or filter the enforcement points list.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.8 Configuring Oracle Database Firewall for Databases That Use Network Encryption

Learn about configuring Oracle Database Firewall for databases that use network encryption.

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

6.8.1 Step 1: Apply the Specified Patch to Oracle Database

Learn how to apply the 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.

6.8.2 Step 2: Run the Oracle Advance Security Integration Script

To run the Network Encryption integration script:

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

This directory now contains the uncompressed file:

`advanced_security_integration.sql`.

3. If the installed version is release 12.2.0.11.0 and prior, then execute the following command as a user that has privileges to create users and grant privileges:

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

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

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

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

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

4. If the installed version is release 12.2.0.12.0 and later, then execute the following command as a user with privileges to create users and grant privileges. This is a DDI enhancement to retrieve session information for Oracle Database targets which is available from release 12.2.0.12.0 and onwards. This is applicable for Database Firewall in Monitoring and Blocking mode, or in Monitoring only mode.

```
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`

`ASO` retrieves oracle native network encryption key and session information

`SESSION_INFO` retrieves session information

 **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:

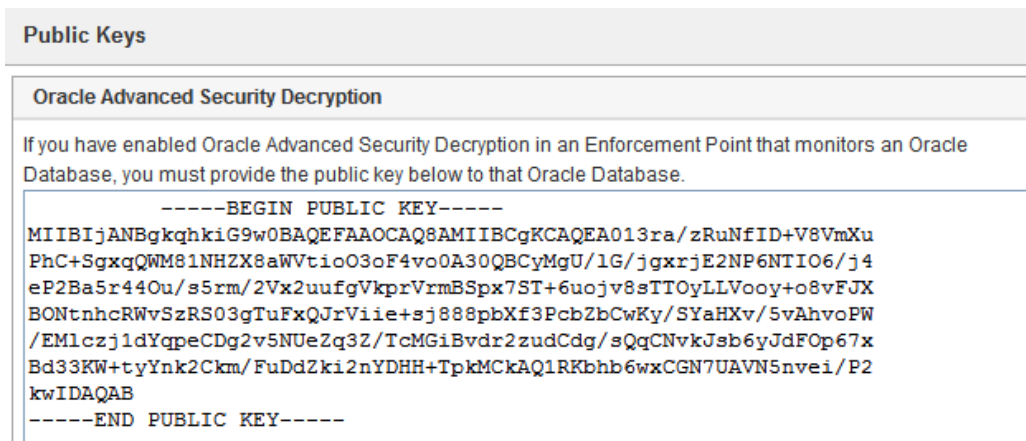
```
Invalid value is provided for <param3>
The valid values are ASO, SESSION_INFO.
ASO retrieves oracle native network encryption key and session
information
SESSION_INFO retrieves session information
```

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

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

To provide the public key to the Oracle Database:

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



Public Keys

Oracle Advanced Security Decryption

If you have enabled Oracle Advanced Security Decryption in an Enforcement Point that monitors an Oracle Database, you must provide the public key below to that Oracle Database.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE013ra/zRuNfID+V8VmXu
PhC+SgxqQWM81NHZX8aWVtio03oF4vo0A30QBCyMgU/lG/jgxrjE2NP6NTIO6/j4
eP2Ba5r44Ou/s5rm/2Vx2uufgVkpVrmBSpX7ST+6uojv8sTTOyLLVooy+o8vFJX
BONtnhcRWvSzRS03gTuFxFQJrViie+sJ888pbXf3PcbZbCwKy/SYaHXv/5vAhvoPW
/EM1czj1dYqpeCDg2v5NUeZq3Z/TcMGiBvdr2zudCdg/sQqCNvkJsb6yJdFOp67x
Bd33KW+tyYnk2Ckm/FuDdZki2nYDHH+TpkMCkAQ1RKbhb6wxCGN7UAVN5nvei/P2
kwIDAQAB
-----END PUBLIC KEY-----
```

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

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

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

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

- a. Put the file you created in Step 2 on the Oracle Database server, preferably in the same directory as the `sqlnet.ora` file.
- b. Open the `sqlnet.ora` file and append the following parameters (in this example the public key file is `dbfw_public_key.txt`):

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

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



See Also:

Oracle Database Security Guide for more information on network encryption.

6.8.4 Step 4: Enable Database Interrogation for the Oracle Database

Follow the procedure in "[Enabling Database Interrogation](#) (page 6-27)" to complete the Database Interrogation setup for an Oracle Database that uses Network Encryption.

6.9 Configuring and Using Database Response Monitoring

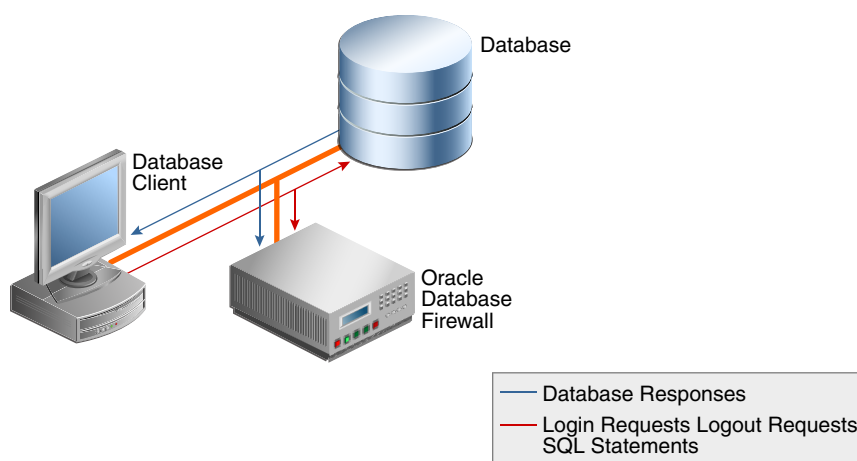
Topics

- [About Database Response Monitoring](#) (page 6-32)
- [Configuring Database Response Monitoring](#) (page 6-33)

6.9.1 About Database Response Monitoring

Enabling the Database Response Monitoring feature allows the Database Firewall to record responses that the secured target database makes to login requests, logout requests and SQL statements sent from database clients, as shown in [Figure 6-1](#) (page 6-33). This feature allows you to determine whether the database executed logins, logouts and statements successfully, and can provide useful information for audit and forensic purposes.

[Figure 6-1](#) (page 6-33) illustrates the process flow of database response monitoring.

Figure 6-1 Database Response Monitoring

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

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

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

6.9.2 Configuring Database Response Monitoring

Topics

- [Enabling Database Response Monitoring](#) (page 6-33)
- [Setting Up Log-in and Log-out Policies in Oracle Database Firewall](#) (page 6-34)

6.9.2.1 Enabling Database Response Monitoring

To enable database response monitoring for a secured target:

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

The Enforcement Points page appears, listing enforcement points and their status. You can sort or filter the list.

3. Find the enforcement point the monitors the secured target, and then click the name of that enforcement point.

The Modify Enforcement Point page appears.

4. In the Database Response section of the page, select the **Enable Database Response** check box.

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

5. Click **Save**.

 **See Also:**

- [Working with Lists of Objects in the UI](#) (page 1-12) to sort or filter the enforcement points list.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

6.9.2.2 Setting Up Log-in and Log-out Policies in Oracle Database Firewall

Learn how to set up Oracle Database Firewall log-in and log-out policies.

The login and logout policies are stored in Oracle Audit Vault and Database Firewall and must be configured in the firewall policy.

 **See Also:**

Oracle Audit Vault and Database Firewall Auditor's Guide

6.10 Securing the Agent and Oracle Database Secure Target Connection

Data security between an AVDF agent and an Oracle Database secure 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 secure target has been setup to accept TCPS/SSL connections, then follow these steps to configure the agent:

1. Ensure that in the secure 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 **Secured Targets** tab.
4. Select the name of the secured target that you want to modify.
5. In the **Modify Secured Target** page, do the following:
 - a. In the Secured Target Location (For Auditing) area, 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 **Secured 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.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

7

Enabling and Using Host Monitoring

Topics

- [About Host Monitoring](#) (page 7-1)
- [Installing and Enabling Host Monitoring](#) (page 7-2)
- [Starting, Stopping, and Other Host Monitor Operations](#) (page 7-9)
- [Updating the Host Monitor \(Unix Hosts Only\)](#) (page 7-11)
- [Using Certificate-based Authentication for the Host Monitor](#) (page 7-11)

7.1 About Host Monitoring

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

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

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

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

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



See Also:

Oracle Audit Vault and Database Firewall Auditor's Guide

 **Note:**

- Host monitoring is supported on Linux, Solaris, AIX, and Windows platforms, and can monitor any database supported by the Database Firewall. See [Table B-1](#) (page B-2) for supported databases.
- Host Monitor Agent supports link type Solaris IPNET on Oracle Solaris SPARC64 and x86-64.
- Host Monitor Agent supports Ethernet (EN10MB) link type for all supported platforms.

7.2 Installing and Enabling Host Monitoring

Topics

- [Host Monitor Requirements](#) (page 7-2)
- [Register the Computer that will Run the Host Monitor](#) (page 7-3)
- [Deploying the Agent and Host Monitor on Microsoft Windows Hosts](#) (page 7-3)
- [Deploying the Agent and Host Monitor on Unix Hosts](#) (page 7-6)
- [Create a Secured Target for the Host-Monitored Database](#) (page 7-7)
- [Create an Enforcement Point for the Host Monitor](#) (page 7-7)
- [Create a Network Audit Trail](#) (page 7-7)

7.2.1 Host Monitor Requirements

Host Monitor enables the Database Firewall to directly monitor SQL traffic in a database.

Recommended requirements for installing Host Monitor:

1. User installing the Host Monitor must have *root* privileges.
2. Ensure Audit Vault Agent is running on the host machine.
3. Ensure the latest version of the following packages from the OS vendor for the specific OS version are installed on the host machine:
 - Libcap (for Linux hosts only)
 - LibPcap
 - OpenSSL
4. Ensure *gmake* is installed. This is required for Host Monitor to run successfully.
5. Verify and allow communication on ports 2050 - 5100 for Database Firewall.
6. Check directory permissions. All the directories in the path of the Host Monitor install location should have 755 as the permission bits starting from the root directory. Also, Host Monitor must be installed in a *root* owned location.

Specific requirements for installing Host Monitor on Windows platform:

1. Host Monitor must be installed by user belonging to *Administrator* group.

2. Install Npcap that is available in the `avdf12.2.0.13.0-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 the latest version of OpenSSL (1.1.1g or higher) libraries. Use OpenSSL version 1.1.1i for release Oracle AVDF 12.2.0.14.0.
4. Ensure the Windows target machine has the latest update of *Visual C++ Redistributable for Visual Studio 2010* (`MSVCR71.dll (*)` or later) package installed. This is a must to use Host Monitor on Windows.

Specific requirements for installing Host Monitor on Linux/Unix/AIX/Solaris platforms:

1. Host Monitor must be installed by *root* user.
2. Ensure the Input Output Completion Ports (IOCP) is set to *available* for IBM AIX on Power Systems (64-bit). It is set to *defined* by default.
3. Ensure Libcap is installed for Linux hosts.



See Also:

Enabling and Using Host Monitoring for host monitoring instructions and prerequisites.

7.2.2 Register the Computer that will Run the Host Monitor

To register a host in the Audit Vault Server, see "[Registering Hosts in the Audit Vault Server](#) (page 5-1)".

7.2.3 Deploying the Agent and Host Monitor on Microsoft Windows Hosts

Oracle Audit Vault and Database Firewall 12.2.0.13.0 (and later) supports Host Monitoring on Windows. This functionality is supported by additionally installing OpenSSL and Npcap. This section contains the necessary details to be followed before upgrading from older releases in 12.2 (other than 12.2.0.11.0, 12.2.0.12.0), or for a fresh installation of 12.2.0.13.0 (or later).

Installing OpenSSL

OpenSSL 1.1.1g or a higher version must be installed on the Windows host machine. Use OpenSSL 1.1.1i for release Oracle AVDF 12.2.0.14.0. Follow these steps to make system related changes before installing OpenSSL:

1. In the Windows 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.

 **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.

7. Click **OK** to save the changes, and then exit all the dialogs.

New Installation of Host Monitor for Windows

Host Monitoring on Windows functionality is supported by additionally installing Npcap. Follow these steps to install Npcap for a fresh installation of Host Monitor in release 12.2.0.13.0 (or later):

1. Log in to ARU.
2. Install Npcap that is available in the `utility.zip` bundle in Oracle Software Delivery Cloud. It is part of the Oracle Audit Vault and Database Firewall installable files.
3. 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.

4. 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.

5. Optionally 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.
6. Confirm the changes in the `Path` environment variable.

Upgrading Host Monitor on Windows

Host Monitoring on Windows functionality is supported by additionally installing Npcap. Follow these steps to continue using Host Monitor on Windows on releases 12.2.0.9.0; 12.2.0.10.0; or 12.2.0.13.0; before upgrading to Oracle AVDF release 12.2.0.14.0:

1. Stop the Audit Vault Agent running on the Windows host machine.
2. Log in to the Audit Vault Server console.
3. Verify the audit trails and the Audit Vault Agent are in `STOPPED` state.
4. Log in to ARU, and download Npcap software that is available with Oracle AVDF `utility.zip` bundle of the specific release.
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/Npcap from the Windows machine.

6. 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.

7. Optionally 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.
 8. Confirm the changes in the `Path` environment variable.

- Restart the Audit Vault Agent on the Windows host machine.
- The Host Monitor is now powered by Npcap during runtime. Verify the network trail collection.
- Proceed with the appliance 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.

 **See Also:**

- [Deploying the Audit Vault Agent on the Host Computer](#) (page 5-5)
- [Registering and Unregistering the Audit Vault Agent as a Windows Service](#) (page 5-7)

7.2.4 Deploying the Agent and Host Monitor on Unix Hosts

Prerequisites

Deploy the Audit Vault Agent. See [Deploying the Audit Vault Agent on the Host Computer](#) (page 5-5).

To install the Host Monitor:

- Log in as `root` and identify a `root`-owned directory on the local hard disk, such as `/usr/local`, where you will install the host monitor.
Note: The entire directory hierarchy must be `root`-owned. All the directories in this hierarchy must have `read` and `execute` permission for other users or groups, but not `write` permission.
- Log in to the Audit Vault Server console as an *administrator*.
- Click on the **Hosts** tab, and then click **Agent**.
- 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 1 (page 7-6), for example `/usr/local`.
- As `root` user, unzip the host monitor file.
This creates a directory named `hm`. This is your *HM_Home* directory, which in this example is `/usr/local/hm`.
- Ensure that the `hostmonsetup` file (in the `hm` directory) has **execute** permission.
- Run the following command:

```
HM_Home/hostmonsetup install [agentuser=Agent_Username] [agentgroup=Agent_Group]
```

- *HM_Home* - The directory created in Step 5 (page 7-6).
- *Agent_Username* - (Optional) Enter the username 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:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

7.2.5 Create a Secured Target for the Host-Monitored Database

To create a secured target, see "[Registering or Removing Secured Targets in the Audit Vault Server](#) (page 6-2)".

7.2.6 Create an Enforcement Point for the Host Monitor

For Host Monitor only deployment, create an enforcement point in **Database Activity Monitoring (DAM)** mode to receive and process the data sent from the Host Monitor.

A network interface card (NIC) must be configured while creating the enforcement point for Database Firewall with Host Monitor only deployment. This must be different from the Management Interface that is used for communication to Audit Vault Server.

 **See Also:**

[Configuring Enforcement Points](#) (page 6-20)

7.2.7 Create a Network Audit Trail

Learn how to create network audit trails.

Create an audit trail for each target you are monitoring with a Host Monitor. Specify `NETWORK` for the **Audit Trail Type**.

 **Note:**

Ensure the collection attribute `network_device_name_for_hostmonitor` is mandatorily configured for the targets which are monitored by Host Monitor. The name of the network interface card is the attribute value. The network interface card receives all the network traffic of the target database.

Linux/AIX/Solaris hosts

Follow these steps to determine the value of the `network_device_name_for_hostmonitor` collection attribute:

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

Follow these steps to determine the value of the `network_device_name_for_hostmonitor` collection attribute:

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`. Hence for a network card with the name `\Device\Tcpip_{*****-****-****-****-*****}` the attribute value is `\Device\NPF_{*****-****-****-****-*****}`.

 **Note:**

This does not involve changing the network device name at a system level.

 **See Also:**

[Adding an Audit Trail in the Audit Vault Server](#) (page 6-9) for instructions on adding audit trails.

7.3 Starting, Stopping, and Other Host Monitor Operations

Topics

- [Starting the Host Monitor](#) (page 7-9)
- [Stopping the Host Monitor](#) (page 7-9)
- [Changing the Logging Level for a Host Monitor](#) (page 7-10)
- [Viewing Host Monitor Status and Details](#) (page 7-10)
- [Checking the Status of a Host Monitor Audit Trail](#) (page 7-10)
- [Uninstalling the Host Monitor \(Unix Hosts Only\)](#) (page 7-10)

7.3.1 Starting the Host Monitor

Learn how to start the host monitor.

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

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

1. Log in to the Audit Vault Server console as an administrator.
2. Start the audit trail(s) you created for host monitoring in [Create a Network Audit Trail](#) (page 7-7).

 **See Also:**

- [Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server](#) (page 6-11)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

7.3.2 Stopping the Host Monitor

To stop the host monitor, stop the audit trail you created for the secured target that is being monitored. See "[Stopping, Starting, and Autostart of Audit Trails in the Audit Vault Server](#) (page 6-11)".

7.3.3 Changing the Logging Level for a Host Monitor

See "[Changing the Logging Level for the Audit Vault Agent](#) (page 5-11)".

7.3.4 Viewing Host Monitor Status and Details

You can view whether a host monitor is installed, and information such as its location, version, update time, and other details.

To view host monitor status and details:

1. Log in to the Audit Vault Server console as an *auditor*.
2. Click the **Hosts** tab.
3. Check the **Host Monitor Status** and the **Host Monitor Details** columns for the host you are interested in.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

7.3.5 Checking the Status of a Host Monitor Audit Trail

To check the status of a host monitor:

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

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

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

7.3.6 Uninstalling the Host Monitor (Unix Hosts Only)

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

To uninstall a host monitor:

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

```
hostmonsetup uninstall
```

7.4 Updating the Host Monitor (Unix Hosts Only)

Learn how to update the host monitor on Unix systems.

When you update the Audit Vault Server to a future release, the host monitor is automatically updated.

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



See Also:

Oracle Audit Vault and Database Firewall Installation Guide for information on downloading upgrade software.

7.5 Using Certificate-based Authentication for the Host Monitor

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

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

- [Requiring a Signed Certificate for Host Monitor Connections to the Firewall](#) (page 7-11)
- [Getting a Signed Certificate from the Audit Vault Server](#) (page 7-12)

7.5.1 Requiring a Signed Certificate for Host Monitor Connections to the Firewall

To require a signed certificate for host monitor connections:

1. Stop the host monitor if it is running.
2. At the Database Firewall, log in as `root`, and run the following commands:

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

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

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



See Also:

[Stopping the Host Monitor](#) (page 7-9)

7.5.2 Getting a Signed Certificate from the Audit Vault Server

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

To get a signed certificate from the Audit Vault Server:

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

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

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

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

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

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

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

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

6. (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
```

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

See Also:

[Starting the Host Monitor](#) (page 7-9)

8

Configuring High Availability

Topics

- [About High Availability Configurations in Oracle Audit Vault and Database Firewall](#) (page 8-1)
- [Managing A Resilient Audit Vault Server Pair](#) (page 8-2)
- [Managing A Resilient Database Firewall Pair](#) (page 8-9)

8.1 About High Availability Configurations in Oracle Audit Vault and Database Firewall

You can configure Database Firewalls pairs or Audit Vault Server pairs, or both, to provide a high-availability system architecture. These are known as **resilient pairs**. For the Database Firewall, the resilient pair configuration described in this chapter applies to Database Activity Monitoring (DAM) mode only.

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

In a high availability Audit Vault Server pair, when failover is enabled, the secondary server becomes the primary in the event of a failover.

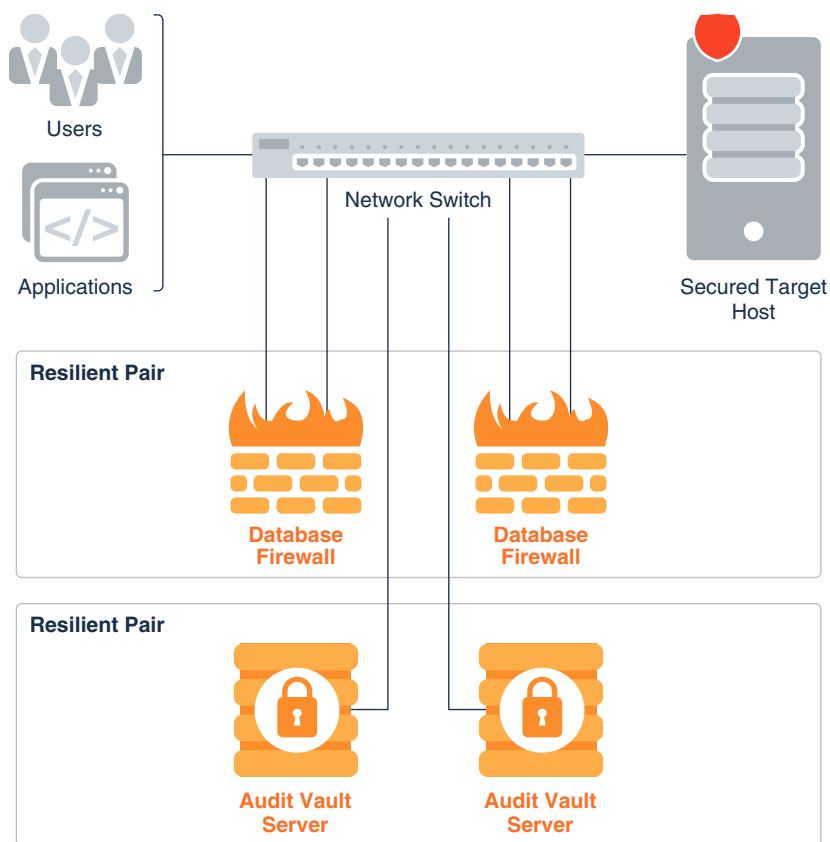
In a resilient Database Firewall pair, both primary and secondary Database Firewall:

- Receive the same span traffic
- Have the same configuration that is synchronized by the Audit Vault Server. This is the configuration of secured targets, enforcement points, policies, and other monitoring settings. This excludes the system configuration like the IP address, network mask, DNS of the primary and secondary Database Firewall instances on the system page of the Database Firewall console. These settings are not synchronized.
- Create log files according to the policy applied
- Send out alerts to the Audit Vault Server. The Audit Vault Server then sends only the alerts from the primary Database Firewall.

The Audit Vault Server collects traffic logs from the primary and secondary instances of Database Firewall. The Audit Vault Server controls the state of the resilient pair. There is no communication between the primary and secondary instances of Database Firewall. If the Audit Vault Server is unable to contact the primary Database Firewall for an extended period, or if there is a time gap in the traffic logs collected from the primary Database Firewall due to non-availability of the specific Database Firewall instance, then the Audit Vault Server uses the traffic log files collected from the secondary Database Firewall. The Audit Vault Server deletes the traffic log files from both instances of Database Firewall after the data is stored for the specified time range in the Audit Vault Server database.

Figure 8-1 (page 8-2) illustrates a pair of Audit Vault Servers and a pair of Database Firewalls in high availability mode.

Figure 8-1 Pairs of Audit Vault Servers and Database Firewalls in High Availability Mode



Note:

High availability pairing or unpairing must only be executed once in a period of one hour.

See Also:

Oracle Audit Vault and Database Firewall Concepts Guide for more information on DAM and DPE (Database Policy Enforcement) modes.

8.2 Managing A Resilient Audit Vault Server Pair

These topics provide an introduction to pairing Audit Vault Servers.

Specifically, these topics describe configuring the primary and secondary Audit Vault Servers, checking the high availability status of the Audit Vault Servers, updating the Audit Vault Agent after pairing the Audit Vault Servers, swapping roles between the primary and secondary Audit Vault Servers, and handling failover of the Audit Vault Server pair.

8.2.1 About Pairing Audit Vault Servers

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

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

Remember that if you are deploying Database Firewalls, and you configure a resilient pair of Audit Vault Servers, you must provide the server certificate and IP address of both the primary and secondary Audit Vault Server to each Database Firewall.

If you have deployed Audit Vault Agents of the secondary server before pairing Audit Vault Servers, then you should manually update the previously deployed Audit Vault Agents of the secondary server once pairing is complete.

This is not required, if you deployed Audit Vault Agents of primary server before performing high availability pairing of the Audit Vault Servers.



See Also:

- [Specifying the Audit Vault Server Certificate and IP Address](#) (page 4-6)
- [Updating Audit Vault Agents and Host Monitor Agents After Pairing Audit Vault Servers](#) (page 8-6)
- [Handling a Failover of the Audit Vault Server Pair](#) (page 8-8)

8.2.2 Prerequisites for Configuring a Resilient Pair of Audit Vault Servers

This topic describes the prerequisites for configuring a pair of Audit Vault Servers.

- Ensure that both the primary and secondary Audit Vault Servers have the same specification. The specification includes:
 - System version
 - System time
 - Encryption status (enabled on both or disabled on both)
 - Shared memory size
 - RAM size
 - ASM disk space
- Ensure that the clock is synchronized on both systems. (An incorrect time setting can cause certificate validation errors.)

- Do the initial system configuration tasks for both primary and secondary Audit Vault Servers.
- The high availability functionality does not work if the number of NFS locations are not the same. The *admin* user must verify and create the same number of archive locations before enabling high availability. When creating an NFS location, select `Create New Filesystem` in the field **Remote Filesystem** to ensure there is a different filesystem for every location added on the primary and secondary Audit Vault Servers. These locations are mapped during high availability pairing. The mapping of these locations is displayed in the primary Audit Vault Server console once high availability pairing is successful.
- The `host:export` and `directory:destination` path combination of NFS archive locations for primary and secondary Audit Vault Servers must be unique.
- The *admin* user must ensure there is sufficient space on the NFS archive location configured for the secondary Audit Vault Server. Before pairing for high availability, the *admin* user must check all of the NFS archive locations where archived datafiles exist on the primary Audit Vault Server. Then, compute the sum of all datafile size in those locations and add the same size or more to the NFS archive locations on secondary Audit Vault Server. The minimum size of the filesystem for a location on secondary Audit Vault Server should be the maximum size of the filesystems created on the primary Audit Vault Server.
- In a high availability environment if the Audit Vault Agents are deployed on the secondary Audit Vault Server before pairing, then manually update the previously deployed Audit Vault Agents pertaining to the secondary Audit Vault Server after pairing is complete.

Related Topics

- [Specifying Initial System Settings and Options \(Required\)](#) (page 3-3)

8.2.3 Configure the Secondary Audit Vault Server

To configure Server2, the secondary server:

1. Copy the server certificate from Server1 (the primary):
 - a. Log in to Server1 as an administrator.
 - b. In the **Settings** tab of Server1, from the **Security** menu, click **Server Certificate**.
 - c. Copy the certificate.
2. In another browser window, log in to Server2 as a super administrator.
3. In the Server2 console, click the **Settings** tab.
4. From the **System** menu, select **High Availability**.
5. In the **Configure this server as** field, select **Secondary server**.
6. Enter the **Primary server IP address** in the field provided.
7. Paste the certificate you copied from Server1 in the **Primary server certificate** field.
8. Click **Save**.

After validation, the primary server's IP address and certificate are saved. If you wish to initiate pairing at this point, you can click the primary server's URL at the top of the page.

A **Reset** button appears, allowing you to cancel the settings configured in this procedure, thereby resetting the system to its original state.

8.2.4 Configure the Primary Audit Vault Server

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

To configure Server1, the primary server:

1. Copy the server certificate from Server2 (the secondary):
 - a. Log in to Server2 as an administrator.
 - b. In the **Settings** tab of Server1, from the **Security** menu, click **Server Certificate**.
 - c. Copy the certificate.
2. In another browser window, log in to Server1 as a super administrator.
3. In the Server1 console, click the **Settings** tab.
4. From the **System** menu, select **High Availability**.
5. In the **Configure this server as** field, select **Primary server**.
An **Initiate Pairing** button appears.
6. Enter the **Secondary server IP address** in the field provided.
7. Paste the certificate you copied from Server2 in the **Secondary server certificate** field.
When you are ready to start the pairing of Server1 and Server2, go to the next step.
8. Initiate high availability pairing at the primary server (Server1). This will take a few minutes, and once it is complete, the secondary server will no longer have a console UI.

Note:

- The user must ensure to execute the high availability pairing procedure prior to archiving of ILM. Else, it may result in an error.
- After completing this procedure, do all configuration tasks on the primary server only. This includes tasks such as deploying the Audit Vault Agent, setting up secured targets and hosts, and adding Database Firewalls and enforcement points. The console UI of Server2 (the standby) will be unavailable and you will be redirected to Server1.

9. Click **Initiate Pairing**.

A message is displayed indicating the progress of the high availability configuration. During this process, which may take at least 10 minutes, the console may be unavailable.

10. Refresh the browser periodically.

When the configuration is complete, the **High Availability Status** is displayed.

8.2.5 Checking the High Availability Status of an Audit Vault Server

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

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

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

- **Standalone** - This server has no partner server.
- **Primary** - This server is currently the primary server.
- **Disconnected** - This primary server switches to this mode if it detects that the standby Audit Vault Server changed its role to Standalone or Primary. In Disconnected mode, the Audit Vault Server stops downloading the traffic log files from the Database Firewall and then blocks Audit Vault agents by blocking external access to the Audit Vault Server database. However, the user interface (Audit Vault console) is accessible.

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

8.2.6 Updating Audit Vault Agents and Host Monitor Agents After Pairing Audit Vault Servers

This topic describes how to update Audit Vault Agents after pairing Audit Vault Servers.

In a high availability pair of Audit Vault Servers, the secondary server becomes the primary in the event of a failover. If you have deployed Audit Vault Agents of secondary server before performing the high availability pairing of the Audit Vault Servers, after failover, then the status of the Agent in the new primary server becomes *UNREACHABLE*. To avoid this scenario, manually update previously deployed Audit Vault Agents of the secondary server once pairing is complete.

This is not required, if you have deployed Audit Vault Agents of primary server before performing high availability pairing of the Audit Vault Servers.

Note:

- Audit Vault Agents and Host Monitor Agents are automatically updated after pairing or unpairing Audit Vault Servers. This is applicable for releases 12.2.0.5.0 and onwards.
- In case the version of Oracle Audit Vault and Database Firewall is below 12.2.0.4.0, then use this procedure to update Audit Vault Agents or Host Monitor Agents manually.

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

1. Remove complete `Agent_Home` folder.
2. Deactivate the host and activate the host again using the Audit Vault Server GUI.

3. Download the new `agent.jar` from the new primary Audit Vault Server GUI, and copy it to the new `Agent_Home` directory on the host machine.

4. In the `Agent_Home` directory execute the following command:

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

5. Execute the following command and provide the Agent activation key:

```
agentctl start -k
```

```
Enter Activation Key:
```

 **Note:**

Enter the activation key when prompted. This key is not displayed as you type.

6. Restart audit trails.

 **Note:**

On Windows, execute the following command, from the `Agent_Home` folder before removing the complete `Agent_Home` folder.

```
agentctl.bat unregistersvc
```

8.2.7 Swapping Roles Between a Primary and Standby Audit Vault Server

Follow this procedure if you want to swap the roles of the primary and standby Audit Vault Servers.

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. In the **SYSTEM** menu, select **High Availability**.
4. Click the **Switch Roles** button.
5. In the Confirmation window, click **OK**.

A message is displayed indicating the progress of the high availability configuration. Be aware that during this process, which can take at least 10 minutes, the console may be unavailable. Click the **Refresh** button periodically. When the configuration is complete, it will redirect to the new primary Audit Vault Server.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

8.2.8 Handling a Failover of the Audit Vault Server Pair

When failover is enabled, during normal operation, the system periodically checks the availability of the primary Audit Vault Server in the resilient pair.

Note the following scenarios:

- If the primary Audit Vault Server becomes unavailable, the system automatically fails over to the secondary Audit Vault Server after a 10 minute delay. The delay prevents a failover due to a reboot of the primary server.
- If the database is shut down properly, there is no failover. If the primary Audit Vault Server is shut down (for example powered off) and it does not come up within 10 minutes, then it results in failover.
- If the primary Audit Vault Server is manually shut down and reinstalled or replaced with another server, then you must perform the following procedure:

1. Manually failover the current standby server by issuing the following command as the `oracle` user:

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

2. Then log in to the Audit Vault console as the super administrative user so that you can unpair the two servers.
3. Select **Settings**, and then select **High Availability**.
4. In the High Availability status page, click the **Unpair** button.
5. Copy the new certificates between the two Audit Vault servers.
6. Initiate the high availability setup again by clicking the **Initiate Pairing** button.

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

1. Log in to the Audit Vault Server console as a super administrator.
2. Click on the **Settings** tab.
3. Select **Settings**, and then select **High Availability**.
4. In the High Availability Status page, unpair the new primary server to convert it to a standalone server by clicking on the **Unpair** button.
5. On the standalone server, configure the network and services settings (for example DNS settings).
6. On the standalone server, manually mount any remote filesystems (NFS shares) defined as archive locations, using this AVCLI command:

```
ALTER REMOTE FILESYSTEM filesystem_name MOUNT
```
7. Disconnect the failed server and replace it. The replacement server can now be configured as the new secondary server.
8. Follow the configuration steps again to pair the two Audit Vault Servers.

 **See Also:**

- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)
- [Specifying the Audit Vault Server System Settings](#) (page 3-5)
- [ALTER REMOTE FILESYSTEM](#) (page A-54)
- [Managing A Resilient Audit Vault Server Pair](#) (page 8-2)
- [Audit Vault Agent in Unreachable state upon Failover](#) (page G-33)

8.2.9 Disabling or Enabling Failover of the Audit Vault Server

Under some conditions you may want to disable automatic failover of a high availability pair of Audit Vault Servers. For example, you may need to disconnect the Audit Vault Server for maintenance without triggering the automatic failover, or you may be in an environment with an unstable network that causes frequent failovers. In these cases, you may choose to disable automatic failover, and to do it manually if needed.

To disable or enable failover for a high availability pair of Audit Vault Servers:

1. Log in to the primary Audit Vault Server as a super administrator.
2. Click the Settings tab, and then in the System menu, click High Availability.
3. Click the **Enable/Disable Failover** button.

 **Note:**

Alternately, you can execute the following commands to disable or enable the failover through the Audit Vault and Database Firewall server as *root* user:

```
sudo -u oracle /usr/local/dbfw/bin/setup_ha.rb --disable_failover
sudo -u oracle /usr/local/dbfw/bin/setup_ha.rb --enable_failover
```

8.2.10 Performing a Manual Failover of the Audit Vault Server

If you have disabled automatic failover, you can perform a manual failover by running this command as *oracle* on the Audit Vault Server:

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

8.3 Managing A Resilient Database Firewall Pair

These topics describe how to manage, configure, switch roles, and break a resilient Database Firewall pair.

8.3.1 About Managing A Resilient Database Firewall Pair

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

Prerequisites

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

If You Configure a Resilient Pair of Audit Vault Servers

If you have also configured a resilient pair of Audit Vault Servers, remember you must provide each Audit Vault Server's IP address and certificate to each Database Firewall in your system.



Note:

[Specifying the Audit Vault Server Certificate and IP Address](#) (page 4-6)

8.3.2 Configuring A Resilient Database Firewall Pair

To configure a resilient Database Firewall pair:

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



Note:

- If you have defined a resilient Audit Vault Server pair, then use the primary server's console.
- In case the Audit Vault Server is configured with resilient firewall pair without configuring enforcement points, then failover may not occur.

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



See Also:

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

8.3.3 Switching Roles in a Resilient Pair of Database Firewalls

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

1. Log in to the Audit Vault Server console as an *administrator*.
If you have defined a resilient pair of Audit Vault Servers, then use the primary server's console.
2. Click the **Database Firewalls** tab.
3. In the **Database Firewalls** menu, select **Resilient Pair**.
4. Click the **Swap**.
5. In the confirmation dialog box, 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 is in effect. In this due course, 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.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

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

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

1. Log in to the Audit Vault Server console as an *administrator*.
If you have defined a resilient pair of Audit Vault Servers, use the primary server's console.
2. Click the **Database Firewalls** tab.
3. In the **Database Firewalls** menu, select **Resilient Pair**.
4. Select the resilient pair you want, and then click **Break**.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

8.4 High Availability For Database Firewall In Proxy Mode

The high availability configuration of a resilient pair of Database Firewall instances is usually set up in Monitoring Only modes. Oracle Audit Vault and Database Firewall provides an option to set up the high availability configuration for Database Firewall that you have deployed in Monitoring / Blocking (Proxy) mode.

Two or more individual Database Firewall instances deployed in proxy mode can be configured to achieve high availability.

8.4.1 Configuring High Availability For Database Firewall In Proxy Mode Through Client Configuration

This topic contains the necessary information about configuring high availability for two or more individual Database Firewall instances in proxy mode. This can be achieved by making changes to the client configuration.

Oracle SQL OCI (Oracle Call Interface) based clients use `tnsnames.ora` file to connect to the database. The parameters in this file need to be modified as part of this configuration.

**Note:**

This feature is available in *Oracle Audit Vault and Database Firewall* release 12.2.0.11.0 and later.

Prerequisite

Complete the basic set up that is required before executing the configuration procedure:

1. Audit Vault Server instance is up and running.
2. Two or more Database Firewall instances are up and running.
3. Register the Database Firewall instances in the Audit Vault Server.
4. Configure the target database.
5. Configure one monitoring point for each Database Firewall instance to the same database target.

The client can be configured using the following parameters:

1. ADDRESS_LIST
2. CONNECT_TIMEOUT
3. LOAD_BALANCE

ADDRESS_LIST

Include multiple Database Firewall IP addresses in the `ADDRESS_LIST` to connect to the Database target.

**Note:**

Avoid using port numbers that are configured for Audit Vault Server or Database Firewall internally.

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)))
```

1. Connect to the database using a client application.

For example: If you are using *SQL*Plus* client, then use the following command:

```
sqlplus <username>/<password>@<net_service_name>
```

2. The client attempts to connect to the first Database Firewall instance. In case the first instance is down or not reachable, then the client attempts to connect to the second instance. It works similar to active and passive deployment.

CONNECT_TIMEOUT**Note:**

The *admin* user must use caution to set this parameter.

Use `CONNECT_TIMEOUT` parameter to quickly detect if the node is down. It also reduces the connection time in case of failover.

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. 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. Later the client attempts to connect to the second instance. This behavior can be modified accordingly.

**Note:**

By default the wait time is 60 seconds.

LOAD_BALANCE

Use `LOAD_BALANCE` parameter to load balance client connections across deployed instances of Database Firewall.

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)))
```

Once this parameter is defined, the clients connect to the list of addresses in a random sequence and balance the load on various Database Firewall instances. It works similar to load balancing deployment.

Related Topics

- [Registering Database Firewall in Audit Vault Server](#) (page 3-20)
Learn how to register Database Firewall in Audit Vault Server.
- [Registering Secured Targets](#) (page 6-3)
- [Configuring Enforcement Points](#) (page 6-20)
Learn about configuring enforcement points.
- [Ports for Services Provided by the Database Firewall](#) (page D-2)
- [Ports for External Network Access by the Database Firewall](#) (page D-4)



See Also:

[Creating Database Firewall Policies](#)

8.4.2 Configuring High Availability For Database Firewall In Proxy Mode Through DNS Setup

This topic contains the necessary information about configuring high availability of two or more individual Database Firewall instances when monitoring points are in proxy mode. This can be achieved by making configuration changes to the local DNS.



Note:

This feature is available in *Oracle Audit Vault and Database Firewall* release 12.2.0.11.0 and later.

Prerequisite

Complete the basic set up that is required before executing the configuration procedure:

1. Audit Vault Server instance is up and running.
2. Two or more Database Firewall instances are up and running.
3. Register the Database Firewall instances in the Audit Vault Server.
4. Configure the target database.

5. Configure one monitoring point for each Database Firewall instance to the same database target.
6. A server with DNS setup is up and running.

Setup a domain name in DNS:

1. In the server where the DNS is configured, create a domain name to represent IP addresses for multiple Database Firewall instances. This is the local DNS that is used by the client for DNS or host name resolution.
2. Make this change in the client that is used to connect to the target database. Define DNS server as name server for the existing domain. This configuration should be done on the client hosts.
3. Clients should use the domain name as hostname while connecting to the database through the Database Firewall.
4. Specify other details like the port number and service name.
5. In case you are using *SQL*Plus* client, use the following string to connect:

```
sqlplus username/password@<domain name>:port/servicename
```
6. In this setup the Domain Name Server 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). In this case 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 while connecting to Database Firewall instances. This is for load balancing and works like active-active setup.

Related Topics

- [Registering Database Firewall in Audit Vault Server](#) (page 3-20)
Learn how to register Database Firewall in Audit Vault Server.
- [Registering Secured Targets](#) (page 6-3)
- [Configuring Enforcement Points](#) (page 6-20)
Learn about configuring enforcement points.
- [Ports for Services Provided by the Database Firewall](#) (page D-2)
- [Ports for External Network Access by the Database Firewall](#) (page D-4)

**See Also:**

[Creating Database Firewall Policies](#)

9

Configuring Integration with BIG-IP ASM

Topics

- [About the Integration of Oracle Audit Vault and Database Firewall with F5 BIG-IP Application Security Manager \(BIG-IP ASM\) \(page 9-1\)](#)
- [How the Integration Works \(page 9-3\)](#)
- [Deploying the Oracle AVDF and F5 BIG-IP Application Security Manager Integration \(page 9-4\)](#)
- [Viewing F5 Data in Oracle Audit Vault and Database Firewall Reports \(page 9-10\)](#)

9.1 System Requirements

This topic describes the system requirements for integrating Oracle Audit Vault and Database Firewall and F5 BIG-IP Application Security Manager (BIG-IP ASM).

The integration requires:

- Oracle Audit Vault and Database Firewall
- F5®BIG-IP® Application Security Manager™ (BIG-IP ASM) versions 9.4.5, 10, or 11. Other F5 products, such as FirePass®, BIG-IP Local Traffic Manager™ (LTM), BIG-IP Global Traffic Manager™ (GTM), WebAccelerator™ or WANJet® are not currently supported.

Visit the F5 Web site for the latest information on F5 BIG-IP Application Security Manager (BIG-IP ASM).

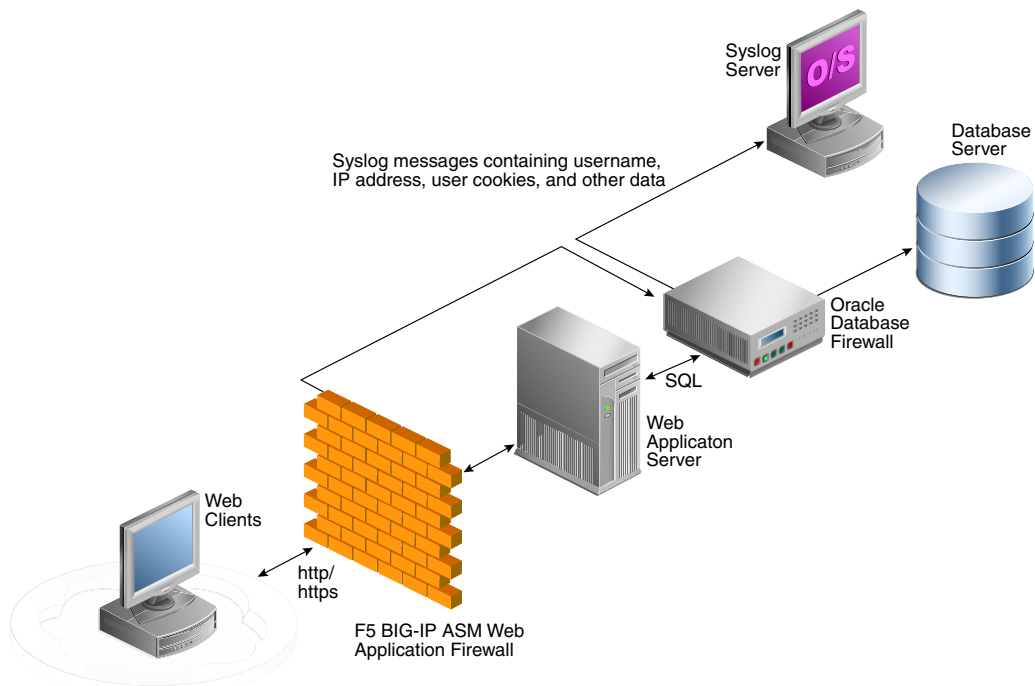
9.2 About the Integration of Oracle Audit Vault and Database Firewall with F5 BIG-IP Application Security Manager (BIG-IP ASM)

This topic discusses integration of Oracle Audit Vault and Database Firewall, F5 BIG-IP Application Security Manager (BIG-IP ASM), Web clients, and the Web application server, how the integration works, and its key benefits.

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

F5 BIG-IP Application Security Manager (BIG-IP ASM) is deployed between the Web clients and the Web application server, see [Figure 9-1](#) (page 9-2). It analyzes each HTTP and HTTPS request, and blocks potential attacks before they reach the Web application server. F5 BIG-IP Application Security Manager (BIG-IP ASM) can be installed on a wide range of BIG-IP platforms.

Figure 9-1 Oracle Audit Vault and Database Firewall with F5 BIG-IP ASM Data Flow Unit



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

A deployment that includes both F5 BIG-IP Application Security Manager (BIG-IP ASM) and the Database Firewall provides all the security benefits of both products and enables the two systems to work in partnership to reach unparalleled levels of data security.

A key benefit of the integration is that it allows F5 BIG-IP Application Security Manager (BIG-IP ASM) to pass to the Database Firewall additional information about the SQL statements sent to the database, including the Web user name and IP address of the Web user who originated them. This information is not usually available from the SQL statements generated by the Web application server.

The information obtained from F5 BIG-IP Application Security Manager (BIG-IP ASM), and from the Database Firewall system itself, is logged by the Database Firewall as attributes of the appropriate statements. Once the data has been logged, it can be retrieved in views of the traffic logs to give complete visibility into the source and nature of any attacks.

 **Note:**

F5 BIG-IP Application Security Manager (BIG-IP ASM) is deprecated in 12.2.0.7.0, and will be desupported in 19.1.0.0.0.

Summary of Key Benefits

The key benefits of this integration are:

- Improves security through a partnership of the two systems.
- Allows Oracle Audit Vault and Database Firewall to provide detailed information about the origin and context of the SQL statements from the Web application layer.
- Enables Oracle Audit Vault and Database Firewall to act as a log store for data generated by F5 BIG-IP Application Security Manager (BIG-IP ASM).
- Provides layered security at the edge of the network, and close to the database.

Related Topics

- [Deploying the Oracle AVDF and F5 BIG-IP Application Security Manager Integration](#) (page 9-4)
These topics describe how to configure Oracle Audit Vault and Database Firewall to work with F5 BIG-IP ASM and BIG-IP ASM iRule.

9.3 How the Integration Works

The integration Oracle Audit Vault and Database Firewall and F5 BIG-IP Application Security Manager (BIG-IP ASM) works by using a syslog messaging system to deliver alerts from BIG-IP ASM.

Standard BIG-IP ASM syslog messages enabled through the ASM logging profile provide details of each alert, such as the target client's IP address and other attributes of the session.

A BIG-IP ASM iRule™ is set up, which generates a syslog message during a user login to provide the Web username. Oracle Audit Vault and Database Firewall provides a sample iRule, which must be customized to match the specific login procedures of the Web application.

During the deployment procedure, F5 BIG-IP Application Security Manager (BIG-IP ASM) is set up to route all its syslog messages to Oracle Audit Vault and Database Firewall. Oracle Audit Vault and Database Firewall attempts to match each relevant BIG-IP ASM syslog message with the appropriate SQL statements generated by the Web application server. If a match is found, it extracts the information contained in the BIG-IP ASM syslog message, and stores that information as attributes of the logged SQL statements. If a match is not found, a separate record is added to the traffic log, containing the attributes from the syslog message.

The software uses cookies to match SQL statements with Web users. When the user logs in, BIG-IP ASM assigns a unique cookie to that user (normally the cookie's name starts with "TS"). The cookie and the name of the user is sent to Oracle Audit Vault and Database Firewall by a syslog message generated by the iRule on the ASM. If the user's actions cause an alert or other event, F5 BIG-IP Application Security Manager (BIG-IP ASM) generates an additional syslog message containing the same identifying cookie, which enables the software to match the syslog message with the specific user. Since the Oracle Audit Vault and Database Firewall system is also able to match syslog messages with SQL statements, this enables individual SQL statements relating to potential threats to be attributed to specific Web users.

Oracle Audit Vault and Database Firewall can automatically relay all syslog messages received from F5 BIG-IP Application Security Manager (BIG-IP ASM) to an external syslog server, up to a maximum size of 2KB each. If required, syslog messages generated by Oracle Audit Vault and Database Firewall itself can be routed to the same destination. Oracle Audit Vault and Database Firewall does not alter the F5 BIG-IP Application Security Manager (BIG-IP ASM) syslog traffic in any way.

Oracle Audit Vault and Database Firewall monitors the status of the connection to F5 BIG-IP Application Security Manager (BIG-IP ASM), and generates syslog messages every two minutes if the connection is not present or has been lost.

Related Topics

- [Developing a F5 BIG-IP Application Security Manager iRule](#) (page 9-7)
These topics describe how to develop a F5 BIG-IP Application Security Manager (BIG-IP ASM) iRule with Oracle Audit Vault and Database Firewall.

9.4 Deploying the Oracle AVDF and F5 BIG-IP Application Security Manager Integration

These topics describe how to configure Oracle Audit Vault and Database Firewall to work with F5 BIG-IP ASM and BIG-IP ASM iRule.

9.4.1 About the Deployment

Deploying F5 BIG-IP Application Security Manager (BIG-IP ASM) with Oracle Audit Vault and Database Firewall requires the configuration of a few straightforward settings in both systems, and the customization of an iRule so that it matches the Web application's configuration.

9.4.2 Configuring Oracle Audit Vault and Database Firewall to Work with F5 BIG-IP Application Security Manager

Learn to configure Oracle AVDF to operate with F5 BIG-IP ASM.

Note:

- This functionality is only supported on F5 BIG-IP Application Security Manager (BIG-IP ASM) version 10.2.1.
- F5 BIG-IP Application Security Manager (BIG-IP ASM) integration is deprecated in release Oracle AVDF 12.2.0.7.0, and is desupported in 20.1.

You can configure Oracle Audit Vault and Database Firewall to operate with F5 BIG-IP Application Security Manager (BIG-IP ASM) only after you have configured the enforcement point for the secured target.

To configure Oracle Audit Vault and Database Firewall to operate with F5 BIG-IP Application Security Manager (BIG-IP ASM) for a secured target:

1. Ensure that an enforcement point has been defined for this secured target.
2. Log in to the Audit Vault Server console as an *administrator*.
3. Click the **Secured Targets** tab, and then from the **Monitoring** menu, click **Enforcement Points**.
4. Click the name of the enforcement point that monitors this secured target.

5. Click **Advanced**.
6. Complete the options:
 - **System Address:** This read-only information shows the IP address of the Database Firewall associated with this enforcement point. F5 BIG-IP Application Security Manager (BIG-IP ASM) must send syslog messages to this address and port.
 - **WAF Addresses:** Delete the word `DISABLED`, and enter the IP address of each F5 BIG-IP Application Security Manager (BIG-IP ASM) system that generates syslog messages to send to the Database Firewall. Separate each IP address with a space character.
 - **Disable WAF Alert Forwarding:** Select this check box to stop the Database Firewall from forwarding syslog messages. The current status of alert forwarding is displayed below this option.
 - **Destination Host and Dest Port:** Specify the IP address and port number of the syslog server that is to receive the F5 BIG-IP Application Security Manager (BIG-IP ASM) syslog messages forwarded by the Database Firewall. The Database Firewall relays these messages unmodified.

The IP address does not need to be the same as the syslog destination used for syslog messages generated by the Database Firewall itself.
 - **Enhance reports with WAF logging data:** Select this check box to enable the Database Firewall to record BIG-IP ASM attributes obtained from the syslog messages, such as the IP address and name of the Web application user. If this box is not checked, the Database Firewall will not attempt to match F5 and Database Firewall SQL messages.
 - **Cookie Prefixes:** F5 adds cookies, with a standard prefix, to the pages it serves up. If necessary change the prefix of these cookies in this field. The Database Firewall searches for cookies with this prefix.
 - **Session Idle Timeout:** The user's cookie is stored only for the length of time specified in this field. This enables the same cookie to be used by different users, providing the time period specified here has elapsed.
 - **Exclude Addresses:** You can specify a list of IP addresses of Web application servers or other SQL-generating sources to ignore for reporting purposes. For example, you may want to add the IP address of an internal Web application server.

 **See Also:**

- [Configuring Enforcement Points](#) (page 6-20)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

9.4.3 Configuring F5 BIG-IP Application Security Manager

These topics describe how to create the logging profile and write policy settings when configuring F5 BIG-IP Application Security Manager (BIG-IP ASM).

Related Topics

- [Logging Profile](#) (page 9-6)
This topic describes how to configure the Web application's logging profile to send F5 BIG-IP Application Security Manager (BIG-IP ASM) syslog messages to Oracle Audit Vault and Database Firewall.
- [Policy Settings](#) (page 9-7)
This topic describes the policy settings for configuring Oracle Audit Vault and Database Firewall with F5 BIG-IP Application Security Manager (BIG-IP ASM).

9.4.3.1 Logging Profile

This topic describes how to configure the Web application's logging profile to send F5 BIG-IP Application Security Manager (BIG-IP ASM) syslog messages to Oracle Audit Vault and Database Firewall.

Use Server IP and Server Port, for example 5514, to specify the IP address of the Database Firewall (this is the same IP address used to connect to the firewall's Administration console). Select TCP for the Protocol.

The Selected Items box must include the following attributes:

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



Note:

The attributes must appear in the Selected Items box in the order shown here.

9.4.3.2 Policy Settings

This topic describes the policy settings for configuring Oracle Audit Vault and Database Firewall with F5 BIG-IP Application Security Manager (BIG-IP ASM).

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

Oracle Audit Vault and Database Firewall recognizes the following events:

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

9.4.4 Developing a F5 BIG-IP Application Security Manager iRule

These topics describe how to develop a F5 BIG-IP Application Security Manager (BIG-IP ASM) iRule with Oracle Audit Vault and Database Firewall.

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

The sample iRule provided with Oracle Audit Vault and Database Firewall contains the required format of the syslog message, but must be customized to handle the specific login requirements of your Web application.

```
# F5 BIG-IP example iRule
# Description: Capture username and cookies from user login to web application
#
# Global variable definitions and other initialisation logic goes here
when RULE_INIT {
    ### Customise this to suit your application
    # The page that user logins from
    set ::login_page "/login.asp"
    # The name of the field holding the user name
    set ::login_parameter_name "Uname"
    # The method of authentication which will be sent to Oracle Database Firewall
```

```

set ::auth_method "webforms"
# HTTP protocol methods that is used by the login form
set ::login_method "POST"
### Don't change these
# Limit the length of the HTTP request for safety
set ::max_header_content_length 5242880
# Log iRule trace messages to /var/log/ltn? 1=yes, 0=no
# Must be set to 0 for production systems
set ::payload_debug 0
}
# HTTP request received, check if it's a login request and start assembling the
# data
when HTTP_REQUEST {
    # Log the debug message if trace is enabled
    if {::$payload_debug}{log local3. "[IP::client_addr]:[TCP::client_port]:
        New HTTP
        [HTTP::method] request to [HTTP::host][HTTP::uri]" }
    # Reset cookies to empty, later used as an indicator of the fact that
    # login HTTP
    request has been received
    set cookie_all ""
    # If the request is to the login page populate cookie_all variable with
    # all the cookies received
    if {[HTTP::path] starts_with $::login_page and [HTTP::method] eq
        $::login_method}
    {
        set cookie_name [HTTP::cookie names]
        for {set c 0}{%c < [HTTP::cookie count]}{incr c}{
            set cookie_string [split [lindex $cookie_name %c] " "]
            set cookie_list $cookie_string=[HTTP::cookie [lindex
                $cookie_string 0]]
            append cookie_all "," $cookie_list
        }
        # Log the debug message if trace is enabled
        if {::$payload_debug}{log local3. "[IP::client_addr]:[TCP::client_port]:
            Matched path and method check"}
        # Validate the Content-Length value and set the content_length variable
        if {[HTTP::header value Content-Length] > $::max_header_content_length }
        {set content_length $::max_header_content_length
        } else {
            set content_length [HTTP::header value Content-Length]
        }
        # Get the payload data
        if {$content_length > 0}{
            HTTP::collect $content_length
            # Log the debug message if trace is enabled
            if {::$payload_debug}{log local3.
                "[IP::client_addr]:[TCP::client_port]: Collecting $content_length
                bytes"}
        }
    }
}
# Got the data, parse them and generate the syslog message
when HTTP_REQUEST_DATA {
    # If cookies are present this is a login request, get the user name
    if {$cookie_all != "" } {
        # Log the debug message if trace is enabled
        if {::$payload_debug}{log local3. "[IP::client_addr]:
            [TCP::client_port]:
            Collected request data: [HTTP::payload]"}
    }
}

```

```

# Reset the error flag to 0
set uname_logged 0
# Find the $::login_parameter_name among the parameters in the request and
extrat its value
set param_value_pairs [split [HTTP::payload] "&"]
for {set i 0} {$i < [llength $param_value_pairs]} {incr i} {
    set params [split [lindex $param_value_pairs $i] "="]
    if { [lindex $params 0] equals $::login_parameter_name } {
        # User name was found, generate the syslog message
        # which includes IP, port, all the cookies, user name and
        # the auth_method string
        set username [lindex $params 1]
        log local3. "DBFIREWALL:CLIENT=[IP::client_
            addr]:[TCP::client_port]$cookie_all,
            USERNAME=$username,AUTHMETHOD=$::auth_method"
        # Set the flag so not to trigger the error reporting log
        message below
        set uname_logged 1
        break
    }
}
# If user name has not been found in parameters log an error
if {$uname_logged == 0} {
    log local0. "ERROR: iRule failed to extract user name from
        page $login_page with parameter $login_parameter_name"
}
}
}

```

9.4.4.1 Required Syslog Message Format

This topic describes the required syslog message format that is generated by the custom F5 BIG-IP Application Security Manager (BIG-IP ASM) iRule.

The required format of the syslog message to be generated by the custom iRule is as follows:

```

Rule [iRuleName] HTTP_REQUEST_DATA:
DBFIREWALL:CLIENT=[ClientIPAddress]:[ClientPort],[Cookies],
USERNAME=[Name],AUTHMETHOD=[AuthMethod]

```

In this specification:

- `[iRuleName]` is the name of the iRule.
- `[ClientIPAddress]` is the secured target IP address of the Web client.
- `[ClientPort]` is the secured target port number of the Web client.
- `[Cookies]` is a list of cookies available from the BIG-IP ASM HTTP object.
- `[Name]` is the user name.
- `[AuthMethod]` is the method of authentication used between the F5 Web server and its Web clients, as set up in F5 BIG-IP Application Security Manager (BIG-IP ASM). Oracle Audit Vault and Database Firewall does not use this information, other than to report the authentication method used.

For example:

```

Rule capture_login_rule HTTP_REQUEST_DATA:
DBFIREWALL:CLIENT=192.0.2.1:443,ASPSESSIONIDSASSBSCD=1234,TS10da7b=23545,
    USERNAME=FredBloggs,AUTHMETHOD=webforms

```

9.4.4.2 Configuring syslog-ng.conf

To enable the iRule syslog messages to be transmitted to Oracle Audit Vault and Database Firewall, it is necessary to log in to the F5 BIG-IP Application Security Manager (BIG-IP ASM) hardware platform and execute the BIG-IP ASM commands listed below for the version you are using. Doing so modifies `/etc/syslog-ng / syslog-ng.conf` (do not modify the file directly, because changes will not persist after you restart the system).

For F5 BIG-IP Application Security Manager (BIG-IP ASM) Version 11

To configure `syslog-ng.conf`:

1. Run this command:

```
modify sys syslog remote-servers add {dbfw_server_name {host dbfw_IP_address
remote-port dbfw_port}}
```

Where `dbfw_server_name` is the name of your Database Firewall server, and `dbfw_IP_address` and `dbfw_port` are the IP address and port number of the Database Firewall. For example:

```
modify sys syslog remote-servers add { d_dbfw {host 192.0.2.181 remote-port
5514}}
```

2. Save the system configuration:

```
save sys config
```

For All Other Supported F5 BIG-IP Application Security Manager (BIG-IP ASM) Versions

To configure `syslog-ng.conf`, run this command:

```
bigpipe syslog include "destination d_dbfw { tcp(\"dbfw_ip_address\"
port(dbfw_port));};log { source(local); filter(f_local3); destination(d_dbfw);};"
```

Where `dbfw_ip_address` and `dbfw_port` are the IP address and port number of the Database Firewall (the value entered for **System Address** in Step 6).

For example (the IP address and port will be different for each enforcement point):

```
bigpipe syslog include "destination d_dbfw { tcp(\"192.0.2.181\"
port(5514));};log { source(local); filter(f_local3); destination(d_dbfw);};"
```

The two instances of the syslog destination name (`d_dbfw`) need to be changed only in the unlikely event that the destination name is already in use.

9.5 Viewing F5 Data in Oracle Audit Vault and Database Firewall Reports

This topic describes viewing F5 BIG-IP Application Security Manager (BIG-IP ASM) data in Oracle Audit Vault and Database Firewall reports.

You can generate several reports from the Audit Vault Server console.

 **Note:**

- This functionality is only supported on F5 BIG-IP Application Security Manager (BIG-IP ASM) version 10.2.1.
- F5 BIG-IP Application Security Manager (BIG-IP ASM) integration is deprecated in release Oracle AVDF 12.2.0.7.0, and is desupported in 20.1.

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.

For the push method where Oracle Audit Vault and Database Firewall sends alerts to the SIEM using SYSLOG, see [Configuring Oracle Audit Vault Server Syslog Destinations](#) (page 3-8) for information.

For the pull method, configure SIEM to view and extract all the data from **AVSYS.EVENT_LOG** table using the collector provided by the SIEM. This requires creating a user in Oracle Audit Vault and Database Firewall with auditor role. Ensure 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 be completed in the SIEM. The Oracle Audit Vault and Database Firewall schema and the specific mapping in **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 due course, 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.

See Also:

- [START COLLECTION FOR SECURED TARGET](#) (page A-26)
- [Oracle Database](#) (page B-4)

Topics

- [How Oracle Audit Vault and Database Firewall Integrates with HP ArcSight SIEM \(page 10-2\)](#)
- [Enabling the HP ArcSight SIEM Integration \(page 10-2\)](#)

10.1 How Oracle Audit Vault and Database Firewall Integrates with HP ArcSight SIEM

The HP ArcSight Security Information Event Management (SIEM) system is a centralized system for logging, analyzing, and managing messages from different sources. The Audit Vault Server forwards messages to ArcSight SIEM from both the Audit Vault Server and Database Firewall components of Oracle Audit Vault and Database Firewall.

You do not need to install additional software if you want to integrate ArcSight SIEM with Oracle Audit Vault and Database Firewall. You configure the integration by using the Audit Vault Server console.

Messages sent to the ArcSight SIEM Server are independent of any other messages that may be sent from Oracle Audit Vault and Database Firewall. This means you can send standard syslog messages to a different destination.

Oracle Audit Vault and Database Firewall categorizes the messages that can be sent to ArcSight SIEM. There are three categories:

- **System** - syslog messages from subcomponents of the Audit Vault Server and Database Firewall components of Oracle Audit Vault and Database Firewall
- **Info** - specific change logging from the Database Firewall component of Oracle Audit Vault and Database Firewall
- **Debug** - a category that should only be used under the direction of Oracle Support

Note:

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

10.2 Enabling the HP ArcSight SIEM Integration

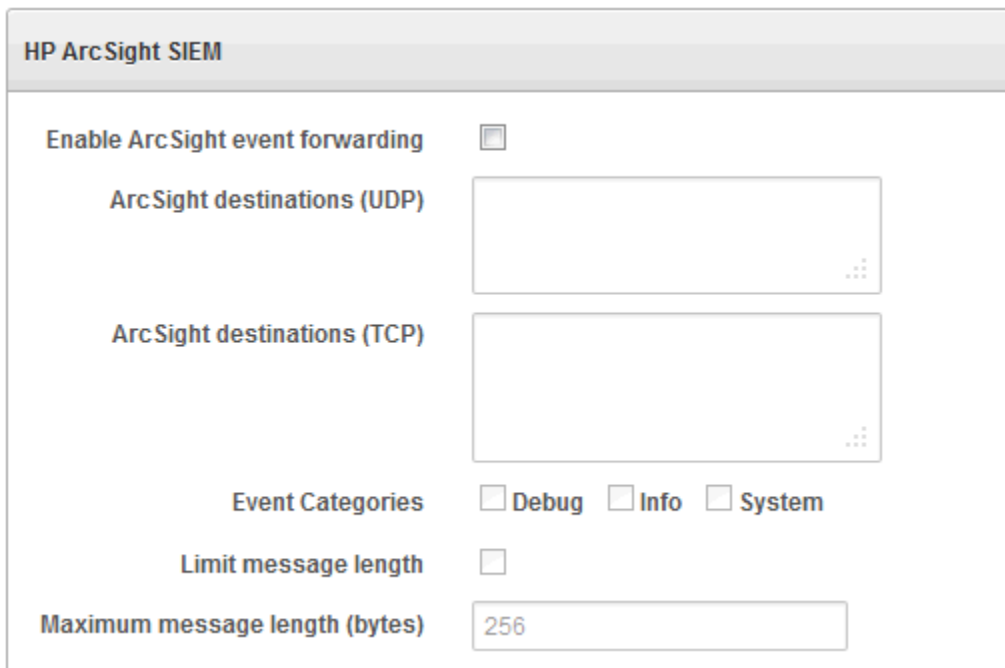
When you enable the ArcSight SIEM integration, the settings take effect immediately. You do not need to restart the Audit Vault Server.

 **Note:**

HP ArcSight SIEM is deprecated in 12.2.0.8.0, and will be desupported in 12.2.0.9.0. It is advisable to use the `syslog` integration feature instead.

To enable ArcSight SIEM integration:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
3. From the **System** menu, click **Connectors**, and scroll down to the **HP ArcSight SIEM** section.



HP ArcSight SIEM

Enable ArcSight event forwarding

ArcSight destinations (UDP)

ArcSight destinations (TCP)

Event Categories **Debug** **Info** **System**

Limit message length

Maximum message length (bytes)

4. Specify the following:
 - **Enable ArcSight event forwarding:** Select this check box to enable ArcSight SIEM integration.
 - **ArcSight destinations:** Depending on the communications protocol you are using, enter the IP address or host name of the ArcSight server in the **UDP** field, or its IP address, host name, and port in the **TCP** field. This setting enables the syslog log output to be sent to this ArcSight server in Common Event Format (CEF).
 - **Event categories:** Select any combination of message categories depending on which type of messages that are needed in the ArcSight server.
 - **Limit message length:** You can choose to limit the message to a specified number of bytes.
 - **Maximum message length (bytes):** If you selected **Limit message length**, enter the maximum length that you want. The range allowed is 1024 to 1048576 characters.

5. Click **Save**.

 **See Also:**

[Logging in to the Audit Vault Server Console UI \(page 1-11\)](#)

11

Using an Oracle Database Firewall with Oracle RAC

You can configure an Oracle Database Firewall to work with Oracle Real Application Clusters (Oracle RAC) so that it can block and substitute statements using Database Policy Enforcement (DPE) proxy mode, or log SQL statements and raise alerts using Database Activity Monitoring (DAM) inline and out-of-band mode.

Topics:

- [Configuring a Database Firewall with Oracle RAC for DPE Mode](#) (page 11-1)
- [Configuring a Database Firewall with Oracle RAC for DAM Mode](#) (page 11-8)

11.1 Configuring a Database Firewall with Oracle RAC for DPE Mode

Topics:

- [About Configuring a Database Firewall with Oracle RAC for DPE Proxy Mode](#) (page 11-1)
- [Step 1: Configure the Listeners for Each Oracle RAC Node](#) (page 11-3)
- [Step 2: Configure the Proxies in the Oracle Database Firewall Console](#) (page 11-4)
- [Step 3: Test the Audit Reports to Ensure That They Can Collect Oracle RAC Node Data](#) (page 11-7)

11.1.1 About Configuring a Database Firewall with Oracle RAC for DPE Proxy Mode

To use Database Policy Enforcement (DPE) mode in an Oracle Database Firewall with Oracle RAC, Oracle recommends that you perform the configuration proxy mode.

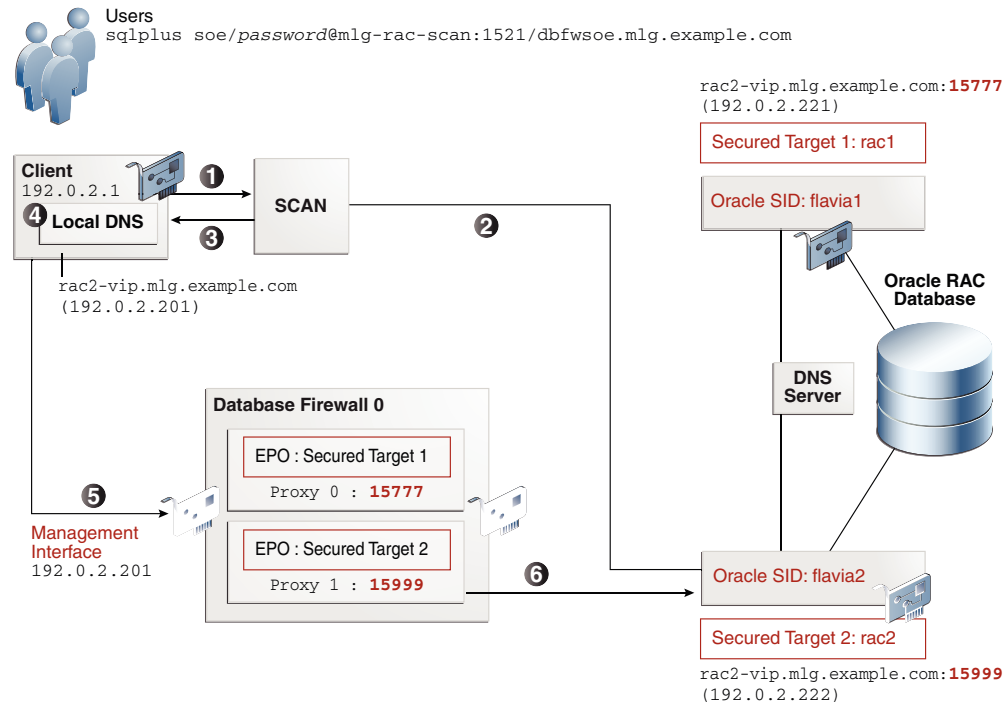
The procedures in this section assume that you have one Oracle Database Firewall and one Oracle Audit Vault Server, but you can easily include more Database Firewalls by following the examples shown. The Database Firewall will be configured in proxy mode, in which the following takes place:

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 an outbound connection to the redirected RAC node.
5. The response from Oracle RAC node is passed to the client.

All components must be in the same subnet. If the client and the SCAN Listener are in different subnets, then 2 Network Interface Cards are needed (one in the client subnet and the other in SCAN Listener subnet). The internal Database Firewall routing must be adjusted if the client, Database Firewall, and database server reside in a different subnet.

Figure 11-1 (page 11-2) shows the setup environment that will be used in the procedure that this chapter covers.

Figure 11-1 Oracle Database Firewall and Oracle RAC SCAN VIP Architecture



Address Resolution		
IP Address	Local DNS (client-site)	Server DNS (server-site)
rac1-vip.mlg.example.com	192.0.2.201	192.0.2.221
rac2-vip.mlg.example.com	192.0.2.201	192.0.2.222

A typical request flow is as follows:

1. An application issues a request to SCAN to find the least loaded instance for the database service (for example, soe.mlg.example.com).
2. SCAN returns the connection information of the least loaded instance, in the form of `node_id_fqdn:node_id_local_port`. Traditionally SCAN will return `node_vip_ip:node_id_local_port`. However, for the procedure that is described here, the IP address is replaced with the corresponding fully qualified domain name.
3. The application looks up and resolves `node_id_fqdn` into the Database Firewall proxy interface IP using a separate local DNS service.

4. The request is forwarded to the respective enforcement point in the Database Firewall, and assuming the proxy in the Database Firewall has already been created using the same port as `node_id_local_port`, the connection takes place.
5. The user then is able to connect to the Database Firewall using the appropriate management interface.
6. When the user makes this connection, the Oracle RAC node is available as a secured target.

11.1.2 Step 1: Configure the Listeners for Each Oracle RAC Node

1. On each Oracle RAC node that you plan to use for with the Oracle Database Firewall, create and start a local listener.

For example:

```
srvctl add listener -l NODE1LISTENER -p 15777
srvctl start listener -l NODE1LISTENER -n rac1
srvctl add listener -l NODE2LISTENER -p 15999
srvctl start listener -l NODE2LISTENER -n rac2
```

Replace the values `NODE1LISTENER`, `15777`, `rac1`, `NODE2LISTENER`, `15999`, and `rac2` with your respective environment values. These example values will be used in this procedure.

For more information about using the `srvctl` utility, see *Oracle Real Application Clusters Administration and Deployment Guide*.

2. Log in to SQL*Plus on each node as a user who has the `ALTER SYSTEM` system privilege.

For example:

```
sqlplus system
Enter password: password
```

3. Run the `ALTER SYSTEM SQL` statement to dynamically register each listener in the nodes.

For example, to register the listeners on the Oracle SIDs `flavia1` and `flavia2`:

```
ALTER SYSTEM SET LOCAL_LISTENER="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=rac1-vip.mlg.example.com)(PORT=15777))))" SCOPE=BOTH SID='flavia1';

ALTER SYSTEM SET LOCAL_LISTENER="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=rac2-vip.mlg.example.com)(PORT=15999))))" SCOPE=BOTH SID='flavia2';
```

4. From the command line, run the following `srvctl` commands to verify the local listeners in the Oracle RAC clusters:

```
srvctl status listener //check listener location
srvctl config listener //check TCP ports
```

For example:

```
[oracle@rac1 bin]$srvctl status listener
Listener LISTENER is enabled
Listener LISTENER is running on node(s): rac2, rac1
Listener NODE1LISTENER is enabled
Listener NODE1LISTENER is running on node(s): rac1
Listener NODE2LISTENER is enabled
Listener NODE2LISTENER is running on node(s): rac2

[oracle@rac1 bin]$srvctl config listener
```

```
Name: LISTENER
Network: 1, Owner: oracle
Home: <CRS home>
End points: TCP:15888
Name: NODE1LISTENER
Network: 1, Owner:oracle
Home: <CRS home>
End points: TCP:15777
Name: NODE2LISTENER
Network: 1, Owner: oracle
Home: <CRS home>
End points: TCP:15999
```

5. On each node, in SQL*Plus, run the `SHOW PARAMETER LISTENER` command to show the local listener on the nodes.

For example, on node `rac1`:

```
SHOW PARAMETER LISTENER
```

NAME	TYPE	VALUE
listener_networks	string	
local_listener	string	((DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=rac1-vip.mlg.example.com)(PORT=15777)))))
remote_listener	string	mlg-rac-scan:1521

For node `rac2`:

```
SHOW PARAMETER LISTENER
```

NAME	TYPE	VALUE
listener_networks	string	
local_listener	string	((DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=rac2-vip.mlg.example.com)(PORT=15999)))))
remote_listener	string	mlg-rac-scan:1521

6. Modify the local DNS on the application site to resolve the database virtual IP fully-qualified domain name into the Database Firewall IP address.

For example, to edit the `/etc/hosts` file in the client, you would add the following settings.

```
192.0.2.201 rac1-vip.mlg.example.com
192.0.2.201 rac2-vip.mlg.example.com
```

A full-fledged DNS service is required if there are more than one Database Firewalls and you want to do load balancing across the servers.

11.1.3 Step 2: Configure the Proxies in the Oracle Database Firewall Console

1. Log in to the Oracle Database Firewall console.
2. Configure the proxy.

After you complete the configuration, the Management Interface page should appear similar to the following:

Management Interface

Settings

IP Address 192.0.2.201
Network Mask 255.255.255.0
Gateway 192.0.2.254
Name dbfw080027cc90b4

Device

MAC Address	Bus Info	Identifier	Manufacturer	Link
08:00:27:cc:90:b4	0000:00:03:0	82540EM Gigabit Ethernet Controller	Intel Corporation	yes

Proxy Ports

Traffic Source Id	Port	Enabled	
Management:15211	15211	no	Remove
Management:15777	15777	yes	Remove
Management:15999	15999	yes	Remove

3. Configure enforcement points.

When you complete this configuration, the Enforcement Points page should appear similar to the following:

Enforcement Points

[Go](#) [Actions ▾](#)

Status	Name ▲	Secured Target	Firewall
↑	rac1ep	rac1	dbfw080027cc90b4
↑	rac2ep	rac2	dbfw080027cc90b4

1 - 3

You can find details about each enforcement point by clicking its name in the Name column. For example, the enforcement point for the rac1 node could appear as follows:

Enforcement Point Details

Mode DPE

Traffic Sources proxy2

▼ **Firewalls**

Status	Name	IP Address
↑	dbfw080027cc90b4	192.0.2.201

1 - 1

▼ **Secured Target**

Name rac1

Database Type Oracle Database

Policy Examine RAC Traffic

Secured Target Addresses

Address	Port	Service Name
192.0.2.221	15777	dbfwsoe.mlg.example.com

1 - 1

4. Test the connection.

Log in to each Oracle RAC node that you configured, and then try running a simple command to see if the connection works.

For example:

```
sqlplus system
Enter password: password

SELECT SYSDATE FROM DUAL;
```


 **See Also:**

- [Configuring Enforcement Points](#) (page 6-20)
- [Configuring Oracle Database Firewall As A Traffic Proxy](#) (page 4-11)
- [Logging in to the Database Firewall Console UI](#) (page 1-13)

11.1.4 Step 3: Test the Audit Reports to Ensure That They Can Collect Oracle RAC Node Data

After the configuration is complete, you should ensure that it can collect data from the various Oracle RAC nodes.

1. Log in to the Audit Vault Server console.
2. Check the reports to ensure that audit data has been collected from the Oracle RAC nodes that you configured.

For example, the following Data Access report shows that audit data has been collected from the `rac2` node.

Data Access Report

Report View < > Row 7 of 9 Exclude Null Values Displayed Columns

Secured Target

Secured Target Name rac2
 Secured Target Type Oracle Database
 Service Name dbfwsoe.mlg.example.com
 Policy Name Examine RAC Traffic
 Secured Target Class Database

Event

Server Time 8/6/2015 12:27:57 PM
 Event Time 8/6/2015 12:25:01 PM
 User Name soe
 Event Status SUCCESS
 Error Code 0
 Error Message
 Event Name statement
 Command Class SELECT
 Action Taken pass
 Threat Severity moderate
 Log Cause unseen
 Location Network

Target

Target Type TABLE
 Target Object CUSTOMERS
 Target Owner

Client/User Information

OS User Name lnhph
 Client Host Name
 Client IP 192.0.2.1
 Network Connection 192.0.2.1:57433, 192.0.2.222:15999
 Client Program sqlplus@Linhs-MacBook-Pro.local (TNS V1-V3)

Statement

Command Text select CUST_FIRST_NAME, CUST_LAST_NAME, CUST_EMAIL from customers where rownum <0
 Command Param

Other

Extension user_name_origin='network':raw_user_name='soe':service_name_origin='network':session_source_type='ProxyIPS':04:25:01.898000::transaction_time='0.064':application_name_origin='network':os_user_name_origin='network'
 Original Content



See Also:

[Logging in to the Audit Vault Server Console UI \(page 1-11\)](#)

11.2 Configuring a Database Firewall with Oracle RAC for DAM Mode

You can configure an Oracle Database Firewall with Oracle RAC to use Database Activity Monitoring (DAM) inline and out-of-band mode. This type of configuration is the most straightforward (that is, it works out of the box).

To accomplish this, you must ensure that all the IP addresses for the Oracle RAC nodes are included in the secured target configuration. This can be a single secured

target configuration with multiple IPs for each Oracle RAC node. Alternatively, it can be a separate secured target for each node.

12

Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment

To begin using Oracle Audit Vault and Database Firewall Hybrid Cloud Deployment, you should perform some preliminary tasks, such as downloading the latest version of this manual and understanding the basic concepts of using Oracle Audit Vault and Database Firewall Hybrid Cloud Deployment as documented in this chapter.

Topics

- [Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment And Pre-requisites](#) (page 12-1)
- [Opening Ports on DBCS](#) (page 12-3)
- [Configuring Hybrid Cloud Secured Target Using TCP](#) (page 12-4)
- [Configuring TCPS Connections for DBCS Instances](#) (page 12-8)
- [Configuring Hybrid Cloud Secured Target Using TCPS](#) (page 12-19)
- [Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCPS](#) (page 12-23)
- [Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCP](#) (page 12-25)
- [Configuring Autonomous Data Warehouse and Autonomous Transaction Processing](#) (page 12-27)

12.1 Oracle Audit Vault And Database Firewall Hybrid Cloud Deployment And Pre-requisites

Oracle recommends you follow these steps to deploy Hybrid Cloud Secured Target instance.

In Oracle Audit Vault and Database Firewall hybrid 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 are configured specifically for cloud targets to collect audit data from Cloud Database instances. These Agents connect to the target database and to the Audit Vault Server. Connections to the Audit Vault Server are made through SQL*Net on ports 1521 and 1522. There is a wide variety of network configurations, firewalls, and cloud providers, each with their own unique ways of configuring network connectivity. 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. 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, where the Audit Vault Server is running in Oracle Public Cloud, configuration of the on-premises network to enable connectivity between the Agents and Audit Vault Server is the responsibility of the customer, and support is for the Agent itself, and not the underlying network components involved in allowing the connections.

TCP and TCPS are the two connection options in DBCS. Setting up connections for TCP and TCPS is similar. The difference is the port numbers. The following are key characteristics of Database Cloud Service (DBCS) 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.

Pre-requisites for deploying Oracle 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 Oracle 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

Feature	DBs On-premises	DBs in OPC	Exadata Express Cloud Service	Data Warehouse Cloud Service
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

Pre-requisites 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 11g Release 11.2	<ul style="list-style-type: none"> • Fine Grained Audit • Database Vault Audit • Traditional Audit data stored in <i>sys.AUD\$</i>
Oracle Database 12c and later	<ul style="list-style-type: none"> • Unified Audit • Database Vault Audit • Fine Grained Audit • Traditional Audit data stored in <i>sys.AUD\$</i>

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 secured target to `DB_EXTENDED`.

12.2 Opening Ports on DBCS

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 Compute 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**.

12.3 Configuring Hybrid Cloud Secured Target Using TCP

This section contains detailed deployment steps for configuring cloud targets for DBCS instances in TCP mode. The Audit Vault server and Audit Vault agent are installed on-premises.

Topics

- [Step 1: Registering On-premises Host on the Audit Vault Server](#) (page 12-4)
- [Step 2: Installing Audit Vault Agent on Registered On-premises Hosts](#) (page 12-5)
- [Step 3: Creating A User Account On The DBCS Target Instance](#) (page 12-5)
- [Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Database Cloud Service Instances](#) (page 12-6)
- [Step 5: Creating a Secured Target on Audit Vault Server for the DBCS Instance](#) (page 12-7)
- [Step 6: Starting Audit Trail On Audit Vault Server For The DBCS Instance](#) (page 12-7)

12.3.1 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 in the Audit Vault Server](#) (page 5-2)

12.3.2 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 and Activating the Audit Vault Agent on Host Computers](#) (page 5-3) for detailed steps on installing on-premises host.

2. Start the Audit Vault agent.

12.3.3 Step 3: Creating A User Account On The DBCS Target Instance

Note:

The connection methodology is different in case on-premises deployment, for TCP connections.

Prerequisite

- Port 1521 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 DBCS](#) (page 12-3) 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 secured target user account.
oracle_AVDF_dbcs_drop_db_permissions.sql	To revoke permission from user.

- Execute the script in order to setup secured target user account in specific mode:

```
oracle_AVDF_dbcs_user_setup.sql <username> <mode>
```

Where <username> is the user name of the Hybrid cloud secured target user.

The <mode> can be one of the following:

Mode	Purpose
AUDIT_COLLECTION	To collect data from Oracle Cloud instance <i>TABLE</i> 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.

12.3.4 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 policies that are enabled and change them as needed. For Oracle Database 11g release 11.2 and Oracle Database 12c 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 Oracle 12c 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.

12.3.5 Step 5: Creating a Secured Target on Audit Vault Server for the DBCS Instance

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. Use the following procedure:

1. Log in to Audit Vault console with administrator privileges.
2. Click **Secured Targets** tab.
3. Click **Register**.
4. In the **Secure target Location (for Auditing)** region, choose **Advanced** option.
5. Enter the following TCP connection string in the text box:

```
jdbc:oracle:thin:@//<Host IP>:<Port Number>/<service name>
```

 **Note:**

This can also be accomplished in the **Basic** option. Enter the details in **Host Name/IP Address**, **Port**, **Service Name** fields.

6. Click **Save** to save the configuration changes.

12.3.6 Step 6: Starting Audit Trail On Audit Vault Server For The DBCS Instance

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 with *administrator* privileges.
2. In the **Secure Target**, select **Audit Trails** and then **Add Audit Trail**.
3. Select **Audit Trail Type** as `TABLE`.

 **Note:**

Other trail types are not supported for DBCS secured target instances.

4. Select the registered **Collection Host** and **Secured Target** in the previous and following steps.
5. The supported table trails for Oracle DBCS secured target are:

- a. UNIFIED_AUDIT_TRAIL
 - b. SYS.AUD\$
 - c. SYS.FGA_LOG\$
 - d. DVSYS.AUDIT_TRAIL\$
6. Click **Save** to add the audit trail.

12.4 Configuring TCPS Connections for DBCS Instances

High level process to configure TCPS connections for DBCS instances:

Topics

- [Step 1: Creating Server Wallet and Certificate](#) (page 12-8)
- [Step 2: Creating Client \(Agent\) Wallet and Certificate](#) (page 12-10)
- [Step 3: Exchanging Client \(Agent\) and Server Certificates](#) (page 12-13)
- [Step 4: Configuring Server Network](#) (page 12-16)
- [Step 5: Connecting to DBCS instances in TCPS mode](#) (page 12-18)

Prerequisite

- Port 1522 has to be opened up on the DBCS Instance for TCPS connection. See [Opening Ports on DBCS](#) (page 12-3) for detailed information. Later some standard tools such as SQL*Plus and SQL*Developer can be used.

12.4.1 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 DBCS](#) (page 12-3) 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-----
MIIB0TCCAToCAQAwDQYJKoZIhvcNAQEEBQAwmTEvMC0GA1UEAxMmQ2xvdWRTVDIuZGVhZGV2MTku
b3JhY2x1Y2xvdWQuaW50ZXJ1YWwHhcNMTYwNTEyMDI2WhcNMjYwNTA5MTEyMDI2
WjAxMS8w
LQYDVQQDEyZDbG91ZFNUMi5kZWJkZXYxOS5vcmFjbGVjbG91ZC5pbmRlcm5hbDBnZAN
BgkqhkiG
9w0BAQEFAAOBjQAwGyKCyYEAfhuQ1y2t3i8gugLVzgp2kFGVXVOzqbggEIC+Qazb15
JuKs0ntk
En9ERGVa0fxHkAkCtIPjCzQD5WYRU9C8AQQOWe7UFHae7PsQX8j smEtecpr5Wkq3818+
26qU3Jyi
XxxK/rRydwbO526G5Tn5XPsovaw/PYJxF/
fIKMG7fzMCAwEAATANBgkqhkiG9w0BAQQFAAOBgQCu
fBYJj4wQYriZIfjij4eac/
jn085Eiff3L3DU8qCHJxOxRgK97GJzD73TiY20xpzQjWKougX73YKV
Tp9yusAx/T/
qXbpAD9JKyHlKj16wPeeMcS06pmDDXtJ2CYqOUwMIk53cK7mLaAHCbYGGM6btqP4V
KYIjP48GrsQ5MOqd0w==
-----END CERTIFICATE-----
```

12.4.2 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 <client 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-----
MIIBsTCCARoCAQAwDQYJKoZIhvcNAQEEBQAwITEfMB0GA1UEAxMWZ2JyMzAxMzkudWsub3JhY2
xl
LmNvbTAeFw0xNjA1MTExMTQzMzFaFw0yNjA1MDkxMTQzMzFaMCEwHzAdBgNVBAMTFmducjMwMT
M5
LnVrLm9yYWNsZS5jb20wgZ8wDQYJKoZIhvcNAQEEBQADgY0AMIGJAoGBAKH8G8sFS6l0llu+RM
fl
7Yt+Ppw8J0PfDEDbTGP5wtsrs/
22dUCipU9l+vif1VgSPLE2UPJbGM8tQzTC6UYbBtWHe4CshmvD
EVlcIMsEFvD7a5Q+P45jqNSEtV9VdbGyxaD6i5Y/
Smd+B87FcQQCX54LaI9BJ8SZwmPXgDweADLf
AgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAai742jfNYyTKMq2xxRygGJGn1LhpFenHvuHLBvnTup
1N
nZOBwBi4VxW3CImvwONYcCEfp3E1SRswS5evlfIfrucZ1xQBouNei3EJ6030dKeRRp2E+muXEt
fe
U+jwUE+SzpnzfpI230kl2vo8Q7VHrSalxE2KEhAzC1UYX7ZYp1U=
-----END CERTIFICATE-----

```

12.4.3 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=machinel.foobar.example.com

Trusted Certificates:

Subject: OU=Class 1 Public Primary Certification
Authority,O=VeriSign\, Inc.,C=US

Subject: CN=machinel.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 machinel-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=machinel.foobar.example.com

Trusted Certificates:

Subject: OU=Class 1 Public Primary Certification

Authority,O=VeriSign\, Inc.,C=US

Subject: CN=machinel.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

12.4.4 Step 4: Configuring Server Network

This step explains how to configure the server network.

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
<i>ACCEPTED</i>	The server does not allow both encrypted and non-encrypted connections. This is the default value in case the parameter is not set.
<i>REJECTED</i>	The server does not allow encrypted traffic.
<i>REQUESTED</i>	The server requests encrypted traffic if it is possible, but accepts non-encrypted traffic if encryption is not possible.
<i>REQUIRED</i>	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
```

12.4.5 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](#) (page 12-8) for detailed steps on configuring TCPS for DBCS instance.
- [Opening Ports on DBCS](#) (page 12-3)

12.5 Configuring Hybrid Cloud Secured Target Using TCPS

This section contains detailed deployment steps for configuring cloud targets for DBCS instances in TCPS mode. The Audit Vault server and Audit Vault agent are installed on-premises.

Topics

- [Step 1: Registering On-premises Host on Oracle Audit Vault Server](#) (page 12-19)
- [Step 2: Installing Oracle Audit Vault Agent on Registered On-premises Hosts and Configuring TCPS](#) (page 12-20)
- [Step 3: Creating User Accounts on Oracle Database Cloud Service Target Instances](#) (page 12-20)
- [Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Database Cloud Service Instances](#) (page 12-21)
- [Step 5: Creating A Secured Target On Audit Vault Server For The DBCS Instance](#) (page 12-22)
- [Step 6: Starting Audit Trail On Audit Vault Server For The DBCS Instance](#) (page 12-23)

12.5.1 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 in the Audit Vault Server](#) (page 5-2) for detailed steps.

12.5.2 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 and Activating the Audit Vault Agent on Host Computers](#) (page 5-3) for detailed steps on installing on-premises host.
2. Start the Audit Vault agent.

12.5.3 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 DBCS](#) (page 12-3) 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.

12.5.4 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 policies 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.

12.5.5 Step 5: Creating A Secured Target On Audit Vault Server For The DBCS Instance

The user must define these specific settings on the **Target configuration** page. Use the following procedure:

1. Log in to Audit Vault console with administrator privileges.
2. Click **Secured Targets** tab.
3. Click **Register**.
4. In the **Secured Target Location (for Auditing)** region, choose **Advanced** option.
5. Enter the following TCPS connection string in the text box **Secured Target Location**:

```
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")))
```

 **Note:**

This can also be accomplished in the **Basic** option. Enter the details in **Host Name/IP Address**, **Server DN**, and the **Wallet** fields.

6. In the **Wallet** field, choose the client wallet by navigating to the location of the wallet where it was previously created.
7. Click **Save** to save the configuration changes.

 **See Also:**

[Configuring TCPS Connections for DBCS Instances](#) (page 12-8) for information on creating a wallet.

12.5.6 Step 6: Starting Audit Trail On Audit Vault Server For The DBCS Instance

Use this procedure to start audit trail on the Audit Vault Server for the DBCS instance:

1. Log in to Audit Vault console with *administrator* privileges.
2. In the **Secured Target** region, select **Audit Trails**, and then **Add Audit Trails** option.
3. Select **Audit Trail Type** as `TABLE`.

 **Note:**

Other trail types are not supported for the DBCS secured target instance.

4. Select the registered **Collection Host** and **Secured Target** mentioned in the previous and following steps.
5. The supported table trails for Oracle DBCS Secured target are:
 - a. `UNIFIED_AUDIT_TRAIL`
 - b. `SYS.AUD$`
 - c. `SYS.FGA_LOG$`
 - d. `DVSYSAUDIT_TRAIL$`
6. Click **Save** to add the audit trail.

12.6 Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCPS

This section contains detailed deployment steps for configuring Oracle Database Exadata Express Cloud Service secured targets in TCPS mode.

Topics

- [Step 1: Installing Audit Vault Agent on registered on-premises Host and configuring TCPS](#) (page 12-24)
- [Step 2: Creating User Accounts on Oracle Exadata Express Cloud Service Instances](#) (page 12-24)
- [Step 3: Creating A Secured Target On Audit Vault Server For Exadata Express Cloud Service Instance](#) (page 12-25)

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>

12.6.1 Step 1: Installing Audit Vault Agent on registered on-premises Host and configuring TCPS

See [Step 2: Installing Oracle Audit Vault Agent on Registered On-premises Hosts and Configuring TCPS](#) (page 12-20).

12.6.2 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](#) (page 12-8) for creating Server Wallet, Client Wallet, certificates, and exchanging certificates.

12.6.3 Step 3: Creating A Secured Target On Audit Vault Server For Exadata Express Cloud Service Instance

1. Create a Secured Target on Audit Vault Server for the DBCS Instance. See [Step 5: Creating A Secured Target On Audit Vault Server For The DBCS Instance](#) (page 12-22).
2. Execute the following command to set mandatory secured target attribute for SSL version:

```
av.collector.stconn.oracle.net.ssl_version = 1.2
```

12.7 Configuring Oracle Database Exadata Express Cloud Service Secured Target Using TCP

This section contains detailed deployment steps for configuring Exadata Express Cloud Targets in TCP mode. The Audit Vault Server and Audit Vault Agent are installed on-premises.

Topics

- [Step 1: Registering On Premises Host On The Audit Vault Server](#) (page 12-25)
- [Step 2: Installing Audit Vault Agent On Registered On Premises Host](#) (page 12-25)
- [Step 3: Creating User Accounts on Oracle Exadata Express Cloud Target Instances](#) (page 12-25)
- [Step 4: Setting Up or Reviewing Audit Policies on Target Oracle Exadata Express Cloud Instances](#) (page 12-26)
- [Step 5: Creating A Secured Target On Audit Vault Server For The Exadata Express Cloud Instance](#) (page 12-26)
- [Step 6: Starting Audit Trail On Audit Vault Server For The Exadata Express Cloud Instance](#) (page 12-26)

12.7.1 Step 1: Registering On Premises Host On The Audit Vault Server

See [Step 1: Registering On-premises Host on the Audit Vault Server](#) (page 12-4).

12.7.2 Step 2: Installing Audit Vault Agent On Registered On Premises Host

See [Step 2: Installing Audit Vault Agent on Registered On-premises Hosts](#) (page 12-5).

12.7.3 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
```

12.7.4 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.

12.7.5 Step 5: Creating A Secured Target On Audit Vault Server For The Exadata Express Cloud Instance

See [Step 5: Creating a Secured Target on Audit Vault Server for the DBCS Instance](#) (page 12-7).

12.7.6 Step 6: Starting Audit Trail On Audit Vault Server For The Exadata Express Cloud Instance

Use this procedure to start audit trail on the Audit Vault Server for the Exadata Express Cloud instance:

1. Log in to Audit Vault console with *administrator* privileges.
2. In the **Secured Target** region, select **Audit Trails**, and then **Add Audit Trails** option.
3. Select **Audit Trail Type** as `TABLE`.

 **Note:**

Other trail types are not supported for the Express Exadata Cloud secured target instance.

4. Select the registered **Collection Host** and **Secured Target** mentioned in the previous and following steps.
5. The supported table trails for Oracle Express Exadata Cloud secured target are:
 - a. `UNIFIED_AUDIT_TRAIL`
6. Click **Save** to add the audit trail.

12.8 Configuring Autonomous Data Warehouse and Autonomous Transaction Processing

This section contains detailed deployment steps for configuring the following Oracle Database Cloud Service types as secured targets in TCPS mode:

- Autonomous Data Warehouse
- Autonomous Transaction Processing

Topics

- [Step 1: Install Audit Vault Agent On Registered On-premises Host And Configuring TCPS \(page 12-27\)](#)
- [Step 2: Create User Accounts on Oracle Cloud Instances \(page 12-27\)](#)
- [Step 3: Create A Secured Target On Audit Vault Server For The Cloud Instance \(page 12-28\)](#)

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>

12.8.1 Step 1: Install Audit Vault Agent On Registered On-premises Host And Configuring TCPS

See [Step 2: Installing Oracle Audit Vault Agent on Registered On-premises Hosts and Configuring TCPS \(page 12-20\)](#).

12.8.2 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 Server Wallet and certificate.
3. Create Client Wallet and certificate.
4. Exchange Client and Server certificates.
5. Configure Server network.

6. Once the above steps are complete, the user can now connect to the Autonomous Data Warehouse Cloud 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 scripts:

```
oracle_AVDF_E1_user_setup.sql  
oracle_AVDF_E1_drop_db_permissions.sql
```

 **See Also:**

[Configuring TCPS Connections for DBCS Instances](#) (page 12-8) for creating Server Wallet, Client Wallet, certificates, and exchanging certificates.

12.8.3 Step 3: Create A Secured Target On Audit Vault Server For The Cloud Instance

Create a Secured Target on Audit Vault Server for the Autonomous Data Warehouse or Autonomous Transaction Processing Cloud Instance. See [Step 5: Creating A Secured Target On Audit Vault Server For The DBCS Instance](#) (page 12-22).

Part II

General Administration Tasks

Part II assumes that you have completed the steps in Part I to configure your Audit Vault and Database Firewall system. This part covers general administrative tasks.

This part contains the following chapters:

- [Managing User Accounts and Access](#) (page 13-1)
- [Managing the Audit Vault Server and Database Firewalls](#) (page 14-1)
- [Configuring a SAN Repository](#) (page 15-1)

13

Managing User Accounts and Access

Topics

- [About Oracle Audit Vault and Database Firewall Administrative Accounts](#) (page 13-1)
- [Security Technical Implementation Guides and Implementation for User Accounts](#) (page 13-2)
- [Configuring Administrative Accounts for the Audit Vault Server](#) (page 13-2)
- [Configuring sudo Access for Users](#) (page 13-5)
- [Managing User Access Rights to Secured Targets or Groups](#) (page 13-7)
- [Changing User Passwords in Oracle Audit Vault and Database Firewall](#) (page 13-8)

13.1 About Oracle Audit Vault and Database Firewall Administrative Accounts

When administrators log in to Oracle Audit Vault and Database Firewall, they have access only to administrative functions, whereas auditors have access only to the auditing functions.

Oracle Audit Vault and Database Firewall has three types of administrative user accounts:

- **Audit Vault Server Super Administrator:**
 - Manages system-wide settings
 - Creates user accounts for super administrators and administrators
 - Has access to all secured targets and secured target groups
 - Grants access to secured targets or secured target groups to administrators
- **Audit Vault Server Administrator:** Has access to specific secured targets or secured target groups granted by a super administrator. Administrators cannot manage system-wide settings.
- **Database Firewall Administrator:** Has access to the Database Firewall administrative interface. The Database Firewall has only one administrator.

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, and one administrator account for the Database Firewall.

Thereafter, the Audit Vault Server super administrator can create other administrative users, and the super auditor can create other auditor users, for the server.

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.

13.2 Security Technical Implementation Guides and Implementation for User Accounts

Oracle Audit Vault and Database Firewall follow STIG rules 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](#) (page F-1) for more information about STIG compliance

13.3 Configuring Administrative Accounts for the Audit Vault Server

Topics

- [Guidelines for Securing the Oracle Audit Vault and Database Firewall User Accounts](#) (page 13-3)
- [Creating Administrative Accounts for the Audit Vault Server](#) (page 13-3)
- [Viewing the Status of Administrator User Accounts](#) (page 13-4)
- [Changing a User Account Type for the Audit Vault Server](#) (page 13-4)
- [Unlocking a User Account](#) (page 13-4)
- [Deleting an Audit Vault Server Administrator Account](#) (page 13-5)

13.3.1 Guidelines for Securing the Oracle Audit Vault and Database Firewall User Accounts

As a best practice, you should use the installed Audit Vault and Database Firewall user accounts only as back-up accounts. Add new user accounts, with unique user names and passwords, for the users who are responsible for the day-to-day Oracle Audit Vault and Database Firewall operations.

Note:

Audit Vault and Database Firewall does not accept user names with quotation marks. For example, "jsmith" would not be a valid user name for an Oracle Audit Vault and Database Firewall user account, or an account created on a secured target for use by Oracle Audit Vault and Database Firewall.

13.3.2 Creating Administrative Accounts for the Audit Vault Server

Audit Vault Server super administrators can create both super administrator and administrator user accounts.

To create an administrative account in the Audit Vault Server:

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

The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.

3. Click **Create**.
4. Enter the **User Name** and **Password**, and re-type the password in the appropriate fields.

Note:

Oracle Audit Vault and Database Firewall does not accept user names with quotation marks, such as "jsmith".

5. In the **Type** drop-down list, select **Admin** or **Super Admin**.
6. Click **Save**.

The new user is listed in the Manage Admins page.

See Also:

[About Oracle Audit Vault and Database Firewall Administrative Accounts](#) (page 13-1) for explanation on roles.

13.3.3 Viewing the Status of Administrator User Accounts

As a super administrator, you can view the status of administrator accounts by clicking the **Settings** tab. The Manage Admins page lists all administrator and super administrator accounts, their status, and password expiry dates.

13.3.4 Changing a User Account Type for the Audit Vault Server

You can change an administrative account type from administrator to super administrator, or vice versa.

Note that if you change a user's account type from administrator to super administrator, that user will have access to all secured targets and secured target groups.

To change a user account type in Oracle AVDF:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.
The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.
3. Click the name of the user account you want to change.
4. In the Modify Admin page, in the **Type** section, click **Change**.
5. In the **Type** drop-down list, select the new administrator type.
6. If you changed the type from **Super Admin** to **Admin**, grant or revoke access to any secured targets or groups as necessary for this user:
 - a. Select the secured targets or groups to which you want to grant or revoke access.
 - b. Click **Grant Access** or **Revoke Access**.
A check mark indicates access granted. An X indicates access revoked.
 - c. Repeat steps a and b if necessary.
7. Click **Save**.

13.3.5 Unlocking a User Account

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.

To unlock an administrator account in Oracle Audit Vault and Database Firewall:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab.
The Manage Admins page appears by default, and displays existing users.
3. Click the name of the user account you want to unlock.
4. In the Modify Admin page, click **Unlock**.

 **See Also:**

[Logging in to the Audit Vault Server Console UI \(page 1-11\)](#)

13.3.6 Deleting an Audit Vault Server Administrator Account

To delete an Audit Vault Server administrator user account:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.
The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.
3. Select the users you want to delete, and then click **Delete**.

13.4 Configuring sudo Access for Users

Topics

- [About Configuring sudo Access \(page 13-5\)](#)
- [Configuring sudo Access for a User \(page 13-5\)](#)

13.4.1 About Configuring sudo Access

The `sudo` command enables a trusted user to have administrative access to a system without having to log in using the `root` user password.

When users have been given `sudo` access, they can precede an administrative command with `sudo`, and then be prompted to enter their password. Once authenticated, and assuming that the command is permitted, the command is executed as if it had been run by the `root` user.

13.4.2 Configuring sudo Access for a User

You must have `root` privileges to configure `sudo` access for a user.

1. Log in to the system as the `root` user.
2. Create a normal user account using the `useradd` command.

For example, to create a normal user account for the user `psmith`:

```
# useradd 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`.

13.5 Managing User Access Rights to Secured Targets or Groups

Topics

- [About Managing User Access Rights](#) (page 13-7)
- [Controlling Access Rights by User](#) (page 13-7)
- [Controlling Access Rights by Secured Target or Group](#) (page 13-7)

13.5.1 About Managing User Access Rights

Super administrators have access to all secured targets and secured target groups, and can grant access to specific targets and groups to administrators.

You can control access to secured targets or groups in two ways:

- Modify a secured target or group to grant or revoke access for one or more users.
- Modify a user account to grant or revoke access to one or more secured targets or groups.

13.5.2 Controlling Access Rights by User

To control which secured targets or groups are accessible by a user:

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

The Manage Admins page appears by default, and displays existing users and the secured targets or groups to which they have access.

3. Click the name of the user account you want to modify.

The Modify Admin page appears.

4. In the Targets and Groups section, select the secured targets or secured target groups to which you want to grant or revoke access for this user.

5. Click **Grant Access** or **Revoke Access**.

A check mark indicates access granted. An "x" indicates access revoked.

6. If necessary, repeat steps 4 and 5.
7. Click **Save**.

13.5.3 Controlling Access Rights by Secured Target or Group

To control which users have access to a secured target or group:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **Manage Access Rights**.
3. Click the name of the secured target or secured target group for which you want to define access rights.

The Modify Access for... page appears, listing user access rights to this secured target or group. Super administrators have access by default.

4. In the Modify Access page, select the users for which you want to grant or revoke access to this secured target or group.
5. Click **Grant Access** or **Revoke Access**.
A check mark indicates access granted. An "x" indicates access revoked.
6. If necessary, repeat steps 4 and 5.
7. Click **Save**.

13.6 Changing User Passwords in Oracle Audit Vault and Database Firewall

Topics

- [Password Requirements](#) (page 13-8)
- [Changing the Audit Vault Server Administrator User Password](#) (page 13-9)
- [Changing the Database Firewall Administrator Password](#) (page 13-9)

13.6.1 Password Requirements

You should have a policy in place for changing passwords for the Audit Vault and Database Firewall user accounts. For example, you may require that users change their passwords on a regular basis, such as every 120 days, and that they create passwords that are not easily guessed.

Requirements for Passwords Containing Unicode Characters

If your password contains unicode characters (such as non-English characters with accent marks), 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, 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 word (such as welcome, account, database, and user).
- Not contain any repeating characters.

13.6.2 Changing the Audit Vault Server Administrator User Password

When your Oracle Audit Vault and Database Firewall user passwords expires, you will be prompted to create a new one. However, you can change your password at any time.

Changing Your Own Password

To change your Audit Vault Server user password:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and then click **Change Password**.
3. Type your **Current Password**, **New Password**, and then re-type the new password in the appropriate fields.
Ensure that the password is a custom password.
4. Click **Save**.

Changing the Password of Another Administrator

If you are a super administrator, you can change the password of administrators.

To change the password of another administrator:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab.
3. In the Manage Admins page, click the name of the administrator.
4. In the Change Password section, fill the **New Password** and **Re-enter New Password** fields, and then click **Save**.
Ensure that the password is a custom password.



See Also:

[Password Requirements](#) (page 13-8)

13.6.3 Changing the Database Firewall Administrator Password

To change the Database Firewall administrator Password:

1. Log in to the Database Firewall.
2. In the **Users** menu, click **List**.
3. In the Users List, click the user name whose password you want to change.
4. Enter and confirm your new password in the **Password** and **Password Confirmation** fields.

Ensure that the password is a custom password.

5. In the **User Password** field, enter your old password (the one you are changing).
6. Click **Save**.

 **See Also:**

- [Logging in to the Database Firewall Console UI](#) (page 1-13)
- [Password Requirements](#) (page 13-8)

14

Managing the Audit Vault Server and Database Firewalls

This section describes managing day-to-day Audit Vault Server and Database Firewall operations once the initial configuration is completed.

Topics

- [Managing Audit Vault Server Settings, Status, and Maintenance Operations](#) (page 14-1)
- [Changing the Audit Vault Server's Network or Services Configuration](#) (page 14-6)
- [Managing Server Connectors for Email, Syslog, and Arcsight SIEM](#) (page 14-6)
- [Archiving and Retrieving Audit Data](#) (page 14-7)
- [Managing Repository Encryption](#) (page 14-9)
- [Backing Up and Restoring the Audit Vault Server](#) (page 14-14)
- [Enabling Oracle Database In-Memory for the Audit Vault Server](#) (page 14-26)
- [Managing Plug-ins](#) (page 14-29)
- [Monitoring Server Tablespace Space Usage](#) (page 14-29)
- [Monitoring Server Archive Log Disk Space Use](#) (page 14-29)
- [Monitoring Server Flash Recovery Area](#) (page 14-30)
- [Monitoring Jobs](#) (page 14-31)
- [Scheduling Maintenance Job](#) (page 14-31)
- [Downloading and Using the AVCLI Command Line Interface](#) (page 14-32)
- [Downloading the Oracle Audit Vault and Database Firewall SDK](#) (page 14-38)
- [Managing Database Firewalls](#) (page 14-38)

14.1 Managing Audit Vault Server Settings, Status, and Maintenance Operations

Topics

- [Checking Server Status and System Operation](#) (page 14-2)
- [Running Diagnostics Checks for the Audit Vault Server](#) (page 14-2)
- [Downloading Detailed Diagnostics Reports for the Audit Vault Server](#) (page 14-3)
- [Accessing the Audit Vault Server Certificate and Public Key](#) (page 14-4)
- [Changing Logging Levels and Clearing Diagnostic Logs](#) (page 14-5)
- [Changing the Keyboard Layout](#) (page 14-6)

- [Rebooting or Powering Off the Audit Vault Server](#) (page 14-6)

14.1.1 Checking Server Status and System Operation

To check the Audit Vault Server status:

1. Log in to the Audit Vault Server as an Administrator.
2. Click the **Settings** tab.
3. In the **System** menu, click **Status**.

The status page displays the following:

- Uptime and free space
- High availability status (whether the server is standalone or paired)
- Software and component versions
- Server connect string
- Status for Database Firewall log collector process and background worker process

14.1.2 Running Diagnostics Checks for the 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.

To run 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. In the Diagnostics page, click the **Run Diagnostics** button to perform a series of diagnostic checks.

These diagnostics include testing the existence of the following:

- Existence and access permissions of configuration files
- File system sanity
- Network configuration
- Status of various process that are required to run on the system, for example, database server process(es), event collection process, Java framework process, HTTP server process, etc.

After the system completes the diagnostic tests, it displays a report listing the results of each test.

4. Click the **Back** button to return to the Diagnostics page.

 **See Also:**

- [Viewing the Status and Diagnostics Report for a Database Firewall](#) (page 4-12) if you need to view diagnostic information for an individual Database Firewall.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.1.3 Downloading Detailed Diagnostics Reports for the Audit Vault Server

When you need to debug the Audit Vault Server appliance, you can generate and download a detailed diagnostics report that captures a wide range of information such as ports that are used in the overall configuration, configuration settings, and so on.

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`.

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**.

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.

5. If you are trying to diagnose problems and had set the `LOGLEVEL` to `DEBUG`, consider setting it back to `ERROR` or the original setting (such as `INFO`). Otherwise, in subsequent diagnostic tests, many log or trace files are generated.

 **See Also:**

- [ALTER SYSTEM SET](#) (page A-56) for details about setting the `LOGLEVEL` parameter.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.1.4 Accessing the Audit Vault Server Certificate and Public Key

Topics

- [Accessing the Server Certificate](#) (page 14-4)
- [Accessing the Server Public Key](#) (page 14-4)

14.1.4.1 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.

To access the server certificate:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Settings** tab.
3. In the **Security** menu, click **Certificate**. The server's certificate is displayed. You can copy the certificate and provide it to each Database Firewall.

 **See Also:**

- [Specifying the Audit Vault Server Certificate and IP Address](#) (page 4-6)
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.1.4.2 Accessing the Server Public Key

You must provide the server's public key to another system in order to upload archive files from the Audit Vault Server to that system. This public key must be added to the `authorized_keys` file for that system. For a typical linux installation, this file is in the user's home directory under `.ssh`, and its permissions must be set to 0600, or even 0400.

To access the server public key:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Settings** tab.
3. In the **Archiving** menu, click **Manage Archive Locations**, and then click **Create**. The **Public Key** field contains the public key. You can copy the key and paste it into the appropriate file on another system.



See Also:

[Logging in to the Audit Vault Server Console UI \(page 1-11\)](#)

14.1.5 Changing Logging Levels and Clearing Diagnostic Logs

You can set different logging levels for these system components:

Table 14-1 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

Different logging levels provide more or less information in system logs and affect the size of those logs. 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.

Setting or Changing Logging Levels

To set logging levels:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab, and then under the System menu, click **Diagnostics**.
3. For any of the components listed, select a logging level from the drop-down list.
4. Click **Save**.

Clearing Diagnostic Logs

To clear diagnostic logs from the Audit Vault Server:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab, and then under the System menu, click **Log Management**.

3. Click **Clear Diagnostic Logs**, then click **OK** to confirm.
A confirmation message is displayed when logs have been cleared.

**See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.1.6 Changing the Keyboard Layout

To change the keyboard layout used in the Audit Vault Server:

1. Log in to the Audit Vault Server console as a super Administrator.
2. Click the **Settings** tab, and in the **System** menu, click **Manage**.
3. From the **Keyboard** drop-down list, select the keyboard you want.
4. Click **Save**.

**See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.1.7 Rebooting or Powering Off the Audit Vault Server

To reboot or power off the Audit Vault Server:

1. Log in to the Audit Vault Server as super Administrator.
2. Click the **Settings** tab, and in the **System** menu, click **Manage**.
3. Click **Reboot** or **Power Off**.

14.2 Changing the Audit Vault Server's Network or Services Configuration

To set or change the network or services configuration, follow the relevant procedure below:

- ["Setting or Changing the Audit Vault Server Network Configuration](#) (page 3-5)"
- ["Configuring or Changing the Oracle Audit Vault Server Services](#) (page 3-7)"

14.3 Managing Server Connectors for Email, Syslog, and Arcsight SIEM

To set or change connector information, follow the relevant procedure below:

- [Configuring the Email Notification Service](#) (page 3-10)

- [Configuring Oracle Audit Vault Server Syslog Destinations](#) (page 3-8)
- [Enabling the HP ArcSight SIEM Integration](#) (page 10-2)

**Note:**

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

14.4 Archiving and Retrieving Audit Data

Topics

- [Starting an Archive Job](#) (page 14-7)
- [Retrieving Oracle Audit Vault and Database Firewall Audit Data](#) (page 14-8)

14.4.1 Starting an Archive Job

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. Otherwise the data file copying may fail. Be aware that transferring large files using SCP or SMB may take a long time.

**Note:**

You can register a remote filesystem using the AVCLI utility, so that the filesystem can be selected here. See [REGISTER REMOTE FILESYSTEM](#) (page A-53) for details.

To start an archive job:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and from the **Archiving** menu, click **Archive**.
3. Complete the following fields:
 - **Job Name:** Enter a name for the archive job.
 - **Archive Location:** Select the archive location.

4. Select the files you want to archive.

The files listed are those for which the Months Online period has expired according to the secured target's retention policy.

5. Click the **Archive** button.

 **Note:**

- [Monitoring Jobs](#) (page 14-31) to view the progress of an archive job from the **Jobs** page > **System** menu > **Settings** tab.
- [Defining Archive Locations](#) (page 3-13) to create archiving locations.
- [About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall](#) (page 3-12)

14.4.2 Retrieving Oracle Audit Vault and Database Firewall Audit Data

You can retrieve data files for a specific secured target and time range. The **Months Archived** value in a secured targets retention (archiving) policy determines how long the secured target's data is available to 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.

To retrieve data files from an archive:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab, and from the **Archiving** menu, click **Retrieve**.
3. In the **Job Name** field, enter a name for this retrieve job.
4. Select the **Secured Target** whose data you want to retrieve, and a **Start Date** and **End Date** for the data to be retrieved.

The start and end dates are associated with the event time (the time the event occurred).

5. Click the **Retrieve** button.

You can check the status of the retrieve job in the **Jobs** page (from the **System** menu in the **Settings** tab). When the retrieved data files are available, they are listed in the retrieved data files section of the **Retrieve From Archive** page, and the data will be visible in reports.

6. To purge retrieved files when no longer needed, from the retrieved data files section of the page, select the files you want to unload from the system, and then click the **Release** button. Once the release is successful, the data is not visible in reports.
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.

 **See Also:**

- [Creating Archiving \(Retention\) Policies](#) (page 3-17)
- [About Archiving And Retrieving Data In Oracle Audit Vault And Database Firewall](#) (page 3-12)

14.5 Managing Repository Encryption

Topics

- [About Oracle Audit Vault Server Repository Encryption](#) (page 14-9)
- [Rotating the Master Key for Repository Encryption](#) (page 14-9)
- [Changing the Keystore Password](#) (page 14-9)
- [Backing Up the TDE Wallet](#) (page 14-10)
- [Data Encryption on Upgraded Instances](#) (page 14-10)

14.5.1 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 12.2. 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.

14.5.2 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, and then in the **Storage** menu, click **Repository Encryption**.
3. In the Rotate Master Key section, enter the **Keystore Password**.
This password is originally set as a required post-installation step.
4. Click **Re-key**. A success message is displayed when the re-key is complete.

14.5.3 Changing 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.

To change the Event Repository Encryption password:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab, and then in the **Storage** menu, click **Repository Encryption**.
3. In the Change Keystore Password section, enter the old **Password**, and then enter the **New Password** twice.
4. Click **Change Password**.

See Also:

- [Backing Up and Restoring the Audit Vault Server](#) (page 14-14) for more information on using the keystore password to restore the Audit Vault Server from backup files.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.5.4 Backing Up the TDE Wallet

It is important to perform regular backups of the Audit Vault Server, which include the TDE wallet. However, if you cannot back up the 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.

14.5.5 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.

- Execute the following command to start encryption:

```
/usr/local/dbfw/bin/avdf_data_encryption.sh start
```

- 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):
```

- Type **Y** to continue with encryption.
- 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.

- The following message is displayed in the `/var/log/avdf_data_encryption.log` file:

```
Encrypting <tbsp name> Tablespace : % done
```

- 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
```

- 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
```

- 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.

- 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.
- In case the **dbfwdb** service terminates unexpectedly, contact Oracle Support. The encryption script will not run if this service is down.
- The encryption process collects all the logs to `/var/log/avdf_data_encryption.log` file securely.
- 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.
- 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.
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.

14.6 Backing Up and Restoring the Audit Vault Server

Topics

- [About the Backup and Restore Utility](#) (page 14-14)
- [How Much Space Do I Need for Backup Files?](#) (page 14-16)
- [Backing Up the Audit Vault Server](#) (page 14-16)
- [Restoring the Audit Vault Server](#) (page 14-22)

14.6.1 About the Backup and Restore Utility

The Oracle Audit Vault Server backup utility backs up all Oracle Audit Vault Server data as well as configuration settings.

You can perform full backups as well as incremental backups, which contain only new data and configuration changes since the previous hot backup. For example, you might do full backups on Sundays, then do incremental backups on Mondays, Wednesdays, and Fridays.

The backup utility can perform hot or cold backups. A hot backup runs while Oracle Audit Vault Server is up and running. A cold backup shuts down Oracle Audit Vault Server before running.

You can store the backup files on the Audit Vault Server, but it is better to store them in a remote location, such as an NFS file system, in case the Audit Vault Server computer fails. The location of the backup files should be accessible by the Audit Vault Server.

The restore utility lets you restore the data and configuration to a new Audit Vault Server from backup files. The computer on which you do a restore must have the same version of Oracle Audit Vault and Database Firewall as the computer from which you took the backups.

 **Note:**

- The user must note to have the same path of the backup while performing restore operation. For example, if the backup directory is `/usr/local/backup`, then while performing restore operation specify `/usr/local/backup`, as the backup directory.
- The Database Firewall does not need to be backed up. The Audit Vault Server can reapply all existing Enforcement Point configuration to the Database Firewall. See [Restore Enforcement Points](#) (page 14-42) for more information.
- The backup functionality does not backup archived files. The data files in the archive location are not backed up by `avbackup` as 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 setup as before.
- 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.
- The restore operation takes time to complete. It depends on the amount of data being restored. In case the restore operation is being performed using *SSH* or *Terminus*, the connection may drop if there is no user interaction. Ensure to keep the *SSH* or *Terminus* alive.

How Backup and Restore Operations Work in a High Availability Configuration

If you are using a high availability configuration, then be aware that Oracle Audit Vault and Database Firewall performs the backup only on the primary server, not the secondary server. When you perform a restore operation from the high availability primary backup, then the final restored system becomes a standalone server, which is not in high availability configuration.

Repository Encryption and Backup Encryption

If you did a full install of Oracle Audit Vault and Database Firewall (as opposed to an upgrade), the stored data in the Audit Vault Server is automatically encrypted using Oracle Database Transparent Data Encryption (TDE). This feature is not available on upgraded systems.

If you are restoring from backup files where the system backed up had TDE enabled, you will be prompted for the TDE keystore password during the restore. You must use the TDE keystore password that was in place when the backup was taken. Since the TDE keystore password may change after a backup, it is important that you keep track of the keystore password in place at the time you do each backup.

In addition, you can set encryption on backup files regardless of whether you have the TDE feature available. In this case, you will need a backup encryption password, which will be required if you do a restore.

Therefore, you may need to provide up to two passwords when doing a restore.

 **See Also:**

- [Managing Repository Encryption](#) (page 14-9) for more information on TDE.
- [Configuring High Availability](#) (page 8-1) for information about configuring high availability for Oracle Audit Vault and Database Firewall.

14.6.2 How Much Space Do I Need for Backup Files?

Determine the amount of space you need for backup files.

The amount of space needed for backup files is determined by the size of your Oracle Audit Vault Server database. 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_FILES1
```

 **Note:**

- Ensure that the RAM size and Disk size in the new system is equal or greater than the original system. This ensures that `out of memory` error is not encountered while performing the backup and restore task.
- 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.

14.6.3 Backing Up the Audit Vault Server

Topics

- [Step 1: Configure the Backup Utility](#) (page 14-16)
- [Step 2: Back Up the Audit Vault Server](#) (page 14-20)
- [Step 3: Validate the Backup](#) (page 14-21)

14.6.3.1 Step 1: Configure the Backup Utility

To configure the backup utility:

1. If you are using a high availability configuration and want to perform a cold backup, then do the following:

¹ In this guide, 1 GB represents 2 to the 30th power bytes or in decimal notation 1,073,741,824 bytes.

- a. Log in to the Audit Vault Server console.
 - b. Select **Settings**.
 - c. Under **System**, select **High Availability**.
 - d. Select the **Disable Failover** button.
 - e. In the Confirmation dialog, click **OK**.
2. Log in to the Audit Vault Server as `root`.
 3. Run the command below and input information when prompted:

```
/var/lib/oracle/dbfw/bin/avbackup config
```

The system prompts you for the following:

```
BACKUP_DIR
```

This prompt specifies the directory where the backup files are stored. The directory name is limited to 200 character. After you specify this directory, do not change this directory path, because Oracle Recovery Manager (RMAN) tracks the backup files in this directory. Files are written to this directory by the Oracle user `. All access to this directory is handled by the user oracle. (The user oracle is in the oinstall group.) Oracle automatically uses this directory path during the restore operation.`

This directory should be accessible by the Audit Vault Server, and owned by `oracle:oinstall`. This value should never change once set, and must be the same whether you are doing a full or an incremental backup.

Do not put closed backups and online backups in the same `BACKUP_DIR` location. Follow these guidelines:

- Place the online incremental 1 backup on top of the online full (incremental 0) backup in the same `BACKUP_DIR` directory. Alternatively, you can place a closed incremental 1 backup on top of a closed incremental 0 backup in the same `BACKUP_DIR` directory.
- Do not place a closed incremental 1 backup on top of an online incremental 0 backup in the same `BACKUP_DIR` directory, nor an online incremental 1 backup on top of a closed incremental 0 backup in the same `BACKUP_DIR` directory. Doing so cause the restore operation of these backup files to fail.

The same directory path will be used automatically during the restore operation. This backup destination must be a mounted file system with enough free space to hold the backup files. This may be an NFS file system (to mount this, see "[Remote File System AVCLI Commands](#) (page A-53)"), but not a SAN storage location.

For example:

```
BACKUP_DIR[/backup]:/AVBACKUP
```

```
TMP_DIR
```

This directory is a temporary working parent directory where the work directory is created. This directory must have at least 100 MB of free space. The `oracle` user must have read-write access to `TMP_DIR`.

For example:

```
TMP_DIR[/tmp]:/usr/local/dbfw/tmp/BCKTMP
```

```
KEEP_LOGS
```

This setting determines where the log files are kept after a successful backup operation. Log files are always kept after a failure. Enter **YES** to retain logs upon successful backup or restore. Enter **NO** to automatically delete logs after successful backup or restore.

For example:

```
KEEP_LOGS[NO]:yes
```

```
INCREMENTAL_STRATEGY
```

This setting selects the RMAN incremental backup level. Enter **0** to do a full backup. Enter **1** to do an incremental backup. An incremental backup backs up the changes since the previous backup.

For example:

```
INCREMENTAL[0]:0
```

```
BACKUP_TYPE
```

This setting specifies the type of backup to perform. Enter **HOT** or **COLD**. A hot backup runs while the Audit Vault Server database is running. However, archive log mode must be enabled during the hot backup process. If archive log mode is not enabled, then you must shut down the database to turn on archive log mode, and then restart the database. The operation to turn on archive log mode is quick, but a shutdown and restart must be performed. For a cold backup, the Audit Vault server database is shut down during the backup process. You should schedule a maintenance shutdown before you perform a cold backup.

For example:

```
BACKUP_TYPE[HOT]:COLD
```

```
PASSWD
```

(Optional) This setting sets an encryption password for the backup files. You will need this password when you restore from backup files. Unlike other parameters, the password parameter cannot be automatically retrieved from the backup. If you omit this setting, then the backup files are not encrypted.

For example:

```
PASSWD[-- not set --]: password  
Confirm password: password
```

```
MAXPIECESIZE
```

This setting specifies the maximum backup file size. The valid maximum file size depends on the actual file system. This is set only if **CHANNEL_PARALLELISM** is set to **1**.

For example:

```
MAXPIECESIZE[2G]:
```

```
CHANNEL_PARALLELISM
```

This setting specifies the number of channels (processes) used in executing commands. It should match the number of devices accessed.

If parallelism is more than 1, then the user is prompted for location and section size. If parallelism is equal to 1, then the user is prompted for `MAXPIECESIZE`.

For example: One for each physical disk.

If the number of channels is larger than 1, then specify the location for each channel and section size next.

```
CHANNEL_PARALLELISM[1]:4
```

Best Practice:

In case there are multiple physical disks, then it is advised to set `CHANNEL_PARALLELISM` to an appropriate value according to the number of physical disks. To backup large databases, set `CHANNEL_PARALLELISM` and `SECTION_SIZE` according to the actual physical disks setup to improve the time needed to backup the system.

```
CHANNEL_LOCATION
```

Specifies the location for channel. The user can set multiple locations for each channel. All locations can be the same for all channels. The location is the full path for backup files. To improve performance, the user must specify different locations on a different physical hard disk. The user may specify all locations to the same path.

For example:

```
CHANNEL_LOCATION_1[:]/disk_1  
CHANNEL_LOCATION_2[:]/disk_2  
CHANNEL_LOCATION_3[:]/disk_3  
CHANNEL_LOCATION_4[:]/disk_4
```

```
SECTION_SIZE
```

The section size is smaller than the largest data file or parallelism and smaller than the size the physical disk can handle.

For example:

```
SECTION_SIZE[:]32G
```

```
USE_NEW_IP
```

For restore operation it specifies the new (current) IP address of the restore system, instead of the old IP address from the backup system. The allowed values are `Y` or `N`.

```
USE_NEW_IP[N]:Y
```

```
REDUNDANCY
```

This setting specifies a number that sets how many full backups to keep. When you run the `backup` command, backups that are older than this number of backups (as well as their related incremental backups) are deleted. More redundancy requires more disk space for the backup, specified in the `BACKUP_DIR` parameter.

For example:

```
REDUNDANCY[1]:
```

After you complete these settings, a summary of your selection is displayed similar to the following:

```
BACKUP_DIR=/
long_backup_directory_name_so_three_times_is_more_than_two_hundred_c
hars
TMP_DIR=/tmp
KEEP_LOGS=NO
INCREMENTAL=0
BACKUP_TYPE=HOT
PASSWD=-- not set --
CHANNEL_PARALLELISM=3
CHANNEL_LOCATION=/
long_backup_directory_name_so_three_times_is_more_than_two_hundred_c
hars /
long_backup_directory_name_so_three_times_is_more_than_two_hundred_c
hars /
long_backup_directory_name_so_three_times_is_more_than_two_hundred_c
hars
SECTION_SIZE=500M
REDUNDANCY=1
USE_NEW_IP=Y
```

If you changed the archivelog mode during the backup configuration process, after the database restarts, then ensure that the Java Framework internal tool is running on the Audit Vault Server.

For example:

```
/usr/local/dbfw/bin/javafwk status
```

If the output is `Java framework process is stopped`, then restart it as follows:

```
/usr/local/dbfw/bin/javafwk start
```

14.6.3.2 Step 2: Back Up the Audit Vault Server

This step backs up the Audit Vault Server database and configuration.

1. If applicable, ensure you have the backup file encryption password and/or event repository encryption (keystore) password.

 **See Also:**

[Repository Encryption and Backup Encryption](#) (page 14-15)

2. Log in to the Audit Vault Server as `root`.
3. Run the following command and input information at the prompts:

```
/var/lib/oracle/dbfw/bin/avbackup backup
```

When the backup is complete, you should see a number of files in your backup directory, similar to the following:

```
DBID_1440353975_09Q7EF7L_1_1  
DBID_1440353975_C-1440353975-20150520-00
```

 **Note:**

Oracle recommends the user to reboot the system in case there is a failure while performing a cold backup operation.

14.6.3.3 Step 3: Validate the Backup

This step validates the backup. It performs the `validate` operation on the last backup that you created, regardless the settings of the `avbackup config` file.

 **Note:**

The backup configuration file is release specific. It works only for the same release. It is advisable to execute the `avbackup config` command and create a new configuration file before performing the backup operation after every upgrade.

1. Log in to the Audit Vault Server as `root`.
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. Check these 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
```

If you need help diagnosing errors, contact Oracle Support.

The location of closed backup and online backup must be different. Do not use the same `BACKUP_DIR` location. Once you specify this location, it is advisable not to change the directory path as **Oracle Recovery Manager (RMAN)** tracks the backup files in this directory.

 **Note:**

If you use *avbackup* to do regular backup, or setup cron job for full and incremental backup, or using your own script to perform a backup operation, then:

- The *avbackup* tool performs a back up of the database and the configuration of Oracle Audit Vault and Database Firewall.
- RMAN backup is only backing up the Oracle Audit Vault and Database Firewall database. RMAN plays a crucial role in the archive, backup, and upgrade processes. The default RMAN settings of the Audit Vault Server must not be altered.
- For RMAN only backup, in the event of a system crash, you cannot restore on a new system. The backup does not work as the original configuration is missing.
- The backup strategy with RMAN works only in the event of the database crash and the system is still running.

To resolve this issue of *avbackup* configuration execute the following commands. These commands are example only and work for the cron job setup. However, any issues resulting out of this is not supported by Oracle.

Task	Procedure
To run the <i>avbackup</i> configuration once for the full backup.	Move <code>/var/lib/oracle/dbfw/av/backup/.backup_restore_config</code> to <code>/var/lib/oracle/dbfw/av/backup/.full_backup_restore_config</code>
To run the <i>avbackup</i> configuration once for the full incremental backup.	Move <code>/var/lib/oracle/dbfw/av/backup/.backup_restore_config</code> to <code>/var/lib/oracle/dbfw/av/backup/.incr_backup_restore_config</code>
To setup one cron job for full backup.	Copy <code>full_backup_restore_config</code> to <code>backup_restore_config</code> . Run the command <code>avbackup backup</code> .
To setup one cron job for incremental backup.	Copy <code>incr_backup_restore_config</code> to <code>backup_restore_config</code> . Run the command <code>avbackup backup</code> .

14.6.4 Restoring the Audit Vault Server

Topics

- [About Restoring the Audit Vault Server](#) (page 14-23)
- [Prerequisites for Restoring Audit Vault Server](#) (page 14-23)
- [Step 1: Configure the Backup Utility on the Audit Vault Server](#) (page 14-24)
- [Step 2: Restore Audit Vault Server](#) (page 14-24)

14.6.4.1 About Restoring the Audit Vault Server

The following actions take place after you restore the contents of the Audit Vault Server:

- All database accounts are replaced by the accounts from the earlier system. After the restore process, you can modify these accounts as needed.
- The keystore password is replaced by the keystore password that was used in the earlier system. After the restore process is complete, you can modify the keystore password as needed.
- Operating system accounts are not affected by the restore process. Therefore, the passwords that you set for the `root` and `support` accounts remain the same as before the restore.

14.6.4.2 Prerequisites for Restoring Audit Vault Server

Examine the prerequisites for restoring Audit Vault Server.

Before restoring backup files to a new Audit Vault Server:

- Shut down and remove the earlier Audit Vault Server from the subnet on which it resides. This task enables the new Audit Vault Server to be restored on the same subnet as the previous server.
- Perform full installation of the same release version of Oracle AVDF, including the post-installation tasks, on the system to which you are restoring. See *Oracle Audit Vault and Database Firewall Installation Guide* for instructions.
- Ensure that the new Audit Vault Server is on the same subnet as the Audit Vault Server from which you took the backups.
- Ensure that the new Audit Vault Server has a different IP address than the Audit Vault Server from which you took the backups.

Note:

- After you complete the restore process, the IP address of the new Audit Vault Server is automatically changed to the IP address of the old system. If you want to restore the system with the IP address of the old system (prior to backup), ensure the new Audit Vault Server is on the same subnet as the Audit Vault Server from which you took the backup. Set the `USE_NEW_IP` parameter to `N` while executing the `avbackup config` command on the restore system. For this case, if the original system is still up and running, the restore fails because it cannot switch the IP address which is in use.
- If you plan to restore the system to a new IP, not to the original backed up system IP, make sure you set `USE_NEW_IP` parameter to `Y` while executing the `avbackup config` command on the restore system. In this case, you do not need to restore on the same subnet as the backup system. You may use this configuration when you are restoring on a different data center, which is on a different subnet, or restore the backup on a new IP while the backup system is up and running.

14.6.4.3 Step 1: Configure the Backup Utility on the Audit Vault Server

To restore the new Audit Vault Server from backup files, first you configure the backup utility on the new Audit Vault Server.

Follow the same procedure as in "[Step 1: Configure the Backup Utility](#) (page 14-16)", providing the same values for `BACKUP_DIR` and `PASSWD` as you did on the backed up system.

14.6.4.4 Step 2: Restore Audit Vault Server

Learn how to restore Audit Vault Server.

To restore the Audit Vault Server:

1. Copy the backup files to your new Audit Vault Server, placing the files in the `BACKUP_DIR` directory that you specified in "[Step 1: Configure the Backup Utility on the Audit Vault Server](#) (page 14-24)".

Make sure the backup files are owned by `oracle:oinstall`.

2. Log in to Audit Vault Server as root.
3. In case the backup files are in NFS, then ensure the NFS location is mounted on the system used for restore. The backup directory must be accessible through the mount point. Run the following command to manually mount the NFS location prior to performing the restore operation:

```
/bin/mount -t nfs <NFS server IP>:<NFS export> <mount point of  
Audit Vault Server>
```

4. Run the following command:

```
/var/lib/oracle/dbfw/bin/avbackup restore
```

5. If you have TDE enabled, then when prompted, then enter the keystore password, using the same value for the keystore password for the original system.

For example:

```
Enter keystore password:
```

If TDE is not enabled, then this step is bypassed.

6. When restore is complete, 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
```

Common errors and their solutions are as follows:

- **No access to `BACKUP_DIR`:** Ensure that the `BACKUP_DIR` directory is owned by `oracle:oinstall`.
- **Disk full:** Ensure that the `BACKUP_DIR` disk has enough room for the backup files.

- Incorrect password: Re-run the `avbackup config` command to set the password correctly.
- In addition, a common error is not running the script as root.
- The restore operation takes time to complete. It depends on the amount of data being restored. In case the restore operation is being performed using *SSH* or *Terminus*, the connection may drop if there is no user interaction. Ensure to keep the *SSH* or *Terminus* alive.

14.6.5 Restoring a Backup to a New System with a New or Different IP Address

Learn how to restore a backup to a new system with a new or different IP address.

After performing the restore operation, the system has the same IP address. The user has an option to keep the new IP address without disrupting the service and functionality of the system. If the new IP address is used, the system restores the database and keeps the new IP address. This section contains the necessary steps to be performed after the restore operation so that the system or Audit Vault Server does not retain the original IP address by default.

Follow these steps after the restore operation when the system has a new IP address:

1. Log in to the Audit Vault Server as root user.
2. Restore the backup on a new Audit Vault Server with a new IP address.
3. Update the IP addresses in the `av/conf/bootstrap.prop` files of the Agent deployments. Replace all the old IP address with the new IP address in `bootstrap.prop` file.
4. Restart the Agent. It downloads the new `agent.jar` from the Audit Vault Server with the new IP address.

 **Note:**

Execute this operation on all Audit Vault Agents and restart them.

5. Log in to the Database Firewall console as *admin* user.
6. Click **Database Firewall** tab.
7. In the **System** menu, click **Audit Vault Server**.
8. In the **Audit Vault Server 1 IP Address** field, enter the new IP address of the Audit Vault Server.

Result:

This ensures that new communication between Audit Vault Server and Database Firewall is established.

 **Note:**

If this communication is not established, then Oracle Audit Vault Server cannot access Oracle Database Firewall. It may result in a common access issue error or an incomplete restore operation.

9. Update the IP address on all instances of Database Firewall.

 **Note:**

- Upon completion of restore process on a new IP, the console certificate in the backup system is no longer valid or in use. You must generate a new certificate and upload it.
- The restore operation takes time to complete. It depends on the amount of data being restored. In case the restore operation is being performed using *SSH* or *Terminus*, the connection may drop if there is no user interaction. Ensure to keep the *SSH* or *Terminus* alive.

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

Topics

- [About Enabling Oracle Database In-Memory for the Audit Vault Server](#) (page 14-26)
- [Enabling and Allocating Memory for Oracle Database In-Memory](#) (page 14-27)
- [Setting the Oracle Database In-Memory Options](#) (page 14-28)
- [Disabling Oracle Database In-Memory](#) (page 14-28)
- [Monitoring Oracle Database In-Memory Usage](#) (page 14-28)

14.7.1 About Enabling Oracle Database In-Memory for the 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 the 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 secured targets and enforcement points. You can find some guidelines for calculating RAM requirements in the Oracle Audit Vault and Database Firewall Sizing Advice (MOS Doc ID 2223771.1). 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.

14.7.2 Enabling and Allocating Memory for Oracle Database In-Memory

To enable and allocate memory for Oracle Database In-Memory:

1. Log in to the Audit Vault Server console as a super administrator.
2. In the home page, click Oracle Database In-Memory.
Alternatively, click the **Settings** tab, and then click **Oracle Database In-Memory** under the **System** menu.
3. If there is sufficient memory, click the check box **Enable Oracle Database In-Memory**.
The system displays the total available RAM and the maximum available for in-memory.
4. In the Oracle Database In-Memory page, select from the following options to send data to Oracle Database In-Memory:
 - **Date Range:** Enables the memory to be available for a specific period of time.
 - **Keep Latest Data:** Retains the data that has just been collected and enables the system to automatically select the most recent dates, based on the in-memory size that was configured.
5. In the **Allocated for 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 page.
6. Click **Save**.

After enabling or disabling 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.

See Also:

[Logging in to the Audit Vault Server Console UI \(page 1-11\)](#)

14.7.3 Setting the Oracle Database In-Memory Options

After you enable Oracle Database In-Memory, you can choose to have it perform based on a date range or to keep the latest data. This procedure does not restart the database and has no effect on any components such as the agent collectors.

1. Log in to the Audit Vault Server console as a super administrator.
2. In the home page, click Oracle Database In-Memory.
Alternatively, click the **Settings** tab, and then click **Oracle Database In-Memory** under the **System** menu.
3. In the Oracle Database In-Memory page, select from the following options to send data to Oracle Database In-Memory:
 - **Date Range:** Enables the memory to be available for a specific period of time.
 - **Keep Latest Data:** Retains the data that has just been collected and enables the system to automatically select the most recent dates, based on the in-memory size that was configured.
4. Click **Save**.



See Also:

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.7.4 Disabling Oracle Database In-Memory

To disable Oracle Database In-Memory:

1. Log in to the Audit Vault Server console as a super administrator.
2. In the home page, click Oracle Database In-Memory.
Alternatively, click the **Settings** tab, and then click **Oracle Database In-Memory** under the **System** menu.
3. Click the **Enable Oracle Database In-Memory** check box to clear it.
4. Click **Save**.

After enabling or disabling 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.



See Also:

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.7.5 Monitoring Oracle Database In-Memory Usage

To see in-memory usage in the Audit Vault Server dashboard:

1. Log in to the Audit Vault Server console as an *administrator*.
2. In the home page, click Oracle Database In-Memory.
Alternatively, click the **Settings** tab, and then click **Oracle Database In-Memory** under the **System** menu.
3. Note the data next to **Database In-Memory utilization**.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.8 Managing Plug-ins

You can deploy additional plug-ins to support more types of secured targets, or un-deploy plug-ins that are no longer needed.

 **See Also:**

[Deploying Plug-ins and Registering Plug-in Hosts](#) (page 5-13)

14.9 Monitoring Server Tablespace Space Usage

You can monitor server table space usage in Oracle Audit Vault Server.

Oracle Audit Vault Server contains the `SYSAUX` tablespace, which by default has one data file. The `SYSAUX` tablespace is a locally managed tablespace with automatic segment space management.

You should monitor the space usage for the `SYSAUX` tablespace and create additional data files for storage as needed.

 **See Also:**

- *Oracle Database Administrator's Guide* for more information about the `ALTER TABLESPACE` SQL statement, which you can use to add more storage data files.
- *Oracle Database SQL Tuning Guide* for information about optimizing a tablespace.

14.10 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.

 **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.

14.11 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*

14.12 Monitoring Jobs




You can see the status of various jobs that run on the Audit Vault Server, such as report generation, and user entitlement or audit policy retrieval from secured targets.

To see the status of jobs on the Audit Vault Server:

1. Log in to the Audit Vault Server as an Administrator.
2. Click the **Settings** tab.
3. In the **System** menu, click **Jobs**.

A list of jobs is displayed, showing the job type, ID, timestamp, status, and associated user name.

4. To see details for an individual job, click the icon to the left of that job.

	Job Type	Timestamp ▼	Current Status	Message	User Name
	Audit Settings	05/10/2012 09:53:39	Completed		AVAUDITOR1
	Audit Settings	04/10/2012 17:46:45	Completed		AVAUDITOR
	User Entitlement	04/10/2012 17:46:05	Completed		AVAUDITOR

14.13 Scheduling Maintenance Job

There are some jobs on the Audit Vault Server which needs to be scheduled for proper and effective functioning of the system. These jobs should run during a period when the Audit Vault server usage is low. For example, during the night.

The user can schedule these jobs as per their time zone, using this functionality.

To schedule maintenance jobs on the Audit Vault Server, follow this procedure:

1. Log in to the Audit Vault Server as an *administrator*.
2. Click **Settings** tab, and then **Manage**.
3. To schedule a new maintenance job, select **Start Time**. Enter the time in hours and minutes for the maintenance job to start at a specific time. The time specified here is the time on the browser.
4. In the **Time Out (In hours)** field, enter the duration of the maintenance job in hours.

 **Note:**

In case the job does not complete within the duration specified, it is timed out.

5. In the **Repeat Frequency** field, select the frequency of the maintenance job to be repeated.

 **Note:**

This field cannot be edited, and by default the value remains *Daily*. The job runs at the specified start time daily.

 **See Also:**

[Monitoring Jobs](#) in the *Oracle Audit Vault and Database Firewall Administrator's Guide* to check the status of the job scheduled.

14.14 Downloading and Using the AVCLI Command Line Interface

Topics

- [About the AVCLI Command Line Interface](#) (page 14-32)
- [Downloading the AVCLI Command Line Utility and Setting JAVA_HOME](#) (page 14-33)
- [Starting AVCLI](#) (page 14-33)
- [Running AVCLI Scripts](#) (page 14-36)
- [Specifying Log Levels for AVCLI](#) (page 14-37)
- [Displaying Help and the Version Number of AVCLI](#) (page 14-37)

14.14.1 About the AVCLI Command Line Interface

As an alternative to using the Audit Vault Server console (Web) UI, you can use the AVCLI command line interface to manage Oracle Audit Vault and Database Firewall, including registering and configuring secured targets and their connections to the Audit Vault Server.

You can run AVCLI from the Audit Vault Server, or download the AVCLI utility from the Audit Vault Server and install and run the utility on another computer.

The syntax used for AVCLI is similar to SQL*Plus. For example, from within AVCLI, you can use the `CONNECT` command to log in as another user. In addition, the AVCLI commands are not case sensitive. In this manual, the commands are entered in upper case.

 **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](#) (page A-1) for details of the available AVCLI commands.

14.14.2 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.

To download the AVCLI command line utility:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Settings** tab, and in the **System** menu, click **Manage**.
3. Click the **Download Command Line Utility** button, and save the `avcli.jar` file.
4. Copy the `avcli.jar` file to the computer from which you want to run AVCLI, and then run this command:

```
java -jar avcli.jar
```

The AVCLI utility is installed in the current directory with the necessary permissions. To install in a different directory, use the command:

```
java -jar avcli.jar -d directory_name
```

5. Set the `JAVA_HOME` environment variable to point to the JDK installation directory. On Windows, add `%JAVA_HOME%\bin` to the `PATH` environment variable.

**See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.14.3 Starting AVCLI

You can invoke AVCLI interactively (that is, you must provide a password) with or without a user name. You can also start AVCLI by using stored credentials. This section contains instructions for the two methods of starting AVCLI.

Topics

- [Starting AVCLI Interactively](#) (page 14-34)
- [Starting AVCLI Using Stored Credentials](#) (page 14-34)

**Note:**

Set the `JAVA_HOME` environment variable to point to JDK installation directory.

14.14.3.1 Starting AVCLI Interactively

Follow one of the methods below to invoke AVCLI interactively. Except for a few commands where it is optional, all AVCLI commands must end in a semi-colon (;). For simplicity, in this guide we use a semi-colon for all AVCLI commands.

Using Interactive Mode with a User Name

The command syntax for invoking AVCLI with a user name is:

```
avcli -u username
Enter password: password
```

For example:

```
avcli -u psmith
AVCLI : Release 12.2.0.0.0 - Production on timestamp
Copyright (c) 1996, 2015 Oracle. All Rights Reserved.
Enter password for 'psmith': password
```

```
Connected to:
Oracle Audit Vault Server 12.2.0.0.0
```

```
AVCLI>
```

Using Interactive Mode Without a User Name

If you invoke AVCLI without a user name, you must connect to the Audit Vault Server as a valid user who has been granted the `AV_ADMIN` role. The command syntax for invoking AVCLI with a user name is:

```
avcli
AVCLI> CONNECT [username];
```

For example:

```
avcli

AVCLI : Release 12.2.0.0.0 - Production on timestamp
Copyright (c) 1996, 2015 Oracle. All Rights Reserved.

AVCLI> CONNECT psmith
Enter password: password;
Connected.
```

If you do not enter a user name you will be prompted for one.

14.14.3.2 Starting AVCLI Using Stored Credentials

Storing credentials for an Oracle AVDF administrator is useful when you need to run AVCLI scripts without user intervention or without putting credentials in the script.

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.

Storing or Overwriting Administrator Credentials

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.

To store credentials for the designated administrator:

1. As the AVCLI owner, run `avcli` without connecting to the Audit Vault Server. For example:

```
avcli
```

```
AVCLI : Release Release 12.2.0.0.0 - Production on timestamp
Copyright (c) 1996, 2015 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.

Note:

If this administrator's password changes, follow this procedure again to store the new credentials.

Starting AVCLI Using Stored Credentials (Non-Interactively)

To start AVCLI without having to enter credentials, your credentials must be stored, as detailed in the previous procedure.

There are two ways of starting AVCLI using stored credentials:

- **From the shell**

In the Audit Vault Server, enter:

```
avcli /@
```

This command logs you in to AVCLI and connects to the Audit Vault Server.

- **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 12.2.0.0.0 - Production on timestamp
Copyright (c) 1996, 2015 Oracle. All Rights Reserved.

AVCLI> CONNECT /@;
Connected.
```



See Also:

[Running AVCLI Scripts \(page 14-36\)](#)

14.14.4 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 12.2.0.0.0 - Production on timestamp
Copyright (c) 1996, 2015 Oracle. All Rights Reserved.
Enter password for 'psmith': password

Connected to:
Oracle Audit Vault Server 12.2.0.0.0

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.

14.14.5 Specifying Log Levels for AVCLI

When you invoke AVCLI, you can specify the following log levels. 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 12.2.0.0.0 - Production on timestamp
Copyright (c) 1996, 2015 Oracle. All Rights Reserved.
Enter password for 'psmith': password
```

```
Connected to:
Oracle Audit Vault Server 12.2.0.0.0
```

```
AVCLI>
```

To invoke AVCLI using a script and with the `debug warning` level:

```
avcli -l debug -f myscript.av
AVCLI : Release 12.2.0.0.0 - Production on timestamp
Copyright (c) 1996, 2015 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.

14.14.6 Displaying Help and the Version Number of AVCLI

To display the AVCLI help information and version number:

```
avcli -h
```

If you only want to find the version number, then use the `v` argument:

```
avcli -v
```

14.15 Downloading the Oracle Audit Vault and Database Firewall SDK

An SDK is available for developing custom Oracle Audit Vault and Database Firewall plug-ins.

To download the SDK:

1. Log in to the Audit Vault Server console as an *administrator*.
2. Click the **Settings** tab, and then click **Plug-ins** (under the System subsection).
3. Click **Download SDK**.

See Also:

- [Oracle Audit Vault and Database Firewall Installation Guide](#) for developer information.
- [Logging in to the Audit Vault Server Console UI](#) (page 1-11)
- [About Plug-ins](#) (page 5-13)

14.16 Managing Database Firewalls

Topics

- [Changing the Database Firewall's Network or Services Configuration](#) (page 14-38)
- [Viewing Network Traffic in a Database Firewall](#) (page 14-39)
- [Capturing Network Traffic in Oracle Database Firewall](#) (page 14-39)
- [Restarting or Powering Off Oracle Database Firewall](#) (page 14-40)
- [Removing Oracle Database Firewall from Oracle Audit Vault Server](#) (page 14-40)
- [Fetching an Updated Certificate from Oracle Database Firewall](#) (page 14-40)
- [Viewing Diagnostics for Oracle Database Firewall](#) (page 14-41)
- [Resetting Oracle Database Firewall](#) (page 14-41)
- [Restore Enforcement Points](#) (page 14-42)

14.16.1 Changing the Database Firewall's Network or Services Configuration

See one of the topics below if you need to change a Database Firewall's network, traffic sources, or services configuration:

- ["Configuring Network Settings For A Database Firewall](#) (page 4-3)"
- ["Configuring Network Services For A Database Firewall](#) (page 4-4)"

- ["Configuring Traffic Sources \(page 4-9\)"](#)
- ["Configuring a Bridge in the Database Firewall \(page 4-9\)"](#)
- ["Configuring Oracle Database Firewall As A Traffic Proxy \(page 4-11\)"](#)

14.16.2 Viewing Network Traffic in a Database Firewall

You can view network traffic for debugging purposes. You can view live network traffic going through a firewall.

To view live network traffic in a Database Firewall:

1. Log in to the Database Firewall administration console.
2. Under **Network Traffic**, select **Live Capture**.
3. In the **Level of Detail** region, select **Summary** or **Packet Content**.
4. In the **Duration** field, select the number of seconds to capture live traffic.
5. In the **Network** field, select the network traffic source for which to capture traffic.
6. Click the **Show Traffic** button. In the Network traffic (first 1000 packets) region, the live traffic is displayed for the selected duration.

See Also:

[Logging in to the Database Firewall Console UI \(page 1-13\)](#)

14.16.3 Capturing Network Traffic in Oracle Database Firewall

Learn how to capture network traffic in Oracle Database Firewall.

You can capture traffic to a file (.pcap file type) that you can download and analyze.

To capture network traffic to a file:

1. Log in to the Database Firewall administration console.
2. Under **Network Traffic**, select **File Capture**.
3. In the **Duration** field, select the number of seconds to capture traffic.
4. In the **Network** field, select the network traffic source for which to capture traffic.
5. Click the **Capture** button.

The traffic file (.pcap format) is displayed in the Network Traffic Files list.

6. Click **Download** for the network traffic file you want to download.

See Also:

[Logging in to the Database Firewall Console UI \(page 1-13\)](#)

14.16.4 Restarting or Powering Off Oracle Database Firewall

Use this procedure to restart or power off Oracle 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, and then select the firewall(s) you want to reboot or power off.
3. Click the **Reboot** or **Power Off** button.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.16.5 Removing Oracle Database Firewall from Oracle Audit Vault Server

You can remove Oracle Database Firewall from Oracle Audit Vault Server.

To remove Oracle Database Firewall from Oracle Audit Vault Server:

1. Log in to the Audit Vault Server as an *administrator*.
2. Click the **Database Firewalls** tab, and then select the firewall(s) you want to remove.
3. Click the **Delete** button.

 **See Also:**

[Logging in to the Audit Vault Server Console UI](#) (page 1-11)

14.16.6 Fetching an Updated Certificate from Oracle Database Firewall

Learn how to obtain updated certificates from Oracle Database Firewall.

You can update the Database Firewall certificate stored in the Audit Vault Server using the Audit Vault Server console UI. You must update this certificate when you upgrade the Database Firewall to maintain communication between the firewall and the Audit Vault Server.

To update the Database Firewall certificate stored in the Audit Vault Server:

1. After upgrading the Database Firewall, log in to the Audit Vault Server console as an administrator.
2. Click the **Database Firewalls** tab.

A list of firewalls appears.

Firewalls					
<input type="text"/>		<input type="button" value="Go"/>		<input type="button" value="Actions ▾"/>	
<input type="checkbox"/>		Status	Name ▲	IP Address	Added At
<input type="checkbox"/>		Certificate Validation Failed	fw	192.0.2.123	2/16/2014 5:53:28 PM
<input type="checkbox"/>		Primary	fwUpgrade	192.0.2.122	2/17/2014 8:38:19 PM

3. Click the name of a firewall with the status Certificate Validation Failed.
4. In the Modify Firewall page, click **Update Certificate**.

See Also:

[Logging in to the Audit Vault Server Console UI \(page 1-11\)](#)

14.16.7 Viewing Diagnostics for Oracle Database Firewall

See Also:

[Viewing the Status and Diagnostics Report for a Database Firewall \(page 4-12\)](#) for viewing Database Firewall diagnostics.

14.16.8 Resetting Oracle Database Firewall

Learn how to reset Oracle Database Firewall.

This block contains information about the Oracle Database Firewall settings and the details of resetting a Firewall ID. The **Reset ID** button, in the **Reset Database Firewall ID** tab performs a reset of the Firewall ID. The Firewall ID is a unique identification number of the Firewall. It is derived from the Management Network Interface card. Once the reset is performed, it removes the existing enforcement points and creates new ones using the configuration information stored in Audit Vault Server. The enforcement points 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 of the Firewall is not altered. This action also resets the Firewall ID.

 **Note:**

- Whenever the Network Interface Card is replaced, the Firewall ID must be reset.
- The network settings of the Firewall is not altered. Ensure the 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 Network Interface card on the Database Firewall.
2. After replacing an existing and configured Firewall with a newly installed Firewall.

14.16.9 Restore Enforcement Points

When an Audit Vault Server is restored from backup, it is necessary to restore the status of the Enforcement Points registered on the Database Firewall.

 **See Also:**

[Resetting Oracle Database Firewall](#) (page 14-41) for more information.

15

Configuring a SAN Repository

Topics

- [About Configuring a SAN Repository](#) (page 15-1)
- [Configuring a SAN Server to Communicate with Oracle Audit Vault and Database Firewall](#) (page 15-2)
- [Registering or Dropping SAN Servers in the Audit Vault Server](#) (page 15-3)
- [Discovering Targets on a SAN Server](#) (page 15-4)
- [Adding or Dropping SAN Disks in the Audit Vault Server Repository](#) (page 15-6)

15.1 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 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.

15.2 Configuring a SAN Server to Communicate with Oracle Audit Vault and Database Firewall

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:

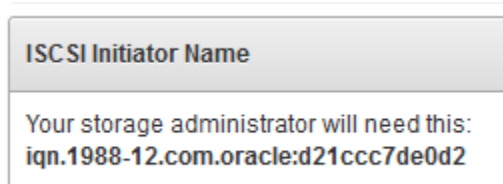
Ensure that you do not have more than one target mapped to the same disk on the SAN storage server.

Some SAN servers may also require the Audit Vault Server's IP address.

To find the Audit Vault Server's iSCSI initiator name and IP address:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.

The SAN Servers page is displayed with the iSCSI initiator name at the bottom.



In a high availability environment, you will see two iSCSI initiator names, one for the primary Audit Vault Server and one for the secondary.

3. To find the Audit Vault Server's IP address, click the **Settings** tab, then click **Network**. The IP address is at the top of this page.



Note:

Do not restart the iSCSI service on either the Audit Vault Server or the SAN server that is servicing the Audit Vault Server. If there is a need to restart either of these services, contact Oracle support.

15.3 Registering or Dropping SAN Servers in the Audit Vault Server

Topics

- [Registering a SAN Server](#) (page 15-3)
- [Dropping a SAN Server](#) (page 15-3)

15.3.1 Registering a SAN Server

This procedure registers a SAN server in the Audit Vault Server. In a high availability environment, you can use this procedure to register a SAN server to the primary or the secondary Audit Vault Server. Note that while you can register the same SAN server to both the primary and secondary Audit Vault Servers, they must not share (read or write to) the same SAN disks.

To register a SAN server in the Audit Vault Server:

1. 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 Audit Vault Server is authenticated by the SAN server.
5. Click **Submit**.

15.3.2 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](#) (page 15-8)
Learn how to drop a SAN disk from a disk group.

15.4 Discovering Targets on a SAN Server

Topics

- [About SAN Targets and Disks](#) (page 15-4)
- [Discovering Targets on a SAN Server and Making Disks Available](#) (page 15-4)
- [Logging Out of Targets on SAN Servers](#) (page 15-5)

15.4.1 About SAN Targets and Disks

Once you have registered SAN servers in the Audit Vault Server, in order to make SAN disks available for storing Audit Vault Server data, you must discover and log in to the available target(s) on the SAN server.

When you log in to a target on the SAN server, a number of storage disks are made available to the Audit Vault Server, corresponding to the number of LUNs available on the SAN server for that target.

15.4.2 Discovering Targets on a SAN Server and Making Disks Available

You can discover targets on a SAN server that is registered with the Audit Vault Server.

To make SAN server disks available for storing Audit Vault Server data, you must log in to a target on the SAN server, and provide login credentials if required.

To discover targets on a SAN server:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **SAN**.
3. Find the SAN server you want, and then click the corresponding **Discover** link.

A list of targets appears, showing the status of each target.

Discovered Targets from testa				
Target Name	IP Address	Port	Status	Action
iqn.2006-01.com.openfiler:tsn.671b295c3fcc	192.0.2.254	3260	In Use	-
iqn.2006-01.com.openfiler:tsn.8fbbe0b0162d	192.0.2.254	3260	Logged In	Log Out
iqn.2006-01.com.openfiler:tsn.a023eebee223	192.0.2.254	3260	Login Required	Log In
iqn.2006-01.com.openfiler:tsn.94cc7bab3dcf	192.0.2.254	3260	Login Required	Log In

1 - 4

- Click **Log In** to log in to a target on this SAN server and make its disks available for storage.

If the SAN server is configured so that the target does not require credentials, you can leave those fields empty and click **Log in**.

See Also:

[Registering a SAN Server](#) (page 15-3)

15.4.3 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 Oracle 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:

- Log in to the Audit Vault Server as a super administrator.
- Click the **Settings** tab, and then click **SAN**.
- Find the SAN server you want, and then click the corresponding **Discover** link.

A list of targets appears, showing the status of each target.

- 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](#) (page 15-8)

15.5 Adding or Dropping SAN Disks in the Audit Vault Server Repository

Topics

- [About Disk Groups in the Audit Vault Server Repository](#) (page 15-6)
- [Adding SAN Disks to the Audit Vault Server Repository](#) (page 15-7)
- [Dropping SAN Disks from the Audit Vault Server Repository](#) (page 15-8)

15.5.1 About Disk Groups in the Audit Vault Server Repository

There are three disk groups used for storing Audit Vault Server data, corresponding to three data types:

- EVENTDATA
- SYSTEMDATA
- RECOVERY

If desired, you can add disks from a registered SAN server to the EVENTDATA, SYSTEMDATA, and RECOVERY disk groups to increase the storage capacity for those types of data. Otherwise, these data types are stored in disk partitions on the Audit Vault Server.

Adding SAN disks to these disk groups is optional.

In a high availability environment: You must ensure that the secondary server has at least the same amount of space in each disk group as the primary server.

[Figure 15-1](#) (page 15-7) shows the **Repository** page, available from the **Settings** menu. In the repository shown here:

- The EVENTDATA disk group uses a SAN disk for extra storage.
- The SYSTEM DATA and RECOVERY disk groups use only the Audit Vault Server disk partitions for storage.
- For the EVENTDATA, SYSTEMDATA, and RECOVERY disk groups, the amount of free space available on the local Audit Vault Server partitions is also shown.

Figure 15-1 The Repository Page

EVENTDATA (22 GB, 10.5% used)					
Drop Disk Add Disk					
Disk Name	IP Address	Port	Capacity	Free	
<input type="radio"/>	DISK10	192.0.2.123	3260	5118MB	4580MB
1 - 1					

SYSTEMDATA (17 GB, 16.5% used)					
Drop Disk Add Disk					
No disk found.					

RECOVERY (26 GB, 14.0% used)					
Drop Disk Add Disk					
No disk found.					

The Repository Page in a High Availability Environment

In a high availability environment, you would see the above disk groups for the Primary Audit Vault Server, followed by the same disk groups for the Secondary Audit Vault Server. You must ensure that the secondary server has at least the same amount of space in each disk group as the primary server.



See Also:

[About Configuring a SAN Repository](#) (page 15-1)

15.5.2 Adding SAN Disks to the Audit Vault Server Repository

You can add SAN disks that are not already in use to any of the disk groups in the repository.



Note:

- Adding an additional disk creates two `VG_ROOT` volume groups. This results in failure during upgrade. Ensure that any disk added to the appliance has no pre-existing LVM or other device mapper metadata.
- Fiber Channel based storage with multipath is not supported in Oracle Audit Vault and Database Firewall.

To add disks to a disk group in the repository:

1. Log in to the Audit Vault Server as a super administrator.
2. Click the **Settings** tab, and then click **Repository**.

3. Click the **Add Disk** button corresponding the disk group you want.
Details for available disks are displayed, including disk capacity and free space.
4. Select the disk(s) you want to add to this disk group, and then click **Use Disk(s)**.
5. Click **OK** to confirm.

The selected disk(s) are displayed under the specified disk group.

15.5.3 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 as a super administrator.
2. Click the **Settings** tab, and then click **Repository**.
3. Find the disk you want to drop under one of the disk groups, select the disk, and then click **Drop Disk**.
4. Click **OK** to confirm.

Part III

General Reference

Part III provides general reference information for administering the Audit Vault and Database Firewall system.

This part contains the following appendixes:

- [AVCLI Commands Reference](#) (page A-1)
- [Plug-in Reference](#) (page B-1)
- [REDO Logs Audit Data Collection Reference](#) (page C-1)
- [Ports Used by Audit Vault and Database Firewall](#) (page D-1)
- [Troubleshooting Oracle Audit Vault and Database Firewall](#) (page G-1)

A

AVCLI Commands Reference

Topics

- [About the AVCLI Commands](#) (page A-1)
- [Agent Host AVCLI Commands](#) (page A-2)
- [Database Firewall AVCLI Commands](#) (page A-7)
- [Enforcement Point AVCLI Commands](#) (page A-12)
- [Secured Target AVCLI Commands](#) (page A-16)
- [Target Group AVCLI Commands](#) (page A-24)
- [Audit Trail Collection AVCLI Commands](#) (page A-25)
- [SMTP Connection AVCLI Commands](#) (page A-36)
- [Security Management AVCLI Commands](#) (page A-43)
- [SAN Storage AVCLI Commands](#) (page A-47)
- [Remote File System AVCLI Commands](#) (page A-53)
- [Server Management AVCLI Commands](#) (page A-56)
- [Collection Plug-In AVCLI Commands](#) (page A-59)
- [General Usage AVCLI Commands](#) (page A-61)
- [AVCLI User Commands](#) (page A-65)

A.1 About the AVCLI Commands

You can use the AVCLI commands to configure host connections from the command line. You must be granted the AV_ADMIN role before you can run these commands. This appendix does not list all of the AVCLI commands, however. It only covers the commands that an Audit Vault and Database Firewall administrator needs to configure secured target connections.

All AVCLI commands must end in a semi-colon (;).



See Also:

[Using the Audit Vault Command-Line Interface](#) (page 1-15) for general usage information about using the AVCLI command line interface.

Setting the JAVA_HOME Environment Variable

In the Audit Vault Server, you must set the JAVA_HOME environment variable to point to JDK installation directory.

A.2 Agent Host AVCLI Commands

The AVCLI host commands enable you to configure the host computer on which the Audit Vault Agent will reside.

[Table A-1](#) (page A-2) lists the AVCLI agent host commands.

Table A-1 AVCLI Agent Host Commands

Command	Description
REGISTER HOST (page A-2)	Adds the host to Audit Vault Server and identifies it as a host on which an agent can be deployed
ALTER HOST (page A-3)	Alters a host registered with the Audit Vault Server
LIST HOST (page A-5)	Lists the names of the currently registered agent host computers
DROP HOST (page A-5)	Drops the specified agent host from Audit Vault Server
ACTIVATE HOST (page A-6)	Activates the host on Audit Vault Server
DEACTIVATE HOST (page A-6)	Deactivates the specified host

A.2.1 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 on which an agent can be deployed.

Syntax

```
REGISTER HOST host_name [WITH IP ip_address]
```

Arguments

Argument	Description
<i>host_name</i>	The name of the host computer that you want to register.

See Also:

- [LIST HOST](#) (page A-5) to find the names of currently registered hosts.
- [LIST ATTRIBUTE FOR SECURED TARGET](#) (page A-23)

Argument	Description
<i>ip_address</i>	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](#) (page A-3) command.

Examples

```
avcli> REGISTER HOST sample_host.example.com;
```

Registers the host, `sample_host.example.com`, to run the agent process with the Audit Vault Server.

```
avcli> REGISTER HOST sample_host.example.net with ip 192.0.2.1;
```

Registers the host, `sample_host.example.net`, and associates it with the IP address `192.0.2.1`.

A.2.2 ALTER HOST

The `ALTER HOST` command alters a host registered with the Audit Vault Server.

Syntax

```
ALTER HOST hostname SET {key=value [,key=value...]}
```

```
ALTER HOST hostname SET {key=value [,LOGLEVEL=component_name:loglevel_value...]}
```

```
ALTER HOST hostname DROP ATTRIBUTE {attribute name}
```

Arguments

Argument	Description
<i>hostname</i>	The name of the host.
<i>key</i>	The attribute being changed. See Table A-2 (page A-4) for supported <i>key</i> values.

Usage Notes

This command alters the attributes associated with the named host using key/value pairs. To modify multiple attributes in a single command invocation, specify comma-separated key/value pairs.

The following host name attributes are supported:

Table A-2 Host Attributes (key values)

Parameter	Description
NAME	The new host name that replaces the existing one.
IP	The new IP address that replaces the existing IP address.
LOGLEVEL	<p>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.</p> <p>The LOGLEVEL attribute takes a two part value, separated by a colon, as follows:</p> <p><i>component_name:loglevel_value</i></p> <p>where <i>component_name</i> can be <i>av.agent</i>, <i>av.common</i>, <i>av.server</i>:</p> <p>See Table A-3 (page A-4) for descriptions of LOGLEVEL component names, and Table A-4 (page A-4) for LOGLEVEL values.</p> <p>Multiple components log levels can be changed by delimiting them using the symbol.</p>

The following are valid values for the LOGLEVEL attribute:

Table A-3 LOGLEVEL Component Names

Parameter	Description
<i>av.agent</i>	<i>agent component_name</i> of LOGLEVEL value
<i>av.server</i>	Audit Vault Server <i>component_name</i> of LOGLEVEL value
<i>av.common</i>	shared Server and Agent <i>component_name</i> of LOGLEVEL value

Table A-4 LOGLEVEL Values

Loglevel Value	Description
INFO	INFO level, <i>loglevel_value</i> of LOGLEVEL value
WARNING	WARNING level, <i>loglevel_value</i> of LOGLEVEL value
ERROR	ERROR level, <i>loglevel_value</i> of LOGLEVEL value
DEBUG	DEBUG level, <i>loglevel_value</i> 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.2.3 LIST HOST

The `LIST HOST` command lists the names of the currently registered agent host computers.

Syntax

```
LIST HOST
```

Example

```
avcli> LIST HOST;
```

The various active hosts registered with the Audit Vault Server are listed.

A.2.4 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
<i>hostname</i>	The name of the host computer being dropped.

See Also:

- [LIST HOST](#) (page A-5) to find the names of currently registered hosts.
- [LIST ATTRIBUTE FOR SECURED TARGET](#) (page A-23)

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.

A.2.5 ACTIVATE HOST

The `ACTIVATE HOST` command activates the host specified by *hostname*.

Syntax

```
ACTIVATE HOST hostname
```

Arguments

Argument	Description
<i>hostname</i>	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.2.6 DEACTIVATE HOST

The `DEACTIVATE HOST` command deactivates the host specified by *hostname*.

Syntax:

```
DEACTIVATE HOST hostname
```

Arguments

Argument	Description
<i>hostname</i>	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.3 Database Firewall AVCLI Commands

The AVCLI Database Firewall commands enable you to configure the Database Firewall.

[Table A-5](#) (page A-7) lists the AVCLI Database Firewall commands.

Table A-5 Database Firewall Commands

Command	Description
REGISTER FIREWALL (page A-7)	Registers the Database Firewall that has the specified IP address with the Audit Vault Server
DROP FIREWALL (page A-8)	Drops an already registered Database Firewall from the Audit Vault Server.
LIST FIREWALL (page A-8)	Lists all the Database Firewalls registered with the Audit Vault Server
REBOOT FIREWALL (page A-9)	Reboots a named Database Firewall that is already registered with the Audit Vault Server
POWEROFF FIREWALL (page A-9)	Powers off a named Database Firewall that is already registered with the Audit Vault Server
CREATE RESILIENT PAIR (page A-9)	Creates a resilient pair with two Database Firewalls for high availability
SWAP RESILIENT PAIR (page A-10)	Swaps Database Firewalls in a resilient pair that includes the named Database Firewall
DROP RESILIENT PAIR (page A-10)	Drops the resilient pair that contains the specified Database Firewall
ALTER FIREWALL (page A-11)	Alters the Database Firewall attributes
SHOW STATUS FOR FIREWALL (page A-11)	Displays the status for a particular Database Firewall

A.3.1 REGISTER FIREWALL

The `REGISTER FIREWALL` command registers the Database Firewall that has the specified IP address with the Audit Vault Server.

Syntax

```
REGISTER FIREWALL firewall_name WITH IP ip_address
```

Arguments

Argument	Descriptions
<i>firewall_name</i>	The name of the Database Firewall.

Argument	Descriptions
<i>ip_address</i>	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.3.2 DROP FIREWALL

The `DROP FIREWALL` command drops an already registered Database Firewall from the Audit Vault Server.

Syntax

```
DROP FIREWALL firewall_name
```

Arguments

Argument	Descriptions
<i>firewall_name</i>	The name of the Database Firewall.

Example

```
avcli> DROP FIREWALL sample_fw;
```

The Database Firewall `sample_fw` is dropped.

A.3.3 LIST FIREWALL

The `LIST FIREWALL` command lists all the Database Firewalls registered with the Audit Vault Server.

Syntax

```
LIST FIREWALL
```

Example

```
avcli> LIST FIREWALL;
```

A list of the Database Firewalls registered with Audit Vault Server appears.

A.3.4 REBOOT FIREWALL

The `REBOOT FIREWALL` command reboots a named Database Firewall that is already registered with the Audit Vault Server.

Syntax

```
REBOOT FIREWALL firewall_name
```

Arguments

Argument	Descriptions
<i>firewall_name</i>	The name of the Database Firewall.

Example

```
avcli> REBOOT FIREWALL sample_fw;
```

The Database Firewall `sample_fw` reboots.

A.3.5 POWEROFF FIREWALL

The `POWEROFF FIREWALL` command powers off a named Database Firewall that is already registered with the Audit Vault Server.

Syntax

```
POWEROFF FIREWALL firewall_name
```

Arguments

Argument	Descriptions
<i>firewall_name</i>	The name of the Database Firewall.

Example

```
avcli> POWEROFF FIREWALL sample_fw;
```

The Database Firewall `sample_fw` switches off.

A.3.6 CREATE RESILIENT PAIR

The `CREATE RESILIENT PAIR` command creates a resilient pair with two Database Firewalls for high availability.

Syntax

```
CREATE RESILIENT PAIR FOR FIREWALL PRIMARY primary_firewall  
SECONDARY secondary_firewall
```

Arguments

Argument	Descriptions
<i>primary_firewall</i>	The name of the primary Database Firewall. Only this Firewall can generate syslog alerts
<i>secondary_firewall</i>	The name of the secondary Database Firewall.

Example

```
avcli> CREATE RESILIENT PAIR FOR FIREWALL PRIMARY sample_fw1 SECONDARY
sample_fw2;
```

A resilient pair is created with primary Database Firewall *sample_fw1* and secondary Database Firewall *sample_fw2*.

A.3.7 SWAP RESILIENT PAIR

The `SWAP RESILIENT PAIR` command swaps Database Firewalls in a resilient pair that includes the named Database Firewall.

Syntax

```
SWAP RESILIENT PAIR HAVING FIREWALL firewall_name
```

Arguments

Argument	Descriptions
<i>firewall_name</i>	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.3.8 DROP RESILIENT PAIR

The `DROP RESILIENT PAIR` command drops the resilient pair that contains the specified Database Firewall.

Syntax

```
DROP RESILIENT PAIR HAVING FIREWALL firewall_name
```

Arguments

Argument	Descriptions
<i>firewall_name</i>	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.3.9 ALTER FIREWALL

The `ALTER FIREWALL` command alters the Database Firewall attributes.

Syntax

```
ALTER FIREWALL firewall_name SET attribute=value [, attribute=value]
```

Arguments

Argument	Description
<i>firewall_name</i>	The name of the Database Firewall.
<i>attribute</i>	The pair (attribute and new value) for the Database Firewall. Separate multiple pairs by a space on the command line. See Table A-6 (page A-11) for a list of attributes.

Usage Notes

[Table A-6](#) (page A-11) lists Database Firewall attributes that you can specify for the `attribute=value` argument.

Table A-6 Oracle Database Firewall Attributes

Parameter	Description
NAME	The new name of the Database Firewall.
IP	The IP address of the Database Firewall.

Example

```
avcli> ALTER FIREWALL sample_fw1 SET NAME=sample_newfw1;
```

Database Firewall name changes from `sample_fw1` to `sample_newfw1`.

```
avcli> ALTER FIREWALL sample_fw1 SET IP=192.0.2.169;
```

Database Firewall IP address is set to 192.0.2.169.

A.3.10 SHOW STATUS FOR FIREWALL

The `SHOW STATUS` command displays the status for a particular Database Firewall.

Syntax

```
SHOW STATUS FOR FIREWALL firewall_name
```


Arguments

Argument	Descriptions
<i>firewall_name</i>	The name of the Database Firewall.

Example

```
avcli> SHOW STATUS FOR FIREWALL sample_fw1;
```

The running information for Database Firewall *sample_fw1* appears.

A.4 Enforcement Point AVCLI Commands

The AVCLI Enforcement Point commands enable you to configure the Database Firewall.

[Table A-7](#) (page A-12) lists the AVCLI Enforcement Point commands.

Table A-7 Enforcement Point Commands

Command	Description
CREATE ENFORCEMENT POINT (page A-12)	Creates an enforcement point with the specified name and protects the Database Firewall using either mode DAM or DPE
DROP ENFORCEMENT POINT (page A-13)	Drops the enforcement point
LIST ENFORCEMENT POINT (page A-13)	Lists all the enforcements points associated with the Database Firewall or secured target
START ENFORCEMENT POINT (page A-14)	Starts an enforcement point that was previously suspended
STOP ENFORCEMENT POINT (page A-14)	Stops the enforcement point monitoring the secured target
ALTER ENFORCEMENT POINT (page A-15)	Alters the enforcement point and attributes

A.4.1 CREATE ENFORCEMENT POINT

The `CREATE ENFORCEMENT POINT` command creates an enforcement point with the specified name and protects the Database Firewall using either mode DAM or DPE.

Syntax

```
CREATE ENFORCEMENT POINT enforcement_point_name
FOR SECURED TARGET secured_target_name
USING FIREWALL firewall_name
TRAFFIC SOURCE traffic_source_name
WITH MODE DPE|DAM
```

Arguments

Argument	Descriptions
<i>enforcement_point_name</i>	The name of the enforcement point.
<i>secured_target_name</i>	The name of the secured target.
<i>firewall_name</i>	The name of the Database Firewall.
<i>traffic_source_name</i>	The name of the traffic source

Example

```
avcli> CREATE ENFORCEMENT POINT sample_ep FOR SECURED TARGET sample_source USING
      FIREWALL sample_fw TRAFFIC SOURCE sample_trafficsource WITH MODE DPE;
```

An enforcement point named `sample_ep` is created on Database Firewall `sample_fw`, using DPE mode to protect the secured target `sample_source`, and using the traffic source `sample_trafficsource`.

A.4.2 DROP ENFORCEMENT POINT

The `DROP ENFORCEMENT POINT` command drops the enforcement point.

Syntax

```
DROP ENFORCEMENT POINT enforcement_point_name
```

Arguments

Argument	Descriptions
<i>enforcement_point_name</i>	The name of the enforcement point.

Example

```
avcli> DROP ENFORCEMENT POINT sample_ep;
```

The enforcement point named `sample_ep` is dropped from the Database Firewall.

A.4.3 LIST ENFORCEMENT POINT

The `LIST ENFORCEMENT POINT` command lists all the enforcements points associated with either the Database Firewall or the secured target.

Syntax

```
LIST ENFORCEMENT POINT FOR FIREWALL firewall_name
```

```
LIST ENFORCEMENT POINT FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Descriptions
<i>firewall_name</i>	The name of the Database Firewall.
<i>secured_target_name</i>	The name of the secured target.

Example

```
avcli> LIST ENFORCEMENT POINT FOR FIREWALL sample_fw;
```

A list of all the enforcement points associated with Database Firewall *sample_fw* appears.

```
avcli> LIST ENFORCEMENT POINT FOR SECURED TARGET sample_source;
```

A list all the enforcement points associated with secured target *sample_source* appears.

A.4.4 START ENFORCEMENT POINT

The `START ENFORCEMENT POINT` command starts an enforcement point that was previously suspended.

Syntax

```
START ENFORCEMENT POINT enforcement_point_name
```

Arguments

Argument	Descriptions
<i>enforcement_point_name</i>	The name of the enforcement point.

Example

```
avcli> START ENFORCEMENT POINT sample_ep;
```

The enforcement point named *sample_ep* starts.

A.4.5 STOP ENFORCEMENT POINT

The `STOP ENFORCEMENT POINT` command stops the enforcement point monitoring the secured target.

Syntax

```
STOP ENFORCEMENT POINT enforcement_point_name
```

Arguments

Argument	Descriptions
<i>enforcement_point_name</i>	The name of the enforcement point.

Example

```
avcli> STOP ENFORCEMENT POINT sample_ep;
```

The enforcement point named `sample_ep` stops.

A.4.6 ALTER ENFORCEMENT POINT

The `ALTER ENFORCEMENT POINT` command alters the enforcement point and attributes.

Syntax

```
ALTER ENFORCEMENT POINT enforcement_point_name SET attribute=value
    [, attribute=value]
```

Arguments

Argument	Description
<i>enforcement_point_name</i>	The name of the enforcement point.
<i>attribute</i>	The pair (attribute and new value) for the enforcement point being altered. Separate multiple pairs by a space on the command line. See Table A-8 (page A-15) for enforcement point attributes.

Usage Notes

Attributes are specified by a comma-separated list of key=value/pairs. The following key values are supported:

Table A-8 Enforcement Point Attributes

Parameter	Description
TARGET	The new secured target name, which should be registered already in the Audit Vault Server, including the address.
MODE	The mode which monitors the enforcement point. Valid modes are: DAM or DPE.
PRESERVE_CONNECTION	True or False where True indicates that when the database firewall starts operating in DPE mode (either because it had been changed from DAM, or because it has restarted), any existing connections passing through the firewall are allowed to continue. This favors availability over security, because the firewall cannot enforce policy on these connections. False indicates that any preexisting connections are broken. The database firewall can then enforce the policy when clients reconnect. This is the default behavior.
TRAFFIC_SOURCE	New valid traffic sources for enforcement point.

Table A-8 (Cont.) Enforcement Point Attributes

Parameter	Description
DATABASE_RESPONSE	True or False indicates whether or not to activate database response monitoring function for enforcement point.
FULL_ERROR_MESSAGE	True or False enables this option. This starts logging the error message associated with the error code.
DATABASE_INTERROGATION	True or False enables this option. This starts the database interrogation feature for enforcement point.
HOST_MONITOR	True or False enables this option. This specifies whether or not the remote agent needs to be enabled.
HOST_MONITOR_ADDRESS	The new IP Address for Remote agent.

Examples

```
avcli> ALTER ENFORCEMENT POINT ep1 SET TARGET=newsource;
```

The enforcement point to monitor new secured target is altered.

```
avcli> ALTER ENFORCEMENT POINT ep1 SET MODE=dam;
```

The enforcement point monitoring is altered to DAM mode.

```
avcli> ALTER ENFORCEMENT POINT ep1 SET database_response=true,
Full_error_message=true;
```

The enforcement point is altered to activate database response and log error messages associated with error codes.

```
avcli> ALTER ENFORCEMENT POINT ep1 SET database_interrogation=true;
```

The enforcement point is altered to activate direct database interrogation.

A.5 Secured Target AVCLI Commands

The AVCLI secured target commands enable you to configure both database and nondatabase secured targets for Audit Vault Server.

[Table A-9](#) (page A-16) lists the AVCLI secured target commands.

Table A-9 AVCLI Secured Target Commands

Command	Description
REGISTER SECURED TARGET (page A-17)	Registers a secured target to be monitored by Audit Server
ALTER SECURED TARGET (page A-19)	Modifies the attributes of a secured target
LIST ADDRESS FOR SECURED TARGET (page A-22)	Lists all the addresses registered with the secured target

Table A-9 (Cont.) AVCLI Secured Target Commands

Command	Description
LIST SECURED TARGET (page A-22)	Lists the various active secured targets registered with the Audit Vault Server
LIST SECURED TARGET TYPE (page A-22)	Lists the secured target types currently registered with Audit Vault Server
LIST ATTRIBUTE FOR SECURED TARGET (page A-23)	Lists the attributes of a given secured target
LIST METRICS (page A-23)	Lists the metrics of a given secured target, such as the various trails
DROP SECURED TARGET (page A-24)	Removes the registration of the specified secured target from Audit Vault Server

A.5.1 REGISTER SECURED TARGET

The `REGISTER SECURED TARGET` command registers a secured target to be monitored by Audit Vault Server.

Syntax

```
REGISTER SECURED TARGET secured_target_name OF SECURED TARGET TYPE
  "secured_target_type" [AT location] [AUTHENTICATED BY username/password]
```


Arguments

Argument	Description
<i>secured_target_name</i>	Name of secured target. Must be unique.
<i>secured_target_type</i>	A valid secured target type, for example "Oracle".



See Also:

[LIST SECURED TARGET TYPE](#)
(page A-22) to find a list of supported secured target types.

Argument	Description
<i>location</i>	The secured target database connection information.
	<div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;">  See Also: ALTER SECURED TARGET (page A-19) </div> <p>This is optional. It can be added later.</p> <p>The <i>location</i> is an opaque string that specifies how to connect to the secured target, typically a JDBC connect string. The syntax that you use depends on the secured target type. See the database-specific Usage Notes below.</p> <p>If <i>location</i> is not provided, certain features such as entitlement retrieval, audit settings management, SPA retrieval, and audit trail collection are disabled if applicable to this secured target type.</p>
<i>user_name/password</i>	<p>Optional. Credentials to connect to the secured target.</p> <p>After you enter this argument and run the <code>REGISTER SECURED TARGET</code> command, Audit Vault Server prompts you for the user name and password of the secured target user account. For secured target databases, this account must exist on the secured target database. Optional.</p> <p>See the database-specific Usage Notes in the following sections.</p>



Note:

The syntax of this command will be changed in Oracle Audit Vault and Database Firewall release 20.1.0.0.0.

General Examples

```
avcli> HELP REGISTER SECURED TARGET;
```

Displays detailed help for the `REGISTER SECURED TARGET` command.

Oracle Database Usage Notes and Examples

- For the *location* argument, enter the host name, port number, and service ID (SID), separated by a colon. Use the following syntax:

```
AT host:port:service
```

For example:

```
Oracle Database: jdbc:oracle:thin:@//host:port/service
```

If you are unsure of this connection information, then run the `lsnrctl status listener_name` command on the computer where you installed the secured target database.

- The `AUTHENTICATED BY` command prompts for the secured target user name and password. This user account must exist in the secured target database.

To find this user, query the `SESSION_PRIVS` and `SESSION_ROLES` data dictionary views.

Oracle Database Examples:

```
avcli> REGISTER SECURED TARGET sample_source OF SECURED TARGET TYPE "Oracle Database"
      AT jdbc:oracle:thin:@//anymachinename:1521/example.com
      AUTHENTICATED BY system/welcome_1;
```

Registers a Oracle secured target, `sample_source`, of secured target type Oracle Database, reachable using connect string `jdbc:oracle:thin:@//anymachinename: 1521/example.com` using credentials `system/welcome_1`.

SQL Server Example With DB

```
avcli > REGISTER SECURED TARGET sample_mssqldb OF SECURED TARGET TYPE "Microsoft
SQL Server" AT jdbc:av:sqlserver://hostname:port authenticated by <user>/
<password>;
```

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>/<windows user password>;
```

IBM DB2 Example

```
avcli> REGISTER SECURED TARGET sample_db2db OF SECURED TARGET TYPE "IBM DB2 LUW"
AT jdbc:av:db2://host:port;
```

Registers a DB2 secured target, `sample_db2db`, of secured target type "IBM DB2 LUW", reachable using connect string `jdbc:av:db2://host:port` using credentials `sa/welcome_1`.

A.5.2 ALTER SECURED TARGET

The `ALTER SECURED TARGET` command modifies the attributes of a secured target.

Syntax

```
ALTER SECURED TARGET secured_target_name
      SET attribute=value [, attribute=value]
```

```
ALTER SECURED TARGET secured target name ADD ADDRESS ip:port:[service]
```

```
ALTER SECURED TARGET secured target name DROP ADDRESS ip:port:[service]
```


Arguments

Argument	Description
<code>secured_target_name</code>	The name of the secured target database to be modified. The name is case-sensitive.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> See Also:</p> <p>LIST SECURED TARGET (page A-22) to find a list of existing secured targets.</p> </div>
<code>attribute=value</code>	The key/value pair for the secured target attributes of the secured target to be modified. You can modify one or more secured target attributes at a time using a space on the command line.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> See Also:</p> <ul style="list-style-type: none"> • Table A-10 (page A-21) for secured target attributes. • Collection Attributes (page B-38) as some types of secured targets also require collection attributes. • LIST ATTRIBUTE FOR SECURED TARGET (page A-23) to find a list of attribute values for a secured target. </div>
<code>ip</code>	The IP address
<code>port</code>	The port number
<code>service</code>	REQUIRED FOR ORACLE DATABASE ONLY: The service name or SID

 **Note:**

The syntax of this command will be changed in Oracle Audit Vault and Database Firewall release 20.1.0.0.0.

[Table A-10](#) (page A-21) lists secured target attributes that you can specify,

Table A-10 Secured Target Attributes

Attribute	Description
NAME	The name for this secured target database instance. This must not be defined already in the Audit Vault Server for another secured target.
LOCATION	The location of the secured target
CREDENTIALS	The new set of username and password pair used to connect to the secured target. This is a two part value separated by a slash (/).
DESCRIPTION	The description for this secured target database instance
MAXIMUM_ENFORCEMENT_POINT_THREADS	The maximum number of enforcement point threads for the secured target. The valid range is between 1 and 16 (inclusive). The default value is 1.

General Usage Examples:

```
avcli> ALTER SECURED TARGET sample_source SET name=sample_source2;
```

The secured target name of `sample_source` changed to `sample_source2`.

```
avcli> ALTER SECURED TARGET sample_source SET credentials=scott/leopard;
```

The credentials used to connect to the secured target, `sample_source`, are changed.

```
avcli> ALTER SECURED TARGET sample_source SET description='This is a new description';
```

Number of enforcement point threads is set for secured target, `sample_source`.

```
avcli> ALTER SECURED TARGET sample_source SET maximum_enforcement_point_threads=14;
```

The description for the secured target, `sample_source`, is changed.

```
avcli> ALTER SECURED TARGET sample_source ADD address 192.0.2.2:1234:srcdb;
```

New secured target address is registered with secured target `sample_source`.

```
avcli> ALTER SECURED TARGET sample_source DROP address 192.0.2.2:1234:srcdb;
```

Secured target address registered before with secured target, `sample_source`, is dropped.

```
avcli> ALTER SECURED TARGET sample_source set maximum_enforcement_point_threads = 10;
```

Sets the maximum number of enforcement point threads for secured target `sample_source` to 10.

Oracle Example:

```
avcli> ALTER SECURED TARGET secured target sample_source set
location=jdbc:oracle:thin:@//new_sample_host:1521:sample_db;
```

The location of the secured target, `sample_source`, changes.

A.5.3 UPLOAD OR DELETE WALLET FILE

This command is used to upload and delete a secured 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 secured target.
WALLET_FILE	Name of wallet attribute (Key).
<Path of the wallet file>	Path to wallet file (Value).

A.5.4 LIST ADDRESS FOR SECURED TARGET

The `LIST ADDRESS FOR SECURED TARGET` command lists all the addresses registered with the secured target.

Syntax

```
LIST ADDRESS FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Descriptions
<i>secured_target_name</i>	The name of the secured target.

Example

```
avcli> LIST ADDRESS FOR SECURED TARGET sample_source;
```

All the addresses for secured target, `sample_source`, appear.

A.5.5 LIST SECURED TARGET

The `LIST SECURED TARGET` command lists the active secured targets registered with the Audit Vault Server.

Syntax

```
LIST SECURED TARGET;
```

Lists the active secure targets registered with the Audit Vault Server.

A.5.6 LIST SECURED TARGET TYPE

The `LIST SECURED TARGET TYPE` command lists the secured target types currently supported in the Audit Vault Server.

Syntax

```
LIST SECURED TARGET TYPE
```

Examples

```
avcli> LIST SECURED TARGET TYPE;
```

Lists the secured target types currently supported in the Audit Vault Server.

A.5.7 LIST ATTRIBUTE FOR SECURED TARGET

The `LIST ATTRIBUTE FOR SECURED TARGET` command lists the attributes of a given secured target.

Syntax

```
LIST ATTRIBUTE FOR SECURED TARGET secured target name;
```

Arguments

Argument	Description
<i>secured target name</i>	The name of the secured target. To find all registered secured targets, see " LIST SECURED TARGET (page A-22)".

A.5.8 LIST METRICS

The `LIST METRICS` command lists the metrics of a given secured target, such as various trails.

Syntax

```
LIST METRICS FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Description
<i>secured_target_name</i>	The name of the secured target To find all registered secured targets, see " LIST SECURED TARGET (page A-22)".

Usage Notes

The `LIST METRICS` command has the same usage for all secured target types.

Examples

```
avcli> LIST METRICS FOR SECURED TARGET sample_source;
```

Metrics available for the secured target, `sample_source`, are listed.

A.5.9 DROP SECURED TARGET

The `DROP SECURED TARGET` command removes the registration of the specified secured target from Audit Vault Server.

Syntax

```
DROP SECURED TARGET secured_target_name
```

Arguments

Argument	Description
<i>secured_target_name</i>	The name of the secured target. To find all registered secured targets, see " LIST SECURED TARGET (page A-22)".

Usage Notes

Ensure that all trails associated with this secured target are in stopped state before dropping the secured target. Otherwise, the `DROP SECURED TARGET` command fails. See `HELP STOP COLLECTION` for an explanation of how to stop active trails.

Dropping a secured target stops the Audit Vault Server from monitoring it. Any audit data collected earlier continues to be available in the Audit Vault Server repository.

Examples

```
avcli> DROP SECURED TARGET sample_source;
```

Drops the `sample_source` secured target.

A.6 Target Group AVCLI Commands

The AVCLI target group commands enable you to alter a target group.

[Table A-11](#) (page A-24)

Table A-11 AVCLI Target Group Commands

Command	Description
ADD TARGET (page A-24)	Adds a specific target to a target group.
DELETE TARGET (page A-25)	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.
target group name	The name of the specific target group.

Example

```
alter targetgroup tgl add target t1
```

A.6.2 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 tgl delete target t1
```

A.7 Audit Trail Collection AVCLI Commands

The AVCLI secured target audit trail collection commands enable you to manage the audit trail collections for the secured targets.

[Table A-12](#) (page A-25) lists the AVCLI secured target connection commands.

Table A-12 AVCLI Secured Target Connection Commands

Command	Description
START COLLECTION FOR SECURED TARGET (page A-26)	Starts the collection of specified audit trail data from a given secured target
STOP COLLECTION FOR SECURED TARGET (page A-30)	Stops the audit trail collection

Table A-12 (Cont.) AVCLI Secured Target Connection Commands

Command	Description
LIST TRAIL FOR SECURED TARGET (page A-34)	Lists the available audit trails that have been started with the <code>START COLLECTION</code> command or stopped with the <code>STOP COLLECTION</code> command
DROP TRAIL FOR SECURED TARGET (page A-35)	Drops an audit trail

A.7.1 START COLLECTION FOR SECURED TARGET

The `START COLLECTION FOR SECURED TARGET` command starts the collection of specified audit trail data from a given secured target, optionally using the specified collection plug-in.

Syntax

```
START COLLECTION FOR SECURED TARGET secured_target_name USING HOST host FROM
location
    [USING PLUGIN plugin id]
```

Arguments

Argument	Description
<i>secured_target_name</i>	The name of the secured target whose audit trail collection you want to begin.
<i>host</i>	The name of the host where the secured target agent resides.
<i>location</i>	The <i>location</i> is one of following: <ul style="list-style-type: none"> • DIRECTORY <i>directory name/mask</i> • TABLE <i>tablename</i> • SYSLOG DEFAULT <i>filename/file mask</i> • NETWORK • EVENT LOG <i>eventlog_name</i> • TRANSACTION LOG • CUSTOM <i>name</i>
<i>plugin id</i>	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.

 **See Also:**

- [LIST SECURED TARGET](#) (page A-22) to find all registered secured targets.
- [LIST HOST](#) (page A-5) to find a list of configured agent hosts.
- [LIST ATTRIBUTE FOR SECURED TARGET](#) (page A-23) for detailed information about a secured target.
- [LIST PLUGIN FOR SECURED TARGET TYPE](#) (page A-60) 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 secured target, the secured target must be up and running. When multiple plug-ins can process audit data from a secured target, use the optional `USING PLUGIN` directive to disambiguate the collection process.

A trail starts in the `START_REQUESTED` state and transitions to a starting state, followed by a running state. If there is no outstanding audit data to process from the given trail, the collection process switches to an idle state. The current state can be viewed using the `LIST TRAIL` command.

If a trail must be authenticated, the Audit Vault Server uses the credentials provided in the `AUTHENTICATED BY` argument of the `REGISTER SECURED TARGET` command.

After you run the `START COLLECTION` command, the Audit Vault Server begins to collect audit data from the configured secured targets. If you want to stop the collection, then run the `STOP COLLECTION` command.

 **See Also:**

- [REGISTER SECURED TARGET](#) (page A-17)
- [STOP COLLECTION FOR SECURED TARGET](#) (page A-30)

Windows Systems Usage Notes

On Windows systems, enter directory and file name locations in either double-quoted strings or as a nonquoted string using forward slashes. For example:

```
... FROM DIRECTORY "c:\app\oracle\product\11.1\av";
```

```
... FROM DIRECTORY c:/app/oracle/product/11.1/av;
```

General Examples

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM
      directory /opt/audit_trail;
```

Audit data collection from trail `/opt/audit_trail` for secured target `sample_source` starts.


```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM
TABLE sys.aud$;
```

Audit data collection from table trail sys.aud\$ for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM
syslog
  /usr/syslog/syslog*;
```

Collecting syslog trail /usr/syslog/syslog* for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM
event
  log application;
```

Collecting application event log trail for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo
FROM transaction log;
```

Collecting transaction log trails for secured target sample_source starts.

```
avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo
FROM TABLE sys.aud$ USING PLUGIN com.sample_plugin;
```

Audit data collection from table trail sys.aud\$ for the secured target sample_source, using the com.sample_plugin, plug-in starts.

Oracle Database Secured Target Usage Notes

Audit Trail Settings

For the operating system type of audit trail, use the following settings:

Type of Audit Trail	trail_type Setting	audit_trail Setting
Operating system directory	DIRECTORY	directory_location
Syslog file	SYSLOG	file_name
Windows event log	EVENTLOG	N/A

SQL Server Secured Target Usage Notes

Audit Trail Settings

You can write the SQL Server audit trail to the Windows event log, C2 trace files, or server side trace files. The FROM *trail_type audit_trail* arguments are as follows:

Type of Audit Trail	trail_type Setting	audit_trail Setting
Windows event log	EVENTLOG	N/A
C2 trace file	DIRECTORY	file_wildcard
Server-side trace files	DIRECTORY	file_wildcard
SQLAUDIT files	DIRECTORY	file_wildcard

 **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 Secured Target Usage Notes and Examples

For the Sybase ASE audit trail, set the *trail_type audit_trail* setting to `TABLE SYSAUDITS`.

Sybase ASE Example

```
avcli> START COLLECTION FOR SECURED TARGET hr_syb_db USING HOST sybserver
FROM TABLE SYSAUDITS;
```

MySQL Usage Notes

The trail *location* is the path to the directory where converted XML files are created by running the MySQL XML transformation utility.

 **See Also:**

[Converting Audit Record Format For Collection](#) (page 6-14)

IBM DB2 Usage Notes and Examples

For the IBM DB2 audit trail, set the *trail_type audit_trail* setting to `DIRECTORY directory_location`.

IBM DB2 Example

```
avcli> START COLLECTION FOR SECURED TARGET hr_db2_db USING HOST db2server
FROM DIRECTORY "d:\temp\trace";
```

Oracle Solaris Secured Target Usage Notes

For an Oracle Solaris secured target, the trail *location* used in this command must be in the format:

```
hostname:path_to_trail
```

where *hostname* matches the hostname in the audit log names, which look like this:

```
timestamp1.timestamp2.hostname
```

Windows Secured Target Usage Notes

For a Windows secured target, the event log audit trail type collects data from the Windows Security Event Log. The trail *location* used in this command must be *security*.

 **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 Secured Target Usage Notes

For *Active Directory* secured 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 <code>Overwrite event as needed (Oldest event first)</code> or <code>Do not overwrite events</code> . 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.7.2 STOP COLLECTION FOR SECURED TARGET

The `STOP COLLECTION FOR SECURED TARGET` command stops the audit trail collection.

Syntax

```
STOP COLLECTION FOR SECURED TARGET secured_target_name USING HOST hostname FROM
location
[USING PLUGIN plugin_id]
```

Arguments

Argument	Description
<i>secured_target_name</i>	The name of the secured target for the trail collection you want to stop.
<i>hostname</i>	The name of the host where the secured target agent resides.
<i>location</i>	The <i>location</i> is one of following: <ul style="list-style-type: none"> • DIRECTORY <i>directory name/mask</i> • TABLE <i>tablename</i> • SYSLOGDEFAULT <i>filename/file mask</i> • NETWORK • EVENT LOG <i>eventlog name</i> • TRANSACTION LOG • CUSTOM <i>name</i>
<i>plugin_id</i>	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.



See Also:

- [LIST SECURED TARGET](#) (page A-22) to find a list of all registered secured targets.
- [LIST HOST](#) (page A-5) to find a list of configured agent hosts.
- [LIST ATTRIBUTE FOR SECURED TARGET](#) (page A-23) for detailed information about a secured target.
- [LIST PLUGIN FOR SECURED TARGET TYPE](#) (page A-60) to find a list of existing plug-ins for the type.
- [LIST TRAIL FOR SECURED TARGET](#) (page A-34) to view the current state of secured 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 secured target, use the optional `USING PLUGIN` directive to disambiguate the process.

A trail will be in a `STOP_REQUESTED` state when stopped and transitions to a stopping state, followed by a stopped state.

Windows Systems Usage Notes

On Windows systems, enter directory and file name locations in either double-quoted strings or as a nonquoted string using forward slashes. For example:

```
... FROM DIRECTORY "c:\app\oracle\product\11.1\av";
```

```
... FROM DIRECTORY c:/app/oracle/product/11.1/av;
```

General Examples

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host  
FROM directory /opt/audit_trail;
```

Audit data collection from trail /opt/audit_trail for secured target sample_source stops.

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host  
FROM TABLE sys.aud$;
```

Audit data collection from table trail sys.aud\$ for secured target sample_source stops.

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host  
FROM syslog  
/usr/syslog/syslog*;
```

Collecting syslog trail /usr/syslog/syslog* for secured target sample_source stops.

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host  
FROM event log application;
```

Collecting application event log trail for secured target sample_source stops

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host  
FROM transaction log;
```

Collecting transaction log trail for secured target sample_source stops

```
avcli> STOP COLLECTION FOR SECURED TARGET sample_source USING HOST sample_host  
FROM TABLE sys.aud$ USING PLUGIN com.sample_plugin;
```

Audit data collection from table sys.aud\$ for the secured target, sample_source, using the com.sample_plugin, plug-in stops

Oracle Database Usage Notes and Examples

Audit Trail Settings

For the operating system type of audit trail, use the following settings:

Oracle Database Examples

Operating system directory example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com  
FROM DIRECTORY $ORACLE_HOME/logs;
```

Operating system syslog file example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com  
FROM SYSLOG /etc/syslog.conf;
```

Operating system Windows event log example:

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com  
FROM EVENTLOG;
```

Database audit trail example:

```
avcli> START COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com
FROM TABLE sys.aud$;
```

REDO log example:

```
avcli> START COLLECTION FOR SECURED TARGET hr_sql_db USING HOST hrdb.example.com
FROM TRANSACTION LOG;
```

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	<i>file_wildcard</i>
Server-side trace files	SERVERSIDETRACE	<i>file_wildcard</i>

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:**

[Converting Audit Record Format For Collection \(page 6-14\)](#)

IBM DB2 Usage Notes and Example

For the IBM DB2 audit trail, set the `trail_type audit_trail` setting to `DIRECTORY directory_location`.

IBM DB2 Example

```
avcli> STOP COLLECTION FOR SECURED TARGET hr_db2_db USING HOST db2server
FROM DIRECTORY "d:\temp\trace";
```

Oracle Solaris Usage Notes

For Oracle Solaris, the trail location must be in the format:

```
hostname:path_to_trail
```

where `hostname` matches the hostname in the audit log names, which look like this:

```
timestamp1.timestamp2.hostname
```

Windows Secured Target Usage Notes

For a Windows secured target, the event log audit trail type collects data from the Windows Security Event Log. The trail `location` used in this command must be `security`.

A.7.3 LIST TRAIL FOR SECURED TARGET

The `LIST TRAIL FOR SECURED TARGET` command lists the available audit trails that have been started with the `START COLLECTION` command or stopped with the `STOP COLLECTION` command.

Syntax

```
LIST TRAIL FOR SECURED TARGET secured_target_name
```

Arguments

Argument	Description
<i>secured_target_name</i>	The name of the secured target. To find a list of existing secured targets, see " LIST SECURED TARGET (page A-22)".

Usage Notes

`LIST TRAIL FOR SECURED TARGET` does not list audit trails have been created but not yet started or stopped.

Examples

```
avcli> LIST TRAIL FOR SECURED TARGET sample_source;
```

The trails available for the secured target `sample_souce` are listed.

A.7.4 DROP TRAIL FOR SECURED TARGET

The `DROP TRAIL FOR SECURED TARGET` drops a trail that no longer needs to be monitored.

Note:

An audit trail must be in a STOPPED state in order for it to be dropped. A trail that has previously collected audit data associated with it cannot be dropped.

Syntax

```
DROP TRAIL FOR SECURED TARGET secured_target_name USING HOST hostname FROM location
```

Arguments

Argument	Description
<i>secured_target_name</i>	The name of the secured target whose audit trail you want to drop.
<i>hostname</i>	The name of the host where the secured target agent resides.
<i>location</i>	The <i>location</i> is one of following: <ul style="list-style-type: none"> • DIRECTORY <i>directory name/mask</i> • TABLE <i>tablename</i> • SYSLOG DEFAULT <i>filename/file mask</i> • NETWORK • EVENT LOG <i>eventlog name</i> • TRANSACTION LOG • CUSTOM <i>name</i>

See Also:

- [LIST SECURED TARGET](#) (page A-22) to find all registered secured targets.
- [LIST HOST](#) (page A-5) to find a list of configured agent hosts.
- [LIST ATTRIBUTE FOR SECURED TARGET](#) (page A-23) for detailed information about a secured 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 secured target `sample_source` is dropped.

```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo FROM TABLE sys.aud$;
```

The audit trail from table trail `sys.aud$` for secured target `sample_source` is dropped.


```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo FROM SYSLOG
DEFAULT
/usr/syslog/syslog*;
```

Syslog trail /usr/syslog/syslog* for secured target sample_source is dropped.

```
avcli> DROP TRAIL FOR SECURED TARGET sample_source USING HOST foo
FROM TRANSACTION LOG;
```

The transaction log trail for secured target sample_source is dropped.

A.8 SMTP Connection AVCLI Commands

The AVCLI SMTP commands enable you to manage SMTP email notifications for Audit Vault Server reports and alert.

Table A-13 (page A-36) lists the SMTP-specific AVCLI commands.

Table A-13 AVCLI SMTP Commands

Command	Description
REGISTER SMTP SERVER (page A-36)	Registers the SMTP server configuration with the Audit Vault Server
ALTER SMTP SERVER (page A-38)	Modifies the SMTP server configuration and state
ALTER SMTP SERVER ENABLE (page A-39)	Enables SMTP server configurations for servers registered with the REGISTER SMTP SERVER command or modified with the ALTER SMTP SERVER command
ALTER SMTP SERVER DISABLE (page A-39)	Disables the SMTP server configuration
ALTER SMTP SERVER SECURE MODE ON (page A-40)	Enables the SMTP server configuration and specifies the secure protocol mode used
ALTER SMTP SERVER SECURE MODE OFF (page A-41)	Disables secure mode in an existing secure SMTP server
TEST SMTP SERVER (page A-41)	Tests SMTP integration with the Audit Vault Server by sending a test email
LIST ATTRIBUTE OF SMTP SERVER (page A-42)	Displays the current SMTP configuration details used by Audit Vault Server
DROP SMTP SERVER (page A-43)	Unregisters the SMTP Server registered with the Audit Vault Server and removes any associated configuration metadata

A.8.1 REGISTER SMTP SERVER

The REGISTER SMTP SERVER command registers the SMTP server configuration with the Audit Vault Server.

Syntax

```
REGISTER SMTP SERVER AT host:[port] SENDER ID sender_id SENDER EMAIL
sender_email
[AUTHENTICATED BY username/password]
```

Arguments

Argument	Description
<i>host:[port]</i>	The name, and optionally, the outgoing port number of the SMTP server. The <i>port</i> defaults to 25, if unspecified.
<i>sender_id</i>	The user ID of the person responsible for sending the email (that is, the email address that appears after <code>From</code>).
<i>sender_email</i>	The email address of the person whose ID you entered for the SENDER ID, in Request For Comments (RFC) 822 format.
<i>username/password</i>	Optional. The authentication credentials for the recipient user. If the SMTP server runs in authenticated mode and needs a valid <i>username/password</i> to connect to send emails, use the <code>AUTHENTICATED BY</code> clause to specify those credentials.



Note:

The syntax of this command will be changed in Oracle Audit Vault and Database Firewall release 20.1.0.0.0.

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](#) (page A-40)
- [TEST SMTP SERVER](#) (page A-41)

Examples

```
avcli> REGISTER SMTP SERVER AT sample_mail.example.com sender id "do-not-reply";
```

For an SMTP server running in non-authentication mode at `sample_mail.example.com`, all email is generated and sent from the address: `do-not-reply<donotreply@example.com>`.

```
avcli> REGISTER SMTP SERVER AT sample_mail.example.com:455 SENDER ID av-alerts SENDER
EMAIL avalerts@example.com AUTHENTICATED BY smtpuser/smtppass;
```

For an SMTP server running in authentication mode at `sample_mail.example.com`, port 455; all email is generated and sent from the address: `av-alerts<avalerts@example.com>`. The credentials `smtppuser/smtppass` connect to this server to send emails.

A.8.2 ALTER SMTP SERVER

The `ALTER SMTP SERVER` command modifies the SMTP server configuration and state.

Syntax

```
ALTER SMTP SERVER AT host[:port] [SENDER ID sender_id] |
[SENDER EMAIL sender_email] | [AUTHENTICATED BY username/password]
```

Arguments

Argument	Description
<i>host</i> [: <i>port</i>]	The name, and optionally, the outgoing port number of the SMTP server. The <i>port</i> defaults to 25.
<i>sender_id</i>	The user ID of the person responsible for sending the email (that is, the email address that appears after <code>From</code>).
<i>sender_email</i>	The email address of the person whose ID you entered for the <code>SENDER ID</code> , in Request For Comments (RFC) 822 format.
<i>username/password</i>	Optional. The authentication credentials for the recipient user. If the SMTP server runs in authenticated mode and needs a valid <i>username/password</i> to connect to send emails, use the <code>AUTHENTICATED BY</code> clause to specify those credentials.



Note:

The syntax of this command will be changed in Oracle Audit Vault and Database Firewall release 20.1.0.0.0.

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](#) (page A-40)
- [TEST SMTP SERVER](#) (page A-41)

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 ENABLE

The `ALTER SMTP SERVER ENABLE` command enables SMTP server configurations for servers registered with the `REGISTER SMTP SERVER` command or modified with the `ALTER SMTP SERVER` command.

Syntax

```
ALTER SMTP SERVER ENABLE
```

Usage Notes

- When you enable the configuration, Audit Vault Server uses the configuration that was in place when you last disabled the SMTP configuration.
- To find details about the most recent service configuration, see "[LIST ATTRIBUTE OF SMTP SERVER](#) (page A-42)".

Example

```
avcli> ALTER SMTP SERVER ENABLE;
```

SMTP integration is enabled.

Enables the integration between the Audit Vault and SMTP server.

A.8.4 ALTER SMTP SERVER DISABLE

The `ALTER SMTP SERVER DISABLE` command disables the SMTP server configuration.

Syntax

```
ALTER SMTP SERVER DISABLE
```

Usage Notes

- After you disable the configuration, Audit Vault Server preserves the most recent configuration. So, when you re-enable the configuration, this configuration is made active again.
- To find details about the most recent service configuration, see "[LIST ATTRIBUTE OF SMTP SERVER](#) (page A-42)".
- 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.8.5 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: <ul style="list-style-type: none"> • SSL: Secure Sockets Layer (default) • TLS: Transport Layer Security
<i>location</i>	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](#) (page A-36)
- [ALTER SMTP SERVER](#) (page A-38)

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.8.6 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](#) (page A-36) or [ALTER SMTP SERVER](#) (page A-38) 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.8.7 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
<i>email_address</i>	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](#) (page A-38)
- [REGISTER SMTP SERVER](#) (page A-36)
- [LIST ATTRIBUTE OF SMTP SERVER](#) (page A-42)

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.8.8 LIST ATTRIBUTE OF SMTP SERVER

The `LIST ATTRIBUTE OF SMTP SERVER` command displays the current SMTP configuration details used by Audit Vault Server.

Syntax

```
LIST ATTRIBUTE OF SMTP SERVER
```

Usage Notes

To reconfigure the SMTP service connection, run the `ALTER SMTP SERVER` ("[ALTER SMTP SERVER](#) (page A-38)") command.

Example

```
avcli> LIST ATTRIBUTE OF SMTP SERVER;
```

The configuration data/attributes for the SMTP server appear.

A.8.9 DROP SMTP SERVER

The `DROP SMTP SERVER` command unregisters the SMTP Server registered with the Audit Vault Server and removes any associated configuration metadata.

Syntax

```
DROP SMTP SERVER
```

Example

```
avcli> DROP SMTP SERVER;
```

```
SMTP server unregistered successfully.
```

The SMTP Server is unregistered and any associated configuration metadata is removed.

A.9 Security Management AVCLI Commands

The AVCLI security management command enable you to manage various administrator and super administrator privileges.

Table A-14 AVCLI Security Management Commands

Command	Description
ALTER DATA ENCRYPTION (page A-43)	Changes Transparent Data Encryption (TDE) configuration to rekey or to reset the repository encryption password
SHOW DATA ENCRYPTION STATUS (page A-44)	Shows whether data encryption is enabled or disabled for the Audit Vault Server repository
GRANT SUPERADMIN (page A-44)	Grants super administrator privileges to the user specified by <i>username</i>
REVOKE SUPERADMIN (page A-45)	Revokes super administrator privileges from users specified by <i>username</i>
GRANT ACCESS (page A-45)	Grants access to secured target name or secured target group name to specified user
REVOKE ACCESS (page A-46)	Revokes access to secured target or secured target group name from specified user
GRANT ADMIN (page A-46)	Grants administrator privileges to specified user
REVOKE ADMIN (page A-46)	Revokes administrator privileges from specified user
ALTER USER (page A-47)	Unlocks a user account

A.9.1 ALTER DATA ENCRYPTION

The `ALTER DATA ENCRYPTION` command lets a super administrator change the Transparent Data Encryption (TDE) configuration in the 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.9.2 SHOW DATA ENCRYPTION STATUS

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.9.3 GRANT SUPERADMIN

The `GRANT SUPERADMIN` command grants super administrator privileges to the user specified by *username*.

Syntax

```
GRANT SUPERADMIN TO username
```

Arguments

Argument	Description
<i>username</i>	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.9.4 REVOKE SUPERADMIN

The `REVOKE SUPERADMIN` command revokes super administrator privileges from users specified by *username*.

Syntax:

```
REVOKE SUPERADMIN FROM username
```

Arguments

Argument	Description
<i>username</i>	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.9.5 GRANT ACCESS

The `GRANT ACCESS` command grants access to a secured target name or secured target group name to a specified user.

Syntax

```
GRANT ACCESS ON SECURED TARGET secured_target_name TO username
```

```
GRANT ACCESS ON SECURED TARGET GROUP secured_target_group_name TO username
```

Arguments

Argument	Description
<i>username</i>	The specified user.
<i>secured_target_name</i>	The name of the secured target.
<i>secured_target_group_name</i>	The name of the secured target group.

Example

```
avcli> GRANT ACCESS ON SECURED TARGET sample_source TO scott;
```

User `scott` granted access to secured target `sample_source`.

```
avcli> GRANT ACCESS ON SECURED TARGET GROUP hr_db_group TO hr;
```

User `hr` granted access to group of secured targets specified by the group `hr_db_group`.

A.9.6 REVOKE ACCESS

The `REVOKE ACCESS` command revokes access to a secured target or secured target group name from a specified user.

Syntax

```
REVOKE ACCESS ON SECURED TARGET secured_target_name FROM username
```

```
REVOKE ACCESS ON SECURED TARGET GROUP secured_target_group_name FROM username
```

Arguments

Argument	Description
<i>username</i>	The specified user.
<i>secured_target_name</i>	The name of the secured target.
<i>secured_target_group_name</i>	The name of the secured target group.

Example

```
avcli> REVOKE ACCESS ON SECURED TARGET sample_source FROM scott;
```

Access to secured target `sample_source` revoked from user `scott`.

```
avcli> REVOKE ACCESS ON SECURED TARGET GROUP hr_db_group FROM hr;
```

Access to a group of secured targets specified by the group `hr_db_group` revoked from user `hr`.

A.9.7 GRANT ADMIN

The `GRANT ADMIN` command grants administrator privileges to specified user.

Syntax

```
GRANT ADMIN TO username
```

Arguments

Argument	Description
<i>username</i>	The specified user.

Example

```
avcli> GRANT ADMIN TO scott;
```

Administrator privileges granted to user `scott`.

A.9.8 REVOKE ADMIN

The `REVOKE ADMIN` command revokes administrator privileges from specified user.

Syntax:

```
REVOKE ADMIN FROM username
```

Arguments

Argument	Description
<i>username</i>	The specified user.

Example:

```
avcli> REVOKE ADMIN FROM scott;
```

Administrator privileges revoked from user *scott*.

A.9.9 ALTER USER

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.

A.10 SAN Storage AVCLI Commands

[Table A-15](#) (page A-47) lists SAN storage AVCLI commands.

Table A-15 AVCLI SAN Storage Commands

Command	Description
REGISTER SAN SERVER (page A-48)	Registers a SAN server of a specified storage type with the Audit Vault Server
ALTER SAN SERVER (page A-49)	Alters a SAN server registered with the Audit Vault Server by logging into or logging out of a target available on the SAN server
LIST TARGET FOR SAN SERVER (page A-50)	Displays the details of targets available on a specified SAN server
DROP SAN SERVER (page A-50)	Drops a SAN server registered with Audit Vault Server
LIST DISK (page A-50)	Displays details of disks available on the system
ALTER DISKGROUP (page A-51)	Alters a diskgroup by adding or dropping disks
LIST DISKGROUP (page A-51)	Displays details of all diskgroups in the system
LIST SAN SERVER (page A-52)	Displays details of SAN servers registered with the Audit Vault Server

Table A-15 (Cont.) AVCLI SAN Storage Commands

Command	Description
SHOW iSCSI INITIATOR DETAILS FOR SERVER (page A-52)	Displays iSCSI initiator details for the Audit Vault Server

A.10.1 REGISTER SAN 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
<i>SAN_server_name</i>	Name of the SAN server. Must be unique.
<i>storage_type</i>	Storage type. Currently, only iSCSI is supported (case-insensitive).
<i>address</i>	IP address SAN server
<i>port</i>	Optional. Port number. Default is 3260.
<i>discovery_method</i>	Optional. Method used to discover targets. Possible values are: SENDTARGETS [AUTHENTICATED BY <i>username/password</i>] ISNS Default is SENDTARGETS.



Note:

The syntax of this command will be changed in Oracle Audit Vault and Database Firewall release 20.1.0.0.0.

Examples:

```
avcli> REGISTER SAN SERVER testServer1 OF TYPE iSCSI ADDRESS 192.0.2.1;
```

Registers a SAN server `testServer1` of storage type `iSCSI` at address `192.0.2.1`. The default port number `3260` and the default discovery method `sendtargets` will be used.

```
avcli> REGISTER SAN SERVER testServer2 Of Type iSCSI ADDRESS 192.0.2.1 METHOD sendtargets AUTHENTICATED BY username2/password2;
```

Registers a SAN server `testServer2` of storage type `iSCSI` at address `192.0.2.1` using the discover method `sendtargets` with credentials `username2` and `password2`.

A.10.2 ALTER SAN SERVER

Use the `ALTER 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 `ALTER SAN SERVER` command alters a SAN server registered with the Audit Vault Server by logging in or logging out of a target available on the SAN server.

Syntax:

```
ALTER SAN SERVER server_name LOGIN target_name ADDRESS address [PORT port]
[AUTHENTICATED BY username/password] [ON SECONDARY]
```

```
ALTER SAN SERVER server_name LOGOUT target_name ADDRESS address [PORT port]
[AUTHENTICATED BY username/password] [ON SECONDARY]
```

Use the `[ON SECONDARY]` option in a high availability configuration to apply this command to secondary Audit Vault Server.

Arguments

Argument	Description
<i>server_name</i>	Name of the SAN server registered with the Audit Vault Server.
<i>target_name</i>	Name of the target on the SAN server. To get a list of targets, use the command " LIST TARGET FOR SAN SERVER (page A-50)".
<i>address</i>	IP address or hostname of the target on the SAN server
<i>port</i>	Optional. Default is 3260.
<i>username/password</i>	If needed, credential used to log in to the target.



Note:

The syntax of this command will be changed in Oracle Audit Vault and Database Firewall release 20.1.0.0.0.

Example:

```
avcli> ALTER SAN SERVER testServer1 LOGIN target1 ADDRESS sample_target.example.com
AUTHENTICATED BY username1/password1;
```

Alter the SAN server `testServer1` by logging into `target1` at address `sample_target.example.com` using credentials `username1` and `password1`. The default port number 3260 will be used.

```
avcli> ALTER SAN SERVER testServer2 LOGOUT target2 ADDRESS sample_target.example.com;
```

Alter the SAN server `testServer2` by logging out of `target2` at address `sample_target.example.com`.

A.10.3 LIST TARGET FOR 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
<i>server_name</i>	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.10.4 DROP SAN 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
<i>server_name</i>	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.10.5 LIST DISK

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.10.6 ALTER DISKGROUP

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
<i>disk_name</i>	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 (page A-50)".

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.10.7 LIST DISKGROUP

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](#) (page A-50)".

A.10.8 LIST SAN SERVER

The LIST SAN SERVER command displays details of SAN servers registered with the Audit Vault Server.

Syntax:

```
LIST SAN SERVER [ON SECONDARY]
```

Use the [ON SECONDARY] option in a high availability configuration to apply this command to secondary Audit Vault Server.

Example:

```
avcli> LIST SAN SERVER;
```

Displays details of SAN servers registered in the system, for example, storage name, storage type, etc.

A.10.9 SHOW iSCSI INITIATOR DETAILS FOR SERVER

The SHOW iSCSI INITIATOR DETAILS FOR SERVER command displays iSCSI initiator details for the Audit Vault Server. These initiator details are used in the SAN server configuration to allow it to connect to the Audit Vault Server.

Syntax:

```
SHOW iSCSI INITIATOR DETAILS FOR SERVER [ON SECONDARY]
```

Use the [ON SECONDARY] option in a high availability configuration to apply this command to secondary Audit Vault Server.

Example:

```
avcli> SHOW iSCSI INITIATOR DETAILS FOR SERVER;
```

Displays the iSCSI initiator details for the Audit Vault Server.

A.11 Remote File System AVCLI Commands

Table A-16 (page A-53) lists the remote filesystem AVCLI commands. Currently these commands support registering and managing connections to NFS filesystems that are used as archive locations.

Table A-16 AVCLI Remote Filesystem Commands

Command	Description
REGISTER REMOTE FILESYSTEM (page A-53)	Registers a remote filesystem with the Audit Vault Server
ALTER REMOTE FILESYSTEM (page A-54)	Alters a remote filesystem registered with the Audit Vault Server
DROP REMOTE FILESYSTEM (page A-55)	Drops a remote filesystem registered with the Audit Vault Server
LIST EXPORT (page A-55)	Displays the list of exports available on an NFS server
LIST REMOTE FILESYSTEM (page A-55)	Lists all remote filesystems registered with the Audit Vault Server
SHOW STATUS OF REMOTE FILESYSTEM (page A-56)	Shows the status of a remote filesystem registered with the Audit Vault Server

A.11.1 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 filesystem with the Audit Vault Server. This command currently supports registering an NFS filesystem. After registering a remote filesystem, an administrator can select it when specifying an archive location.

Syntax:

```
REGISTER REMOTE FILESYSTEM filesystem_name OF TYPE NFS ON HOST NFS_server_address
USING EXPORT export [MOUNT]
```

Arguments

Argument	Description
<i>filesystem_name</i>	A unique name for the remote filesystem
<i>NFS_server_address</i>	Hostname or IP address of the NFS server
<i>export</i>	Name of the export directory on the NFS server. This directory must be created in <code>etc/exports</code> file of the NFS server.

 **Note:**

1. Log in as *Oracle* user 503 to register the remote filesystem. 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 sample_FileSystem OF TYPE NFS ON HOST
example_host.example.com USING EXPORT /export/home1;
```

Registers a remote NFS filesystem named `sample_FileSystem` on the host `example_host.example.com` using the export directory `/export/home1`. This will mount the registered remote filesystem.

```
avcli> REGISTER REMOTE FILESYSTEM sample_FileSystem OF TYPE NFS ON HOST
example_host.example.com USING EXPORT /export/home1 MOUNT;
```

Registers a remote NFS filesystem named `sample_FileSystem` on the host `example_host.example.com` using the export directory `/export/home1`. This will also mount the registered remote filesystem.

A.11.2 ALTER REMOTE FILESYSTEM

The `ALTER REMOTE FILESYSTEM` command alters a remote filesystem registered with the Audit Vault Server.

Syntax:

```
ALTER REMOTE FILESYSTEM filesystem_name SET {key=value [,key=value...]}
```

```
ALTER REMOTE FILESYSTEM filesystem_name MOUNT
```

```
ALTER REMOTE FILESYSTEM filesystem_name UNMOUNT [FORCE]
```

Arguments

Argument	Description
<i>filesystem_name</i>	Name of the remote filesystem
<i>key</i>	For an NFS remote filesystem, the <i>key</i> 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.11.3 DROP REMOTE FILESYSTEM

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
<i>filesystem_name</i>	Name of the remote filesystem.

Examples:

```
avcli> DROP REMOTE FILESYSTEM filesystem1;
```

Drops the remote filesystem `filesystem1`.

A.11.4 LIST EXPORT

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
<i>address</i>	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.11.5 LIST REMOTE FILESYSTEM

The `LIST REMOTE FILESYSTEM` command lists all remote filesystems registered with the Audit Vault Server.

Syntax:

```
LIST REMOTE FILESYSTEM
```

Example:

```
avcli> LIST REMOTE FILESYSTEM;
```

Lists all remote filesystems registered with the Audit Vault Server.

A.11.6 SHOW STATUS OF REMOTE FILESYSTEM

The `SHOW STATUS OF REMOTE FILESYSTEM` command shows the status of a specified remote filesystem.

Syntax:

```
SHOW STATUS OF REMOTE FILESYSTEM filesystem_name
```

Arguments

Argument	Description
<i>filesystem_name</i>	Name of the remote filesystem

Examples:

```
avcli> SHOW STATUS OF REMOTE FILESYSTEM filesystem1;
```

Shows the status of remote filesystem `filesystem1`.

A.12 Server Management AVCLI Commands

Table A-17 AVCLI Server Management Commands

Command	Description
ALTER SYSTEM SET (page A-56)	Modifies system configuration data
SHOW CERTIFICATE (page A-58)	Displays the certificate for the Audit Vault Server
DOWNLOAD LOG FILE (page A-59)	Downloads the Audit Vault Server log file for diagnostics

A.12.1 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
<i>attribute</i>	System attributes as key/value pairs. See Table A-18 (page A-57).

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-18 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: <i>component_name:loglevel_value</i> See Table A-19 (page A-57) 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 will retry starting failed audit trails. Default: 5

[Table A-19](#) (page A-57) shows valid values for *component_name* and *loglevel_value* for the LOGLEVEL attribute:

Table A-19 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

Table A-19 (Cont.) Logging component names and values

Logging component name	Values
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-20 Logging level and values

Parameter	Description
ERROR	The ERROR log level
WARNING	The WARNING log level (not supported for GUIlog)
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 the Audit Vault Server \(page 14-3\)](#) for information about generating a diagnostics report that captures Audit Vault Server appliance information.

A.12.2 SHOW CERTIFICATE

The SHOW CERTIFICATE command displays the certificate for the Audit Vault Server.

Syntax

```
SHOW CERTIFICATE FOR SERVER
```

Example

```
avcli> SHOW CERTIFICATE FOR SERVER;
```

The Audit Vault Server certificate appears.

A.12.3 DOWNLOAD LOG FILE

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 Collection Plug-In AVCLI Commands

The AVCLI collection plug-in commands enable you to manage the deployment of collection plug-ins.

[Table A-13](#) (page A-36) lists the collection plug-in AVCLI commands.

Table A-21 AVCLI Collection Plug-In Commands

Command	Description
DEPLOY PLUGIN (page A-59)	Deploys a plug-in into Audit Vault Server home from a given archive file
LIST PLUGIN FOR SECURED TARGET TYPE (page A-60)	Lists all the plug-ins in an Audit Vault Server installation
UNDEPLOY PLUGIN (page A-61)	Undeploys a plug-in from an Audit Vault Server home

A.13.1 DEPLOY PLUGIN

The `DEPLOY PLUGIN` command deploys a plug-in into the Audit Vault Server home from a given archive file.

Syntax

```
DEPLOY PLUGIN plugin archive
```


Arguments

Argument	Description
<i>plugin archive</i>	The plug-in archive. Archive files have an <code>.zip</code> extension, specifying custom plug-ins that third-party vendors or partners develop to add functionality to Audit Vault Server.

Usage Notes

No action is required after this command.

The `DEPLOY PLUGIN` command updates the agent archive with the contents of this plug-in for future Agent deployments.

When a newer version of the plug-in is available, use the `DEPLOY PLUGIN` command to update the plug-in artifacts. Multiple plug-ins can support a single secured target type.

Example

```
avcli> DEPLOY PLUGIN /opt/avplugins/sample_plugin.zip;
```

Deploys the plug-in at `/opt/avplugins/sample_plugin.zip` into the Audit Vault Server and updates the agent archive by adding the plug-in to its contents.

A.13.2 LIST PLUGIN FOR SECURED TARGET TYPE

The `LIST PLUGIN FOR SECURED TARGET TYPE` command lists all the plug-ins that support a particular secured target type.

Syntax

```
LIST PLUGIN FOR SECURED TARGET TYPE secured target type name
```

Arguments

Argument	Description
<i>secured target type name</i>	The name of the secured target type

Usage Notes

To find a list of available secured target types, see "[LIST SECURED TARGET TYPE \(page A-22\)](#)".

Examples

```
avcli> LIST PLUGINS FOR SECURED TARGET TYPE "Oracle Database";
```

The plug-ins that support the secured target type "Oracle Database" are listed.

A.13.3 UNDEPLOY PLUGIN

The `UNDEPLOY PLUGIN` command deletes a plug-in from an Audit Vault Server home.

Syntax

```
UNDEPLOY PLUGIN plugin_id
```

Arguments

Argument	Description
<i>plugin_id</i>	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.14 General Usage AVCLI Commands

[Table A-22](#) (page A-61) lists the general usage AVCLI commands.

Table A-22 AVCLI HELP and EXIT Commands

Command	Description
CONNECT (page A-62)	Connects the current user in AVCLI as a different user
STORE CREDENTIALS (page A-62)	Stores administrator credentials in the AVCLI wallet, or overwrites previously stored credentials.
SHOW USER (page A-63)	Displays the currently logged in AVCLI user
CLEAR LOG (page A-63)	Clears the systems's diagnostic logs
HELP (page A-63)	Lists all AVCLI commands with their categories
-HELP (page A-63)	Displays help information for all of the commands in the AVCLI utility

Table A-22 (Cont.) AVCLI HELP and EXIT Commands

Command	Description
-VERSION (page A-64)	Displays the version number for AVCLI
QUIT (page A-65)	Exits AVCLI

A.14.1 CONNECT

The `CONNECT` command enables you to connect as a different user in AVCLI.

Syntax

```
CONNECT [username]
```

Usage Notes

- If you have logged into to AVCLI without specifying a username and password, then you must use the `CONNECT` command to connect as a valid user.
- For additional ways to connect to AVCLI, see "[Using the Audit Vault Command-Line Interface](#) (page 1-15)".

Example 1

```
avcli> CONNECT psmith;
Enter password: password
```

Connected.

Example 2

```
avcli> CONNECT;
Enter user name: username
Enter password: password
```

Connected.

A.14.2 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.14.3 SHOW USER

The `SHOW USER` command displays the currently logged in AVCLI user.

Syntax

```
SHOW USER
```

Example

```
avcli> SHOW USER;
```

A.14.4 CLEAR LOG

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.14.5 HELP

The `HELP` command lists all available AVCLI commands and their categories.

Syntax

```
HELP
```

Example

```
avcli> HELP;
```

A.14.6 -HELP

The `-HELP` command displays version number and help information about the AVCLI commands. Run the `-HELP` command from outside of AVCLI.

Syntax

```
avcli -h
avcli -H
avcli -help
avcli -HELP
```

Example

```
avcli -help:
```

```
[oracle@slc02vjp ~]$ avcli -help
```

```
AVCLI : Release 12.2.0.0.0 - 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.14.7 -VERSION

The `-VERSION` command displays the version number for AVCLI. Run the `-VERSION` command from outside of AVCLI.

Syntax

```
avcli -v
avcli -V
avcli -version
avcli -VERSION
```

Example

```
avcli -v;
```

AVCLI : Release 12.2.0.0.0 - Production on Tue Apr 26 14:25:31 PDT 2011

Copyright (c) 2014, Oracle. All Rights Reserved.

A.14.8 QUIT

The `QUIT` command exits AVCLI.

Syntax

```
QUIT
```

Example

```
avcli> QUIT;
```

A.15 AVCLI User Commands

You can use the AVCLI user commands to create user, assign necessary roles, reset password, and delete the user.

Table A-23 AVCLI User Commands

Command	Description
CREATE AUDITOR (page A-65)	To create a user with <i>auditor</i> role. Only a <i>superauditor</i> can create a user with <i>auditor</i> role.
ALTER AUDITOR (page A-66)	To reset the password for existing <i>auditor</i> or <i>superauditor</i> user. Only a <i>superauditor</i> can reset password for <i>auditor</i> or <i>superauditor</i> user.
DROP AUDITOR (page A-67)	To drop or delete an existing <i>auditor</i> or <i>superauditor</i> user. Only a <i>superauditor</i> can drop an <i>auditor</i> or <i>superauditor</i> user.
CREATE ADMIN (page A-67)	To create a user with <i>admin</i> role. Only a <i>superadmin</i> can create a user with <i>admin</i> role.
ALTER ADMIN (page A-68)	To reset the password for existing <i>admin</i> or <i>superadmin</i> user. Only a <i>superadmin</i> can reset password for <i>admin</i> or <i>superadmin</i> user.
DROP ADMIN (page A-68)	To drop or delete an existing <i>admin</i> or <i>superadmin</i> user. Only a <i>superadmin</i> can drop an <i>admin</i> or <i>superadmin</i> user.

A.15.1 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
<i>user name</i>	The name of the user being created with <i>auditor</i> role. The <i>user name</i> 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 (#).
<i>password</i>	The command prompts a password before creating a user with <i>auditor</i> 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.

A.15.2 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
<i>user name</i>	The existing user with <i>auditor</i> role who requires a password reset.
<i>password</i>	The command prompts a password for modifying the password of the user with <i>auditor</i> 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.

A.15.3 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
<i>user name</i>	The existing user with <i>auditor</i> 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.15.4 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
<i>user name</i>	The name of the user being created with <i>admin</i> role. The <i>user name</i> 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 (<code>_</code>), dollar sign (<code>\$</code>), and pound sign (<code>#</code>).
<i>password</i>	The command prompts a password before creating a user with <i>admin</i> role. The password must have at least one uppercase letter, one lowercase letter, one digit(0-9), and one special character(<code>.,+;!_</code>). 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.

A.15.5 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
<i>user name</i>	The existing user with <i>admin</i> role who requires a password reset.
<i>password</i>	The command prompts a password for modifying the password of the user with <i>admin</i> 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.

A.15.6 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
<i>user name</i>	The existing user with <i>admin</i> 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.

B

Plug-in Reference

Topics

- [About Oracle Audit Vault and Database Firewall Plug-ins](#) (page B-1)
- [Plug-ins Shipped with Oracle Audit Vault and Database Firewall](#) (page B-1)
- [Scripts for Oracle AVDF Account Privileges on Secured Targets](#) (page B-21)
- [Audit Collection Consideration](#) (page B-31)
- [Audit Trail Cleanup](#) (page B-32)
- [Procedure Look-ups: Connect Strings, Collection Attributes, Audit Trail Locations](#) (page B-36)

B.1 About Oracle Audit Vault and Database Firewall Plug-ins

Oracle Audit Vault and Database Firewall supports different types of secured targets by providing a plug-in for each secured 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.

This appendix contains high-level data for each plug-in shipped with Oracle Audit Vault and Database Firewall. The appendix also contains look-up information you will need to complete the procedures for registering secured targets and configuring audit trails. These procedures link directly to the relevant section of this appendix.

See Also:

- *Oracle Big Data Appliance Owner's Guide*. Oracle Audit Vault and Database Firewall also supports Oracle Big Data Appliance as a secured target.
- [Deploying Plug-ins and Registering Plug-in Hosts](#) (page 5-13)

B.2 Plug-ins Shipped with Oracle Audit Vault and Database Firewall

This section describes each plug-in shipped with Oracle Audit Vault and Database Firewall.



See Also:

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

In addition, you can find platform information for prior releases in **Article 1536380.1** at My Oracle Support.

Topics

- [Out-of-the Box Plug-ins at a Glance](#) (page B-2)
- [Oracle Database](#) (page B-4)
- [Microsoft SQL Server](#) (page B-6)
- [Sybase ASE](#) (page B-8)
- [Sybase SQL Anywhere](#) (page B-9)
- [IBM DB2](#) (page B-9)
- [MySQL](#) (page B-10)
- [Oracle Solaris](#) (page B-12)
- [Linux](#) (page B-12)
- [IBM AIX](#) (page B-14)
- [Microsoft Windows](#) (page B-15)
- [Microsoft Active Directory](#) (page B-15)
- [Oracle ACFS](#) (page B-16)
- [Oracle Big Data Appliance](#) (page B-16)
- [Summary of Data Collected for Each Audit Trail Type](#) (page B-17)

B.2.1 Out-of-the Box Plug-ins at a Glance

Oracle Audit Vault and Database Firewall out-of-the-box plug-ins support the secured target versions listed in [Table B-1](#) (page B-2). Click the link for each secured target to get detailed information.

Table B-1 Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall

Secured Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor	Database Interrogation
Oracle Database (page B-4)	No	No	No	No	Yes	No	No

9i

Table B-1 (Cont.) Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall

Secured Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor	Database Interrogation
Oracle Database (page B-4) 10g, 11g, 12c	Yes	Yes (except Unified Audit Policies)	Yes	Yes	Yes	Yes	Yes
Oracle Database (page B-4) 18c (18.3) in release 12.2.0.9.0 and later	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Oracle Database (page B-4) 19c in release 12.2.0.11.0 and later	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft SQL Server (page B-6) 2008, 2008 R2, 2012, 2014, 2016	Yes	No	Yes (Versions 2000, 2005, 2008, 2008 R2)	Yes	Yes	Yes (on Windows 2008 and onwards)	Yes (Microsoft SQL Server 2005, 2008, 2008 R2)
Sybase ASE (page B-8) 12.5.4 to 15.7	Yes	No	Yes	No	Yes	Yes	No
Sybase SQL Anywhere (page B-9) 10.0.1	No	No	Yes	No	Yes	Yes	Yes
IBM DB2 (page B-9) 9.5 - 11.1	Yes	No	Yes	No	Yes (Versions 9.1 - 10.5)	Yes	No
MySQL (page B-10) 5.5 - 5.7	Yes	No	Yes	Yes	Yes	Yes	No
Oracle Solaris (page B-12) 10 and 11, on SPARC64 and x86-64 platforms	Yes	No	No	No	No	Yes (Versions 11, 11.1, 11.2)	No
Oracle Solaris - other versions, see Note below.	Yes	No	No	No	No	No	No
Oracle Linux (page B-12) 5.8, 6.0 - 6.9, 7.0 - 7.3	Yes	No	No	No	No	Yes	No

Table B-1 (Cont.) Out-of-the-Box Plug-ins and Features Supported in Oracle Audit Vault and Database Firewall

Secured Target Version	Audit Trail Collection	Audit Policy Creation, Entitlement Auditing	Stored Procedure Auditing	Audit Trail Cleanup	Database Firewall	Host Monitor	Database Interrogation
Red Hat Enterprise Linux (page B-12) 6.7 - 6.9 7.0 - 7.3	Yes	No	No	No	No	Yes	No
SUSE Linux Enterprise Server 11-12	No	No	No	No	No	Yes	No
IBM AIX (page B-14) 6.1 - 7.2 on Power Systems (64-bit)	Yes	No	No	Yes	No	Yes	No
Microsoft Windows (page B-15) Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, and 2016 on x86-64	Yes	No	No	No	No	No	No
Microsoft Active Directory (page B-15) 2008, 2008 R2, 2012, and 2016 on 64 bit	Yes	No	No	No	No	No	No
Oracle ACFS (page B-16) 12c Release 1 (12.1)	Yes	No	No	No	No	No	No
Oracle Big Data Appliance (page B-16) 2.3, 4.3	Yes	No	No	No	No	No	No



Note:

Audit data can also be collected from Solaris version 2.3 or later (contact Oracle Support for guidance).

B.2.2 Oracle Database

[Table B-2](#) (page B-5) lists features of the Oracle Database Plug-in.

Table B-2 Oracle Database Plug-in


Plug-in Specification	Description
Plug-in directory	<code>AGENT_HOME/av/plugins/com.oracle.av.plugin.oracle</code>
Secured Target Versions	Oracle 10g Oracle 11g Oracle 12c Release 1 (12.1) Oracle 12c Release 2 (12.2)
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>Oracle 12c Release 2 (12.2) as a secured target is supported from Oracle Audit Vault and Database Firewall release 12.2.0.4.0 and onwards for audit data collection.</p> </div>
	18c (18.3) in release 12.2.0.9.0 and later 19c in release 12.2.0.11.0 and later
Secured Target Platforms	Linux/x86-64 Solaris /x86-64 Solaris /SPARC64 AIX/Power64 Windows /x86-64 HP-UX Itanium See Audit Vault Agent: Supported Platforms and Versions in <i>Oracle Audit Vault and Database Firewall Installation Guide</i> for complete details on supported target platforms and versions.
Setup Script(s)	Yes. See " Oracle Database Setup Scripts (page B-22)" for instructions.
Secured Target Location (Connect String)	<code>jdbc:oracle:thin:@//hostname:port/service</code>
Collection Attribute(s)	ORLCOLL.NLS_LANGUAGE ORLCOLL.NLS_TERRITORY ORLCOLL.NLS_TERRITORY ORLCOLL.MAX_PROCESS_TIME ORLCOLL.MAX_PROCESS_RECORDS ORLCOLL.RAC_INSTANCE_ID ORLCOLL.HEARTBEAT_INTERVAL ORLCOLL.HEARTBEAT_INTERVAL
	See Table B-19 (page B-39) for details.

Table B-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 B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	For TABLE audit trails: SYS.AUD\$, SYS.FGA_LOG\$, DVSYS.AUDIT_TRAIL\$, UNIFIED_AUDIT_TRAIL 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 TRANSACTION LOG, EVENT LOG, and NETWORK audit trails: no trail location required. 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 (page B-33) for instructions.
OS user running the Agent	For Oracle Database Directory Audit Trail: Any user who has <i>read</i> permission on audit files, i.e <i>oracle</i> user, or user in DBA group. For Table Trail: Any database user (preferably not DBA). For any other directory audit trail: Any user who has <i>read</i> permission on audit files.
Cluster support	Yes

B.2.3 Microsoft SQL Server

[Table B-3](#) (page B-6) lists the features of the Microsoft SQL Server plug-in.

Table B-3 Microsoft SQL Server Plug-in

Plug-in Specification	Description
Plug-in directory	<code>AGENT_HOME\av\plugins\com.oracle.av.plugin.mssql</code>
Secured Target Versions	Enterprise Edition 2000, 2005, 2008, 2008 R2, 2012, 2014. Enterprise Edition 2016 is supported in release 12.2.0.2.0 and later. Enterprise Edition 2017 is supported in release 12.2.0.10.0 and later.

Table B-3 (Cont.) Microsoft SQL Server Plug-in

Plug-in Specification	Description
Secured Target Platforms	Windows/x86-64 See Audit Vault Agent: Supported Platforms and Versions in <i>Oracle Audit Vault and Database Firewall Installation Guide</i> for complete details on supported target platforms and versions.
Setup Script(s)	Yes. " Microsoft SQL Server Setup Scripts (page B-27)" for instructions.
Secured Target Location (Connect String for SQL server authentication)	<code>jdbc:av:sqlserver://hostname:port</code>
Secured Target Location (Connect String for Windows Authentication)	<code>jdbc:av:sqlserver://<Host Name>:<Port>;authenticationMethod=ntlmjava</code> Use Windows user credentials along with domain. For example: <code><domain name>\<user name > and password</code>
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY EVENT LOG NETWORK See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	For DIRECTORY audit trail: <code>*.sqlaudit</code> files, or <code>*.trc</code> (trace) files. Examples: <code>directory_path*.sqlaudit</code> <code>directory_path\prefix*.sqlaudit</code> <code>directory_path\prefix*.trc</code> For <i>prefix</i> , you can use any prefix for the <code>.trc</code> or <code>*.sqlaudit</code> files. #C2_DYNAMIC and #TRACE_DYNAMIC are only supported for SQL Server 2000, 2005, and 2008 versions. For EVENT LOG audit trail: <ul style="list-style-type: none"> • application • security (SQL Server 2008 and 2012 only)
Audit Trail Cleanup Support	Yes. See " SQL Server Audit Trail Cleanup (page B-34)" for instructions.
Cluster support	Yes
Secured Target Platform for Cluster	Windows 2012 R2 Version 2012 R2 for audit collection on Windows platform, starting <i>Oracle Audit Vault and Database Firewall</i> release 12.2.0.12.0
Cluster Collection Attribute	Attribute Name: <code>av.collector.clusterEnabled</code> Attribute Value: 1



Note:

Oracle Audit Vault and Database Firewall does not support audit collection and Database Firewall monitoring of Microsoft SQL Server cluster.

B.2.4 Sybase ASE

Table B-4 (page B-8) lists the features of the Sybase ASE plug-in.

Table B-4 Sybase ASE Plug-in

Plug-in Specification	Description
Plug-in directory	<i>AGENT_HOME</i> /av/plugins/com.oracle.av.plugin.sybase
Target Versions	15.7 16.0 is supported in release 12.2.0.11.0 and later.
Secured Target Platforms	All platforms
Setup Script(s)	Yes. See " Sybase ASE Setup Scripts (page B-24)" for instructions.
Secured Target Location (Connect String)	<code>jdbc:av:sybase://hostname:port</code>
Collection Attribute(s)	None
AVDF Audit Trail Types	TABLE NETWORK See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	SYSAUDITS
Audit Trail Cleanup Support	No
Cluster support	No

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 Sybase server version 16.0.

3. Restart the Audit Vault Agent.
4. Start the collection.

B.2.5 Sybase SQL Anywhere

[Table B-5](#) (page B-9) lists the features of the Sybase SQL Anywhere plug-in.

Table B-5 Sybase SQL Anywhere Plug-in

Plug-in Specification	Description
Plug-in directory	<i>AGENT_HOME/av/plugins/com.oracle.av.plugin.sqlanywhere</i>
Secured Target Versions	10.0.1
Secured Target Platforms	All platforms
Setup Script(s)	Yes. See " Sybase SQL Anywhere Setup Scripts (page B-26)" for instructions.
Secured Target Location (Connect String)	<i>jdbc:av:sybase://hostname:port</i>
Collection Attributes	None
AVDF Audit Trail Types	NETWORK (used for host monitoring only) See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	Not required
Audit Trail Cleanup Support	No

B.2.6 IBM DB2

[Table B-6](#) (page B-9) lists the features of the IBM DB2 plug-in.

Table B-6 IBM DB2 Plug-in

Plug-in Specification	Description
Plug-in directory	<i>AGENT_HOME/av/plugins/com.oracle.av.plugin.db2</i>
Secured Target Versions	9.1 - 11.1
Secured Target Platforms	Linux (x86-64): OL 5.x, 6.x, 7.x and RHEL 5.x, 6.x, 7.x Microsoft Windows (x86-64): 8 Microsoft Windows Server (x86-64): 2008, 2008R2, 2012, 2012R2, 2016 IBM AIX on Power Systems (64-bit): 7.1 is supported from release 12.2.0.12.0 and onwards
Setup Script(s)	Yes. See " IBM DB2 for LUW Setup Scripts (page B-29)" for instructions.
Secured Target Location (Connect String)	<i>jdbc:av:db2://hostname:port/dbname</i> Note: <ul style="list-style-type: none"> • Connect string is not required from release 12.2.0.11.0 and onwards. • Connect string is not required for IBM DB2 cluster.

Table B-6 (Cont.) IBM DB2 Plug-in

Plug-in Specification	Description
Collection Attribute(s)	<code>av.collector.databasesname</code> (case sensitive) - (Required) Specifies the IBM DB2 for LUW database name.
AVDF Audit Trail Types	DIRECTORY NETWORK See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	Path to a directory, for example: <code>d:\temp\trace</code>
Audit Trail Cleanup Support	No
Cluster Support	Yes HADR (High Availability and Disaster Recovery)
Secured Target Platform for Cluster	HADR on OL 7.x

B.2.7 MySQL

[Table B-7](#) (page B-10) lists the features of the MySQL plug-in.

Table B-7 MySQL Plug-in

Plug-in Specification	Description
Plug-in directory	<code>AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql</code>
Secured Target Versions	For Database Firewall: Enterprise Edition 5.0, 5.1, 5.5, 5.6. For audit data collection the following Enterprise Edition versions are supported: <ul style="list-style-type: none"> • 5.5.29 to 5.5.59 • 5.6.10 to 5.6.39 • 5.7.0 to 5.7.21 (supported in release 12.2.0.7.0 and later) • 8.0 (supported in release 12.2.0.11.0 and later)
Secured Target Platforms	Linux (x86-64): OL 5.x, 6.x, 7.x and RHEL 5.x, 6.x, 7.x Microsoft Windows (x86-64): 8 Microsoft Windows Server (x86-64): 2008, 2008R2, 2012, 2012R2, 2016
Setup Script(s)	Yes. See " MySQL Setup Scripts (page B-31)".
Secured Target Location (Connect String)	<code>jdbc:av:mysql://hostname:port/mysql</code> Note: Connect string is not required from release 12.2.0.11.0 and onwards.
Collection Attributes	<code>av.collector.securedTargetVersion</code> - (Required) Specifies the MySQL version. Default is 8.0. <code>av.collector.AtcTimeInterval</code> - (Optional) Specifies the audit trail cleanup file update time interval in minutes. Default is 20. Note: Collection Attribute <code>av.collector.securedTargetVersion</code> is not required from release 12.2.0.11.0 and onwards.

Table B-7 (Cont.) MySQL Plug-in

Plug-in Specification	Description
AVDF Audit Trail Types	DIRECTORY NETWORK See Table B-17 (page B-18) 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 B-8 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 B-9 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.

 **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:**

- [Converting Audit Record Format For Collection](#) (page 6-14)
- [MySQL Audit Trail Cleanup](#) (page B-35)

B.2.8 Oracle Solaris

[Table B-10](#) (page B-12) lists the features of the Oracle Solaris plug-in.

Table B-10 Oracle Solaris Plug-in

Plug-in Specification	Description
Plug-in directory	<code>AGENT_HOME/av/plugins/com.oracle.av.plugin.solaris</code>
Secured Target Versions	Version 10, Version 11, on SPARC64 and x86-64 platforms
Secured Target Platforms	Solaris/x86-64 Solaris/SPARC64
Setup Script(s)	No
Secured Target Location (Connect String)	<code>hostname</code> (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	<code>hostname:path_to_trail</code> The <code>hostname</code> matches the hostname in the audit log names, which look like this: <code>timestamp1.timestamp2.hostname</code>
Audit Trail Cleanup Support	No

B.2.9 Linux

[Table B-11](#) (page B-13) lists the features of the Linux plug-in that collects audit data from Oracle Linux (OL) and Red Hat Enterprise Linux (RHEL).

Table B-11 Linux Plug-in

Plug-in Specification	Description
Plug-in directory	<code>AGENT_HOME/av/plugins/com.oracle.av.plugin.linux</code>
Secured Target Versions	<p>Oracle Linux (OL)</p> <ul style="list-style-type: none"> • OL 5.8 (with auditd package 1.8) • 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 - 6.10 (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) <p>Red Hat Enterprise Linux (RHEL)</p> <ul style="list-style-type: none"> • 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) <p>Run <code>rpm -q audit</code> to get the audit package version.</p>
Secured Target Platforms	Linux/x86-64
Setup Script(s)	<p>No. However, the following user/group access rights are needed to start a Linux audit trail:</p> <p>If the agent process is started with <code>root</code> user, no changes to access rights are needed.</p> <p>If the agent process is started with a user other than <code>root</code>:</p> <ol style="list-style-type: none"> 1. Assign the group name of the Agent user (the one who will start the Agent process) to the <code>log_group</code> parameter in the <code>/etc/audit/auditd.conf</code> file. 2. The Agent user and group must have read and execute permissions on the folder that contains the <code>audit.log</code> file (default folder is <code>/var/log/audit</code>). 3. Restart the Linux audit service after you make the above changes.
Secured Target Location (Connect String)	<code>hostname</code> (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	<p>DIRECTORY</p> <p>See Table B-17 (page B-18) for descriptions of audit trail types.</p>

Table B-11 (Cont.) Linux Plug-in

Plug-in Specification	Description
Audit Trail Location	Default location of <code>audit.log</code> (<code>/var/log/audit/audit*.log</code>) or any custom location configured in the <code>/etc/audit/auditd.conf</code> file
Audit Trail Cleanup Support	No

B.2.10 IBM AIX

[Table B-12](#) (page B-14) lists the features of the IBM AIX plug-in.

Table B-12 IBM AIX Plug-in

Plug-in Specification	Description
Plug-in directory	<code>AGENT_HOME/av/plugins/com.oracle.av.plugin.aixos</code>
Secured Target Versions	AIX 6.1 - 7.2
Secured Target Platforms	Power Systems (64-bit)
Setup Script(s)	<p>No. However, the following user/group access rights are needed to start an AIX audit trail:</p> <p>If the Agent process is started with <code>root</code> user, no changes to access rights are needed.</p> <p>If the Agent process is started with a user other than <code>root</code>, run the following commands in the AIX system as <code>root</code> to authorize another user:</p> <ol style="list-style-type: none"> 1. Create a new role and grant it <code>aix.security.audit</code> authorization: <pre>mkrole authorizations= (aix.security.audit) (role_name)</pre> 2. Alter the Agent user to assign the newly created role: <pre>chuser roles=role_name agent_user_name</pre> 3. Update the kernel table with the newly created role by running the command: <code>setkst</code> 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 <code>/audit</code> directory where the audit trail files are located. 6. To start the Agent with the Agent user, log in to the AIX terminal with <code>agent_user_name</code> and switch to the role created in this procedure: <pre>swrole role_name</pre>
Secured Target Location (Connect String)	<code>hostname</code> (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	DIRECTORY See Table B-17 (page B-18) for descriptions of audit trail types.

Table B-12 (Cont.) IBM AIX Plug-in

Plug-in Specification	Description
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: <i>AGENT_HOME/av/atc/SecuredTargetName_TrailId.atc</i> The .atc file contains the following information: <i>trail_location end_time_of_audit_event_collection</i>

B.2.11 Microsoft Windows

[Table B-13](#) (page B-15) lists the features of the Microsoft Windows plug-in.

Table B-13 Microsoft Windows Plug-in

Plug-in Specification	Description
Plug-in directory	<i>AGENT_HOME\av\plugins\com.oracle.av.plugin.winos</i>
Secured Target Versions	Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, and 2016
Secured Target Platforms	Windows/x86-64
Setup Script(s)	No
Secured Target Location (Connect String)	<i>hostname</i> (fully qualified machine name or IP address)
Collection Attribute(s)	None
AVDF Audit Trail Types	EVENT LOG See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	<i>security</i> (case-sensitive)
Audit Trail Cleanup Support	No

B.2.12 Microsoft Active Directory

[Table B-14](#) (page B-15) lists the features of the Microsoft Active Directory plug-in.

Table B-14 Microsoft Active Directory Plug-in

Plug-in Specification	Description
Plug-in directory	<i>AGENT_HOME\av\plugins\com.oracle.av.plugin.msad</i>
Secured Target Versions	2008, 2008 R2, 2012, and 2016 on 64 bit
Secured Target Platforms	Windows/x86-64
Setup Script(s)	No
Secured Target Location (Connect String)	<i>hostname</i> (fully qualified machine name or IP address)
Collection Attribute(s)	None

Table B-14 (Cont.) Microsoft Active Directory Plug-in

Plug-in Specification	Description
AVDF Audit Trail Types	EVENT LOG See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	directory service or security (case-sensitive)
Audit Trail Cleanup Support	No

B.2.13 Oracle ACFS

[Table B-15](#) (page B-16) lists the features of the Oracle ACFS plug-in.

Table B-15 Oracle ACFS Plug-in

Plug-in Specification	Description
Plug-in directory	<i>AGENT_HOME</i> /av/plugins/com.oracle.av.plugin.acfs
Secured Target Versions	12c Release 1 (12.1)
Secured Target Platforms	Linux/x86-64 Solaris/x86-64 Solaris/SPARC64 Windows 2008, 2008 R2 64-bit
Setup Script(s)	No
Secured Target Location (Connect String)	<i>hostname</i> (fully qualified machine name or IP address)
Collection Attribute(s)	av.collector.securedtargetversion - (Required) Specify the Oracle ACFS version.
AVDF Audit Trail Types	DIRECTORY See Table B-17 (page B-18) 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 <i>\$MOUNT_POINT</i> , the audit trail location is: <i>\$MOUNT_POINT/.Security/audit/</i>
Audit Trail Cleanup Support	No

B.2.14 Oracle Big Data Appliance

[Table B-16](#) (page B-16) lists the features of the Oracle Big Data Appliance.

Table B-16 Big Data Appliance Plug-in

Plug-in Specification	Description
Plug-in directory	<i>AGENT_HOME</i> /av/plugins/com.oracle.av.plugin.bda
Secured Target Versions	2.3, 4.3
Secured Target Platforms	Linux x86-64

Table B-16 (Cont.) Big Data Appliance Plug-in

Plug-in Specification	Description
Setup Script(s)	No
Secured Target Location (Connect String)	<i>hostname</i> (fully qualified machine name or IP address)
Collection Attribute(s)	<code>av.collector.securedtargetversion</code> - (Required) Specify the Oracle Big Data Appliance version.
AVDF Audit Trail Types	DIRECTORY See Table B-17 (page B-18) for descriptions of audit trail types.
Audit Trail Location	<code>/var/log/hadoop-hdfs/hdfs-audit.log</code>
Audit Trail Cleanup Support	No

B.2.15 Summary of Data Collected for Each Audit Trail Type

When you configure an audit trail for a secured target, you select the type of audit trail in the **Audit Trail Type** field. The audit trail type depends on your secured target type. [Table B-17](#) (page B-18) describes the types of audit trails that can be configured for each secured target type.

Refer to the product documentation for your secured target type for details on its auditing features and functionality. Refer to the following documentation for Oracle products:

- Oracle Database 12c Release 1 (12.1): *Oracle Database Security Guide*
- Oracle Database 11g Release 2 (11.2): *Oracle Database Security Guide*
- Oracle Solaris 11.1
- Oracle Solaris 10.6
- Oracle ACFS 12c Release 1 (12.1): *Oracle Automatic Storage Management Administrator's Guide*

Table B-17 Summary of Audit Trail Types Supported for Each Secured Target Type


Secured Target Type	Trail Type	Description
Oracle Database	TABLE	Collects from the following audit trails:
	Releases 10.2.x, 11.x, and 12.x	<ul style="list-style-type: none"> Oracle Database audit trail, where standard audit events are written to the <code>SYS.AUD\$</code> dictionary table Oracle Database fine-grained audit trail, where audit events are written to the <code>SYS.FGA_LOG\$</code> dictionary table Oracle Database Vault audit trail, where audit events are written to the <code>DVSYS.AUDIT_TRAIL\$</code> dictionary table Oracle database 12.x Unified Audit trail, where audit events are written to the <code>UNIFIED_AUDIT_TRAIL</code> data dictionary view
<div style="border-left: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px; margin-left: 20px;"> <p> Note:</p> <p>The <code>SYS.AUD\$</code> and <code>SYS.FGA_LOG\$</code> tables have an additional column <code>RLS\$INFO</code>. The Unified Audit trail table has <code>RLS_INFO</code> column. This column describes row level security policies configured. This is mapped to the extension field in Audit Vault and Database Firewall. In order to populate this column, the user needs to set the <code>AUDIT_TRAIL</code> parameter of the secured target to <code>DB EXTENDED</code>.</p> </div>		
Oracle Database	DIRECTORY	Collects data from the following audit trails:
	Releases 10.2.x, 11.x, and 12.x	<ul style="list-style-type: none"> On Linux and UNIX platforms: The Oracle database audit files written to the operating system (<code>.aud</code> and <code>.xml</code>) files On Windows platforms: The operating system Windows Event Log and operating system logs (audit logs) XML (<code>.xml</code>) files

Table B-17 (Cont.) Summary of Audit Trail Types Supported for Each Secured Target Type

Secured Target Type	Trail Type	Description
Oracle Database	TRANSACTION LOG 11.2 for REDO connection	Collects audit data from logical change records (LCRs) from the REDO logs. If you plan to use this audit trail type, you can define the data to audit by creating capture rules for the tables from which the Transaction Log trail type will capture audit information.

 **See Also:**

Oracle Audit Vault and Database Firewall Auditor's Guide for more information.

 **Note:**

- For Oracle Database 12c, the Transaction Log audit trail is only supported when not using a PDB/CDB.
- Transaction Log audit trail is not supported for Oracle Database versions 18c and 19c.

Table B-17 (Cont.) Summary of Audit Trail Types Supported for Each Secured Target Type

Secured Target Type	Trail Type	Description
Oracle Database	SYSLOG	<p>Collects Oracle audit records from either <code>syslog</code> or <code>rsyslog</code> audit files on Linux and Unix platforms only. If the system has both <code>syslog</code> and <code>rsyslog</code> installed, the exact <code>rsyslog</code> audit file location must be specified in order to collect data from <code>rsyslog</code> files.</p> <p>The following <code>rsyslog</code> formats are supported:</p> <ul style="list-style-type: none"> • <code>RSYSLOG_TraditionalFileFormat</code> (has low-precision time stamps) • <code>RSYSLOG_FileFormat</code> (has high-precision time stamps and time zone information) <p>Events from both formats appear the same on reports, however with <code>RSYSLOG_FileFormat</code>, the <code>AVSYS.EVENT_LOG</code> table shows <code>EVENT_TIME</code> with microsecond precision.</p>
Oracle Database	EVENT LOG	Collects Oracle audit records from Microsoft Windows Event Log on Windows platforms only
Oracle Database	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Microsoft SQL Server	DIRECTORY	Collects audit data from C2 audit logs, server-side trace logs, and <code>sqlaudit</code> log files
Microsoft SQL Server	EVENT LOG	Collects audit data from Windows Application Event Logs. For Microsoft SQL Server 2008 and 2012, collection from the Security Event Log is also supported.
Microsoft SQL Server	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Sybase ASE	TABLE	Collects audit data from system audit tables (<code>sysaudits_01</code> through <code>sysaudits_08</code>) in the <code>sybsecurity</code> database
Sybase ASE	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Sybase SQL Anywhere	NETWORK	(For host monitoring only) Collects network traffic (all database operations using a TCP connection).

 **See Also:**

Oracle Audit Vault and Database Firewall Auditor's Guide for details on this table, and Audit Vault Server schema documentation.

Table B-17 (Cont.) Summary of Audit Trail Types Supported for Each Secured Target Type

Secured Target Type	Trail Type	Description
IBM DB2 for LUW	DIRECTORY	Collects audit data from ASCII text files extracted from the binary audit log (<code>db2audit.log</code>). These files are located in the <code>security</code> subdirectory of the DB2 database instance.
IBM DB2 for LUW	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
MySQL	DIRECTORY	Collects XML-based audit data from a specified location
MySQL	NETWORK	Collects network traffic (all database operations using a TCP connection). Used for host monitor.
Oracle Solaris	DIRECTORY	Collects Solaris Audit records (version 2) generated by the <code>audit_binfile</code> plug-in of Solaris Audit
Linux	DIRECTORY	Collects audit data from <code>audit.log</code>
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.
Oracle Linux	DIRECTORY	Collects audit data from <code>audit.log</code>
Oracle Big Data Appliance	DIRECTORY	Collects audit data from <code>hdfs-audit.log</code>

B.3 Scripts for Oracle AVDF Account Privileges on Secured Targets

Topics

- [About Scripts for Setting up Oracle Audit Vault and Database Firewall Account Privileges](#) (page B-22)
- [Oracle Database Setup Scripts](#) (page B-22)
- [Sybase ASE Setup Scripts](#) (page B-24)
- [Sybase SQL Anywhere Setup Scripts](#) (page B-26)
- [Microsoft SQL Server Setup Scripts](#) (page B-27)
- [IBM DB2 for LUW Setup Scripts](#) (page B-29)
- [MySQL Setup Scripts](#) (page B-31)

B.3.1 About Scripts for Setting up Oracle Audit Vault and Database Firewall Account Privileges

You must set up a user account with appropriate privileges on each secured target for Oracle Audit Vault and Database Firewall to use in performing functions related to monitoring and collecting audit data. Oracle Audit Vault and Database Firewall provides setup scripts for database secured targets. Depending on the type of secured target, the scripts set up user privileges that allow Oracle Audit Vault and Database Firewall to do the following functions:

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

When you deploy the Audit Vault Agent on a host computer (usually the same computer as the secured target), the setup scripts for creating the user permissions for Oracle Audit Vault and Database Firewall are located in the following directory (Linux example below):

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.secured_target_type/config/
```

B.3.2 Oracle Database Setup Scripts

The Oracle Audit Vault and Database Firewall setup scripts for an Oracle Database secured target, `oracle_user_setup.sql` and `oracle_drop_db_permissions.sql`, are located in the following directory (Linux example below):

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

These scripts are used to set up or revoke user privileges on the Oracle Database in order for Oracle Audit Vault and Database Firewall to do the following functions:

- Audit data collection
- Audit policy management
- Stored procedure auditing (SPA)
- User entitlement auditing

To set up or revoke Oracle Audit Vault and Database Firewall user privileges on an Oracle Database secured 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 username and password when registering this Oracle Database as a secured target in the Audit Vault Server.

2. Connect as user `SYS` with the `SYSDBA` privilege. For example:


```
SQL> CONNECT SYS / AS SYSDBA
```

3. To set up Oracle Audit Vault and Database Firewall user privileges, run the setup script as follows:

```
SQL> @oracle_user_setup.sql username mode
```

- *username*: Enter the name of the user you created in Step 1.
- *mode*: Enter one of the following:
 - **SETUP**: To set up privileges for managing the Oracle Database audit policy from Oracle Audit Vault and Database Firewall, and for collecting data from any audit trail type except the REDO logs. For example, use this mode for a TABLE audit trail in Oracle Audit Vault and Database Firewall.
 - **REDO_COLL**: To set up privileges for collecting audit data from the REDO logs. Use this mode only for a TRANSACTION LOG audit trail in Oracle Audit Vault and Database Firewall.
 - **SPA**: To enable stored procedure auditing for this database
 - **ENTITLEMENT**: To enable user entitlement auditing for this database

 **Note:**

When setting up audit collection for a CDB, create a separate local user in the CDB and each PDB instance. Execute the `oracle_user_setup.sql` script for each user. For each PDB instance first alter the session to switch to the PDB before running the script.

4. If Database Vault is installed and enabled on the Oracle database, log in as a user who has been granted the `DV_OWNER` role do the following:
 - a. Grant the Oracle 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.

- b. For `REDO_COLL` mode (TRANSACTION LOG audit trail) only, execute one of these procedures depending on your Oracle Database version:

For Oracle Database 12c:

```
SQL> GRANT DV_STREAMS_ADMIN TO username;
```

For *username*, enter the user name you created in Step 1.

For all other supported Oracle Database versions:

```
SQL> EXEC DBMS_MACADM.ADD_AUTH_TO_REALM('Oracle Data Dictionary', 'username',  
null, dbms_macutl.g_realm_auth_participant);  
SQL> COMMIT;
```

For *username*, enter the user name you created in Step 1.

5. To revoke Oracle Audit Vault and Database Firewall user privileges, connect to this database as user SYS with the SYSDBA privilege, and run the following script:

```
SQL> @oracle_drop_db_permissions.sql username mode
```

- *username* - Enter the name of the user you created in Step 1.
- *mode* - Enter one of the following:
 - SETUP: To revoke privileges for managing the Oracle Database audit policy from Oracle Audit Vault and Database Firewall, and for collecting data from any audit trail type except the REDO logs.
 - REDO_COLL: To revoke privileges for collecting audit data from the REDO logs.
 - SPA: To disable stored procedure auditing for this database
 - ENTITLEMENT: To disable user entitlement auditing for this database



See Also:

[Configuring Audit Trail Collection For CDB And PDB \(page 6-19\)](#)

B.3.3 Sybase ASE Setup Scripts

Topics

- [About the Sybase ASE Setup Scripts \(page B-24\)](#)
- [Setting Up Audit Data Collection Privileges for a Sybase ASE Secured Target \(page B-25\)](#)
- [Setting Up Stored Procedure Auditing Privileges for a Sybase ASE Secured Target \(page B-25\)](#)

B.3.3.1 About the Sybase ASE Setup Scripts

The following scripts are provided for configuring necessary user privileges for Oracle Audit Vault and Database Firewall in a Sybase ASE secured target:

```
sybase_auditcoll_user_setup.sql
sybase_auditcoll_drop_db_permissions.sql
sybase_spa_user_setup.sql
sybase_spa_drop_db_permissions.sql
```

The scripts are located in the following directory (Linux example below):

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

These scripts allow Oracle Audit Vault and Database Firewall to perform the following functions for Sybase ASE:

- Audit data collection
- Stored procedure auditing (SPA)

B.3.3.2 Setting Up Audit Data Collection Privileges for a Sybase ASE Secured Target

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

1. Create a user account for Oracle 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 secured target in the Audit Vault Server.

2. Run the setup `sybase_auditcoll_user_setup.sql` script as follows:

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

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

3. When prompted for a password, enter the system administrator password.

4. To revoke the Oracle 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.

B.3.3.3 Setting Up Stored Procedure Auditing Privileges for a Sybase ASE Secured Target

To set up or revoke stored procedure auditing privileges on a Sybase ASE secured target:

1. If you have not already done so, create a user account for Oracle AVDF in Sybase ASE with the user name `avdf_sybuser`. For example:

```
sp_addlogin avdf_sybuser, password
```

You will use the user name `av_sybuser` and password when registering this Sybase ASE database as a secured target in the Audit Vault Server.

2. Run the `sybase_spa_user_setup.sql` script as follows:

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

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

3. When prompted for a password, enter the system administrator password.
4. To revoke the SPA user privileges, run the `sybase_spa_drop_db_permissions.sql` script as follows:

```
isql -S server_name -U sa -i sybase_spa_drop_db_permissions.sql
```

- *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the `-S server_name` argument.
- *sa*: Enter the system administrator user name.
- When prompted for a password, enter the system administrator password.

B.3.4 Sybase SQL Anywhere Setup Scripts

The Oracle AVDF setup scripts for a Sybase SQL Anywhere secured target, `sqlanywhere_spa_user_setup.sql` and `sqlanywhere_spa_drop_db_permissions.sql`, are located in the following directory (Linux example below):

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.sqlanywhere/config/
```

These scripts are used to set up or revoke user privileges on the SQL Anywhere database for Oracle AVDF to do stored procedure auditing (SPA).

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

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

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

- *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the `-S server_name` argument.
- *sa*: Enter the system administrator user name.
- *username*: Enter the name of the user you want to create for Oracle AVDF to use for SPA. Enclose this user name in double quotation marks.
- *password*: Enter a password for the Oracle AVDF SPA user you are creating. Enclose the password in double quotation marks.

After running the script, the user is created with privileges for SPA.

3. When prompted for a password, enter the system administrator password.
4. To revoke these privileges and remove this user from the database, run the `sqlanywhere_spa_drop_db_permissions.sql` as follows:

```
isql -S server_name -U sa -i sqlanywhere_spa_drop_db_permissions.sql -v  
username="username"
```

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

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

B.3.5 Microsoft SQL Server Setup Scripts

Topics

- [About the SQL Server Setup Script](#) (page B-27)
- [Setting Up Audit Data Collection Privileges for a SQL Server Secured Target](#) (page B-27)
- [Setting Up Stored Procedure Auditing Privileges for a SQL Server Secured Target](#) (page B-28)

B.3.5.1 About the SQL Server Setup Script

The Oracle AVDF setup scripts for a Microsoft SQL Server secured target, `mssql_user_setup.sql` and `mssql_drop_db_permissions.sql`, are located in the following directory:

```
AGENT_HOME\av\plugins\com.oracle.av.plugin.mssql\config\
```

The scripts set up or revoke user privileges for Oracle AVDF to perform the following functions for SQL Server:

- Audit data collection
- Stored procedure auditing (SPA)

B.3.5.2 Setting Up Audit Data Collection Privileges for a SQL Server Secured Target

To set up or revoke Oracle AVDF user privileges for audit data collection:

1. Create a user account for Oracle Audit Vault and Database Firewall in SQL Server or use Windows authenticated user. For example:

In SQL Server 2000:

```
exec sp_addlogin 'username', 'password'
```

In SQL Server 2005, 2008, 2012, 2014, 2016:

```
exec sp_executesql N'create login username with password = ''password'',  
check_policy= off'
```

```
exec sp_executesql N'create user username for login username'
```

You will use this user name and password when registering this SQL Server database as a secured target in the Audit Vault Server.

2. Run the `mssql_user_setup.sql` script as follows:

For SQL Server authentication:

```
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:

```
sqlcmd -S localhost -U sa -i mssql_user_setup.sql -v
username="[<domain name>\<user name>]" mode="AUDIT_COLL"
all_databases="NA" database="NA"
```

- *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the `-S server_name` argument.
 - *sa*: Enter the system administrator user name.
 - *username*: Enter the name of the user you created in Step 1.
3. When prompted for a password, enter the system administrator password.
 4. To revoke audit data collection privileges run the `mssql_drop_db_permissions.sql` script as follows:

For SQL Server Authentication:

```
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:

- a.

```
sqlcmd -S server_name -U sa -i mssql_drop_db_permissions.sql -v
username="[<domain name>\<user name>]" mode="AUDIT_COLL"
all_databases="NA" database="NA"
```

 - *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the `-S server_name` argument.
 - *sa*: Enter the system administrator user name.
 - *username*: Enter the name of the user you created in Step 1.
- b. When prompted for a password, enter the system administrator password.

B.3.5.3 Setting Up Stored Procedure Auditing Privileges for a SQL Server Secured Target

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

1. If you have not already done so, create a user account for Oracle AVDF in SQL Server. For example:

In SQL Server 2000:

```
exec sp_addlogin 'username', 'password'
```

In SQL Server 2005 and 2008:

```
exec sp_executesql N'create login username with password = 'password',
check_policy= off'
```

```
exec sp_executesql N'create user username for login username'
```

You will use this user name and password when registering this SQL Server database as a secured target in the Audit Vault Server.

2. Run the `mssql_user_setup.sql` script as follows:

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

- *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the `-S server_name` argument.
 - *sa*: Enter the system administrator user name.
 - *username*: Enter the name of the user you created in Step 1.
 - *Y/N*: Enter *Y* if all databases should be audited for stored procedures. Enter *N* to specify one database name in the *database* parameter.
 - *NA/database_name*: If you entered *Y* for *all_databases*, enter *NA*. If you entered *N* for *all_databases*, enter the database name that should be audited for stored procedures.
3. When prompted for a password, enter the system administrator password.
 4. To revoke SPA privileges run the `mssql_drop_db_permissions.sql` script as follows:

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

- *server_name*: Only use this argument if the database is remote. Enter the name of the remote server or its IP address. If you are running the script locally, then omit the `-S server_name` argument.
- *sa*: Enter the system administrator user name.
- *sa_password*: Enter the system administrator password.
- *Y/N*: Enter *Y* if SPA privileges for all databases should be revoked. Enter *N* to specify one database name in the *database* parameter.
- *NA/database_name*: If you entered *Y* for *all_databases*, enter *NA*. If you entered *N* for *all_databases*, enter the database name for which SPA privileges should be revoked.
- When prompted for a password, enter the name of the user you created in Step 1.

B.3.6 IBM DB2 for LUW Setup Scripts

Topics

- [About the IBM DB2 for LUW Setup Scripts](#) (page B-29)
- [Setting Up Audit Data Collection Privileges for IBM DB2 for LUW](#) (page B-30)
- [Setting Up SPA Privileges for an IBM DB2 for LUW Secured Target](#) (page B-30)

B.3.6.1 About the IBM DB2 for LUW Setup Scripts

The Oracle Audit Vault and Database Firewall setup scripts for a DB2 secured target, `db2_auditcoll_user_setup.sql` and `db2_spa_user_setup.sql`, are located in the following directory (Linux example below):

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/
```

**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)

B.3.6.2 Setting Up Audit Data Collection Privileges for IBM DB2 for LUW

To set up or revoke Oracle AVDF user privileges for audit data collection:

1. Create a new user account in DB2 to be used by Oracle AVDF for audit data collection.

You will use this user name and password when registering this DB2 database as a secured target in the Audit Vault Server.

2. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/` directory, locate the `db2_auditcoll_user_setup.sql` script and open it for editing.
3. In the script, put the user name of the account from Step 1 in the `grant` statement, then save the modified script.
4. Execute the modified script as follows:

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

5. To revoke audit collection privileges:
 - a. Modify the `db2_auditcoll_drop_db_permissions.sql` script as in Step 3 (page B-30) above.
 - b. Run the script as follows:

```
$> db2 -tvf db2_auditcoll_drop_db_permissions.sql
```

B.3.6.3 Setting Up SPA Privileges for an IBM DB2 for LUW Secured Target

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

1. Create a new user account in DB2 to be used by Oracle AVDF for stored procedure auditing.

You will use this user name and password when registering this DB2 database as a secured target in the Audit Vault Server.

2. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.db2/config/` directory, locate the `db2_spa_user_setup.sql` script and open it for editing.
3. In the script, put the user name of the account from Step 1 in the `grant` statement, then save the modified script.
4. Execute the modified script as follows:

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

5. To revoke SPA privileges:

- a. Modify the `db2_spa_drop_db_permissions.sql` script as in Step 3 (page B-30) above.

- b. Run the script as follows:

```
$> db2 -tvf db2_spa_drop_db_permissions.sql
```

B.3.7 MySQL Setup Scripts

The Oracle AVDF setup scripts for a MySQL secured target, `mysql_spa_user_setup.sql` and `mysql_spa_drop_db_permissions.sql`, are located in the following directory (Linux example below):

```
$AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/config/
```

These scripts are used to set up or revoke user privileges on the MySQL database for Oracle AVDF to do stored procedure auditing (SPA).

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

1. Log in to MySQL as a user who can create users and set user privileges.
2. Create a user for stored procedure auditing. For example:

```
create user 'username'@'hostname' identified by 'password'
```

You will use this user name and password when registering this MySQL database as a secured target in the Audit Vault Server.

3. In the `$AGENT_HOME/av/plugins/com.oracle.av.plugin.mysql/config/` directory, locate the `mysql_spa_user_setup.sql` script and open it for editing.
4. Modify the script to provide the same values for `username`, `hostname`, and `password` that you used in Step 1.
5. Execute the `mysql_spa_user_setup.sql` script.
6. To revoke SPA privileges:
 - a. Modify the `mysql_spa_drop_db_permissions.sql` script as in Step 4 (page B-31) above.
 - b. Execute the `mysql_spa_drop_db_permissions.sql` script.

B.4 Audit Collection Consideration

Considerations for audit collection on other target types.

B.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.

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

Audit data can be collected from the primary database in Oracle Active 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 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.

 **Note:**

Oracle AVDF supports audit collection from the traditional audit trail in both the primary and standby databases of Oracle Active Data Guard. When unified audit is enabled, audit collection is supported only from the unified audit trail of the primary database, and not from the standby database.

B.5 Audit Trail Cleanup

Some Oracle AVDF plug-ins support audit trail cleanup. This section describes the available audit trail cleanup (ATC) utilities:

- [Oracle Database Audit Trail Cleanup](#) (page B-33)
- [SQL Server Audit Trail Cleanup](#) (page B-34)
- [MySQL Audit Trail Cleanup](#) (page B-35)

B.5.1 Oracle Database Audit Trail Cleanup

Topics

- [About Purging the Oracle Database Secured Target Audit Trail](#) (page B-33)
- [Scheduling an Automated Purge Job](#) (page B-33)

B.5.1.1 About Purging the Oracle Database Secured Target Audit Trail

You can use the `DBMS_AUDIT_MGMT` PL/SQL package to purge the database audit trail.

The `DBMS_AUDIT_MGMT` package lets you perform audit trail cleanup tasks such as scheduling purge jobs, moving the audit trail to a different tablespace, setting archive timestamps in the audit trail, and so on. You must have the `EXECUTE` privilege for `DBMS_AUDIT_MGMT` before you can use it.

Oracle Database 11g Release 2 (11.2) or higher, includes the `DBMS_AUDIT_MGMT` package and its associated data dictionary views installed by default. If your secured target database does not have this package installed, then you can download the package and data dictionary views from My Oracle Support.

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 11g Release 2 (11.2) documentation:

- The section "Purging Audit Trail Records" in *Oracle Database Security Guide* for conceptual and procedural information
- *Oracle Database PL/SQL Packages and Types Reference* for reference information about the `DBMS_AUDIT_MGMT` PL/SQL package
- *Oracle Database Reference* for information about the `DBA_AUDIT_MGMT_*` data dictionary views

B.5.1.2 Scheduling an Automated Purge Job

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 secured target:

1. Log in to SQL*Plus on the secured target database as a user who has been granted the `EXECUTE` privilege for the `DBMS_AUDIT_MGMT` PL/SQL package.

For example:

```
sqlplus tjones
Enter password: password
```

2. Initialize the audit trail cleanup operation.

In the following example, the `DEFAULT_CLEANUP_INTERVAL` setting runs the job every two hours:

```

BEGIN
  DBMS_AUDIT_MGMT.INIT_CLEANUP(
    AUDIT_TRAIL_TYPE      => DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
    DEFAULT_CLEANUP_INTERVAL => 2 );
END;
/

```

Note:

In case you are collecting audit data from CDB, then execute this step every time there is any change in the PDB instance.

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;
/

```

B.5.2 SQL Server Audit Trail Cleanup

If the SQL Server audit trail has collected data from a trace or `sqlaudit` file and that file is inactive, then you can clean up this file. The SQL Server audit trail writes the names of the SQL Server audit text files to a plain text file with the `.atc` extension. The `.atc`

file resides in the `AGENT_HOME\av\atc` directory on the computer on which the agent is installed.

To manually clean up files that Oracle AVDF has completed extracting audit records from:

1. Go to the `AGENT_HOME\av\plugins\com.oracle.av.plugin.mssql\bin` directory of the computer where the Audit Vault Agent is installed.

Ensure that the `AGENT_HOME` environment variable is correctly set to the directory path where the `agent.jar` file is extracted.

2. Run the following utility:

```
SQLServerCleanupHandler secured_target_name
```

For example:

```
SQLServerCleanupHandler mssqldb4
```

If you do not set the `AGENT_HOME` environment variable, you can provide the agent home location in the command line using the following syntax:

```
SQLServerCleanupHandler -securedtargetname secured_target_name agent_home_location
```

For example:

```
SQLServerCleanupHandler mssqldb4 c:\AV_agent_installation
```

Important: If the name of the Audit Vault Agent installation directory contains spaces, enclose the name in double quotes, for example "C:\Agent Directory".

To automate the cleanup of SQL Server trace files, you can use the Windows Scheduler.

Note:

If the SQL Server trace definition is redefined or reinitialized, then you must ensure that the file names of the trace files do not overlap with trace files that were created earlier.

For example, suppose you start SQL Server with a trace definition in which the trace files names use the following format:

```
c:\serversidetraces.trc  
c:\serversidetraces_1.trc  
c:\serversidetraces_2.trc  
...  
c:\serversidetraces_259.trc
```

Then you restart the SQL Server with a new trace definition. This new trace definition must use a different file name from the current trace files (for example, the current one named `c:\serversidetraces.trc`). If you do not, then when you purge the audit trail, the new trace files that have same names as the old ones will be deleted.

B.5.3 MySQL Audit Trail Cleanup

To run the MySQL audit trail cleanup utility:

1. On the host machine, go to the directory
`AGENT_HOME\av\plugins\com.oracle.av.plugin.mysql\bin`
2. Run the following command:
`MySQLServerCleanupHandler.bat secured_target_name AGENT_HOME`
 The above command has the following variables:
 - `secured_target_name` - the name of the MySQL secured target
 - `AGENT_HOME` - the path to the directory where the Audit Vault Agent is deployed.

B.6 Procedure Look-ups: Connect Strings, Collection Attributes, Audit Trail Locations

This section contains reference information you will need to complete procedures in this manual for registering secured targets and configuring audit trails. The procedural steps include links to the topics in this section.

Topics

- [Secured Target Locations \(Connect Strings\)](#) (page B-36)
- [Collection Attributes](#) (page B-38)
- [Audit Trail Locations](#) (page B-42)

B.6.1 Secured Target Locations (Connect Strings)

When registering a secured target in the Audit Vault Server console, you enter a connect string in the **Secured Target Location** field. Use a connect string format from [Table B-18](#) (page B-36) depending on the secured target type.

Note: A connect string is not required for a Database Firewall-only deployment.

Table B-18 Secured Target Connect Strings (for Secured Target Location Field)

Secured Target Type	Connect String
Oracle Database	<code>jdbc:oracle:thin:@//hostname:port/service</code>
Sybase ASE	<code>jdbc:av:sybase://hostname:port</code>
Sybase SQL Anywhere	<code>jdbc:av:sybase://hostname:port</code>

Table B-18 (Cont.) Secured Target Connect Strings (for Secured Target Location Field)

Secured Target Type	Connect String
Microsoft SQL Server (SQL Server Authentication)	<p><code>jdbc:av:sqlserver://hostname:port</code></p> <p>When SSL Encryption is used with MSSQL sever and the server certificate validation is required.</p> <p><code>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</code></p> <p>When SSL Encryption is used with MSSQL sever and the server certificate validation is not required.</p> <p><code>jdbc:av:sqlserver://<MSSQL Host name>:<Port number>;encryptionMethod=SSL;validateServerCertificate=false</code></p>
Microsoft SQL Server (Windows Authentication)	<p><code>jdbc:av:sqlserver://<Host Name>:<Port>;authenticationMethod=ntlmjava</code></p> <p>(Use Windows user credentials along with domain. For example, <domain name>\<user name > and password.)</p> <p>OR</p> <p><code>jdbc:av:sqlserver://<Host Name>:<Port>;authenticationMethod=ntlmjava;domain=<domain name></code></p> <p>Use Windows user credentials without domain. For example, <user name > and password.</p>
IBM DB2 for LUW	<p><code>jdbc:av:db2://hostname:port</code></p> <p>Note: Connect string is not required from release 12.2.0.11.0 and onwards.</p>
MySQL	<p><code>jdbc:av:mysql://hostname:port/mysql</code></p> <p>Note: Connect string is not required from release 12.2.0.11.0 and onwards.</p>
Oracle Solaris	<code>hostname</code> (fully qualified machine name or IP address)
Oracle Linux	<code>hostname</code> (fully qualified machine name or IP address)
Microsoft Windows	<code>hostname</code> (fully qualified machine name or IP address)
Microsoft Active Directory Server	<code>hostname</code> (fully qualified machine name or IP address)
Oracle ACFS	<code>hostname</code> (fully qualified machine name or IP address)

**See Also:**

[Registering or Removing Secured Targets in the Audit Vault Server \(page 6-2\)](#)

B.6.2 Collection Attributes

Topics

- [About Collection Attributes](#) (page B-38)
- [Oracle Database Collection Attributes](#) (page B-38)
- [IBM DB2 for LUW Collection Attribute](#) (page B-41)
- [MySQL Collection Attributes](#) (page B-41)
- [Oracle ACFS Collection Attributes](#) (page B-41)

B.6.2.1 About Collection Attributes

Some types of secured targets have optional or required audit trail collection attributes. You can specify collection attributes when registering or modifying a secured target in the **Collection Attributes** fields.

The following secured target types do not require collection attributes:

- Microsoft SQL Server
- Sybase ASE
- Oracle Solaris
- Windows
- Linux
- Microsoft Active Directory Server



See Also:

[Registering or Removing Secured Targets in the Audit Vault Server](#)
(page 6-2)

B.6.2.2 Oracle Database Collection Attributes

You can specify collection attributes for a DIRECTORY audit trail for Oracle Database. [Table B-19](#) (page B-39) describes the collection attributes you can use if you select DIRECTORY as the **Audit Trail Type** when registering an Oracle Database secured target in Oracle Audit Vault and Database Firewall.

Table B-19 Collection Attributes for DIRECTORY Audit Trail for Oracle Database

Attribute Name and Description	Required?	Default	Comments
ORLCCOLL.NLS_LANGUAGE The NLS language of the data source	Yes: If the started audit trail cannot establish a connection to the Oracle secured target (e.g., secured target is not running) No: If the started audit trail is able to connect to the Oracle secured target and get these parameter values from the secured target (e.g., the secured target is running when the trail is started)	NA	The value is not case sensitive.
ORLCCOLL.NLS_TERRITORY The NLS territory of the data source	Yes: If the started audit trail cannot establish a connection to the Oracle secured target (e.g., secured target is not running) No: If the started audit trail is able to connect to the Oracle secured target and get these parameter values from the secured target (e.g., the secured target is running when the trail is started)	NA	The value is not case sensitive.
ORLCCOLL.NLS_CHARSET The NLS character set of the data source	Yes: If the started audit trail cannot establish a connection to the Oracle secured target (e.g., secured target is not running) No: If the started audit trail is able to connect to the Oracle secured target and get these parameter values from the secured target (e.g., the secured target is running when the trail is started)	NA	The value is not case sensitive.

Table B-19 (Cont.) Collection Attributes for DIRECTORY Audit Trail for Oracle Database

Attribute Name and Description	Required?	Default	Comments
ORLCCOLL.MAX_PROCESS_TIME The maximum processing time, in centiseconds, for each call to process the audit trail	No	600	A valid value is an integer value from 10 to 10000. Cannot be reconfigured at run time. Indicates the maximum time for which the collection process records before sending a batch of records to the Audit Vault Server. If the value is too low it can affect performance. If the value is too high, it will take a longer time to stop the audit trail.
ORLCCOLL.MAX_PROCESS_RECORDS The maximum number of records to be processed during each call to process the audit trail	No	1000	A valid value is an integer value from 10 to 10000. Cannot be reconfigured at run time. Indicates the maximum number of records processed before sending a batch of records to the Audit Vault Server. If the value is too low it can affect performance. If the value is too high, it will take a longer time to stop the audit trail.
ORLCCOLL.RAC_INSTANCE_ID The instance ID in an Oracle RAC environment	No	1	None.
ORLCCOLL.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.
ORLCCOLL.NT_ORACLE_SID The Oracle SID name on a Microsoft Windows systems	No	No default	The value is not case sensitive. If no value is specified then the audit trail queries the value from the secured target.

B.6.2.3 IBM DB2 for LUW Collection Attribute

[Table B-20](#) (page B-41) describes the collection attribute required when you register an IBM DB2 for LUW secured target in Oracle AVDF.

Table B-20 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 collection attribute is not required from release 12.2.0.11.0 and onwards.

B.6.2.4 MySQL Collection Attributes

[Table B-21](#) (page B-41) describes the required and optional collection attributes when you register a MySQL secured target in Oracle Audit Vault and Database Firewall.

Table B-21 Collection Attributes for MySQL Database

Attribute Name and Description	Required?	Default	Comments
av.collector.securedTargetVersion The MySQL database version	Yes	NA	NA
av.collector.AtcTimeInterval Specifies a time interval, in minutes, at which the audit trail cleanup time is updated	No	20	Example: If this value is 20, the audit trail cleanup time is updated every 20 minutes. Audit log files that have a time stamp before the audit trail cleanup time will be cleaned from the source folder when you run the audit trail cleanup utility.



See Also:

[MySQL Audit Trail Cleanup](#) (page B-35)

B.6.2.5 Oracle ACFS Collection Attributes

[Table B-22](#) (page B-42) describes the collection attribute required when you register an Oracle ACFS secured target in Oracle Audit Vault and Database Firewall.

Table B-22 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.

B.6.3 Audit Trail Locations

When you configure an audit trail for a secured target in the Audit Vault Server, you must specify a **Trail Location**. The trail location depends on the type of secured target. Use the format below that corresponds to your secured target type.

Important: Trail locations are case sensitive. To avoid duplicate data collection, we recommend that you provide the entire trail location either in all capital letters or all small letters.

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

[Table B-23](#) (page B-42) shows the supported formats for **Trail Location**.

Table B-23 Supported Trail Locations for Secured Targets

Secured Target Type	Trail Type	Supported Trail Locations
Oracle Database	Table	SYS.AUD\$, SYS.FGA_LOG\$, DVSYS.AUDIT_TRAIL\$, UNIFIED_AUDIT_TRAIL
Oracle Database	Directory	Full path to directory containing AUD or XML files.
Oracle Database	syslog	Full path to directory containing 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, an example path might be: /scratch/user1/rsyslogbug/dbrecord/messages You can also enter Default and the system will search for either the syslog or rsyslog location. If both are present, entering Default causes the audit trail to collect data from the syslog files.
Oracle Database	Transaction log, Event log, and Network	No trail location required.

Table B-23 (Cont.) Supported Trail Locations for Secured Targets

Secured Target Type	Trail Type	Supported Trail Locations
Microsoft SQL Server	Directory	<p>*.sqlaudit files, or *.trc (trace) files.</p> <p>Examples:</p> <pre>directory_path*.sqlaudit directory_path\prefix*.sqlaudit directory_path\prefix*.trc</pre> <p>For <i>prefix</i>, you can use any prefix for the .trc or *.sqlaudit files.</p> <p>#C2_DYNAMIC and #TRACE_DYNAMIC are only supported for SQL Server 2000, 2005, 2008, 2012, 2014, 2016.</p>
Microsoft SQL Server	Event log	application or security (SQL Server 2008, 2012, 2014, and 2016)
Sybase ASE	Table	SYSAUDITS
IBM DB2 for LUW	Directory	Path to a directory, for example: d:\temp\trace
MySQL	Directory	The path to the directory where converted XML files are created when you run the MySQL XML transformation utility.
Oracle Solaris	Directory	<pre>hostname:path_to_trail</pre> <p>The <i>hostname</i> matches the hostname in the audit log names, which look like this:</p> <pre>timestamp1.timestamp2.hostname</pre>
Microsoft Windows	Event log	<pre>security (case-insensitive)</pre> <p>You can use any case combination in the word <i>security</i>. However, once you start collecting a trail using a particular case combination, you must use the same combination in subsequent collections, otherwise, a new audit trail will start collecting records from the start of the security event log.</p>
Microsoft Active Directory Server	Event log	<pre>directory service or security (case-insensitive)</pre> <p>You can use any case combination in the words <i>directory service</i> or <i>security</i>. However, once you start collecting a trail using a particular case combination, you must use the same combination in subsequent collections, otherwise, a new audit trail will start collecting records from the start of the security event log.</p>
Oracle ACFS	Directory	<p>The path to the directory containing XML audit files. For example, for a file system mounted at <i>\$MOUNT_POINT</i>, the audit trail location is:</p> <pre>\$MOUNT_POINT/.Security/audit/</pre>
Linux	Directory	Default location of <i>audit.log</i> (<i>/var/log/audit/audit*.log</i>) or any custom location configured in the <i>/etc/audit/auditd.conf</i> file
AIX	Directory	<i>/audit/trail</i>

 **See Also:**

- [Adding an Audit Trail in the Audit Vault Server](#) (page 6-9)
- [Converting Audit Record Format For Collection](#) (page 6-14)

C

REDO Logs Audit Data Collection Reference

Topics

- [About the Recommended Settings for Collection from REDO Logs](#) (page C-1)
- [Oracle Database 11g Release 2 \(11.2\) and 12c Secured Target Audit Parameter Recommendations](#) (page C-2)
- [Oracle Database 11g Release 1 \(11.1\) Secured Target Audit Parameter Recommendations](#) (page C-8)
- [Oracle Database 10g Release 2 \(10.2\) Secured Target Audit Parameter Recommendations](#) (page C-13)
- [Populating Client ID In Reports for REDO Collector](#) (page C-18)

C.1 About the Recommended Settings for Collection from REDO Logs

This chapter describes recommendations for setting initialization parameters if you plan to use the TRANSACTION LOG audit trail type to collect audit data from the REDO logs of an Oracle Database secured target. After you change the initialization parameters described in these sections, you must restart the secured target database before configuring the TRANSACTION LOG audit trail to collect audit data.



Note:

- The Transaction Log collector uses Streams to collect the Audit Trail. When Transaction Log trail is added, it creates the capture process on the secured target. When the capture process begins, it creates a Logminer dictionary in an archive log. From then onwards, only the *Before and After* records from the archive logs is captured. It is not possible to acquire the *Before and After* values prior to the creation of Logminer dictionary. So Transaction Log trail cannot capture the old data. This is a limitation.
- While setting up REDO collector, no role should be granted to the source user other than `DV_STREAMS_ADMIN`. To set up `DVSYS.AUDIT_TRAIL$` table trail, first set up the REDO collector with `DV_STREAMS_ADMIN` role granted to the source user. Once REDO collector is up and running, grant `DV_SECANALYST` role to the source user.

 **See Also:**

- [Oracle Database Setup Scripts](#) (page B-22) for instructions on setting up privileges in the Oracle Database for collecting audit data from the REDO logs.
- *Oracle Audit Vault and Database Firewall Auditor's Guide* for instructions on creating a capture rule for redo log files

C.2 Oracle Database 11g Release 2 (11.2) and 12c Secured Target Audit Parameter Recommendations

For best results in a REDO collection environment, set the following initialization parameters at each participating database: COMPATIBLE, GLOBAL_NAMES, _job_queue_interval, SGA_TARGET, STREAMS_POOL_SIZE.

 **Note:**

Oracle Audit Vault and Database Firewall REDO collector does not support Oracle 12c pluggable databases (PDBs) or multitenant container databases (CDBs).

[Table C-1](#) (page C-2) lists the initialization parameters that you must configure for each secured target database that will use the TRANSACTION LOG audit trail.

Table C-1 Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
COMPATIBLE	Mandatory	Default: 11.2.0 Range: 10.0.0 to default release Modifiable? No	This parameter specifies the release with which the Oracle server must maintain compatibility. Oracle servers with different compatibility levels can interoperate. To use the new Oracle Streams features introduced in Oracle Database 11g Release 2, this parameter must be set to 11.2.0 or higher.

Table C-1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
GLOBAL_NAMES	Recommended	Default: false Range: true or false Modifiable? Yes	Specifies whether a database link is required to have the same name as the database to which it connects. Recommended value is TRUE. Ensure that the global name for the secured target database is a fully qualified name (for example, orcl.example.com). If you must change the global database, then run the following ALTER statement in SQL*Plus: <pre>ALTER DATABASE RENAME GLOBAL_NAME TO new_name;</pre> To use Oracle Streams to share information between databases, set this parameter to true at each database that is participating in your Oracle Streams environment.
LOG_ARCHIVE_CONFIG	Recommended	Default: 'SEND, RECEIVE, NODG_CONFIG' Range: Values: <ul style="list-style-type: none"> • SEND • NOSEND • RECEIVE • NORECEIVE • DG_CONFIG • NODG_CONFIG Modifiable? Yes	Enables or disables the sending of redo logs to remote destinations and the receipt of remote redo logs, and specifies the unique database names (DB_UNIQUE_NAME) for each database in the Data Guard configuration To use downstream capture and copy the redo data to the downstream database using redo transport services, specify the DB_UNIQUE_NAME of the secured target database and the downstream database using the DG_CONFIG attribute. This parameter must be set at both the secured target database and the downstream database.
LOG_ARCHIVE_DEST_n	Recommended	Default: None Range: None Modifiable? Yes	Defines up to 31 log archive destinations, where <i>n</i> is 1, 2, 3, ... 31. To use downstream capture and copy the redo data to the downstream database using redo transport services, at least one log archive destination must be set at the site running the downstream capture process.
LOG_ARCHIVE_DEST_STATE_n	Recommended	Default: enable Range: One of the following: <ul style="list-style-type: none"> • alternate • defer • enable Modifiable? Yes	Specifies the availability state of the corresponding destination. The parameter suffix (1 through 31) specifies one of the corresponding LOG_ARCHIVE_DEST_n destination parameters. To use downstream capture and copy the redo data to the downstream database using redo transport services, ensure that the destination that corresponds to the LOG_ARCHIVE_DEST_n destination for the downstream database is set to enable.

Table C-1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
LOG_BUFFER	Recommended	Default: 5 MB to 32 MB depending on configuration Range: Operating system-dependent Modifiable? No	Specifies the amount of memory (in bytes) that Oracle uses when buffering redo entries to a redo log file. Redo log entries contain a record of the changes that have been made to the database block buffers. If an Oracle Streams capture process is running on the database, then set this parameter properly so that the capture process reads redo log records from the redo log buffer rather than from the hard disk.
MEMORY_MAX_TARGET	Recommended	Default: 0 Range: 0 to the physical memory size available to Oracle Database Modifiable? No	Specifies the maximum systemwide usable memory for an Oracle database. If the MEMORY_TARGET parameter is set to a nonzero value, then set this parameter to a large nonzero value if you must specify the maximum memory usage of the Oracle database.
MEMORY_TARGET	Recommended	Default: 0 Range: 152 MB to MEMORY_MAX_TARGET setting Modifiable? Yes	Specifies the systemwide usable memory for an Oracle database. Oracle recommends enabling the autotuning of the memory usage of an Oracle database by setting MEMORY_TARGET to a large nonzero value (if this parameter is supported on your platform).
OPEN_LINKS	Recommended	Default: 4 Range: 0 to 255 Modifiable? No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, as well as external procedures and cartridges, each of which uses a separate process. In an Oracle Streams environment, ensure that this parameter is set to the default value of 4 or higher.
PROCESSES	Recommended	Default: 100 Range: 6 to operating system-dependent Modifiable? No	Specifies the maximum number of operating system user processes that can simultaneously connect to Oracle. Ensure that the value of this parameter allows for all background processes, such as locks and slave processes. In Oracle Streams, capture processes, apply processes, XStream inbound servers, and XStream outbound servers use background processes. Propagations use background processes in combined capture and apply configurations. Propagations use Oracle Scheduler slave processes in configurations that do not use combined capture and apply.

Table C-1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
SESSIONS	Recommended	Default: Derived from: (1.1 * PROCESSES) + 5 Range: 1 to 2 ³¹ Modifiable? No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes, apply processes, XStream outbound servers, or XStream inbound servers in a database, you might need to increase the size of this parameter. Each background process in a database requires a session.
SGA_MAX_SIZE	Mandatory	Default: Initial size of SGA at startup Range: 0 to operating system-dependent Modifiable? No	Specifies the maximum size of System Global Area (SGA) for the lifetime of a database instance. If the SGA_TARGET parameter is set to a nonzero value, then set this parameter to a large nonzero value if you must specify the SGA size.
SGA_TARGET	Mandatory	Default: 0 (SGA autotuning is disabled) Range: 64 MB to operating system-dependent Modifiable? Yes	Specifies the total size of all System Global Area (SGA) components. If MEMORY_MAX_TARGET and MEMORY_TARGET are set to 0 (zero), then Oracle recommends enabling the autotuning of SGA memory by setting SGA_TARGET to a large nonzero value. If this parameter is set to a nonzero value, then the size of the Oracle Streams pool is managed by Automatic Shared Memory Management.

Table C-1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
SHARED_POOL_SIZE	Recommended	<p>Default: When SGA_TARGET is set to a nonzero value: If the parameter is not specified, then the default is 0 (internally determined by Oracle Database). If the parameter is specified, then the user-specified value indicates a minimum value for the shared memory pool.</p> <p>When SGA_TARGET is not set (32-bit platforms): 64 MB, rounded up to the nearest granule size.</p> <p>When SGA_TARGET is not set (64-bit platforms): 128 MB, rounded up to the nearest granule size.</p> <p>Range: The granule size to operating system-dependent</p> <p>Modifiable? Yes</p>	<p>Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures.</p> <p>If the MEMORY_MAX_TARGET, MEMORY_TARGET, SGA_TARGET, and STREAMS_POOL_SIZE initialization parameters are set to zero, then Oracle Streams transfers an amount equal to 10% of the shared pool from the buffer cache to the Oracle Streams pool.</p>

Table C-1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE	Mandatory	<p>Default: 0</p> <p>Range: 0 to operating system-dependent limit</p> <p>Modifiable? Yes</p>	<p>Specifies (in bytes) the size of the Oracle Streams pool. The Oracle Streams pool contains buffered queue messages. In addition, the Oracle Streams pool is used for internal communications during parallel capture and apply.</p> <p>If the <code>MEMORY_TARGET</code> or <code>MEMORY_MAX_TARGET</code> initialization parameter is set to a nonzero value, then the Oracle Streams pool size is set by Automatic Memory Management, and <code>STREAMS_POOL_SIZE</code> specifies the minimum size.</p> <p>If the <code>SGA_TARGET</code> initialization parameter is set to a nonzero value, then the Oracle Streams pool size is set by Automatic Shared Memory Management, and <code>STREAMS_POOL_SIZE</code> specifies the minimum size.</p> <p>This parameter is modifiable. If this parameter is reduced to zero when an instance is running, then Oracle Streams processes and jobs might not run.</p> <p>Ensure that there is enough memory to accommodate the Oracle Streams components. The following are the minimum requirements:</p> <ul style="list-style-type: none"> • 15 MB for each capture process parallelism • 10 MB or more for each buffered queue. The buffered queue is where the buffered messages are stored. • 1 MB for each apply process parallelism • 1 MB for each XStream outbound server • 1 MB for each XStream inbound server parallelism <p>For example, if parallelism is set to 3 for a capture process, then at least 45 MB is required for the capture process. If a database has two buffered queues, then at least 20 MB is required for the buffered queues. If parallelism is set to 4 for an apply process, then at least 4 MB is required for the apply process.</p> <p>You can use the <code>V\$STREAMS_POOL_ADVICE</code> dynamic performance view to determine an appropriate setting for this parameter.</p>

Table C-1 (Cont.) Initialization Parameters for an Oracle 11.2 or 12c Secured Target Database

Parameter	Mandatory or Recommended Parameter	Default Value	Description
TIMED_STATISTICS	Recommended	Default: If STATISTICS_LEVEL is set to TYPICAL or ALL, then true If STATISTICS_LEVEL is set to BASIC, then false The default for STATISTICS_LEVEL is TYPICAL. Range: true or false Modifiable? Yes	Specifies whether statistics related to time are collected. To collect elapsed time statistics in the dynamic performance views related to Oracle Streams, set this parameter to true. The views that include elapsed time statistics include: V\$STREAMS_CAPTURE, V\$STREAMS_APPLY_COORDINATOR, V\$STREAMS_APPLY_READER, V\$STREAMS_APPLY_SERVER.
UNDO_RETENTION	Recommended	Default: 900 Range: 0 to 2 ³² - 1 Modifiable? Yes	Specifies (in seconds) the amount of committed undo information to retain in the database. For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period. If you run one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least 3600. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the UNDO_RETENTION setting.

C.3 Oracle Database 11g Release 1 (11.1) Secured Target Audit Parameter Recommendations

For best results in a REDO collection environment, set the following initialization parameters at each participating database: `compatible`, `GLOBAL_NAMES`, `_job_queue_interval`, `SGA_TARGET`, `STREAMS_POOL_SIZE`.

[Table C-2](#) (page C-8) describes the hidden parameter that you must configure for each secured target database that will use the TRANSACTION LOG audit trail.

Table C-2 Hidden Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
<code>_job_queue_interval=1</code>	Recommended	5	Scan rate interval (seconds) of job queue

Table C-3 (page C-9) lists the initialization parameters that you must configure for each secured target database that will use the TRANSACTION LOG audit trail. Enable autotuning of the various pools within the SGA, by setting `SGA_TARGET` to a large nonzero value. Leave the `STREAMS_POOL_SIZE` value set to 0. The combination of these to parameters enables autotuning of the SGA and the Streams Pool size will be automatically adjusted to meet the workload requirements.

Table C-3 Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
<code>COMPATIBLE=11.1.0</code>	Mandatory	Default: 11.1.0 Range: 10.1.0 to Current Release Number Modifiable? No	This parameter specifies the release with which the Oracle server must maintain compatibility. Oracle servers with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10g release 1, this parameter must be set to 10.1.0 or higher. To use downstream capture, this parameter must be set to 10.1.0 or higher at both the secured target database and the downstream database. To use the new Streams features introduced in Oracle Database 10g release 2, this parameter must be set to 10.2.0 or higher. To use the new Streams features introduced in Oracle Database 11g release 1, this parameter must be set to 11.1.0 or higher.
<code>GLOBAL_NAMES=true</code>	Recommended	Default: false Range: true or false Modifiable? Yes	Specifies whether a database link is required to have the same name as the database to which it connects. To use Streams to share information between databases, set this parameter to <code>true</code> at each database that is participating in your Streams environment.
<code>JOB_QUEUE_PROCESSES=4</code>	Mandatory	Default: 0 Range: 0 to 1000 Modifiable? Yes	Specifies the number of <i>Jnnn</i> job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by <code>DBMS_JOB</code> . This parameter must be set to at least 2 at each database that is propagating events in your Streams environment, and should be set to the same value as the maximum number of jobs that can run simultaneously plus two.

Table C-3 (Cont.) Initialization Parameters for a Release 11.1 Secured Target Database


Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
LOG_ARCHIVE_DEST_n	Recommended	Default: None Range: None Modifiable? Yes	Defines up to ten log archive destinations, where n is 1, 2, 3, ... 10. To use downstream capture and copy the redo log files to the downstream database using log transport services, at least one log archive destination must be at the site running the downstream capture process.
<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;">  See Also: <i>Oracle Data Guard Concepts and Administration</i> </div>			
LOG_ARCHIVE_DEST_STATE_n	Recommended	Default: enable Range: One of the following: alternate reset defer enable Modifiable? Yes	Specifies the availability state of the corresponding destination. The parameter suffix (1 through 10) specifies one of the ten corresponding LOG_ARCHIVE_DEST_n destination parameters. To use downstream capture and copy the redo log files to the downstream database using log transport services, ensure that the destination that corresponds to the LOG_ARCHIVE_DEST_n destination for the downstream database is set to enable.
OPEN_LINKS	Recommended	Default: 4 Range: 0 to 255 Modifiable? No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, as well as external procedures and cartridges, each of which uses a separate process. In a Streams environment, ensure that this parameter is set to the default value of 4 or higher.
PROCESSES	Recommended	Default: Derived from PARALLEL_MAX_SERVERS Range: 6 to operating system dependent limit Modifiable? No	Specifies the maximum number of operating system user processes that can simultaneously connect to Oracle. Ensure that the value of this parameter allows for all background processes, such as locks, job queue processes, and parallel execution processes. In Streams, capture processes and apply processes use background processes and parallel execution processes, and propagation jobs use job queue processes.
SESSIONS	Recommended	Default: Derived from: (1.1 * PROCESSES) + 5 Range: 1 to 231 Modifiable? No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes or apply processes in a database, then you may need to increase the size of this parameter. Each background process in a database requires a session.

Table C-3 (Cont.) Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SGA_MAX_SIZE Increase by at least 200M	Mandatory	Default: Initial size of SGA at startup Range: 0 to operating system dependent limit Modifiable? No	Specifies the maximum size of SGA for the lifetime of a database instance. To run multiple capture processes on a single database, you may need to increase the size of this parameter. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
SGA_TARGET >0 Increase this parameter by at least 200M.	Mandatory	Default: 0 (SGA autotuning is disabled) Range: 64 to operating system-dependent Modifiable? Yes	Specifies the total size of all System Global Area (SGA) components. If this parameter is set to a nonzero value, then the size of the Streams pool is managed by Automatic Shared Memory Management. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
SHARED_POOL_SIZE =0	Recommended	Default: 32-bit platforms: 32 MB, rounded up to the nearest granule size 64-bit platforms: 84 MB, rounded up to the nearest granule size Range: Minimum: the granule size Maximum: operating system-dependent Modifiable? Yes	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. If the SGA_TARGET and STREAMS_POOL_SIZE initialization parameters are set to zero, then Streams transfers an amount equal to 10% of the shared pool from the buffer cache to the Streams pool. The STREAMS_POOL_SIZE initialization parameter should be set to 200 MB and, if necessary, increment the SGA_TARGET and SGA_MAX initialization parameters appropriately. For example, if the SGA_TARGET initialization parameter is already set to 2 GB, setting STREAMS_POOL_SIZE=200 MB would not require that the SGA_TARGET initialization parameter be increased. However, if the SGA_TARGET initialization parameter is set to 600 MB and the STREAMS_POOL_SIZE initialization parameter is increased to 200 MB, then it is recommended that the SGA_TARGET initialization parameter value be increased similarly.

Table C-3 (Cont.) Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE=200	Mandatory	Default: 0 Range: Minimum: 0 Maximum: operating system-dependent Modifiable? Yes	Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, the Streams pool is used for internal communications during parallel capture and apply. If the SGA_TARGET initialization parameter is set to a nonzero value, then the Streams pool size is set by Automatic Shared memory management, and STREAMS_POOL_SIZE specifies the minimum size. This parameter is modifiable. If this parameter is reduced to zero when an instance is running, then Streams processes and jobs will not run. You should increase the size of the Streams pool for each of the following factors: 10 MB for each capture process parallelism 10 MB or more for each buffered queue. The buffered queue is where the Logical Change Records (LCRs) are stored. 1 MB for each apply process parallelism You can use the V\$STREAMS_POOL_ADVICE dynamic performance view to determine an appropriate setting for this parameter. For example, if parallelism is set to 3 for a capture process, then increase the Streams pool by 30 MB. If parallelism is set to 5 for an apply process, then increase the Streams pool by 5 MB.
TIMED_STATISTICS	Recommended	Default: If STATISTICS_LEVEL is set to TYPICAL or ALL, then true If STATISTICS_LEVEL is set to BASIC, then false The default for STATISTICS_LEVEL is TYPICAL. Range: true or false Modifiable? Yes	Specifies whether statistics related to time are collected. To collect elapsed time statistics in the data dictionary views related to Stream, set this parameter to true. The views that include elapsed time statistics include: V\$STREAMS_CAPTURE V\$STREAMS_APPLY_COORDINATOR V\$STREAMS_APPLY_READER V\$STREAMS_APPLY_SERVER

Table C-3 (Cont.) Initialization Parameters for a Release 11.1 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
UNDO_RETENTION=3600	Recommended	Default: 900 Range: 0 to 2 ³² -1 (max value represented by 32 bits) Modifiable? Yes	Specifies (in seconds) the amount of committed undo information to retain in the database. For a database running one or more capture processes, ensure that this parameter is set to specify an adequate undo retention period. If you are running one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least 3600. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the UNDO_RETENTION setting. See Also: <i>Oracle Database Administrator's Guide</i> for more information about the UNDO_RETENTION parameter

C.4 Oracle Database 10g Release 2 (10.2) Secured Target Audit Parameter Recommendations

For best results in a REDO collection environment, set the following initialization parameters at each participating database: COMPATIBLE, GLOBAL_NAMES, _job_queue_interval, SGA_TARGET, STREAMS_POOL_SIZE.

[Table C-4](#) (page C-13) describes the hidden parameter that you must configure for each secured target database that will use the TRANSACTION LOG audit trail.

Table C-4 Hidden Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
_job_queue_interval=1	Recommended	5	Scan rate interval (seconds) of job queue

[Table C-5](#) (page C-14) lists the initialization parameters that you must configure for each secured target database. Enable autotuning of the various pools within the SGA, by setting SGA_TARGET to a large nonzero value. Leave the STREAMS_POOL_SIZE value set to 0. The combination of these two parameters enables autotuning of the SGA and the Streams Pool size will be automatically adjusted to meet the workload requirements.

Table C-5 Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
COMPATIBLE=10.2.0	Mandatory	Default: 10.0.0 Range: 10.0.0 to Current Release Number Modifiable? No	This parameter specifies the release with which the Oracle database must maintain compatibility. Oracle databases with different compatibility levels can interoperate. To use the new Streams features introduced in Oracle Database 10g release 1, set this parameter to 10.1.0 or higher. To use downstream capture, set this parameter 10.1.0 or higher for both the secured target database and the downstream database. To use the new Streams features introduced in Oracle Database 10g release 2, set this parameter to 10.2.0 or higher.
GLOBAL_NAMES=true	Recommended	Default: false Range: true or false Modifiable? Yes	Specifies whether a database link is required to have the same name as the database to which it connects. To use Streams to share information between databases, set this parameter to <code>true</code> for each database that participates in your Streams environment.
JOB_QUEUE_PROCESSES=4	Mandatory	Default: 0 Range: 0 to 1000 Modifiable? Yes	Specifies the number of job queue processes for each instance (J000 ... J999). Job queue processes handle requests created by the <code>DBMS_JOB</code> PL/SQL package. Set this parameter to at least 2 for each database that propagates events in your Streams environment, and then set it to the same value as the maximum number of jobs that can run simultaneously, plus 2.
LOG_ARCHIVE_DEST_n	Recommended	Default: None Range: None Modifiable? Yes	Defines up to ten log archive destinations, where <i>n</i> is 1, 2, 3, ... 10. To use downstream capture and copy the redo log files to the downstream database using log transport services, at least one log archive destination must be at the site running the downstream capture process.

**See Also:**

Oracle Data Guard Concepts and Administration

Table C-5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
LOG_ARCHIVE_DEST_ STATE_ n	Recommended	Default: enable Range: One of the following: alternate reset defer enable Modifiable? Yes	Specifies the availability state of the corresponding destination. The parameter suffix (1 through 10) specifies one of the ten corresponding LOG_ARCHIVE_DEST_ n destination parameters. To use downstream capture and copy the redo log files to the downstream database using log transport services, ensure that the destination that corresponds to the LOG_ARCHIVE_DEST_ n destination for the downstream database is set to enable.
OPEN_LINKS	Recommended	Default: 4 Range: 0 to 255 Modifiable? No	Specifies the maximum number of concurrent open connections to remote databases in one session. These connections include database links, external procedures, and cartridges, each of which uses a separate process. In a Streams environment, set this parameter to the default value of 4 or higher.
PARALLEL_MAX_SERVERS Set this parameter to at least 20.	Mandatory	Default: Derived from the values of the following parameters: CPU_COUNT PARALLEL_ADAPTIVE_MULTI_USER PARALLEL_AUTOMATIC_TUNING Range: 0 to 3599 Modifiable? Yes	Specifies the maximum number of parallel execution processes and parallel recovery processes for an instance. As demand increases, Oracle Database increases the number of processes from the number created at instance startup up to this value. In a Streams environment, each capture process and apply process can use multiple parallel execution servers. Set this initialization parameter to an appropriate value to ensure that there are enough parallel execution servers.
PROCESSES	Recommended	Default: Derived from PARALLEL_MAX_SERVERS Range: 6 to operating system dependent limit Modifiable? No	Specifies the maximum number of operating system user processes that can simultaneously connect to an Oracle database. Ensure that the value of this parameter allows for all background processes, such as locks, job queue processes, and parallel execution processes. In Streams, capture processes and apply processes use background processes and parallel execution processes, and propagation jobs use job queue processes.
SESSIONS	Recommended	Default: Derived from: (1.1 * PROCESSES) + 5 Range: 1 to 231 Modifiable? No	Specifies the maximum number of sessions that can be created in the system. To run one or more capture processes or apply processes in a database, then you may need to increase the size of this parameter. Each background process in a database requires a session.

Table C-5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
SGA_MAX_SIZE Increase by at least 200M	Mandatory	Default: Initial size of SGA at startup Range: 0 to operating system dependent limit Modifiable? No	Specifies the maximum size of SGA for the lifetime of a database instance. To run multiple capture processes on a single database, you may need to increase the size of this parameter. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
SGA_TARGET >0 Increase this parameter by at least 200M.	Mandatory	Default: 0 (SGA autotuning is disabled) Range: 64 to operating system-dependent Modifiable? Yes	Specifies the total size of all System Global Area (SGA) components. If you set this parameter to a nonzero value, then the size of the Streams pool is managed by Automatic Shared Memory Management. See the STREAMS_POOL_SIZE initialization parameter for more specific recommendations.
SHARED_POOL_SIZE =0	Recommended	Default: 32-bit platforms: 32 MB, rounded up to the nearest granule size 64-bit platforms: 84 MB, rounded up to the nearest granule size Range: Minimum: the granule size Maximum: operating system-dependent Modifiable? Yes	Specifies (in bytes) the size of the shared pool. The shared pool contains shared cursors, stored procedures, control structures, and other structures. If you set the SGA_TARGET and STREAMS_POOL_SIZE initialization parameters to zero, then Streams transfers an amount equal to 10 percent of the shared pool from the buffer cache to the Streams pool.

Table C-5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
STREAMS_POOL_SIZE=200	Mandatory	Default: 0 Range: Minimum: 0 Maximum: operating system-dependent Modifiable? Yes	<p>Specifies (in bytes) the size of the Streams pool. The Streams pool contains captured events. In addition, Oracle Database uses the Streams pool for internal communications during parallel capture and apply.</p> <p>If you set the <code>SGA_TARGET</code> initialization parameter to a nonzero value, then the Streams pool size is set by Automatic Shared memory management, and <code>STREAMS_POOL_SIZE</code> specifies the minimum size.</p> <p>You should set the <code>STREAMS_POOL_SIZE</code> initialization parameter to 200 MB and, if necessary, increment the <code>SGA_TARGET</code> and <code>SGA_MAX</code> initialization parameters appropriately. For example, if the <code>SGA_TARGET</code> initialization parameter is already set to 2 GB, setting <code>STREAMS_POOL_SIZE=200 MB</code> does not require you to increase the <code>SGA_TARGET</code> initialization parameter setting. However, if the <code>SGA_TARGET</code> initialization parameter is set to 600 MB and the <code>STREAMS_POOL_SIZE</code> initialization parameter is increased to 200 MB, then you should increase the <code>SGA_TARGET</code> initialization parameter value similarly.</p> <p>This parameter is modifiable. If you reduce this parameter setting to zero when an instance is running, then Streams processes and jobs cannot run.</p> <p>You should increase the size of the Streams pool for each of the following factors:</p> <ul style="list-style-type: none"> • 10 MB for each capture process parallelism • 10 MB or more for each buffered queue. The buffered queue is where the Logical Change Records (LCRs) are stored. • 1 MB for each apply process parallelism <p>You can use the <code>V\$STREAMS_POOL_ADVICE</code> dynamic performance view to determine an appropriate setting for this parameter.</p> <p>For example, if you set parallelism to 3 for a capture process, then increase the Streams pool by 30 MB. If you set parallelism to 5 for an apply process, then increase the Streams pool by 5 MB.</p>

Table C-5 (Cont.) Initialization Parameters for a Release 10.2 Secured Target Database

Parameter Name and Recommendation	Mandatory or Recommended Parameter	Default Value	Description
TIMED_STATISTICS	Recommended	<p>Default: If STATISTICS_LEV EL is set to TYPICAL or ALL, then true</p> <p>If STATISTICS_LEV EL is set to BASIC, then false</p> <p>The default for STATISTICS_LEV EL is TYPICAL.</p> <p>Range: true or false</p> <p>Modifiable? Yes</p>	<p>Specifies whether statistics related to time are collected.</p> <p>To collect elapsed time statistics in the data dictionary views related to Stream, set this parameter to true. The following views include elapsed time statistics:</p> <p>V\$STREAMS_CAPTURE V\$STREAMS_APPLY_COORDINATOR V\$STREAMS_APPLY_READER V\$STREAMS_APPLY_SERVER</p>
UNDO_RETENTION=3600	Recommended	<p>Default: 900</p> <p>Range: 0 to 2³²-1 (max value represented by 32 bits)</p> <p>Modifiable? Yes</p>	<p>Specifies (in seconds) the amount of committed undo information to retain in the database.</p> <p>For a database running one or more capture processes, set this parameter to specify an adequate undo retention period.</p> <p>If you are running one or more capture processes and you are unsure about the proper setting, then try setting this parameter to at least 3600. If you encounter "snapshot too old" errors, then increase the setting for this parameter until these errors cease. Ensure that the undo tablespace has enough space to accommodate the UNDO_RETENTION setting.</p> <p>See Also: <i>Oracle Database Administrator's Guide</i> for more information about the UNDO_RETENTION parameter</p>

C.5 Populating Client ID In Reports for REDO Collector

Generate client identifiers in your event log reports for REDO Collector.

Use this procedure to generate the Client ID in the event log report for REDO Collector.

 **Note:**

This functionality is available on *Oracle Audit Vault and Database Firewall* release 12.2.0.5.0 or later.

The user has to download and install one or more mandatory patches so that the REDO collector can populate the Client ID column in the event log report. The **Data Modification Before-After Values Report** also contains the Client ID.

Platform and Database Release Support Matrix

Database Release Version	Platform
11.2.0.4.0	HP-UX Itanium
11.2.0.4.0	HP-UX PA-RISC (64-bit)
11.2.0.4.0	IBM AIX
11.2.0.4.0	Linux x86-64
11.2.0.4.0	Oracle Solaris x86-64
11.2.0.4.0	Oracle Solaris SPARC
12.1.0.2.0	HP-UX Itanium
12.1.0.2.0	Oracle Solaris x86-64
12.1.0.2.0	Oracle Solaris SPARC
12.1.0.2.0	Linux x86-64
12.1.0.2.161018ProactiveBP	Linux x86-64
12.1.0.2.170418ProactiveBP	Linux x86-64
12.1.0.2.170418	Linux x86-64



Note:

Check **My Oracle Support** for the latest available patches.

To download and install the patches, do the following:

1. Log in to My Oracle Support.
2. Click **Patches & Updates**.
3. Select **Patch name or Number**.
4. Enter the patch number as 25516250.
5. Click **Search**.
6. Download and install the patch.



Note:

In case of any issues, use the help documentation available. Select the patch, and then click **Read Me** button in the pop-up to access the same.

D

Ports Used by Audit Vault and Database Firewall

This appendix lists the TCP and UDP ports used by Oracle Audit Vault and Database Firewall.

Topics

- [Ports Required When Database Firewall is Deployed for Secured Targets](#) (page D-1)
- [Ports for Services Provided by Oracle Audit Vault Server](#) (page D-2)
- [Ports for Services Provided by the Database Firewall](#) (page D-2)
- [Ports for External Network Access by the Audit Vault Server](#) (page D-3)
- [Ports for External Network Access by the Database Firewall](#) (page D-4)
- [Ports for Internal TCP Communication](#) (page D-5)

D.1 Ports Required When Database Firewall is Deployed for Secured Targets

These following two classes of ports must be open in external network firewalls for these Database Firewall deployments:

- When a Database Firewall is configured to protect a Secured Target database, traffic directed to that database must be able to pass through external network firewalls to the Database Firewall. The ports required are configured in the Secured Target's page in the Audit Vault Server.
- A Database Firewall can be configured to accept proxy connections, which are passed on to the database. The ports required for the proxy connection are configured in the Network Configuration page on the Database Firewall.

Note:

It is recommend that you do not change these ports.

See Also:

- [Registering or Removing Secured Targets in the Audit Vault Server](#) (page 6-2)
- [Configuring Oracle Database Firewall As A Traffic Proxy](#) (page 4-11)

D.2 Ports for Services Provided by Oracle Audit Vault Server

Learn about the ports for services that are provided by Oracle Audit Vault Server.

[Table D-1](#) (page D-2) lists the ports for services that are provided by Oracle 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 Oracle Audit Vault Server.

Table D-1 Ports for Services Provided by Audit Vault Server

Port	Protocol Family	Protocol	Purpose	Notes
22	TCP	SSH	Command line access to system	Disabled by default
161	UDP	SNMP	SNMP Access	Disabled by default
443	TCP	HTTPS	Administration Console (web interface)	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	TCPS	Audit Vault Servers in high availability mode.	This is between primary and secondary Audit Vault Servers when high availability is configured.

D.3 Ports for Services Provided by the Database Firewall

[Table D-2](#) (page D-2) lists ports for general services provided by the Database Firewall. These services are used by outside users of the system, and access to all them can be controlled within the Audit Vault and Database Firewall system. If external network firewalls are used, these ports must be open to allow connections from the users (clients) of these services to the Database Firewall(s) in the Audit Vault and Database Firewall system.

Table D-2 Ports for Services Provided by Database Firewall

Port	Protocol Family	Protocol	Purpose	Notes
22	TCP	SSH	Command line access to system	Disabled by default
161	UDP	SNMP	SNMP Access	Disabled by default
443	TCP	HTTPS	Administration Console (web interface)	None

Table D-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. The Host Monitor forwards the data securely to Database Firewall.	<p>This applies when deployed in Host Monitor mode and ports need not be open during out-of-band, in-line bridge, or proxy mode.</p> <p>For each enforcement point, a unique port is created in the given range. The exact port for each enforcement point can be found at <code>/usr/local/dbfw/va/XX/etc/appliance.conf</code> where <code>XX</code> represents the enforcement points created and have the value of <code>1, 2, 3, ..., N</code>.</p> <p><code>REMOTE_AGENT_LISTEN_PORT</code> is the key in <code>appliance.conf</code> file that represents the port Database Firewall is listening for data from Host Monitor.</p>
2050 - 5100	TCP	Syslog	Incoming WAF (F5) violation alerts	<p>The exact port number used by an enforcement point can be found in the Advanced settings page of the enforcement point.</p> <p>See Also: Finding the Port Number Used by an Enforcement Point (page 6-24)</p>

D.4 Ports for External Network Access by the Audit Vault Server

[Table D-3](#) (page D-3) lists ports for external services that may be used by the Audit Vault Server. If external network firewalls are used, the relevant ports must be open so that the Audit Vault Server can use these services as a client.

Table D-3 Ports for External Network Access by the Audit Vault Server

Port	Protocol Family	Protocol	Purpose	Notes
25	TCP	SMTP	Email delivery	None
53	UDP	DNS	Domain name service	None
123	UDP and TCP	NTP	Time Synchronization	None

Table D-3 (Cont.) Ports for External Network Access by the Audit Vault Server

Port	Protocol Family	Protocol	Purpose	Notes
514	UDP, or configured as TCP	Syslog	Syslog alerts	For TCP-transport connections to syslog server(s) the port must be configured in the Audit Vault Server console. See Also: Configuring Oracle Audit Vault Server Syslog Destinations (page 3-8)
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 (page 15-3)
Secured Target listener port. It is the same as the port provided in secured target location.	Oracle Database	TCP or TCPS	User Entitlement Reporting Stored Procedure Auditing Audit Policy Retrieval	The direct connection between Audit Vault Server and the Secured Target. The connection details is provided with the secured target location used.



See Also:

[Out-of-the Box Plug-ins at a Glance](#) (page B-2) for a complete list of supported secured target types.

D.5 Ports for External Network Access by the Database Firewall

[Table D-4](#) (page D-4) lists ports for external services that may be used by the Database Firewall. If external network firewalls are used, the relevant ports must be open so that the Database Firewall can use these services as a client.

Table D-4 Ports for External Network Access by the Database Firewall

Port	Protocol Family	Protocol	Purpose	Notes
53	UDP	DNS	Domain name service	None
123	UDP and TCP	NTP	Time Synchronization	None

Table D-4 (Cont.) Ports for External Network Access by the Database Firewall

Port	Protocol Family	Protocol	Purpose	Notes
514	UDP, or configured as TCP	Syslog	Syslog alerts	For TCP-transport connections to syslog server(s) the port must be configured in the Audit Vault Server console.
514	TCP	WAF (F5) alerts	WAF (F5) alerts	The port can be changed from the Audit Vault Server console.

**See Also:**

- [Configuring Oracle Audit Vault Server Syslog Destinations](#) (page 3-8)
- [Configuring Oracle Audit Vault and Database Firewall to Work with F5 BIG-IP Application Security Manager](#) (page 9-4)

D.6 Ports for Internal TCP Communication

Learn about ports for internal TCP communication between Oracle Database Firewall and Oracle Audit Vault Server.

[Table D-5](#) (page D-5) lists ports for services that are used between Oracle Database Firewall and Oracle Audit Vault Server. If you configure an external network firewall between these systems, then you must open the relevant ports.

Table D-5 Ports for Internal TCP Communication

Port	Protocol Family	Protocol	Direction	Notes
7443	TCP	HTTPS	<ul style="list-style-type: none"> • Oracle Database Firewall accepts connections from Oracle Audit Vault Server • Oracle Database Firewall accepts connections from Oracle 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	Oracle Audit Vault Server accepts connections from Database Firewall	Event reporting and monitoring

E

Message Code Dictionary

This appendix lists the following:

- [Audit Vault Messages](#) (page E-1)
- [Database Firewall Messages](#) (page E-40)

E.1 Audit Vault Messages

This table lists the Oracle 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 secured target "*string*"; audit trail does not exist.

Cause: User attempted to drop a trail which does not exist.

Action: One cannot drop audit trail which does not exist.

46518: start collection failed for plug-in:"*string*". plug-in does not exist.

Cause: User attempted to start collection for a secured target using a plug-in that does not exist.

Action: Check the plug-in specified in the command and re-try the command with a valid plug-in.

46519: start collection failed. host "string" is not registered with the audit vault server

Cause: User attempted to start a collection using a host which is not registered with the audit vault server.

Action: Register the host with the audit vault server, activate it, and then re-try the command.

46520: host with ip address "string" is already registered with the audit vault server

Cause: User attempted to register a host with an ip address that is already registered with an existing host.

Action: User cannot register two hosts with the same IP address.

46521: NULL value passed for a mandatory attribute

Cause: A mandatory attribute was set to a NULL value.

Action: Provide a non-NULL value for the mandatory attribute.

46522: mandatory attribute string missing in the input

Cause: Mandatory attribute name was missing in the attribute value list.

Action: Provide the value for mandatory attribute.

46523: attempting to drop Event Category with active Events

Cause: Event Category specified had active Events.

Action: Drop the active Events before dropping this Event Category.

46524: at least one audit trail being collected for secured target

Cause: Secured Target specified had trails which were active.

Action: Stop all the active trails for the given Secured Target.

46525: Sourcetype-specific extension for Category already exists

Cause: Event Category was specified which already has a Format extension for the given 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 secured target '*string*'.

Cause: The specified attribute was not set for the secured target.

Action: Set the specified attribute for the secured target.

46533: Invalid lock type '*string*' specified.

Cause: An invalid 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 secured target address: address '*string*' is used by Secured Target '*string*'.

Cause: The user tried to add a duplicate address for a secured target.

Action: Check existing address for the secured target.

46536: firewall cannot be paired with itself

Cause: User tries to pair a firewall with itself.

Action: Choose a different firewall and try again.

46537: firewall *string* is not registered with the Audit Vault Server

Cause: User tries to create a resilient pair using a non-existent firewall.

Action: Register the firewall first and then try again.

46538: invalid enforcement point attribute "*string*". Run HELP *string* for help.

Cause: User attempted to alter an invalid attribute for the enforcement point.

Action: Check syntax and re-try the command with the correct syntax.

46539: Secured Target Name is too long.

Cause: Secured Target Name failed length validation checks.

Action: Provide valid Secured Target Name.

46540: Secured Target Description is too long.

Cause: Secured Target Description failed length validation checks.

Action: Provide valid Secured Target Description.

46541: attempting to drop Collector Type with active Collectors

Cause: One or more Collectors for this Collector Type were active.

Action: Drop all active Collectors for this Collector Type.

46542: attempting to drop an Agent with active Collectors

Cause: One or more Collectors for this Agent were active.

Action: Drop all active Collectors for this Agent.

46543: attempting to drop a Collector before disabling the collection

Cause: The collection for the Collector specified was not disabled.

Action: Disable the collection before dropping the Collector.

46544: attempting to drop an Agent before disabling it

Cause: The Agent specified was not disabled.

Action: Disable the Agent before dropping it.

46545: failed to start collection; trail is already being collected. 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 Secured Target Location requires setting User Name and Password; please specify User Name and Password along with the Secured Target Location.

Cause: The user tried to set secured target location without setting user name and password.

Action: Set user name and password along with the secured target location.

46548: Failed to generate secured target location string.

Cause: User did not specify the correct components of secured target location string.

Action: Specify the correct components of secured target location string and then try again.

46549: No NTP servers are specified.

Cause: The user chose to enable NTP synchronization, but did not specify any NTP server.

Action: Specify NTP server and then try again.

46550: Secured Target Location is required for registering this secured target.

Cause: User tried to register a secured target without providing secured target location, which is required to connect to the secured target.

Action: Provide secured target location and try again.

46551: attempting to change the type of an attribute currently in use

Cause: Attribute specified was in use.

Action: Provide an attribute that is not being used.

46552: attempting to drop an attribute currently in use

Cause: Attribute specified was in use.

Action: Provide an attribute that is not being used.

46553: attempting to change the type of an attribute without providing a new default value

Cause: Current type of the default value did not match with the new type specified.

Action: Provide a new default value for the attribute.

46554: Secured Target Location is too long.

Cause: Secured Target Location failed length validation checks.

Action: Provide valid Secured Target Location.

46555: User Name is too long.

Cause: User Name failed length validation checks.

Action: Provide valid User Name.

46556: Single and double quotes are not allowed in the User Name.

Cause: Illegal characters were supplied in the User Name.

Action: Remove single and double quotes from User Name.

46557: Password must contain at least 8 characters and at most 30 bytes.

Cause: Password failed length validation checks.

Action: Provide valid Password.

46558: Secured Target Attribute Name is too long.

Cause: Secured Target Attribute Name failed length validation checks.

Action: Provide valid Secured Target Attribute Name.

46559: Secured Target Attribute Value is too long.

Cause: Secured Target Attribute Value failed length validation checks.

Action: Provide valid Secured Target Attribute Value.

46560: Setting User Name and Password requires enabling Secured Target Location; please specify Secured Target Location along with User Name and Password.

Cause: The user tried to set user name and password without enabling secured target location.

Action: Set secured target location along with user name and password.

46561: no Format defined for the Source Type and Category

Cause: Format for the specified Source Type and Category pair was not present in the system.

Action: Provide Source Type and Category pair which already has a Format defined.

46562: error in Alert condition

Cause: Invalid Alert condition was specified.

Action: Correct the Alert condition.

46563: Attempt to delete alert '*string*' failed.

Cause: User is trying to drop an alert he does not own.

Action: Ask the owner of the alert to drop it.

46564: Setting alert threshold value to *string* failed.

Cause: An invalid value was specified for the alert threshold.

Action: Provide an alert threshold value in the valid range (> 1).

46565: Failed to update alert '*string*' due to insufficient privileges.

Cause: User is trying to update an alert he does not own.

Action: Ask the owner of the alert to update it.

46566: no changes specified

Cause: The user attempted to alter an alert, but no changes were specified.

Action: No action is required.

46567: Cannot modify, or delete built-in alert

Cause: The user attempted to alter, or delete a built-in alert.

Action: No action is required.

46568: Setting alert duration value to *string* failed.

Cause: An invalid value was specified for the alert duration.

Action: Provide an alert duration value in the valid range (≥ 0).

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 Secured Target.

Cause: User tried to start a collection of type network for a secured target which has no enforcement point configured.

Action: Configure an enforcement point for the secured target and then try again.

46592: firewall with name *string* and/or IP address *string* already exists.

Cause: User tries to register a firewall which already exists.

Action: Check the name and/or IP of the firewall then try again.

46593: secured target address does not exist. cannot drop secured target address.

Cause: User tries to drop a secured target address which does not exist.

Action: Check the secured target address and then try again.

46594: unable to resolve host *string*

Cause: The user did not provide an IP address when registering a host and the host name is not resolvable.

Action: Provide a valid IP address or a resolvable host name.

46595: failed to drop host *string*. agent process may be running and needs to be stopped first before dropping. if you already stopped the agent, please wait for the agent to be fully stopped.

Cause: User tries to drop a host on which an agent process is running or the agent has not been fully stopped.

Action: Stop the agent process first and then try again.

46596: host *string* has already been activated.

Cause: User tries to activate a host which has already been activated.

Action: Check the current status of the host.

46597: no pending activation request for host *string*.

Cause: Activation request for agent on host was not found.

Action: Request activation for the agent.

46598: stop collection failed for plug-in:"*string*". plug-in does not exist.

Cause: User attempted to stop collection for a secured target using a plug-in that does not exist.

Action: Check the plug-in specified in the command and re-try the command with a valid plug-in.

46599: internal error *string string string string string*

Cause: Internal error occurred in Audit Vault.

Action: Contact Oracle Support Services.

46601: The authenticated user is not authorized with audit source

Cause: User is not authorized to send audit data on behalf of this audit source.

Action: Connect as the user who is associated with the source. Or grant this user appropriate authorization by changing the source's properties.

46602: Error on audit record insert as RADS partition full

Cause: RADS partition table is full.

Action: Purge the RADS partition table through archive.

46603: Error on audit record insert as RADS_INVALID table full

Cause: RADS_INVALID table is full.

Action: Need to purge RADS_INVALID table or make its size larger.

46604: Error on insert as Error table full

Cause: Error table is full.

Action: Need to purge the error table.

46605: There are more recovery entries than the maximum member can be returned

Cause: There are more recovery entries for this collector.

Action: Need to purge the old entries from the recovery table.

46606: There is no recovery entry for the given name

Cause: There was no recovery context matching to the given name.

Action: Need to check if the name was correct or if the recovery context was saved for this name.

46607: There are more configuration entries than the maximum member can be returned

Cause: There were more configuration entries for this collector.

Action: Need to reduce the configuration entries for this collector.

46608: Failed to drop Secured Target; Stored Procedure Auditing collection is in progress.

Cause: User tried to drop secured target while SPA job is running.

Action: Wait for SPA job to complete and then try again.

46620: invalid interval *string* for data warehouse duration; must be positive

Cause: Invalid interval was specified for data warehouse duration.

Action: Specify valid interval, the interval should be positive.

46621: invalid start date *string* for data warehouse operation; must be less than *string*

Cause: Invalid start date was specified for data warehouse load/purge operation.

Action: Specify valid start date, the start date must be less than current date - warehouse duration.

46622: invalid number of days *string* for data warehouse operation; must be greater than 0

Cause: Invalid number of days was specified for data warehouse load/purge operation.

Action: Specify valid number of days, the number of days must be positive.

46623: cannot execute warehouse operation; another operation is currently running

Cause: A warehouse operation was executed while another operation is currently running.

Action: Wait for the operation to complete before reissuing the command.

46624: invalid schedule *string* for data warehouse refresh schedule

Cause: Invalid schedule was specified for data warehouse refresh.

Action: Specify valid non-null schedule.

46625: invalid repeat interval *string* for data warehouse refresh schedule

Cause: Invalid schedule was specified for data warehouse refresh.

Action: Specify valid non-null repeat interval.

46626: invalid number of years *string* for audit data retention; must be positive

Cause: Invalid number of years was specified for audit data retention.

Action: Specify valid number, the number should be positive.

46627: error in acquiring the global lock for secured 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 Secured Target *string*.
Cause: User tried to drop a secured target which an enforcement point is monitoring.

Action: Stop the enforcement point and try again.

46651: Retention Policy *string* is in use.
Cause: Operation failed because Retention Policy is in use.

Action: Delete the assignment of this Retention Policy to Secured Target(s) and try again.

46652: Cannot delete built-in Retention Policies.
Cause: Cannot delete built-in Retention Policies.

Action: 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 Secured Target of type "*string*".

Cause: User entered service name as part of secured target address for a secured target which does not support service name.

Action: Do not provide service name when providing secured target address.

46663: Secured Target Address is not supported for Secured Target of type "*string*".

Cause: User tried to add a secured target address for a secured target which cannot be monitored by the firewall.

Action: Users are not allowed to add secured target address for a secured 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 a 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 operation.

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 secured target and firewall.

Action: Two EPs with the same firewall and secured 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 DPE, bridged interfaces must be enabled.

Action: Enable the bridged interface on the Firewall and retry operation.

46984: Firewalls not in the same resilient pair.

Cause: Only a resilient pair can be swapped. You cannot swap Firewalls from different resilient pairs.

Action: Ensure that the Firewalls are part of the same resilient pair and retry operation.

46985: Unable to create resilient pair because Firewall *string* has Enforcement Points configured.

Cause: The Firewalls being paired for resilience must not have any Enforcement Points configured.

Action: Please delete all Enforcement Points and try again.

46986: Firewall at IP address *string* does not have a valid Audit Vault Server certificate.

Cause: Audit Vault Server certificate is not present on the Firewall, or is invalid.

Action: Please supply server certificate on the Firewall UI.

46987: Firewall Name is too long.

Cause: Firewall Name failed length validation checks.

Action: Provide a valid Firewall Name.

46988: Invalid IP address '*string*'. IP address must be a valid IPv4 address.

Cause: IP address does not conform to IPv4 standard.

Action: Please specify an IPv4 address and try again.

46990: More than one proxy interface specified.

Cause: In DPE mode, only one proxy interface must be specified.

Action: Specify one proxy most and retry the operation.

46991: Invalid monitoring mode (DAM) for proxy interface.

Cause: Monitoring mode must be DPE when proxy interface is specified.

Action: Specify DAM as monitoring mode.

46992: Enforcement Point mode cannot be DPE when the Firewall is in a resilient pair configuration.

Cause: Monitoring mode must be DAM when Firewall is in a resilient configuration.

Action: Specify DAM as monitoring mode.

46993: Full error message reporting can only be enabled if database response monitoring is enabled.

Cause: Database response monitoring not enabled.

Action: Please enable database response and try again.

46994: Enforcement Point Name is too long.

Cause: Enforcement Point Name failed length validation checks.

Action: Provide a valid Enforcement Point Name.

46995: Secured Target Address cannot be deleted.

Cause: There must be at least one address defined when there are active Enforcement Points.

Action: Add a new Secured Target Address and try again.

46996: Invalid IP addresses list. IP addresses list must be a space-separated list of valid IPv4 addresses. For example, '10.240.114.168 10.240.114.169'.

Cause: Invalid IP address list specified.

Action: The IP addresses must be valid IPv4 addresses and separated by spaces.

46997: Invalid Port '*string*'. Port must be a number between 1 and 65535.

Cause: Port Number is not between 1 and 65535.

Action: Specify a value between 1 and 65535 and try again.

46998: Invalid WAF session timeout '*string*'. WAF session timeout value is specified in minutes, and must be at least 30 and at most 1440.

Cause: WAF session timeout must be at least 30 minutes and no more than a day.

Action: Please specify a valid timeout value and try again.

46999: Database address, port number, database name and credentials must be specified in order to enable Database Interrogation.

Cause: User tried to enable database interrogation without specifying database address/port/database name/credentials.

Action: Specify database address/port/database name/credentials and then try again.

47000: Activation approval for agent on host *string* failed.

Cause: Activation request for agent on host was not found.

Action: Request activation for the agent.

47001: Agent deactivation for host *string* failed.

Cause: Agent Deactivation failed.

Action: Check if agent on the host is activated.

47002: Agent version *string* is invalid.

Cause: Agent version must be in 'YYYY-MM-DD HH24:MI:SS.FF3 TZHTZM' format

Action: Check the agent version.

47003: Agent on host *string* is incompatible with Audit Vault Server.

Cause: Agent version is not supported by the Audit Vault Server.

Action: Upgrade the agent to the latest version.

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 until the archive period expires.

47112: Cannot drop Archive Location. It is being used to store archived data.

Cause: Specified Archive Location is being used to store archive data.

Action: Wait until the archive period expires.

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 exists.

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 member 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 filesystem 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 request is not compatible with server.

Cause: Certificate signing 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 secured target "*string*"; audit trail does not exist.

Cause: User attempted to stop a trail which does not exist

Action: One cannot stop audit trail which does not exist

47504: Cannot stop trail of type "*string*" at "*string*" for secured target "*string*"; audit trail is already stopped. 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 specified 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 cannot 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 $\min((\text{total system memory} - 8\text{GB}), 90\% \text{ of total system memory})$.

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.

E.2 Database Firewall Messages

This table lists the Database Firewall messages. These messages are captured in the `/var/log/messages` file.

Code ODF	Cause	Action
10001	Internal error	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 Audit Vault Server	A connection has been successfully established to the Audit Vault Server. No action is required.

Code ODF	Cause	Action
10107	<i>TrafficTrace</i> starting	The <i>TrafficTrace</i> logging system has started. No action is required.
10108	<i>TrafficTrace</i> data	The <i>TrafficTrace</i> logging system is logging data. No action is required.
10109	<i>TrafficTrace</i> stopping	The <i>TrafficTrace</i> 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 Enforcement Point is in DPE mode, and the option to Maintain Existing Connections was not selected. No action is required.
10114	Stopped receiving heartbeat data	Information about the Enforcement Point. No action is required.
10200	Failed parsing Exclude Addresses	Check the configuration of the WAF Exclude Addresses.
10201	Failed parsing alert forwarding address	Check the configuration of the WAF Destination Host and Port for alert forwarding.
10202	Failed parsing Cookie Prefixes	Check the configuration of the WAF Cookie Prefixes.
10203	Failed parsing F5 message	Check that the F5 machine is configured as per the instructions in the <i>Oracle Audit Vault and Database Firewall Administrator's Guide</i> .
10204	Failed parsing F5 HTTP headers	Check that the F5 machine is configured as per the instructions in the <i>Oracle Audit Vault and Database Firewall Administrator's Guide</i> .
10205	F5 device connected	An F5 appliance has established a connection to the Database Firewall. No action required.
10206	F5 device disconnected	An F5 appliance has disconnected from the Database Firewall. Ensure that the F5 device is functioning correctly.
10207	WAF messages dropped	Messages from the WAF appliance have been dropped as the queue was full. Check the settings on your WAF appliance to ensure that the threshold for sending alerts is correct.
10208	The HTTP Content-Type value is unsupported	The Content-Type value found in the HTTP header is unsupported. Contact Oracle Support.
10209	F5 message size too large	The message from the F5 appliance is too large for the Database Firewall to process. Check that the F5 appliance is configured as per the instructions in the <i>Oracle Audit Vault and Database Firewall Administrator's Guide</i> .

Code ODF	Cause	Action
10210	F5 feed not established	No F5 <code>syslog</code> feed established. Ensure that the F5 appliance is functioning correctly and that the Database Firewall is configured correctly to receive data from that appliance.
10211	Failed connecting to F5 <code>syslog</code> destination	Check the configuration for WAF Alert Forwarding. Check that the specified host is running and prepared to accept connections.
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. Investigate the source of this unexpected connection attempt.
10400	No ASO records found	Check that database has been configured for ASO as per the instructions in the <i>Oracle Audit Vault and Database Firewall Administrator's Guide</i> .
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 delayed that the request was purged from the queue before the response was received. Verify that the secured target is configured for ASO and is functioning correctly.
10403	ASO is using unsupported encryption algorithm	ASO processing found the session is using unsupported encryption algorithm. If the enforcement point is configured with DPE mode, the session will be terminated. In DAM mode the message is decoded and SQL statements extracted if there are any.
10500	Unable to connect to Audit Vault Server	A connection could not be established to the Audit Vault Server. This message is seen in normal operation when the Database Firewall is first associated with the Audit Vault Server. If the message persists, or is seen under different circumstances then check the settings of the Database Firewall and the Audit Vault Server in the GUI.
10501	Failed connecting to Secured Target	Check the secured target configuration. Check the secured 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.

Code ODF	Cause	Action
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 Database Firewall.
10505	Failed to resolve host name	Check the DNS settings on your appliance, and that the host name is specified correctly.
10506	IP packet fragmented	An IP packet intercepted in DAM 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 Audit Vault Server	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 the router or Firewall settings.
10509	Failed to find MAC address	Failed to find database MAC address. MAC address substitution will not work. The possible causes are: <ul style="list-style-type: none"> Database server is down or unreachable through the specified traffic source Database server is connected to the client port in the bridge. Connect the Database and Firewall properly, and then reboot the Firewall.
10510	The TCP connection to the Audit Vault Server has been lost	Check the network path between the Database Firewall and the Audit Vault Server. Note: This problem may be seen when the Audit Vault Server is restarted.
10511	IPC communication disrupted	See other messages in log file for more information.
10512	A badly formed TCP URG packet was received	This problem has been seen in <code>Fuzz-Testing</code> of the Database Firewall where bad TCP packets are transmitted. Verify that the clients using the Database Firewall are behaving correctly.
10513	SSL handshake failed	An SSL client has failed to connect to the Database Firewall due a failure in the initial handshake. Examine the additional information in this message, and confirm that the client is correctly configured.

Code ODF	Cause	Action
10514	Peer has reset the connection	The remote peer of this TCP session has reset the connection. Ensure that the remote peer is behaving correctly. Note: 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. Examine other related error messages to determine the context of this failure.
10516	Failed opening socket	An attempt to open a socket has failed. Examine other related error messages to determine the context of this failure.
10600	Invalid Secured Target IP address	Ensure the secured target IP address has been correctly specified in the GUI.
10601	Secured target clash	Two secured 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 the new configuration as it cannot be applied to the system that is running	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. Contact Oracle Support.
10605	Cannot generate new configuration, retry the operation	The system management software failed to generate the new configuration. Workaround is provided.
10606	Internal error, invalid configuration	Contact Oracle Support.
10607	Value of system configuration <code>rmem_max</code> may be excessive	The value of the system setting <code>rmem_max</code> is unexpectedly high. On some hardware, it has been observed that this can lead to DAM mode traffic not being intercepted as expected. Verify that your system can support this value successfully.
10608	Invalid argument for certificate operation	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. Verify your signing process.
10611	Error processing certificate	The uploaded certificate was not valid. Check the uploaded certificate.

Code ODF	Cause	Action
10612	Proxy-mode Enforcement Points clash	More than one Enforcement Point is configured to use the same proxy port. Examine the Enforcement Points configured for the specific Database Firewall 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. 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 <code>TRACE_SQL</code> .
10615	Unable to parse the expiry time in configuration file	Edit the configuration file and enter the expiry time against key <code>EXPIRES_AT</code> in the format <code>yyyy-mm-dd hh:mm:ss</code> . For example: <code>2015-11-23 12:13:14</code> .
10616	Expiry time has already passed	Edit the configuration file and alter the <code>EXPIRES_AT</code> time as required.
10617	<i>TrafficTrace</i> period set for greater than the permitted value	Edit the configuration file and alter the <code>EXPIRES_AT</code> time as required.
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 Protocol configured	This is an informational message. No action required.
10700	Queue of messages destined for Audit Vault Server is full	Check the status of the Audit Vault Server associated with the specific Database Firewall. Also check the Audit Vault Server and Database Firewall are correctly paired.
10701	Network packets not intercepted	Some network packets were not captured because the system was overloaded (DAM mode).
10702	Capacity exceeded	The system is not able to capture all the requested DAM mode traffic.
10703	Capacity no longer exceeded	The system is now capturing all the requested DAM mode traffic again. No action required.
10704	Internal capacity exceeded	Internal system capacity has been exceeded for the protected database. 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.

Code ODF	Cause	Action
10706	syslog message too big	A message being processed for forwarding to the Audit Vault Server is too large to send. 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. Examine the log file for other errors to determine the cause of this failure.
10709	Failed to start monitoring processes	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 DAM mode traffic again. No action required.
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 this information is required in reports, the 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 an Enforcement Point. No action required, unless this error is seen repeatedly.
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.
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.

Code ODF	Cause	Action
11008	Confirm you wish to start upgrade	Read the following messages, and re-run this utility as follows to begin upgrade: <code>/usr/bin/avdf-upgrade --confirm</code>
11009	Check before continuing	Power loss during upgrade may cause data loss. Do not power off during upgrade.
11010	Check before continuing	This upgrade will erase <code>/root</code> and <code>/images</code> .
11011	Check before continuing	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. Wait until the upgrade completes or contact support.
11015	Last migration: failed	Fix the failure cause. Migration can be executed again.
11016	Last migration: failed	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 <code>--confirm</code> option.
11018	Attempt to resume upgrade without confirmation	Confirm that you have fixed the original error cause by running the tool again with <code>--confirm</code> 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	Download the diagnostics package and contact Oracle Support. Review <code>/var/log/messages</code> and <code>/var/log/debug</code> for more information. To download the diagnostics package, 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. Generate a new hash if you are using a new migration index.
11060	Migration file result: FATAL ERROR - ABORTED	Do not use this system in a production environment. Download the diagnostics package and contact Oracle Support. Review <code>/var/log/messages</code> and <code>/var/log/debug</code> for more information. To download the diagnostics package, follow the instructions from the documentation.

Code ODF	Cause	Action
11061	Migration group result: failed	Do not use this system in a production environment. Download the diagnostics package and contact Oracle Support. Review <code>/var/log/messages</code> and <code>/var/log/debug</code> for more information. To download the diagnostics package, follow the instructions from the documentation.
11062	Migration stanza result: failed to start because its preconditions were not met	Do not use this system in a production environment. Download the diagnostics package and contact Oracle Support. Review <code>/var/log/messages</code> and <code>/var/log/debug</code> for more information. To download the diagnostics package, follow the instructions from the documentation.
11063	Migration file result: incomplete	Download the diagnostics package and contact Oracle Support. Review <code>/var/log/messages</code> and <code>/var/log/debug</code> for more information. To download the diagnostics package, follow the instructions from the documentation.
11064	The install or upgrade is incomplete	Download the diagnostics package and contact Oracle Support. Review <code>/var/log/messages</code> and <code>/var/log/debug</code> for more information. To download the diagnostics package, follow the instructions from the documentation.

F

Security Technical Implementation Guides

Oracle Audit Vault and Database Firewall follows the Security Technical Implementation Guides (STIG)-based compliance standards.

Topics:

- [About Security Technical Implementation Guides](#) (page F-1)
- [Enabling and Disabling STIG Rules on Oracle Audit Vault and Database Firewall](#) (page F-3)
- [Current Implementation of STIG Rules on Oracle Audit Vault and Database Firewall](#) (page F-3)



See Also:

["Security Technical Implementation Guides and Implementation for User Accounts](#) (page 13-2)"

F.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 rules 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](#)

F.2 Enabling and Disabling STIG Rules on Oracle Audit Vault and Database Firewall

You can enable STIG rules on Oracle Audit Vault and Database Firewall by enabling Strict mode.

F.2.1 Enabling STIG Rules on Oracle Audit Vault and Database Firewall

Learn how to enable STIG rules 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
```

F.2.2 Disabling STIG Rules on Oracle Audit Vault and Database Firewall

Learn how to disable STIG Rules 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
```

F.3 Current Implementation of STIG Rules on Oracle Audit Vault and Database Firewall

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 F-1](#) (page F-3) lists the three vulnerability categories that STIG recommendations.

Table F-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.

F.4 Current Implementation of Database STIG Rules

Learn about the current implementation of database STIG rules on Oracle Audit Vault and Database Firewall.

[Table F-2](#) (page F-4) shows the current implementation of Database STIG rules on Oracle Audit Vault and Database Firewall.

Table F-2 Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Addressed by Script	Addressed by Document	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.
DG0008-ORACLE11	DBMS application object ownership	No	No	Yes	No	No	For more information, see DG0008-ORACLE11 STIG Rule (page F-12).
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.

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action required	Implemented	Notes
DG0075-ORACLE11	DBMS links to external databases	CAT II	No	Yes	No	No	For more information, see DG0075-ORACLE11 , DO0250-ORACLE11 STIG Rules (page F-12).
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 <code>DBFS_ROLE</code> from <code>AV_ADMIN</code> . For more information, see DG0116-ORACLE11 STIG Rule (page F-13).
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
DG0125-ORACLE11	DBMS account password expiration	CAT II	Yes	No	No	No	<code>MONITORING_PROFILE</code> no longer exists in Oracle Audit Vault and Database Firewall 12.2. For other profiles, <code>PASSWORD_LIFE_TIME</code> is set to the required limit in the script.
DG0126-ORACLE11	DBMS account password reuse	CAT II	No	No	None	No	Password reuse is not allowed on Oracle Audit Vault and Database Firewall.

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Address ed by Script	Ad dre sse d by Doc um ent atio n	Acti on req uire d	Imp lem ent ed	Notes
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	Non e	No	No
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 , DO0250-ORACLE11 STIG Rules (page F-12).
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

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Address ed by Script	Ad dre sse d by Doc um ent atio n	Acti on req uire d	Imp lem ent ed	Notes
DO3540-ORACLE11	Oracle <code>SQL92_SECURITY</code> parameter	CAT II	No	No	No	No	Parameter <code>SQL92_SECURITY</code> is already set to <code>TRUE</code> .
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 <code>RESOURCE_LIMIT</code> parameter	CAT II	No	No	No	No	Currently not supported
O121-BP-021900	The Oracle <code>REMOTE_OS_AUTHENT</code> parameter must be set to <code>FALSE</code> .	CAT I	No	No	No	Yes	None
O121-BP-022000	The Oracle <code>REMOTE_OS_ROLES</code> parameter must be set to <code>FALSE</code> .	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
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 <code>SYSDBA</code> . 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	<code>DVSY</code> is assigned custom password in product. Other users are assigned passwords through the STIG script.

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Addressed by Script	Addressed by Documentation	Action Required	Implemented	Notes
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 <i>sqlnet.ora</i> : <i>SQLNET.ENCRYPTION_TYPES_SERVER = (AES256,AES192,AES128)</i> . 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.
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	Can not complete	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

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Address ed by Script	Ad dre sse d by Doc um ent atio n	Acti on req uire d	Imp lem ent ed	Notes
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 Not e.	No	No	See note (page F-12)
O121- BP-022100	The Oracle <i>SQL92_SECURITY</i> parameter must be set to <i>TRUE</i> .	CAT II	No	No	No	Yes	None
O121- BP-022200	The Oracle <i>REMOTE_LOGIN_PASSWORDFILE</i> parameter must be set to <i>EXCLUSIVE</i> or <i>NONE</i> .	CAT II	No	No	No	Yes	None
O121- BP-022300	System privileges granted using the <i>WITH ADMIN OPTION</i> must not be granted to unauthorized user.	CAT II	No	No	No	Yes	None
O121- BP-022400	System privileges must not be granted to <i>PUBLIC</i> role.	CAT II	No	No	No	Yes	None
O121- BP-022500	Oracle roles granted using the <i>WITH ADMIN OPTION</i> must not be granted to unauthorized accounts.	CAT II	No	No	No	Yes	None
O121- BP-022600	Object permissions granted to <i>PUBLIC</i> role must be restricted.	CAT II	No	No	No	Yes	None
O121- BP-022800	Application role permissions must not be assigned to the Oracle <i>PUBLIC</i> role.	CAT II	No	No	No	Yes	None
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 Not e.	No	No	See note (page F-12)
O121- BP-023600	Only authorized system accounts must have the <i>SYSTEM</i> table space specified as the default table space.	CAT II	No	No	No	Yes	None

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Addressed by Script	Addressed by Document	Action required	Implemented	Notes
O121-BP-023900	The Oracle <code>_TRACE_FILES_PUBLIC</code> parameter if present must be set to <code>FALSE</code> .	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 (page F-12)
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 <code>sqlnet.ora</code> on the Audit Vault Server is set to <code>SQLNET.ALLOWED_LOGON_VERSION_SERVER = 11</code>
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
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

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Addressed by Script	Addressed by Document	Action Required	Implemented	Notes
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
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.

Table F-2 (Cont.) Current Implementation of Database STIG Rules

STIG ID	Title	Severity	Address ed by Script	Ad dre sse d by Doc um ent atio n	Acti on req uire d	Imp lem ent ed	Notes
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.

F.5 Additional Notes

Additional notes regarding STIG IDs are in [Table F-2](#) (page F-4).

F.5.1 DG0008-ORACLE11 STIG Rule

Object owner accounts in Audit Vault Server:

- AVSYS
- APEX_040100
- MANAGEMENT
- AVRULEOWNER
- SECURELOG
- AVREPORTUSER

Object owner accounts in Database Firewall:

- APEX_040100
- MANAGEMENT
- SECURELOG

F.5.2 DG0075-ORACLE11, DO0250-ORACLE11 STIG Rules

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 the Oracle Audit Vault Server and is used by the REDO collector.

F.5.3 DG0116-ORACLE11 STIG Rule

[Table F-3](#) (page F-13) lists accounts and role assignments in Audit Vault Server.

Table F-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 F-4](#) (page F-13) lists accounts and role assignments in Database Firewall.

Table F-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

F.6 Current Implementation of Operating System STIG Rules

Learn about the current implementation of operating system STIG rules.

This topic contains information on the current implementation of Operating System STIG Rules on Oracle Audit Vault and Database Firewall.

 **Note:**

The Operating System STIG Rule set reference is as follows:

Table F-5 Operating System STIG Rule Set Reference

Reference	Detail
Document	Oracle Linux 6 Security Technical Implementation Guide
Version	1
Release	6
Release Date	22/April/ 2016
Document Link	Oracle Linux 6 Security Technical Implementation Guide

Table F-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 <i>strict</i> mode	The guideline can be implemented by switching the appliance to <i>strict</i> mode.
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 administrator configuration action after installation or upgrade. It can also be a regularly used and defined administrative procedure.

 **See Also:**

[Enabling and Disabling STIG Rules on Oracle Audit Vault and Database Firewall](#) (page F-3)

[Table F-7](#) (page F-14) shows the current implementation of Operating System STIG Rules on Oracle Audit Vault and Database Firewall.

Table F-7 Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000008	CAT I	None	Vendor provided cryptographic certificates must be installed to verify the integrity of system software.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000019	CAT I	None	There must be no <code>.rhosts</code> or <code>hosts.equiv</code> files on the system.	Implemented by default
OL6-00-000030	CAT I	None	The system must not have accounts configured with blank or null passwords.	Implemented by default
OL6-00-000206	CAT I	None	The <code>telnet-server</code> package must not be installed.	Implemented by default
OL6-00-000211	CAT I	None	The telnet daemon must not be running.	Implemented by default
OL6-00-000213	CAT I	None	The <code>rsh-server</code> package must not be installed.	Implemented by default
OL6-00-000214	CAT I	None	The <code>rshd</code> service must not be running.	Implemented by default
OL6-00-000216	CAT I	None	The <code>rexecd</code> service must not be running.	Implemented by default
OL6-00-000218	CAT I	None	The <code>rlogind</code> service must not be running.	Implemented by default
OL6-00-000227	CAT I	None	The SSH daemon must be configured to use only the SSHv2 protocol.	Implemented by default
OL6-00-000239	CAT I	None	The SSH daemon must not allow authentication using an empty password.	Implemented by default
OL6-00-000284	CAT I	Administrative task	The system must use and update a DoD approved virus scan program.	Audit Vault and Database Firewall does not ship with an anti-virus. The administrator may install one.
OL6-00-000286	CAT I	None	The x86 <code>Ctrl-Alt-Delete</code> key sequence must be disabled.	Implemented by default
OL6-00-000309	CAT I	None	The NFS server must not have the insecure file locking option enabled.	Implemented by default
OL6-00-000338	CAT I	None	The TFTP daemon must operate in secure mode which provides access only to a single directory on the host file system.	Implemented by default
OL6-00-000341	CAT I	Administrative task	The <code>snmpd</code> service must not use a default password.	Audit Vault and Database Firewall randomizes the SNMP community string at install time. Use the WUI to set a specific value.
OL6-00-000005	CAT II	Administrative task	The audit system must alert designated staff members when the audit storage volume approaches capacity.	Configure remote <code>syslog</code> forwarding. Detailed note on Alerts through syslog (page F-29).

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000011	CAT II	Administrative task	System security patches and updates must be installed and up to date.	Apply bundle patches in a timely manner.
OL6-00-000013	CAT II	None	The system package management tool must cryptographically verify the authenticity of system software packages during installation.	Implemented by default
OL6-00-000016	CAT II	None	A file integrity tool must be installed.	Implemented by default
OL6-00-000017	CAT II	None	The system must use a Linux Security Module at boot time.	Implemented by default
OL6-00-000027	CAT II	None	The system must prevent the <i>root</i> account from logging in from virtual consoles.	Implemented by default
OL6-00-000031	CAT II	None	The <i>/etc/passwd</i> file must not contain password hashes.	Implemented by default
OL6-00-000032	CAT II	None	The <i>root</i> account must be the only account having a UID of 0.	Implemented by default
OL6-00-000033	CAT II	None	The <i>/etc/shadow</i> file must be owned by <i>root</i> .	Implemented by default
OL6-00-000034	CAT II	None	The <i>/etc/shadow</i> file must be group-owned by <i>root</i> .	Implemented by default
OL6-00-000035	CAT II	None	The <i>/etc/shadow</i> file must have mode 0000.	Implemented by default
OL6-00-000036	CAT II	None	The <i>/etc/gshadow</i> file must be owned by <i>root</i> .	Implemented by default
OL6-00-000037	CAT II	None	The <i>/etc/gshadow</i> file must be group-owned by <i>root</i> .	Implemented by default
OL6-00-000038	CAT II	None	The <i>/etc/gshadow</i> file must have mode 0000.	Implemented by default
OL6-00-000039	CAT II	None	The <i>/etc/passwd</i> file must be owned by <i>root</i> .	Implemented by default
OL6-00-000040	CAT II	None	The <i>/etc/passwd</i> file must be group-owned by <i>root</i> .	Implemented by default
OL6-00-000041	CAT II	None	The <i>/etc/passwd</i> file must have mode 0644 or less permissive.	Implemented by default
OL6-00-000042	CAT II	None	The <i>/etc/group</i> file must be owned by <i>root</i> .	Implemented by default
OL6-00-000043	CAT II	None	The <i>/etc/group</i> file must be group-owned by <i>root</i> .	Implemented by default
OL6-00-000044	CAT II	None	The <i>/etc/group</i> file must have mode 0644 or less permissive.	Implemented by default
OL6-00-000046	CAT II	None	Library files must be owned by a system account.	Implemented by default
OL6-00-000047	CAT II	None	All system command files must have mode 755 or less permissive.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000048	CAT II	None	All system command files must be owned by <i>root</i> .	Implemented by default
OL6-00-000050	CAT II	Enable strict mode	The system must require passwords to contain a minimum of 15 characters.	Implemented in strict mode
OL6-00-000051	CAT II	None	Users must not be able to change passwords more than once every 24 hours.	Implemented by default
OL6-00-000053	CAT II	Enable strict mode	User passwords must be changed at least every 60 days.	Implemented in strict mode
OL6-00-000061	CAT II	None	The system must disable accounts after three consecutive unsuccessful login attempts.	Implemented by default
OL6-00-000062	CAT II	None	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (system-auth).	Implemented by default
OL6-00-000063	CAT II	None	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (login.defs).	Implemented by default
OL6-00-000064	CAT II	None	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (libuser.conf).	Implemented by default
OL6-00-000065	CAT II	None	The system boot loader configuration files must be owned by <i>root</i> .	Implemented by default
OL6-00-000066	CAT II	None	The system boot loader configuration files must be group-owned by <i>root</i> .	Implemented by default
OL6-00-000067	CAT II	None	The system boot loader configuration files must have mode 0600 or less permissive.	Implemented by default
OL6-00-000069	CAT II	Administrative task	The system must require authentication upon booting into single-user and maintenance modes.	Detailed note on OL6-00-000069 (page F-30).
OL6-00-000070	CAT II	None	The system must not permit interactive boot.	Implemented by default
OL6-00-000078	CAT II	None	The system must implement virtual address space randomization.	Implemented by default
OL6-00-000079	CAT II	None	The system must limit the ability of processes to have simultaneous write and execute access to memory.	Implemented by default
OL6-00-000080	CAT II	None	The system must not send ICMPv4 redirects by default.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000081	CAT II	None	The system must not send ICMPv4 redirects from any interface.	Implemented by default
OL6-00-000082	CAT II	None	IP forwarding for IPv4 must not be enabled, unless the system is a router.	Implemented by default
OL6-00-000083	CAT II	None	The system must not accept IPv4 source-routed packets on any interface.	Implemented by default
OL6-00-000084	CAT II	None	The system must not accept ICMPv4 redirect packets on any interface.	Implemented by default
OL6-00-000086	CAT II	None	The system must not accept ICMPv4 secure redirect packets on any interface.	Implemented by default
OL6-00-000089	CAT II	None	The system must not accept IPv4 source-routed packets by default.	Implemented by default
OL6-00-000090	CAT II	None	The system must not accept ICMPv4 secure redirect packets by default.	Implemented by default
OL6-00-000095	CAT II	None	The system must be configured to use TCP syncookies when experiencing a TCP SYN flood.	Implemented by default
OL6-00-000096	CAT II	None	The system must use a reverse-path filter for IPv4 network traffic when possible on all interfaces.	Implemented by default
OL6-00-000097	CAT II	None	The system must use a reverse-path filter for IPv4 network traffic when possible by default.	Implemented by default
OL6-00-000098	CAT II	None	The IPv6 protocol handler must not be bound to the network stack unless needed.	Implemented by default
OL6-00-000099	CAT II	None	The system must ignore ICMPv6 redirects by default.	Implemented by default
OL6-00-000103	CAT II	None	The system must employ a local IPv6 firewall.	Not applicable
OL6-00-000106	CAT II	None	The operating system must connect to external networks or information systems only through managed IPv6 interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Not applicable
OL6-00-000107	CAT II	None	The operating system must prevent public IPv6 access into the organizations internal networks, except as appropriately mediated by managed interfaces employing boundary protection devices.	Not applicable
OL6-00-000113	CAT II	None	The system must employ a local IPv4 firewall.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000116	CAT II	Site policy	The operating system must connect to external networks or information systems only through managed IPv4 interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	This is outside of the scope of Audit Vault and Database Firewall and must be enforced externally.
OL6-00-000117	CAT II	None	The operating system must prevent public IPv4 access to internal networks of an organization. This excludes appropriately mediated and managed interfaces employing boundary protection devices.	Implemented by default
OL6-00-000120	CAT II	None	The local IPv4 firewall of the system must implement a <i>deny-all</i> and <i>allow-by-exception</i> policy for inbound packets.	Implemented by default
OL6-00-000124	CAT II	None	The Datagram Congestion Control Protocol (DCCP) must be disabled unless required.	Implemented by default
OL6-00-000125	CAT II	None	The Stream Control Transmission Protocol (SCTP) must be disabled unless required.	Implemented by default
OL6-00-000127	CAT II	None	The Transparent Inter-Process Communication (TIPC) protocol must be disabled unless required.	Implemented by default
OL6-00-000133	CAT II	None	All <code>rsyslog-generated</code> log files must be owned by <code>root</code> .	Implemented by default
OL6-00-000145	CAT II	None	The operating system must produce audit records containing sufficient information to establish the identity of any user/subject associated with the event.	Implemented by default
OL6-00-000148	CAT II	None	The operating system must employ automated mechanisms to facilitate the monitoring and control of remote access methods.	Implemented by default
OL6-00-000154	CAT II	None	The operating system must produce audit records containing sufficient information to establish what type of events occurred.	Implemented by default
OL6-00-000159	CAT II	None	The system must retain enough rotated audit logs to cover the required log retention period.	Implemented by default
OL6-00-000160	CAT II	None	The system must set a maximum audit log file size.	Implemented by default
OL6-00-000161	CAT II	None	The system must rotate audit log files that reach the maximum file size.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000163	CAT II	None	The audit system must switch the system to single-user mode when available audit storage volume becomes dangerously low.	Implemented by default
OL6-00-000202	CAT II	None	The audit system must be configured to audit the loading and unloading of dynamic kernel modules.	Implemented by default
OL6-00-000203	CAT II	None	The <code>xinetd</code> service must be disabled if no network services utilizing it are enabled.	Implemented by default
OL6-00-000220	CAT II	None	The <code>ypserv</code> package must not be installed.	Implemented by default
OL6-00-000221	CAT II	None	The <code>ypbind</code> service must not be running.	Implemented by default
OL6-00-000222	CAT II	None	The <code>tftp-server</code> package must not be installed unless required.	Implemented by default
OL6-00-000223	CAT II	None	The <code>TFTP</code> service must not be running.	Implemented by default
OL6-00-000224	CAT II	None	The <code>cron</code> service must be running.	Implemented by default
OL6-00-000234	CAT II	None	The SSH daemon must ignore <code>.rhosts</code> files.	Implemented by default
OL6-00-000236	CAT II	None	The SSH daemon must not allow host-based authentication.	Implemented by default
OL6-00-000237	CAT II	None	The system must not permit <code>root</code> login using remote access programs such as <code>ssh</code> .	Implemented by default
OL6-00-000243	CAT II	None	The SSH daemon must be configured to use only FIPS 140-2 approved ciphers.	Implemented by default
OL6-00-000247	CAT II	Administrative task	The system clock must be synchronized continuously, or at least daily.	Use the WUI to configure NTP servers.
OL6-00-000248	CAT II	None	The system clock must be synchronized to an authoritative DoD time source.	Implemented by default
OL6-00-000249	CAT II	None	Mail relaying must be restricted.	Implemented by default. Audit Vault and Database Firewall does not contain an SMTA.
OL6-00-000252	CAT II	None	If the system is using LDAP for authentication or account information, the system must use a TLS connection using FIPS 140-2 approved cryptographic algorithms.	Audit Vault and Database Firewall does not use LDAP for authentication or account information.

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000253	CAT II	None	The LDAP client must use a TLS connection using trust certificates signed by the site CA.	Audit Vault and Database Firewall does not use LDAP client.
OL6-00-000257	CAT II	None	The graphical desktop environment must set the idle time out value not exceeding 15 minutes.	Implemented by default
OL6-00-000258	CAT II	None	The graphical desktop environment must automatically lock after 15 minutes of inactivity and the system must require user re-authentication to unlock the environment.	Implemented by default
OL6-00-000259	CAT II	None	The graphical desktop environment must have automatic lock enabled.	Implemented by default
OL6-00-000269	CAT II	None	Remote file systems must be mounted with the <code>nodev</code> option.	Implemented by default
OL6-00-000270	CAT II	None	Remote file systems must be mounted with the <code>nosuid</code> option.	Implemented by default
OL6-00-000274	CAT II	None	The system must prohibit the reuse of passwords within five iterations.	Implemented by default
OL6-00-000278	CAT II	None	The system package management tool must verify permissions on all files and directories associated with the audit package.	Implemented by default
OL6-00-000279	CAT II	None	The system package management tool must verify ownership on all files and directories associated with the audit package.	Implemented by default
OL6-00-000280	CAT II	None	The system package management tool must verify group-ownership on all files and directories associated with the audit package.	Implemented by default
OL6-00-000281	CAT II	None	The system package management tool must verify contents of all files associated with the audit package.	Implemented by default
OL6-00-000282	CAT II	None	There must be no world-writable files on the system.	Implemented by default
OL6-00-000285	CAT II	None	The system must have a host-based intrusion detection tool installed.	Implemented by default
OL6-00-000288	CAT II	None	The <code>sendmail</code> package must be removed.	Implemented by default
OL6-00-000290	CAT II	None	X Windows must not be enabled unless required.	Implemented by default
OL6-00-000311	CAT II	Administrative task	The audit system must provide a warning when allocated audit record storage volume reaches a documented percentage of maximum audit record storage capacity.	Configure remote <code>syslog</code> forwarding. Detailed note on Alerts through syslog (page F-29) .

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000313	CAT II	None	The audit system must identify staff members to receive notifications of audit log storage volume capacity issues.	Implemented by default
OL6-00-000315	CAT II	None	The Bluetooth kernel module must be disabled.	Implemented by default
OL6-00-000320	CAT II	None	The systems local firewall must implement a deny-all, allow-by-exception policy for forwarded packets.	Implemented by default
OL6-00-000324	CAT II	None	A login banner must be displayed immediately prior to, or as part of, graphical desktop environment login prompts.	Implemented by default
OL6-00-000326	CAT II	None	The Department of Defense (DoD) login banner must be displayed immediately prior to, or as part of, graphical desktop environment login prompts.	Audit Vault and Database Firewall does not contain a graphical desktop environment.
OL6-00-000331	CAT II	None	The Bluetooth service must be disabled.	Implemented by default
OL6-00-000347	CAT II	None	There must be no .netrc files on the system.	Implemented by default
OL6-00-000348	CAT II	None	The FTPS/FTP service on the system must be configured with the Department of Defense (DoD) login banner.	Audit Vault and Database Firewall does not serve FTP or FTPS.
OL6-00-000356	CAT II	Enable strict mode	The system must require administrator action to unlock an account locked by excessive failed login attempts.	Implemented in strict mode
OL6-00-000357	CAT II	None	The system must disable accounts after excessive login failures within a 15 minute interval.	Implemented by default
OL6-00-000372	CAT II	None	The operating system, upon successful login or access, must display to the user the number of unsuccessful login or access attempts since the last successful login or access.	Implemented by default
OL6-00-000383	CAT II	None	Audit log files must have mode 0640 or less permissive.	Implemented by default
OL6-00-000384	CAT II	None	Audit log files must be owned by root.	Implemented by default
OL6-00-000385	CAT II	None	Audit log directories must have mode 0755 or less permissive.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000503	CAT II	None	The operating system must enforce requirements for the connection of mobile devices to operating systems.	Implemented by default
OL6-00-000504	CAT II	Site policy	The operating system must conduct backups of user-level information contained in the operating system per organization defined frequency to conduct backups consistent with recovery time and recovery point objectives.	Detailed note on Backup (page F-29).
OL6-00-000505	CAT II	Site policy	The operating system must conduct backups of system-level information contained in the information system per organization defined frequency to conduct backups that are consistent with recovery time and recovery point objectives.	Detailed note on Backup (page F-29).
OL6-00-000507	CAT II	None	The operating system, upon successful logon, must display to the user the date and time of the last logon or access through <i>ssh</i> .	Implemented by default
OL6-00-000522	CAT II	None	Audit log files must be group-owned by <i>root</i> .	Implemented by default
OL6-00-000523	CAT II	None	The systems local IPv6 firewall must implement a <i>deny-all, allow-by-exception</i> policy for inbound packets.	Not applicable
OL6-00-000524	CAT II	Site policy	The system must provide automated support for account management functions.	None
OL6-00-000527	CAT II	None	The login user list must be disabled.	Audit Vault and Database Firewall does not include a graphical login.
OL6-00-000529	CAT II	None	The sudo command must require authentication.	Implemented by default. Accounts which are permitted to use sudo are not permitted to login.
OL6-00-000001	CAT III	None	The system must use a separate file system for <i>/tmp</i> .	Implemented by default
OL6-00-000002	CAT III	None	The system must use a separate file system for <i>/var</i> .	Audit Vault and Database Firewall uses separate file systems for directories under <i>/var</i> .
OL6-00-000003	CAT III	None	The system must use a separate file system for <i>/var/log</i> .	Implemented by default
OL6-00-000007	CAT III	None	The system must use a separate file system for user home directories.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000009	CAT III	None	The Red Hat Network Service (<code>rhnsd</code>) service must not be running, unless it is being used to query the Oracle Unbreakable Linux Network for updates and information.	Implemented by default
OL6-00-000015	CAT III	None	The system package management tool must cryptographically verify the authenticity of all software packages during installation.	Implemented by default
OL6-00-000023	CAT III	None	The system must use a Linux Security Module configured to limit the privileges of system services.	Implemented by default
OL6-00-000028	CAT III	None	The system must prevent the <code>root</code> account from logging in from serial consoles.	Implemented by default
OL6-00-000054	CAT III	None	Users must be warned 7 days in advance of password expiration.	Implemented by default
OL6-00-000056	CAT III	None	The system must require passwords to contain at least one numeric character.	Implemented by default
OL6-00-000057	CAT III	None	The system must require passwords to contain at least one uppercase alphabetic character.	Implemented by default
OL6-00-000058	CAT III	None	The system must require passwords to contain at least one special character.	Implemented by default
OL6-00-000059	CAT III	None	The system must require passwords to contain at least one lower-case alphabetic character.	Implemented by default
OL6-00-000060	CAT III	Administrative task	The system must require at least eight characters be changed between the old and new passwords during a password change.	Detailed note on OL6-00-000060 (page F-30).
OL6-00-000091	CAT III	None	The system must ignore ICMPv4 redirect messages by default.	Implemented by default
OL6-00-000092	CAT III	None	The system must not respond to ICMPv4 sent to a broadcast address.	Implemented by default
OL6-00-000093	CAT III	None	The system must ignore ICMPv4 bogus error responses.	Implemented by default
OL6-00-000126	CAT III	None	The Reliable Datagram Sockets (RDS) protocol must be disabled unless required.	Implemented by default
OL6-00-000138	CAT III	None	System logs must be rotated daily.	Implemented by default
OL6-00-000165	CAT III	None	The audit system must be configured to audit all attempts to alter system time through <code>adjtimex</code> .	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000167	CAT III	None	The audit system must be configured to audit all attempts to alter system time through <code>settimeofday</code> .	Implemented by default
OL6-00-000169	CAT III	None	The audit system must be configured to audit all attempts to alter system time through <code>stime</code> .	Implemented by default
OL6-00-000171	CAT III	None	The audit system must be configured to audit all attempts to alter system time through <code>clock_settime</code> .	Implemented by default
OL6-00-000173	CAT III	None	The audit system must be configured to audit all attempts to alter system time through <code>/etc/localtime</code> .	Implemented by default
OL6-00-000174	CAT III	None	The operating system must automatically audit account creation.	Implemented by default
OL6-00-000175	CAT III	None	The operating system must automatically audit account modification.	Implemented by default
OL6-00-000176	CAT III	None	The operating system must automatically audit account disabling actions.	Implemented by default
OL6-00-000177	CAT III	None	The operating system must automatically audit account termination.	Implemented by default
OL6-00-000183	CAT III	None	The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).	Implemented by default
OL6-00-000184	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>chmod</code> .	Implemented by default
OL6-00-000185	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>chown</code> .	Implemented by default
OL6-00-000186	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>fchmod</code> .	Implemented by default
OL6-00-000187	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>fchmodat</code> .	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000188	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>fchown</code> .	Implemented by default
OL6-00-000189	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>fchownat</code> .	Implemented by default
OL6-00-000190	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>removexattr</code> .	Implemented by default
OL6-00-000191	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>setxattr</code> .	Implemented by default
OL6-00-000192	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>lchown</code> .	Implemented by default
OL6-00-000193	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>lremovexattr</code> .	Implemented by default
OL6-00-000194	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>lsetxattr</code> .	Implemented by default
OL6-00-000195	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>removexattr</code> .	Implemented by default
OL6-00-000196	CAT III	None	The audit system must be configured to audit all discretionary access control permission modifications using <code>setxattr</code> .	Implemented by default
OL6-00-000197	CAT III	None	The audit system must be configured to audit failed attempts to access files and programs.	Implemented by default
OL6-00-000199	CAT III	None	The audit system must be configured to audit successful file system mounts.	Implemented by default
OL6-00-000200	CAT III	None	The audit system must be configured to audit user deletions of files and programs.	Implemented by default
OL6-00-000201	CAT III	None	The audit system must be configured to audit changes to the <code>/etc/sudoers</code> file.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000204	CAT III	None	The <code>xinetd</code> service must be uninstalled if no network services utilizing it are enabled.	Implemented by default
OL6-00-000230	CAT III	None	The SSH daemon must set a time out interval on idle sessions.	Implemented by default
OL6-00-000231	CAT III	None	The SSH daemon must set a time out count on idle sessions.	Implemented by default
OL6-00-000241	CAT III	None	The SSH daemon must not permit user environment settings.	Implemented by default
OL6-00-000246	CAT III	None	The <code>avahi</code> service must be disabled.	Implemented by default
OL6-00-000256	CAT III	None	The <code>openldap-servers</code> package must not be installed unless required.	Implemented by default
OL6-00-000260	CAT III	None	The system must display a publicly viewable pattern during a graphical desktop environment session lock.	Implemented by default
OL6-00-000261	CAT III	None	The Automatic Bug Reporting Tool (<code>abrtd</code>) service must not be running.	Implemented by default
OL6-00-000262	CAT III	None	The <code>atd</code> service must be disabled.	Implemented by default
OL6-00-000265	CAT III	None	The <code>ntupdate</code> service must not be running.	Implemented by default
OL6-00-000266	CAT III	None	The <code>oddjobd</code> service must not be running.	Implemented by default
OL6-00-000267	CAT III	None	The <code>qpidd</code> service must not be running.	Implemented by default
OL6-00-000268	CAT III	None	The <code>rdisc</code> service must not be running.	Implemented by default
OL6-00-000271	CAT III	None	The <code>noexec</code> option must be added to removable media partitions.	The Audit Vault and Database Firewall <code>fstab</code> has no entries for removable media partitions.
OL6-00-000273	CAT III	None	The system must use SMB client signing, for connecting to samba servers using <code>mount.cifs</code> .	Audit Vault and Database Firewall does not use <code>mount.cifs</code> .
OL6-00-000289	CAT III	None	The <code>netconsole</code> service must be disabled unless required.	Implemented by default
OL6-00-000291	CAT III	None	The <code>xorg-x11-server-common</code> (X Windows) package must not be installed, unless required.	Implemented by default
OL6-00-000294	CAT III	None	All GIDs referenced in <code>/etc/passwd</code> must be defined in <code>/etc/group</code> .	Implemented by default
OL6-00-000296	CAT III	None	All accounts on the system must have unique user or account names.	Implemented by default

Table F-7 (Cont.) Current Implementation of Operating System STIG Rules

STIG ID	Severity	User action	Title	Notes
OL6-00-000297	CAT III	None	Temporary accounts must be provisioned with an expiration date.	Audit Vault and Database Firewall does not support temporary accounts.
OL6-00-000298	CAT III	None	Emergency accounts must be provisioned with an expiration date.	Audit Vault and Database Firewall does not support emergency accounts.
OL6-00-000299	CAT III	None	The system must require passwords to contain no more than three consecutive repeating characters.	Implemented by default
OL6-00-000308	CAT III	Administrative task	Process core dumps must be disabled unless needed.	Detailed note on OL6-00-000308 (page F-29).
OL6-00-000319	CAT III	Administrative task	The system must limit users to 10 simultaneous system logins, or a site-defined number, in accordance with operational requirements.	Detailed note on OL6-00-000319 (page F-29).
OL6-00-000336	CAT III	None	The sticky bit must be set on all public directories.	Implemented by default
OL6-00-000337	CAT III	None	All public directories must be owned by a system account.	Implemented by default
OL6-00-000339	CAT III	None	The FTP daemon must be configured for logging or verbose mode.	Audit Vault and Database Firewall does not include an FTP daemon.
OL6-00-000345	CAT III	None	The system default <code>umask</code> in <code>/etc/login.defs</code> must be <code>077</code> .	Implemented by default
OL6-00-000346	CAT III	None	The system default <code>umask</code> for daemons must be <code>027</code> or <code>022</code> .	Implemented by default
OL6-00-000508	CAT III	None	The system must allow locking of graphical desktop sessions.	Audit Vault and Database Firewall does not include a graphical desktop.
OL6-00-000515	CAT III	None	The NFS server must not have the <code>all_squash</code> option enabled.	Audit Vault and Database Firewall does not serve NFS.
OL6-00-000525	CAT III	None	Auditing must be enabled at boot by setting a kernel parameter.	Implemented by default
OL6-00-000526	CAT III	None	Automated file system mounting tools must not be enabled unless needed.	Implemented by default

 **Note 1 - Alerts through syslog:**

Oracle Audit Vault and Database Firewall sends alerts through *syslog*. Use the **WUI** to configure an appropriate *syslog* destination.

The *syslog* option is acceptable when it can be demonstrated that the local log management infrastructure notifies an appropriate administrator in a timely manner.

The messages are in the following form:

```
Audit daemon has no space left on logging partition
Audit daemon is suspending logging due to no space left on logging
partition.
```

 **Note 2 - Backup:**

This is outside of the scope of Oracle Audit Vault and Database Firewall.

Oracle Audit Vault and Database Firewall provides the tools to support this. (For example: *ssh*, *tar*).

 **Note 3 OL6-00-000319 - administrator actions:**

1. Log in as root user.
2. Create the following file:
`/etc/security/limits.d/99-avdf-maxlogins.conf`
3. Include the following content in the file:

```
# Bug 24398453
* hard maxlogins 10
```

 **Note 4 OL6-00-000308 - administrator actions:**

1. Log in as root user.
2. Create the following file:
`/etc/security/limits.d/99-avdf-core.conf`
3. Include the following content in the file:

```
# Bug 24397420
* hard core 0
```

 **Note 5 OL6-00-000060 - administrator actions:**

1. Log in as root user.
2. Take backup of the following file:
`/usr/local/dbfw/templates/template-system-auth`
3. Upon successfully taking a backup, edit the original file. Search for the string `difok=4` and replace it with `difok=8`
4. Run the following command as root user:
`/usr/local/dbfw/bin/stig --apply`
5. Verify the change. Review the output of the following command:
`find /etc/pam.d -type f \! -name *.bak -exec fgrep difok {} +`

 **Note 6 OL6-00-000069 - administrator actions:**

1. Log in as root user.
2. Make a backup of the following file:
`/etc/sysconfig/init`
3. Upon successfully taking the backup, edit the file. Find the key `SINGLE` and replace it with `SINGLE=/sbin/sulogin`

G

Troubleshooting Oracle Audit Vault and Database Firewall

This appendix describes common troubleshooting advice.

G.1 Audit Vault Agent or Host Monitor is not Upgraded to the Latest Bundle Patch

Learn how to upgrade the Audit Vault Agent or Host Monitor Agent manually.

Problem

After upgrading to Oracle AVDF 12.2.0.13.0 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 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 is installed.
3. Execute the following command to uninstall the Host Monitor:

```
./hm/hostmonsetup uninstall
```

4. Download the new Host Monitor installable bundle from the Audit Vault Server console, for the specific platform on which it will be reinstalled.
5. Extract the Host Monitor bundle inside the `hm` directory.
6. Execute the following command to reinstall the Host Monitor in a `root` owned location:

```
./hostmonsetup install
```

G.2 Enable Archiving Functionality Post Upgrade From BP11 to Later Releases

Learn how to fix disabled archiving functionality post upgrade from Oracle AVDF 12.2.0.11.0 to later releases (12.2.0.12.0 or 12.2.0.13.0).

Problem

Archiving functionality may be disabled after upgrading from Oracle AVDF 12.2.0.11.0 or 12.2.0.12.0, to 12.2.0.12.0 or 12.2.0.13.0.

Archiving functionality for high availability environment is supported starting Oracle AVDF release 12.2.0.11.0. This problem arises when you are upgrading from older releases where archiving functionality is supported only on the primary Audit Vault Server. Execute the steps only if you are upgrading from Oracle AVDF 12.2.0.11.0 to later releases.



Note:

If you are upgrading from any release prior to Oracle AVDF 12.2.0.11.0, then follow the steps documented in section Enable Archiving Functionality Post Upgrade.

Solution

If archive locations were present before upgrading to 12.2.0.13.0, execute the following steps to enable archiving functionality. These steps must be executed post upgrade process.

1. Create a new archive location using the Audit Vault Server console. While creating this new archive location enter the details of both the primary and standby location. This will mount the new archive location on the primary or standby Audit Vault Server and update the `fstab` with both archive locations.

2. SSH to the primary Audit Vault Server as *support* user and then unlock the *avsys* user by executing the following commands:

```
su root
```

```
su dvaccountmgr
```

```
sqlplus /
```

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

```
exit;
```

```
exit;
```

3. Execute the following commands as *avsys* user:

```
su oracle
```

```
sqlplus avsys
```

4. Enter the *avsys* password when prompted. Execute the following SQL commands:

```
delete from avsys.system_configuration where property =  
'_ILM_ARCHIVING_DISABLED';
```

```
COMMIT;
```

```
insert into avsys.system_configuration values  
( '_ILM_HA_UPGRADE_COMPLETED', 'Y');
```

```
COMMIT;
```

```
exit;
```

```
exit;
```

5. Execute the following command to lock the avsys user:

```
su dvaccountmgr
```

```
sqlplus /
```

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

6. Delete the new archive location that was created in the initial step. Navigate to **Settings** tab, then click **Manage Archive Locations** in the left navigation menu. Delete the specific archive location.

G.3 Partial or No Traffic Seen for an Oracle Database Monitored by Database Firewall

Problem

I see no traffic, or only partial traffic, captured in reports for an Oracle Database monitored by the Database Firewall.

Solutions

Go through the following checks to find the trouble:

1. In the Audit Vault Server, check that the report filters are set correctly, including the time slot.
2. Check that the system time on the Database Firewall is synchronized with the time on the Audit Vault Server and the secured target system.
3. Check that the secured target's network traffic is visible to the Database Firewall using the Live Capture utility on the firewall.
4. Check that the Oracle Database service name or SID is used correctly. If you specified an Oracle Database service name in the Enforcement Point settings for this secured target, you will only see traffic for that service name. To see all traffic, remove the service name from the Enforcement Point settings to see all traffic.

If you have entered a service name in the Enforcement Point, and see no traffic, check to see that the service name is entered correctly in the Enforcement Point settings.

For Enforcement Points set to use DAM mode, the Database Firewall may be monitoring traffic for existing client connections to the database. Since these connections were in place before you deployed the Database Firewall, it will not be able to detect the service name you specify in the Enforcement Point. In this case, restart the client connections to the database.

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 Enforcement Points](#) (page 6-20) for information on Enforcement Points.
- [Viewing Network Traffic in a Database Firewall](#) (page 14-39)

G.4 RPM Upgrade Failed

Problem

An RPM upgrade failed with the following error:

```
error: %post(dbfw-mgmtsvr-###) scriptlet failed, exit status 1
```

Solution

1. Check that there is at least 10MB of free `/tmp` space.
2. Remove the new RPM:

```
rpm -e dbfw-mgmtsvr-###
```
3. Retry the upgrade.

G.5 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.

G.6 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.

G.7 Operation Fails When I Try to Build Host Monitor or Collect Oracle Database Trail

Problem

This problem may manifest with various symptoms:

- When I try to build a host monitor, the operation fails or cannot find the correct binaries.
- When I try to collect audit data from an Oracle Database secured target, the operation fails.
- The Audit Vault Agent cannot connect to the Audit Vault Server.
- Audit trail does not start.

Solution

1. Unset all environment variables except the following:

- PATH
- TERM
- PS1
- LANG
- LC_*
- JAVA_HOME

Then run the `java -jar agent.jar` command again on the host machine.

**See Also:**

[Deploying the Audit Vault Agent on the Host Computer](#) (page 5-5)

2. If you deployed the Audit Vault Agent in a Linux environment, ensure that the host machine name is present in the `/etc/hosts` file.

G.8 'java -jar agent.jar' Failed on Windows Machine

Problem

The command `java -jar agent.jar` failed on my Windows secured target machine, and I noticed in the log files that the Audit Vault Agent services installation/un-installation failed.

Solution

1. Follow the instructions for unregistering the agent in [Registering and Unregistering the Audit Vault Agent as a Windows Service](#) (page 5-7).

If Method 1 fails, then try Method 2.

2. Run the `java -jar agent.jar` command again.

G.9 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.

G.10 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 in [Registering and Unregistering the Audit Vault Agent as a Windows Service](#) (page 5-7).

If Method 1 fails, then try Method 2.

G.11 Access Denied Error While Installing Agent as a Windows Service

Problem

I got an error during installation of the Audit Vault Agent on Windows, and I noticed the following error in the `AGENT_HOME\av\log\av.agent.prunsrvr.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.

G.12 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.

G.13 Error When Starting the Agent

Problem

After I installed the Audit Vault Agent, I set the username and password in the `OracleAVAgent` Windows Service Properties **Log On** tab. However, when I try to start the `OracleAVAgent` service, I see the following error in the `Agent_Home\av\log\av.agent.prunsrvr.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.

G.14 Error When Running Host Monitor Setup

Problem

I am setting up a Host Monitor. When I run the command `bin/hostmonsetup install`, the following error is displayed:

```
[root@dbsecl av]# bin/hostmonsetup install /usr/bin/ld: cannot find -lpcap
collect2: ld returned 1 exit status make: *** [hostmonitor] Error 1 Line
105: Failed to generate executables for Host monitor.
```

Solution

This means the host computer does not have the required libraries for the Host Monitor. Install the required libraries listed in [Host Monitor Requirements](#) (page 7-2).

G.15 Alerts on Oracle Database Secured Target are not Triggered for a Long Time

Problem

I configured an Oracle Database secured target to audit to XML files, configured an audit trail in Oracle AVDF of type DIRECTORY, and then configured an alert to trigger on certain events. My alert did not get triggered for a long time.

Solution

This issue can occur if the Oracle Database secured target is not flushing the audit records to the file immediately. Contact Oracle Support in order to access support note *1358183.1 Audit Files Are Not Immediately Flushed To Disk*.

G.16 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.

G.17 Connection Problems when Using Database Firewall DPE Mode

Problem

In DPE (blocking) mode, my client application cannot connect to the secured target database.

Solution 1

1. Log in as `root` on the Database Firewall server.
2. Execute this command, using the secured target database IP address or host name:

```
ping -I secured_target_ip_address_or_hostname
```

If no response is received, check that:

- The bridge IP settings are correct.
- The bridge IP address is on the same subnet as the secured target database.
- DNS is configured on the Database Firewall

If a response is received, check:

- The firewall policy to ensure it is not blocking the connection attempt.
- The client connection settings to ensure that the client is attempting to connect to the correct secured target database.

See Also:

- [Configuring Database Firewall and its Traffic Sources on Your Network \(page 4-8\)](#)
- [Configuring Network Services For A Database Firewall \(page 4-4\)](#)

Solution 2

If your client application computer is on a different subnet than the secured target database, see document number **1566766.1** on My Oracle Support <https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1566766.1>.

G.18 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 **Secured 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.

See also document number **1566766.1** on My Oracle Support <https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1566766.1>.

G.19 Cannot Access the Audit Vault Server UI

Problem

The Audit Vault Server console UI is not accessible.

Solution

There are two steps you can take depending on when this problem occurs:

- The problem occurs immediately after Audit Vault Server installation.
In this case the installation may not have been completed correctly. Perform the installation again.
- The problem occurs after the system is already running.
In this case, check that the disk is not full, and that the Audit Vault Server database is running. To check that the database is running, execute this command:

```
/etc/init.d/dbfwdb status
```


To restart the database, use execute this command as `root`:

```
/etc/init.d/dbfwdb start
```


If you have a problem restarting the database, contact Oracle Support.

G.20 Cannot See Data for My Secured Target

Problem

Data for my Secured 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 Secured 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](#) (page 6-9)

- Check the audit policy on the secured 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 secured 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 enforcement point is created and running.
- Check that the enforcement point traffic source is correct.
- If the Database Firewall is in DAM 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 Secured Target Addresses section of your Secured Target configuration.



See Also:

[Viewing Network Traffic in a Database Firewall](#) (page 14-39)

- Check that you have used the correct Oracle Database service name when configuring the Secured Target Address in your Secured Target configuration.
Also, have you included all available Oracle Service names in the Secured Target Addresses section of the Secured 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 Secured 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
```

G.21 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 Database Firewall administration console, and then in the **Security** menu, click **Certificate**.
- 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](#) (page 3-3)
- [Setting the Date and Time in the Database Firewall](#) (page 4-5)

G.22 User 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 secured target, check to make sure that database interrogation 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.

 **See Also:**

- [Configuring and Using Database Interrogation](#) (page 6-24)
- [Viewing Network Traffic in a Database Firewall](#) (page 14-39)

G.23 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.
 - [Logging in to the Audit Vault Server Console UI](#) (page 1-11) for more information about logging in to the Audit Vault Server console.
- Restart job framework on the Audit Vault Server. See document **1592181.1** on My Oracle Support <https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1592181.1>.

G.24 Problems Retrieving or Provisioning Audit Settings on Oracle Secured Target

Problem

I have a problem either retrieving audit settings from an Oracle Database secured target, or provisioning audit settings to an Oracle Database secured 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 secured target configuration:
Log in to the Audit Vault Server as an administrator, click the **Secured Targets** tab, and then click the name of this Oracle secured target. Check the **Secured Target Location** field for the connect string.

 **See Also:**

[Secured Target Locations \(Connect Strings\)](#) (page B-36)

If you have problems provisioning audit settings, and the Oracle Database secured 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.

G.25 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
```

G.26 Failure While Adding Disks

If you experience disk failures when adding disks during an upgrade, then use this procedure.

Problem

Failure while adding additional disk or failure during upgrade. The symptoms include, but are not limited to:

- Two `vg_root` volume groups. This results in failure during install or upgrade.
- Hard drive devices becoming unavailable during install or upgrade. This leads to input or output errors and failure.

Solution

Ensure that any disk added to the appliance has no pre-existing LVM or other device mapper metadata. To remove any such metadata, follow these steps:

1. Execute the following command:

```
dd of=/dev/<device name> if=/dev/zero bs=1024k
```

 **Best Practice:**

To ensure you only erase the correct drive, place it in a standalone system to execute this command. On successful completion, add the drive to the Oracle Audit Vault and Database Firewall appliance.

2. Reboot the device.
3. Verify the partition table and metadata.

 **Note:**

Fiber Channel based storage with multipath is not supported in Oracle Audit Vault and Database Firewall.

G.27 Out of Memory Error Message During 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.

G.28 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 secured 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 secured target listener.
5. Once the secured target listener is started, start the agent, and the audit trail.

G.29 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
Successfully 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.

G.30 Internal capacity exceeded messages seen 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 Secured Target on which the issue is observed through the setting of the `MAXIMUM_ENFORCEMENT_POINT_THREADS` collection attribute.



See Also:

[Registering Secured Targets](#) (page 6-3)

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 Database Firewall 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 `/etc/init.d/dbfw restart`.

There is also a second setting available to alter the maximum size that the inter-process communication buffer can grow to. It's units are in megabytes, and has a default value of 64 megabytes. To change the configuration for this value execute the following procedure:

1. Log in to the Database Firewall console as the `root` user.
2. Edit the file `/var/dbfw/va/N/etc/appliance.conf`, where `N` is the number of the enforcement point in question. Look for an entry with the key `IPC_BUF_SIZ_MB`. If it exists, this is the line to change. If it does not exist, add a new line beginning with `IPC_BUF_SIZ_MB`.
3. Change the `IPC_BUF_SIZ_MB` to reflect the desired maximum buffer size. For example, if you wished to change the buffer size to 80 megabytes, the configuration line should be `IPC_BUF_SIZ_MB="80"`. Save the changes.
4. From the command line restart the Database Firewall processes so that the new setting is used with the command line `/etc/init.d/dbfw restart`.

If the problem persists and after altering the above settings the `Internal capacity exceeded error` is still encountered, then further investigation by support is required.

Perform the following:

1. Log in to the Database Firewall 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 `/etc/init.d/dbfw 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.

G.31 A Client Is Unable To Connect To The AVS Using SSH With A Secondary Network Interface Card

Problem

The Audit Vault Server is configured with a secondary Network Interface card for SSH connections. The secondary Network Interface card uses a gateway to access the wider network. When attempting to connect from the client to the Audit Vault Server, the connection cannot be established.

Solution

The Audit Vault Server implements spurious IP rules that prevent server connections forming on the secondary network interfaces.

This issue can be resolved by following this procedure:

1. Diagnose the connection issue by checking the incoming packets on the Audit Vault Server. Execute the following command while attempting to connect to the Audit Vault Server with the client using SSH:

```
# tcpdump -e -i any host <client IP address> and host <AVS IP address>
```

Result: The following output is displayed in case the client request is being received but dropped:

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size
65535 bytes
 11:01:25.455535 In <Client MAC> (oui Unknown) ethertype IPv4
(0x0800), length 100: <Client IP> >
eth1.oracle_database_firewall_internal: ICMP echo request, id 24456, seq
1, length 64
 11:01:25.455627 Out <AVS MAC> (oui Unknown) ethertype IPv4 (0x0800),
length 128: eth1.oracle_database_firewall_internal >
<Client IP>: ICMP host eth1.oracle_database_firewall_internal unreachable
- admin prohibited, length 92
```

2. In case there is no output displayed, then check the command argument. If the command is valid, then the connection is not being established to the Audit Vault Server. This indicates a wider networking problem.

In case the connection is established, then check the IP rules. There should be no specific IP rules on the Audit Vault Server. The IP rules enabled on the system can be checked with the following command:

```
# ip rule show
```

3. Systems with problem display the following output:

```
0:      from all lookup local
500:    from <Eth0 Address> lookup 1
501:    from <Eth1 Address> lookup 1
32766:  from all lookup main
32767:  from all lookup default
```

4. To fix this problem edit the following file:

```
/usr/local/dbfw/templates/template-rule-ethN
```

5. Delete the following line in the file:

```
from <%= @appliance_address %>/32 tab 1 priority <%= @ip_rule_base %>
```

6. Execute the following command for all IP addresses presented in the output received when the command `ip rule show` was executed:

```
ip rule del from IPADDRESS lookup 1
```

7. Restart every network interface.

8. Execute the following command to check the rule status again:

```
# ip rule show
```

Result: The following output is displayed:

```
0:      from all lookup local
32766:  from all lookup main
32767:  from all lookup default
```

9. SSH will now connect to the AVS.

G.32 First Archive Or Retrieve Job After Upgrade

Learn what to do if after an upgrade, the first archive or retrieve 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.

G.33 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:

[Updating Audit Vault Agents and Host Monitor Agents After Pairing Audit Vault Servers](#) (page 8-6)

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.

G.34 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](#) (page 3-11).
- 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.

G.35 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.

G.36 DB2 Collector Fails Due To Connection or Permission Issue From Database

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.SQLException: [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 secured target)
```

G.37 ORA-12660 Error While Registering Secured Target

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 G-1 Server Encryption Types

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.

G.38 Failure During High Availability Pairing in Oracle Audit Vault Server

Learn what to do when high availability pairing in Oracle Audit Vault Server fails.

Problem

There may be some errors encountered while executing high availability pairing Oracle Audit Vault Server. The errors may be in stored script memory, failure to verify some of the files in the backup set, failure to verify some of the data files, and failure to read or create files.

Solution

Check if ILM archival was run before you perform the high availability pairing in Oracle Audit Vault Server. This is due to presence of archive files in the primary server.

To avoid this, ensure that you delete archive files from the primary Oracle Audit Vault Server and later run the high availability pairing.

G.39 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.

G.40 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**.

G.41 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.

G.42 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.

G.43 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`.

G.44 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 `ORAUDIT` 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(Re  
doCollector.java:634)
```

Solution

Terminate the user application that is blocking the creation of streams. Restart the `Transaction Log` audit trail.

G.45 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 remain in a `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.

G.46 Pending Reports In Scheduled Status

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. Switch to *oracle* user using the command:

```
su oracle
```
4. Execute the following command to check the status of the Java Framework:

```
/usr/local/bin/javafwk status
```
5. Execute the following commands to stop and start the Java Framework:

```
/usr/local/dbfw/bin/javafwk stop
```



```
/usr/local/dbfw/bin/javafwk start
```

Use the following procedure to check the status of the reports from the operating system logs after executing one of the procedures mentioned above and restarting the Java Framework:

1. Log in to AVCLI as *admin* user.
2. Execute 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 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 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.

G.47 The Audit Vault Logs Display A Message To Install Npcap And OpenSSL

Problem

Host Monitor is capable of collecting audit data from Windows 2016 server. A message is displayed alerting the user to install *Npcap* and *OpenSSL*.

Solution

A set of *DLL* files may be causing an issue. Execute the following procedure to resolve this problem:

1. Search for the following files in the system:
 - `libssl-1_1-x64.dll`
 - `libcrypto-1_1-x64.dll`
 - `wpcap.dll`
 - `packet.dll`
2. Append the file names with `.bak` format.
3. Go to **Control Panel > Uninstall Programs** and uninstall *OpenSSL* and *WinPcap*.
4. Reinstall *Npcap* and *OpenSSL 1.1.1g*. 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 `.bak` 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 OpenSSL installation location to the path variable.
9. Restart the trail.
10. If the network audit trail 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 logs present at `<AgentHome>\hm\log` location.

Prerequisites are installed and present in PATH variable or System directory
<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 network trail does not start and continues to throw the above error, then ensure the Windows target machine has the latest update of *Visual C++ Redistributable for Visual Studio 2010* (`MSVCRT.dll (*)` or later) package installed. This is a must to use Host Monitor on Windows.
12. If the following message is available in the Host Monitor log, then execute the remaining procedure:

```
Invalid AVS Credentials provided
```
13. Open the `av/conf/bootstrap.prop` file.
14. Copy the following line:

```
CONNECT_STRING_PARAM_POSTFIX=9999
```
15. Paste this line in the `hm/bootstrap.prop` file.
16. Restart the trail.
17. In case the network audit trail starts without any errors, then the collection status on the Audit Vault Server console confirms the same.
18. Go to **AVAUDIT > Secured Target > Firewall Policies > Log All**.
19. Connect to the secured target database instance using SQL Developer, or any other tool.
20. Generate the traffic for collecting data.
21. It must be recorded in the reports of the `event_log` table.

G.48 Host Monitor Agent Fails to Start

Learn what to do when the Host Monitor Agent fails to start.

Problem

The Host Monitor 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. Ensure the Audit Vault Agent user belongs to the group that owns `hm` (Host Monitor installation) directory. Also ensure that the group that owns Host Monitor installation (`hm`) directory has `read` and `execute` permission on the `hm` directory and `execute` permission on `hostmonmanager` binary.

Note:

- `AgentHome` is the Audit Vault Agent installation directory.
- `hm` is the Host Monitor installation directory.

G.49 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.

G.50 Network Audit Trail Does Not Start on Unix Platforms

Learn the resolution when the network audit trail failst to start on Unix platforms.

Problem

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 are installed.
2. In the Agent Home location there is an `hm` symlink pointing to Host Monitor installation location.
3. Run the following command from the Agent Home as the user who installed Oracle Audit Vault Agent:
`ls -lrt hm`
4. Check if it is possible to list the contents of Host Monitor install directory.
5. Check the permission of all directories in the hierarchy of the path under which Host Monitor 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.

6. Grant the necessary permissions as stated above.
7. Restart the network audit trail.

G.51 Audit Vault Agent in Unreachable state upon Failover

Problem

Audit Vault Agent goes into *Unreachable* state in the event of a failover of the Audit Vault Server or reboot of the primary Audit Vault Server.

Symptom

Audit Vault Agent and audit trails go into *Unreachable* state.

Solution

1. For the Primary Audit Vault Server reboot instance - *Restart the Oracle Database Listener process on the standby Audit Vault Server.*
2. For the failover instance, restart the Oracle Database Listener process on the primary (old) Audit Vault Server. This is the Audit Vault Server which was primary prior to failover.

G.52 Unable to Reach Gateway Error

Learn to fix incorrect Gateway details entered during installation.

Problem

Incorrect or invalid Gateway details entered while installing Audit Vault Sever or Database Firewall. The following error message may be encountered:

```
Gateway is not reachable from host
```

Solution

The Gateway details can to be corrected by following these steps:

1. Log in to **Terminal-1** as *root* user. Alternately, **Terminal-1** can be accessed by pressing `Ctrl+Alt+Right Arrow Key`.
2. Access and open the `dbfw.conf` file by executing this command:

```
vi /usr/local/dbfw/etc/dbfw.conf
```

3. Set the correct value for the **GATEWAY** field by overwriting the existing value.
4. Save and close the file.
5. Execute the command to apply the modified value:

```
/usr/local/dbfw/bin/priv/configure-networking
```

6. Return back to the appliance screen by pressing `Ctrl+Alt+Left Arrow Key`.

Note:

The network settings entered during installation can be modified, by choosing the **Change IP Settings** option in the installer or appliance screen.

H

Multiple Network Interface Cards

The Audit Vault Server (AVS) supports network separation through addition and initialization of additional network interfaces.

Oracle Audit Vault and Database Firewall enables additional network interfaces to allow services on the Audit Vault Server to be accessible on networks other than the default management interface.

Note:

- Multiple Network Interface Cards are supported on Audit Vault from release 12.2.0.4.0 and onwards. The previous releases support one interface card on the Audit Vault Server.
- This feature is not available on the Database Firewall.

Different services can be enabled on a number of defined auxiliary network interfaces. The **Management Interface** on the `eth0` provides web user interface and Audit Vault Server to Database Firewall communication.

Note:

It is not possible to change the network interface used to serve the user interface. See [Features Of Network Interfaces For Audit Vault Server](#) (page H-15) for more information.

Topics:

- [Enabling A Secondary Network Interface For Audit Vault Server](#) (page H-2)
- [Configuring Physical Network Separation For Database Firewall](#) (page H-4)
- [Enabling NFS On Secondary Network Interface Card For Audit Vault Server](#) (page H-4)
- [Enabling SPA On Secondary Network Interface Card For Audit Vault Server](#) (page H-5)
- [Enabling SSH On A Secondary Network Interface Card For Audit Vault Server](#) (page H-5)
- [Applying Static Routing Rules On Network Interfaces For Audit Vault Server And Database Firewall](#) (page H-7)
- [Enabling Agent Connectivity On Secondary NICs for Audit Vault Server](#) (page H-8)

- [Enabling Agent To Operate In High Availability Environment With Secondary Network Interface Card For Audit Vault Server](#) (page H-12)
- [Disabling A Secondary Network Interface For Audit Vault Server](#) (page H-14)
- [Changing The IP Address On A Secondary Network Interface Card For Audit Vault Server](#) (page H-14)
- [Features Of Network Interfaces For Audit Vault Server](#) (page H-15)

H.1 Enabling A Secondary Network Interface For Audit Vault Server

Use this procedure to enable and configure a secondary network interface as an auxiliary access point to the appliance.

See Also:

[Changing The IP Address On A Secondary Network Interface Card For Audit Vault Server](#) (page H-14) to change the IP address of a secondary network interface card that has already been configured.

Note:

There can be multiple Secondary Network Interface cards on the Audit Vault.

Note:

Here is a description of the names, examples, and other terminology used in this document:

Terminology	Description
<code>SECONDARY_NIC_N_AGENT</code>	Agent ID or the IP.
<code>SECONDARY_NIC_N_DB_PORT</code>	Port ID.
<code>SECONDARY_NIC_N_</code>	A numerical value matching the <i>ethN</i> number of an existing NIC defined in the configuration.
<code>agent_id</code>	Agent name that is manually generated without the use of the UI.
Primary	AVS1 or Audit Vault Server 1
Secondary	AVS2 or Audit Vault Server 2

Follow this procedure:

1. Log in to the Audit Vault Server as *root* user.
2. Find a network interface that can be used. Execute the following command:

```
grep NIC_MAPPING /usr/local/dbfw/etc/dbfw.conf
```

The following output is displayed:

```
# The NIC_MAPPING variable maps the ethernet (MAC) addresses to device
names
NIC_MAPPING="eth0/08:00:27:3a:b7:17,eth1/08:00:27:9e:f6:55,eth2/08:00:27:7
0:11:c8"
```

 **Note:**

eth0 is always used for the default management interface. However, in the above example both eth1 and eth2 are available.

3. It is important at this point to check that the interface intended to be used has not been configured previously. Execute the following command by taking eth1 as an example:

```
ifconfig eth1
```

The following is the example output:

```
eth1 Link encap:Ethernet HWaddr 08:00:27:9E:F6:55
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:928 errors:0 dropped:0 overruns:0 frame:0
TX packets:571 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:84409 (82.4 KiB) TX bytes:130699 (127.6 KiB)
```

4. Execute the following command to take a backup of the configuration file:
- ```
cp /usr/local/dbfw/etc/dbfw.conf /usr/local/dbfw/etc/dbfw.conf.backup
```
5. Open the configuration file of the appliance using *vi*:
- ```
vi /usr/local/dbfw/etc/dbfw.conf
```
6. Scroll down to the end of the file and add the following lines with the IP address and network mask for the new interface:

```
# Enable an auxiliary network interface on eth1.
SECONDARY_NIC_1_ADDRESS="<ip-address>"
SECONDARY_NIC_1_NETMASK="<network-mask>"
```

7. Save the file and exit *vi*:

```
:w [return]
:q [return]
```

8. Alternately execute the following command:

```
cat <<EOF >> /usr/local/dbfw/etc/dbfw.conf
```

```
# Enable an auxiliary network interface on eth1.
```

```
SECONDARY_NIC_1_ADDRESS="<IP address>"  
SECONDARY_NIC_1_NETMASK="<Network mask>"  
EOF
```

9. Execute the following command to apply the configuration changes by the network configuration application:

```
/usr/local/dbfw/bin/priv/configure-networking
```

The following output is displayed:

```
Shutting down system logger: [ OK ]  
Starting system logger:  
Determining if ip address xxx.yyy.xy.zz is already in use for  
device eth1...
```

10. Execute the following command to check the status of the interface:

```
ifconfig eth1
```

NIC is online. The following output now confirms the correct IP address and network mask:

```
eth1 Link encap:Ethernet HWaddr 08:00:27:9E:F6:55  
inet addr:xxx.yyy.xy.zz Bcast:xxx.yyy.xy.zz Mask:xxx.yyy.zzz.0  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:120 errors:0 dropped:0 overruns:0 frame:0  
TX packets:53 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:22890 (22.3 KiB) TX bytes:13892 (13.5 KiB)
```

H.2 Configuring Physical Network Separation For Database Firewall

To provide network separation for services provided by the Database Firewall appliance, see [Configuring a Bridge in the Database Firewall](#) (page 4-9).

H.3 Enabling NFS On Secondary Network Interface Card For Audit Vault Server

Use this topic to enable Network File Storage on a secondary Network Interface Card.

Network File Storage can be enabled on an auxiliary interface. This consists of the following steps:

1. Follow the procedure in [Enabling A Secondary Network Interface For Audit Vault Server](#) (page H-2) first.
2. Configure the Network File Storage to directly access the NFS server on the local network. Follow the procedure in [REGISTER REMOTE FILESYSTEM](#) (page A-53).

H.4 Enabling SPA On Secondary Network Interface Card For Audit Vault Server

Use this topic to enable Stored Procedure Auditing on a secondary Network Interface Card for Audit Vault Server.

Stored Procedure Auditing can be enabled on an auxiliary interface. This consists of the following steps:

1. Follow the procedure in [Enabling A Secondary Network Interface For Audit Vault Server](#) (page H-2) first.
2. Configure the Stored Procedure Auditing host to directly access the secured targets intended for SPA on the local network. Follow the procedure in [Configuring Stored Procedure Auditing \(SPA\)](#) (page 6-24).

H.5 Enabling SSH On A Secondary Network Interface Card For Audit Vault Server

Use this procedure to enable SSH on a secondary network interface card.

To enable and configure SSH on a secondary network interface card, follow these steps:

1. Enable the secondary Network Interface Card.
2. Execute the following commands to open the appliance configuration file:
3. Scroll down to the end of the file, below the new `SECONDARY_NIC_` keys and add the following to enable incoming SSH connections from all addresses:

```
# Enable SSH on eth1.  
SECONDARY_NIC_1_SSH="all"
```

 **Note:**

This is optional. Replace `all` with `disabled` or with a blank string. This disables SSH connections on the network interface card.

4. To limit the incoming connections to specific addresses use a space separated list of IP addresses as follows:

```
SECONDARY_NIC_1_SSH="<IP address 1> <IP address 2>"
```

5. The default port for SSH connections is 22. To use a different port number, add the following key and port value as below:

```
SECONDARY_NIC_1_SSH_PORT="22222"
```

6. Alternately replace the values as required:

```
cat <<EOF >> /usr/local/dbfw/etc/dbfw.conf
# Enable SSH on eth1.
SECONDARY_NIC_1_SSH="all"
SECONDARY_NIC_1_SSH_PORT="22222"
```

7. Execute the network configuration code to complete configuring the appliance with the new port specification:

```
/usr/local/dbfw/bin/priv/configure-networking
```

The following output confirms that terminal connection through SSH is now possible over local network through the configured network interface:

```
$ ssh -p22222 support@xxx.yyy.yy.zz
Warning: Permanently added '[xxx.yyy.yy.zz]:22222' (RSA) to the
list of known hosts.
support@xxx.yyy.yy.zz's password:
Last login: Tue Oct 11 13:11:14 2016 from 10.167.202.82
[support@avs0800273ab717 ~]$ su -
Password:
Last login: Tue Oct 11 13:11:20 UTC 2016 on pts/0
[root@avs0800273ab717 ~]#
```

8. Execute the following command to view the current services listening on the appliance:

```
netstat -pean | grep sshd
```

The following output verifies the established connections configured listening, to the intended interface through the SSH daemon:

```
tcp 0 0 xxx.yyy.yy.zz:22222 0.0.0.0:* LISTEN
0 1043313 21098/sshd
tcp 0 0 xx.yyy.yy.zz:22 0.0.0.0:* LISTEN
0 1043315 21098/sshd
tcp 0 0 xxx.yyy.yy.zz:22222 xxx.yyy.yy.z:42568 ESTABLISHED
0 1100215 24276/sshd
tcp 0 0 xx.yyy.yy.zz:22 xx.yyy.yy.zz:48340 ESTABLISHED
0 957675 15987/sshd
unix 3 [ ] STREAM CONNECTED 1100576 24317/sshd
unix 2 [ ] DGRAM 957849 15987/sshd
unix 3 [ ] STREAM CONNECTED 957853 15987/sshd
unix 3 [ ] STREAM CONNECTED 1100577 24276/sshd
unix 3 [ ] STREAM CONNECTED 957852 16015/sshd
unix 2 [ ] DGRAM 1100573 24276/sshd
```

 **See Also:**

- [A Client Is Unable To Connect To The AVS Using SSH With A Secondary Network Interface Card](#) (page G-21) for more information in case you are unable to connect to the Audit Vault Server through SSH.
- [Enabling A Secondary Network Interface For Audit Vault Server](#) (page H-2)

H.6 Applying Static Routing Rules On Network Interfaces For Audit Vault Server And Database Firewall

Use this procedure to apply static routing rules on network interfaces for Audit Vault Server and Database Firewall.

The default configuration for a secondary network interface is to route to the directly connected subnet only. As the *root* user, execute the steps below to add routes to other networks.

The Audit Vault Server has network interface devices with the name `ethN`. The Database Firewall has bridge device with the name `brN`, or a regular network interface device with the name `ethN`.

 **Note:**

`eth1` is the network interface in the example below. Replace it with the actual device name.

1. Create the template include directory if it does not exist. Execute:

```
install -m 0755 -d /usr/local/dbfw/templates/include
```
2. Create a routing file `after-route-eth1` if it does not exist. Execute:

```
touch /usr/local/dbfw/templates/include/after-route-eth1
```
3. Ensure the file is writable only by *root* user. Execute:

```
chown root:root /usr/local/dbfw/templates/include/after-route-eth1  
chmod 444 /usr/local/dbfw/templates/include/after-route-eth1
```
4. Add your static route. Add a line similar to the following to `after-route-eth1`. Replace the values with those from your network.

```
198.51.100.0/24 via 192.0.2.100 dev eth1
```

In this example:

- `eth1` is the appliance's interface, which is directly connected to the `192.0.2.0/24` network.
- `198.51.100.0/24` is the remote network. The appliance directs traffic to it through the gateway.

- 192.0.2.100 is the gateway's address on the directly connected 192.0.2.0/24 network.
 - Ensure your network administrator configures the gateway to route packets in both directions between the 192.0.2.0/24 and 198.51.100.0/24 networks.
5. Save the file.
 6. Execute the network configuration utility:

```
/usr/local/dbfw/bin/priv/configure-networking
```
 7. Apply your changes. Execute:

```
ifdown eth1  
ifup eth1
```
 8. Verify your route is present. Execute:

```
ip route list
```

The output should include the route you specified above. In the example, the following line is present:

```
198.51.100.0/24 via 192.0.2.100 dev eth1
```

 **See Also:**

Oracle® Linux Administrator's Guide for more information on network configuration.

H.7 Enabling Agent Connectivity On Secondary NICs for Audit Vault Server

Use this procedure to enable agent connectivity on a secondary network interface card.

After a secondary NIC is online, you can enable it for agent database communication. This topic describes how to enable this agent connectivity on secondary network interface cards.

To enable agent connectivity on secondary network interfaces card for Audit Vault Server:

1. Enable the secondary Network Interface card.
2. Run the following commands to open the appliance configuration file:

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

```
vi /usr/local/dbfw/etc/dbfw.conf
```

3. Scroll down to the end of the file, below the new `SECONDARY_NIC_1` keys and add the following to enable incoming agent connections from all addresses:

```
# Enable agent connectivity on eth1.
```

```
SECONDARY_NIC_1_AGENT="all"
```

 **Note:**

Optionally, you can replace `all` with `disabled` or with a blank string. This disables agent connections on the network interface card.

4. To limit the incoming connections to specific addresses, use a space-separated list of IP addresses as follows:

```
SECONDARY_NIC_1_AGENT="<IP address 1> <IP address 2>"
```

5. The default ports for agent connections are 1521 and 1522. To use a different port number, add the following keys:

```
SECONDARY_NIC_1_AGENT_PORT="21521"
```

```
SECONDARY_NIC_1_AGENT_PORT_TLS="21522"
```

6. Alternately, replace the values as required:

```
cat <<EOF>> /usr/local/dbfw/etc/dbfw.conf
```

```
# Enable agent connectivity on eth1.
SECONDARY_NIC_1_AGENT="all"
SECONDARY_NIC_1_AGENT_PORT="21521"
SECONDARY_NIC_1_AGENT_PORT_TLS="21522"
EOF
```

7. Run the following commands to apply the configuration changes using the network configuration application:

```
/usr/local/dbfw/bin/priv/configure-networking
```

```
/usr/local/dbfw/bin/os_manager execute_script update_connect_string_ip.sh
```

8. You can view the database listener active configuration by running the following command:

```
netstat -pean | grep tnslsnr
```

The following output confirms that a listener is waiting for an incoming connection:

```

tcp 0 0 127.0.0.1:5700 0.0.0.0:* LISTEN
503 9423978 13596/tnslnsr
tcp 0 0 127.0.0.1:1521 0.0.0.0:* LISTEN
503 9423976 13596/tnslnsr
tcp 0 0 <IP address>:21521 0.0.0.0:* LISTEN
503 9423970 13596/tnslnsr
tcp 0 0 10.170.90.16:1521 0.0.0.0:* LISTEN
503 9423935 13596/tnslnsr
tcp 0 0 <IP address>:21522 0.0.0.0:* LISTEN
503 9423974 13596/tnslnsr
tcp 0 0 10.170.90.16:1522 0.0.0.0:* LISTEN
503 9423966 13596/tnslnsr
tcp 0 0 127.0.0.1:1523 0.0.0.0:* LISTEN
507 272087 32752/tnslnsr
tcp 0 0 127.0.0.1:1521 127.0.0.1:10272 ESTABLISHED
503 9433031 13596/tnslnsr
tcp 0 0 127.0.0.1:1521 127.0.0.1:10273 ESTABLISHED
503 9433032 13596/tnslnsr
unix 2 [ ACC ] STREAM LISTENING 272084 32752/tnslnsr
/var/tmp/.oracle/sEXTPROC1523
unix 2 [ ACC ] STREAM LISTENING 272085 32752/tnslnsr
/var/tmp/.oracle/s#32752.1
unix 2 [ ACC ] STREAM LISTENING 272088 32752/tnslnsr
/var/tmp/.oracle/s#32752.2
unix 2 [ ACC ] STREAM LISTENING 9423930 13596/tnslnsr
/var/tmp/.oracle/sEXTPROC1521
unix 2 [ ACC ] STREAM LISTENING 9423931 13596/tnslnsr
/var/tmp/.oracle/s#13596.1
unix 2 [ ACC ] STREAM LISTENING 9423979 13596/tnslnsr
/var/tmp/.oracle/s#13596.2

```

9. You can now connect to the database on the local network from another computer:

```

sqlplus64 avadmin/<password>@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=<IP address>)(PORT=21521))(CONNECT_DATA =
(SERVICE_NAME=dbfwdb)))

```

 **Note:**

This connects to the clear text communication port of Audit Vault Server, which you must avoid. Use encrypted communication protocols whenever possible.

The following output verifies the established connection:

```

SQL*Plus: Release 12.1.0.2.0 Production on Wed Oct 12 11:37:00 2016
Copyright (c) 1982, 2014, Oracle. All rights reserved.
Last Successful login time: Wed Oct 12 2016 11:36:23 +01:00
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit

```



```

Production
With the Partitioning, Automatic Storage Management, Oracle Label
Security, OLAP,
Advanced Analytics, Oracle Database Vault and Real Application Testing
options
SQL> select 1 from dual;
1
-----
1
SQL>

```

10. Deploy the Audit Vault agent on the host computer.

11. You must upgrade all of the agents. To do this, run the following PL/SQL block as Audit Vault administrator to initiate the auto upgrade process:

```

DECLARE
    hostName VARCHAR2(300 CHAR);
    CURSOR HOST_NAMES
IS
    SELECT HOST_NAME
    FROM AVSYS.AGENT_VIEW
    WHERE STATUS IN ('RUNNING');
BEGIN
OPEN HOST_NAMES;
LOOP
    FETCH HOST_NAMES INTO hostName;
    EXIT WHEN HOST_NAMES%notfound;
    BEGIN
        AVSYS.ADM.send_update_message(hostName);
    EXCEPTION
        WHEN NO_DATA_FOUND THEN
            -- no host to auto upgrade.
            EXIT;
        END;
    END LOOP;
CLOSE HOST_NAMES;
END;

```

 **See Also:**

- [Deploying the Audit Vault Agent on the Host Computer](#) (page 5-5)
- [Enabling A Secondary Network Interface For Audit Vault Server](#) (page H-2)

H.8 Enabling Agent To Operate In High Availability Environment With Secondary Network Interface Card For Audit Vault Server

Use this procedure to enable Agent to operate in high availability environment with secondary NIC for Audit Vault Server.

In configurations with high availability enabled it is necessary to first enable the data network for the agent on the primary and the secondary Audit Vault Server. This topic contains the necessary steps to enable Agent to operate in high availability environment with secondary NIC.

Note:

The user must use the same port for the primary and secondary network interface card while configuring the secondary card for High Availability.

Note:

In case you are performing an upgrade to 12.2.0.4.0, follow these steps first:

1. Log in as *administrator* and execute the upgrade task on Audit Vault Server appliance.
2. Upgrade each AVS appliance to 12.2.0.4.0 and follow high availability upgrade procedure.
3. Follow steps from the note below to enable agent data network on secondary Network Interface card.

Note:

To enable agent data network on the preconfigured HA setup, perform the following:

1. Enable the agent data network on the primary Audit Vault Server (AVS1).
2. Execute Audit Vault Server switchover.
3. Enable the agent data network on the new primary Audit Vault Server AVS2.

To enable Agent to operate in high availability environment with secondary NIC for Audit Vault Server, follow these steps:

1. Both the appliances in the configuration must be updated with the new auxiliary network interface information from the other appliance. On both the primary and secondary Audit Vault Server appliances execute the steps mentioned in [Enabling Agent Connectivity On Secondary NICs for Audit Vault Server](#) (page H-8). This enable the Agent on the auxiliary interface.

2. In the primary appliance, add the address of the newly defined auxiliary interface of the secondary appliance. Open the configuration file of the primary appliance:

```
vi /usr/local/dbfw/etc/dbfw.conf
```

3. Scroll to the bottom of the file and add the following:

```
# The address of the network interface defined for the agent on the
secondary AVS.
```

```
SECONDARY_NIC_1_ADDRESS_HA="<IP address>"
```

4. On the secondary appliance, add the address of the newly defined auxiliary interface of the primary appliance.

5. Open the configuration file of the secondary appliance:

```
vi /usr/local/dbfw/etc/dbfw.conf
```

6. Scroll to the bottom of the file and add the following:

```
# The address of the network interface defined for the agent on the primary
AVS.
```

```
SECONDARY_NIC_1_ADDRESS_HA="<IP address>"
```

7. Execute the following commands on AVS1 and AVS2 after updating the configuration:

```
/usr/local/dbfw/bin/priv/configure-networking
```

```
/usr/local/dbfw/bin/os_manager execute_script update_connect_string_ip.sh
```

8. Configure the resilient pair between the AVS1 and AVS2 Audit Vault Servers. It is necessary to define routes for the agents to access the original networks in case they use the default gateway device.



See Also:

[Adding User Content To System Configuration Files](#) (page I-1) for more information on configuring the required routes, if the agents are on a different subnet than the Audit Vault Server.

9. The agent must be redeployed to the host.

Result: The agent is now able to communicate with the primary Audit Vault Server on the newly defined Network Interface Card.

H.9 Disabling A Secondary Network Interface For Audit Vault Server

Use this procedure to disable the configured secondary network interface card for Audit Vault Server.

Note:

The secondary network interface card cannot be disabled temporarily. However, it is possible to restrict access to the services running on the network interface card by setting a blank string or mark *disabled* for the keys `SECONDARY_NIC_[N]_SSH` and `SECONDARY_NIC_[N]_AGENT`. See sections [Enabling SSH On A Secondary Network Interface Card For Audit Vault Server](#) (page H-5) and [Enabling Agent Connectivity On Secondary NICs for Audit Vault Server](#) (page H-8) for similar information.

To disable a secondary Network Interface, follow this procedure:

1. Execute the following command to open the configuration file:

```
vi /usr/local/dbfw/etc/dbfw.conf
```

2. Remove all keys from the file beginning `SECONDARY_NIC`.
3. Execute the following command:

```
/usr/local/dbfw/bin/priv/configure-networking
```

4. Execute the commands listed in the table below depending on configuration:

Configuration	Commands
<code>SECONDARY_NIC_[N]_AGENT</code>	<code>/etc/init.d/dbfwlistener restart</code>
<code>SECONDARY_NIC_[N]_SSH</code>	<code>/usr/local/dbfw/etc/privileged-migrations/ssh-sshd-conf.rb</code> <code>/etc/init.d/sshd reload</code>

H.10 Changing The IP Address On A Secondary Network Interface Card For Audit Vault Server

Use this procedure to change the previously configured IP address of the secondary network interface card for Audit Vault Server.

To change the IP address on a secondary network interface card for Audit Vault Server, follow this procedure:

1. Execute the following command to open the file `/usr/local/dbfw/etc/dbfw.conf`:

```
vi /usr/local/dbfw/etc/dbfw.conf
```

- Execute the following command to change the key pertaining to the IP address of the secondary network interface card:

```
SECONDARY_NIC_[n]_ADDRESS="<New IP Address>"
```

- Execute the following command to update the network mask if required:

```
SECONDARY_NIC_[n]_NETMASK="<New Network Mask>"
```

- Run the following network configuration script:

```
/usr/local/dbfw/bin/priv/configure-networking
```

- Execute the commands listed in the table below depending on configuration and restart the specified component:

Network card configuration	Restart component	Command
Agent connectivity	Listener	/etc/init.d/dbfwlistener restart
SSH connectivity	SSH daemon	/etc/init.d/sshd restart

H.11 Features Of Network Interfaces For Audit Vault Server

This section contains some of the features of Management Interfaces and Secondary Network Interfaces for the Audit Vault Server.

Management Interfaces

Every Audit Vault Server has a **Management Interface** which provides the following features:

- Web UI console
- High Availability
- Database Firewall communication. This includes configuration of the Database Firewall appliance from the Audit Vault Server and retrieval of the log.
- Network File Storage
- Stored Procedure Auditing
- SSH
- Static Routes
- Agent connectivity

Secondary Network Interfaces

You can add Secondary Network Interfaces and use them for some or all of the following features:

- Auxiliary access
- Network File Storage
- Stored Procedure Auditing
- SSH
- Static Routes
- Agent connectivity

- Agent high availability



Note:

You can add only one interface with one address on each network. You cannot bind multiple addresses on the same network to secondary network interfaces. You cannot add multiple network interfaces using the same address for load balancing or bonding.

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.

Index

Symbols

- HELP command, [A-63](#)
- VERSION command, [A-64](#)

A

access

- remote, security guidelines for, [2-1](#)
- revoking for secured targets, [13-4](#)

access rights

- about managing, [13-1](#)
- administrator account types, [13-1](#)
- controlling by user, [13-7](#)
- planning, [1-10](#)
- secured targets. controlling by target or group, [13-7](#)

accounts

- administrative accounts, [13-1](#)
- setting up on secured targets
 - about, [B-22](#)
 - IBM DB2, [B-30](#)
 - Microsoft SQL Server, [B-27](#)
 - MySQL, [B-31](#)
 - Oracle Database, [B-22](#)
 - Sybase ASE, [B-25](#)
 - Sybase SQL Anywhere, [B-26](#)

ACFS

- See Oracle ACFS

Actions button, [1-12](#)

ACTIVATE HOST command, [A-6](#)

activate, Audit Vault Agent with key, [5-6](#)

Active Directory

- See Microsoft Active Directory

add target to a group, [A-24](#)

add target to a target group, [A-24](#)

Adding

- User Content To System Configuration Files, [I-1](#)

additional information

- audit collection from Oracle Active Data Guard, [B-31](#)

administrative features, [1-3](#)

administrators

- access rights, [13-1](#)

administrators (*continued*)

- roles, [1-6](#)
- tasks, [1-5](#)
- user account types, [13-1](#)

advise on implementation

- Security Technical Implementation Guides (STIG), [F-1](#)

agent host commands, [A-2](#)

agentctl command

- start/stop, [5-9](#)
- to register Audit Vault Agent as Windows service, [5-8](#)

alerts

- configuring email service for, [3-10](#)
- forwarding to syslog, [3-8](#)

ALTER DATA ENCRYPTION command, [A-43](#)

ALTER DISKGROUP command, [A-51](#)

ALTER ENFORCEMENT POINT command, [A-15](#)

ALTER FIREWALL command, [A-11](#)

ALTER HOST command, [A-3](#)

ALTER REMOTE FILESYSTEM command, [A-54](#)

ALTER SAN SERVER command, [A-49](#)

ALTER SECURED TARGET command, [A-19](#)

ALTER SMTP SERVER command, [A-38](#)

ALTER SMTP SERVER DISABLE command, [A-39](#)

ALTER SMTP SERVER ENABLE command, [A-39](#)

ALTER SYSTEM SET command, [A-56](#)

ALTER SYSTEM SMTP SERVER SECURE MODE OFF command, [A-41](#)

ALTER SYSTEM SMTP SERVER SECURE MODE ON command, [A-40](#)

ALTER USER command, [A-47](#)

Applying Static Routing Rules

- Secondary Network Interface card for Audit Vault Server, [H-7](#)

architecture

- high availability resilient pairs, [8-1](#)

Archive data files are required (link), [6-12](#)

archiving

- disk space
 - additional for SMB and scp archive data transfer, [3-13](#)

- archiving (*continued*)
 - expired audit records
 - archive files required, [6-13](#)
 - how treated, [3-13](#)
 - filesystem
 - additional space for SMB and scp
 - archive data transfer, [3-13](#)
 - NFS filesystem, [3-13](#)
 - policies
 - creating, [3-17](#)
 - described, [3-12](#)
 - port for Windows File Sharing transfer
 - method, [3-13](#)
 - purging data files after retrieving, [14-8](#)
 - retrieving from archives, [14-8](#)
 - security guidelines, [2-1](#)
 - SMB
 - See Windows File Sharing
 - starting an archive job, [14-7](#)
 - transfer method, [3-13](#)
 - scp, [3-12](#)
 - SMB, [3-12](#), [3-13](#)
- ArcSight Security Information Event Management (SIEM)
 - about, [10-2](#)
 - deployment procedure, [10-3](#)
 - enabling interface, [10-3](#)
 - specifying ArcSight server, [10-3](#)
- audit data
 - date range in memory, [14-26](#)
 - storing in memory on Audit Vault Server, [14-26](#)
- audit trails
 - Autostart parameters, avcli, [A-56](#)
 - Autostart status, [6-13](#)
 - Autostart, about, [6-11](#)
 - cleanup
 - IBM DB2 audit files, [6-16](#)
 - Microsoft SQL Server audit trail, [B-34](#)
 - Oracle Database, [B-33](#)
 - collections, AVCLI command for, [A-25](#)
 - configurations
 - REDO logs, recommended settings, [C-1](#)
 - configuring collection, [6-9](#)
 - dropping a trail, [A-35](#)
 - finding list of, [A-34](#)
 - IBM DB2
 - about, [B-21](#)
 - prerequisite for starting, [6-16](#)
 - MySQL
 - trail location, [6-14](#), [A-29](#), [A-33](#), [B-11](#), [B-43](#)
 - XML transformation, [6-14](#)
 - planning, [1-9](#)
 - planning configurations, [1-9](#)
- audit trails (*continued*)
 - platform support, [B-17](#)
 - purging Oracle Database trail, [B-33](#)
 - restart, automatic, [6-11](#)
 - starting and stopping, [6-11](#)
 - starting collection, [A-26](#)
 - status
 - Collecting, [6-12](#)
 - Idle, [6-12](#)
 - Recovering, [6-12](#)
 - Stopped, [6-12](#)
 - Unreachable, [6-12](#)
 - status, checking, [6-12](#)
 - stopping collection, [A-30](#)
 - TABLE, [B-18](#)
 - types, [B-17](#)
 - location for DIRECTORY type, [6-11](#), [B-42](#)
- Audit Vault Agent
 - activating, [5-6](#)
 - deactivating, [5-12](#)
 - debug, logging, [5-11](#), [14-5](#)
 - deploying and activating, [5-3](#)
 - log files location, [5-11](#)
 - logging levels, setting, [5-11](#)
 - OS user account for deployment, [5-5](#)
 - planning deployments, [1-8](#)
 - plug-ins
 - about, [5-13](#), [B-1](#)
 - deploy and activate procedure, [5-14](#)
 - undeploying, [5-15](#)
 - removing, [5-12](#)
 - requirements, Java SE, [5-5](#)
 - start in console mode, [5-9](#)
 - starting, [5-9](#)
 - starting, initial, [5-6](#)
 - stop in console mode, [5-9](#)
 - stopping, [5-9](#), [5-12](#)
 - timestamps for Oracle Database trail purge
 - process, [B-33](#)
 - Windows service, autostarting, [5-10](#)
 - Windows service, registering, [5-7](#)
 - Windows service, unregistering, [5-8](#)
- Audit Vault and Database Firewall
 - administrative features, [1-3](#)
 - administrator roles, [1-6](#)
 - administrator tasks, [1-5](#)
 - auditing features, [1-4](#)
 - configuration workflow, [1-6](#)
 - documentation, downloading latest, [1-1](#)
 - IPv6 not supported, [2-4](#)
- Audit Vault Server
 - administrative tasks
 - archiving log disk space, monitoring, [14-29](#)

- Audit Vault Server (*continued*)
 - administrative tasks (*continued*)
 - changing user passwords, [13-8](#)
 - flash recovery area, [14-30](#)
 - SYSAUX tablespace usage, [14-29](#)
 - Audit Vault Server
 - reboot upon changing host name, [3-5](#)
 - backup/restore, [14-14](#)
 - certificate
 - location, [14-4](#)
 - supplying to Database Firewall, [4-6](#)
 - certificate renewal, [2-12](#)
 - certificate rotation, [2-12](#)
 - certificate warning, UI, [3-2](#)
 - changing keyboard layout, [14-6](#)
 - configuration
 - about, [3-1](#)
 - initial tasks, [3-3](#)
 - network settings, [3-5](#)
 - configuring
 - SSH access, [3-7](#)
 - detailed diagnostics, [14-3](#)
 - diagnostic checks, [14-2](#)
 - encryption
 - changing keystore password, [14-9](#)
 - of repository, about, [14-9](#)
 - rotating key, [14-9](#)
 - failover, [8-8](#)
 - high availability
 - about, [8-3](#)
 - failover, [8-8](#)
 - status, [8-6](#)
 - host name, changing, reboot required, [3-5](#)
 - in-memory usage, [14-28](#)
 - IP address
 - changing, reboot required, [3-5](#)
 - supplying to Database Firewall, [4-6](#)
 - jobs monitoring, [14-31](#)
 - log files location, [A-56](#)
 - logging in to UI, [1-11](#)
 - network configuration, [3-5](#)
 - pairing, [8-3](#)
 - planning configuration, [1-8](#)
 - primary server in resilient pair, [8-5](#)
 - public key, [14-4](#)
 - reboot
 - upon changing host name, [3-5](#)
 - rebooting, powering off, [14-6](#)
 - registering Database Firewall in, [3-20](#)
 - removing Database Firewall from, [14-40](#)
 - removing secured targets from, [6-5](#)
 - restore, [14-23](#)
 - SNMP access, [3-7](#)
 - status, checking, [14-2](#)
 - syslog destinations, configuring, [3-8](#)
- Audit Vault Server (*continued*)
 - testing system operation, [3-21](#)
 - UI, tabs described, [1-11](#)
 - user accounts, creating in, [13-3](#)
 - auditing features, [1-4](#)
 - AUDITOR and ADMIN commands, [A-65](#)
 - authentication
 - using for host monitor-Database Firewall communication, [7-11](#)
 - Autostart
 - audit trail, about, [6-11](#)
 - avcli parameters, [A-56](#)
 - status, audit trail, [6-13](#)
 - AVCLI commands
 - HELP, [A-63](#)
 - VERSION, [A-64](#)
 - ACTIVATE HOST, [A-6](#)
 - ALTER DATA ENCRYPTION, [A-43](#)
 - ALTER DISKGROUP, [A-51](#)
 - ALTER ENFORCEMENT POINT, [A-15](#)
 - ALTER FIREWALL, [A-11](#)
 - ALTER HOST, [A-3](#)
 - ALTER REMOTE FILESYSTEM, [A-54](#)
 - ALTER SAN SERVER, [A-49](#)
 - ALTER SECURED TARGET, [A-19](#)
 - ALTER SMTP SERVER, [A-38](#)
 - ALTER SMTP SERVER DISABLE, [A-39](#)
 - ALTER SMTP SERVER ENABLE, [A-39](#)
 - ALTER SYSTEM SET, [A-56](#)
 - ALTER SYSTEM SMTP SERVER SECURE MODE OFF, [A-41](#)
 - ALTER SYSTEM SMTP SERVER SECURE MODE ON, [A-40](#)
 - ALTER USER, [A-47](#)
 - CLEAR LOG, [A-63](#)
 - CONNECT, [A-62](#)
 - CREATE ENFORCEMENT POINT, [A-12](#)
 - CREATE RESILIENT PAIR, [A-9](#)
 - DEACTIVATE HOST, [A-6](#)
 - DEPLOY PLUGIN, [A-59](#)
 - DOWNLOAD LOG FILE, [A-59](#)
 - DROP ENFORCEMENT POINT, [A-13](#)
 - DROP FIREWALL, [A-8](#)
 - DROP HOST, [A-5](#)
 - DROP REMOTE FILESYSTEM, [A-55](#)
 - DROP RESILIENT PAIR, [A-10](#)
 - DROP SAN SERVER, [A-50](#)
 - DROP SECURED TARGET, [A-24](#)
 - DROP SMTP SERVER, [A-43](#)
 - DROP TRAIL FOR SECURED TARGET, [A-35](#)
 - GRANT ACCESS, [A-45](#)
 - GRANT ADMIN, [A-46](#)
 - GRANT SUPERADMIN, [A-44](#)

AVCLI commands (*continued*)

- LIST ADDRESS FOR SECURED TARGET, [A-22](#)
- LIST ATTRIBUTE FOR SECURED TARGET, [A-23](#)
- LIST ATTRIBUTE OF SMTP SERVER, [A-42](#)
- LIST DISK, [A-50](#)
- LIST DISKGROUP, [A-51](#)
- LIST ENFORCEMENT POINT, [A-13](#)
- LIST EXPORT, [A-55](#)
- LIST FIREWALL, [A-8](#)
- LIST HOST, [A-5](#)
- LIST METRICS, [A-23](#)
- LIST PLUGIN FOR SECURED TARGET TYPE, [A-60](#)
- LIST REMOTE FILESYSTEM, [A-55](#)
- LIST SAN SERVER, [A-52](#)
- LIST SECURED TARGE, [A-22](#)
- LIST SECURED TARGET TYPE, [A-22](#)
- LIST TARGET FOR SAN SERVER, [A-50](#)
- LIST TRAIL FOR SECURED TARGET, [A-34](#)
- POWEROFF FIREWALL, [A-9](#)
- QUIT, [A-65](#)
- REBOOT FIREWALL, [A-9](#)
- REGISTER FIREWALL, [A-7](#)
- REGISTER HOST, [A-2](#)
- REGISTER SAN SERVER, [A-48](#)
- REGISTER SECURED TARGET, [A-17](#)
- REGISTER SMTP SERVER, [A-36](#)
- REVOKE ACCESS, [A-46](#)
- REVOKE ADMIN, [A-46](#)
- REVOKE SUPERADMIN, [A-45](#)
- SHOW CERTIFICATE, [A-58](#)
- SHOW ISCSI INITIATOR DETAILS FOR SERVER, [A-52](#)
- SHOW STATUS FOR FIREWALL, [A-11](#)
- SHOW STATUS OF REMOTE FILESYSTEM, [A-56](#)
- START COLLECTION FOR SECURED TARGET, [A-26](#)
- START ENFORCEMENT POINT, [A-14](#)
- STOP COLLECTION FOR SECURED TARGET, [A-30](#)
- STOP ENFORCEMENT POINT, [A-14](#)
- SWAP RESILIENT PAIR, [A-10](#)
- TEST SMTP SERVER, [A-41](#)
- UNDEPLOY PLUGIN, [A-61](#)
- UPLOAD OR DELETE WALLET FILE, [A-21](#)

AVCLI utility

- about, [14-32](#)
- downloading, [14-33](#)
- finding version of, [14-37](#)
- help information, [14-37](#)
- invoking, [14-33](#)
- invoking, with stored credentials, [14-35](#)

AVCLI utility (*continued*)

- Java_Home environment variable, [14-33](#), [14-34](#)
- log files location, [14-37](#)
- logging levels, setting, [14-37](#)
- running scripts, [14-36](#)
- stored credentials, using, [14-34](#)

BBackup/Restore, [14-14](#)

- about restoring Audit Vault Server, [14-23](#)
- backup up Audit Vault Server, [14-20](#)
- configuring the backup utility, [14-16](#)
- configuring backup utility for restore, [14-24](#)
- high availability configuration, [14-14](#)
- prerequisites to restore, [14-23](#)
- repository encryption, [14-14](#)
- required space, [14-16](#)
- restoring Audit Vault Server, [14-24](#)
- validating the backup, [14-21](#)

Big Data Appliance, as secured target, [1-3](#), [B-1](#)

BIG-IP ASM (Application Security Manager)

- benefits of integration with Oracle Database Firewall, [9-1](#)
- integration with Database Firewall, [9-1](#)

blocking

- Database Firewall inline mode, enabling bridge, [4-10](#)
- DPE mode in enforcement point, [6-20](#)
- IPv6 traffic, [2-4](#)

bridge IP addresses

- in Database Firewall, [4-10](#)
- subnet restriction for DPE mode, [4-10](#)

CCDB, registering secured target, [6-3](#)

certificate

- Audit Vault Server, [14-4](#)
- supplying to Database Firewall, [4-6](#)

certificate renewal

- Audit Vault Server, [2-12](#)
- Database Firewall, [2-16](#)

certificate warning

- Audit Vault Server, changing UI certificate, [3-2](#)
- Database Firewall, changing UI certificate, [4-2](#)

change IP address

- Database Firewall, [4-7](#)

Changing

- IP Address On A Secondary Network Interface Card, [H-14](#)

CLEAR LOG command, [A-63](#)

Client IP Addresses, and TCP invited nodes, [2-5](#)
 client program name
 security considerations, [2-5](#)
 client-side security, [2-5](#)
 COLLECTING trail status, [6-12](#)
 collection attributes
 about, [B-38](#)
 Active Directory, not required, [B-38](#)
 IBM DB2, [B-41](#)
 Linux, not required, [B-38](#)
 MySQL, [B-41](#)
 Oracle ACFS, [B-41](#)
 Oracle Database, [B-38](#)
 Solaris, not required, [B-38](#)
 SQL Server, not required, [B-38](#)
 Sybase ASE, not required, [B-38](#)
 Windows, not required, [B-38](#)
 collection plug-ins
 deploying with AVCLI command, [A-59](#)
 finding list of, [A-60](#)
 undeploying, [A-61](#)
 command line utility
 downloading AVCLI, [14-33](#)
 configuration
 audit trails, [6-9](#)
 Database Firewall
 about, [4-1](#)
 database interrogation, [6-25](#)
 enforcement points, [6-21](#)
 F5 BIG-IP Application Security Manager
 (BIG-IP ASM), [9-4](#)
 high availability
 Database Firewall, [8-10](#)
 secured targets
 about, [6-1](#)
 registering, [6-2](#)
 understanding workflow, [1-6](#)
 configuring high availability for Database Firewall
 in proxy mode
 through client configuration, [8-12](#)
 through DNS setup, [8-14](#)
 CONNECT command, [A-62](#)
 connect strings (for Secured Target Location
 field), [B-36](#)
 connections, maintaining for database clients,
 [6-22](#)
 console
 filtering and sorting lists, [1-12](#)
 reset view, [1-12](#)
 console certificate
 Audit Vault Server, [3-2](#)
 CREATE ENFORCEMENT POINT command,
 [A-12](#)
 CREATE RESILIENT PAIR command, [A-9](#)
 Custom Collector Development, [2-6](#)

D

DAM mode, [8-1](#)
 enforcement point monitoring mode, [6-20](#)
 with SQL blocking firewall policy, [6-21](#)
 Data Encryption
 starting, [14-10](#)
 data files, purging after retrieve, [14-8](#)
 data retention policies
 about, [3-12](#)
 creating, [3-17](#)
 data security, [2-1](#)
 database clients
 connecting through proxy Database Firewall,
 [4-11](#)
 database connections
 and Database Firewall, [2-4](#)
 Database Firewall
 adding Database Firewall to Audit Vault
 Server, [3-20](#)
 certificate renewal, [2-16](#)
 certificate rotation, [2-16](#)
 certificate warning, UI, [4-2](#)
 change IP address, [4-7](#)
 configuration, [4-1](#)
 Audit Vault Server certificate and IP
 address, [4-6](#)
 network services, [4-4](#)
 network settings, [4-3](#)
 proxy, [4-11](#)
 traffic sources, [4-9](#)
 diagnostics, [4-12](#)
 high availability, configuring, [8-10](#)
 integration with F5 BIG-IP Application
 Security Manager (BIG-IP ASM), [9-1](#)
 requirements, [9-4](#)
 logging in to UI, [1-14](#)
 network placement, [4-8](#)
 network services configuration, [4-4](#)
 network settings, changing, [4-3](#)
 network traffic, capturing to file, [14-39](#)
 non-TCP-based connections, [2-4](#)
 planning configuration, [1-8](#)
 ports
 for external network access, [D-4](#)
 for firewall services, [D-2](#)
 required to be open, [D-1](#)
 proxy
 configuration, [4-11](#)
 database client connections, [4-11](#)
 public key, [6-31](#)
 removing from Audit Vault Server, [14-40](#)
 restart, power off, [14-40](#)
 SNMP access, [4-4](#)
 SSH access, [4-4](#)

Database Firewall (*continued*)

- status
 - viewing, [4-12](#)
- traffic sources, configuring, [4-9](#)
- Web access, [4-4](#)

database interrogation, [B-2–B-4](#)

- about, [6-25](#)
- configuring for Microsoft SQL Server databases, [6-26](#)
- configuring for Oracle databases with Network Encryption, [6-25](#)
- configuring for Sybase SQL Anywhere databases, [6-26](#)
- disabling, [6-28](#)
- enabling, [6-27](#)
- enforcement point setting, [6-22](#)
- Sybase SQL Anywhere, installing ODBC driver for Linux, [6-26](#)

database response monitoring

- about, [6-32](#)
- enabling, [6-33](#)
- enforcement point setting, [6-22](#)

databases supported, [1-3](#)

date and time

- setting
 - in Audit Vault Server, [3-3](#)
 - in Database Firewall, [4-5](#)
- timestamps in reports, [3-3](#)

DB2

- See IBM DB2

DEACTIVATE HOST command, [A-6](#)

debugging

- Audit Vault Agent, [5-11](#), [14-5](#)
- AVCLI debug log level, setting, [14-37](#)
- Java framework (Jfwklog) LOGLEVEL, [A-56](#)
- Syslog, generating debug messages, [3-8](#)

delete target from a group, [A-24](#)

delete target from a target group, [A-25](#)

deleting hosts, [5-16](#)

DEPLOY PLUGIN command, [A-59](#)

developers, downloading SDK, [14-38](#)

diagnostic logs

- clearing, [14-5](#)
- clearing with AVCLI, [A-63](#)

diagnostics

- Audit Vault Server detailed diagnostics, [14-3](#)
- Audit Vault Server diagnostic checks, [14-2](#)
- Database Firewall, [4-12](#)

DIRECTORY audit trail

- about, [B-18](#)

directory mask

- trail location for DIRECTORY trail type, [6-11](#), [B-42](#)

Disabling

- Secondary Network Interface, [H-14](#)

disk groups

- about repository, [15-6](#)

disk space

- additional for SMB and scp archive data transfer, [3-12](#)
- monitoring archive log space, [14-29](#)

dispatcher service, security considerations, [2-4](#)

DNS servers

- configuring for Database Firewall, [4-4](#)

documentation, AVDF, downloading latest, [1-1](#)

DOWNLOAD LOG FILE command, [A-59](#)

DPE mode

- and spoofing detection rules, [6-21](#)
- bridge IP addresses, [4-10](#)
- connections, switching from DAM mode, [6-22](#)
- enforcement point monitoring mode, [6-20](#)
- traffic disruption on time synchronization, [4-5](#)

DROP ENFORCEMENT POINT command, [A-13](#)

DROP FIREWALL command, [A-8](#)

DROP HOST command, [A-5](#)

DROP REMOTE FILESYSTEM command, [A-55](#)

DROP RESILIENT PAIR command, [A-10](#)

DROP SAN SERVER command, [A-50](#)

DROP SECURED TARGET command, [A-24](#)

DROP SMTP SERVER command, [A-43](#)

DROP TRAIL FOR SECURED TARGET command, [A-35](#)

E

email notifications

- about configuring service, [3-10](#)
- altering SMTP configuration, [A-38](#)
- configuring (in UI), [3-11](#)
- disabling SMTP configuration, [A-39](#)
- enabling SMTP configuration, [A-39](#)
- finding SMTP configuration, [A-42](#)
- registering for, [A-38](#)
- registering SMTP service, [A-36](#)
- removing configuration for secure server, [A-41](#)
- time stamp shown in, [3-3](#)
- unregistering SMTP service, [A-43](#)

Enable NFS

- Secondary Network Interface Cards, [H-4](#)

Enable SPA

- Secondary Network Interface Cards For Audit Vault Server, [H-5](#)

Enabling

- Secondary Network Interface, [H-2](#)

Enabling Agent To Operate In High Availability Environment

- Secondary Network Interface card for Audit Vault Server, [H-12](#)

Enabling SSH
 Secondary Network Interface for Audit Vault Server, [H-5](#)

encryption
 AVCLI commands, [A-43](#)
 Network Encryption, [6-32](#)
 network encryption, handling, [2-3](#)
 Oracle Databases, configuration for handling, [6-29](#)
 providing public key to encrypted Oracle Database, [6-31](#)
 security guidelines, [2-3](#)
 show status, AVCLI command, [A-44](#)

enforcement points
 configuring, [6-20](#), [6-21](#)
 database interrogation setting, [6-22](#)
 database response setting, [6-22](#)
 definition, [6-20](#)
 deleting, [6-23](#)
 DPE mode and IP spoofing, [6-21](#)
 Maintain Existing Connections setting, [6-22](#)
 modifying, [6-22](#)
 port number used, [6-24](#)
 starting and stopping, [6-23](#)
 status, [6-21](#)
 status values, defined, [6-23](#)
 status, viewing, [6-23](#)

Enterprise Manager, Audit Vault and Database Firewall Plug-in for, [1-16](#)

entitlement auditing, [B-2–B-4](#)

EVENT LOG audit trail, [B-20](#)

Event Repository Encryption, [14-9](#)
 wallet, [14-10](#)

exiting AVCLI, [A-65](#)

expired audit records, archiving, [6-13](#)

external
 network dependencies, [2-2](#)

F

F5 BIG-IP Application Security Manager (BIG-IP ASM)
 about integration, [9-1](#)

F5 BIG-IP Application Security Manager (BIG-IP ASM))
 configuration requirements, [9-4](#)
 configuring with Database Firewall, [9-4](#)
 creating logging profile, [9-5](#)
 custom iRule, [9-9](#)
 how integration works, [9-3](#)
 iRules syslog messages, [9-9](#)
 policy settings, [9-7](#)
 system requirements for integration, [9-1](#)
 transmitting iRule syslog messages, [9-10](#)

F5 BIG-IP Application Security Manager)
 sample iRule, [9-7](#)

failover
 Audit Vault Server, [8-8](#)
 disabling/enabling, [8-9](#)
 manual, [8-9](#)

filesystem
 additional space for SMB and scp archive data transfer, [3-12](#)

filtering, lists in Audit Vault Server console, [1-12](#)

firewall policies, login and logout, [6-34](#)

flash recovery area, monitoring in Audit Vault Server, [14-30](#)

formatting, lists in Audit Vault Server console, [1-12](#)

G

GRANT ACCESS command, [A-45](#)

GRANT ADMIN command, [A-46](#)

GRANT SUPERADMIN command, [A-44](#)

granting access privileges, [A-45](#)

granting ADMIN privileges, [A-46](#)

granting super admin privileges, [A-44](#)

groups
 access rights
 controlling by group, [13-7](#)
 controlling by user, [13-7](#)
 creating secured target groups, [6-6](#)

guidelines, general security, [2-2](#)

H

help information about AVCLI, [A-63](#)

high availability
 about resilient pairs, [8-1](#)
 backup and restore impact on, [14-14](#)
 backup encryption, [14-14](#)
 for Audit Vault Server, [8-2](#)
 for Database Firewall, [8-10](#)
 peer system IP/certificate, [8-6](#)
 SAN repository, [15-6](#)
 status, checking, [8-6](#)

host monitor
 enforcement point for, [7-7](#)

host monitor requirements, [7-2](#)

host monitors, [7-2](#)
 about, [7-1](#)
 authentication, using, [7-11](#)
 checking status of, [7-10](#)
 deploying on Unix, [7-6](#)
 deploying on Windows, [7-3](#)
 installing, [7-2](#)
 uninstalling (Unix hosts only), [7-10](#)
 updating, Linux only, [7-11](#)

hosts

- AVCLI commands used for, [A-2](#)
- AVCLI User Commands, [A-65](#)
- changing names, [5-3](#)
- deleting from Audit Vault Server, [5-16](#)
- registering
 - procedure, [5-2](#)
 - registering, about, [5-1](#)

hybrid cloud

- deployment, [12-1](#)
- pre-requisites, [12-1](#)

hybrid cloud, deployment, [12-1](#)

I

IBM DB2,

- audit trail location, [B-10](#)
- collection attributes, [B-41](#)
- converting binary audit files to ASCII format, [6-16](#)
- starting audit trail, prerequisite ASCII conversion, [6-10](#)
- supported versions, [B-3](#)
- user account script, [B-30](#)

IDLE trail status, [6-12](#)

In-Memory usage

- monitoring, [14-28](#)

initialization parameters

- REDO log
 - audit secured target release 10.2, [C-9](#), [C-13](#)
 - audit secured target release 11.2, [C-2](#)

installation, security guidelines, [2-1](#)

integrations

- with ArcSight SIEM, [10-2](#)
- with F5 BIG-IP Application Security Manager (BIG-IP ASM), [9-1](#)
- with Oracle Audit Vault and Database Firewall, about, [1-4](#)

Interface Masters Niagara Server adapter card, [4-12](#)

IP Address On A Secondary Network Interface Card

- change, [H-14](#)

IP addresses

- and spoofing detection in DPE mode, [6-21](#)
- Audit Vault Server
 - changing, reboot required, [3-5](#)
 - subnet restrictions for proxy interface, [4-11](#)

IPv6

- connections not supported, [2-4](#)
- traffic blocked, [2-4](#)

iRule syslog messages

- BIG-IP ASM command, [9-10](#)

J

Java framework, logging levels, debugging, [A-56](#)

Java SE, Audit Vault Agent requires, [5-5](#)

jobs, monitoring, [14-31](#)

K

key, for activating agent, [5-6](#)

keyboards

- changing layout, [14-6](#)
- settings, [3-3](#)

keystore password, changing, [14-9](#)

L

link properties

- network setting
 - in Audit Vault Server, [3-5](#)
 - in Database Firewall, [4-4](#)

Linux

- audit trail location, [B-14](#), [B-15](#)
- user/group access required for audit trail, [B-13](#), [B-14](#)

LIST ADDRESS FOR SECURED TARGET

- command, [A-22](#)

LIST ATTRIBUTE FOR SECURED TARGET

- command, [A-23](#)

LIST ATTRIBUTE OF SMTP SERVER command, [A-42](#)

LIST DISK command, [A-50](#)

LIST DISKGROUP command, [A-51](#)

LIST ENFORCEMENT POINT command, [A-13](#)

LIST EXPORT command, [A-55](#)

LIST FIREWALL command, [A-8](#)

LIST HOST command, [A-5](#)

LIST METRICS command, [A-23](#)

LIST PLUGIN FOR SECURED TARGET TYPE

- command, [A-60](#)

LIST REMOTE FILESYSTEM command, [A-55](#)

LIST SAN SERVER command, [A-52](#)

LIST SECURED TARGET command, [A-22](#)

LIST SECURED TARGET TYPE command, [A-22](#)

LIST TARGET FOR SAN SERVER command, [A-50](#)

LIST TRAIL FOR SECURED TARGET

- command, [A-34](#)

lists, finding objects in Audit Vault Server console, [1-12](#)

locked user accounts

- unlocking, [13-4](#)

log files

- Audit Vault Agent, location, [5-11](#)
- AVCLI, location, [14-37](#)
- clearing, [14-5](#)

log files (*continued*)
 Java framework, location, [A-56](#)
 system, location, [A-56](#)
 traffic logs, collected, [8-1](#)

log in
 to Audit Vault Server, [1-11](#)

logging in
 to Database Firewall, [1-14](#)

logging levels
 Audit Vault Agent, setting, [5-11](#)
 Java framework, [A-56](#)
 setting, changing for all components, [14-5](#)
 specifying for AVCLI utility, [14-37](#)

login/logout policies, [6-34](#)

M

MAC addresses, spoofing detection and DPE
 mode, [6-21](#)

Maintain Existing Connections enforcement point
 setting, [6-22](#)

Maintenance Job
 Scheduling, [14-31](#)

Management Interfaces For Audit Vault Server
 features, [H-15](#)

messages
 Audit Vault, [E-1](#)
 Database Firewall, [E-40](#)

metrics of secured targets, [A-23](#)

Micro Focus Security ArcSight Security
 Information Event Management (SIEM)
 defined, [1-4](#)

Microsoft Active Directory,
 audit trail location, [B-16](#)
 supported versions, [B-4](#)

Microsoft SQL Server,
 audit trail location, [B-7](#)
 database interrogation
 configuring, [6-25](#)
 registering, [B-35](#)
 trace files, preventing from being deleted by
 accident, [B-35](#)
 user account script, [B-27](#)

Microsoft Windows,
 audit trail location, [B-15](#)
 file sharing
 archiving transfer, recommended port,
[3-13](#)
 host monitors, deploying on, [7-3](#)
 secured target user, administrative
 permissions, [6-9](#)
 services, registering AV Agent as, [5-8](#)
 supported versions, [B-4](#)

monitoring
 Audit Vault Server detailed diagnostics, [14-3](#)

monitoring (*continued*)
 Audit Vault Server diagnostic checks, [14-2](#)
 Database Firewall diagnostics, [4-12](#)

monitoring mode
 and SQL blocking, [6-21](#)
 enforcement point setting, [6-20](#)

Months Archived field, [3-17](#)

Months Online field, [3-17](#)

Multiple
 Network Interface Cards, [H-1](#)

Multiple Network Interface Cards, [H-1](#)

MySQL
 adding audit trail, prerequisite XML
 conversion, [6-10](#)
 collection attributes, [B-41](#)
 supported versions, [B-3](#)
 trail location, [6-14](#), [A-29](#), [A-33](#), [B-11](#), [B-43](#)
 user account script, [B-31](#)
 XML transformation utility, [6-14](#)

N

NETWORK audit trail, [B-20](#)

Network Encryption,
 configuring database interrogation to handle,
[6-29](#)
 decrypting in Database Firewall, [6-25](#)
 native encryption required, [6-32](#)
 providing public key to encrypted Oracle
 Database, [6-31](#)

network mask, Database Firewall network
 settings, [4-3](#)

network services
 configuring for Database Firewall, [4-4](#)

network traffic, capturing to file in Database
 Firewall, [14-39](#)

NFS filesystem
 archiving transfer method, [3-13](#)

AVCLI commands
 REGISTER REMOTE FILESYSTEM,
[A-53](#)
 REGISTER REMOTE FILESYSTEM
 command, [A-53](#)
 registering with the Audit Vault Server, [A-53](#)

non-SQL protocol access, [2-4](#)

non-TCP-based connections, and Database
 Firewall, [2-4](#)

O

ODBC driver
 required for SQL Anywhere database
 interrogation, [6-26](#)

opening port
 DBCS, [12-3](#)

- operating systems supported, [1-3](#)
 - Oracle ACFS,
 - audit trail location, [B-16](#), [B-17](#)
 - collection attributes, [B-41](#)
 - supported versions, [B-4](#)
 - Oracle Advanced Security
 - See Network Encryption
 - Oracle database
 - decrypting Network Encryption traffic, [6-25](#)
 - enabling auditing, [6-8](#)
 - Oracle Database
 - 12c, PDB/CDB and secured targets, [6-3](#)
 - audit trail location, [B-6](#)
 - collection attributes, [B-38](#)
 - decrypting Network Encryption traffic, [6-25](#)
 - In-Memory
 - about, [14-26](#)
 - disabling, [14-28](#)
 - enabling, [14-27](#)
 - purging audit trails, [B-33](#)
 - REDO logs, audit data collection reference, [C-1](#)
 - supported versions, [B-2](#)
 - user account script, [B-22](#)
 - using Network Encryption, configuration for handling, [6-29](#)
 - Oracle RAC
 - secured target location, registering, [6-3](#)
 - Oracle shared server, security considerations, [2-4](#)
 - OS username, security considerations, [2-5](#)
- ## P
-
- passwords
 - changing for Audit Vault Server administrator, [13-9](#)
 - changing for Database Firewall administrator, [13-9](#)
 - expiry dates, [13-4](#)
 - requirements, [13-8](#)
 - PDB, registering secured target, [6-3](#)
 - peer system IP/certificate, high availability, [8-6](#)
 - platforms supported, [1-1](#), [B-2](#)
 - for audit trail types, [B-17](#)
 - latest matrix, [5-5](#)
 - plug-ins
 - about, [5-13](#), [B-1](#)
 - deploy and activate procedure, [5-14](#)
 - enabling auditing, [5-14](#)
 - SDK for developing, [14-38](#)
 - un-deploying, [5-15](#)
 - policies
 - archiving, [3-12](#)
 - login and logout policies, [6-34](#)
 - ports
 - archiving
 - defining archiving locations, [3-13](#)
 - transfer method
 - scp, [3-13](#)
 - enforcement point, finding, [6-24](#)
 - for Audit Vault Server external network access, [D-3](#)
 - for Audit Vault Server services, [D-2](#)
 - for Database Firewall external network access, [D-4](#)
 - for internal TCP communication, [D-5](#)
 - recommended for archiving using Windows file sharing transfer, [3-13](#)
 - required for Database Firewall deployment, [D-1](#)
 - scp
 - See Secure Copy
 - Secure Copy
 - archive datafile transfer, [3-13](#)
 - used by AVDF, [D-1](#)
 - power off
 - Audit Vault Server, [14-6](#)
 - Database Firewall, [14-40](#)
 - POWEROFF FIREWALL command, [A-9](#)
 - proxy
 - and database client connections, [4-11](#)
 - configuring Database Firewall as, [4-11](#)
 - IP address, subnet restrictions, [4-11](#)
 - public key
 - Audit Vault Server, [14-4](#)
 - Database Firewall, [6-31](#)
 - providing to encrypted Oracle Database, [6-31](#)
 - purging audit trails
 - IBM DB2 audit files, [6-16](#)
 - Oracle Database, [B-33](#)
 - source database in Audit Vault environment, [B-33](#)
- ## Q
-
- QUIT command, [A-65](#)
 - quitting AVCLI, [A-65](#)
 - quotation marks
 - invalid in user names, [6-9](#), [13-3](#)
- ## R
-
- reboot
 - Audit Vault Server, [14-6](#)
 - REBOOT FIREWALL command, [A-9](#)
 - RECOVERING trail status, [6-12](#)
 - REDO logs
 - audit data collection reference, [C-1](#)

REGISTER FIREWALL command, [A-7](#)
 REGISTER HOST command, [A-2](#)
 REGISTER SAN SERVER command, [A-48](#)
 REGISTER SECURED TARGET command, [A-17](#)
 REGISTER SMTP SERVER command, [A-36](#)

registering

hosts

procedure, [5-2](#)

remote access, security guidelines, [2-1](#)

remote monitors

See host monitors

reports

direct database interrogation, [6-25](#)

host monitoring, [7-1](#)

time stamp shown in PDF/XLS, [3-3](#)

repository

about disk groups, [15-6](#)

adding SAN disks, [15-7](#)

dropping SAN disks, [15-8](#)

dropping SAN servers, [15-3](#)

high availability environment, [15-6](#)

registering SAN servers, [15-3](#)

Repository Page described, [15-6](#)

requirements

Audit Vault Agent, Java SE, [5-5](#)

host monitor, [7-2](#)

reset console view, [1-12](#)

resilient pairs

about, [8-1](#)

of Audit Vault Servers, [8-3](#)

restart

Database Firewall, [14-40](#)

restore, Audit Vault Server, [14-23](#)

retrieving, from archives, [14-8](#)

REVOKE ACCESS command, [A-46](#)

REVOKE ADMIN command, [A-46](#)

REVOKE SUPERADMIN command, [A-45](#)

revoking

access privileges, [13-4](#), [A-46](#)

ADMIN privileges, [A-46](#)

super admin privileges, [A-45](#)

S

SAN disks

adding to repository, [15-7](#)

dropping from repository, [15-8](#)

SAN servers

discovering targets on, [15-4](#)

dropping, [15-3](#)

logging in to targets, [15-5](#)

logging out of targets, [15-5](#)

registering, [15-3](#)

SAN storage

iSCSI initiator name, configuring, [15-2](#)

Scheduling

Maintenance Job, [14-31](#)

Scheduling Maintenance Job, [14-31](#)

scp

See Secure Copy

scripts

account privileges on secured targets

about, [B-22](#)

IBM DB2, [B-30](#)

Microsoft SQL Server, [B-27](#)

MySQL, [B-31](#)

Oracle Database, [B-22](#)

Sybase ASE, [B-25](#)

Sybase SQL Anywhere, [B-26](#)

running AVCLI scripts, [14-36](#)

SDK, downloading for plug-in development, [14-38](#)

Secondary Network Interface

Applying Static Routing Rules, [H-7](#)

disable, [H-14](#)

enable, [H-2](#)

Enable SSH, [H-5](#)

Enabling Agent To Operate In High Availability Environment, [H-12](#)

Secondary Network Interface Card

Enable Agent Connectivity, [H-8](#)

Secondary Network Interface Card for Audit Vault Server, [H-8](#)

Secondary Network Interface Cards, [H-4](#), [H-5](#)

Secondary Network Interfaces For Audit Vault Server

features, [H-15](#)

Secure Copy, [3-13](#)

archive datafile transfer, [3-12](#)

Secure Sockets Layer (SSL)

SMTP configuration, [A-40](#)

Secured Target Location field, [6-3](#), [B-36](#)

secured targets

about configuring, [6-1](#)

access rights

controlling by secured target or group, [13-7](#)

controlling by user, [13-7](#)

altering, [A-19](#)

attributes

listing with AVCLI, [A-23](#)

Big Data Appliance, [1-3](#), [B-1](#)

collection attributes

about, [B-38](#)

Active Directory, not required, [B-38](#)

IBM DB2, [B-41](#)

Linux, not required, [B-38](#)

MySQL, [B-41](#)

Oracle ACFS, [B-41](#)

Oracle Database, [B-38](#)

- secured targets (*continued*)
 - collection attributes (*continued*)
 - Solaris, not required, [B-38](#)
 - SQL Server, not required, [B-38](#)
 - Sybase ASE, not required, [B-38](#)
 - Windows, not required, [B-38](#)
 - commands used for, [A-16](#)
 - configuring TCPS/SSL connections, [6-34](#)
 - defined, [1-3](#)
 - dropping, [A-24](#)
 - finding attributes, [A-23](#)
 - finding metrics, [A-23](#)
 - groups, creating, [6-6](#)
 - hosts, registering, [5-1](#)
 - listing address, [A-22](#)
 - Microsoft Windows, administrative permissions, [6-9](#)
 - name change, and reports, [6-5](#)
 - nondatabase sources, about, [1-3](#)
 - Oracle 12c PDB/CDB, [6-3](#)
 - planning audit trail configuration, [1-9](#)
 - registering, [6-2](#), [A-17](#)
 - removing from Audit Vault Server
 - about, [6-5](#)
 - service name, [6-3](#)
 - SID, [6-3](#)
 - SPA (stored procedure auditing)
 - configuring, [6-24](#)
 - supported types, [1-3](#)
 - upload or delete, [A-21](#)
- security
 - and installing, [2-1](#)
 - Audit Vault and Database Firewall account guidelines, [13-3](#)
 - client-side context information, [2-5](#)
 - Custom Collector Development, [2-6](#)
 - database access handling, [2-4](#)
 - encryption, [2-3](#)
 - general recommendations, [2-2](#)
 - guidelines, [2-1](#)
 - multiple databases on shared listener, [2-5](#)
 - Oracle shared server configuration, [2-4](#)
 - recommendations, [2-2](#)
 - TCP invited nodes, [2-5](#)
- Security Technical Implementation Guides (STIG)-based advise on implementation, [F-1](#)
- Security Technical Implementation Guides (STIG)user account rules, [13-2](#)
- Service Name field, [6-3](#), [A-20](#)
- settings, keyboard, [3-3](#)
- shared listener, security considerations, [2-5](#)
- SHOW CERTIFICATE command, [A-58](#)
- SHOW ISCSI INITIATOR DETAILS FOR SERVER command, [A-52](#)
- SHOW STATUS FOR FIREWALL command, [A-11](#)
- SHOW STATUS OF REMOTE FILESYSTEM command, [A-56](#)
- SID, [6-3](#)
- SID field, [6-3](#), [A-20](#)
- SMB
 - See Windows File Sharing
- SMTP
 - configuring connection (UI), [3-10](#)
 - enabling (AVCLI), [A-39](#)
- SNMP access
 - Audit Vault Server
 - configuring
 - services, [3-7](#)
 - Web access, [3-7](#)
 - configuring for Audit Vault Server, [3-7](#)
 - configuring for Database Firewall, [4-4](#)
 - DNS servers
 - configuring for Audit Vault Server, [3-7](#)
 - network services
 - configuring for Audit Vault Server, [3-7](#)
 - system services
 - configuring for Audit Vault Server, [3-7](#)
 - Web access
 - configuring for Audit Vault Server, [3-7](#)
- Solaris
 - audit trail location, [B-12](#)
 - audit trail location format, [B-12](#), [B-43](#)
 - audit trail location format (avcli), [A-29](#)
 - supported versions, [B-3](#)
- sorting lists in Audit Vault Server console, [1-12](#)
- SPA, configuring, [6-24](#)
- spoofing detection
 - MAC and IP address, and DPE mode, [6-21](#)
- SQL Anywhere
 - See Sybase SQL Anywhere
- SQL Server
 - See Microsoft SQL Server
- SQL, types not captured by Database Firewall, [2-3](#)
- SQL*Net
 - and Sybase ASE, required on Agent host, [5-6](#)
- SSH access
 - configuring for Audit Vault Server, [3-7](#)
 - configuring for Database Firewall, [4-4](#)
- SSL connections
 - configuring secured targets for, [6-34](#)
- START COLLECTION FOR SECURED TARGET command, [A-26](#)
- Start data encryption
 - process, [14-10](#)
- START ENFORCEMENT POINT command, [A-14](#)

- status
 - audit trails, checking, [6-12](#)
 - Audit Vault Server
 - checking, [14-2](#)
 - Database Firewall, viewing for, [4-12](#)
 - high availability, [8-6](#)
 - host monitor, checking, [7-10](#)
 - jobs in Audit Vault Server, [14-31](#)
 - STOP COLLECTION FOR SECURED TARGET
 - command, [A-30](#)
 - STOP ENFORCEMENT POINT command, [A-14](#)
 - STOPPED trail status, [6-12](#)
 - stored credentials
 - AVCLI, configuring, [14-34](#)
 - stored procedure auditing, [B-2–B-4](#)
 - configuring, [6-24](#)
 - stored procedure auditing (SPA)
 - configuring, [6-24](#)
 - subnet
 - bridge IP address restriction, [4-10](#)
 - Database Firewall network settings, default gateway, [4-3](#)
 - Database Firewall network settings, network mask, [4-3](#)
 - for proxy IP address, [4-11](#)
 - ports
 - proxy, [4-11](#)
 - proxy
 - port numbers, [4-11](#)
 - system settings, default gateway, [3-5](#)
 - system settings, network mask, [3-5](#)
 - sudo access configuration, [13-5](#)
 - super administrators
 - access rights, [13-1](#)
 - defined, [1-6](#)
 - supported operating systems, [1-3](#)
 - supported platforms, [1-1](#), [B-2](#)
 - for audit trail types, [B-17](#)
 - latest matrix, [5-5](#)
 - supported secured targets, [1-3](#)
 - Suspended, enforcement point status, [6-23](#)
 - SWAP RESILIENT PAIR command, [A-10](#)
 - Sybase ASE
 - audit trail location, [B-8](#)
 - SQL*Net on Agent host, requirement, [5-6](#)
 - supported versions, [B-3](#)
 - user account script, [B-25](#)
 - Sybase SQL Anywhere,
 - audit trail location, [B-9](#)
 - database interrogation
 - configuring, [6-25](#)
 - ODBC driver required, [6-26](#)
 - supported versions, [B-3](#)
 - user account script, [B-26](#)
 - synchronizing time
 - traffic disruption in DPE mode, [4-5](#)
 - SYSAUX tablespace
 - monitoring in Audit Vault Server, [14-29](#)
 - syslog
 - Audit Vault and Database Firewall alert
 - forwarding, format, [3-8](#)
 - debug messages, generating, [3-8](#)
 - forward to destinations, configuring, [3-8](#)
 - IP addresses for forwarding, [3-8](#)
 - SYSLOG audit trail, [B-20](#)
 - syslog files, [B-18](#)
 - system configuration
 - understanding workflow, [1-6](#)
 - workflow
 - with Audit Vault Agent, [1-6](#)
 - with Database Firewall, [1-7](#)
 - system services
 - configuring for Database Firewall, [4-4](#)
- ## T
-
- TABLE audit trail, [B-18](#)
 - tabs, UI, described, [1-11](#)
 - target group, [A-24](#)
 - target group AVCLI commands
 - ADD TARGET, [A-24](#)
 - DELETE TARGET, [A-25](#)
 - TCP invited nodes, security considerations, [2-5](#)
 - TCPS/SSL connections
 - configuring secured targets for, [6-34](#)
 - TEST SMTP SERVER command, [A-41](#)
 - testing, Audit Vault Server operation, [3-21](#)
 - third-party products used with Oracle Audit Vault and Database Firewall, [1-4](#)
 - time synchronization, traffic disruption in DPE mode, [4-5](#)
 - Time Zone Offset field, [3-3](#)
 - timestamps, and Audit Vault Server date and time, [3-3](#)
 - trace files, Microsoft SQL Server, preventing deletion, [B-35](#)
 - traffic disruptions, and time synchronization in DPE mode, [4-5](#)
 - traffic log files, collected, [8-1](#)
 - traffic sources
 - changing in enforcement point, [6-22](#)
 - Database Firewall, configuring in, [4-9](#)
 - Trail Location field
 - directory mask for DIRECTORY trail type, [6-11](#), [B-42](#)
 - trail locations
 - supported per secured target, [B-42](#)
 - TRANSACTION LOG
 - audit trail, about, [B-19](#)

TRANSACTION LOG (*continued*)
 recommended settings reference, [C-1](#)
 transfer method, archiving, [3-13](#)
 Transport Layer Security (TLS)
 SMTP configuration, [A-40](#)
 troubleshooting
 Agent activation error using avcli, [G-5](#)
 Agent cannot connect to Audit Vault Server,
[G-6](#)
 Audit Vault Agent
 access denied while installing as
 Windows service, [G-8](#)
 error on startup, [G-9](#)
 java -jar agent.jar failed, [G-7](#)
 unable to start through services applet,
[G-9](#)
 unable to uninstall Windows service, [G-8](#)
 avcli agent activation error, [G-5](#)
 cannot collect Oracle Database trail, [G-6](#)
 Database Firewall, partial traffic only, [G-4](#)
 host monitor fails, [G-6](#)
 Host Monitor, setup error, [G-10](#)
 Oracle Database alerts not triggered, [G-10](#)
 RPM upgrade failed, [G-5](#)

U

UI
 Audit Vault Server, tabs described, [1-11](#)
 UI certificates
 Audit Vault Server, changing, [3-2](#)
 Database Firewall, changing, [4-2](#)
 UIDatabase Firewall, about UIDatabase Firewall,
 about, [1-15](#)
 UNDEPLOY PLUGIN command, [A-61](#)
 Unix
 deploying host monitor on, [7-6](#)
 unlock user account, [13-4](#), [A-47](#)
 UNREACHABLE trail status, [6-12](#)
 Unreachable, enforcement point status, [6-23](#)
 Update Certificate button
 certificate
 fetching from upgraded firewall, [14-40](#)
 Validation Failed, [14-40](#)
 Database Firewall
 certificate validation failed, [14-40](#)
 updating
 host monitors, Linux only, [7-11](#)

updating (*continued*)
 upload or delete wallet file command, [A-21](#)
 user accounts
 about managing, [13-1](#)
 Audit Vault Agent deployment, OS user, [5-5](#)
 changing type, [13-4](#)
 creating, [13-3](#)
 deleting, [13-5](#)
 planning, [1-10](#)
 status and password expiry, [13-4](#)
 sudo access, configuring, [13-5](#)
 unlock, [13-4](#)
 unlock (AVCLI), [A-47](#)
 User Content To System Configuration Files
 add, [I-1](#)
 users
 logging in to the Audit Vault Server console,
[1-11](#)
 user names with quotes invalid, [6-9](#), [13-3](#)

V

version number of AVCLI, finding, [A-64](#)

W

wallet
 event repository encryption, backing up,
[14-10](#)
 Web access
 configuring for Database Firewall, [4-4](#)
 Web Application Firewall (WAF)
 defined, [1-4](#)
 reports in F5 BIG-IP Application Security
 Manager (BIG-IP ASM), [9-10](#)
 Windows
 See Microsoft Windows
 Windows Event Log, and DIRECTORY audit trail,
[B-18](#)
 Windows File Sharing, [3-13](#)
 archive datafile transfer, [3-12](#), [3-13](#)
 Windows service
 Audit Vault Agent, registering as, [5-7](#)
 Audit Vault Agent, unregistering as, [5-8](#)

X

XML files, and DIRECTORY audit trail, [B-18](#)