

Oracle® Audit Vault And Database Firewall

Release Notes

Release 20

E93406-29

March 2026

Release Notes

Release Notes contain important information about Oracle Audit Vault and Database Firewall Release 20.

New Features In Oracle Audit Vault and Database Firewall Release 20

Learn about new features and enhancements in Oracle AVDF 20.

New features in Oracle AVDF Release 20.17

In AVDF 20.17, we have streamlined the AVDF release update (RU) process and improved its robustness by handling some of the common error cases. For the security of the deployment, it is critical to regularly apply the latest AVDF release updates.

Feature/Bug/ER:

- Custom UDP ports support for syslog connector
- Translation log collection using Golden Gate 26ai
- Transaction log collection from Microsoft SQL Server 2022
- Increased robustness of the auto archival process based on the configured ILM policy

Bug fixes, platform updates, and security improvements:

- Security and stability fixes from Oracle Database Server Release Update 19.30 for the underlying AVDF repository. There are two CVEs addressed since AVDF RU 20.16 from the [January 2026](#) Critical Patch Updates.
- Security and stability fixes for the underlying components, Oracle APEX, Oracle Rest Data Services (ORDS), Oracle Java SE, Oracle Autonomous Health Framework (AHF), and Oracle GoldenGate. There are 23 CVEs addressed in these underlying components since AVDF RU 20.16 from the [January 2026](#) Critical Patch Updates.
- Security and stability fixes for the embedded Oracle Linux 8.10 operating system.

- Fixes for several customer-reported and internally discovered issues.
- Some of the critical bugs fixed in 20.17 are listed in the [Release Notes](#).

New features in Oracle AVDF Release 20.16

In AVDF 20.16, we have streamlined the AVDF release update (RU) process and improved its robustness by handling some of the common error cases. For the security of the deployment, it is critical to regularly apply the latest AVDF release updates.

Feature/Bug/ER:

Increased robustness of the auto archival process based on the configured ILM policy.

Bug fixes, platform updates, and security improvements:

- Security and stability fixes from Oracle Database Server Release Update 19.29 for the underlying AVDF repository. There are two CVEs addressed since AVDF RU 20.15 from the [Oct 2025](#) Critical Patch Updates.
- Security and stability fixes for the underlying components, Oracle APEX, Oracle Rest Data Services (ORDS), Oracle Java SE, Oracle Autonomous Health Framework (AHF), and Oracle GoldenGate. There are five CVEs addressed in these underlying components since AVDF RU 20.15 from the [Oct 2025](#) Critical Patch Updates.
- Security and stability fixes for the embedded Oracle Linux 8.10 operating system.
- Fixes for several customer-reported and internally discovered issues.
- Some of the critical bugs fixed in 20.16 are listed in the [Release Notes](#).

New features in Oracle AVDF Release 20.15

In AVDF 20.15, we have streamlined the AVDF release update (RU) process and improved its robustness by handling some of the common error cases. For the security of the deployment, it is critical to regularly apply the latest AVDF release updates.

Increased robustness of the update process

- Disable backup and restore during the update process.
- Warning message updated if UNDO tablespace is full, and additional storage is needed.

Bug fixes, platform updates, and security improvements:

- Security and stability fixes from Oracle Database Server Release Update 19.28 for the underlying AVDF repository. There are six CVEs addressed since AVDF RU 20.14 from the [July 2025](#) Critical Patch Updates.
- Security and stability fixes for the underlying components, Oracle APEX, Oracle Rest Data Services (ORDS), Oracle Java SE, Oracle Autonomous Health Framework (AHF), and Oracle GoldenGate. There are six CVEs addressed in these underlying components since AVDF RU 20.14 from the [July 2025](#) Critical Patch Updates.
- Security and stability fixes for the embedded Oracle Linux 8.10 operating system.

- Fixes for several customer-reported and internally discovered issues.
- Some of the critical bugs fixed in 20.15 are listed in the [Release Notes](#).

New features in Oracle AVDF Release 20.14

Oracle Audit Vault and Database Firewall (AVDF) continues to expand support for enterprise-class features. We have streamlined the AVDF release update (RU) process and improved its robustness by handling some of the common error cases. For the security of the deployment, it is critical to regularly apply the latest AVDF release updates.

Expanded Enterprise Support:

1. [Expanding support for tracking before/after values](#): AVDF currently collects before/after values from Oracle, Microsoft SQL Server, and MySQL databases to help customers meet compliance requirements where they need to track the change in values. However, the session information (Program name, OS username, Client host name/IP, OS terminal) is not available in the change data capture table of the Microsoft SQL Server, limiting our ability to show that. AVDF 20.14 now captures session information for before/after value changes related to customer selected tables in Microsoft SQL Server transactions.
2. [Oracle AI Database 26ai SQL Firewall log](#): Introduced in Oracle AI Database 26ai, SQL Firewall is built into the Oracle AI Database 26ai kernel to effectively address SQL injection attacks and unauthorized SQL statements. With AVDF 20.13, SQL Firewall violation events are available in the All Activity Report. In AVDF 20.14, we have now added a new SQL Firewall Violations Report.

Increased robustness of the update process:

- Ensure archive locations are mounted and accessible before starting the upgrade
- For HA mode, ensure the Audit Vault servers are properly configured:
 - Primary and standby Audit Vault servers must be in sync.
 - The standby Audit Vault server should have sufficient space in the ASM disk groups before pairing.
 - Update on the primary Audit Vault server should start only after the standby is updated.
- Improved pre-update warning messages to
 - Remove the schemas not shipped with AVDF
 - Avoid unexpected reboots during the update process.
- Diagnostic improvements for faster debugging.

Operational improvements in audit data archiving:

- Fixed insufficient space issues during the data archiving operation.
- Fixed inaccessible data file issues during data purge operation.
- Updated diagnostics for efficient debugging.

Bug fixes, platform updates, and security improvements:

- Security and stability fixes from Oracle Database Server Release Update 19.27 for the underlying AVDF repository. There are eight CVEs addressed since AVDF RU 20.13 from the two Critical Patch Updates, [April 2025](#), and [January 2025](#).
- Security and stability fixes for the underlying components, Oracle APEX, Oracle Rest Data Services (ORDS), Oracle Java SE, Oracle Autonomous Health Framework (AHF), and Oracle GoldenGate. There are sixty-two CVEs addressed in these underlying components since AVDF RU 20.13 from the 2 Critical Patch Updates, [April 2025](#), and [January 2025](#).
- Security and stability fixes for the embedded Oracle Linux 8.10 operating system.
- [Support for VMware vSphere 8.0](#) to install and run Oracle Audit Vault and Database Firewall from 20.13 onwards.
- Fixes for several customer-reported and internally discovered issues.
- Some of the critical bugs fixed in 20.14 are listed in the [Release Notes](#).

New features in Oracle AVDF Release 20.13

Oracle Audit Vault and Database Firewall (AVDF) 20.13 continues to expand support for enterprise-class features along with significant improvements in usability.

Here is what's new in the latest AVDF Release Update 13 (20.13):

Expanded Enterprise Support:

1. **[Monitor Oracle AI Database 26ai](#)**: AVDF 20.13 extends support for Oracle AI Database 26ai.
 - Support for audit collection and database firewall monitoring of Oracle AI Database 26ai.
 - When monitoring the Oracle AI Database 26ai target, you can manage and provision Oracle AI Database 26ai audit policies from AVDF.
2. **[Monitor local or bequeath connection with Host Monitor](#)**: Database Firewall host monitor is an agent-based deployment that monitors network-based SQL traffic. With AVDF 20.13, you can monitor even local connections to the database through loopback (non-Oracle and Oracle) and bequeath (Oracle), giving complete visibility of all the activities happening on the database either through the network, direct connection, or both.
3. **[Oracle AI Database 26ai SQL Firewall log](#)**: Introduced in Oracle AI Database 26ai, SQL Firewall is built into the Oracle AI Database 26ai kernel to effectively address both SQL injection attacks and compromised account issues. With AVDF 20.13, you can now collect SQL Firewall violation logs into AVDF to analyze possible threats and generate alerts based on SQL Firewall policy violations. SQL Firewall violation events are available in the **All Activity Report** of AVDF from the auditor user.
4. **[Audit AVDF application](#)**: AVDF already audits critical operating system and database-level activities performed at the AVDF appliance. AVDF now introduces a self-audit feature at the AVDF application level by monitoring the activities performed at the web console and command line interface by administrators and auditors. A new set of reports is introduced under AVDF system audit reports,

including Application, Database, and Operating System auditing. These reports will help you to view and analyze admins' and auditors' activities and meet many regulatory bodies' requirements on self-audit.

5. [AVDF integration with the latest release of Database Security Assessment Tool \(DBSAT\)](#): The latest release of DBSAT brings valuable updated checks and recommendations that come from the Oracle Best Practices, US Department of Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) for Oracle Database, and the latest CIS Benchmark V1.2. AVDF's security assessment (20.13) feature is updated with the latest release of DBSAT to provide the latest security checks and recommendations.

Usability:

1. [Global Sets in Alert Policy Conditions](#) The global set concept is already used in database firewall policies, all activity reports, and GDPR compliance reports. You can now use these global sets in alert policy conditions to create more effective alert policies. You can also filter **All Activity Reports** based on the Global Sets and use the filter to create Alert Policy conditions with a single click.
2. [Agent-less collection in High Availability configuration](#) Agent-less audit collection is a popular choice when testing use cases, doing proof of concept, or even in scenarios where the target machine is not available to install local agents. Enhancing this functionality in AVDF 20.13, the agent-less collection is now extended to work seamlessly when the AVDF Server is configured in High Availability mode.
3. [Database security assessment severity customization](#) With AVDF 20.13, the security assessment feature gives you the flexibility to change the default severity level of the security check or defer it according to your organization's requirements and set that as a baseline for the subsequent scheduled assessments.

Multi-Cloud Support:

1. [AVDF deployment in AWS](#): To extend multi-cloud support, AVDF can now be installed on AWS, giving you the option to choose your deployment. You can download AVDF 20.13 AWS-supported images from [Oracle Software Delivery Cloud](#), upload them to an AWS S3 bucket, and create working instances of AVDF on AWS.

Platform updates and security improvements, bug fixes:

- VMWare VSphere 8.0 can now be used to install and run Oracle Audit Vault and Database Firewall
- Security and stability fixes from Oracle Database Release Update 19.25 (October 2024) for the underlying AVDF repository.
- Security and stability fixes for the embedded Oracle Linux 8.9 operating system.
- Security and stability fixes for the underlying components, including Oracle APEX, Oracle Rest Data Services (ORDS), Java Runtime Environment (JRE), Oracle Clusterware, and Oracle Instant Client.
- Fixes for several customer-reported and internally discovered issues.

New features in Oracle AVDF Release 20.12

This release of Oracle Audit Vault and Database Firewall (AVDF) 20.12 primarily focused on security and stability fixes, along with a few significant usability improvements.

Here is what's new in the latest AVDF Release Update 12 (20.12):

Usability:

1. **[Discover unmonitored databases:](#)** Visibility of all the databases on your network is essential to avoid gaps in security monitoring. With AVDF 20.12's new database discovery feature, you can achieve the following use cases by performing a Nmap scan and uploading the scan results to AVDF.
 - You can quickly identify and register databases that you wish to monitor with AVDF.
 - You can also identify new databases that AVDF does not currently monitor and register them by periodically scanning and uploading the Nmap file into AVDF.With this feature, you can make sure that no database goes unmonitored.
2. **[Centralized view of enabled audit policies:](#)** In earlier versions of AVDF, you could view a list of enabled audit policies but only for a specific Oracle database target. With AVDF 20.12, you can view the audit policies enabled on all Oracle databases in a single report from the audit policies page. This report also displays container-wise audit policies of all the container databases and their corresponding pluggable databases.
3. **[Increased control over network interface device name:](#)** AVDF 20.12 introduces the ability to configure the network device name for database firewall servers from the administration console.

Security improvements, bug fixes, and platform updates:

This release update focused on fixing bugs and improving product security:

- Security and stability fixes from Oracle Database Release Update 19.23 (April 2024) for the underlying AVDF repository.
- Security and stability fixes for the embedded Oracle Linux 8.9 operating system.
- Security and stability fixes for the underlying components, including Oracle APEX, Oracle Rest Data Services (ORDS), Java Runtime Environment (JRE), Oracle Clusterware, and Oracle Instant Client.
- Fixes for several customer-reported and internally discovered issues.

In addition, the following platform updates were made:

- Audit Vault agents now support JRE 21 on the agent host machine.
- Audit Vault agents can now be installed on ARM hardware running Linux-based operating systems.

New features in Oracle AVDF Release 20.11

Oracle Audit Vault and Database Firewall (AVDF) continues to expand support for enterprise-class features along with significant improvements in usability and operations.

Here is what's new in the latest AVDF Release Update 11 (20.11):

Extended Enterprise Support:

1. **Integration with identity provider for single sign-on:** Many of you implement single sign-on (SSO) using an enterprise identity service for your applications to minimize account proliferation and authentication mechanisms. Now, with AVDF 20.11, you can integrate with identity providers (IdP) such as Azure, Active Directory Federation Services (ADFS), and Oracle Access Manager (OAM) through SAML 2.0 integration. After integrating AVDF with your IdP, AVDF console users can be authenticated by your IdP using SSO.
2. **QuickCSV audit collector:** In addition to the existing support to collect audit data from the database, network-based SQL traffic, OS, directory, Rest, JSON, XML, and custom tables, AVDF 20.11 can now collect audit logs in CSV format. We have seen that comma-separated value (CSV) is one of the most popular audit log formats used in applications, databases, and infrastructure components. With the new QuickCSV Collector in AVDF 20.11, you can easily import CSV audit files and map them to the AVDF audit schema as a one-time task. Once mapping is complete, audit data will be collected periodically from the CSV audit files like any other supported targets.
For example, you may use the QuickCSV collector to collect audit data from MariaDB, EnterpriseDB (Postgres), and other systems that create audit data in CSV. This approach helps you generate audit reports and alerts and protect and manage audit logs within the AVDF repository.
3. **Expanding support for tracking before/after values:** AVDF currently collects before/after values from Oracle and Microsoft SQL Server databases and helps customers meet compliance requirements where they need to track the value change. AVDF 20.11 now extends the same before/after value change auditing support for MySQL, helping customers meet their compliance requirements for MySQL database also.

Usability:

1. **Revamped alert UI workflow:** AVDF's alert policy creation is completely revamped in AVDF 20.11, providing an intuitive and user-friendly experience. New alert policies can be created with
 - the interactive report filters to define complex conditions
 - pre-defined templates
 - by modifying existing policies with new conditionsYou can have a quick view of all the alerts generated on the alert policy page without going away from the alert definition, improving the overall user experience of alert usability.
In addition, we made it much easier to notify the recipients of any alerts raised. Now, your auditor dashboard provides multiple actionable insights on the generated alerts.
2. **Fleet-wide security assessment drift chart:** In AVDF 20.9 and 20.10, we introduced fleet-wide security assessment and drift management, respectively. AVDF 20.11 now allows you to quickly see how the security posture of all your Oracle databases is changing by introducing the security assessment drift chart. The chart on the auditor's dashboard compares the latest assessment with the

defined baseline for all databases and quickly identifies any drift requiring attention.

3. **[Finely scoped database firewall policies and reports](#)** Until now, Database Firewall (DBFW) policies and reports were based on command groups such as DML, DDL, and DCL, and customers could not easily create policies on just a specific command. With AVDF 20.11, the command class has been expanded to commands such as DELETE, INSERT, UPDATE, DROP TABLE, etc. This enhancement helps you define narrow alert conditions and create unified reports – irrespective of whether the event data was from the audit logs or network-based SQL.
4. **[Use of global sets in all activity and GDPR reports](#)**: Until now, global sets of IP addresses, OS/DB users, sensitive objects, privileged users, and client programs have been used across Database Firewall policies, making it easier to apply the same rules. Starting in AVDF 20.11, you can now apply the same global set to filter all activity reports, including the compliance reports. For example, in GDPR compliance reports, you can use sensitive object sets to view user activity on sensitive data.

Operational Management:

1. **[Audit trail migration](#)**: Customers have requested easy ways to migrate their audit trails to different agents due to aging agent hardware or the need for improved load balancing across agents. AVDF 20.11 provides flexibility to migrate the audit trail from one agent to another or agentless configuration and vice versa without losing any audit data and restarting the agent/trail.
2. **[AVDF certificate rotation from UI](#)**: AVDF uses certificates for internal communication among various services. The current process was lengthy and only partially automated. Now, with 20.11, you can have a clear picture of the certificate validity status from the AVDF console, and you can rotate these certificates with a single click when needed.

Platform Updates and Improved Stability:

1. Security and stability fixes from Oracle Database Release Update 19.22 (Jan 2024) for the underlying AVDF repository.
2. Security and stability fixes for the embedded Oracle Linux 8.8 operating system.
3. Includes the latest security and stability fixes for the underlying Oracle and non-Oracle components, including APEX, JRE, Oracle Clusterware, Oracle Instant Client, ORDS, etc.
4. Fixed several internally discovered and customer-reported issues.

New features in Oracle AVDF Release 20.10

Oracle Audit Vault and Database Firewall (AVDF) Release Update 10 (RU10) focuses on usability improvements. We've also used this release to deliver several customer-requested enhancements. Here is what's new in RU10.

Usability:

1. **[Managing configuration drift with Database Security Posture Management](#)**: RU10 extends Database Security Posture Management (introduced in AVDF 20.9) to

identify security configuration drift. Now you can define an assessment baseline and determine deviation from that baseline by viewing security assessment drift reports. Insights from the drift reports help you focus only on the changes since the last assessment.

2. [Tracking changes to business records](#): AVDF could already track before and after values for Oracle and Microsoft SQL Server Databases. Now with AVDF 20.10, the primary value for each row change is available to track business records and values such as the user, event time, and event status. This will help you sort and filter before and after value reports with the associated primary key(s).
3. [Audit insights](#): Audit Insight feature provides a bird's-eye view of the top user activities across one or multiple databases with the option to drill down for further analysis. The audit insights dashboard now provides insights into both audit and network events. Additionally, in RU10, the summarized view of all events lets you drill down for more information.
4. [Remote and agentless audit collection for Microsoft SQL Server](#): In addition to Oracle Database, you can now collect audit data from Microsoft SQL Server in an agentless mode or a remote host without installing any agent on target machines. Agentless audit collection accelerates your AVDF deployment. For Microsoft SQL Server, this capability is available for directory audit trails for SQL audit (.sqlaudit) and extended audit events (.xel).
5. [Pre-upgrade agent checks](#): When updating from AVDF 20.9 to 20.10 or later, you can now run a pre-update check for Audit Vault Agent and Host Monitor to check issues that might cause problems with the update. For example, a pre-update agent check will verify that agent host machines have compatible operating systems and Java versions.
6. [Simplifying DBFW policy management with Global sets](#): AVDF RU9 introduced global sets of privileged user and sensitive objects across Oracle Database in database firewall (DBFW) policies. With AVDF 20.10, global sets can also include session context information, such as IP Address, OS User, Client Program, and Database User, simplifying DBFW policy management even further.
7. [Test connection during target creation](#): Now, you can test the database connection while registering Oracle Database and Microsoft SQL Server targets through the Audit Vault Server console. This helps you proactively address mistakes in the database connection information instead of carrying forward the misconfiguration at the audit trail collection level and then diagnosing issues later through the log files.
8. [System alert email notifications](#): RU9 introduced system alert capability; now, with RU10, administrators can receive email notifications for critical and high severity system alerts. For example, notifications are triggered if an audit trail goes down or becomes unreachable. AVDF 20.10 also introduces new alerts for Database Firewall certificate expiration, host monitoring, and audit collection.

Expanded Enterprise Support:

1. [Broaden audit log collection](#) support for the following platforms.
 - Microsoft SQL Server 2022 Enterprise Edition and Standard Edition
 - PostgreSQL 14 and 15
 - Red Hat Enterprise Linux (RHEL) 8 and 9 on IBM Z

2. [Transaction Log Collector using GoldenGate 21c](#) for Oracle Database (19c) and Microsoft SQL Server (2017, 2019)

Platform Updates and Improved Stability:

1. Security and stability fixes from Oracle Database Release Update 19.20 (July 2023) for the underlying AVDF repository.
2. Security and stability fixes for the embedded Oracle Linux 8.8 operating system.
3. Includes the latest security and stability fixes for the underlying Oracle and Non-Oracle components, including APEX, JRE, Oracle Clusterware, Oracle Instant Client, Oracle REST Data Services, and so on.
4. Fixed several internally discovered and customer-reported issues.

New features in Oracle AVDF Release 20.9

Oracle Audit Vault and Database Firewall (AVDF) Release Update 9 (RU9) introduces many capabilities to help organizations advance their current security posture and increase their team's productivity. Here are some of the highlights:

- **[Security Assessment](#)**: AVDF 20.9 introduces a centralized security assessment solution for enterprises by integrating the popular Database Security Assessment Tool (DBSAT) for Oracle Databases. The full-featured assessment with compliance mappings and recommendations will help organizations clearly understand their security posture for all their Oracle databases in one central place.
- **[Discover sensitive objects and privileged users](#)**: AVDF 20.9 now helps customers discover sensitive data and privileged users in the Oracle database. Customers can also create Database Firewall global sets with the discovered privileged users and sensitive objects, and use them to create database firewall policy in just three steps.
- **[Audit Insights](#)**: Customers can now get immediate insight into the top user activities across one or multiple databases. This feature offers a bird's-eye view with summary sections featuring counts and distribution charts and the option to drill down for further analysis with interactive reports.
- **[Before/After reporting for Microsoft SQL Server](#)**: The Before/After report for the Microsoft SQL server is a valuable addition to the already available before/after report for the Oracle database, helping organizations improve their compliance posture.
- **[Agentless Audit Collection](#)**: Customers can now accelerate the deployment of AVDF with the agentless audit collection service for Oracle databases. With this feature, there's no need for agent installation or upgrades on target Oracle databases, making deployment quick and effortless. The agentless audit collection service helps small or remote deployments and proof of concepts where time and resources are limited.
- **[System Alerts](#)**: Administrators can now be alerted on the status of critical AVDF changes, such as high availability configuration, storage availability, certificate expiration, and password expiration.

- **[Out-of-Place Upgrade](#)**: Increase system availability during updates and upgrades with minimal downtime, typically in minutes.
- **[Data Retention](#)**: Administrators can streamline data retention with a simplified lifecycle management process and a target-focused view. The new feature provides single-click operations, such as release, retrieve, and move to remote, for both online and archived data.
- **[Upgraded Platform](#)**: The operating system for the Oracle Audit Vault Server and Database Firewall Server has been updated to Oracle Linux 8, delivering enhanced security and stability to the embedded platform.

With the Security Assessment for enterprises and the discovery of sensitive data and privileged user capabilities, AVDF 20.9 is the most important release yet. It provides a comprehensive solution that covers all aspects of database security and helps organizations stay ahead of the ever-evolving security landscape.

Like every Release Update, AVDF 20.9 includes critical functional and security fixes. We strongly recommend that you apply the AVDF 20.9 release update to enhance the usability, stability, and security of your Oracle AVDF deployment.

New features in Oracle AVDF Release 20.8

The primary focus of Oracle Audit Vault and Database Firewall (AVDF) release 20.8 is quality and usability improvements, along with fixes for several customer-reported issues. We think this is the most important update to AVDF 20 since its initial release in September 2020.

Oracle AVDF Release 20.8 introduces many new features and enhancements, some of which are listed below.

Ease of Use: To improve the user experience, we have revised many pages of the AVDF console. Key highlights include:

-
- Improved user experience with a more logical flow of the multistage Database Firewall policy
- Consistent look-and-feel and column ordering across all reports
- Simplified AD/LDAP configuration page
- Included hints to simplify the flow of the activity and renamed several labels to provide more contextual meaning

Improved Security:

- Introducing a read-only auditor role. This role improves the separation of duty between those who can configure and modify audit policies and those who merely need to analyze and report on audit data. [Read-only Auditor Role](#)
- Users can block SQL traffic for undefined database service names in the Database Firewall. [Block Traffic for Undefined Service Names](#)
- Fixes for several internally discovered and customer-reported issues
- Customers can now [rotate certificates](#) for Audit Vault Server, Audit Vault Agents, and Database Firewalls

Expanded Enterprise Support:

- Database Firewall can now decrypt [TLS Traffic](#) and analyze SQL statements for Oracle RAC targets
- Database Firewall now supports Oracle Autonomous Database
- Broaden audit collection support for PostgreSQL 12 and 13, and MongoDB 5.0. Please refer to Oracle AVDF [Product Compatibility Matrix for all supported versions](#).

Operational Enhancements:

- [TLS proxy certificates](#) for Database Firewall can now be set using AVDF Console
- Audit Vault agents can now be [restarted](#) centrally from the AVDF console
- Introducing a new AVCLI command to [Retrieve Audit Policies](#)

Platform Updates:

- VMWare VSphere 7.0 can now be used to install and run Oracle Audit Vault and Database Firewall
- Audit Vault agents can now be installed on a host machine with JRE 17. For the AIX platform, we also support JRE 11. See [Audit Vault agent: Supported and Tested Java Runtime Environment](#) for complete information.
- Includes security and stability fixes from Oracle Database Release Update 19.16 (July 2022) for the underlying Oracle AVDF repository.
- Includes security and stability fixes for the embedded Oracle Linux 7.9 operating system.
- Includes the latest security and stability fixes for the underlying Oracle and Non-Oracle components, including APEX, JRE, Oracle Clusterware, Oracle Instant Client, etc.

We **strongly recommend** that you apply the AVDF 20.8 release update to enhance the usability, stability, and security of your Oracle AVDF deployment.

New features in Oracle AVDF Release 20.7

- New Features in Database Firewall:
 - Capability to decrypt TLS traffic and analyze the SQL statements going to Oracle Database targets. See [Monitoring TLS Encrypted SQL Traffic](#) for more information.
 - A new **Default** Database Firewall policy which logs all login and logout events to the database along with DDL or DCL activities. See [Types of Database Firewall Policies](#) for more information on the rules of this policy.
 - To reduce deployment time **User-defined** Database Firewall policies can be exported for one target database (such as test instance) and imported for another target database (such as production instance). See [Exporting and Importing Database Firewall Policies](#) for more information.

- ERSPAN support for Database Firewall deployed in **Monitoring (Out of Band)** mode. See [Configuring Encapsulated Remote Switched Port Analyzer with Database Firewall](#) for more information.
- In case a Linux host machine has multiple network devices, then the Host Monitor Agent can now monitor all those network devices. See [Create a Monitoring Point for the Host Monitor](#) and [Create a Network Audit Trail](#) for more information.
- New Features in Audit Vault Server:
 - Introducing support for monitoring of Audit Vault Server. See [Monitoring Audit Vault Server](#) for more information.
 - Improved audit trail status reporting mechanism in the Audit Vault Server console. This feature eliminates incorrect reporting of unreachable trails. See [Checking the Status of Trail Collection in Audit Vault Server](#) and [ALTER SYSTEM SET](#) for more information.
 - Network and system settings for the standby Audit Vault Server can now be configured using the primary Audit Vault Server console. See [Changing the Standby Audit Vault Server Network Configuration](#) and [Changing the Standby Audit Vault Server System Settings](#) for more information.
 - Ability for super administrator to create and edit a user defined data retention policy and set it as default. The retention policy can be selected during target registration. See [Creating Archiving and Retention Policies](#) and [Registering Targets](#) for more information.
- New Features in Audit Vault Agent:
 - Introducing Audit Vault Agent auto restart functionality that restarts the Agent in case host machine is restarted or the Agent goes down for any reason. See [Configuring Agent Auto Restart Functionality](#) for more information.
 - Oracle AVDF can collect unified audit trail data from both primary and standby Oracle Active Data Guard databases consistently. With this feature Oracle AVDF can now collect audit data generated on the standby database. See [Additional Information for Audit Collection from Oracle Active Data Guard](#) for more information.

New features in Oracle AVDF Release 20.6

- Improved operation and system management with:
 - Automated pre-check of Audit Vault Agent on the host machine. See [Validation During Audit Vault Agent Deployment](#) and [Validation During Host Monitor Agent Deployment](#) for more information.
 - Provide historical data of audit trail downtime for better visibility of audit trail status. See [Checking the Status of Trail Collection in Audit Vault Server](#) for more information.
 - Database Firewall instances with existing monitoring points can now be paired for high availability. See [Configuring High Availability of Database Firewall Instances With Monitoring Points](#) for more information.

- Providing flexibility by setting user's preferred time zone in Audit Vault Server console for a specific session. See [Changing the Time Zone](#) for more information.
- Automatic renewal of Audit Vault Server and Database Firewall platform certificates before they expire. See [Platform Certificates](#)
- Broaden Oracle AVDF [Product Compatibility Matrix](#) with support of:
 - Microsoft SQL Server (Standard Edition) version 2019 for audit collection.
 - Database Firewall monitoring of Microsoft SQL Server Cluster (Windows Failover Cluster) in addition to existing audit collection.
 - Audit Vault Server and Database Firewall on Kernel-based Virtual Machine (KVM).
- For installation of Host Monitor on Windows, manual installation of Npcap is no longer needed. Npcap is automatically installed along with the Agent installation. See [Deploying the Agent and Host Monitor on Windows Host Machine](#) for more information.

New features in Oracle AVDF Release 20.5

- To improve security posture, introducing Security Technical Implementation Guidelines (STIG) unified audit policy for provisioning on Oracle Database targets. See [Security Technical Implementation Guidelines \(STIG\)](#) and [ENABLE UNIFIED AUDIT POLICY](#) for more information.
- Broaden Oracle AVDF platform compatibility with support for IBM DB2 Database Partitioning Feature (DPF) on Linux and AIX platform for audit collection. See [Oracle AVDF Administrators Guide](#) and [Oracle AVDF Installation Guide](#) for more information.
- For improved visibility, **Database Firewall Reports** and **All Activity** reports now include **Rule Name** and **Rule Type**. See [Database Firewall Reports](#) for more information.
- For better granularity, alert definitions now include **Rule Name**, and alert reports now include **Policy Name**, **Rule Type**, and **Rule Name**. See [Writing an Alert Condition](#) for more information.
- For Host Monitoring on Windows, Npcap is automatically downloaded along with the Agent software (agent.jar) file. See [Deploying the Agent and Host Monitor on Windows Host Machine](#) for more information.
- Security and stability fixes are applied to the embedded Oracle Linux 7 operating system.
- Includes Oracle Database 19.12 security fixes from July 2021 CPU. See [Oracle Critical Patch Update Advisory - July 2021](#) for complete information.

Warning: If you are using Database Firewall for monitoring native network encrypted traffic of Oracle Database (patched with July 2021 CPU), then refer to the topic [Database Firewall is Unable to Decrypt Native Network Encrypted Traffic](#) to analyze any impact on your Oracle AVDF implementation.

New features in Oracle AVDF Release 20.4

- Introducing capability to enable FIPS 140-2 for Audit Vault Server and Database Firewall. See [Enabling FIPS 140-2 in Oracle AVDF](#) for more information.
- Support for audit collection and network monitoring (using Database Firewall) of Oracle Database 21.
- Support for audit collection from Autonomous Data Warehouse (Dedicated) and Autonomous Transaction Processing (Dedicated).
- 2X audit collection rate. See [Registering Targets](#) for more information.
- Introducing support for audit collection from Oracle Linux and RHEL versions 7.9; 8.2; and 8.3.
- Enable conditional auditing for Unified Audit policies. See [Custom and Oracle Predefined Unified Policies](#) for more information.
- Support for profiles in Database Object rule in Firewall policy. See [Creating and Managing Profiles](#) and [Database Object Rule](#) for more information.
- CSV format support for audit collection. See [CSV File Collection Plug-ins](#) for more information.
- MongoDB 4.4 support for audit collection.
- Additional user management capability through AVCLI. See [AVCLI User Commands](#) for more information.

New features in Oracle AVDF Release 20.3

- Database Firewall can now detect exfiltration attempts by capturing the number of rows returned for Oracle Database. See [Database Firewall Policy for Capturing Return Row Count](#) and [Database Object Rule](#) for complete information.
- Support for audit collection and network monitoring (using Database Firewall) of Microsoft SQL Server (Enterprise Edition) 2019. See [Product Compatibility Matrix](#) for complete information.
- Support for Microsoft SQL Server Always On availability group.
- Support for audit collection from Microsoft SQL Server Extended events. See [Microsoft SQL Server Plug-in for Oracle Audit Vault and Database Firewall](#) for complete information.
- Filter audit activity using application attributes or database component (such as Data Pump) fields in reports. These new fields can also be utilized in Alert policy for monitoring. See the following sections for complete information:
 - [Audit Record Fields](#)
 - [Data for Event Reports](#)
 - [Writing an Alert Condition](#)

New Features in Oracle AVDF Release 20.2

- Audit Vault Agent can be associated with more than one IP address for Audit Vault Server communication. See section [Deploying and Activating the Audit Vault Agent on Host Computers](#) for complete information.
- Supporting audit collection, Audit Vault Agent deployment, and Host Monitor deployment on Microsoft Windows Server (x86-64) version 2019.
- Supporting audit records collection from DB2 instance level audit.

New Features in Oracle AVDF Release 20.1

Expanded Audit Collection

- Supports new target types such as PostgreSQL and many other targets through REST JSON framework. See [Product Compatibility Matrix](#) for complete information.
- Introduced Quick JSON collector that can be configured to collect audit data from JSON files. For example, it can be configured to collect data from MongoDB JSON audit file. See [Configuring Quick JSON Target Type to Collect Audit Data from MongoDB](#) for complete information.
- Supports audit collection from Oracle Container Database. See [Configuring Audit Trail Collection for CDBs and PDBs](#) for complete information.
- Supports before and after value capture for Oracle Databases using Oracle GoldenGate Integrated Extract. A limited license for Oracle GoldenGate is included to support this functionality. See [Transaction Log Audit Data Collection Reference](#) for complete information.

Simplified Database Firewall

- Multi-stage Firewall with simplified configuration as part of the Audit Vault Server console.
- Simpler policy creation using SQL cluster sets which consist of one or more SQL clusters. See [Creating And Managing Database Firewall SQL Cluster Sets](#) for complete information.
- Easier configuration of Oracle Real Application Clusters through SCAN listener. See [Using Oracle Database Firewall with Oracle RAC](#) for complete information.
- Supports [Bonding of Network Interface Cards](#) for increased throughput and resiliency.
- Reintroducing Host Monitor functionality on Windows platform. See [Deploying the Agent and Host Monitor on Windows Host Machine](#) for complete information.
- Enhanced DDI capability to retrieve session information for Oracle Database targets. See [Run the Oracle Advance Security Integration Script](#) for complete information.
- Introduced new commands for Database Firewall configuration tasks. See [System Configuration Utilities](#) for complete information.

Enhanced User Interface

- A new redesigned user interface with simplified navigation for common workflows.
- Rich dashboards for auditors and administrators.
- Supports provisioning of recommended Unified audit policies. See [Provisioning Unified Audit Policies](#) for complete information.
- Unified console for Audit and Firewall management. Registering a target for audit collection and Database Firewall monitoring is simplified. See [Registering Targets](#) for complete details.

Improved Enterprise Support

- Supports user authentication with Microsoft Active Directory and OpenLDAP for users connecting to Audit Vault Server console. See [Integrating Oracle Audit Vault and Database Firewall with Microsoft Active Directory or OpenLDAP](#) for complete information.
- Supports automatic archival of all the monitored data. See [Enabling Automatic Archival](#) for complete information.
- Supports multi-path fiber channel based storage for high availability. See [Configuring Fiber Channel-Based Storage for Audit Vault Server](#) for complete information.
- Supports changing the TCP/TCPs ports used by Audit Vault Server database. See [Configuring Custom Ports on Network Interfaces](#) for complete information.
- The installable *iso* files can be copied to a USB medium. See [Installing Audit Vault Server or Database Firewall](#) for complete information.

Bugs Fixed in Oracle AVDF

Customer reported bugs fixed in Oracle AVDF. In addition, internal bugs that enhance the security and stability of Oracle AVDF are also fixed

Release 20.17

Bug Number	Summary
38377281	In AVDF 20.13 HA setup, false critical alerts indicated excessive time differences between primary and standby servers, despite minimal actual discrepancies.
38464451	The Audit Vault Server console lacked support for custom UDP ports in syslog connectors, requiring manual edits and risking configuration errors.
38508711	Data retention: Offline tablespaces in the EVENT_DATA diskgroup are not archived to NFS.
38517983	Audit records for the AVDF System target in AVDF were not purged after six months, resulting in excessive storage consumption.

Bug Number	Summary
38681464	Online data in AVDF did not expire or archive as expected, leading to storage space constraints and inefficient data management.
38723557	In a 20.9 AVDF HA setup, switchback operations failed with a 404 error, disrupting high availability and involving authentication errors like ORA-01017.
38824540	In the auditor view of the Audit Vault Server console's Security Assessment section, the number of targets assessed does not match the counts shown in graph.
38835529	Database Firewall experienced delayed data processing due to DNS resolution issues.

Release 20.16

Bug Number	Description
37694127	System alert has been added for when the inode usage reaches 90% for the /home/oracle and /var/temp directories
38062189	Auto archive job does not automatically archive datafiles after online period expires
38206634	AVDF 20.12: Fix issue where a monitoring point in proxy mode was preventing queries from executing on a database
38207191	Restoring from a backup fails when data encryption (TDE) password contains the \$ character.
38252094	DBSAT Data Discovery job no longer runs for deleted(inactive) targets
38365806	AVDF system OS trail collection fails when the logs contain hostname with . (dot character)
38371091	AVDF 20.14: AVDF 20.14: OS audit log on Audit Vault server running out of filesystem space
38455454	Data retention GUI page on a system with large number of datafiles fails to load
38458547	Manual archiving of datafiles fails with Unable to acquire lock error
38570640	Host monitoring points no longer falsely display being in a "down" state on the Audit Vault Server console
38350120	Purge of older data when retention period expires does not work when network trails are present
38274169	AVDF 20.12: Implementation changes to ensure that automatic password rotation is successful for the AVSRCUSR user on the Audit Vault Agent

Release 20.15

Bug Number	Description
36911032	Audit Vault: Creating the monitoring point failed with OAV-46535 after re-registering the Database Firewall

Bug Number	Description
37056706	Session information is missing in before-after values report for Microsoft SQL Server target
37129007	Audit trails: one target service name modification updating all target service names
37129902	ORA-01956: Invalid command when os_roles are being used
37163906	Health check job failed when system has active critical alerts for password check

Release 20.14

Bug Number	Description
36911032	Audit Vault: Creating the monitoring point failed with OAV-46535 after re-registering the Database Firewall
37056706	Session information is missing in before-after values report for Microsoft SQL Server target
37129007	Audit trails: one target service name modification updating all target service names
37129902	ORA-01956: Invalid command when os_roles are being used
37163906	Health check job failed when system has active critical alerts for password check
37179121	Application audit: normal/readonly auditor cannot see generated report of super auditor's even with access to all targets
37193358	Alert: the Database Firewall 'Database Firewall' diagnostics reported a problem
37201144	Client ID is missing in before-after values report for Microsoft SQL Server target
37224687	Add button greyed out under Database Firewall monitoring
37246309	High inactive session count for target with transaction log audit trail
37286445	Database Firewall performance issue
37320603	Querying on primary key values column is very slow in before-after values report
37390603	AVDF and Microsoft SQL Server DDI (Logon) trigger optimization
37399682	SQL Developer session through Database Firewall IP has no output
37468411	Database Firewall upgraded to 20.12 but unstable and getting stopped frequently after sometime
37491270	AVDF: Database Firewall showing as "Down" in Audit Vault Server console

Bug Number	Description
37586510	Audit Vault and MS-SQL: Directory audit trail connection issue due to incorrect connect string
37661069	Tablespace deletion failing during dropping of sub-partitions with error ORA-00376: File 13 Cannot Be Read At This Time

Release 20.13

Bug Number	Description
34008900	AVDF 20.3: Alerts raised when alert condition is not met
34333159	The same SQL from a different target gets a different cluster ID and GUID
36365170	Status of Database Firewall instance in Audit Vault Server console show "down" but DBFW instance is up and running
36428513	AVDF 20.10: Transaction logs:(redo):client_id,host,program ,os user,terminal field unknown or empty in data modification report
36430124	AVDF config framework currently doesn't support values with embedded '#' in them.
36430162	Upgrade started even though the fs (/var/lib/oracle) was not mounted
36457097	AVDF 20.8: Unknown values received in AVDF report from Microsoft SQL Server target
36591828	AVS 20.9: Unable to retrieve - 1. agent user 2. agent location 3. platform validation 4. host monitor install state
36625438	CIS summary report not reflecting correct oracle database patch version
36711389	Not allowing to add service name with hyphen in AVDF
36735401	AVDF 20.11: Pairing of Database Firewall servers fails
36826387	Firewall syslog settings does not save more than one category
36872959	AVDF upgrade to 20.12 failed with 'rest_enable_agentbootstrap_pkg.py (as root)
36889751	AVS 20.11: Host list drop down to be sorted
36920849	AVDF 20.12: Target name is showing incorrect for alert policy's from Audit Vault Server console
37013636	Space crunch, as deleted files of /var/dbfw are still held by various Oracle and Microsoft Wecsvc processes.

Release 20.12

Bug Number	Description
31757999	Display policies enabled only for local Pluggable Databases (PDBs)
33125674	The certificate must include at least one Subject Alternative Name (SAN)

Bug Number	Description
34867556	AVDF 20.8: Enforcement points do not start after upgrading from 12.2 to 20.8
34964739	AVDF 20.6: restoring Database Firewall configuration on a new instance encounters I/O Error: socket read interrupted
35342421	AVDF 20.6: Oracle Database Firewall unavailable due to certificate validation failure
35374285	AVDF 20.8: Network audit trail fails to start due to Host Monitoring process error
35485705	AVDF 20.9: login as avadmin fails due to proxy server receiving an invalid response from an upstream server
35609128	OCI Marketplace: inconsistent disk group usage display in the AVDF console
35717840	AVDF 20.8: Database Firewall fails to associate with Audit Vault Server
35735914	AVDF 20.7: Firewall Policy creation - table exclusion fails
35963312	AVDF login as avadmin fails due to proxy error
36094288	Network audit trail not starting for Microsoft SQL Database
36102728	AVDF 20.9: Data Modification report - old and new values missing
36196227	Filters associated with saved report are not displayed
36263859	AVDF 20.8: MySQL audit trail stopped due to directory path issue
36286439	Unknown username detected in network trail for Microsoft SQL Target
3630927	AVDF 20.9: I/O calls causing performance issues of SQL queries
36344728	AVDF 20.8: Database Firewall certificate error
36357162	AVDF 20.9: Audit Vault Agent not prompting for activation key
36422817	Database Firewall login events not logged for Native Network Encryption (NNE) traffic
36459103	Transaction log audit collection is lagging and reporting errors in the log
36502612	AVDF 20.9: Before-After value rows for data modifications display as blank, require data in old and new value columns - fix needed in interactive UI report
36502759	Error retrieving unified audit policy for Auditor and Read-Only auditor roles

Release 20.11

Bug Number	Description
34527918	Unable to delete a Database Firewall policy if it has been imported twice with the same name
34983175	AVDF 20.7: Reports in AVDF display unknown_program and unknown_username
35181278	Failure in database object rules creation when importing a large file (approximately 4,000 tables)
35274716	Requires a blocking policy when attempting to drop and delete tables

Bug Number	Description
35694612	AVDF 20.9: <code>syslog</code> audit trail on Linux 8 is non-functional compared to Linux 7
35705013	Unable to login to Audit Vault Server after reboot facing network device name not in runtime: 'EN06'
35745322	AVDF 20.9: unable to add a user with double quotes, for example, "XX", to the database user set of the Database Firewall policy
35762564	ODF-10704: internal capacity exceeded error persists despite setting <code>IPC_BUF_SIZ_MB = 3072 MB</code>
35777769	The Audit Vault Server is not reading data from the Firewall server
35870790	AVS 20.9: AVDF can't collect the <code>syslog</code> audit trail when the hostname of the secure target contains special characters
35892498	AVDF 20.7: Alerts closure (date and time) details are not available in Audit Vault Console
35961768	The <code>last_archive_timestamp</code> is not updating in the secured target, and the Audit Vault agent is encountering errors in the <code>COLLFWK</code> file
36063464	Capture FGA policy name in the <code>policy_name</code> column of the <code>event_log</code>
36063573	OAV-46986: the firewall at IP address 127.0.0.1 does not have a valid Audit Vault Server certificate
36086343	Updating from 20.6 to 20.10, Audit Vault Server fails on Network Config
36130410	Display relevant details for unknown entries in AVDF Network Trail Activity Report
36140746	AVDF 20.4: Directory audit trail issue specific to MS-SQL: directories in the path are not modifiable by others, and the path cannot have more than 5 levels of symbolic links

Release 20.10

Bug Number	Description
24673782	Add mechanism to boot to AVDF recovery mode from the grub menu
35142617	Truncate statement appears under select command class
35153240	ODF-10704: internal capacity exceeded: data dropped for protected database
35156710	AVDF 20.8 - AVS execution of <code>/usr/local/bin/gensslcert destroy-certs create-ca</code> failed
35234065	Is is not possible to create monitoring point using bonded device using AVCLI
35234141	It is not possible to create a bond without providing an IP address
35234183	It is not possible to select multiple NIC's for a single MP in Out-of-Band mode
35258728	AVDF 20.6 - Checking controller connection failed on Database Firewall
35270853	AVDF 20.8 - Users unable to connect using FQDN

Bug Number	Description
35304189	Allow the use of multiple services for a single target in proxy mode
35380623	Migrate bridge fails if management NIC name is changed by OS

Release 20.9

Bug Number	Description
23477697	Multiple alerts raised from single event on database firewall
34072228	AVDF 20.3 - OCI image database not coming up as root and grid user has expired
34507813	Traffic not captured on bonded NICs by 20.7 database firewall
34543909	Gateway vault is not shown and not being updated in the database firewall network settings
34579703	Data loads getting stuck with some commits not occurring using database firewall
34702834	AVS 20.6 - Increase the keysize of Audit Vault certificate
34866101	AVDF 20.7 - Database Firewall rejects SQL from Oracle Database as "Invalid SQL" though it is valid
35031525	Issue in handling marker packets by database firewall

Release 20.8

Bug Number	Description
32918951	Unable to delete the Database Firewall instance from the Audit Vault Server console.
33180809	Oracle AVDF 20.3: Email notification is not working.
33300562	Description of Database Firewall policy should also be copied when the Database Firewall policy is copied.
33538979	Oracle AVDF 20.3: Active Directory login error observed when attempting to log in to the Audit Vault Server console.
33568308	Oracle AVDF 20.3: Cron file messages observed in /var/log/cron directory.
33601352	Oracle AVDF 20.2: Logging in as AUDITOR user results in "processing condition error".
33606254	AVS 20.5 - After audit policies successfully, audit policy displays error "Error computing item" when selecting specific target.
33712231	Oracle AVDF 20.4 : "ALL ACTIVITY REPORTS" contain ORA-01874 error.
33730683	Warn and prevent the user from adding multiple network interface cards to the same subnet.
33756069	Oracle AVDF 20.1: Cannot start audit trail and goldengatexmlrecordreader: getNext: error is observed in XML stream.
33805703	AVS 20.3 - is missing before and after values on exporting to Excel

Bug Number	Description
33826913	Auditor is unable to select secured target in UI, when stored procedure auditing is enabled
33837147	Issues observed when upgrading from Oracle AVDF release 20.5 to 20.6.
33844557	Null value validation missing for some Database Firewall policy fields.
33921302	Host Monitor installation fails on AIX machines with OpenSSL 1.1.1.
33959045	Oracle AVDF 20.6: Viewing database policy shows error "COMPUTING ITEM SOURCE VALUE FOR PAGE ITEM P109_STIG_LIST2"
33975512	Secondary network interface card migration failed when upgrading Audit Vault Server from Oracle AVDF release 12.2 to 20.6.
33976669	Oracle AVDF 20.6: Solaris 11.4 OS audit trail stops with unexpected error.
33978456	Oracle AVDF 20.6: Unable to set the server date time using Audit Vault Server console.
33979369	Imported Database Firewall policies are not displayed in the list of policies for the specific auditor's view and displayed only in the super auditor's view.
33994053	Audit Vault Server backup does not clear the "exclude tablespace" option for archived tablespaces. This can cause HA pairing to fail
33994387	Sync NFS locations should not execute when HA pairing is re-run after standby database mode is changed
34011144	Hash collision error seen in Arbiter session database.
34019838	Invalid CREATE_ARCHIVED_TBSP_CONTENT_UPDATE error observed after upgrading Oracle AVDF 20.3 to 20.5.
34041292	Transaction Log audit trail is stopping due to invalid character in Oracle GoldenGate Extracted XML files.
34076937	Oracle AVDF 20.5: Java class installation error observed when upgrading the Audit Vault Agent.
34127355	Network trail drops packets under high load.
34284705	AVCLI DROP HOST command gives : OAV-46599: INTERNAL ERROR

Release 20.7

Bug Number	Description
33495883 33659100	SERVER_ERROR 500 is observed when attempting to log in to Audit Vault Server console version 20.2.
33465646	Oracle AVDF 20.3: Alert policy condition in the console is limited to 4000 characters.
33253875	Oracle AVDF 20.4: ERROR_PROCESSING_CONDITION is observed when a super auditor is attempting to log in after upgrade to release 20.4 from 20.3.
33030240	Adding sets in Database Firewall policy and related pages do not open in the Audit Vault Server console.

Bug Number	Description
33515971	Host Monitor deployment sometimes fails on Solaris SPARC64 11.3 and Solaris X64 11.3.
33674867	Manual update of Audit Vault Agents fail on some Agents.
33893518	Remove Host Monitor Agent dependency during runtime debugging on Windows platform.
33665863	AVCLI cannot be installed on the remote host without the -d option.
33628801	SV20.6SQLINJ: potential SQL injection observed in AVSYS.ILMCHECK package.
33584294	Improvement in diagnostics and checks for NFS configuration during high availability pairing.
33465739	FLATFILEAUDITDATAPARSER : PARSE : EXCEPTION observed in Oracle AVDF 20.5 while parsing the directory audit records.
33007779	Include the audit file name in the error or warning logs when parsing error occurs for directory audit trails.
31388982	Stop JAVAFWK during Audit Vault Server cold backup.
32621379	Enhance Database Firewall to support ERSPAN (Encapsulated Remote Switched Port Analyzer).

Release 20.6

Bug Number	Description
33300330	Oracle AVDF 20.3: Default Database Firewall policies are using unassigned value
33184853	Include support for Fibre Channel over Ethernet (FCoE).
33175278	Oracle AVDF 20.4: Unable to add routing on secondary network interface cards (NIC).
33175212	After upgrading from Oracle AVDF 20.3 to 20.4, the <code>/etc/resolv.conf</code> file is reset to default.
32842510	The <code>/etc/resolv.conf</code> file does not have DNS Ip address after upgrade.
33157319	After upgrade the console certificate functionality is broken.
33155309	Unable to collect audit data from database targets where Database Firewall monitors native network encrypted traffic.
33081876	Oracle AVDF 20.3: Database Firewall is not gracefully closing existing client sessions, resulting in inactive sessions in the database.
33384072	Update runtime dependency for Audit Vault Agent on Windows.
33330165	Network trail does not start in Windows due to <code>hm</code> directory permission issue.
33263539	Host Monitor should attempt to reconnect to the Database Firewall instance for longer duration.

Bug Number	Description
33291796	Oracle AVDF 20.4: p107_first_run_time dialog error when <i>auditor</i> clicks on a specific target.
33253782	Oracle AVDF 20.4: A <i>super auditor</i> is unable to see the target, results in APEX error.
33213228	Oracle AVDF 20.3: ORA-01422 error in Audit Vault Server console related to registered targets.
33067408	Oracle AVDF 20.1: Restoring Audit Vault Server appliance does not include the new management network interface card.
33423711	Oracle AVDF 20.4: Error when attempting to run an entitlement report.
33456143	Oracle AVDF 20.3: The last archived timestamp of unified audit trail does not get updated. There are multiple parse errors ERROR=6550.
33385297	The database instance crashed when upgrading from Oracle AVDF release 12.2.0.13.0 to 20.4 and pointed to memory issue.
33247649	Oracle AVDF 20.4: Microsoft SQL Server database records high number of audit records due to incorrect syntax specified for connectivity.
33238795	Oracle AVDF 20.3: Alerts are not sent at specified time.
33186418	Oracle AVDF 20.3: Microsoft SQL Server setup script returns an error.
33170060	Oracle AVDF 20.4: Audit Vault Agent started with errors on Solaris 11.3.
33154268	Oracle AVDF 20.3: Switching back to default ports does not work.
33040501	Oracle AVDF 20.3: Deploying Audit Vault Agent on Microsoft SQL Server database fails with internal error.

Release 20.5

Bug Number	Description
32851526	XML parsing error in Transaction Log collector.
32924611	AGENTCTL.bat REGISTERSVC command displays an error even if the command runs successfully.
32985529	AGENTCTL.BAT STARTSVC command fails on some host machines.
33187856	Agents fail during upgrade.
33070155	Oracle AVDF Active Directory authentication errors OAV-47804, ORA-31202, and ORA-06502 observed.
32759027	Trail autostart details missing from the audit trail page.
32604725	Auditor users unable to log in to the Audit Vault Server console after upgrading to release 20.3.
32569788	Unable to create a target group without adding at least one member.
32986506	Failed to copy datafile internal error observed for archiving ILM tablespace.

Bug Number	Description
32519208	Entitlement jobs failing constantly.
32969281	Audit Vault Server upgrade from 20.3 to 20.4 failed due to permission issue.
32943329	Difference in Event_Time between the source database and Audit Vault Event_Log table observed.
32901866	Audit Vault Server upgrade failure from 12.2.0.12.0 to 20.3.0.0.0 during modification of high availability configuration.
33091980	Issue in handling cursor management in alert module and adding additional diagnostics.
32762328	Issue with ILM tablespace deletion observed in Oracle AVDF 20.2.
32907433	Connectivity between Firewall applications and Database Firewall is very slow.
32964387	Jobs pertaining to a specific application are hung when used with Database Firewall and also having more records.
32491616	Warnings observed in WebLogic Server when used with Database Firewall.
32700988	Connecting to Database Firewall deployed in proxy mode failed with ORA-12541: TNS:NO LISTENER error.
32683976	Service name is captured as UNKNOWN_SERVICES in Database Firewall when connected using ORACLE_SID.

Release 20.4

Bug Number	Description
32683399	AVCLI commands backward compatibility for syntax prior to Oracle AVDF 20.3
32633707	Archival check functionality in diagnostics results in error when avbackup or RMAN is running.
32554388	Audit Vault backups are not cleaning up all of the old backup files.
32201286	Active Directory login fails after selecting the group.
32578360	Failure in high availability migration when upgrading to Oracle AVDF 20.x.
32522447	User defined retention policies with - or space in the name results in truncated names.
32484690	Automatic upgrade of Audit Vault Agent fails with JAVA.LANG.NUMBERFORMATEXCEPTION error.
32325673	Oracle AVDF 20.1: Adding network audit trail fails with OAV-46599 error.
32778846	Memory leak in Database Firewall server.
32678630	Oracle AVDF 20.3: Database Firewall health indicators displaying red monitoring points.

Bug Number	Description
32537067	Errors observed when upgrading Oracle AVDF 12.2 to 20, with a cluster path larger than 32K.
32385800	Database Objects with ALL rule in Database Firewall policy fails and does not evaluate as expected.
32291555	All Database Firewall monitoring points are getting restarted when attempting to stop one monitoring point.
32227614	Memory consumption in SYSLOG tunnel increases when the connection to Audit Vault Server fails.
32592028	Oracle AVDF BP12: Failover due to file system errors on the primary listener.
32201286	Active Directory login fails after selecting the group.

Release 20.3

Bug Number	Description
32124026	Network trail failed to collect data after upgrading to 20.2 from 20.1
31881216	ORA-16037: High availability managed recovery operation crashed.
31583963	ORA_LOGON_FAILURES is listed under custom policy instead of Oracle Pre-defined policies.
31907672	Audit Settings report only displays audit statements, the NOAUDIT statements are missing.
31905939	Sybase audit trail is in recovering mode for a very long time.
32007524	Database Firewall is down as there are no spare processes to run core functionality.
28944745	Firewall internal error: Unexpected request for Mocoder result
31992216	ORA-1427: Occurred when Database Firewall Monitoring tab is clicked.

Release 20.2

Bug Number	Description
31807628	Keyboard settings for Audit Vault Server do not function properly.
31560831	Inconsistency between Audit Vault Server console and AVCLI commands for super auditor related tasks.
30633787	Input validation issue while creating archive location.
31075324	Configuring a network interface card for Database Firewall through Audit Vault Server console does not enable it by default.
30397365	Improper alignment of text displayed in the installation screen.
31066450	Help text for register SMTP server is not correct.

Bug Number	Description
31378537	Audit Vault Server console displays an error when attempting to change IP address of the management interface.
31551749	ALTER SESSION command is wrongly categorized as DDL.
31597006	Oracle AVDF 20 Firewall policy names on the Audit Vault Server console still reflect 12.2 terminology.
31602847	Bonded network interface card is deleted after adding a proxy port through the Audit Vault Sever console.
31613342	Unable to add proxy ports for interfaces that were previously part of bonded network interface cards.
31715004	Incorrect login banner for support user.
31764401	Error when attempting to update the description of SQL cluster set.
31764605	Unable to create Database Firewall policy.
30776841	Clusters imported from release 12.2.0.9.0 (and later) are difficult to use after upgrade to 20.1.
32071860	Ability to create cluster sets on 12.2 traffic.
31772109	Error when saving the modified values for DB client set add flow.
31805070	DESCRIBE statement is incorrectly categorized as invalid SQL in Oracle Database 19.5.
31735004	Audit collection for CDB_UNIFIED_AUDIT_TRAIL stops.
31606578	Post upgrade, Oracle DIRECTORY and SYSLOG audit trails second time recovery may skip few records.
31945902	Status of DIRECTORY audit trails sometimes becomes UNREACHABLE.
31854375	Null pointer exception found in Sybase collector.
31571601	Host Monitor displays 12.2 version post upgrade.
31561697	Unable to drop the disk from Audit Vault Server console.
31236889	Unable to set the network interface for Database Firewall.
31583443	Deleting session context rule in firewall policy fails with error.
31180117	Unable to apply firewall policies to any target.
30565002	Unable to synchronize NTP server time.
30422676	Firewall policies applied on non Oracle databases.
31562786	OAV-46992 error observed while creating firewall monitoring point.

Release 20.1

Bug Number	Description
28854500	PRE_CREATE_SUBPARTITIONS_JOB fails with ORA-14098 error. Index mismatch for tables in ALTER TABLE EXCHANGE PARTITION
26949391	ORA-12012: error encountered on auto execution of AVSYS job SPA\$_822

Bug Number	Description
24438861	A remote filesystem is dropped even when it has an associated archive destination.
31217870	Archiving is disabled after upgrading to 12.2.0.12.0 and requires to be manually enabled again.
31203634	Agent is in unreachable state after high availability upgrade.
31391462	Network trail is in unreachable state intermittently after high availability switchover and failover.
31328993	Host Monitor installation in DAM mode fails with error 0403-011.
30002119	Job hangs with user entitlement in 12.2.0.8.0.
30825748	Database Firewall is not processing the data from Host Monitor in 12.2.0.11.0.
30670219	Audit Vault Agent installation fails on AIX in 12.2.0.11.0.
31301129	High Input/Output issue noticed when Host Monitor is monitoring SQL Server on Windows Server 2012.
30826438	Issues encountered while processing FGA audit data of Enterprise users.
28981812	Background worker process is down with handshake error: asio.ssl
31178253	Enabling native network encryption on Database Firewall does not collect any SQL messages.
30688042	Issue determining integrity for ASO requests.
31419900	Request to allocate specific space for alert threshold messages.
26795578	Missing sub partition for error on auto execute of AVSYS job avs_maintenance_j

About Oracle AVDF Installable Files

Oracle AVDF software is installed using the .iso files.

Oracle AVDF software contains the following installation files:

- Audit Vault Server install:

Oracle AVDF 20.4 and Later	Oracle AVDF 20.1 to 20.3
<p>vpart_number.iso Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server</p> <p>Note: Starting with Oracle AVDF 20.4, there is a single Audit Vault Server ISO file and there is no need to concatenate.</p>	<p>Audit Vault Server installer file is split into 3 parts or files as follows:</p> <ul style="list-style-type: none"> – vpart_number.iso Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server - Part 1 of 3 (MUST DOWNLOAD ALL THE 3 PARTS AND CONCATENATE BEFORE ATTEMPTING INSTALLATION)

- `vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server - Part 2 of 3 (MUST DOWNLOAD ALL THE 3 PARTS AND CONCATENATE BEFORE ATTEMPTING INSTALLATION)

- `vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Audit Vault Server - Part 3 of 3 (MUST DOWNLOAD ALL THE 3 PARTS AND CONCATENATE BEFORE ATTEMPTING INSTALLATION)

Note: Concatenate all the three ISO files to get Audit Vault Server 20.x ISO (`avdf-install.iso`) before proceeding with installation.

- Database Firewall install:

`vpart_number.iso` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Database Firewall

Note

Verify the checksum value for both (the Audit Vault Server ISO file and the Database Firewall ISO file). In case of any error or mismatch in the checksum values, download the ISO files and validate the checksum values again.

- Database Firewall utility:

`vpart_number.zip` Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Utilities. This bundle contains the following files:

- Npcap installer required for Host Monitoring on Windows: `npcap-utility.zip`
- Database Firewall utilities to examine Native Network Encryption traffic for Oracle Database and to gather session information from other database types: `dbfw-utility.zip`
- `Utilities_README`: Instructions for deploying Npcap and Database Firewall utilities patch.

- Deprecated cipher utility bundle:

Oracle AVDF 20.4 and Later	Oracle AVDF 20.1 to 20.3
Not applicable.	<p><code>vpart_number.zip</code> Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Deprecated-Cipher-Removal Utility</p> <p>Note: Apply the deprecated cipher removal patch on Audit Vault Server 20.x after installation.</p>

This is optional. However, it is highly recommended.

- [Vpart_number.pdf Oracle Audit Vault and Database Firewall 20.x.0.0.0 - Release Notes](#)

Note

The installation process wipes out existing operating system on the machine on which you install the Audit Vault Server or Database Firewall, and automatically installs the new operating system that comes along.

Oracle AVDF 12.2 Premier Support Alert

End of premier support for Oracle AVDF release 12.2.

Upgrade to Oracle AVDF 20 at the earliest as premier support for release 12.2 ends in March 2021 as specified in the [Oracle Lifetime Support Policy Guide](#). Refer to [Oracle AVDF 20 Upgrade Documentation](#) for complete information.

Before you begin the upgrade, be aware of the following issues:

- For upgrading to Oracle AVDF version 20, you must be on 12.2.0.9.0 or above.
- In case you have to perform multiple upgrades to 20, then a single backup operation prior to the first upgrade is enough.

Product Compatibility Matrix

Types of targets (databases and operating systems) supported by Oracle AVDF 20.

See section [Product Compatibility Matrix](#) in the Oracle Audit Vault and Database Firewall Installation Guide for information on supported targets and deployment options for Audit Vault Server.

Downloading Oracle AVDF Documentation

Learn how to access documentation for Oracle AVDF.

- [Oracle Audit Vault and Database Firewall 20 Documentation](#) to download the most current version of this document, and the complete set of Oracle Audit Vault and Database Firewall documentation.
- [Documentation for other Oracle products](#)

Known Issues

Learn how to fix some known issues with Oracle AVDF.

This section lists current known issues with workarounds if available. Be sure to apply the latest bundle patch. New installations include the latest bundle patch.

In general, if you experience a problem using the Audit Vault Server console, try running the same command using the `AVCLI` command line utility.

Note

For additional known issues in Oracle AVDF 20 refer to the MOS note (Doc ID 2688423.1) and the README for specific release.

Database Firewall is Unable to Decrypt Native Network Encrypted Traffic

Learn how to fix the issue when Database Firewall is unable to decrypt Native Network Encrypted traffic.

Issue

Database Firewall is unable to decrypt Native Network Encrypted traffic. The issue is observed when the Oracle Database server and the SQL client are patched with July 2021 or October 2021 Critical Patch Updates.

Symptom

The **Database Firewall Reports** and **All Activity** reports will have the string `extracted_from_protocol encrypted` in the **Command Text** column.

Refer to the table to understand Database Firewall capability to decrypt Native Network Encrypted traffic.

Oracle Database Target Patched with July 2021 or October 2021 CPU	SQL Client Patched with July 2021 or October 2021 CPU	Capability of Database Firewall to Decrypt Native Network Traffic
No	No	Yes
Yes	No	Yes
No	Yes	Yes
Yes	Yes	No

Note

Oracle Database and SQL clients with versions starting 11.1 to 19c with July 2021 or October 2021 CPU may be impacted.

Workaround

Apply the Oracle Database January 2022 DBRU patch. This issue is not observed after applying the patch on the database, in Oracle AVDF release 20.5 or later.

Error When Starting Audit Vault Agent as a Service on Windows in Oracle AVDF 20.5

Learn how to manage an issue when starting Audit Vault Agent as a service on Windows.

Issue

Audit Vault Agents on Windows machine do not start as service. After installing or upgrading to Oracle AVDF release 20.5, this issue is observed on the Windows host machine.

The following error is observed when attempting to start Agent service on Windows:

```
The application was unable to start correctly
```

Workaround

Follow these steps:

1. After installing or upgrading Oracle AVDF 20.5, apply the patch 33492214 on Audit Vault Server. Then, download and redeploy the Audit Vault Agents on Windows host machine.
2. Install Visual C++ Redistributable for Visual Studio 2017 package from *Microsoft* on the Windows target machine. Ensure `vcruntime140.dll` file is available in the `C:\Windows\System32` directory.
3. If the `vcruntime140.dll` file is not present, then add it to the `<Agent Home>/bin` and `<Agent Home>/bin/mswin-x86-64` directories.
4. Follow the complete requirements as mentioned in Audit Vault Agent Requirements.
5. Download and redeploy all the Audit Vault Agents on the Windows host machine.

Audit Data Collection is Stalled in High Availability

Learn how to fix the issue with Agents going into `UNREACHABLE` state after configuring high availability.

Issue

Agents may go to `UNREACHABLE` state in a high availability environment after multiple pairing or unpairing operations. Few of the Audit Vault Agents may go to `UNREACHABLE` state if multiple high availability operations like pairing or unpairing are performed

within a period of one hour. Agents may also go to `UNREACHABLE` state if the failover occurs within one hour of pairing or unpairing.

Workaround

Avoid performing pairing or unpairing operations more than once in a period of one hour. Redeploy those Agents that have gone to `UNREACHABLE` state.

Database Firewall is Unable to Monitor Root Container Database Targets With Native Encryption Enabled

Learn about the inability of Database Firewall to monitor root container database targets with native encryption enabled.

Issue

Database Firewall does not support decryption of traffic using with native encryption for root container databases. Running ASO advance security integration script on root container database does not work. Set up Database Firewall ASO integration on every pluggable databases and configure the Database Firewall to monitor them.

Workaround

None.

Secondary Audit Vault Server Upgrade Failed Due to Database Mounting Error

Issue: Upgrading secondary Audit Vault Server fails with an error.

Log in as `root` user, and run the command:

```
/opt/avdf/bin/privmigutl --status
```

Check if the following errors are present in the `/var/log/debug` file:

```
upgrade_start_asm_db.py: Could not mount the database
```

```
upgrade_start_asm_db.py: Mounting the database
```

Workaround: Follow these steps to resolve this error:

1. Check the status of `dbfwdb` service by running the following command as `oracle` user:

```
/usr/local/dbfw/bin/dbfwdb status
```

2. Switch user to `root`.

3. Edit `/etc/sysconfig/avdf` and change `SYSTEM_STATE` to `UPGRADE`.
4. If the status is `ORACLE` instance is running, then run this command as `oracle` user to stop the process:

```
/usr/local/dbfw/bin/dbfwdb stop
```

5. Start the `dbfwdb` service by running the command as `oracle` user:

```
/usr/local/dbfw/bin/dbfwdb start
```

6. Run the following command to check if it is running:

```
/usr/local/dbfw/bin/dbfwdb status
```

7. Ensure the status is running. Then edit `/etc/sysconfig/avdf` and change `SYSTEM_STATE` to `RECOVERY` as `root` user.
8. Resume the remaining upgrade process by running the following command as `root` user:

```
/opt/avdf/bin/privmigutl --resume -confirm
```

Note

In case you are running the above commands through SSH, then ensure the SSH session does not timeout. Start the SSH session with `ServerAliveInterval` option and set to a reasonable value. For example, 20 minutes.

Archived Files Copied from Primary Path in High Availability Environment

Issue: The archived files exist for both the primary and secondary Audit Vault Servers in a high availability environment. When configuring the archival locations before pairing, the following path is set.

Primary Audit Vault Server: `/dir1`

Secondary Audit Vault Server: `/dir2`

There is an issue where the archive files pertaining to the secondary Audit Vault Server are copied to the path `/dir1` instead of `/dir2`. When such a path (`/dir1`) does not exist in the secondary Audit Vault Server, it is created when they are paired during high availability configuration.

Workaround: None. The archived files are present in the path `/dir1` of the secondary Audit Vault Server.

Error While Running Pre-upgrade RPM

Issue: The following error is observed when running the pre-upgrade RPM on the secondary Audit Vault Server in a high availability environment:

```
Unable to stop observer
```

Workaround: Follow these steps to resolve this error:

1. Uninstall the pre-upgrade RPM.
2. Re-install the RPM.

GoldenGate Integrated Extract fails to Clone Existing LogMiner Session and Invalid XML Records are Generated

Issue: The following issues are observed while configuring Oracle GoldenGate Integrated Extract:

- GoldenGate Integrated Extract does not wrap the text data inside CDATA tag.
- GoldenGate Integrated Extract failed to clone existing LogMiner session when the dictionary log is not available for a specific SCN.

Workaround: After installing Oracle GoldenGate, contact Oracle Support to create a Merge Label Request for applying the patch (Bug 32175609 and Bug 32063871). This patch needs to be applied on Oracle GoldenGate installation.

Unable to Access Audit Vault Server Console After Upgrade

Issue: After upgrading to Oracle AVDF 20.1 or later, the Audit Vault Server console cannot be launched. This may be due to inactive `httpd` service. Upon observing the `/var/log/httpd/error_log` file contains the following error message pertaining to `httpd` service restart:

```
AH00060: seg fault or similar nasty error detected in the parent process
```

Workaround: If this error is observed, then log in as `root` user and run the following command:

```
systemctl start httpd
```

Unsupported Character Sets in Oracle Database Directory Trails

Issue: Oracle Database related `DIRECTORY` and `SYSLOG` audit trails do not support some of the database character sets.

They are NE8ISO8859P10, JA16DBCS, KO16DBCS, CE8BS2000, CL8BS2000, CL8EBCDIC1158R, EE8BS2000, EL8EBCDIC423R, SE8EBCDIC1143, WE8BS2000, WE8BS2000E, and WE8BS2000L5.

There are 5 characters that are not supported in WE8DEC database character set.

Workaround: None.

DIRECTORY and SYSLOG Audit Trails Do Not Stop

Issue: For Oracle DIRECTORY and SYSLOG audit trails, when the system is unable to determine the character set to open the audit file, the audit trails do not stop.

Workaround: None.

Unable to Set Custom Ports in Audit Vault Server

Issue: Unable to set custom ports in Audit Vault Server.

Workaround: Attempt to set the custom port again using same steps.

Unable to Access the AVS Console After Changing the AVS Time Manually or using NTP Server

Issue: After changing the Audit Vault Server time manually or using NTP server, there may be a difference in few minutes. This may bring down the Automatic Storage Management and the database. This results in an error and the Audit Vault Server console is not accessible.

Workaround:

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

```
systemctl stop monitor
```

```
systemctl stop javafwk
```

```
systemctl stop dbfwdb
```

Note

Check the exit status of the command by running the `echo $?` command. If the exit status is non-zero, then contact Oracle Support. If the exit status is zero, then only proceed with running the next commands.

3. Run the remaining commands in a sequence and proceed only if the exit status is zero:

```
systemctl stop asmdb
```

```
systemctl start asmdb
```

```
systemctl start dbfwdb
```

```
systemctl start javafwk
```

```
systemctl start monitor
```

Archive Location Is Not Accessible During Archiving Or Retrieving

Issue: The archive location is not accessible. This issue may be encountered during archiving or retrieving post upgrade or installation.

Workaround: This may be due to a "-" (dash or hyphen) in the export directory name for NFS archiving locations. Check for "-" (dash or hyphen) in the export directory name and delete that filesystem from the Audit Vault Server.

Note

- Oracle AVDF 20.1 and later supports archive and retrieve functionality with Network File System (NFS) server which support both versions v3 and v4.
- Only NFS version v3 is not supported for releases 20.3 and prior. It is supported starting Oracle AVDF release 20.4.
- If your NFS server supports and permits both v3 and v4 for archive or retrieve, then no action is required.
- In case you have NFS v4 only in your environment for archive or retrieve, then set the `_SHOWMOUNT_DISABLED` parameter to `TRUE` using the following steps:
 1. Log in to the Audit Vault Server as `root`.
 2. Switch user to oracle: `su - oracle`
 3. Start SQL*Plus connection as `sqlplus /nolog` without the username or password.
 4. In SQL*Plus execute the command: `connect <super administrator>`
 5. Enter the password when prompted. Alternatively, execute the command: `connect <super administrator/password>`
 6. Execute the command: `exec avsys.adm.add_config_param('_SHOWMOUNT_DISABLED', 'TRUE');`

Unable To SSH Into Oracle Audit Vault And Database Firewall After Upgrade

Issue: *SSH* no longer connects after upgrade to Oracle Audit Vault And Database Firewall 12.2.0.11.0.

Workaround: Upgrade *SSH* client to a version that supports SHA-256.

AVS Reboot with SAN Storage Can Cause Proxy Errors

Cause: If the same iSCSI target is shared between more than one AVS instance, it can cause proxy errors.

Workaround: Ensure that each iSCSI target is exclusive to an AVS instance.

Pre-Upgrade Process Failed After Remove and Re-Install

Cause: The RPM process can hold open file descriptors after it has removed the pre-upgrade RPM, making it produce an error when attempting to re-install.

Workaround: Reboot the appliance and reinstall the pre-upgrade RPM to work round this issue.

Rebooting After Running Pre-Upgrade RPM Results in /var/dbfw/upgrade Not Mounted

Cause: After the pre-upgrade RPM is installed, you must manually mount the upgrade media partition if the appliance is rebooted.

Workaround: Run `mount /var/dbfw/upgrade` to remount the partition.

Check For Busy Devices Before Starting The Upgrade Process

Cause: Check for any busy devices before starting the upgrade process. The upgrade may not check for busy volumes and may result in an error.

Workaround: Run `lsdf` against `/tmp` and `/usr/local/dbfw/tmp` to discover any open temporary files. Ensure that no logs are open when starting the upgrade process.

Upgrade Fails If The Time Settings For The Primary And Standby Servers Are Out Of Synch By More Than 3 Minutes

Cause: If the primary and standby server time settings are out of sync by more than 3 minutes, then upgrade will fail raising the following error: `ORA-29005: The certificate is invalid.`

Workaround: You must synchronize the time on the primary and standby servers before commencing upgrade.

"Failed Install Or Upgrade" Dialog Box Appears During Installation Or Upgrade

Problem: I see a blue screen that states:

The system has encountered a problem, and will start minimal services so that you can log in and recover.

It provides the current status of the installation or upgrade and asks you to check the system log for more information and contact Oracle Support.

Workaround: Upon seeing this blue screen, perform the following:

1. Log in as `root` user.
2. Execute the following command to install the diagnostic tool:

```
rpm -i /usr/local/dbfw/packages/avs-  
diagnostic-20.1.0.0.0-0_*.x86_64.rpm
```

3. Capture the diagnostics archive by running the following diagnostics package to output the name of the archive file:

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

Note

If this command creates a file `diagnostics-not-enabled.readme` follow the instructions in that file to enable the diagnostics and generate the archive.

4. File a Service Request (SR) and attach the archive to the SR.

Note

Once Oracle Audit Vault and Database Firewall detects an error in the installation or upgrade, it will not start any more services, but it will retain any started services so that they can be debugged.

Oracle Audit Vault And Database Firewall May Fail To Install On Sun X4-2

Symptoms: The pre-reboot part of install is normal. However, after reboot, the system presents the user with a black screen containing only the text `Hard disk error`.

Cause: These servers include a small internal USB drive for the Oracle System Assistant. This device contains a Linux installation, which conflicts with the bootloader in Oracle Audit Vault and Database Firewall 20.1 and later.

Solution: To install Oracle Audit Vault and Database Firewall 20.1 or later, you must first disable Oracle System Assistant from the BIOS menu. If the option to disable the OSA is greyed out, reset the BIOS to enable it.

See Also

https://docs.oracle.com/cd/E36975_01/html/E38042/z40000091408680.html for more information.

Before Re-booting The System During The Upgrade Process,
Check The Group Status Volume To Ensure Only A Single
Instance Of VG (`vg_root`) Exists

Cause: Re-using storage from a previous installation. Having two instances of `vg_root` in the (VG), may result in kernel panic or upgrade failure upon reboot of the system. The cases may include iSCSI or re-using the hard drives.

In addition, it is possible for the system to go into kernel panic mode if the additional storage to `vg_root` VG is iSCSI-based storage.

Solution: Only a single instance of VG (`vg_root`) can exist. In case there are more instances, they must be removed. Failure to comply may result in kernel panic or upgrade failure.

Contact *Oracle Support* for assistance.

Error While Pairing Database Firewall With Audit Vault Server

Cause: An error OAV-46599: internal error Unable to remove data from previous pairing of this firewall with AVS is encountered while pairing Database Firewall which impacts registration of a newly installed Database Firewall with Audit Vault Server.

Workaround: Reboot Firewall and register Firewall again on the Audit Vault Server.

Missing Data File In The Archive Page Post Upgrade Of Oracle Audit Vault And Database Firewall

Cause: In case there are archive files in the Audit Vault Server that are not encrypted post upgrade followed by restore and release operations, it may result in missing data file.

Workaround:

1. Execute the encryption script. See section [Data Encryption on Upgraded Instances](#).
2. In case the archive files are remote, click **Set Tablespaces Available** on the Audit Vault GUI to encrypt the remote data file.
3. The data file is now listed on the archive page.

Unable To Remove Pre-Upgrade RPM

Cause: It may not be possible to remove the pre-upgrade RPM if there are open SSH connections on the appliance.

Workaround: Close all the open SSH connections and attempt to remove the pre-upgrade RPM.

Host Monitor Selects Wrong Net Device On Windows With Multiple Preferred

Host Monitor might choose incorrect network device if multiple preferred devices exist.

This can occur when the default network adapter that the host monitor uses (of type Intel(R) PRO/1000 MT Network Adapter) is for the wrong network.

Workaround:

Change the network adapter the host monitor uses so that traffic is captured from the correct network for the target. Follow these steps:

1. Check the Host Monitor log file and look for a section similar to:

```
The selected network device for capturing is:  
\Device\NPF_{22E6D6FF-43E2-4212-9970-05C446A33A35}. To change the device  
update the network_device_name_for_hostmonitor attribute at Collection  
Attributes to any one value from the list:  
\Device\NPF_{17C832B3-B8FC-44F4-9C99-6ECFF1706DD1},  
\Device\NPF_{22E6D6FF-43E2-4212-9970-05C446A33A35},  
\Device\NPF_{60611262-3FCC-4374-9333-BD69BF51DEEA} and restart the trail
```

This indicates which device is being used, and which devices are available. For more information on the available devices, you can run the host monitor in debug mode.

2. In the Audit Vault Server console, **Targets** tab, click the target you want.
3. In the Modify Collection Attributes section, **Attribute Name** field, enter:

```
network_device_name_for_hostmonitor
```

4. In the **Attribute Value** field, enter the device name. For example:
`\Device\NPF_{17C832B3-B8FC-44F4-9C99-6ECFF1706DD1}`
5. Click **Add**, and then **Save**.
6. Restart the audit trail for this target.

Note

Alternatively follow the steps documented in section Create a Network Audit Trail for Windows hosts in Administrators Guide.

Custom Collection Plugin Packaged on Windows Does Not Work on Linux

The `avpack` plug-in that is packaged on Windows does not work on Linux. In other words, you cannot run the `avpack` plug-in on Linux after you have packaged it on Windows. To produce this error:

1. Download the Oracle AVSDK on Windows.
2. Package the plug-in on Windows.
3. Deploy the plug-in on Oracle AVDF.
4. Install an Oracle AVDF Agent on Linux.

5. Start an audit trail for this Linux host. However, the audit trail cannot start.

Workaround: If you want to run the Agent and audit trail collection on Linux, then package the plug-in on Linux, not on Windows. If you package the plug-in on Linux, then Agent and audit trail collection can run on either Linux or Windows.

Microsoft SQL Server Extended Events Collector is in Unreachable State

Learn how to fix the issue when Microsoft SQL Server extended events collector is in `UNREACHABLE` state.

Issue

In case the size of the extended events file is more than 400 MB, then during recovery of the audit trail or when stopping the trail, may leave the collector in `UNREACHABLE` state for a short duration.

Workaround

Enable only the necessary events in the extended events session of the target database. Maintain the extended events file in smaller size (not exceeding 400 MB).

Recovery Issues in Microsoft SQL Server Extended Events Collector

Learn about recovery issues in Microsoft SQL Server collector.

Issue

In case there are extended events with same event timestamp, and if all the fields are the same between the events, then only one of the event is collected by Oracle AVDF during recovery and others are omitted.

Workaround

None.

Audit Data Collection Issue in Microsoft SQL Server Event Log

Learn how to fix audit data collection issue in Microsoft SQL Server.

Issue

Audit data collection issue from the event log is observed in Oracle AVDF releases 20.4 and 20.5. Audit events with Event ID 33205 are not being collected by the SQL collector.

Workaround

This issue is fixed in Oracle AVDF release 20.6 and later. Upgrade to Oracle AVDF 20.6 and later at the earliest.

In Oracle AVDF release 20.5, apply the patch available in *MOS Note Doc ID 24676845*.

Unable to Use the Audit Vault Server Console to Associate a Standby Audit Vault Server with a Database Firewall for High Availability

Learn how to associate a standby Audit Vault Server with the Database Firewall when the primary Audit Vault Server is already registered with a Database Firewall.

Issue

When pairing an Audit Vault Server with another Audit Vault Server for high availability, if the Database Firewall is already registered with the potential primary Audit Vault Server, there is no way to use the Audit Vault Server console to configure the standby Audit Vault Server in the firewall.

Workaround

1. Connect to the Database Firewall appliance through SSH and switch to the *root* user.

```
su - root
```

2. Copy the server certificate to the Database Firewall appliance using one of the following options.

If the Audit Vault Server is not yet paired with another Audit Vault Server, follow these steps:

- a. Log in to the standby Audit Vault Server console as an administrator.
- b. Select the **Settings** tab.
- c. Select the **Security** tab in the left navigation menu.
- d. Select the **Certificate** tab on the main page.
- e. Click **Copy Certificate** on the **Server Certificate** subtab.
- f. Copy the server certificate of the Audit Vault Server into a file on the Database Firewall appliance.

If the Audit Vault Server is already paired, follow these steps:

- a. Log in to the primary Audit Vault Server console as an administrator.
- b. Select the **Settings** tab.

- c. Select the **System** tab in the left navigation menu.
 - d. Click **High Availability** in the **Configuration** section.
 - e. Copy the standby server certificate of the Audit Vault Server into a file on the Database Firewall appliance.
3. Run the following command on the Database Firewall appliance:

```
/opt/avdf/config-utils/bin/config-avs set avs=secondary address=<IP address of standby Audit Vault Server> certificate=<location of certificate>
```

Error OAV-47842 When Changing the IP Address for the Database Firewall

Learn how to resolve error OAV-47842 when trying to change the IP address for the Database Firewall.

Issue

When monitoring points are enabled and you try to change the IP address for the Database Firewall, the following error appears:

```
OPERATION FAILED OAV-47842: DATABASE FIREWALL (FW91) REPORTED AN ERROR. THE NETWORK DEVICE &#x27;ENPOS3&#x27; USED BY EP: [1, 2].
```

Workaround

If any monitoring points are associated with this firewall, stop them first and then try to change the IP address of the Database Firewall. See [Starting, Stopping, or Deleting Database Firewall Monitoring Points](#).

Transaction Log Audit Trail Before-After Report Issues with CSV Format

Learn how to resolve issues with the transaction log audit trail before-after report in CSV format.

Issue

When downloading the CSV report from the Audit Vault Console UI, the before-after data does not download.

Workaround

Before downloading the CSV report, click the **Actions** menu and select **Select Columns**. Move the **Column Name**, **Old Value**, and **New Value** columns to the **Display in Report** box below the **Data Modification** column.

Error with Gateway Value Not Showing and Not Being Updated in Database Firewall Network Settings

Issue

The IP value for the gateway field in the Database Firewall Network Settings does not save save properly and remains blank.

Workaround

As a root user on the Database Firewall execute following command: `config-route set device=NICNAME gateway=GATEWAY`. After executing the command the Database Firewall gateway will be changed, but the gateway field will remain blank in the Audit Vault Server UI.

For example,

```
/opt/avdf/config-utils/bin/config-route set device=enp0s3  
gateway=192.168.0.1
```

In a High Availability Environment, Audit Vault Server GUI Is Not Accessible After Reboot of Standby Audit Vault Server

Issue

In a high availability environment, Audit Vault Server GUI is not accessible after reboot of standby Audit Vault Server.

Workaround

1. Check the status of the database, listener, httpd, and ords services on the primary Audit Vault Server. All these services should be up/active. Run all the commands as the `root` user on the primary Audit Vault Server.

```
systemctl status dbfwdb  
systemctl status dbfwlistener  
systemctl status httpd  
systemctl status ords
```

2. Check the status of the database and listener services on the standby Audit Vault Server. Both services should be up/active. Run all the commands as the `root` user on the standby Audit Vault Server.

```
systemctl status dbfwdb  
systemctl status dbfwlistener
```

3. If any of the services on the primary or standby servers are down, start the service(s) by running the following command as the `root` user on the respective server.

```
systemctl start <service name>
```

- Check the status of the service again to confirm it's up.

```
systemctl status <service name>
```

4. Once all the services are up, try to access the GUI. If the GUI is accessible, the issue is resolved and there is no need to complete the remaining steps. If the GUI is still not accessible, login to the primary Audit Vault Server as the `oracle` user and run the following command:

```
dgmgrl /
```

The `dgmgrl` command prompt will start.

5. In the prompt, run the following command to check the configuration:

```
show configuration verbose;
```

If the configuration shows the following error, continue with the remaining steps, otherwise contact Oracle Support.

```
Potential Targets: "DBFWDB_HA<N>"
DBFWDB_HA<N> invalid - member is disabled
OR
DBFWDB_HA<N> - (*) Physical standby database (disabled)
ORA-16906: The member was shutdown.
```

For example:

```
Potential Targets: "DBFWDB_HA2"
DBFWDB_HA2 invalid - member is disabled
OR
DBFWDB_HA2 - (*) Physical standby database (disabled)
ORA-16906: The member was shutdown.
```

6. Get the primary database name from the `dgmgrl` configuration output from step 5. The configuration will have an entry like

```
DBFWDB_HA<N> - Primary database.
```

For example:

```
DBFWDB_HA1 - Primary database.
```

7. Run the following command on `dgmgrl` command prompt:

```
show database <Primary Database>;
```

For example:

```
show database DBFWDB_HA1;
```

If the above command shows the following error, continue with the remaining steps, otherwise contact Oracle Support.

```
Database Error(s):
  ORA-16820: fast-start failover observer is no longer observing
this database
Database Warning(s):
  ORA-16735: primary redo generation suspended
```

8. Enable the standby database, which is listed in the potential targets from the configuration output from step 5. To do this, run the following command on `dgmgrl` prompt:

```
enable database <Standby Database>;
```

For example:

```
enable database DBFWDB_HA2;
```

9. Wait for five minutes, after this the GUI should be accessible. If the GUI is still not accessible, contact Oracle Support.

Error messages in `/var/log/messages` for Oracle AVDF 20.9

Issue

When you run diagnostics on the **Diagnostics** page, the output shows the following errors in the `/var/log/messages`:

```
systemd[1]: Starting acfssihamount.service...
acfssihamount[908]: Unable to locate Oracle binaries, exiting...
systemd[1]: acfssihamount.service: Control process exited, code=exited
status=1
systemd[1]: acfssihamount.service: Failed with result 'exit-code'.
systemd[1]: Failed to start acfssihamount.service.
```

For more information on the **Diagnostics** page, see [Managing Diagnostics](#).

Workaround

These errors have no impact on your Oracle AVDF system. Continue using your Oracle AVDF system as normal.

"Start At Does Not Match Format" Message When Scheduling or Retrieving Jobs in Oracle AVDF 20.9

Issue

If you're using the Audit Vault Server console and your browser is set to any language other than English, you might see the following message when you schedule or retrieve a job for a target on the Schedule Retrieval Jobs page.

"Start At does not match format DS HH12:MI:SS AM."

This message prevents you from saving your changes. It appears when one or more jobs are already scheduled and you attempt to schedule or retrieve any job on this page. For example, if an audit policy job is already scheduled and you attempt to retrieve a user entitlements job immediately, you might see this message.

Workaround

1. Log in to the Audit Vault Server console as an auditor.
2. Click the **Targets** tab.
3. Click the **Schedule Retrieval Jobs** icon for the target.
4. On the Schedule Retrieval Jobs page, complete the following steps under each section that already has a scheduled job.

If a job is scheduled, it has a date in the **Next Scheduled Run** field.

- a. Select **Create/Update Schedule**.
 - b. If you see the "Start At does not match format DS HH12:M1:SS AM" message, then select a new date in the **Start At** field, and click **Close**.

You can select any date because you don't need to save the changes.
 - c. Deselect **Create/Update Schedule**.
5. Repeat the preceding steps for each section that already has a scheduled job.
 6. Proceed with scheduling or retrieving the job that originally resulted in the error. When you click **Save**, the error should no longer appear.

Download and Run Target Setup Scripts Only for Auditing Oracle Database

Issue

When you're configuring an Oracle Database target in the Audit Vault Server console and you click the **Target Setup Script** button, a dialog box displays the following message:

"Download and execute target setup script only for Oracle Database user."

You only need to download and run the target setup script for auditing Oracle Database targets. The scripts aren't required for Database Firewall monitoring.

Workaround

If you plan to configure auditing for the Oracle Database target, click **OK** in the dialog box and download the scripts. Otherwise, click **Cancel**.

Data Retention UI Error

Issue

After submitting any of the retrieve, move to remote, or release jobs on Data Retention page, the Data Retention page may throw UI errors:

```
ORA-01187: cannot read from file because it failed verification tests  
ORA-01157: cannot identify/lock data file 4 - see DBWR trace file
```

Workaround

Please refresh the page and then check the status of the submitted job in the **Jobs** page. To view the jobs page:

1. Click the **Settings** tab.
2. Click the **Jobs** tab in the left navigation.

Upgrade of Standby Audit Vault Server Delaying and Causing Errors

Issue

The upgrade of the standby Audit Vault Server (AVS) never completes and the following message is the last update in the `/var/log/debug` file in the standby AVS:

```
DEBUG - secure_sql_privs: System altered.  
DEBUG - secure_sql_privs:  
DEBUG - Stopping managed recovery process
```

Workaround

Run the following steps on the standby AVS:

1. Login as the `root` user.

2. Switch to oracle user.

```
su - oracle
```

3. Run:

```
sqlplus / as sysdba  
shutdown abort;  
exit;  
/usr/local/dbfw/bin/dbfwdb restrict
```

4. Switch to the root user:

```
su - root
```

5. Run:

```
/opt/avdf/bin/privmigutl --resume --confirm
```

Error `ORA-00001` When Creating Sensitive Object Sets in Data Discovery

Issue

When creating a Sensitive Objects Set in Data Discovery, after selecting the target, some categories are selected by default and sensitive objects are loaded accordingly. But it may take time to load sensitive objects and if you select more categories while the sensitive objects are loading, then the following error is thrown: `Ajax call returned server error ORA-00001: unique constraint.`

Workaround

You need to wait until the sensitive objects are loaded before selecting more categories.

Install/Uninstall of Pre-Upgrade RPM Gives "Database not mounted" Error

When patching to the most recent RU pre-upgrade RPM file needs to be installed and uninstalled as per [Run the Pre-upgrade RPM](#). When patching from Oracle AVDF 20.3 to 20.10 the uninstallation of the Pre-Upgrade RPM file causes a "Database not mounted" error.

Problem

When patching from Oracle AVDF 20.3 to 20.10 the installation and uninstallation of the Pre-Upgrade RPM file causes a "Database not mounted" error.

Workaround

Reboot the system after uninstalling the pre-upgrade RPM file to bring back the services to normal.

During Installation and Upgrade Database User `ORDS_PUBLIC_USER` Gets Locked

Problem

Intermittently during install and upgrade of Oracle AVDF `ORDS_PUBLIC_USER` database user account gets locked resulting in this error in the web UI:

"The username or password for the connection pool named [default|lo], are invalid, expired, or the account is locked".

Workaround

Rotate the password of the `ORDS_PUBLIC_USER` database user before it expires

See [Rotating the ORDS_PUBLIC_USER User Password](#) in the *Oracle Audit Vault and Database Firewall Administrator's Guide*.

If `ANONYMOUS` Password is Changed, Expired, or Account is Locked Then The Audit Vault Server UI Can't Be Accessed

Problem

In Oracle AVDF 20.7-20.10 the Audit Vault Server UI can't be accessed if `ANONYMOUS` password is changed, expired, or account is locked.

Workaround

Rotate the password of the `ANONYMOUS` user before it expires.

-
- [Oracle AVDF 20.7 and 20.8](#)
 - [Oracle AVDF 20.9 and 20.10](#)

Oracle AVDF 20.7 and 20.8

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.
See [Logging In to Oracle AVDF Appliances Through SSH](#).
2. Unlock the `ANONYMOUS` account.

- a. Switch to the `dvaccountmgr` user.

```
su - dvaccountmgr
```

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

```
sqlplus /
```

- c. Run the following command to unlock `ANONYMOUS`:

```
alter user ANONYMOUS identified by <New Password> account unlock;
```

- d. Exit SQL*Plus.

```
exit
```

3. Switch to the `root` user.

```
su - root
```

Note

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

4. Run the following commands:

```
systemctl stop monitor
systemctl stop ords
systemctl stop dbfwdb
systemctl start dbfwdb
systemctl start ords
systemctl start monitor
```

Oracle AVDF 20.9 and 20.10

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

See [Logging In to Oracle AVDF Appliances Through SSH](#).

2. Unlock the `ANONYMOUS` account.

- a. Switch to the `dvaccountmgr` user.

```
su - dvaccountmgr
```

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

```
sqlplus /
```

- c. Run the following command to unlock ANONYMOUS:

```
alter user ANONYMOUS identified by <New Password> account unlock;
```

- d. Exit SQL*Plus.

```
exit
```

3. Navigate to the directory of the `apex.xml` file.

```
cd /var/lib/oracle/ords/conf/ords/conf
```

4. Update the `apex.xml` file with the same password, adding `!` before the password string. The password will be encrypted after restarting the services.

```
<entry key="db.password">!<New Password></entry>
```

5. Switch to the `root` user.

```
su - root
```

 **Note**

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

6. Run the following commands:

```
systemctl stop monitor
systemctl stop ords
systemctl stop dbfwdb
systemctl start dbfwdb
systemctl start ords
systemctl start monitor
```

Security Assessment Excel Reports Fail to Generate

Issue

In Oracle AVDF 20.9 the below security assessment Excel reports failed to generate if they contained more than 32,767 characters:

- Security Assessment Detailed Report
- STIG Security Assessment Report
- GDPR Security Assessment Report

Solution

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See [Patching Oracle Audit Vault and Database Firewall Release 20](#).

When Browser Language is Set to Spanish, the Option to Enable or Disable FIPS 140-2 is Not Available For the Database Firewall

Issue

For AVDF 20.10 when the internet browser language is set to Spanish, the pop-up dialog where you typically enable or disable FIPS 140-2 on your Database Firewall does not contain the checkbox required to make the selection.

Workaround

Set your internet browser to a different language when enabling or disabling FIPS 140-2 on your Database Firewall.

Insufficient Space Error in / File System Reported by Pre-upgrade RPM

Learn how to fix insufficient space error issue in the / file system reported by pre-upgrade RPM.

Problem

An error similar to the below message is observed when running pre-upgrade RPM. There is insufficient space in the / file system.

```
Checking upgrade preconditions
This upgrade requires at least 2.35GiB free on / (actual: 2.29GiB)
```

```
AVDF::Installer::Upgrade::InvalidPreconditions
```

```
Precondition: 'space-check.rb'
```

```
Result: 'Please follow the instructions in the Administrator's
Guide to add storage, then retry.'
```

```
Summary: AVDF::Installer::Upgrade::InvalidPreconditions
```

```
System is not ready for upgrade.
```

Solution

Extend / using the free space from `vg_root`:

```
lvextend --resizefs -L+2.35G /dev/vg_root/lv_ol8root
```

Receiving Error OAV-46502 When Registering a Target and Creating a Monitoring Point with a Named Network Interface Card Issue

You may encounter the error `OAV-46502: NULL IN TRAFFIC SOURCES` when registering a target and creating a monitoring point with a named network interface card (NIC) in Oracle AVDF 20.10.

Workaround

To avoid this issue, perform one of the following workarounds:

- If you're using the UI to register a target and create a monitoring point, remove the NIC name.
- Use AVCLI commands to register a target and create a monitoring point.
[Register a Target Using AVCLI](#)
[Create a Monitoring Point Using AVCLI](#)
- Use separate workflows for registering a target and creating a monitoring point. You will have to save after successfully registering a target and prior to creating a monitoring point.
[Registering Targets](#)
[Creating and Configuring a Database Firewall Monitoring Point](#)

Fix

1. Go to My Oracle Support and sign in.
2. Click the **Patches & Updates** tab.
3. Use the **Patch Search** box to search for the patch.
 - a. Click the **Product or Family (Advanced)** link on the left.
 - b. In the **Product** field, enter *Oracle Audit Vault and Database Firewall*.
 - c. In the **Release** field, select the 20.10 Oracle AVDF release from the drop-down list.
 - d. Click **Search**.
4. In the **Patch Name** column of the search results, click the link for the 35861954 patch number.
5. Click **Download**.

6. Download and extract the contents of the `p35861954_2010000_Linux-x86-64.zip` file.

Error Indicating Passwords Do Not Match In SMTP Settings

Attempting to save password in SMTP settings results in an error due to Bug 34349964. To resolve this error, upgrade to AV 20.8 to successful save the SMTP settings.

Issue

This issue arises while trying to save Simple Mail Transfer Protocol (SMTP) settings, when attempting to configure an SMTP server. Users are logged in as `AVADMIN` and click the **Settings** tab. In the left navigation menu, they click **System**; under **Configuration**, click **Connectors**. Further details related to this process can be found at [Configuring Email Notifications](#). After entering the necessary details, the SMTP server is registered successfully, however, after entering password and clicking save, an error arises: `Passwords do not match`.

Workaround

This issue is only present in Oracle AVDF release 20.7.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See [Patching Oracle Audit Vault and Database Firewall Release 20](#).

Starting with AVDF 20.10, the Upgrade or Installation Will Fail with Oracle Linux 6

Upgrading the Audit Vault Server to 20.10 or later or installing the Host Monitor Agent will fail if using Oracle Linux 6.

Issue

[Oracle Linux 6](#) was deprecated in Oracle AVDF 20.10, and it will be desupported in one of the future releases.

Because of this, upgrading the Audit Vault Server to 20.10 or later or installing the Host Monitor Agent will fail if using Oracle Linux 6.

Workaround

To prevent this issue, apply patch 36286507 before upgrading the Audit Vault Server to 20.10 or later or during Host Monitor Agent installation.

Related Topics

- Behavior Changes, Deprecated, and Desupported Platforms and Features

ORA-22835 Error During Upgrade of Audit Vault Server to Version 20.3

When upgrading the Audit Vault Server to 20.3, users may encounter the following error: "ORA-22835: Buffer too small for CLOB to CHAR or BLOB to RAW conversion."

Issue

When upgrading to AVS version 20.3, users may encounter the ORA-22835: Buffer too small for CLOB to CHAR or BLOB to RAW conversion error caused by the changeset_191016_ZUJYPYZENY migration.

Workaround

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See [Patching Oracle Audit Vault and Database Firewall Release 20](#).

If encountering the above error, it is recommended to restore from the upgrade or revert to a before-upgrade snapshot. Consider upgrading to Oracle AVDF version 20.4 instead of 20.3.

To recover from the upgrade failure, complete the following steps:

1. Edit `/usr/local/dbfw/bin/migration/2019/changeset_191016_ZUJYPYZENY/database.sql` by commenting out all the lines in the file.
2. Add the following at the end of the file:

```
UPDATE avsys.fw_cluster SET representation=SUBSTR(representation,
1, 32767) WHERE LENGTH(representation) > 32767;
CREATE INDEX avsys.fw_cluster_rep_hash_idx ON
avsys.fw_cluster(ora_hash( CAST(representation AS
VARCHAR2(32767)) ));
```

3. Complete the database migration by running as root:

```
/opt/avdf/install/privileged_migration/database-migrations.rb
```

4. Complete the AVS upgrade procedure by running as root:

```
/opt/avdf/bin/privmigutl --resume --confirm
```

Note

It is recommended to run the commands directly from the terminal console to avoid errors due to SSH session timeout or broken network connectivity.

AVDF 20.3-20.6 Character Limit in Alert Condition Is Exceeded at 4,000 Characters

Issue

In Oracle AVDF 20.3-20.6, the character limit in the **Condition** field when attempting to create alerts is restricted to 4,000 characters. This limit is lower than in previous versions such as Oracle AVDF 12.2. When attempting to create alerts, you may experience an error stating the character limit has been exceeded.

Solution

The character limit issue in the alert condition has been resolved in Oracle AVDF 20.7 and later.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See [Patching Oracle Audit Vault and Database Firewall Release 20](#).

In 20.12 Pop-ups and Tooltips are Not Readable

When the browser language is set to country-specific English, then pop-ups and tooltips are not readable. Set the browser language to English (en) to resolve the issue.

Issue

Various confirmation pop-ups and tooltips show messages similar to `CNF_DEL_DB_MSG` when the browser language is set to country-specific English, for example, (en-us), (en-nz), or (en-ca).

Workaround

Set the browser's language to English (en) and reload the Audit Vault Server console.

Audit Collection for Autonomous Databases Throws `Failed to connect with db` Error

Issue

Audit Collection for Oracle Autonomous AI Database Serverless and Oracle Autonomous AI Database on Dedicated Exadata Infrastructure may fail with error.

Solution

Contact Oracle Support for a patch for Bug 36566154.

Upgrade Fails on OCI Appliances When Using iSCSI to Extend

`vg_root`

After extending file system storage based on the recommendations of the pre-upgrade RPM, the upgrade may still fail due to issues with the Internet Small Computer Systems Interface (iSCSI). To resolve the issue, remove the iSCSI attachments and replace them with para-virtualized attachments.

Issue

If the Oracle AVDF (20.1 - 20.8) appliance is on OCI and has an Oracle block volume using iSCSI as part of the `vg_root` volume group, it should not be upgraded to Oracle AVDF 20.9 or later as the upgrade will fail.

Workaround

To successfully upgrade to Oracle AVDF 20.9 or later, the iSCSI attachments must be removed and replaced with para-virtualized attachments. Oracle recommends taking a backup and restoring it on an appliance that has appropriately extended storage prior to starting the upgrade.

For more information see [Backup and Restore of Oracle AVDF Instances in OCI](#) in the *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Related Topics

- [Extending Storage](#)
- [Pre-upgrade RPM Warnings](#)

AVDF 20.3 Time Zone Issue

Issue

After successfully installing AVDF 20.3, the AVDF server time incorrectly displays as -5:30 hours, even when the time zone offset is correctly set to +5:30. This discrepancy causes event times to be incorrectly reported to the AV server.

From AVDF 20.3 to 20.7, the NTP Server time is not accurately reflected in AVDF reports. This issue occurs because event times are sent without time zone information, leading the AV server to interpret the local time as UTC, resulting in incorrect time storage.

Solution

The time zone issue has been resolved in Oracle AVDF 20.8 and later versions.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See [Patching Oracle Audit Vault and Database Firewall Release 20](#).

AVDF 20.6: Configuring Custom Ports Fails

Symptoms

In Oracle AVDF 20.6, changing custom ports from ports 1521 (TCP) to port 1522 (TCPS) does not work. As a result, the AV listener is found to be inactive due to protocol adapter error. This also causes the AV console to become inaccessible.

Cause

This error is caused by duplicate entries for the same ports (two for TCP and two for TCPS). There should only be one entry for each in `/var/lib/oracle/dbfw/network/admin/listener.ora`.

Solution

Adding a custom port twice would create duplicate entries in the `dbfw.conf` and `listener.ora` files, which can lead to operational failures. A bug fix has been implemented to prevent duplicate port entries.

This issue has been resolved in Oracle AVDF 20.7 and later versions.

To prevent this issue, apply the patch to update Oracle AVDF to the latest release update (RU). See [Patching Oracle Audit Vault and Database Firewall Release 20](#).

AVDF 20.11 - 20.13: Connecting to Listener Results in `ORA-28865:`

`SSL connection closed error`

Problem

In Oracle AVDF 20.11 - 20.13, when connecting to a TLS enabled Real Application Cluster (RAC) or Autonomous Database (ADB) targets through the Database Firewall, the connection fails with error `ORA-28865: SSL connection closed error`.

Cause

The Database Firewall only supports using a single cipher suite for the outbound connection to the target database, it doesn't support using a list of cipher suites.

Workaround

1. Find the `TLS_RAC_PROXY_OUTBOUND_USE_NS_CIPHERS` parameter in `/usr/local/dbfw/va/monitoring_point_number/etc/appliance.conf`.
To find the monitoring point number:
 - a. Log in to the Database Firewall through SSH and switch to the `root` user.
See [Logging In to Oracle AVDF Appliances Through SSH](#).

- b. Change to `/var/dbfw/va` directory.
- c. Identify the Database Firewall monitoring point by searching for the target name configured in the Audit Vault Server. Run the following command:

```
grep -lr <TARGET NAME> *
```

- d. Find the monitoring point number from the output which contains the name and path of the configuration file. For example: `1/etc/appliance.conf`. In this example, 1 is the monitoring point number.
2. Set the `TLS_RAC_PROXY_OUTBOUND_USE_NS_CIPHERS` parameter to 1:

```
TLS_RAC_PROXY_OUTBOUND_USE_NS_CIPHERS = "1"
```

3. Save the changes.
4. Restart the monitoring point.

Note

The outbound TLS cipher suite level chosen from AVDF console will not be considered after the above changes are applied. Rather the default set of ciphers supported by the operating system will be tried ordered from strongest to weakest.

Related Topics

- [Configuring Database Firewall Monitoring Points](#)

Upgrading 20.12 to 20.13 Fails on VMware With Error at Privileged Migrations Step

Learn how to resolve a privileged migrations error when upgrading from Oracle AVDF 20.12 to 20.13.

Problem

When upgrading from Oracle AVDF 20.12 to 20.13, the upgrade fails on VMware with the following error:

```
run-privileged-migrations ERROR - ODF-10001: Internal error: Fatal error running migrations
```

Solution

To resolve this issue, first confirm that you are experiencing the same error. If so, follow the subsequent steps:

1. As the `root` user, check the integrity of the RPM database:

```
cd /var/lib/rpm
/usr/lib/rpm/rpmd_verify Packages
```

If there are no errors, these instructions do not apply, contact Oracle Support.

2. If errors are found, execute the following commands to rebuild the RPM database:

```
cd /var/lib
cp -ax --backup=t rpm rpm.old
rm -i rpm/__.db.???
rpm --rebuilddb
```

3. Once you have rebuilt the RPM database, check the validity of the rebuilt package database:

```
cd /var/lib/rpm
/usr/lib/rpm/rpmdb_verify Packages
```

4. Once confirmed, proceed with the upgrade according to the specific type of RPM database corruption encountered. Follow the appropriate steps based on the scenario experienced:

- Resume the upgrade if the privileged migrations have not yet started:

- a. Reboot the system.
- b. Log in as the `root` user.
- c. Run the following command:

```
systemctl isolate avdf-upgrade.target
```

- d. To review the upgrade status, re-log in on the console as the `root` user.

- Resume the upgrade after the privileged migrations have started:

- a. Apply the AVDF 20.13 update to the recovery utility:

```
rpm -U /media/avdf-install/bootstrap/Packages/avdf-
bootstrap-20.13.0.0.0-*.noarch.rpm
```

- b. Check the current status:

```
/opt/avdf/bin/privmigutl --status
```

- c. Review the output to find the failing migration and re-run it manually as the `root` user.

- d. Once the migration has completed successfully, run the following command:

```
/opt/avdf/bin/privmigutl --resume
```

The Length of Password Expiry for the `AVS_DEFAULT` Profile and the STIG Setting Changes After Patching

After patching Oracle AVDF, the password for the `AVS_DEFAULT` profile will reset to expire after 90 days. STIG enablement setting also changes after patching. Follow these steps to revert these changes.

Issue

After patching Oracle AVDF, the `password_life_time` setting for the `AVS_DEFAULT` profile is set to 90 days. The `password_life_time` setting dictates how often, in days, the password for the `AVS_DEFAULT` profile needs to be changed. This impacts super administrator users.

Additionally, after patching Oracle AVDF, STIG guidelines are disabled.

Workaround

To update the password expiry length in the Audit Vault Server console:

1. [Log in to the Audit Vault Server Console](#) as a super administrator.
2. Click **Settings**.
3. Click the **Password Expiry** tab on the **Security** page.
4. Enter the new password expiry length.
Password expiry setting is applicable to both admin and auditor users.
5. Click **Change**.

To enable STIG guidelines see [Enabling STIG Guidelines on Oracle Audit Vault and Database Firewall](#).

Unable to Start Network Trail for MSSQL Database on Windows

Learn how to resolve a startup failure for the Host Monitor on Windows when OpenSSL 3 is installed instead of the expected OpenSSL 1.1 version.

Issue

The Host Monitor fails to start on a Windows system, even though it was installed as part of the AV Agent Installation.

Attempting to start the network trail manually using the command:

```
hostmanager command-start trailid=<trail id> stname=<target name>  
loglevel=debug
```

results in the following error:

```
The process can't start because libcrypto-1_1-x64.dll does not exist on
this computer.
```

Environment Clues:

- OpenSSL 3.1.4 is installed on the server (e.g., under C:\Program Files\FireDaemon OpenSSL 3\bin\).
- The libcrypto-3-x64.dll file exists, but the expected libcrypto-1_1-x64.dll is missing.
- The OpenSSL 3 path is included in the system's PATH environment variable.

Cause

The AV Agent expects OpenSSL 1.1, but OpenSSL 3 is installed. This incompatibility prevents the Host Monitor from starting correctly.

Workaround

Apply the patch provided for this issue:

1. Download Patch 36094288 for Oracle AVDF 20.9.
2. Follow the patch README instructions carefully, which include:
 - a. Applying the patch.
 - b. Reinstalling the AV Agent on the affected Windows server.

After patch application and re-installation, the Host Monitor should start successfully.

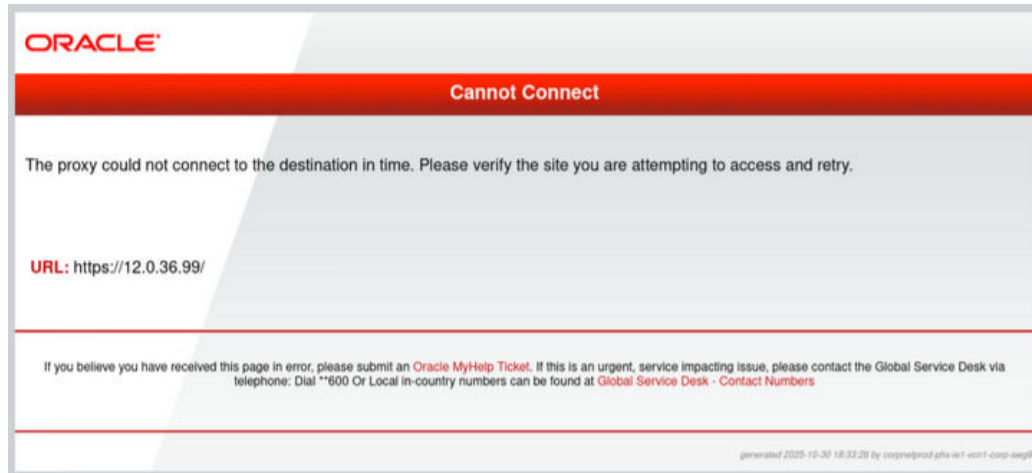
AVDF 20.16 High Availability Set Up Failure

When setting up AVDF 20.16 in high availability, an error is occurring due to the secondary Audit Vault Server not being in the same subnet.

Issue

A `Cannot Connect` error is shown when attempting to connect to the secondary Audit Vault Server. This is happening because the browser can't connect to the private IP despite the primary private IP forwarding happening correctly.

The error is displayed in the following image:



Solution

1. Create a VM on the same subnet as the primary Audit Vault Server.
2. Use a browser on this freshly created VM to connect the primary and secondary Audit Vault Servers.
Because the VM's are now on the same subnet, connection will succeed.

Encountering `ORA-06550` Error When Registering a Database With an Audit Vault Server from OCI Marketplace Image

Problem

When an Audit Vault Server is installed from the OCI Marketplace image, target database registration may fail with an `ORA-06550` error. It will be similar to:

```
OAV-46599: internal error ORA-06550: line 1, column 7: PLS-00352:
Unable to access another database 'database_name'
ORA-06550: line 1, column 7: PLS-00201: identifier 'database_name' must
be declared
ORA-06550: line 1, column 7: PL/SQL: Statement ignored
```

Solution

1. Log in to the Audit Vault Server through SSH and switch to the `root` user.
See Logging In to Oracle AVDF Appliances Through SSH.
2. Execute the following command:

```
/usr/bin/python3 /usr/local/dbfw/lib/python/avs/scripts/
update_avreportuser_user_password.py -FORCE
```

Once this script is executed, ORA-06550 will no longer occur when registering a target database.

Oracle Audit Vault And Database Firewall Release Notes, Release 20

E93406-29

Copyright © 2012, 2026, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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, MySQL, and NetSuite 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.