Oracle® Audit Vault and Database Firewall

Release Notes

Release 12.2.0

E49588-19

March 2021

Release Notes

These *Release Notes* contain important information about Oracle Audit Vault and Database Firewall (Oracle AVDF) Release 12.2.0.

This document contains these topics:

What's New in This Release

The following are new features in this release:

- A backup and restore utility for the Audit Vault Server has been integrated into the product.
- Audit trails will automatically start when the Audit Vault Agent is restarted or when Oracle AVDF is upgraded.
- The AVCLI command line utility can be used non-interactively by storing an administrator's credentials in the AVCLI wallet.
- You can configure Oracle Database In-Memory to speed up reports.
- New (full) installations of Oracle AVDF 12.2 will have all audit data encrypted using Oracle Database Transparent Data Encryption (TDE).
- When new audit trails collect data that is older than limits set in the retention (archiving) policy, that data will be automatically archived according to the policy.
- You can change the certificate for the Audit Vault Server and Database Firewall Web UIs.

- You can register hosts with a host name or a domain name.
- You can change the logging levels of system components from the Web UI.
- You can unlock user accounts from the Web UI.
- New reports have been added including: the Oracle Database Vault report, summary reports, IRS compliance reports, and reports that correlate database audit events with OS users that used `su` or `sudo` to execute commands.
- In the Administrator's Web UI, the Hosts tab has new Host Monitor details, and added Audit Vault Agent details.
- The Audit Vault Server's high availability pairing UI has been improved for usability.
- Support for IBM AIX secured targets has been added.
- The Oracle AVDF auditor can create an alert syslog template.
- The Oracle AVDF auditor can set a schedule for retrieval of audit data and entitlements from Oracle Database.
- We have added *Oracle Audit Vault and Database Firewall Concepts Guide* to the documentation library.
- Included important information on upgrade from `12.1` or older versions. See About Installing or Upgrading Oracle Audit Vault and Database Firewall (page 2) for complete information.

Upgrading Oracle Audit Vault and Database Firewall

You must download the executables for upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF) from My Oracle Support.

Topics:

About Installing or Upgrading Oracle Audit Vault and Database Firewall

This procedure contains information for installation or upgrade of Oracle Audit Vault and Database Firewall (Oracle AVDF) in a single-appliance environment and for a high availability environment.

> **Note:**
>
> 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 Installation Guide > Chapter 5 Upgrading Oracle Audit Vault and Database Firewall for complete information.

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

- The upgrade process preserves user accounts and passwords from the previous Oracle Audit Vault and Database Firewall installation.
- Oracle Audit Vault and Database Firewall versions 12.2.0.0.0 and above must first upgrade to 12.2.0.9.0, before upgrading to any later release in 12.2.
- Perform a single backup operation prior to performing the first upgrade.

The installer checks for the following conditions before it will allow the upgrade to complete:

- Compatibility with the currently installed version
- A minimum of at least 8 GB of memory. You can force the upgrade to complete if your system has a lower amount of memory (for example, 4 GB), because it is not difficult to extend memory for an Oracle Audit Vault and Database Firewall installation. However, Oracle Audit Vault and Database Firewall will send daily reminders to upgrade your system's memory.
- Space checks on available directory space. The upgrade process does not take into account the installed data. The space checks are a bare minimum below known failed upgrades. The space checks are as follows:

File System	Space Check
`/home`	100 MB
`/usr/local/dbfw`	200 MB
`/usr/local/dbfw/tmp`	7.5 GB
`/var/lib/oracle`	5.5 GB for Audit Vault Server 10 GB for Database Firewall
`/`	2 GB
`/tmp`	1.4 GB
`/var/dbfw`	100 MB
`/var/log`	100 MB
`/var/tmp`	5 GB

Step 1: Download the Upgrade Software and Instructions

Ensure you have the latest upgrade software before starting the upgrade. This software is in the latest available bundle patch.

Whether upgrading from an earlier release or applying a patch to the latest release, follow the detailed instructions in the README included with the upgrade software.

To download the upgrade software and README:

1. Go to My Oracle Support and sign in.
2. Click the **Patches & Updates** tab.
3. Use the **Patch Search** box to find the patch.
   a. Click the **Product or Family (Advanced)** link on the left.
   b. In the **Product** field, start typing `Audit Vault and Database Firewall`, and then select the product name.
   c. In the **Release** field, select the latest patch from the drop-down list.
   d. Click **Search**.
4. In the search results page, in the **Patch Name** column, click the number for the latest Bundle Patch.

   A corresponding patch page appears.
5. Click **Readme** to get the installation instructions.
6. Click **Download**.

   The File Download page appears.
7. Click **Download File Metadata**, and then **Download**, to save the metadata `.txt` file.

   You can use the data in this file to verify the patch file download.
8. Click the `.zip` file for the patch to download it.
9. In the next dialog, save the patch `.zip` file in a selected location.
10. Unzip the downloaded file to access the upgrade software (`.iso` file).

    The downloaded Oracle AVDF zip file contains the following files:

    - `avdf-pre-upgrade-12.2.0.11.0-1.x86_64.rpm`: This executable file is pre-upgrade check that you should install before beginning the upgrade. It checks if the system meets conditions for a successful upgrade, prepares the system by creating a volume to copy main upgrade ISO and installs the `avdf-upgrade` script. This script simplifies the upgrade process.
    - The following three ISO files, which include all the files that are required to perform the upgrade:
      - `avdf-upgrade-12.2.0.11.0-part1.iso`
      - `avdf-upgrade-12.2.0.11.0-part2.iso`
      - `avdf-upgrade-12.2.0.11.0-part3.iso`

- `readme_12.2.0.11.0.html`: This file contains detailed upgrade instructions for more complex upgrades, such as high availability.

11. Combine the three ISO files into one ISO file.
    - Microsoft Windows:

      ```
      copy /b avdf-upgrade-12.2.0.11.0-part1.iso+avdf-upgrade-12.2.0.11.0-
      part2.iso+avdf-upgrade-12.2.0.11.0-part3.iso avdf-upgrade-12.2.0.11.0.iso
      ```

    - Linux:

      ```
      cat avdf-upgrade-12.2.0.11.0-part1.iso avdf-upgrade-12.2.0.11.0-
      part2.iso avdf-upgrade-12.2.0.11.0-part3.iso > avdf-
      upgrade-12.2.0.11.0.iso
      ```

12. Generate an MD5 checksum file for the combined ISO files.
    - Microsoft Windows: Use the Microsoft File Checksum Integrity Verifier. You can download this tool from Microsoft Download Center
    - Linux:

      ```
      md5sum avdf-upgrade-12.2.0.11.0.iso
      ```

13. Ensure that the checksum file matches the following value:

    ```
    b2a709d49eb23930639de1b95bcdbab9
    ```

14. Use the metadata `.txt` file to verify the patch download.

Step 2: Back Up the Current Oracle AVDF Installation

Before upgrading or applying a patch update to Oracle Audit Vault and Database Firewall (Oracle AVDF), you must back up the following components:

- The Audit Vault Server database
- The Audit Vault Server appliance
- The Audit Vault Agent home directory

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide* for backup instructions.

Step 3: Install the Oracle AVDF Pre-Upgrade RPM

The `avdf-pre-upgrade-12.2.0.11.0-1.x86_64.rpm` executable checks the upgrade preconditions described earlier and prepares the system for upgrade by creating the `/var/dbfw/upgrade` directory with enough space to hold the main upgrade ISO file.

1. Log in to the Audit Vault Server through SSH as user `support`, and then switch user (`su`) to `root`.

2. Copy the `avdf-pre-upgrade-12.2.0.11.0-1.x86_64.rpm` executable from the download location to the appliance on which you want to perform the upgrade.

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-12.2.0.11.0-1.x86_64.rpm /root
   ```

3. Install the `avdf-pre-upgrade-12.2.0.11.0-1.x86_64.rpm` executable.

   ```
   rpm -i /root/avdf-pre-upgrade-12.2.0.11.0-1.x86_64.rpm
   ```

   The following message should appear:

   ```
   SUCCESS:

   The upgrade media can now be copied to '/var/dbfw/upgrade'.

   The upgrade can then be started by running:

     /usr/bin/avdf-upgrade
   ```

> **Note:**
>
> In case an error is encountered when running the pre-upgrade RPM, remove the package, correct the issue, and reinstall it again. Execute the following command to uninstall the pre-upgrade RPM package before installing again:
>
> ```
> rpm -e avdf-pre-upgrade-12.2.0.11.0-1.x86_64
> ```
>
> The above command successfully uninstalls the pre-upgrade RPM. Execute the pre-upgrade RPM install command again.

Step 4: Transfer the ISO File to the Appliance

The `avdf-upgrade-12.2.0.11.0.iso` file is the main upgrade ISO that is included.

1. Log in to the appliance as the Oracle AVDF `support` user.
2. Copy the `avdf-upgrade-12.2.0.11.0.iso` file as follows:

   ```
   scp remote_host:/path/to/avdf-upgrade-12.2.0.11.0.iso /var/dbfw/upgrade
   ```

Step 5: Start the upgrade script

The upgrade script mounts the ISO, makes changes to the correct working directory, executes the upgrade process, and then after the upgrade process is complete, it unmounts the ISO.

1. Log in to the Audit Vault Server through SSH as user `support`, and then switch user (`su`) to `root`.

   You must have `root` privileges to start the upgrade script.

2. Start the upgrade script as follows:

   ```
   /usr/bin/avdf-upgrade --confirm
   ```

Output similar to the following appears:

```
WARNING: power loss during upgrade may cause data loss. Do not power
off during upgrade.

Verifying upgrade preconditions
1/19: Mounting filesystems (1)
2/19: Allocating space for upgrade
3/19: Mounting new install root
4/19: Extracting minimal root filesystem
5/19: Mounting required filesystems (2)
6/19: Mounting required filesystems (3)
7/19: Creating mountpoints for ASM
8/19: Populating new root filesystem
9/19: Adding required platform packages
10/19: Adding preconditions for AVDF packages
11/19: Ensuring sufficient space on oracle filesystem
Extending oracle file system
12/19: Installing AVDF packages
13/19: Migrating configuration
14/19: Creating mountpoints for NFS
15/19: Installing ASM initscripts
16/19: Applying LVM adjustments
17/19: Migrating old root log files
18/19: Unmounting
19/19: Migrating old network log files
Remove media and reboot now to fully apply changes.
Unmounted /var/dbfw/upgrade/avdf-upgrade-12.2.0.11.0.iso on /images
```

Step 6: Restart the Appliance

After the upgrade is complete, you can restart the appliance and complete the upgrade.

1. Log in to the Audit Vault Server through SSH as user `support`, and then switch user (`su`) to `root`.
2. Restart the appliance. For example:

   ```
   reboot
   ```

   The restart process enables the upgrade to complete. When the appliance restarts, the pre-database and post-database migrations are run automatically. This process performs any system configurations that could not be completed when you ran the upgrade helper Step 5: Start the upgrade script (page 6). This process also removes the pre-upgrade `avdf-pre-upgrade-12.2.0.11.0-1.x86_64.rpm` executable, so you do not need to manually remove this file.

> **Note:**
>
> - Optionally the user may reset the Firewalls. The Audit Vault Server stores Firewall settings in the local repository. This can later be used for recovery purpose. To reset the Database Firewall:
>
> a. Log in to the Audit Vault Server console as an administrator.
>
> b. Click **Database Firewalls** tab.
>
> c. Click the name of the specific Database Firewall instance on the main page. The details are displayed.
>
> d. Click **Reset Firewall** button in the top right corner.
>
> - The **Reset Firewall** removes existing monitoring points and creates new ones using the configuration already stored on the Audit Vault Server. Those monitoring points not listed on the Audit Vault Server are removed. The captured data which is not processed is also deleted. The network setting of the Firewall is not altered. This action will also reset the Firewall ID. A Database Firewall is uniquely identified by a Firewall ID. This Firewall ID is derived from the Management Network Interface Card (NIC). Whenever the Network Interface Card is replaced, the Firewall ID must be reset.

3. If you have upgraded an Oracle Database Firewall, then re-register it on the Audit Vault Server.
   a. Log in to the Audit Vault Server as an Administrator.
   b. Select the **Database Firewalls** tab, click **Register**, and enter a name and IP address for the firewall. Then click **Save**.
   c. Click **Save**.

> **See Also:**
>
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for information about logging in to the Audit Vault Server.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information about registering a Database Firewall.

Step 7: Upgrade the Audit Vault Server Pair for High Availability

> **Note:**
>
> Do not change the primary and standby roles before completing the upgrade on both Audit Vault Servers.

To upgrade a pair of Audit Vault Servers configured for high availability:

1. Upgrade the standby Audit Vault Server.

   Follow the steps in "Upgrading Oracle Audit Vault and Database Firewall (page 2)", from Steps 1 through 6 to upgrade the standby (secondary).
2. After the standby Audit Vault Server is rebooted, ensure that it is up and running before proceeding to upgrade the primary Audit Vault Server.
3. Upgrade the primary Audit Vault Server.

   Follow the steps in "Upgrading Oracle Audit Vault and Database Firewall (page 2)", from Steps 1 through 6, to upgrade the primary.

After the primary Audit Vault Server is rebooted and is running, no additional reboot is needed. It should be fully functional at this point.

Step 8: Upgrade the Database Firewall Pair for High Availability

If you are updating a pair of Audit Vault Servers or Database Firewalls that are configured for high-availability, then you must upgrade both servers in the pair.

1. Follow the procedures in "Upgrading Oracle Audit Vault and Database Firewall (page 2)", from Steps 1 through 6, to upgrade the standby (secondary) Database Firewall.
2. Ensure that the standby Database Firewall has been restarted.
3. Swap this standby Database Firewall so that it now becomes the primary Database Firewall.
   a. Log in to the Audit Vault Server console as an Administrator.

      > **See Also:**
      >
      > *Oracle Audit Vault and Database Firewall Administrator's Guide* for information about logging in to the Audit Vault Server.

   b. In the Audit Vault Server console, select the **Database Firewalls** tab.
   c. Select **Resilient Pairs**.
   d. Select this resilient pair of firewalls, and then click **Swap**.

   The Database Firewall you just upgraded is now the primary firewall.
4. Follow the procedures in "Upgrading Oracle Audit Vault and Database Firewall (page 2)", from Steps 1 through 6, to upgrade the primary.

Downloading the Audit Vault and Database Firewall Documentation

> **See Also:**
>
> - http://www.oracle.com/pls/topic/lookup?ctx=avdf122 to download the most current version of this document, and the complete set of Oracle Audit Vault and Database Firewall documentation.
> - http://docs.oracle.com for documentation of other Oracle products.

Supported Secured Targets and Platforms

> **Note:**
>
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for the latest information on supported secured targets.
> - *Oracle Audit Vault and Database Firewall Installation Guide* to find the platform support information for the current release and for other releases.
>
> This information can also be found in the Article **1536380.1** at My Oracle Support.

Known Issues

This section lists the system's 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 UI, try running the same command using the `AVCLI` command line utility.

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.

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 of release `12.2.0.11.0`.

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.

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.

Pre-Upgrade RPM Process Failed Due To Patch Validation

Cause: The pre-upgrade RPM process failed during patch validation.

> **Note:**
>
> This issue is encountered only while upgrading to Oracle Audit Vault and Database Firewall release `12.2.0.9.0`.

Workaround:

1. Check for errors in the `/var/log/messages` file.
2. In case there are any errors with the tag `com.oracle.preBP9UpgradeAgentPatch.isPatchApplied`, then validate that Oracle Audit Vault and Database Firewall release `12.2.0.9.0` has been successfully applied.
3. Log in to the Audit Vault Server console. Verify that version is listed as `12.2.0.9.0`. This ensures that Oracle Audit Vault and Database Firewall release `12.2.0.9.0` has been successfully applied.
4. In case you still encounter this error, then contact Oracle Support.

Upgrade Process Failed Due To Patch Validation

Cause: The upgrade process failed during patch validation.

> **Note:**
>
> This issue is encountered only while upgrading to Oracle Audit Vault and Database Firewall release `12.2.0.9.0`.

Workaround: Check for errors in the `/var/log/messages` file. In case there are any errors with the tag `com.oracle.preBP9UpgradeAgentPatch.isPatchApplied`, then contact Oracle Support.

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 `lsof` 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.

Creating Entitlement Snapshot Labels After A Full Backup And Before An Incremental Backup Causes The Restore Operation Of Audit Vault Server From A Cold Incremental Backup To Fail With Missing Data

Cause: If you create Entitlement Snapshot Labels after a full backup of the Audit Vault Server and before an incremental backup operation, then when restoring Audit Vault Server from a cold, incremental backup, the restore operation fails with missing data. The missing data is from Audit Vault Server Entitlement Reports associated with labels created for Entitlement Snapshots.

Workaround: Do not create Entitlement Snapshot labels after a full backup and before an incremental backup operation. If you do so, perform a full backup operation to ensure this data will not be missing from the incremental backup operation.

"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. Install the diagnostic tool.
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 12.2.0.0.0 and later versions.

Solution: To install Oracle Audit Vault and Database Firewall 12.2.0.0.0 or a later version, 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 paring 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.

Problem Encountered While Installing Agent On Host Computer With Multiple Network Interface Cards

Cause: You may encounter a problem while installing the agent on a host computer with Multiple Network Interface Cards leading to Audit Vault Server.

Workaround:

- The administrator has to ensure that relevant routes are in place on the host machine in such a way that one network interface card leads to one Audit Vault Server.
- The administrator must configure the network and plan the routing table to accommodate multiple network interface cards. The network routing table determines how the packets are routed, their path, and the preferred network adapter. In case this is not effectively designed, then the agent installation may fail.

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.

RPM Error If Existing Installation Is Patched With Oracle Linux Errata

Cause: You may encounter RPM related issues if you are attempting to upgrade your existing Oracle Audit Vault and Database Firewall that is previously patched with Oracle Linux errata as detailed in MOS note **(Doc ID 2359424.1)**.

Workaround: Execute the below mentioned workaround as *root* user before upgrading your patched Oracle Audit Vault and Database Firewall release to the recent release:

Existing Release	Workaround Command Before Installing Pre-upgrade RPM
12.2.0.0.0	`mount /boot; rm -rf /boot/ initramfs-3.8.13-98.1.2.el6uek.x86_64.img; yum -y erase kernel-2.6.32-573.3.1.el6.x86_64; umount /boot`
12.2.0.1.0	`mount /boot; rm -rf /boot/ initramfs-3.8.13-118.3.2.el6uek.x86_64.img; yum -y erase kernel-2.6.32-573.12.1.el6.x86_64; umount /boot`
12.2.0.2.0	`mount /boot; rm -rf /boot/ initramfs-3.8.13-118.6.1.el6uek.x86_64.img; yum -y erase kernel-2.6.32-573.26.1.el6.x86_64; umount /boot`
12.2.0.3.0	`mount /boot; rm -rf /boot/ initramfs-3.8.13-118.8.1.el6uek.x86_64.img; yum -y erase kernel-2.6.32-642.3.1.el6.x86_64; umount /boot`

> **Note:**
>
> The above issue may not be encountered for Oracle Audit Vault and Database Firewall release `12.2.0.4.0` and onwards.

15963372: Agent Install Fails for agent.jar Downloaded With Internet Explorer

Agent install fails when `agent.jar` is downloaded from IE browser, with "Invalid or corrupt jarfile" error.

Workaround:

Use a different browser (such as Firefox) to download the `agent.jar` file, then run `java -jar agent.jar` again.

16868457: Agent Upgrade Fails if 12.1 Agent Has Deployed Custom Plug-ins

Agent upgrade fails if 12.1.0 Agent has deployed plug-ins.

Workaround:

Re-deploy the plug-ins, and then download and install the Agent again.

17862296: 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 secured 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, **Secured Targets** tab, click the secured 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 secured target.

18363490 - Audit Vault Agent Start Fails on Windows without Visual C++ 2010 Redistributable Package

Need to install Visual C++ 2010 Package to run Windows Agent.

Workaround:

Install Microsoft Visual C++ 2010 Redistributable Package to run the Audit Vault Agent on a Windows host.

18381322: Invalid Database Firewall Network Configurations Must Be Resolved Before Upgrade

Invalid DB Firewall network configurations should be resolved before upgrade.

This is relevant for users with Database Firewall and, in particular, Host Monitor Deployed. Before upgrading to 12.1.2 you should ensure that your Database Firewall configuration is valid.

Workaround:

Ensure that any enabled traffic sources on the Database Firewall have two ports in the traffic source.

Also ensure that any enforcement point in DPE mode is using an enabled traffic source.

18420068: oracle_user_setup.sql Asks to Add User to Data Dictionary Realm for Oracle Database Vault on Release 12c

Update `oracle_user_setup.sql` script to avoid using Oracle Data Dictionary realm for Database Vault.

This issue affects Oracle Database 12*c* secured targets that have Database Vault enabled. When using the Oracle Audit Vault and Database Firewall user setup script oracle_user_setup.sql, and running the script with `REDO_COLL` mode, the script outputs the following message, which does not apply to Oracle Database 12*c*:

```
Connect to the secured target database as DV Owner and execute:
exec dbms_macadm.add_auth_to_realm('Oracle Data Dictionary', 'C##USER1',
null,dbms_macutl.g_realm_auth_participant);
```

Workaround:

Ignore the above message if you see it when running the script for an Oracle Database 12*c*. Instead, execute the following on the database as `DV Owner`:

```
SQL> GRANT DV_STREAMS_ADMIN TO username;
```

For *username*, use the name of the account you created for Oracle Audit Vault and Database Firewall on this Oracle Database secured target.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide* for complete instructions on this setup script .

18636139: No UI Option to Remove Audit Vault Server HA Configuration

Provide option to remove HA configuration from UI.

Workaround:

This workaround is available starting with AVDF 12.1.1.4 (12.1.1 BP4).

To unpair two paired Audit Vault Servers:

1. Shut down the standby (secondary) Audit Vault Server.
2. Log in to the primary Audit Vault Server as `root`.
3. Run this command:

   ```
   sudo -u oracle /usr/local/dbfw/bin/setup_ha.rb --unconfigure
   ```

18948614: HA - After Failover AVSERVER Fails to Forward Syslog And Arcsight Messages

In a High Availability configuration, after a failover, Audit Vault Server does not forward `syslog` and Arcsight messages

Workaround:

1. Log in to the Audit Vault Server console as a super administrator.
2. Click the **Settings** tab, and then click **Connectors**.
3. In the **Syslog** section, and then click **Save**.
4. Scroll down to the **HP ArcSight SIEM** section, and then click **Save**.

20189422: Oracle Audit Vault and Database Firewall Installation Freezes After Disk Formatting Step

When you are installing Oracle Audit Vault and Database Firewall, the install screen may freeze after the disk formatting step. This issue can occur if you are trying to install Oracle Audit Vault and Database Firewall on hardware that does not match the exact Oracle Audit Vault and Database Firewall system requirement.

Workaround: Ensure that the hardware meets the requirements for installing Oracle Audit Vault and Database Firewall.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Installation Guide*

21117647: AUDIT/SU SUDO Reports Show Numbers for OSUSER Name for Deleted OS Users

The Linux collector has a limitation that affects the SU SUDO Audit report. The audit record contains the user ID, and the collector plugin gets the mapping of this user name from the `/etc/passwd` file that corresponds to the user ID for local users. It executes the command `getent passwd | grep` *`user id`* for LDAP/NIS users. If the user has been deleted from the system or the collector cannot access the mapping for the user ID, then the user ID (number) value is populated for the **USER_NAME** field in the Linux SU SUDO Transition report. The report displays **OSUSER NAME** as a number, that is, the user ID.

Workaround: None

21512210: 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, agent and audit trail collection can run on either Linux or Windows.

21838633: JAVA -JAR agent.jar Fails on Machines Which on Different Domain With AVSERVER

After you have installed the agent or upgraded the Oracle Audit Vault Server and it is restarted, the agent does not start. (The upgrade process should automatically restart the agent.) Errors similar to the following appear in the agent side log:

```
[2015-12-02T09:50:39.292+00:00] [agent] [ERROR] [] [] [tid: 10] [ecid:
1498028073:5013:1449049839300:0,0] Unexpected error occurred in thread
main[[java.lang.NumberFormatException: For input string: "Error occurred in
createFileFromBlob"
```

```
        at
java.lang.NumberFormatException.forInputString(NumberFormatException.java:48)
...
```

If you try to start the agent manually by running the `agentctl start` command, the following error appears:

```
Agent integrity check failed. Please upgrade the agent manually.
```

An error similar to the following appears in the agent log file:

```
[2015-12-02T10:38:06.482+00:00] [agent] [ERROR] [] [] [tid:
10] [ecid:1498028073:93254:1449052686488:0,0] Internal Error status:
-1, message :Agent validation failed. agentversion=[12.2.0.0.0],
serverversion=[12.2.0.0.0],hostversion=[12.1.2.5.0]
```

Workaround for failure during a fresh installation of the agent:

1. As the oracle user (log in as `support`, then `su root`, then `su oracle`), and then stop the Audit Vault Oracle Database server.

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

2. In the `/var/lib/oracle/dbfw/network/admin` directory, update the sqlnet.ora file to use the `sqlnet.recv_timeout = 1` setting.
3. As the oracle user, start the Audit Vault Oracle Database server.

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

4. Install the agent.
5. When the agent installation is complete, try starting the collection.

   The following error may appear:

   ```
   java.sql.SQLException: ORA-00604: error occurred at recursive SQL level 1
   ORA-01882: timezone region  not found
   ```

   If this error appears, then do the following:

   a. Stop the agent.
   b. Modify the `agentctl` file, located in the `./bin` directory, as follows, for `JAVA_OPTS`:

      ```
      add property -Doracle.jdbc.timezoneAsRegion=false
      ```

   c. Restart the agent.

Workaround for failure during an upgrade of the agent:

1. In the Audit Vault Console as an administrator, deactivate the host.

   Log in as an administrator, select the **Host** tab, and then click **Deactivate Host**.

2. Download a new `agent.jar` file from the upgraded Audit Vault Database Firewall server.
3. Activate the host from the Audit Vault console.
4. As the oracle user (log in as `support`, then `su root`, then `su oracle`), and then stop the Audit Vault Oracle Database server.

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

5. In the `/var/lib/oracle/dbfw/network/admin` directory, update the sqlnet.ora file to use the `sqlnet.recv_timeout = 1` setting.
6. As the oracle user, start the Audit Vault Oracle Database server.

   ```
   /usr/local/dbfw/bin/dbfwdb start
   ```
7. Install the agent in a new location or clean the files in the old agent location.
8. When the upgrade is complete, try starting the collection.

   The following error may appear:

   ```
   java.sql.SQLException: ORA-00604: error occurred at recursive SQL level 1
   ORA-01882: timezone region  not found
   ```

   If this error appears, then do the following:

   a. Stop the agent.
   b. Modify the `agentctl` file, located in the `./bin` directory, as follows, for `JAVA_OPTS`:

      ```
      add property -Doracle.jdbc.timezoneAsRegion=false
      ```
   c. Restart the agent.

22260134: Oracle AVDF: Old Primary Fails to Restart After Switchover

The previous primary database for Audit Vault Server fails to restart after the switchover operation. The following error appears, visible in the `/var/log/messages` file:

```
ORA-01102: Cannot mount database in EXCLUSIVE mode
```

Workaround: Restart the previous primary Audit Vault Server.

22351660 - AGENT HOST IS NOT REGISTERED WHEN MACHINE HAS MULTIPLE INTERFACES

Agent installation fails with `java -jar agent.jar -d $ORACLE_BASE/av_agent` error.

Workaround:

- The administrator has to ensure that relevant routes are in place on the host machine in such a way that one network interface card leads to one Audit Vault Server.
- The user must have sufficient privileges to the Management Interface to add hosts and assign IP addresses.
- The administrator must configure the network and plan the routing table to accommodate multiple network interface cards. The network routing table determines how the packets are routed, their path, and the preferred network

adapter. In case this is not effectively designed, then the agent installation may fail.

25207104 - ARCHIVE JOB HANGS AFTER THE ENCRYPTION SCRIPT EXECUTION

After upgrade the first archive or retrieve job submission may display the status as `Starting`.

Workaround:

Submit the job again. This is a known issue and subsequent submission of job succeeds.

Failure During High Availability Pairing in Oracle Audit Vault Server

Learn what to do when high availability pairinng in Oracle Audit Vault Server fails.

Problem

There may be some errors encountered while executing high availability pairing Oracle Audit Vault Server. The errors may be in stored script memory, failure to verify some of the files in the backup set, failure to verify some of the data files, and failure to read or create files.

Solution

Check if ILM archival was run before you perform the high availability pairing in Oracle Audit Vault Server. This is due to presence of archive files in the primary server.

To avoid this, ensure that you delete archive files from the primary Oracle Audit Vault Server and later run the high availability pairing.

25099312: Secured Target group created by avadmin cannot be seen by avauditor

The secured target group created by *avadmin* user is not visible to *avauditor* user. If *avauditor* attempted to create the group with the same name, it fails with the message `Group Already Exists.`

Workaround:

A secured target created by an *avadmin* user cannot be viewed or recreated by an *avauditor* user. Use a different name to create the secured target group.

Bugs Fixed In Release 12.2.0.0.0

Table 1-1 (page 24) lists bugs fixed in this release.

Table 1-1 Bugs Fixed In Release 12.2.0.0.0

Bug Number	Description
21178040	ALERT EMAIL NOTIFICATIONS ARE RESENT WHENEVER JAVA FRAMEWORK RESTART
21110266	DE-SUPPORT WINDOWS 2003 FOR AVDF AGENT
21043775	EZTABLE COLLECTOR PLUGIN DOES NOT WORK WITH TIMESTAMP WITH LOCAL TIME ZONE
20865266	DV REPORT - MAP OUR TARGET_OBJECT TO DV'S TARGET_OBJECT:ACTION_TARGET_OBJECT
20669301	START AGENT IN STOPPED STATE
20560732	ORCL COLLECTOR: EVENTLOG TRAIL DOES NOT START ON WINDOWS PLATFORM
20551923	UNIFIED AUDIT TRAIL DOES NOT COLLECT ALL DATABASE VAULT EVENTS
20529504	TRAIL STOPS WITH EXCEPTION FOR EVENTLOG TRAIL TYPES
20519073	NLS: WINDOWS: START AGENT FAILS AFTER DEACTIVATE/ ACTIVATE HOST
20476030	AVDF : COLLECTOR STOPS WITH ORA 12899 ERROR
20304150	DATABASE VAULT ACTIVITY CAN NOT SHOW DATA COLLECTED FROM DVSYS.AUDIT_TRAIL$
19685004	DATA MODIFICATION BEFORE-AFTER VALUES REPORT TIMING OUT
19592979	A HOST IN RUNNING STATE IS ALLOWED TO BE ALTERED.
19585084	ADD TERMINAL COLUMN IN EVENT_LOG TABLE.
19521326	CANNOT REGISTER SQL SERVER ST WITH SSL PARAMETERS IN CONNECT STRING
19184532	DROP LOGIN EVENT COLLECTED BY THE COLLECTOR DOES NOT HAVE PROPER MAPPING
18535118	AGENTCTL BATCH FILE CHECK FOR JAVA VERSION NOT PROPER AND NEED TO BE UPDATED

Documentation Accessibility

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

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/

lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle® Audit Vault and Database Firewall Release Notes, Release 12.2.0
E49588-19