Oracle® Audit Vault and Database Firewall

Release Notes

Release 12.1.2

E27781-09

July 2014

These *Release Notes* contain important information about Oracle Audit Vault and Database Firewall Release 12.1.2.

This document contains these topics:

Downloading the Audit Vault and Database Firewall Documentation

You can download the most current version of this document, and the full set of Oracle Audit Vault and Database Firewall documentation, from the following website:

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

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

`http://docs.oracle.com`

Upgrading to Oracle AVDF 12.1.2 from a Previous Release

You can upgrade to Oracle AVDF version 12.1.2.1.0 (Bundle Patch 1) from all Oracle AVDF versions up to, and including 12.1.1.4.0, and from version 12.1.2.0.0. However, you can not upgrade from a subsequent 12.1.1 bundle patch, for example 12.1.1.5.0, if it was released after version 12.1.2.1.0 (Bundle Patch 1). To upgrade from such a bundle patch, please contact Oracle Support to obtain the most recent bundle patch for AVDF 12.1.2.

Supported Secured Targets and Platforms

You can find the latest information on supported secured targets and platforms in *Oracle Audit Vault and Database Firewall Administrator's Guide*, and in Article **1536380.1** at the following website:

`https://support.oracle.com`

ORACLE

What's New in this Release

The following are new features in this release:

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

Known Issues

Table 1 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. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for a command line reference.

Table 1 Audit Vault and Database Firewall Known Issues

Bug Number	Description

18850821	Syslog (audit trail) collector does not work for systems with rsyslog
	This affects Oracle secured targets running on computers on Oracle Linux 6 (OEL6) platforms.
	Workaround:
	1. Set the following parameters in the `/etc/rsyslog.conf` file:
	`# Use default timestamp format`
	`$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat`
	2. Start syslog audit trails using the full path to the syslog files. For example, when configuring a syslog audit trail in the Audit Vault Server console, in the **Trail Location** field, provide a full path such as `/usr/local/syslog*`.
	If you are using AVCLI, you can execute a command such as the following:
	`avcli> START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM syslog /usr/local/syslog*;`

18948614	HA: After failover Audit Vault Server fails to 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**.
18899700	Agent install throws message "`/BIN/ENV NO SUCH FILE OR DIRECTORY`" You can ignore this message as it has no impact on Agent installation.
18636139	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`

Table 1 (Cont.) Audit Vault and Database Firewall Known Issues

Bug Number	Description

18404241	AVS HA - Under heavy load the standby and primary Audit Vault Server databases may freeze.
	
	The following error messages will first appear on the standby Audit Vault Server, and some time later (depending on traffic) on the primary server:
	
	`ORA-16038: log 2 sequence# 3505 cannot be archived`
	`ORA-19809: limit exceeded for recovery files`
	
	Workaround:
	
	To reduce the likelihood of this occuring - If the database is not yet in a blocked state, you can increase the Fast Recovery Area (FRA) size. The FRA size should be increased to about 25% of total available space on the RECOVERY disk group.
	
	If you expect a lot of data to be processed and the RECOVERY disk group is not used for any other purpose (like backups) then the FRA can be increased further.
	
	Example:
	
	`ALTER SYSTEM SET DB_RECOVERY_FILE_DEST_SIZE=100G SCOPE=BOTH;`
	
	To recover from a freeze - If the database is blocked, SSH to the standby Audit Vault Server, and using RMAN delete the oldest `archivelog` file:
	
	1. Run `RMAN` as `oracle` user and enter:
	
	`CONNECT TARGET /;`
	`LIST ARCHIVELOG ALL;`
	
	2. From the above list, copy the sequence number of the oldest `archivelog` file and run:
	
	`DELETE ARCHIVELOG UNTIL SEQUENCE` *`oldest_sequence_number`*`;`

18363490	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 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.

Table 1 (Cont.) Audit Vault and Database Firewall Known Issues

Bug Number	Description

18420068	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 AVDF 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 AVDF on this Oracle Database secured target.
	
	For full instructions on this setup script, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

18391942	Online help lists four disk groups in the Audit Vault Server repository. The online help for the **Repository** page in the **Settings** tab incorrectly indicates there is an ARCHIVE disk group. There are only three disk groups available in Oracle AVDF 12.1.2: ■ EVENTDATA ■ SYSTEMDATA ■ RECOVERY

18267269	ORA-28000 error occurs when starting the Audit Vault Agent.
	
	This error can occur when the Agent user on the host computer is locked.
	
	Workaround:
	
	1. In the Audit Vault Server, find the locked Agent user by running the following command as SYSDBA:
	
	`select locked_agent_user from (select 'AGENTUSR'||HOST_USER_INDEX locked_agent_user from avsys.host where host_name='host_name' and deleted_at is null) where locked_agent_user in (select username from dba_users where account_status like '%LOCKED%' and lock_date is not null);`
	
	For *host_name*, enter the name of the registered host on which you get the ORA 28000 error.
	
	This returns the name of the locked Agent user.
	
	2. In the Audit Vault Server, using the locked Agent user name returned in the previous step, unlock this user by running the following command:
	
	`alter user locked_agent_user account unlock;`
	
	3. Restart the Agent.

Table 1 (Cont.) Audit Vault and Database Firewall Known Issues

Bug Number	Description
18161187	Interface Masters bypass NIC's are not supported, and therefore, cannot be used with Database Firewall. Contact Oracle Support for help with this issue, and refer to document number **1681384.1**.
17862296	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.
16868457	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.
15963372	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.

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 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 Release Notes, Release 12.1.2
E27781-09