

# Oracle® Audit Vault and Database Firewall

Release Notes

Release 12.1.2

**E27781-12**

July 2017

---

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](#)
- [Upgrading to Oracle AVDF 12.1.2 from a Previous Release](#)
- [Supported Secured Targets and Platforms](#)
- [What's New in this Release](#)
- [Known Issues](#)
- [Documentation Accessibility](#)

## 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>

## 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 12c.
- 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 9i 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**

<b>Bug Number</b>	<b>Description</b>
18850821	<p>Syslog (audit trail) collector does not work for systems with rsyslog</p> <p>This affects Oracle secured targets running on computers on Oracle Linux 6 (OEL6) platforms.</p> <p><b>Workaround:</b></p> <ol style="list-style-type: none"><li>1. Set the following parameters in the <code>/etc/rsyslog.conf</code> file: <pre># Use default timestamp format \$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat</pre></li><li>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 <b>Trail Location</b> field, provide a full path such as <code>/usr/local/syslog*</code>. If you are using AVCLI, you can execute a command such as the following: <pre>avcli&gt; START COLLECTION FOR SECURED TARGET sample_source USING HOST foo FROM syslog /usr/local/syslog*;</pre></li></ol>
18948614	<p>HA: After failover Audit Vault Server fails to forward syslog and arcsight messages</p> <p><b>Workaround:</b></p> <ol style="list-style-type: none"><li>1. Log in to the Audit Vault Server console as a super administrator.</li><li>2. Click the <b>Settings</b> tab, and then click <b>Connectors</b>.</li><li>3. In the <b>Syslog</b> section, and then click <b>Save</b>.</li><li>4. Scroll down to the <b>HP ArcSight SIEM</b> section, and then click <b>Save</b>.</li></ol>
18636139	<p>Provide option to remove HA configuration from UI.</p> <p><b>Workaround:</b></p> <p>This workaround is available starting with AVDF 12.1.1.4 (12.1.1 BP4). To unpair two paired Audit Vault Servers:</p> <ol style="list-style-type: none"><li>1. Shut down the standby (secondary) Audit Vault Server.</li><li>2. Log in to the primary Audit Vault Server as <code>root</code>.</li><li>3. Run this command: <pre>sudo -u oracle /usr/local/dbfw/bin/setup_ha.rb --unconfigure</pre></li></ol>
18363490	<p>Need to install Visual C++ 2010 Package to run Windows Agent.</p> <p><b>Workaround:</b></p> <p>Install Microsoft Visual C++ 2010 Redistributable Package to run the Audit Vault Agent on a Windows host. If you are using Microsoft Windows 2003, then you must also install Windows 2003, Microsoft Visual C++ 2005 Redistributable Package.</p>
18381322	<p>Invalid DB Firewall network configurations should be resolved before upgrade.</p> <p>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.</p> <p><b>Workaround:</b></p> <p>Ensure that any enabled traffic sources on the Database Firewall have two ports in the traffic source.</p> <p>Also ensure that any enforcement point in DPE mode is using an enabled traffic source.</p>

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

Bug Number	Description
18420068	<p data-bbox="618 243 1438 296">Update <code>oracle_user_setup.sql</code> script to avoid using Oracle Data Dictionary realm for Database Vault.</p> <p data-bbox="618 310 1438 417">This issue affects Oracle Database 12c secured targets that have Database Vault enabled. When using the Oracle AVDF user setup script <code>oracle_user_setup.sql</code>, and running the script with <code>REDO_COLL</code> mode, the script outputs the following message, which does not apply to Oracle Database 12c:</p> <p data-bbox="618 432 1438 516">Connect to the secured target database as DV Owner and execute: <code>exec dbms_macadm.add_auth_to_realm('Oracle Data Dictionary', 'C##USER1', null, dbms_macutl.g_realm_auth_participant);</code></p> <p data-bbox="618 554 764 579"><b>Workaround:</b></p> <p data-bbox="618 594 1438 646">Ignore the above message if you see it when running the script for an Oracle Database 12c. Instead, execute the following on the database as DV Owner:</p> <pre data-bbox="618 661 1109 686">SQL&gt; GRANT DV_STREAMS_ADMIN TO username;</pre> <p data-bbox="618 724 1438 777">For <i>username</i>, use the name of the account you created for Oracle AVDF on this Oracle Database secured target.</p> <p data-bbox="618 791 1438 842">For full instructions on this setup script, see <i>Oracle Audit Vault and Database Firewall Administrator's Guide</i>.</p>
18391942	<p data-bbox="618 863 1438 888">Online help lists four disk groups in the Audit Vault Server repository.</p> <p data-bbox="618 903 1438 978">The online help for the <b>Repository</b> page in the <b>Settings</b> tab incorrectly indicates there is an ARCHIVE disk group. There are only three disk groups available in Oracle AVDF 12.1.2:</p> <ul data-bbox="618 993 833 1108" style="list-style-type: none"><li data-bbox="618 993 833 1018">■ EVENTDATA</li><li data-bbox="618 1033 833 1058">■ SYSTEMDATA</li><li data-bbox="618 1073 833 1098">■ RECOVERY</li></ul>

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

<b>Bug Number</b>	<b>Description</b>
17862296	<p>Host monitor might choose incorrect network device if multiple preferred devices exist.</p> <p>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.</p> <p><b>Workaround:</b></p> <p>Change the network adapter the host monitor uses so that traffic is captured from the correct network for the secured target. Follow these steps:</p> <ol style="list-style-type: none"><li>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 <code>network_device_name_for_hostmonitor</code> 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</li></ol> <p>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.</p> <ol style="list-style-type: none"><li>2. In the Audit Vault Server console, <b>Secured Targets</b> tab, click the secured target you want.</li><li>3. In the Modify Collection Attributes section, <b>Attribute Name</b> field, enter <code>network_device_name_for_hostmonitor</code>.</li><li>4. In the <b>Attribute Value</b> field, enter the device name, for example: \\Device\\NPF_{17C832B3-B8FC-44F4-9C99-6ECFF1706DD1}</li><li>5. Click <b>Add</b>, and then <b>Save</b>.</li><li>6. Restart the audit trail for this secured target.</li></ol>
16868457	<p>Agent upgrade fails if 12.1.0 Agent has deployed plug-ins.</p> <p><b>Workaround:</b></p> <p>Re-deploy the plug-ins, and then download and install the Agent again.</p>
15963372	<p>Agent install fails when <code>agent.jar</code> is downloaded from IE browser, with "Invalid or corrupt jarfile" error.</p> <p><b>Workaround:</b></p> <p>Use a different browser (such as Firefox) to download the <code>agent.jar</code> file, then run <code>java -jar agent.jar</code> again.</p>

## 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 Release Notes, Release 12.1.2  
E27781-12

Copyright © 2012, 2017, Oracle and/or its affiliates. All rights reserved.

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

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

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

**U.S. GOVERNMENT END USERS:** Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.