Oracle® Audit Vault and Database Firewall

Installation Guide

Release 12.2.0

E49587-35

June 2022

Oracle Audit Vault and Database Firewall Installation Guide, Release 12.2.0

E49587-35

Primary Authors: Karthik Shetty, Sheila Moore, Gigi Hanna

Contributors: Tejas Bajaj, Andrey Brozhko, Paul Betteridge, Sunil Channapatna Ravindrachar, Ravindranath Chennoju, Marek Dulko, Nithin Gomez, Paul Hackett, William Howard-Jones, Srivatsan Kannan, K. Karun, Slawek Kilanowski, Shubhdeep Kochhar, Shirley Kumamoto, Ravi Kumar, Paul Laws, Sreedhar Madiraju, Vijay Medi, Sidharth Mishra, Sarma Namuduri, Eric Paapanen, Abdulhusain Rahi , Mahesh Rao , Vipin Samar, Lok Sheung, Yan Shi, Rajesh Tammana, Tom Taylor, Graham Thwaites, Madhusudhan Yellu

Contents

Preface

Changes In This Document

1 Installing Oracle Audit Vault and Database Firewall Software

2 Overview of Oracle Audit Vault and Database Firewall Installation

3 Oracle Audit Vault and Database Firewall Pre-Install Requirements

4 Post-Install Configuration Tasks

5 Migrating the Configuration from Oracle Audit Vault to Oracle Audit Vault and Database Firewall

List of Figures

List of Tables

Preface

Oracle Audit Vault and Database Firewall Installation Guide explains how to install Oracle Audit Vault and Database Firewall (Oracle AVDF).

Preface Topics

Audience

Oracle Audit Vault and Database Firewall Installation Guide is intended for anyone who is responsible for installing Oracle AVDF.

Documentation Accessibility

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

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

For more information see the following documents in the Oracle Audit Vault and Database Firewall documentation set:

- *Oracle Audit Vault and Database Firewall Release Notes*

  Contains release note material for Oracle Audit Vault and Database Firewall.
- *Oracle Audit Vault and Database Firewall Installation Guide*

  Explains how to install or upgrade Oracle Audit Vault and Database Firewall.
- *Oracle Audit Vault and Database Firewall Concepts Guide*

  Contains conceptual information for Oracle Audit Vault and Database Firewall.
- *Oracle Audit Vault and Database Firewall Administrator's Guide*

  Explains how to administer Oracle Audit Vault and Database Firewall.
- *Oracle Audit Vault and Database Firewall Auditor's Guide*

  Explains how to use Oracle Audit Vault and Database Firewall to create audit and firewall policies, and to generate reports.
- *Oracle Audit Vault and Database Firewall Developer's Guide*

  Explains how to create custom Oracle Audit Vault collectors.

> **See Also:**
>
> `http://www.oracle.com/technetwork/database/security/index.html`

Conventions

This document uses these text conventions:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Changes In This Document

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

Revision History

The following are the updates and correction in this document.

E49587-35 (June 2022)

Included important information in Pre-upgrade Tasks (page 6-3).

E49587-33 (September 2020)

- Host Monitor functionality on Windows platform is re-certified in 12.2.0.13.0. For using Host Monitoring on Windows platform install Npcap and update OpenSSL libraries on Windows before upgrading to 12.2.0.13.0. See Host Monitor Migration on Windows (page 6-4) and Host Monitor Requirements (page 3-5) for complete information.
- Apply the deprecated ciphers patch (`Deprecated-Cipher-Removal.zip`) to remove old ciphers, post AVS install or upgrade. Apply this patch on Audit Vault Server after installation or upgrade to 12.2.0.13.0 (or later). See Downloading and Verifying the Software (page 1-2) and Audit Vault Server Post-Installation Tasks (page 4-1) for complete information.
- Updated supported components in sections Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) and Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5).

E49587-32 (March 2020)

- Database Activity Monitoring with Host monitor on Windows platform is not certified in release `12.2.0.11.0` and `12.2.0.12.0`. Upgrade to these releases only when you are sure that network trail monitoring functionality on Windows platform is not required.
- Updated supported components in sections Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) and Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5).
- Supporting audit collection from Microsoft SQL Server Cluster on Windows 2012 R2 starting release `12.2.0.12.0`.
- Supporting audit collection from IBM DB2 (version 11.1) HADR (High Availability and Disaster Recovery) on OL 7.x starting release `12.2.0.12.0`.
- IBM DB2 collects audit data from IBM AIX on Power Systems (64-bit) version 7.1 starting release `12.2.0.12.0`.

E49587-31 (February 2020)

Minor correction to the document.

E49587-30 (December 2019)

- Updates and correction to Platform Support (page 2-2).
- Included instructions to Reimage Oracle Database Firewall and Restore from Audit Vault Server (page 6-28).

E49587-29 (November 2019)

- Updates and correction to Platform Support (page 2-2).
- Correction to the command in Enable Archiving Functionality Post Upgrade From Release BP10 and Prior (page 6-24).

E49587-28 (October 2019)

Updates to Platform Support (page 2-2).

E49587-27 (September 2019)

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

- Added support for the following new targets:

Target	Version	Audit collection	Database Firewall
Autonomous Transaction Processing (Serverless)	Latest version	Yes	No
Autonomous Transaction Processing (Dedicated)	Latest version	Yes	No
Oracle Database	19c	Yes	Yes
MySQL	8.0	Yes	No
SAP Sybase	16	Yes	No

See Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) and Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5) for complete information.

- Enable Archiving Functionality Post Upgrade From Release BP10 and Prior (page 6-24) in case of high availability environment.
- Support for Java `11.0.3` on Audit Vault Agent. See section Audit Vault Agent: Supported and Tested Java Runtime Environment (page 2-11) for all supported versions.

E49587-26 (July 2019)

Oracle Audit Vault and Database Firewall is supported on *VMware vSphere 6.0*. Updated section Supported Server Platforms (page 2-2).

E49587-25 (June 2019)

- Included important information on upgrade path in section Upgrading Oracle Audit Vault and Database Firewall (page 6-2).
- Updates to section Downloading and Verifying the Software (page 1-2).

E49587-24 (March 2019)

- Included support for the following secured target versions for Host Monitor and Audit Vault Agent functionality:

Secured Target	Version	Host Monitor	Audit Vault Agent	Database Firewall
Oracle Linux	7.4 - 7.5	Yes	Yes	Not applicable
Oracle Linux	6.9	Yes	Already exists	Not applicable
Oracle Linux	6.10	Yes	Yes	Not applicable
Red Hat Enterprise Linux	7.4 - 7.5	Yes	Yes	Not applicable
Red Hat Enterprise Linux	6.9	Yes	Already exists	Not applicable
Red Hat Enterprise Linux	6.10	Yes	Yes	Not applicable
IBM AIX on Power Systems (64-bit)	7.2	Yes	Already exists	Not applicable
Microsoft Windows Server x86-64	2016	Yes	Already exists	Not applicable
Microsoft SQL Server	2017	No	Yes	Yes

- Review the following upgrade procedures where ever applicable:
  - Pre-upgrade Tasks (page 6-3)
  - Upgrade Tasks (page 6-11)
  - Post Upgrade Tasks (page 6-19)
- Included important information on log rotate file. See sections Preserve Customization In Log Rotate File (page 6-10) and Resolve Missing Log Rotate File Post Upgrade (page 6-26) for complete information.
- Included important information on hardware platform supported by Oracle Audit Vault and Database Firewall. See sections Oracle Audit Vault and Database Firewall Hardware Requirements (page 3-2) and Supported Server Platforms (page 2-2) for complete information.

- Updated section Supported Browsers (page 2-10).

E49587-23 (December 2018)

- Minor correction to section Applying The Agent Patch Manually On Individual Agents (page 6-8).
- Included a note that *Oracle Audit Vault and Database Firewall* is compatible with all editions of Microsoft Windows Server. See section Audit Vault Agent: Supported Platforms and Versions (page 2-6) for complete information.

E49587-22 (October 2018)

- **Required Action:**
  - If any Agent is using `Java` *1.6*, then upgrade the `Java` version to *1.8*. See Audit Vault Agent: Supported and Tested Java Runtime Environment (page 2-11) for complete information.
  - Install the Mandatory Pre-upgrade Patch (page 6-4) before upgrading to *Oracle Audit Vault and Database Firewall* release `12.2.0.9.0`.
- Added support for setting TLS levels across all components of *Oracle Audit Vault and Database Firewall*.
- Included important information on upgrade from `12.1` or older versions. See Upgrading Oracle Audit Vault and Database Firewall (page 6-2) for complete information.
- Added support for Oracle Database 18c (18.3) as a secured target. Updated section Audit Data Collection: Supported Secured Target Types and Versions (page 2-3).
- Updated the list of Supported Firewall Network Interface Cards (NICs) (page 2-8).
- **F5 BIG-IP ASM** integration is deprecated in release `12.2.0.7.0`, and will be desupported in `19.1.0.0.0`. This functionality is only supported on **F5 BIG-IP ASM** version `10.2.1`.
- **Micro Focus Security ArcSight SIEM** is deprecated in `12.2.0.8.0` and is desupported in `12.2.0.9.0`. Use the `syslog` integration feature instead.
- **SAP Sybase ASE** version `15.7` is supported. The previous versions are desupported. Updated section Platform Support (page 2-2).
- **SAP Sybase SQL Anywhere** is desupported. Updated section Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5).
- See the following sections for an updated list of supported systems and components:
  - Platform Support (page 2-2)
  - Compatible Third-Party Products (page 2-14)
  - Support for External Systems (page 2-10)
  - Audit Data Collection: Supported Secured Target Types and Versions (page 2-3)
  - Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5)
  - Compatibility with Oracle Enterprise Manager (page 2-12)
  - Java SE Requirement (page 3-4)

- Minor update to section Supported Server Platforms (page 2-2).
- Included information on Networking Setup And Configuration (page 4-10).

E49587-20 (June 2018)

- Added support for UEFI boot. Installation on *Oracle Server X7-2* is supported. See Supported Server Platforms (page 2-2) for complete information.
- **Micro Focus Security ArcSight SIEM** (previously known as **HP ArcSight SIEM**) is deprecated in `12.2.0.8.0`, and will be desupported in `12.2.0.9.0`. It is advisable to use the `syslog` integration feature instead.
- In-line bridge mode is deprecated in `12.2.0.8.0`, and will be desupported in `19.1.0.0.0`. It is advisable to use proxy mode as an alternative.
- See the following sections for an updated list of supported systems and components:
  - Audit Data Collection: Supported Secured Target Types and Versions (page 2-3)
  - Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5)
  - Audit Vault Agent: Supported and Tested Java Runtime Environment (page 2-11)
  - Support for External Systems (page 2-10)
  - Supported Firewall Network Interface Cards (NICs) (page 2-8)
- Minor update to disk space requirements in section Disk Space Requirements (page 3-3).
- Minor update to section Compatibility with Oracle Enterprise Manager (page 2-12).

E49587-19 (April 2018)

Included an important note on hardware that is enabled only with UEFI. See section Supported Server Platforms (page 2-2) for complete information.

E49587-18 (February 2018)

- **F5** is deprecated in release `12.2.0.7.0`, and will be desupported in `19.1.0.0.0`.
- Update to section Compatibility with Oracle Enterprise Manager (page 2-12).

E49587-17 (December 2017)

- Included support for the following versions of Red Hat Enterprise Linux operating system as secured target for audit collection. See Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) for more information.
  - RHEL 6.7
  - RHEL 6.8
  - RHEL 6.9
  - RHEL 7.1
  - RHEL 7.2
  - RHEL 7.3
- Included support for the following new versions of MySQL with both old and new audit formats. See Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) for more information.
  - 5.5.34 to 5.5.57

  - 5.6.13 to 5.6.37
  - 5.7.0 to 5.7.19
- Included support for AIX 7.2 version as secured target for audit collection. See Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) and Audit Vault Agent: Supported Platforms and Versions (page 2-6) for more information.
- Included support of version 12 of SUSE Linux Enterprise Server operating system for Audit Vault Agent and Host Monitor. See sections Host Monitor: Supported Platforms and Versions (page 2-7) and Audit Vault Agent: Supported Platforms and Versions (page 2-6) for more information.
- Included support for Microsoft Windows Server (x86-64) 2016 and Active Directory 2016 versions. Updated the following sections:
  - Audit Data Collection: Supported Secured Target Types and Versions (page 2-3)
  - Audit Vault Agent: Supported Platforms and Versions (page 2-6)
- Included important information on supported browser versions in sections Supported Browsers (page 2-10) and Browser Requirements (page 3-4).

E49587-15 (September 2017)

Correction to Audit Data Collection: Supported Secured Target Types and Versions (page 2-3).

E49587-14 (August 2017)

- Included IBM DB2 11.1 version support for audit collection. See Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) and Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5) for complete information.
- Included support for Red Hat Enterprise Linux operating system (version 7.0) as secured target for audit collection. Updated Audit Vault Agent: Supported Platforms and Versions (page 2-6) and Host Monitor: Supported Platforms and Versions (page 2-7).
- Included support for the following versions of Oracle Linux operating system as secured targets for audit collection. Updated Audit Data Collection: Supported Secured Target Types and Versions (page 2-3).
  - `6.8`
  - `6.9`
  - `7.3`
- Updated Disk Space Requirements (page 3-3).
- Audit Vault Server is installed using four disks, each created from `.iso` file downloads. Updated sections About the Software Installation Procedure (page 1-1) and Installing an Audit Vault Server or Database Firewall (page 1-5).

E49587-13 (July 2017)

Updated Supported Firewall Network Interface Cards (NICs) (page 2-8).

E49587-12 (June 2017)

- Updated Oracle Linux version supported in section Audit Data Collection: Supported Secured Target Types and Versions (page 2-3).
- Increased the maximum disk space for Provisioning disks. See Disk Space Requirements (page 3-3) for more information.
- While performing Audit Vault Server upgrade, the user must keep sufficient disk space if there is huge amount of event data. See Upgrading Oracle Audit Vault and Database Firewall (page 6-2) for more information.
- Updated Microsoft Windows Server version supported in section Audit Vault Agent: Supported Platforms and Versions (page 2-6).

E49587-11 (December 2016)

- Included new release of Oracle Linux `OL 7.1 (auditd version 2.4.1)` and `OL 7.2 (auditd version 2.4.1)` as supported secured target types. See section Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) for details.
- Oracle Audit Vault and Database Firewall release `12.2.0.4.0` is installed or upgraded with Oracle Linux 6.8. See section Supported Server Platforms (page 2-2) for an important update on compatibility with previous releases of Oracle Linux.
- Included an important note to be followed before performing the upgrade task, if there is a Niagara card in the system. See section Upgrading Oracle Audit Vault and Database Firewall (page 6-2) for details.
- Included an important task that must be completed post upgrading to release 12.2.0.4.0 from 12.2.0.3.0. See Migration of Expired Audit Records (page 6-27) for more information.

E49587-10 (August 2016)

- Ensure to have the latest update of Oracle Linux Release 6. See sections Oracle Audit Vault and Database Firewall Hardware Requirements (page 3-2) and Supported Server Platforms (page 2-2) for details.

1 Installing Oracle Audit Vault and Database Firewall Software

Learn how to install Oracle Audit Vault and Database Firewall (Oracle AVDF).

You can deploy the Audit Vault Agent once you have installed the Audit Vault Server.

> **See Also:**
>
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for important information about installing Oracle Audit Vault and Database Firewall securely and protecting your data.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for instructions on deployment and activation of Audit Vault Agent.

1.1 About the Software Installation Procedure

The Oracle Audit Vault and Database Firewall (Oracle AVDF) software is installed using four discs.

Each disc is created from `.iso` file downloads:

- Three Audit Vault Server installer discs (created from three `.iso` files)
- One Database Firewall installer disc (created from one `.iso` file)
- There is an additional *Utilities* file for Oracle Advanced Security Integration and Database Interrogation setup.

Oracle AVDF release 12.2.0.13.0 software contains the `avdf-12.2.0.13.0-utility.zip` file in addition to three Audit Vault Server installer discs and one Database

Firewall installer disc. The `avdf-12.2.0.13.0-utility.zip` bundle contains the following files:

- `cipher-update.zip`: Oracle Audit Vault and Database Firewall 12.2.0.13.0 - Deprecated-Cipher-Removal Utility

  Note: Apply this patch on Audit Vault Server after installation or upgrade to 12.2.0.13.0 (or later). Before applying the patch, make sure that all the Audit Vault Agents and Host Monitor Agents are upgraded to 12.2.0.13.0.
- `npcap-utility.zip`: Npcap installer required for Host Monitoring on Windows
- `dbfw-utility.zip`: Database Firewall utilities to examine Native Network Encryption traffic for Oracle Database and to gather session information from other database types.
- `README`: Instructions for deploying Npcap and Database Firewall utilities patch.

During the installation, you create an installation passphrase that protects the newly installed component until it is fully configured.

> **See Also:**
>
> Installation Passphrase Requirements (page 1-4)

> **Note:**
>
> The installation process reimages the server on which you install the Audit Vault Server or Database Firewall, automatically installing the operating system.

1.2 Downloading and Verifying the Software

Learn about downloading and verifying the software to install Oracle Audit Vault and Database Firewall (Oracle AVDF).

For a fresh installation, you can download the Oracle Audit Vault and Database Firewall software from the Software Delivery Cloud. You cannot use this package to upgrade. To perform an upgrade from an existing deployment, you can download the upgrade software from the My Oracle Support website.

To download the software:

1. Use a web browser to access the Oracle Software Delivery Cloud portal:

   https://edelivery.oracle.com

   > **Note:**
   >
   > Ensure that the browser version you are using supports TLS 1.2 protocol. See Supported Browsers (page 2-10) for complete information.

2. Click **Sign In**, and if prompted, enter your **User ID** and **Password**.
3. In the **All Categories** menu, select **Release**. In the next field, enter **Oracle Audit Vault and Database Firewall** and then click **Search**.
4. From the list that is displayed, select the **Oracle Audit Vault and Database Firewall** version you want to install. Alternately, click the **+Add to Cart** button against the specific release.

   The download is added to your cart. To check the cart contents, click **View Cart** in the upper right of the screen.
5. Click **Checkout**.
6. In the next page, verify the details of the installation package, and then click **Continue**.
7. Read the **Oracle Standard Terms and Restrictions** displayed on the page. Select **I accept the terms in the license agreement**, and click **Continue**.

   The download page appears and displays the list of ISO files for *Oracle Audit Vault and Database Firewall*. The following is an example for release `12.2.0.11.0`:

   - `V`*`part_number`*`.iso` Oracle Audit Vault and Database Firewall `12.2.0.11.0` (AVDF 12.2 BP11) - Server - Disc 1, 4.6 GB
   - `V`*`part_number`*`.iso` Oracle Audit Vault and Database Firewall `12.2.0.11.0` (AVDF 12.2 BP11) - Server - Disc 2, 3.9 GB
   - `V`*`part_number`*`.iso` Oracle Audit Vault and Database Firewall `12.2.0.11.0` (AVDF 12.2 BP11) - Server - Disc 3, 3.0 GB
   - `V`*`part_number`*`.iso` Oracle Audit Vault and Database Firewall `12.2.0.11.0` (AVDF 12.2 BP11) - Firewall, 4.2 GB
   - `V`*`part_number`*`.iso` Oracle Audit Vault and Database Firewall `12.2.0.11.0` (AVDF 12.2 BP11) - Utilities, 9.1 KB

   Oracle AVDF release 12.2.0.13.0 software contains the `avdf-12.2.0.13.0-utility.zip` file in addition to three Audit Vault Server installer discs and one Database Firewall installer disc. The `avdf-12.2.0.13.0-utility.zip` bundle contains the following files:

   - `cipher-update.zip`: Oracle Audit Vault and Database Firewall 12.2.0.13.0 - Deprecated-Cipher-Removal Utility

     Note: Apply this patch on Oracle Audit Vault Server 12.2.0.13.0 after installation or upgrade. Before applying the patch, make sure that all the Audit Vault Agents and Host Monitor Agents are upgraded to 12.2.0.13.0.
   - `npcap-utility.zip`: Npcap installer required for Host Monitoring on Windows
   - `dbfw-utility.zip`: Database Firewall utilities to examine Native Network Encryption traffic for Oracle Database and to gather session information from other database types.
   - `README`: Instructions for deploying Npcap and Database Firewall utilities patch.
8. To the right of the **Print** button, click **View Digest Details**.

   The listing for the ISO files expands to display the SHA-1 and SHA-256 checksum reference numbers for each ISO file.
9. Copy the SHA-256 checksum reference numbers and store them for later reference.
10. Click **Download**, to download the installer. Then click **Save File**.

11. Choose a location to save the ISO files. Click **Save**.
12. Alternately, you can save each file individually by clicking its name and then specifying a location for the download.
13. The combined size of all ISO files exceeds 4 GB, and takes time to download, depending on the network speed. The estimated download time and speed are displayed in the **File Download** dialog box.
14. After the ISO files are downloaded to the specified location, verify the SHA-256 checksums of the downloaded files:
    1. From a Linux or Unix machine, generate a SHA256 checksum for the first `Vpart_number.iso`:

       ```
       $ sha256sum Vpart_number.iso
       ```

       Ensure that the checksum matches the value that you copied from the **File Download** dialog box in the earlier step.
    2. Generate a SHA-256 checksum for the second `Vpart_number.iso`:

       ```
       $ sha256sum Vpart_number.iso
       ```

       Ensure that the checksum matches the value that you copied from the **File Download** dialog box in the earlier step.
15. Optionally, burn each of the `Vpart_number.iso` files to a DVD-ROM disc with a capacity of 8.5 GB each. Then label the discs as below.

    For example:

    - AVDF Disc 1
    - AVDF Disc 2

    > **Caution:**
    >
    > Do not use a standard DVD disc of capacity 4.7 GB as the iso file does not fit into it.

16. Install the software on a server machine.

1.3 Installation Passphrase Requirements

One step in the installation of an Audit Vault Server or Database Firewall is to create an installation passphrase.

The installation passphrase protects the newly installed component from outside attack until you have done the post-install configuration tasks. To do the tasks, you must enter the installation passphrase that you created during the installation.

After doing the tasks, you no longer need the installation passphrase, and it no longer works.

The installation passphrase must have between 8 to 255 characters in these categories:

- Uppercase letters (A-Z) - must have at least one
- Lowercase letters (a-z) - must have at least one
- Digits (0-9) - must have at least one
- Space
- At least one of the following:
  - Comma (,)
  - Period (.)
  - Colon (:)
  - Plus sign (+)
  - Underscore (_)

If you have created an installation passphrase for a component but not yet completed the post-install configuration tasks, then you can change the passphrase. To do so, select **Change Installation Passphrase** in the Audit Vault Server menu or Database Firewall menu, shown in the later steps of installation.

See Also:

Post-Install Configuration Tasks (page 4-1)

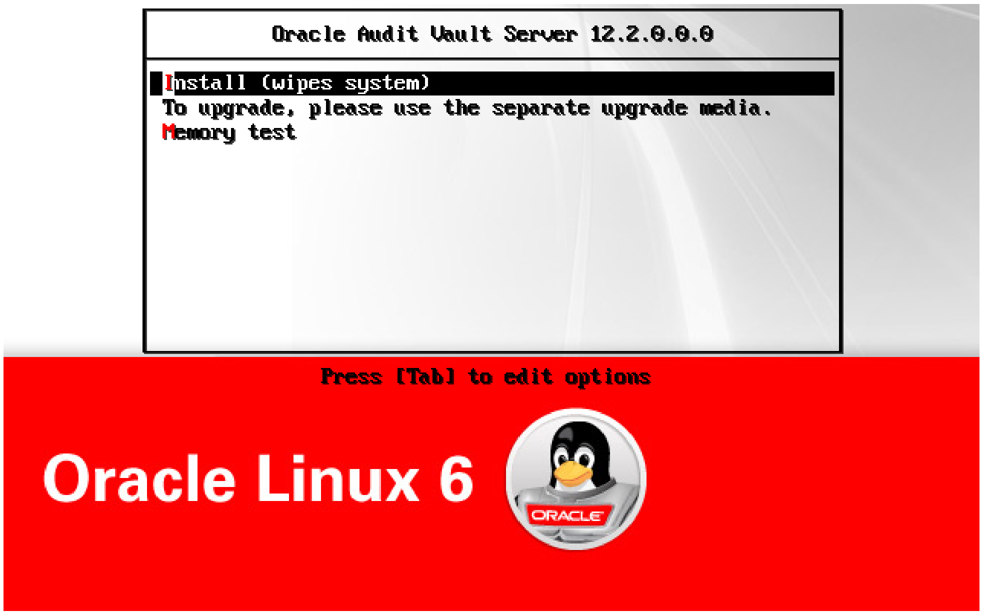
1.4 Installing an Audit Vault Server or Database Firewall

Steps for installing Audit Vault Server or Database Firewall.

To install an Audit Vault Server or Database Firewall:

1. Insert either installer disk 1 for the Audit Vault Server or the single installer disk for the Database Firewall in the disk drive, and then reboot the system.

   The system is booted from the disk, and the initial splash screen appears, similar to the following:



```
Oracle Audit Vault Server 12.2.0.0.0

Install (wipes system)
To upgrade, please use the separate upgrade media.
Memory test

Press [Tab] to edit options
```

Your splash screen will indicate the release number you are installing.

2. Select `install`, and then press the **Enter** key.

   The installation proceeds.

3. (Audit Vault Server Only) Insert disk 2 when prompted, select **OK**, and then press **Enter**.

   After a time, the installer asks you to insert disk 3.

4. Insert disk 3 when prompted, select **OK**, and then press **Enter.**

   After a time, the installer asks you to insert disk 1 again.

5. (Audit Vault Server Only) Insert disk 1 again when prompted, select **OK**, and then press **Enter**.

6. Type the installation passphrase, press **Enter**, and then confirm the passphrase.

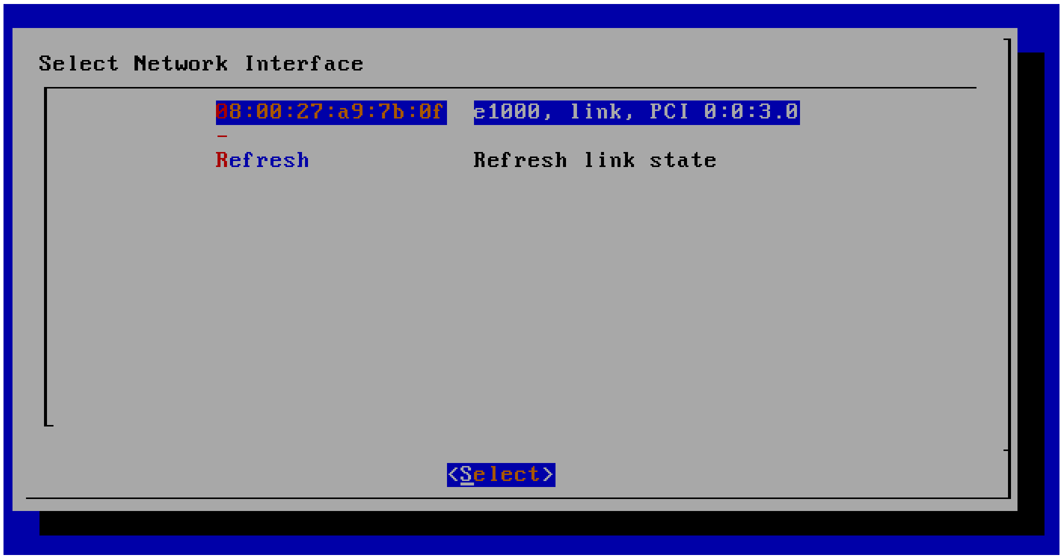
   The screen displays this message:

   ```
   Installation passphrase was successfully configured
   ```

7. Press **Enter**.

   The Select Management Interface screen appears for Database Firewall, or for the Audit Vault Server, the Select Network Interface screen appears.

   For example, for the Select Network Interface screen:



```
Select Network Interface

              08:00:27:a9:7b:0f   e1000, link, PCI 0:0:3.0
              Refresh             Refresh link state
```

8. If more than one interface is available, select the interface that you want to be the management interface.

   This interface is the network interface used by the Audit Vault Server or the Database Firewall.

9. Press the key **Enter**.

   For a Database Firewall, a screen appears with this option selected:

   ```
   Use Use this device as the management port
   ```

   For the Audit Vault Server, a screen appears with this option selected:

   ```
   Use Use this device as the network interface
   ```

10. Press **Enter**.

    For the Database Firewall, the Please enter management interface IP setting screen appears. For the Audit Vault Server, the Please enter network interface IP setting screen appears. Both screens contain the following fields:

    - **IP Address**
    - **Network Mask**
    - **Gateway**

11. In the field **IP Address**, enter the IP address of the network interface and then press **Tab**.

    The cursor moves to the field **Network Mask**.

12. In the field **Network Mask**, enter the network mask for the management interface and then press **Tab**.

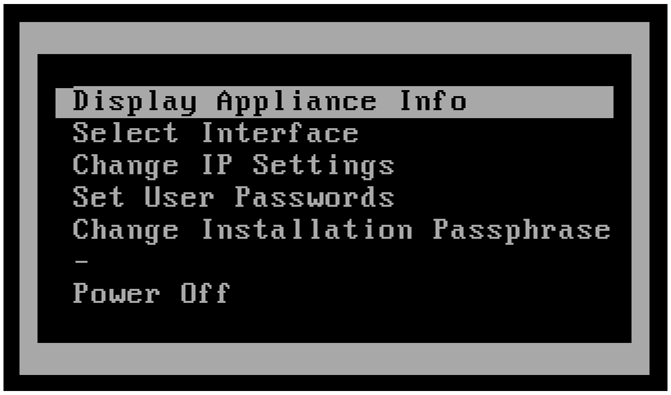
    The cursor moves to the field **Gateway**.

13. In the field **Gateway**, enter the gateway IP address for the management interface and then press **Tab**.

    The cursor moves to **Reboot to complete installation**.

14. Press **Enter**.

    The computer restarts. This may take a long time. When the restart has finished, the system displays the menu settings.



```
Display Appliance Info
Select Interface
Change IP Settings
Set User Passwords
Change Installation Passphrase
-
Power Off
```

15. Press **Enter**.

    The network settings appear.

    At this point, the installation of either the Audit Vault Server or the Database Firewall is complete. You will set user passwords as part of the next step.

16. Perform the appropriate post-install configuration tasks.

    For these tasks, you need the passphrase that you created in step 6 (page 1-6) and the IP address that you provided in step 11 (page 1-7).

> **Note:**
>
> The Audit Vault Server and the Database Firewall server are software appliances. You must not make any changes to the Linux operating system through the command line on these servers unless following official Oracle documentation or under guidance from Oracle Support.

> **See Also:**
>
> - Installation Passphrase Requirements (page 1-4)
> - Post-Install Configuration Tasks (page 4-1)

2

Overview of Oracle Audit Vault and Database Firewall Installation

Learn to install Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide* for general information about secure installation, data protection, and general recommendations for deploying Oracle Audit Vault and Database Firewall in a network and in special configurations.

2.1 Downloading the Latest Version of This Manual

Learn how to download the latest documentation for Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **See Also:**
>
> - `http://www.oracle.com/pls/topic/lookup?ctx=avdf122` to download the latest version of this manual.
> - `http://docs.oracle.com` for documentation of other Oracle products.

2.2 Platform Support

Learn about various platforms supported by Oracle AVDF.

- Supported Server Platforms (page 2-2)
  Learn about supported platforms for Audit vault Agent, Host Monitor, audit collection, and Database Firewall protection.
- Audit Data Collection: Supported Secured Target Types and Versions (page 2-3)
  Learn about the supported secured target types and versions for audit data collection for the current release of Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5)
  Learn about the supported secured target types and versions for Database Firewall protection.
- Audit Vault Agent: Supported Platforms and Versions (page 2-6)
  Learn about the supported platforms and versions for the Audit Vault Agent.
- Host Monitor: Supported Platforms and Versions (page 2-7)
  Learn about the supported platforms and versions for the host monitor for Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Supported Firewall Network Interface Cards (NICs) (page 2-8)
  Learn in what Oracle Audit Vault and Database Firewall (Oracle AVDF) release Niagara cards are supported.
- Supported Browsers (page 2-10)
  Learn what browsers are supported with Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Support for External Systems (page 2-10)
  Learn about the external systems supported by Oracle Audit Vault and Database Firewall.
- Audit Vault Agent: Supported and Tested Java Runtime Environment (page 2-11)
  Learn about the supported and tested Java Runtime Environment (JRE) for the Audit Vault Agent.
- Compatibility with Oracle Enterprise Manager (page 2-12)
  Learn about the supported versions of Oracle Enterprise Manager and Oracle Audit Vault Database Firewall (Oracle AVDF).

2.2.1 Supported Server Platforms

Learn about supported platforms for Audit vault Agent, Host Monitor, audit collection, and Database Firewall protection.

Oracle Audit Vault and Database Firewall (Oracle AVDF) is delivered as software appliance images ready to be deployed on physical hardware or on virtualized environments such as Oracle VM Server or VMware. You can install and run Oracle Audit Vault and Database Firewall on the following platforms:

- Any Intel x86-64-bit hardware platform supported by Oracle Audit Vault and Database Firewall's embedded operating system. Oracle Audit Vault and Database Firewall uses Oracle Linux release 6 with the Unbreakable Enterprise

Kernel (UEK) version 4. For a list of compatible hardware, refer to Hardware Certification List for Oracle Linux and Oracle VM. This list contains the minimum version of Oracle Linux certified with the selected hardware. All Oracle Linux updates starting with Oracle Linux release 6 as the minimum are also certified unless otherwise noted.

- Oracle VM Server for x86, version 3.2.2 - 3.2.9
- VMware vSphere, version 6.0

> **Note:**
>
> - Oracle Audit Vault and Database Firewall release `12.2.0.7.0` and prior, do not support hardware that is enabled only with UEFI.
> - Oracle Audit Vault and Database Firewall release `12.2.0.8.0` and onwards, support hardware that is enabled with UEFI boot. Installation on *Oracle Server X7-2* is supported.
> - Oracle Audit Vault Server and Database Firewall cannot be installed on Exalogic or Exadata servers.

2.2.2 Audit Data Collection: Supported Secured Target Types and Versions

Learn about the supported secured target types and versions for audit data collection for the current release of Oracle Audit Vault and Database Firewall (Oracle AVDF).

The following tables list supported secured target types and versions for audit data collection.

Table 2-1 Audit Collection: Supported Secured Target Types and Versions for Database

Category	Releases/Versions
Autonomous Data Warehouse (Serverless)	Latest version
Autonomous Transaction Processing (Serverless)	Latest version
Oracle Database	10g, 11g, 12c 18c (18.3) in release `12.2.0.9.0 and later` 19c in release `12.2.0.11.0 and later`
Oracle Exadata	10g, 11g, 12c 18c (18.3) in release `12.2.0.9.0 and later` 19c in release `12.2.0.11.0 and later`
Oracle Real Application Clusters	10g, 11g, 12c 18c (18.3) in release `12.2.0.9.0 and later` 19c in release `12.2.0.11.0 and later`
IBM DB2	9.1 - 11.1

Table 2-1 (Cont.) Audit Collection: Supported Secured Target Types and Versions for Database

Category	Releases/Versions
IBM DB2 Cluster HADR (High Availability and Disaster Recovery) on OL 7.x	11.1 is supported in release `12.2.0.12.0` and later
Microsoft SQL Server (Enterprise Edition)	2000, 2005, 2008, 2008R2, 2012, 2014 2016 is supported in release `12.2.0.2.0` and later 2017 is supported in release `12.2.0.10.0` and later
Microsoft SQL Server Cluster	2012 R2 is supported in release `12.2.0.12.0` and later
SAP Sybase ASE	15.7 16.0 is supported in release `12.2.0.11.0` and later.
MySQL (Enterprise Edition)	5.5 - 5.6 5.7 is supported in release `12.2.0.7.0` and later. 8.0 is supported in release `12.2.0.11.0` and later.
REDO Collector using *Oracle Streams*	Up to 12.2 using *Oracle Streams*

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

Table 2-2 Audit Collection: Supported Secured Target Types and Versions for Operating System

Category	Releases/Versions
Oracle Solaris (SPARC64)	10.x, 11.x
Oracle Solaris (x86-64)	10.x, 11.x
Oracle Linux	OL 5.8 (requires `auditd` 1.8) OL 6.0 (requires `auditd` 2.0) OL 6.1-6.5 (requires `auditd` 2.2.2) OL 6.6-6.7 (requires `auditd` 2.3.7) OL 6.8-6.10 (requires `auditd` 2.4.5) OL 7.0 (requires `auditd` 2.3.3) OL 7.1-7.2 (requires `auditd` 2.4.1) OL 7.3 (requires `auditd` 2.6.5) OL 7.4-7.5 (requires `auditd` 2.7.6)

Table 2-2 (Cont.) Audit Collection: Supported Secured Target Types and Versions for Operating System

Category	Releases/Versions
Red Hat Enterprise Linux	RHEL 6.7 (requires `auditd` 2.3.7) RHEL 6.8 (requires `auditd` 2.4.5) RHEL 6.9 (requires `auditd` 2.4.5) RHEL 6.10 (requires `auditd` 2.4.5) RHEL 7.0 (requires `auditd` 2.3.3) RHEL 7.1 (requires `auditd` 2.4.1) RHEL 7.2 (requires `auditd` 2.4.1) RHEL 7.3 (requires `auditd` 2.6.5) RHEL 7.4 (requires `auditd` 2.7.6) RHEL 7.5 (requires `auditd` 2.7.6)
IBM AIX on Power Systems (64-bit)	6.1, 7.1, 7.2
Microsoft Windows Server (x86-64)	2008, 2008 R2, 2012, 2012 R2, 2016

Table 2-3 Audit Collection: Supported Secured Target Types and Versions for Directory Service

Category	Releases/Versions
Microsoft Active Directory	2008, 2008 R2, 2012, 2016

Table 2-4 Audit Collection: Supported Secured Target Types and Versions for File System

Category	Releases/Versions
Oracle ACFS	12c

Table 2-5 Audit Collection: Supported Secured Target Types and Versions for Hadoop System

Category	Releases/Versions
Oracle Big Data Appliance[1]	4.3

[1] This plug-in is not shipped out of the box. Refer to *Oracle Big Data Appliance Owner's Guide* for more information.

2.2.3 Database Firewall Protection: Supported Secured Target Types and Versions

Learn about the supported secured target types and versions for Database Firewall protection.

Table 2-6 (page 2-6) lists supported secured target types and versions for Database Firewall protection for the current release.

Table 2-6 Database Firewall Protection: Supported Secured Target Types and Versions

Database Product	Releases/Versions
Oracle Database	9i, 10g, 11g, 12c, 18c (18.3) in release `12.2.0.9.0` and later 19c in release `12.2.0.11.0` and later
Oracle Exadata	10g, 11g, 12c 18c (18.3) in release `12.2.0.9.0` and later 19c in release `12.2.0.11.0 and later`
Oracle Real Application Clusters	10g, 11g, 12c 18c (18.3) in release `12.2.0.9.0` and later 19c in release `12.2.0.11.0 and later`
MySQL (Enterprise Edition)	5.0, 5.1, 5.5, 5.6
IBM DB2	9.1 - 10.5
Microsoft SQL Server (Enterprise Edition)	2000, 2005, 2008, 2008 R2, 2012, 2014 2016 is supported in release `12.2.0.2.0` and later 2017 is supported in release `12.2.0.10.0` and later
SAP Sybase ASE	15.7

Note:

- Oracle Audit Vault and Database Firewall does not support Database Firewall monitoring of Microsoft SQL Server cluster.
- Oracle Audit Vault and Database Firewall does not support Database Firewall monitoring of IBM DB2 cluster.
- Oracle Audit Vault and Database Firewall does not support Database Firewall monitoring of IBM DB2 on AIX platform.

2.2.4 Audit Vault Agent: Supported Platforms and Versions

Learn about the supported platforms and versions for the Audit Vault Agent.

Table 2-7 (page 2-7) lists supported platforms and versions for the Audit Vault Agent.

Table 2-7 Audit Vault Agent: Supported Platforms and Versions

Operating System	Releases/Versions
Linux (x86-64)	OL 5.x, 6.x, 7.x SLES 11-12 RHEL 5.x, 6.x, 7.x Asianux 3
Linux (x86-32)	OL 5.x, 6.x SLES 11-12 RHEL 5.x, 6.x, 7.x Asianux 3
Microsoft Windows (x86-64)	8
Microsoft Windows Server (x86-64)	2008, 2008R2, 2012, 2012R2, 2016
Microsoft Windows Server (x86-32)[1]	2008, 2008R2, 2012, 2012R2, 2016
Oracle Solaris (SPARC64)	10.x, 11.x
Oracle Solaris (x86-64)	10.x, 11.x
IBM AIX on Power Systems (64-bit)	6.1, 7.1, 7.2
HP-UX on Itanium	11.31 and above

[1] Oracle AVDF is compatible with all editions of `Microsoft Windows Server`.

2.2.5 Host Monitor: Supported Platforms and Versions

Learn about the supported platforms and versions for the host monitor for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Table 2-8 (page 2-7) lists supported platforms and versions for the host monitor.

Table 2-8 Host Monitor: Supported Platforms and Versions

Operating System	Releases/Versions
Linux x86-64	SLES 11-12 RHEL 5-7 OL 5.x, 6.x, 7.x Asianux 3

Table 2-8 (Cont.) Host Monitor: Supported Platforms and Versions

Operating System	Releases/Versions
Microsoft Windows Server x86-64	2008, 2008R2, 2012, 2012R2 2016 (Starting Oracle Audit Vault and Database Firewall release `12.2.0.10.0` **Note:** Ensure that the Windows target machine has Microsoft Visual C++ 2010 (or later) Redistributable package installed for Host Monitor. **Note:** Ensure to install the supported version of Java on the Host Monitor Agent. See Audit Vault Agent: Supported and Tested Java Runtime Environment (page 2-11). **Caution:** Host Monitor on Windows platform is not certified in release `12.2.0.11.0` and `12.2.0.12.0`. On release `12.2.0.10.0` and prior, Host Monitor functionality on Windows platform is certified.
Oracle Solaris (x86-64)	11.x
Oracle Solaris (SPARC64)	11.x
IBM AIX on Power Systems (64-bit)[1]	6.1, 7.1 IBM AIX is supported starting Oracle Audit Vault and Database Firewall release `12.2.0.1.0` and later. IBM AIX 7.2 is supported starting Oracle Audit Vault and Database Firewall release `12.2.0.10.0` and later. **Note:** For IBM AIX on Power Systems (64-bit) the Input Output Completion Ports (IOCP) is set to `defined` by default. Change this to `available` as *root* user.

[1] Ensure that the target machine has all security patches recommended by OS vendor.

2.2.6 Supported Firewall Network Interface Cards (NICs)

Learn in what Oracle Audit Vault and Database Firewall (Oracle AVDF) release Niagara cards are supported.

> **Caution:**
>
> Oracle Audit Vault and Database Firewall release 12.2.0.11.0 and onwards do not support Niagara cards. Do not upgrade to release 12.2.0.11.0 and onwards if you have Niagara cards in your system.

Oracle Audit Vault and Database Firewall is compatible with all cards that are supported by Oracle Linux.

The Supported Server Platforms (page 2-2) section contains the list of certified compatible hardware for most of the firewall deployment architectures. These deployments include out-of-band mode, proxy mode, and in-line bridge mode when fail-closed is appropriate.

The following Network Interface Cards are certified for in-line bridge deployments where fail-open is desired:

Card Number	Number of interfaces	Interface Type	Driver
N2264	4	Copper	Intel e1000/e1000e
N2264L	4	Copper	Intel e1000/e1000e
N2265	2	Copper	Intel e1000/e1000e
N2266	6	Copper	Intel e1000/e1000e
N2284	4	Fiber	Intel e1000/e1000e
N2285	2	Fiber	Intel e1000/e1000e
N2282	2	Fiber	Intel e1000/e1000e
N2283	4	Fiber	Intel e1000/e1000e
N2261E	2	Copper	Intel e1000/e1000e
N32264	4	Copper	Intel IGB
N32265	2	Copper	Intel IGB
N32266	6	Copper	Intel IGB
N32284	4	Fiber	Intel IGB
N32285	2	Fiber	Intel IGB
N42264	4	Copper	Intel IGB
N42264-1620	4	Copper	Intel IGB
N52264	4	Copper	Intel IGB
N52284	4	Fiber	Intel IGB
N52285	2	Fiber	Intel IGB
N32710	2	Fiber	Intel IXGBE
N32710-TX	2	Copper	Intel IXGBE

Note:

For more information visit http://interfacemasters.com/

Note:

In-line bridge mode is deprecated in release 12.2.0.8.0, and will be desupported in release 20.1.

See Also:

- Configuring Database Firewall and its Traffic Sources on Your Network for information on Database Firewall deployment modes.
- Supported Server Platforms (page 2-2) for the list of certified compatible hardware.

2.2.7 Supported Browsers

Learn what browsers are supported with Oracle Audit Vault and Database Firewall (Oracle AVDF).

Browser Requirements (page 3-4) lists supported browsers.

Table 2-9 Browser Support Matrix

Browser	Release/Version
Firefox	38 and later
Chrome	45 and later
Internet Explorer	IE 11 and later

Note:

- Ensure that the browser version you are using supports TLS 1.2 protocol.
- The browser versions listed in the table above are supported for Oracle Audit Vault and Database Firewall releases prior to 12.2.0.9.0.
- Oracle Audit Vault and Database Firewall release 12.2.0.10.0 and onwards, supports all major releases of Google Chrome, Mozilla Firefox, Microsoft Internet Explorer that are JavaScript-enabled.

2.2.8 Support for External Systems

Learn about the external systems supported by Oracle Audit Vault and Database Firewall.

Supported external systems are as follows:

- Integration offered:
  - HP ArcSight

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

  - Syslog
  - E-mail
  - F5 BIG-IP ASM

> **Note:**
>
> * This functionality is only supported on **F5 BIG-IP ASM** version 10.2.1.
> * **F5 BIG-IP ASM** integration is deprecated in release 12.2.0.7.0, and will be desupported in 20.1.

- SAN storage
  - iSCSI: It can be used to extend disk space for storing event data.
- Archive system
  - NFS
  - SMB
  - SCP

2.2.9 Audit Vault Agent: Supported and Tested Java Runtime Environment

Learn about the supported and tested Java Runtime Environment (JRE) for the Audit Vault Agent.

Table 2-10 (page 2-11) lists supported versions of Java Runtime Environment (JRE).

Table 2-10 JRE Support Matrix

JRE Version	Release/Version
1.8	1.8.0_45 and later
11	11.0.3 Starting *Oracle Audit Vault and Database Firewall* release 12.2.0.11.0.

Note:

- If any Agent is using Java 1.6, then upgrade the Java version to 1.8.
- JRE version 1.6 is deprecated in release 12.2.0.8.0 and is desupported in 12.2.0.9.0.
- JRE version 1.7 is deprecated in release 12.2.0.8.0 and is desupported in 12.2.0.11.0.
- JRE version 11 is not supported on AIX platform. For AIX platform use JRE version 1.8.0_241 (minimum).

2.2.10 Compatibility with Oracle Enterprise Manager

Learn about the supported versions of Oracle Enterprise Manager and Oracle Audit Vault Database Firewall (Oracle AVDF).

Oracle Audit Vault and Database Firewall (AVDF) plug-in provides an interface within Enterprise Manager Cloud Control for administrators to manage and monitor Audit Vault and Database Firewall components.

Table 2-11 (page 2-12) lists supported versions of Oracle Enterprise Manager and Oracle Audit Vault Database Firewall.

Table 2-11 Oracle Enterprise Manager Support Matrix

Oracle Enterprise Manager Release	Oracle Audit Vault Database Firewall Release
• 13.2.1 • 13.3	12.2.x

Note:

Oracle Audit Vault and Database Firewall (AVDF) plug-in is supported only with the above mentioned Enterprise Manager releases.

2.3 Learning About Oracle Audit Vault and Database Firewall

Learn more about Oracle Audit Vault and Database Firewall (Oracle AVDF).

See Also:

Oracle Audit Vault and Database Firewall Concepts Guide to understand the features, components, users, and deployment of Oracle Audit Vault and Database Firewall.

2.4 About Oracle Audit Vault and Database Firewall Installation

Understand the process for installing Oracle Audit Vault and Database Firewall (Oracle AVDF).

Briefly, the steps are:

1. Understand the Oracle Audit Vault and Database Firewall components to be installed.
2. Plan the system configuration that best suits your needs.
3. Ensure that your system meets the pre-install requirements.
4. Install the Oracle Audit Vault and Database Firewall software.
5. Do the post-install configuration tasks.
6. If necessary, migrate the Oracle Audit Vault Release 10.3 configuration to Oracle Audit Vault and Database Firewall Release 12.2.

Note:

The Audit Vault Server and the Database Firewall server are software appliances. You must not make any changes to the Linux operating system through the command line on these servers unless following official Oracle documentation or under guidance from Oracle Support.

See Also:

- *Oracle Audit Vault and Database Firewall Concepts Guide* for information about the components.
- *Oracle Audit Vault and Database Firewall Administrator's Guide* to plan the system configuration that best suits your needs.
- Upgrading Oracle Audit Vault and Database Firewall (page 6-1) for instructions to update the Oracle Audit Vault and Database Firewall software periodically.
- Oracle Audit Vault and Database Firewall Pre-Install Requirements (page 3-1)
- Installing Oracle Audit Vault and Database Firewall Software (page 1-1)
- Post-Install Configuration Tasks (page 4-1)
- Migrating the Configuration from Oracle Audit Vault to Oracle Audit Vault and Database Firewall (page 5-1)
- Uninstalling Audit Vault Agents Deployed on Target Host Machines (page 6-28)

2.5 Supported Secured Targets

Secured targets are the systems (such as a database or operating system) that you will monitor using Oracle Audit Vault and Database Firewall (Oracle AVDF).

Each type of supported secured target has a corresponding plug-in in Oracle Audit Vault and Database Firewall.

See Also:

- `https://support.oracle.com` to find information on supported platforms for prior releases in **Article 1536380.1** .
- Audit Data Collection: Supported Secured Target Types and Versions (page 2-3) for secured targets supported for auditing functions.
- Database Firewall Protection: Supported Secured Target Types and Versions (page 2-5) for secured targets supported for firewall functions.
- *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on plug-ins shipped out-of-the-box.

2.6 Compatible Third-Party Products

Learn about the third-party products that you can use with Oracle Audit Vault and Database Firewall.

- HP ArcSight Security Information Event Management (SIEM), which logs, analyzes, and manages network user activity that is recorded in syslog messages from different sources

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

- F5 BIG-IP ASM (Application Security Manager) which provides protection against Web-based attacks

  > **Note:**
  >
  > - This functionality is only supported on **F5 BIG-IP ASM** version 10.2.1.
  > - **F5 BIG-IP ASM** integration is deprecated in release 12.2.0.7.0, and will be desupported in 20.1.

3

Oracle Audit Vault and Database Firewall Pre-Install Requirements

Learn about the requirements that your system must meet before you can install Oracle Audit Vault and Database Firewall (Oracle AVDF).

- Privileges Required to Install Oracle Audit Vault and Database Firewall (page 3-1)
  Learn about the privileges required to install Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Host Monitor Requirements (page 3-1)
  Host Monitor enables the Database Firewall to directly monitor SQL traffic in a database.
- Oracle Audit Vault and Database Firewall Hardware Requirements (page 3-2)
  Install each Audit Vault Server and each Database Firewall (Oracle AVDF) onto its own dedicated x86 64-bit server (or Oracle VM 3.x).
- Oracle Audit Vault and Database Firewall Software Requirements (page 3-4)
  Learn about the software requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).

3.1 Privileges Required to Install Oracle Audit Vault and Database Firewall

Learn about the privileges required to install Oracle Audit Vault and Database Firewall (Oracle AVDF).

Any user can install Oracle Audit Vault and Database Firewall. You do not need administrative privileges to complete the installation.

3.2 Host Monitor Requirements

Host Monitor enables the Database Firewall to directly monitor SQL traffic in a database.

Recommended requirements for installing Host Monitor:

1. User installing the Host Monitor must have *root* privileges.
2. Ensure Audit Vault Agent is running on the host machine.
3. Ensure the latest version of the following packages from the OS vendor for the specific OS version are installed on the host machine:
   - Libcap (for Linux hosts only)
   - LibPcap
   - OpenSSL
4. Ensure *gmake* is installed. This is required for Host Monitor to run successfully.
5. Verify and allow communication on ports 2050 - 5100 for Database Firewall.

6. Check directory permissions. All the directories in the path of the Host Monitor install location should have 755 as the permission bits starting from the root directory. Also, Host Monitor must be installed in a *root* owned location.

Specific requirements for installing Host Monitor on Windows platform:

1. Host Monitor must be installed by user belonging to *Administrator* group.
2. Install Npcap that is available in the `avdf12.2.0.13.0-utility.zip` bundle in Oracle Software Delivery Cloud. It is part of the Oracle Audit Vault and Database Firewall installable files. Ensure to install Npcap in *WinPcap-API-compatible* mode.
3. Install the latest version of OpenSSL (1.1.1g or higher) libraries. Use OpenSSL version 1.1.1i for release Oracle AVDF 12.2.0.14.0.
4. Ensure the Windows target machine has the latest update of *Visual C++ Redistributable for Visual Studio 2010* (`MSVCRT.dll (*)` or later) package installed. This is a must to use Host Monitor on Windows.

Specific requirements for installing Host Monitor on Linux/Unix/AIX/Solaris platforms:

1. Host Monitor must be installed by *root* user.
2. Ensure the Input Output Completion Ports (IOCP) is set to `available` for IBM AIX on Power Systems (64-bit). It is set to `defined` by default.
3. Ensure Libcap is installed for Linux hosts.

> **See Also:**
>
> Enabling and Using Host Monitoring for host monitoring instructions and prerequisites.

3.3 Oracle Audit Vault and Database Firewall Hardware Requirements

Install each Audit Vault Server and each Database Firewall (Oracle AVDF) onto its own dedicated x86 64-bit server (or Oracle VM 3.x).

You can use any Intel x86-64-bit hardware platform that is supported by Oracle Audit Vault and Database Firewall's embedded operating system. Oracle Audit Vault and Database Firewall uses Oracle Linux release 6 with the Unbreakable Enterprise Kernel (UEK) version 4. For a list of compatible hardware, refer to Hardware Certification List for Oracle Linux and Oracle VM. This list contains the minimum version of Oracle Linux certified with the selected hardware. All Oracle Linux updates starting with Oracle Linux release 6 as the minimum are also certified unless otherwise noted.

> **Note:**
>
> Do not install Audit Vault Server or Database Firewall on a server (or Oracle VM) that is used for other activities, because the installation process formats the server, deleting any existing data and operating systems.

3.3.1 Memory Requirements

Learn about the the minimum memory requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Each x86 64-bit server must have the following minimum memory:

- Audit Vault Server: 8 GB[1]
- Database Firewall: 8 GB

3.3.2 Disk Space Requirements

Learn about the minimum disk space requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Each x86 64-bit server must have a single hard drive with a minimum of the following disk space:

- Audit Vault Server: 220 GB (Recommended is 300 GB)
- Database Firewall: 220 GB

> **Note:**
>
> Provisioning disks greater than 4PB each for fresh installation is not optimal. The disks equal to or under 4PB ensure that only one disk partition is allocated per disk group on each physical disk.

3.3.3 Network Interface Cards

Learn about the recommended number of network interface cards (NICs) for each x86 64-bit server.

Oracle recommends the following number of network interface cards (NICs) for each x86 64-bit server on which you install the following components:

- 1 NIC for the Audit Vault Server
- At least 1 NIC for a Database Firewall operating as a proxy
- At least 2 NICs for a Database Firewall in DAM Mode (monitoring only)

[1] In this guide, 1 GB represents 2 to the 30th power bytes or in decimal notation 1,073,741,824 bytes.

- At least 3 NICs for a Database Firewall in DPE Mode (monitoring and blocking. If you install the Database Firewall with fewer than 3 NICs, then you must add more NICs to make the Database Firewall DPE mode possible.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide* for information on Database Firewall modes and proxy configuration.

3.4 Oracle Audit Vault and Database Firewall Software Requirements

Learn about the software requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).

- Java SE Requirement (page 3-4)
  The `AVCLI` command line utility that the Audit Vault Server administrator uses and the `avpack` utility (which is part of the software development kit) require Java SE version 8.
- Browser Requirements (page 3-4)
  Learn about the browser requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Audit Vault Agent Requirements (page 3-5)
  Learn about the Audit Vault Agent requirements.
- Host Monitor Requirements (page 3-5)
  Host Monitor enables the Database Firewall to directly monitor SQL traffic in a database.
- Target Requirements (page 3-6)
  For targets that are on Oracle Solaris running the LDoms Manager service, `svc:/ldoms/ldmd:default`, ensure that the target is using LDoms version 3.2.0.1 or later.

3.4.1 Java SE Requirement

The `AVCLI` command line utility that the Audit Vault Server administrator uses and the `avpack` utility (which is part of the software development kit) require Java SE version 8.

3.4.2 Browser Requirements

Learn about the browser requirements for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Note:

- See section Supported Browsers (page 2-10) for more information on the supported browsers.
- Latest version of Adobe Flash plug-in is required to view charts and interactive reports in the Audit Vault Server console. This requirement is for releases 12.2.0.12.0 and earlier.

3.4.3 Audit Vault Agent Requirements

Learn about the Audit Vault Agent requirements.

Ensure the supported Java version is installed on the Audit Vault Agent.

See Also:

Audit Vault Agent: Supported and Tested Java Runtime Environment (page 2-11)

3.4.4 Host Monitor Requirements

Host Monitor enables the Database Firewall to directly monitor SQL traffic in a database.

Recommended requirements for installing Host Monitor:

1. User installing the Host Monitor must have *root* privileges.
2. Ensure Audit Vault Agent is running on the host machine.
3. Ensure the latest version of the following packages from the OS vendor for the specific OS version are installed on the host machine:
   - Libcap (for Linux hosts only)
   - LibPcap
   - OpenSSL
4. Ensure *gmake* is installed. This is required for Host Monitor to run successfully.
5. Verify and allow communication on ports 2050 - 5100 for Database Firewall.
6. Check directory permissions. All the directories in the path of the Host Monitor install location should have 755 as the permission bits starting from the root directory. Also, Host Monitor must be installed in a *root* owned location.

Specific requirements for installing Host Monitor on Windows platform:

1. Host Monitor must be installed by user belonging to *Administrator* group.
2. Install Npcap that is available in the `avdf12.2.0.13.0-utility.zip` bundle in Oracle Software Delivery Cloud. It is part of the Oracle Audit Vault and Database Firewall installable files. Ensure to install Npcap in *WinPcap-API-compatible* mode.

3. Install the latest version of OpenSSL (1.1.1g or higher) libraries. Use OpenSSL version 1.1.1i for release Oracle AVDF 12.2.0.14.0.
4. Ensure the Windows target machine has the latest update of *Visual C++ Redistributable for Visual Studio 2010* (`MSVCRT.dll (*)` or later) package installed. This is a must to use Host Monitor on Windows.

Specific requirements for installing Host Monitor on Linux/Unix/AIX/Solaris platforms:

1. Host Monitor must be installed by *root* user.
2. Ensure the Input Output Completion Ports (IOCP) is set to `available` for IBM AIX on Power Systems (64-bit). It is set to `defined` by default.
3. Ensure Libcap is installed for Linux hosts.

> **See Also:**
>
> Enabling and Using Host Monitoring for host monitoring instructions and prerequisites.

3.4.5 Target Requirements

For targets that are on Oracle Solaris running the LDoms Manager service, `svc:/ldoms/ldmd:default`, ensure that the target is using LDoms version 3.2.0.1 or later.

4 Post-Install Configuration Tasks

Learn about the post-installation tasks for Oracle Audit Vault and Database Firewall (Oracle AVDF).

Some of these tasks are mandatory.

- Audit Vault Server Post-Installation Tasks (page 4-1)
  After installing the Audit Vault Server, there are post-installation tasks that you must do.
- Database Firewall Post-Installation Tasks (page 4-8)
  Learn about Database Firewall post-installation tasks.
- Networking Setup And Configuration (page 4-10)
  Oracle Audit Vault and Database Firewall (Oracle AVDF) can be setup or configured for access through DNS.

4.1 Audit Vault Server Post-Installation Tasks

After installing the Audit Vault Server, there are post-installation tasks that you must do.

You must set the usernames and passwords of its administrator and auditor, and the passwords of its root and support user. You can also set the time and domain name service (DNS) servers of the Audit Vault Server.

Apply the deprecated ciphers patch (`Deprecated-Cipher-Removal.zip`) to remove old ciphers, post AVS install or upgrade. Apply this patch on Audit Vault Server after installation or upgrade to 12.2.0.13.0 (or later). Before applying the patch, make sure that all the Audit Vault Agents and Host Monitor Agents are upgraded to 12.2.0.13.0.

> **Note:**
>
> The Audit Vault Server reads the audit log from the target that contains the timestamp of the event. Without this synchronization, events may appear to be archived to the Audit Vault Server before they occur and alerts may appear to be sent before their triggering events occur.

- Accessing the Audit Vault Server Post-Install Configuration Page (page 4-2)
  Access the Audit Vault Server post-installation configuration page.
- Setting the Usernames and Passwords of Audit Vault Server Users (Required) (page 4-3)
  Set up usernames and passwords for the Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Setting the Audit Vault Server Time (Strongly Recommended) (page 4-6)
  Steps to set the Audit Vault Server time.
- Setting the Audit Vault Server DNS Servers (Recommended) (page 4-7)
  Steps to set the DNS servers for the Audit Vault Server.

4.1.1 Accessing the Audit Vault Server Post-Install Configuration Page

Access the Audit Vault Server post-installation configuration page.

1. Using a browser, go to the Audit Vault Server console. Ensure that the browser version you are using supports TLS 1.2 protocol. See Supported Browsers (page 2-10) for complete information.

   ```
   https://ip_address
   ```

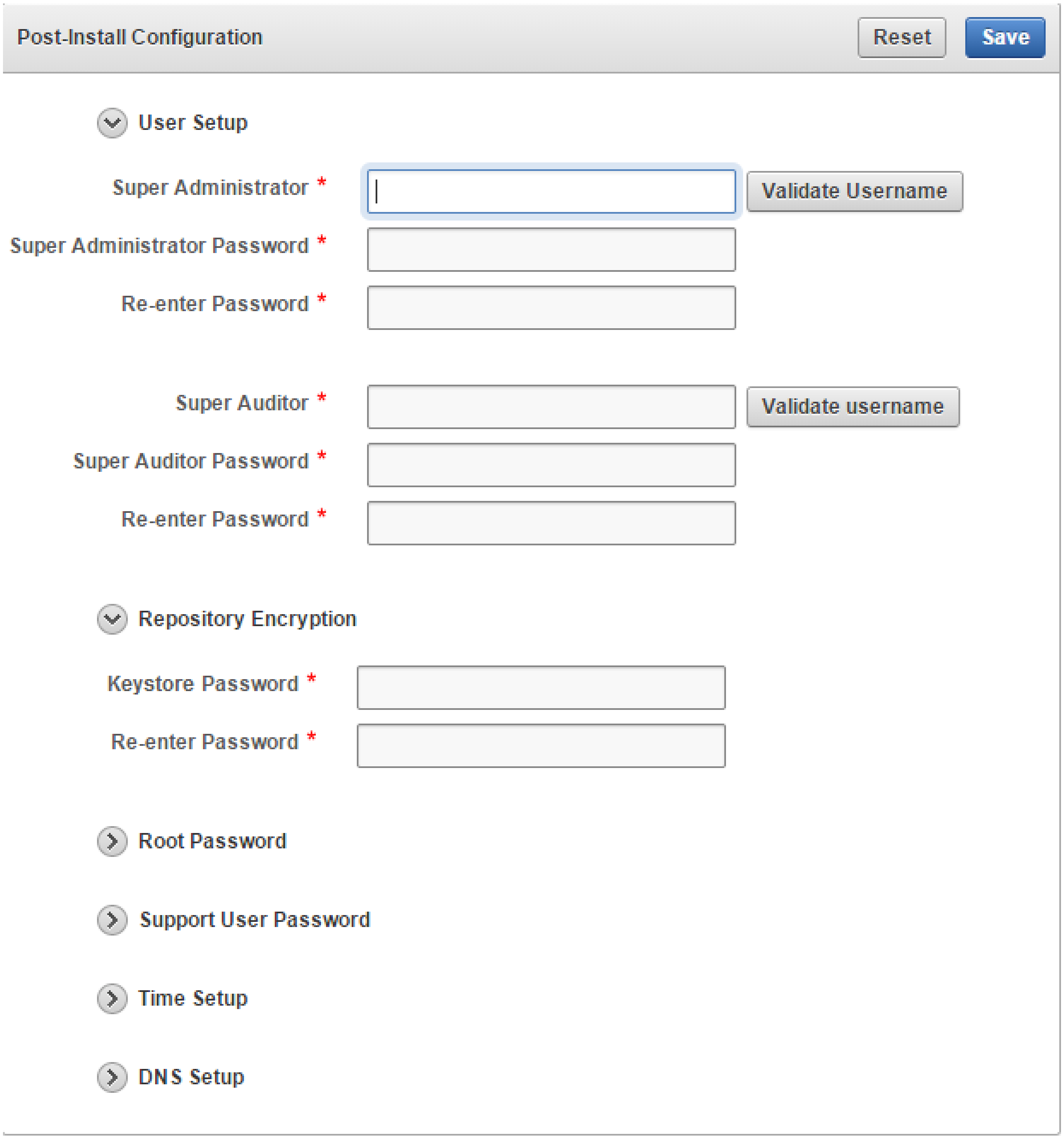
   For *ip_address*, use the IP address of the Audit Vault Server. See Installing an Audit Vault Server or Database Firewall (page 1-5).

   If you see a message saying that there is a problem with the Web site security certificate, this is due to a self-signed certificate. Click the **Continue to this website** (or similar) link. (You can generate a certificate request later to avoid this message. See *Oracle Audit Vault and Database Firewall Administrator's Guide*.)

   You are prompted to enter the installation passphrase you created during the installation procedure.

2. Type the installation passphrase that you created in Installing an Audit Vault Server or Database Firewall (page 1-5) and click **Login**.

   The Post-Install Configuration page appears:



From this page, you must set the usernames and passwords (required), set up the time, and DNS servers.

4.1.2 Setting the Usernames and Passwords of Audit Vault Server Users (Required)

Set up usernames and passwords for the Oracle Audit Vault and Database Firewall (Oracle AVDF).

In the post-install configuration page, you set up usernames and passwords for the Oracle Audit Vault and Database Firewall administrator, auditor, support, and root users.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Concepts Guide* for a description of each user.

> **Note:**
>
> Do not use the root or support users unless instructed to do so in documentation or by a customer support representative.

- About Administrator and Auditor User Names (page 4-4)
  Oracle recommends that you create administrator and auditor user accounts after you install Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Password Requirements (page 4-5)
  Set password management guidelines for the Audit Vault and Database Firewall (Oracle AVDF) user accounts.
- Setting the Passwords For Audit Vault Server Users (page 4-5)
  Steps for setting the passwords for the Audit Vault Server users.

4.1.2.1 About Administrator and Auditor User Names

Oracle recommends that you create administrator and auditor user accounts after you install Oracle Audit Vault and Database Firewall (Oracle AVDF).

The administrator and auditor user names must be simple SQL names of 1 to 30 characters, and must follow these rules:

- The first character is alphabetical.
- Each remaining character is either alphanumeric or an underscore (_), dollar sign ($), or number sign (#).

> **Note:**
>
> The administrator and auditor user names are upshifted (that is, any lowercase alphabetic characters are replaced by their uppercase equivalents). Also, the Audit Vault Server does not support quoted user names.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Concepts Guide* for a description of each user account.

4.1.2.2 Password Requirements

Set password management guidelines for the Audit Vault and Database Firewall (Oracle AVDF) user accounts.

For example, you may require that users change their passwords on a regular basis, such as every 120 days, and that they create passwords that are not easily guessed.

The following sections describe the minimum password requirements for Oracle Audit Vault and Database Firewall.

Requirements for Passwords Containing Unicode Characters

If your password contains unicode characters (such as non-English characters with accent marks), the password requirement is that it:

- Be between 8 and 30 characters long.

Requirements for English-Only (ASCII) Passwords

If you are using English-only, ASCII printable characters, Oracle Audit Vault and Database Firewall requires that passwords:

- Be between 8 and 30 characters long.
- Contain at least one of each of the following:
  - Lowercase letters: a-z.
  - Uppercase letters: A-Z.
  - Digits: 0-9.
  - Punctuation marks: comma (,), period (.), plus sign (+), colon(:), exclamation mark (!), and underscore (_)
- Not contain double quotes ("), back space, or control characters.

In addition, Oracle recommends that passwords:

- Not be the same as the user name.
- Not be an Oracle reserved word.
- Not be an obvious word (such as welcome, account, database, and user).
- Not contain any repeating characters.

> **See Also:**
>
> *Oracle Database Security Guide* for additional guidelines on how you can strengthen passwords for your site.

4.1.2.3 Setting the Passwords For Audit Vault Server Users

Steps for setting the passwords for the Audit Vault Server users.

To set the passwords of the Audit Vault Server administrator, auditor, root, and support user:

1. Access the Audit Vault Server Post-Install Configuration page.
2. Under **User Setup**:
   - In the **Super Administrator** field, enter the administrative user name (recommended).
   - Under the **Super Administrator** field, enter the administrator **Super Administrator Password**, then confirm it in the **Re-enter Password** field.
   - Click **Validate username**.

     The administrator username that you entered is validated. If this name is valid, then you can use it; if not, then you must enter a valid name.
   - In the **Super Auditor** field, enter the super auditor user name (recommended).
   - Under the **Super Auditor**, field, enter the auditor **Super Auditor Password**, then confirm it in the **Re-enter Password** field.
   - Click **Validate username**.

     The auditor username that you entered is validated. If this name is valid, then you can use it; if not, then you must enter a valid name.
3. (New Full Installations Only) Under **Repository Encryption**, enter the **Keystore Password**, and then re-enter it.

   On new, full installations of Oracle Audit Vault and Database Firewall 12.2, audit event data in the Audit Vault Server's repository is automatically encrypted using Oracle Database Transparent Data Encryption (TDE). The repository encryption keystore password is required to reset the TDE master key.
4. Under **Root Password**, in the fields labeled **Root Password** and **Re-enter New Password**, type the password for root.
5. Under **Support User Password**, in the fields labeled **Support Password** and **Re-enter New Password**, type the password for the support user.

> **See Also:**
>
> Accessing the Audit Vault Server Post-Install Configuration Page (page 4-2)

4.1.3 Setting the Audit Vault Server Time (Strongly Recommended)

Steps to set the Audit Vault Server time.

To set the Audit Vault Server time:

1. Access the Audit Vault Server Post-Install Configuration page.
2. Expand the **Time Setup** section.
3. Select either **Set Manually** or **Use NTP**.

> **Note:**
>
> Oracle strongly recommends that you select **Use NTP**. In addition, it is recommended that you also use an NTP service on your secured targets to avoid confusion on timestamps on the alerts raised by the Audit Vault Server.

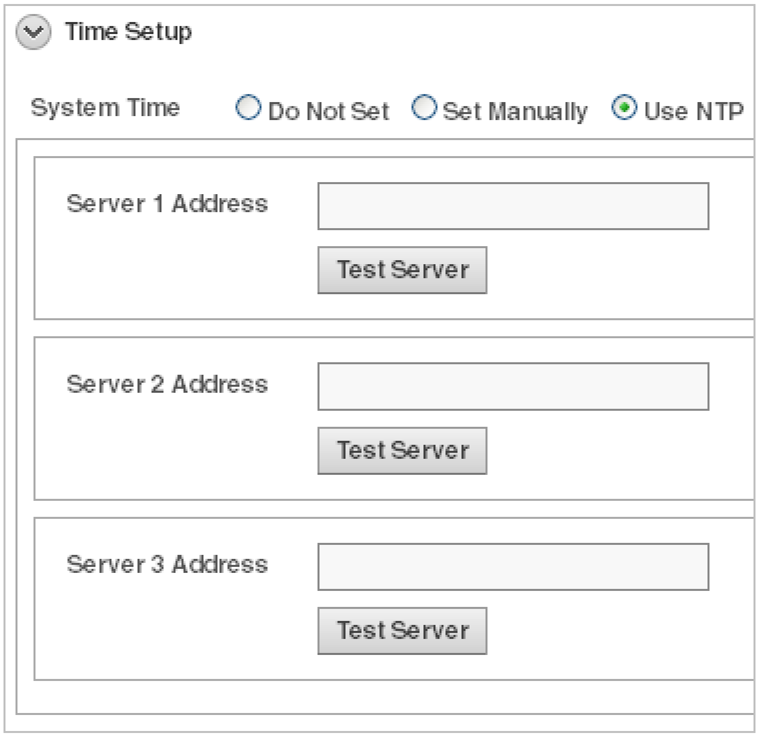
4. If in step 3 (page 4-6) you selected **Use NTP**, then for each of the fields **Server 1 Address**, **Server 2 Address**, and **Server 3 Address**:

   a. Type either the IP address or name of a preferred time server.

      If you type a name, the DNS server specified in the System Services page is used for name resolution.

   b. Click **Test Server**.

      The time from the specified server appears.



Time Setup

System Time ○ Do Not Set ○ Set Manually ● Use NTP

Server 1 Address

Server 2 Address

Server 3 Address

5. If in step 3 (page 4-6) you selected **Set Manually**, then set the **Date** fields to your current local day and time.

6. Either click **Save** or proceed to set the DNS servers for the Audit Vault Server.

4.1.4 Setting the Audit Vault Server DNS Servers (Recommended)

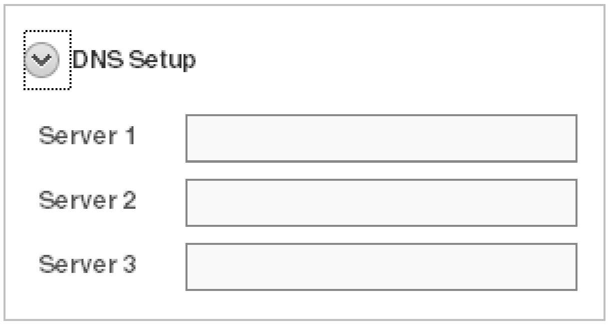
Steps to set the DNS servers for the Audit Vault Server.

The Audit Vault Server DNS servers are used to resolve any host names that Audit Vault Server might use.

> **Note:**
>
> Set Audit Vault Server DNS server values only if the network has DNS servers, otherwise system performance will be impaired.

To set the DNS servers for the Audit Vault Server:

1. Access the Audit Vault Server Post-Install Configuration page.
2. Expand the **DNS Setup** section.



DNS Setup

Server 1	
Server 2	
Server 3	

3. Enter the IP address(es) of up to three DNS servers on the network in the **Server 1**, **Server 2**, and **Server 3** fields.

   Leave the fields blank if there are no DNS servers.
4. Click **Save** (in the upper right corner of the page).

4.2 Database Firewall Post-Installation Tasks

Learn about Database Firewall post-installation tasks.

After you install the Database Firewall, you may set the passwords for `support` user. This is the Linux operating system user account on the Audit Vault Server.

- Accessing the Database Firewall Post-Install Configuration Page (page 4-8)
  Steps on how to access the Database Firewall Post-Install Configuration page.
- Setting the Passwords of Database Firewall Users (Required) (page 4-9)
  Learn about and set the Database Firewall users passwords.

4.2.1 Accessing the Database Firewall Post-Install Configuration Page

Steps on how to access the Database Firewall Post-Install Configuration page.

To access the Database Firewall Post-Install Configuration page:

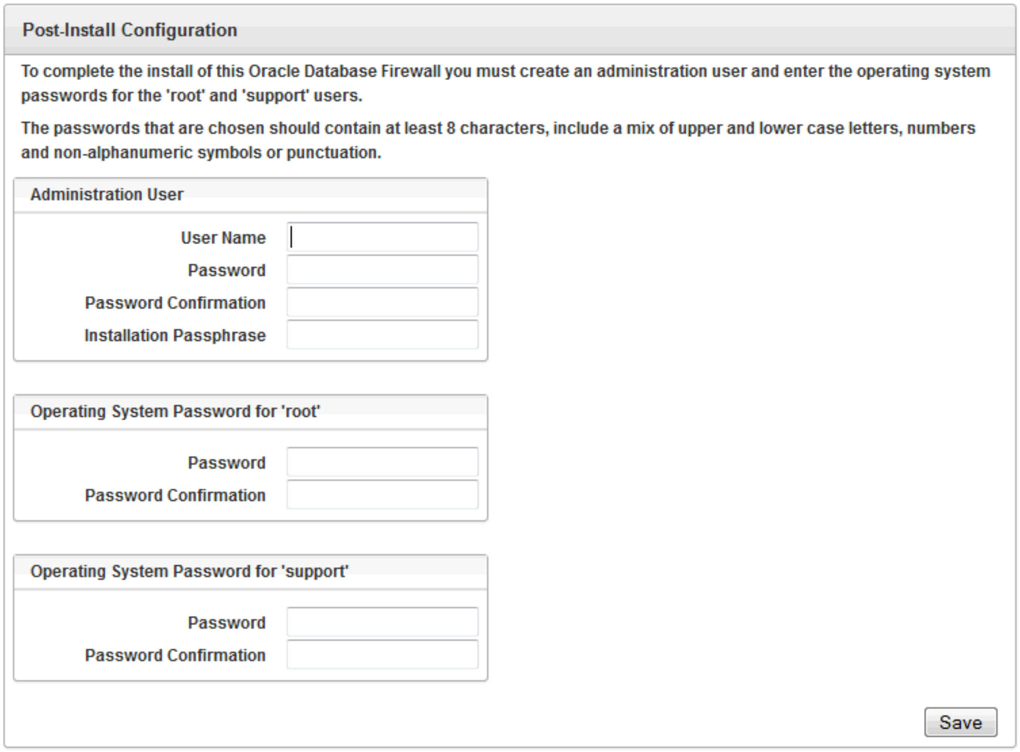
1. Using a browser, go to the Database Firewall console. Ensure that the browser version you are using supports TLS 1.2 protocol. See Supported Browsers (page 2-10) for complete information.

   ```
   https://ip_address
   ```

   For *`ip_address`*, use the IP address of the Database Firewall. See section Installing an Audit Vault Server or Database Firewall (page 1-5).

2. You are prompted to enter the installation passphrase. Type the installation passphrase that you created in "Installing an Audit Vault Server or Database Firewall (page 1-5)", step 6 (page 1-6)) and click **Login**.

   The Post-Install Configuration page appears:



Post-Install Configuration

To complete the install of this Oracle Database Firewall you must create an administration user and enter the operating system passwords for the 'root' and 'support' users.

The passwords that are chosen should contain at least 8 characters, include a mix of upper and lower case letters, numbers and non-alphanumeric symbols or punctuation.

Administration User

User Name
Password
Password Confirmation
Installation Passphrase

Operating System Password for 'root'

Password
Password Confirmation

Operating System Password for 'support'

Password
Password Confirmation

From this page, you can set the passwords of the Database Firewall users.

> **See Also:**
>
> Setting the Passwords of Database Firewall Users (Required) (page 4-9)

4.2.2 Setting the Passwords of Database Firewall Users (Required)

Learn about and set the Database Firewall users passwords.

- About Database Firewall User Passwords (page 4-9)
  Learn about Oracle's recommendations for Database Firewall user passwords.
- Setting The Passwords For Database Firewall Users (page 4-10)
  Set the passwords of the Database Firewall administrator, root, and support user.

4.2.2.1 About Database Firewall User Passwords

Learn about Oracle's recommendations for Database Firewall user passwords.

Passwords need not be unique; however, Oracle recommends that passwords:

- Have at least one uppercase alphabetic, one alphabetic, one numeric, and one special character (plus sign, comma, period, or underscore).
- Be between 8 and 30 characters long.
- Be composed of the following characters:
  - Lowercase letters: a-z.
  - Uppercase letters: A-Z.
  - Digits: 0-9.
  - Punctuation marks: comma (,), period (.), plus sign (+), colon(:), and underscore (_).
- Not be the same as the user name.
- Not be an Oracle reserved word.
- Not be an obvious word (such as welcome, account, database, and user).
- Not contain any repeating characters.

4.2.2.2 Setting The Passwords For Database Firewall Users

Set the passwords of the Database Firewall administrator, root, and support user.

1. Under the heading **Administration User**:
   a. In the field **User Name**, type the user name of the Database Firewall Administration User.
   b. In the field **Password**, type the password of the Database Firewall Administration User.
   c. In the field **Password Confirmation**, retype the password.
   d. In the field **Installation Passphrase**, type the installation passphrase that you created in "Installing an Audit Vault Server or Database Firewall (page 1-5)", step 6 (page 1-6).
2. Under the heading **Operating System Password for root**, in the fields **Password** and **Password Confirmation**, type the password for root.
3. Under the heading **Operating System Password for support**, in the fields **Password** and **Password Confirmation**, type the password for support user.
4. Click **Save**.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Concepts Guide* for a description of each user account.

4.3 Networking Setup And Configuration

Oracle Audit Vault and Database Firewall (Oracle AVDF) can be setup or configured for access through DNS.

In this case the host name must match the FQDN used for access. This regenerates the appliance certificate to match the new host name.

See Also:

- *Oracle Audit Vault and Database Firewall Administrator's Guide*
- *Oracle Audit Vault and Database Firewall Administrator's Guide*

5 Migrating the Configuration from Oracle Audit Vault to Oracle Audit Vault and Database Firewall

You can migrate the configuration from Oracle Audit Vault Release 10.3 to Oracle Audit Vault Database Firewall (Oracle AVDF) Release 12.2.

5.1 About Migrating Oracle Audit Vault to Oracle Audit Vault and Database Firewall

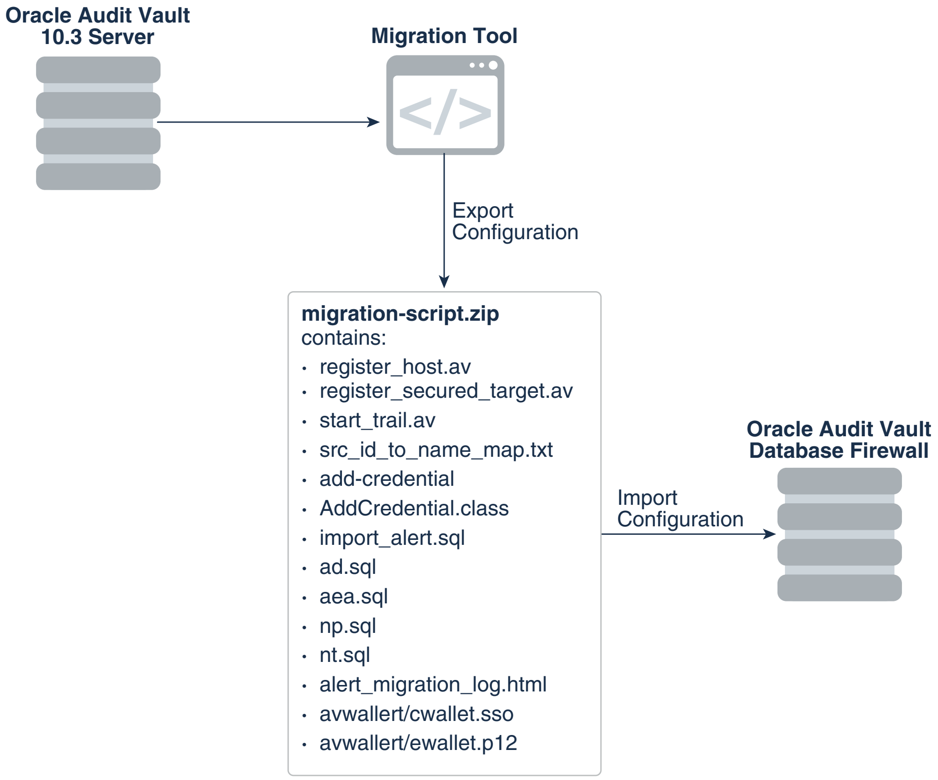
Process to migrate from Oracle Audit Vault to Oracle Audit Vault and Database Firewall (Oracle AVDF).

When you migrate Oracle Audit Vault Release 10.3 to Oracle Audit Vault and Database Firewall Release 12.2, you must perform tasks such as migrating the Audit Vault hosts and alert definitions, setting up the agent, and so on, for Oracle Audit Vault and Database Firewall.

To perform the migration, you use an Oracle-supplied Java migration tool, which is platform independent. You can run it on the Oracle Audit Vault Release 10.3 supported platforms, which are Microsoft Windows and UNIX, and you can run it on the Linux x64 platform for Oracle Audit Vault and Database Firewall Release 12.2.

Figure 5-1 (page 5-2) illustrates the migration path from Oracle Audit Vault Release 10.3 to Oracle Audit Vault and Database Firewall 12.2.

Figure 5-1 Migration Path for Oracle Audit Vault to Oracle Audit Vault and Database Firewall



migration-script.zip
contains:

- register_host.av
- register_secured_target.av
- start_trail.av
- src_id_to_name_map.txt
- add-credential
- AddCredential.class
- import_alert.sql
- ad.sql
- aea.sql
- np.sql
- nt.sql
- alert_migration_log.html
- avwallert/cwallet.sso
- avwallert/ewallet.p12

Configurations Migrated

The migration process migrates the following configurations from Oracle Audit Vault 10.3 to Oracle Audit Vault and Database Firewall 12.2:

- Oracle Audit Vault 10.3 agents to Oracle Audit Vault and Database Firewall 12.2 hosts
- Oracle Audit Vault 10.3 sources to Oracle Audit Vault and Database Firewall 12.2 secured targets
- Oracle Audit Vault 10.3 collectors to Oracle Audit Vault and Database Firewall 12.2 audit trails
- Secured target credentials
- Wallet for secured target user credentials
- Alert definitions

- Alert email actions
- Alert statuses
- Notification profiles
- Notification templates

Migration Overview

The general steps that you will perform are as follows:

1. Prepare Oracle Audit Vault 10.3.
2. Run the migration tool on Audit Vault 10.3 to export the configurations.
3. Check the migration logs for errors.
4. Prepare Oracle Audit Vault and Database Firewall 12.2 to receive the Oracle Audit Vault 10.3 configuration.
5. Run the migration scripts on Oracle Audit Vault and Database Firewall 12.2 to import the Oracle Audit vault 10.3 configuration.
6. Check Oracle Audit Vault and Database Firewall 12.2 status to complete the migration process.

5.2 Step 1: Prepare Oracle Audit Vault Release 10.3 for Migration

In Step 1, before you can perform the migration, you must download the migration utility files and set the correct permissions for the AVSYS user and the migration files.

1. Download the migration-tool.zip file to a temporary directory on the computer where there Audit Vault Server is located.

   The migration tool enables the generation of the Oracle Audit Vault 10.3 avcli scripts that are necessary for the migration. These scripts migrate the agents, sources, and collectors from Oracle Audit Vault 10.3 to the host, secured target, and audit trail used in Oracle Audit Vault and Database Firewall 12.2.

2. Unzip migration-tool.zip file.

   The zip file contains the following files: migration.sql, README.txt, AddCredential.class, gen-migrate (which you will need to invoke to generate the final avcli scripts), add-credential, import_alert.sql, migrate_alert.sql, migrate_ad.sql, migrate_aea.sql, migrate_as.sql, migrate_noti_pro.sql, migrate_noti_temp.sql.

3. Log in to SQL*Plus on the Audit Vault server instance as a user who has been granted the Oracle Database Vault DV_ACCTMGR role.

   Because Oracle Database Vault is enabled in this release of Oracle Audit Vault, you cannot use the SYS or SYSTEM accounts to create or modify user accounts.

   For example:

   ```
   sqlplus dbv_acctmgr
   Enter password: password
   ```

4. Unlock the AVSYS account.

```
ALTER USER AVSYS UNLOCK;
```

5. Connect as the `SYS` user.

   ```
   connect sys as sysdba
   Enter password: password
   ```

6. Grant the `CREATE ANY DIRECTORY` and `DROP ANY DIRECTORY` system privileges to user `AVSYS`.

   ```
   GRANT CREATE ANY DIRECTORY, DROP ANY DIRECTORY TO AVSYS;
   ```

7. Grant the `EXECUTE` privilege to the `SYS.UTL_FILE` file to user `AVSYS`.

   ```
   GRANT EXECUTE ON SYS.UTL_FILE TO AVSYS;
   ```

8. Exit SQL*Plus.

9. If the `gen-migrate` tool is not executable, then change its permissions to make it an executable.

   For example:

   ```
   chmod 744 gen-migrate
   ```

5.3 Step 2: Generate the Oracle Audit Vault Release 10.3 Configuration Data

In Step 2, you run a procedure that generates two files, `migration-script.zip` and `migration.log`. The `migration-script.zip` file contains the Audit Vault 10.3 configuration that you are exporting, and the `migration.log` file contains a log of actions and possible errors that took place during this procedure.

1. Log in to the Audit Vault Server terminal where you downloaded and unzipped the `migration-tool.zip` file.

2. In the Oracle Audit Vault and Database Firewall server, set the `ORACLE_HOME` environment variable.

   C shell:

   ```
   setenv ORACLE_HOME fullpath
   ```

   Bourne/Korn shell:

   ```
   ORACLE_HOME=fullpath
   export ORACLE_HOME
   ```

3. Execute the `gen-migrate` tool.

   ```
   ./gen-migrate
   Enter the path: location_for_output
   Enter AVSYS password: AVSYS_password
   ```

   Provide the directory path where migration scripts will be generated. If you do not provide a path, then the migration script will be generated in the current directory. The path is optional but you must provide the `AVSYS` password.

4. Check the `migration.log` file for possible errors and correct them.

   Typical errors can include the following:

   - `AVSYS cannot create directory`

- `Could not get IP for host "`*`host_name`*`"`: This error can occur if you try to register the host without using the `with ip` option. In the `register_host.av` script, modify the `register host` command to include the `with ip` option.
- `Can not register host "`*`host_name`*`"`. Register the host manually.

If you cannot resolve the errors, then contact Oracle Support.

5.4 Step 3: Prepare Oracle Audit Vault and Database Firewall Release 12.2 for the Migration

In Step 3, put specific settings in place to ensure that Oracle Audit Vault and Database Firewall (Oracle AVDF) is using the same settings as Oracle Audit Vault.

1. Verify that the SMTP server is functioning properly for alert email notifications.
2. Set up the time zone settings and the keyboard settings.
3. Set up the network services.

> **See Also:**
>
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information about configuring the email notification service.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information about specifying the server date, time, and keyboard settings.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information about configuring network services.

5.5 Step 4: Migrate the Oracle Audit Vault Configuration to Oracle Audit Vault and Database Firewall

In Step 4, unzip the `migration-script.zip` file to the Oracle Audit Vault and Database Firewall (Oracle AVDF) server and then complete the migration.

1. Copy the `migration-script.zip` file from the Oracle Audit Vault 10.3 server to the server where the Oracle Audit Vault and Database Firewall 12.2 server is installed.
2. If necessary, set the `ORACLE_HOME` variable for Audit Vault.

   If you had already set the `ORACLE_HOME` variable, then run the following commands.

   ```
   ssh support@avdf-ip
   su -
   su oracle
   ```
3. `cd` to the directory where you want to store the `avcli` scripts.
4. Unzip the `migration-scripts.zip` file into this directory.

   ```
   unzip path_to_zip_file/migration-scripts.zip .
   ```

   The `migration-script.zip` file contains the following files:

- `register_host.av`: Has all the `avcli` commands to register hosts
- `register_secured_target.av`: Has commands to register secured targets
- `start_trail.av`: Has commands to start the trails for registered secured targets
- `AddCredentail.class`: Java class file to add the secured target credential into the Oracle Audit Vault and Database Firewall server.
- `add-credential`: Tool to invoke the `java` program to add the secured target credential into the Oracle Audit Vault and Database Firewall server.
- `avwallet` (directory): Has the wallet which has secured target user credential
- `src_id_to_name_map.txt`: Mapping from the source ID to secured target name
- `import_alert.sql`: The master script to import alert configuration into Oracle Audit Vault and Database Firewall
- `ad.sql`: Alert definitions
- `aea.sql`: Alert email actions
- `as.sql`: Alert statuses
- `np.sql`: Notification profiles
- `nt.sql`: Notification templates
- `nt.sql`: Notification templates

5. Ensure that the files listed in the preceding step have all been unzipped and appear in the directory.

6. Review the `avcli` scripts, `register_host.av` and `register_secured_target.av`, before you use them for the final migration, described later in this procedure.

   If there are any problems, then modify the scripts to rectify the problems.

7. If there is a DB2 source that must be migrated using the scripts, then modify the `register_secured_target.av` file before using it for migration.

   Oracle Audit Vault 10.3 does not store DB2 port and database name information. The Oracle Audit Vault and Database Firewall `register target` setting must have this information, so therefore, you must modify the `register_secured_target.av` file to include it.

   For example, `register_secured_target.av` will have register secured target setting as follows:

   ```
   REGISTER SECURED TARGET my_target OF SECURED TARGET TYPE "IBM DB2 LUW" AT
   jdbc:av:db2://db2host.oracle.com
   authenticated by administrator/password
   ```

   This command omits the port number and database name, which are required to connect to the DB2 source. You must then modify the command in the following way. The port number and database name are in bold.

   ```
   REGISTER SECURED TARGET my_target OF SECURED TARGET TYPE "IBM DB2 LUW" AT
   jdbc:av:db2://db2host.example.com:50000/SAMPLE
   authenticated by administrator/password;
   ```

8. As the Oracle Audit Vault and Database Firewall administrative user, run `register_host.av` using `avcli`.

   ```
   avcli -f register_host.av -u AVDF_admin_user_name
   ```

   This command registers all the hosts that are included in `register_host.av` with the Oracle Audit Vault Server.

9. Manually download the `agent.jar` file from the Audit Vault Server to the host computers that are registered in the previous step.

10. Start the agent on these registered hosts.

    For example:

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

    You must perform this manually because the `agent.jar` file must be put on a different host from the current computer. You can find this key from the Audit Vault Server, under the host tab.

11. After the agents start, register the secured target using `register_secured_target.av`.

    ```
    avcli -f register_secured_target.av -u AVDF_admin_user_name
    ```

12. Run the `add-credential` tool to add the secured target user credential.

    ```
    ./add-credential
    AV admin user: AVDF_admin_user_name
    Password: password
    ```

    Errors are written to the migration log file. This log file is generated in the current directory. Check this log file after you run the `add-credential` tool for possible errors and how to resolve them. The migration log file is described in "Step 2: Generate the Oracle Audit Vault Release 10.3 Configuration Data (page 5-4)".

13. From SQL*Plus, as the Oracle Audit Vault and Database Firewall auditor or super auditor, import the alert-related definitions by running the `import_alert.sql` script.

    ```
    sqlplus auditor-super_auditor
    Enter password: password
    @import_alert.sql
    ```

14. Check the `alert_migration_log.html` file for any alert definitions that must be modified.

    The `alert_migration_log.html` file, generated in the preceding step, lists the alert definitions and notification templates that could not be ported.

15. Check the import.log file if there were any errors while importing alerts.

16. Start the collection audit trails for the secured targets that you registered in Step 11 (page 5-7), using the `start_trail.av` script.

    ```
    avcli -f start_trail.av -u AVDF_admin_user_name
    ```

5.6 Step 5: Perform Post-Migration Procedures

In Step 5, to complete the migration process, you should ensure that the agents, audit trails, alerts, and other components are running, as well as revoke the privileges that you had granted to the Release 10.3 `AVSYS` user before the migration process.

1. Log in to SQL*Plus on the Audit Vault server instance as user who has the `ALTER USER` system privilege.

   For example, if Oracle Database Vault is enabled, then log in as a user who has been granted the `DV_ACCTMGR` role.

   ```
   sqlplus dbv_acctmgr
   Enter password: password
   ```

2. Lock the `AVSYS` account.

   ```
   ALTER USER AVSYS LOCK;
   ```

3. Connect as user `SYS`.

   ```
   sqlplus sys as sysdba
   Enter password: password
   ```

4. Revoke the privileges that you had granted to `AVSYS` earlier.

   ```
   REVOKE CREATE ANY DIRECTORY, DROP ANY DIRECTORY FROM AVSYS;
   ```

5. Test the Audit Vault Server system operation.
6. Ensure that the agents are working.
7. Ensure that the secured targets are set up properly.

   In the Audit Vault Server console, click the **Secured Targets** tab to check the secured targets.

8. Ensure that the audit trails are started and running with new records archived.
9. Check the alert definitions, alert email actions, alert statues, notification profiles, notification templates are set up properly.

   You can check the status of these alerts and notifications from the Audit Vault Server console.

10. Ensure that the alerts are generated and notifications are sent to the correct recipients.

> **See Also:**
>
> - *Oracle Audit Vault and Database Firewall Auditor's Guide* to modify alerts and notifications.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* to view the status of audit trails.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* to view the status and details of an Agent.
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* to test the Audit Vault Server system operation.

6 Upgrading Oracle Audit Vault and Database Firewall

This chapter provides information on upgrades and Bundle Patch updates and how to upgrade from the previous release of Oracle Audit Vault and Database Firewall.

> **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.

6.1 Upgrading Oracle Audit Vault and Database Firewall

Learn the steps to upgrade Oracle Audit Vault and Database Firewall (Oracle AVDF).

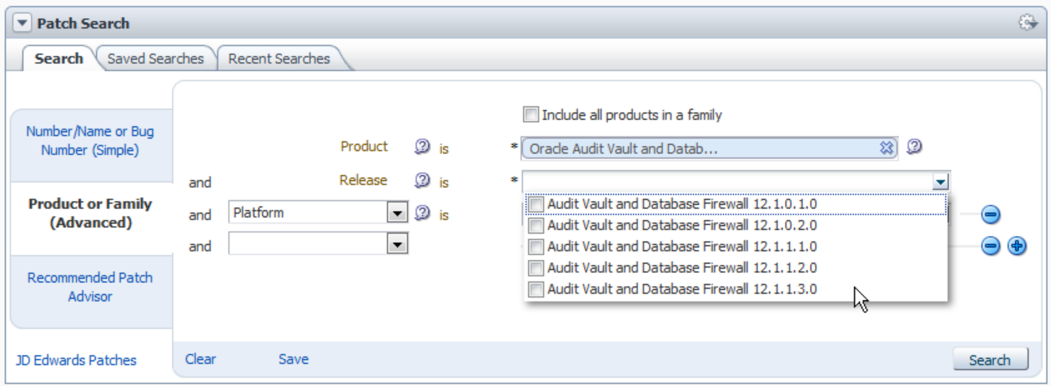
> **Caution:**
>
> *Oracle Audit Vault and Database Firewall* release `12.2.0.11.0` does not support Niagara cards. Do not upgrade to this release if you have Niagara cards in your system.

You can upgrade Oracle Audit Vault and Database Firewall from the previous release.

> **Note:**
>
> - You must first take backup prior to performing any upgrade.
> - Oracle Audit Vault and Database Firewall versions `12.2.0.0.0` and above must first upgrade to `12.2.0.9.0`, and then to the latest version in release `12.2`.
> - Oracle Audit Vault and Database Firewall versions `12.1.2.7.0` and above in `12.1.x` series must first upgrade to `12.2.0.8.0`, then to `12.2.0.9.0`, and then to the latest version in release `12.2`. Follow the instructions in section Mandatory Pre-upgrade Patch (page 6-4) for upgrading to `12.2.0.9.0`.
> - Oracle Audit Vault and Database Firewall versions prior to `12.1.2.7.0` must first upgrade to `12.2.0.2.0`, then to `12.2.0.9.0`, and then subsequently to the latest version in release `12.2`.
> - In all the above cases, you may perform a single backup operation prior to performing the first upgrade.
> - In case you have a Niagara card in your system, then contact Oracle support before performing the upgrade task. The Niagara drivers built for UEK 3 that is shipped with previous versions of Audit Vault and Database Firewall are not compatible with UEK 4 and Audit Vault and Database Firewall `12.2.0.4.0`. This leads to failure of the upgrade and subsequent boots of the system.
> - You must keep sufficient disk space if there is huge amount of event data. The amount of disk space required is about 5% of the total event log data size.

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.

   The following image is an example only:


Patch Search
Search
Saved Searches
Recent Searches
Number/Name or Bug Number (Simple)
Product or Family (Advanced)
Recommended Patch Advisor
JD Edwards Patches
Include all products in a family
Release
and
Audit Vault and Database Firewall 12.1.0.1.0
Audit Vault and Database Firewall 12.1.0.2.0
Audit Vault and Database Firewall 12.1.1.1.0
Audit Vault and Database Firewall 12.1.1.2.0
Audit Vault and Database Firewall 12.1.1.3.0
Clear
Save
Search

Product is * Oracle Audit Vault and Datab...

and Platform is

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 access the README file, which has the upgrade instructions.

6. Follow the instructions in the README file to complete the upgrade.

6.2 Pre-upgrade Tasks

Learn about the pre-upgrade prerequisites before upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF).

- Host Monitor Migration on Windows (page 6-4)
  If you are using Host Monitoring on Windows platform, then install Npcap and update OpenSSL libraries on Windows before upgrading to 12.2.0.13.0.
- Mandatory Pre-upgrade Patch (page 6-4)
  Install a mandatory pre-upgrade patch before upgrading to Oracle Audit Vault and Database Firewall (Oracle AVDF) release `12.2.0.9.0`.
- Back Up The Current Oracle Audit Vault And Database Firewall Installation (page 6-9)
  Before upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), you must back up some Audit Vault Server and Audit Vault Agent components.
- Release Existing Tablespaces That Are Retrieved Manually (page 6-10)
  Learn about releasing tablespaces retrieved manually.
- Preserve Customization In Log Rotate File (page 6-10)
  Preserve customizations applied to the log rotate configuration files during upgrade of Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Check For Busy Devices Before Starting The Upgrade Process (page 6-10)
  Check for any busy devices before starting the Oracle Audit Vault and Database Firewall (Oracle AVDF) upgrade process.

6.2.1 Host Monitor Migration on Windows

If you are using Host Monitoring on Windows platform, then install Npcap and update OpenSSL libraries on Windows before upgrading to 12.2.0.13.0.

Complete the steps in the following sections:

- Deploying the Agent and Host Monitor on Microsoft Windows Hosts
- Step 5: Create a Network Audit Trail to set the `network_device_name_for_hostmonitor` collection attribute post installation of Npcap and OpenSSL.

6.2.2 Mandatory Pre-upgrade Patch

Install a mandatory pre-upgrade patch before upgrading to Oracle Audit Vault and Database Firewall (Oracle AVDF) release `12.2.0.9.0`.

Before upgrading to Oracle AVDF release `12.2.0.9.0`, apply the Mandatory AVDF BP9 Pre-upgrade Patch (Doc ID 2457374.1) (`bug_28581135_agentpatch.zip`).

Note:

- This pre-upgrade patch must be executed only if you are upgrading to Oracle Audit Vault and Database Firewall release `12.2.0.9.0` from any release between `12.2.0.0.0` and `12.2.0.8.0`.
- This pre-upgrade patch is not applicable if you are upgrading to Oracle Audit Vault and Database Firewall release `12.2.0.10.0` or above from release `12.2.0.9.0`.
- This patch **must** be executed only if all the hosts on which your Audit Vault Agents are running, have `Java` version *1.8*. If you have hosts which have `Java` version *1.6*, then update those hosts to `Java` *1.8* before installing this patch.
- In case of High Availability configuration of Audit Vault Server this *Pre-upgrade Agent Patch* has to be applied only on the primary Audit Vault Server.
- For deploying Audit Vault Agent on `IBM AIX`, ensure `OpenSSL 64-bit` version *1.0.1* (or later) is installed.
- Host Monitor requires `OpenSSL 64-bit` version *1.0.1* (or later), on the target machine.

Requirements

> **Note:**
>
> - This patch is located in the zip files extracted in section *Instructions To Apply This Bundle Patch*.
> - If you do not meet the above mentioned requirements, or in case you are not certain that you meet these requirements, log a Service Request and contact Oracle support.
> - Ensure that all Agents are running when this patch is applied.
> - Stopped Agents are not updated with this patch.

To apply the patch:

1. Make sure that all the audit trails are stopped.
   a. Click **Secured Targets** tab in the Audit Vault Server console.
   b. In the **Monitoring** menu, click **Audit Trails**.
   c. Select all the audit trails, and then click **Stop**.
2. Log in to the Audit Vault Server as *support* user.
3. Switch to *root* user using the command:

   ```
   su root
   ```
4. Copy the patch file `bug_28581135_agentpatch.zip` to the `/var/lib/oracle/dbfw/patch` directory of the Audit Vault Server and extract the zip file using the command:

   ```
   unzip bug_28581135_agentpatch.zip -d BUG_28581135_AgentPatch
   ```
5. Change directory by executing the following command:

   ```
   cd /var/lib/oracle/dbfw/patch/BUG_28581135_AgentPatch
   ```
6. Apply the patch by the using the command:

   ```
   ./applyAgentPatch.sh
   ```
7. Once the `AgentPatch.sh` file is successfully executed, all the running Audit Vault Agents with `Java` version *1.8* are upgraded automatically with the patch and restarted.
8. Check for errors in the `/var/log/messages` file with tag `com.oracle.preBP9UpgradeAgentPatch.applyAgentPatch`. In case there are any errors, then contact Oracle Support.

> **Note:**
>
> - The application of `AgentPatch.sh` creates a backup of old Agents and plug-ins in the following directories:
>   - `/var/lib/oracle/dbfw/patch/BUG_28581135_AgentPatch/backup`
>   - `/var/lib/oracle/dbfw/patch/BUG_28581135_AgentPatch/agentjarbackup`
> - Preserve this directory in the same location as this is required in case patch needs to be reverted.
> - This pre-upgrade patch is distributed and applied to all running Audit Vault Agents. The user must allow **24 hours** for all Agents to update before applying the `12.2.0.9.0` bundle patch upgrade.
> - Check the status of the patch to ensure that all Audit Vault Agents are upgraded before continuing with `12.2.0.9.0` bundle patch upgrade.

- Checking The Patch Application Status (page 6-6)
  To check the patch application status, complete an update of the Audit Vault agents.
- Removing The Pre-upgrade Patch On The Audit Vault Server (page 6-7)
  Steps to remove the pre-upgrade patch on the Audit Vault Server.
- Applying The Agent Patch Manually On Individual Agents (page 6-8)
  Steps to download and manually apply the Agent patch on individual Agents.
- Undo Manual Application Of The Agent Patch (page 6-9)
  Steps to undo the manual application of the Agent patch.

6.2.2.1 Checking The Patch Application Status

To check the patch application status, complete an update of the Audit Vault agents.

1. Log in to the Audit Vault Server as *support* user.
2. Switch to *root* user using the command:

   ```
   su root
   ```

3. Change directory by executing the following command:

   ```
   cd /var/lib/oracle/dbfw/patch/BUG_28581135_AgentPatch
   ```

4. Execute the following command:

   ```
   ./getAgentUpdateStatus.sh
   ```

5. This displays the list of all the Agents that have been updated and that have not been updated with the patch.

6. The update of all Agents may take up to 24 hours. You can periodically run `getAgentUpdateStatus.sh` command to get the status update of the Agents.
7. After 24 hours, you can start the audit trails that were stopped earlier using the Audit Vault Server console as *admin* user.
8. Even after 24 hours, there may be some Agents that are not updated. You need to update them manually using steps below.

> **Note:**
>
> See Applying The Agent Patch Manually On Individual Agents (page 6-8) for complete instructions.

9. Log in to each non updated host.
10. Ensure that the `Java` version on the Agent host is updated to version *1.8*.
11. Follow the instructions in Applying The Agent Patch Manually On Individual Agents (page 6-8). If you have any problems installing this patch, or you are not sure about the inventory setup, then contact *Oracle Support*.

6.2.2.2 Removing The Pre-upgrade Patch On The Audit Vault Server

Steps to remove the pre-upgrade patch on the Audit Vault Server.

To remove the pre-upgrade patch:

1. Make sure that all the audit trails are stopped.
2. Click **Secured Targets** tab in the Audit Vault Server console.
3. In the **Monitoring** menu, click **Audit Trails**.
4. Select all the audit trails, and then click **Stop**.
5. Log in to the Audit Vault Server as *support* user.
6. Switch to *root* user using the command:

   ```
   su root
   ```
7. Change directory by executing the following command:

   ```
   cd /var/lib/oracle/dbfw/patch/BUG_28581135_AgentPatch
   ```
8. Execute the following command to revert the patch application:

   ```
   ./revertAgentPatch.sh
   ```
9. After successful execution of the revert patch application process, all the running hosts with `Java` *1.8* are reverted with original binaries and are restarted.
10. Check for errors in the `/var/log/messages` file with tag `com.oracle.preBP9UpgradeAgentPatch.applyAgentPatch`. In case there are any errors, then contact *Oracle Support*.
11. After 24 hours, you can start the audit trails that were stopped earlier using the Audit Vault Server console as *admin* user.

6.2.2.3 Applying The Agent Patch Manually On Individual Agents

Steps to download and manually apply the Agent patch on individual Agents.

In case the Mandatory Pre-upgrade Patch (page 6-4) has failed to upgrade one or more Audit Vault Agents, then use this procedure to apply the Agent patch manually on each Audit Vault Agent.

Steps To Download The Patch

1. Go to `https://support.oracle.com`, sign in, and click the **Patches & Updates** tab.
2. In the **Patch Search** box type `bug 28581683`.
3. From the search results, choose *PRE BP9 PATCH FOR MANUALLY UPDATING AGENT (Patch 28581683)*.
4. Click **README** and follow the instructions in the file.

Steps To Apply The Patch

1. Log in to the Audit Vault Agent host.
2. Stop the Agent using the command:

   ```
   <AGENT_HOME>/bin/agentctl stop -force
   ```

3. Copy the patch file *p28581683_122000_Generic.zip* and extract the zip file using the command:

   ```
   unzip p28581683_122000_Generic.zip -d BUG_28581683_ManualAgentPatch
   ```

4. Create a backup of the file `<AGENT_HOME>/bin/agentctl` using the command:

   ```
   mv <AGENT_HOME>/bin/agentctl <BACKUP_LOCATION>/agentctl
   ```

5. Create a backup of the file `<AGENT_HOME>/bin/agentctl.bat` using the command:

   ```
   mv <AGENT_HOME>/bin/agentctl.bat <BACKUP_LOCATION>/agentctl.bat
   ```

6. Create a backup of the file `<AGENT_HOME>/av/jlib/dep_jre7/ojdbc7.jar` using the command:

   ```
   mv <AGENT_HOME>/av/jlib/dep_jre7/ojdbc7.jar <BACKUP_LOCATION>/
   ojdbc7.jar
   ```

7. Copy the patch `agentctl` file to `<AGENT_HOME>/bin` using the command:

   ```
   cp -f BUG_28581683_ManualAgentPatch/agentctl <AGENT_HOME>/bin
   ```

8. Copy the patch `agentctl.bat` to `<AGENT_HOME>/bin` using the command:

   ```
   cp -f BUG_28581683_ManualAgentPatch/agentctl.bat <AGENT_HOME>/bin
   ```

9. Copy the patch `ojdbc7.jar` to `<AGENT_HOME>/bin` using the command:

   ```
   cp -f BUG_28581683_ManualAgentPatch/ojdbc7.jar <AGENT_HOME>/av/jlib/
   dep_jre7
   ```

10. Start the Agent using the command:

    ```
    <AGENT_HOME>/bin/agentctl start
    ```

11. Log in to the Audit Vault Server console as *admin* user and check the status of audit trails running on this Agent machine. If the audit trail is not running, then contact Oracle Support.

6.2.2.4 Undo Manual Application Of The Agent Patch

Steps to undo the manual application of the Agent patch.

1. Log in to the Audit Vault Agent host.
2. Stop the Agent using the command:

   ```
   <AGENT_HOME>/bin/agentctl stop -force
   ```

3. Copy `agentctl` from the backup location to `<AGENT_HOME>/bin` using the command:

   ```
   cp -f <BACKUP_LOCATION>/agentctl <AGENT_HOME>/bin
   ```

4. Copy `agentctl.bat` from the backup location to `<AGENT_HOME>/bin` using the command:

   ```
   cp -f <BACKUP_LOCATION>/agentctl.bat <AGENT_HOME>/bin
   ```

5. Copy `ojdbc7.jar` from the backup location to `<AGENT_HOME>/av/jlib/dep_jre7` using the command:

   ```
   cp -f <BACKUP_LOCATION>/ojdbc7.jar <AGENT_HOME>/av/jlib/dep_jre7
   ```

6. Start the Agent using the command:

   ```
   <AGENT_HOME>/bin/agentctl start
   ```

> **Note:**
>
> If you have any problems executing these instructions, then contact Oracle Support.

6.2.3 Back Up The Current Oracle Audit Vault And Database Firewall Installation

Before upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), you must back up some Audit Vault Server and Audit Vault Agent components.

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:**
>
> Backing Up and Restoring the Audit Vault Server

> **Note:**
>
> If your current Audit Vault Server is installed on a virtual machine (for example VM on Oracle VM or VMWare), it is recommended to take a VM snapshot before starting the upgrade process.

6.2.4 Release Existing Tablespaces That Are Retrieved Manually

Learn about releasing tablespaces retrieved manually.

Release all the existing tablespaces that were retrieved manually before performing the Oracle Audit Vault and Database Firewall (Oracle AVDF) upgrade process. Else, the index job creation may fail after upgrade because they cannot allocate space. The new indexes may also not be created after the upgrade.

To release the tablespaces follow this procedure:

1. Log in to the Audit Vault Server console as super administrator.
2. Navigate to **Settings**, and then to **Archiving**.
3. Click **Retrieve**.
4. You will find a list of tablespaces retrieved.
5. Select and release all the tablespaces.

6.2.5 Preserve Customization In Log Rotate File

Preserve customizations applied to the log rotate configuration files during upgrade of Oracle Audit Vault and Database Firewall (Oracle AVDF).

Any customization applied to the log rotate configuration files may be lost during upgrade. To preserve such rules:

- Create your own custom configuration file. See *Oracle Linux* documentation for details.
- Move any rules to a custom configuration file before performing the upgrade process.

6.2.6 Check For Busy Devices Before Starting The Upgrade Process

Check for any busy devices before starting the Oracle Audit Vault and Database Firewall (Oracle AVDF) upgrade process.

The upgrade may not check for busy volumes and may result in an error later.

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.

> **Note:**
>
> If you have an Audit Vault Agent running on a Windows machine, then ensure to close all the Agent related directories and open files before upgrading Oracle AVDF.

6.3 Upgrade Tasks

Tasks for upgrading Oracle Audit Vault and Database Firewall.

- Upgrade The Audit Vault Server (Standalone) Or Server Pair (High Availability) (page 6-11)
  You must upgrade the Audit Vault Server before you upgrade the Audit Vault Agents and Database Firewall.
- Automatic Upgrade Of The Audit Vault Agents And Host Monitors (page 6-13)
  The Agents and Host Monitors are automatically upgraded when you upgrade the Audit Vault Server.
- Upgrade The Database Firewall Or Firewall Pair (page 6-13)
  You must first upgrade the Audit Vault Server (or high availability pair of servers), before following these instructions to upgrade all Database Firewalls.
- Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances (page 6-14)
  The steps to upgrade an Audit Vault Server appliance or a Database Firewall appliance are similar.

6.3.1 Upgrade The Audit Vault Server (Standalone) Or Server Pair (High Availability)

You must upgrade the Audit Vault Server before you upgrade the Audit Vault Agents and Database Firewall.

If you have set up a high availability environment, upgrade both your primary and standby Audit Vault Server.

- Upgrading An Audit Vault Server (page 6-11)
  This procedure is for updating an Audit Vault Server that is not part of a pair of Audit Vault Servers configured for high availability (a resilient pair).
- Upgrading A Pair Of Audit Vault Servers Configured For High Availability (page 6-12)
  Learn to upgrade a pair of Audit Vault Servers configured for high availability.

6.3.1.1 Upgrading An Audit Vault Server

This procedure is for updating an Audit Vault Server that is not part of a pair of Audit Vault Servers configured for high availability (a resilient pair).

To upgrade an Audit Vault Server:

1. Make sure that all audit trails are stopped.
   a. Click the **Secured Targets** tab in the Audit Vault Server console.
   b. In the **Monitoring** menu, click **Audit Trails**.
   c. Select all audit trails, and then click **Stop**.

2. Follow the steps in Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances (page 6-14) to upgrade the Audit Vault Server.

Upgrade Notes

- If you have existing secured targets for which you ran Oracle Audit Vault and Database Firewall setup scripts to set user privileges (for example, for stored procedure auditing), no further action is required to update those privileges.
- Password hashing has been upgraded to a more secure standard in versions 12.1.2.x and later. This change affects the operating system passwords (support and root). Change your passwords after upgrade to take advantage of the more secure hash.

6.3.1.2 Upgrading A Pair Of Audit Vault Servers Configured For High Availability

Learn to upgrade a pair of Audit Vault Servers configured for high availability.

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

1. Upgrade the standby Audit Vault Server first.

   Follow the steps in Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances (page 6-14) 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. Stop the audit trails before upgrading the primary Audit Vault Server.
   a. Click the **Secured Targets** tab in the Audit Vault Server console.
   b. In the **Monitoring** menu, click **Audit Trails**.
   c. Select all audit trails, and then click **Stop**.
4. Follow the steps in Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances (page 6-14) to upgrade the primary.

> **Note:**
>
> After the primary Audit Vault Server is rebooted and is running, no additional reboot is needed. It is fully functional at this point.

6.3.2 Automatic Upgrade Of The Audit Vault Agents And Host Monitors

The Agents and Host Monitors are automatically upgraded when you upgrade the Audit Vault Server.

Note:

- If any Agent is using `Java 1.6`, then upgrade the `Java` version to `1.8`. This action ensures the following:
  - Establishes communication between the Audit Vault Server and the Agents.
  - Auto upgrade of Agents to release `12.2.0.9.0`.
- During the Audit Vault Agent auto-update process, its status will be `UNREACHABLE` for a while. It may take as much as 45 minutes to return to `RUNNING` state.
- On Windows hosts, the Audit Vault Agent gets updated automatically only if you have registered it as a Windows service, and you have set this service to use the credentials of the OS user that originally installed the agent.

  When you start the Agent from the command line, the Audit Vault Agent will not auto-update. In this case, update the Agent manually. For example:

  ```
  <agent_home>\bin\agentctl.bat stop
  ```

  Download the new `agent.jar` from the Audit Vault Server Console and extract it using `java -jar agent.jar` from `agent_home` of the existing agent. Then run:

  ```
  <agent_home>\bin\agentctl.bat start
  ```

  Do not delete the existing `agent_home` directory.
- In a high availability environment if the Audit Vault Agents are deployed on the secondary Audit Vault Server before pairing, then manually update the previously deployed Audit Vault Agents pertaining to the secondary Audit Vault Server after pairing is complete.

6.3.3 Upgrade The Database Firewall Or Firewall Pair

You must first upgrade the Audit Vault Server (or high availability pair of servers), before following these instructions to upgrade all Database Firewalls.

When updating Database Firewalls configured for high availability (a resilient pair), upgrade both the primary and secondary Database Firewall.

- Upgrading A Database Firewall (page 6-14)
  This procedure is for updating a Database Firewall that is not part of a pair of Database Firewalls configured for high availability (a resilient pair).
- Upgrading A Pair Of Database Firewalls Configured For High Availability (page 6-14)
  Learn to upgrade a pair of Database Firewalls configured for high availability.

6.3.3.1 Upgrading A Database Firewall

This procedure is for updating a Database Firewall that is not part of a pair of Database Firewalls configured for high availability (a resilient pair).

To upgrade a Database Firewall:

1. Stop all the enforcement points.
    1. Click **Secured Targets** tab in the Audit Vault Server console.
    2. In the **Monitoring** menu, click **Enforcement Points**.
    3. Select all the enforcement points, and then click **Stop**.
2. Follow the procedures in Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances (page 6-14) to upgrade the Database Firewall.

6.3.3.2 Upgrading A Pair Of Database Firewalls Configured For High Availability

Learn to upgrade a pair of Database Firewalls configured for high availability.

1. Follow the steps in Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances (page 6-14) to first upgrade the standby (secondary) Database Firewall.
2. Ensure that the standby Database Firewall has been restarted.
3. After the standby Database Firewall has fully started up after the reboot, swap this Database Firewall so that it now becomes the primary Database Firewall. To do this:
    1. In the Audit Vault Server console, click the **Firewalls** tab.
    2. Click **Resilient Pairs**.
    3. Select this resilient pair of firewalls, and click **Swap**.

       The Database Firewall you just upgraded is now the primary firewall.
4. Follow the steps in Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances (page 6-14) to upgrade the original primary Database Firewall.
5. After the original primary Database Firewall has fully started up after the reboot, swap this Database Firewall so that it now becomes the primary Database Firewall. This is an optional step.

6.3.4 Steps To Upgrade Oracle Audit Vault And Database Firewall Appliances

The steps to upgrade an Audit Vault Server appliance or a Database Firewall appliance are similar.

In the following steps, the term *appliance* refers to Audit Vault Server or Database Firewall depending on the one you are upgrading. Make sure you upgrade all the appliances as described in the sections above.

- Install The Oracle Audit Vault And Database Firewall Pre-Upgrade RPM (page 6-15)
  Steps to install the Oracle Audit Vault and Database Firewall (Oracle AVDF) pre-upgrade RPM.
- Transfer The ISO File To The Appliance (page 6-16)
  Steps to transfer the ISO file to the appliance.
- Start The Upgrade Script (page 6-17)
  The upgrade script mounts the ISO, changes to the correct working directory, executes the upgrade process, and then after the upgrade process is complete, unmounts the ISO.
- Restart The Appliance (page 6-19)
  Steps to reboot the appliance and continue the upgrade process.

6.3.4.1 Install The Oracle Audit Vault And Database Firewall Pre-Upgrade RPM

Steps to install the Oracle Audit Vault and Database Firewall (Oracle AVDF) pre-upgrade RPM.

You must install the pre-upgrade RPM. It puts the system into a state that can be safely upgraded after it checks for suitable space on the file system. When the pre-upgrade RPM is installed, it re-arranges free space on the appliance so that there is enough room to copy the upgrade files to the appliance and start the installation. After the upgrade, the space for the upgrade files is given back to the file system.

The `avdf-pre-upgrade-12.2.0.10.0-1.x86_64.rpm` executable includes the upgrade prerequisites and also checks that the platform conditions are met prior to the installation.

The pre-upgrade RPM prepares the system for upgrade by creating the `/var/dbfw/upgrade` directory with enough space to hold the main upgrade ISO file.

Prerequisite

In case of high availability environment, before running the pre-upgrade RPM, check the failover status on the primary Audit Vault Server. The failover status should not be `STALLED`. If the failover status is `STALLED`, then wait for a while and check the status again. If the status is not changing, then contact Oracle Support.

Follow these steps to check the failover status on the primary Audit Vault Server:

1. Log in to the primary Audit Vault Server console as *oracle* user.
2. Run the following command:

   ```
   /usr/local/dbfw/bin/setup_ha.rb --status
   ```

3. Check the failover status in the output.

Run Pre-Upgrade RPM

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

   If you are upgrading from release 12.2.0.5.0 or later, then run the `screen` command as user `root`.

> **Note:**
>
> Using the `screen` command prevents network disconnections interrupting the upgrade. If the session terminates, resume as follows:
>
> - Connect as `support`.
> - Switch to user `root`.
> - Run command `screen -r`

2. Run the following command to copy the `avdf-pre-upgrade-12.2.0.10.0-1.x86_64.rpm` executable from the download location to this appliance:

   ```
   scp remote_host:/path/to/avdf-pre-upgrade-12.2.0.10.0-1.x86_64.rpm /root
   ```

3. Run the following command to install the `avdf-pre-upgrade-12.2.0.10.0-1.x86_64.rpm` executable:

   ```
   rpm -i /root/avdf-pre-upgrade-12.2.0.10.0-1.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 the installation of the pre-upgrade RPM fails, take the remedial action described in the error message displayed. The appliance may not be ready for installation or the pre-upgrade RPM may have detected a problem. Upon taking the necessary measures, remove the pre-upgrade RPM and attempt installation again.
   >
   > To remove the RPM execute the following command as *root* user:
   >
   > ```
   > rpm -e avdf-pre-upgrade
   > ```
   >
   > Execute the following command if there is an issue with uninstalling the pre-upgrade RPM:
   >
   > ```
   > rpm -e avdf-pre-upgrade --noscripts
   > ```

6.3.4.2 Transfer The ISO File To The Appliance

Steps to transfer the ISO file to the appliance.

The `avdf-upgrade-12.2.0.10.0.iso` file is the main upgrade ISO that you generated earlier by combining the three ISO files downloaded from *My Oracle Support*.

1. Log in to the appliance as user `support`.

2. Copy the `avdf-upgrade-12.2.0.10.0.iso` file as follows:

   ```
   scp remote_host:/path/to/avdf-upgrade-12.2.0.10.0.iso /var/dbfw/upgrade
   ```

6.3.4.3 Start The Upgrade Script

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

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

   > **Note:**
   >
   > If you are upgrading from release `12.2.0.5.0` or later, then run the `screen` command as user *root*. Using the `screen` command prevents network disconnections interrupting the upgrade. If the session terminates, resume by switching to user *root* and then run command `screen -r`.

2. Execute the following command to perform appropriate checks before the upgrade:

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

3. Follow the system prompt, warning, and instruction to proceed with the upgrade accordingly.

   > **Note:**
   >
   > - For upgrade from Oracle Audit Vault and Database Firewall releases prior to 12.2, a data encryption keystore password is prompted as follows. This password prompt appears on primary and standalone systems, but not on standby systems.
   >
   >   In Oracle Audit Vault and Database Firewall release 12.2, the repository is encrypted using Oracle Database Transparent Database Encryption (TDE). This password protects the master encryption key wallet for TDE. After the upgrade, you may choose to integrate Oracle Audit Vault and Database Firewall with Oracle Key Vault to further protect your encryption key.
   > - The password must contain at least 8 characters and at most 30 bytes. It cannot have a leading or trailing space. It must not contain control characters, delete character, non-spacebar white space, or a double-quote (") character. An ASCII only password must have at least one uppercase letter, one lowercase letter, one digit (0-9), and one special character from the following: (.,+:_!).

Output similar to the following appears:

```
Enter Keystore Password: ********

Re-Enter Keystore Password:


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

Verifying upgrade preconditions
1/7: Mounting filesystems (1)
2/7: Cleaning yum configuration
3/7: Cleaning old packages and files
4/7: Upgrading kernel
5/7: Upgrading system
6/7: Installing database bundle patch resources
7/7: Setting final system status
Remove media and reboot now to fully apply changes.
Unmounted /var/dbfw/upgrade/avdf-upgrade-12.2.0.10.0.iso on /images
```

The output above varies depending on the base installation level, the appliance type, and the configuration.

Upgrading the Appliance

The system may take some time to complete the commands. Do not interrupt the upgrade, otherwise the system may be left in an inconsistent state.

For this reason it is important to use a reliable and uninterruptible shell, for example, a direct console login (or iLOM equivalent).

If you use a network (ssh) connection to upgrade the appliance, ensure the connection is reliable. You may also need to set the connection to `keepalive`. If you are using ssh from the Oracle Linux command line, you can use the `ServerAliveInterval` option, for example as follows:

```
# ssh -o ServerAliveInterval=20 [other ssh options]
```

> **Note:**
>
> If you are upgrading from release `12.2.0.5.0` or later, then run the `screen` command as user *root*. Using the screen command prevents network disconnections interrupting the upgrade. If the session terminates, resume as follows:
>
> 1. Connect as user *support*.
> 2. Switch to user *root*.
> 3. Run command `screen -r`

6.3.4.4 Restart The Appliance

Steps to reboot the appliance and continue the upgrade process.

To reboot the appliance, perform the following steps:

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

   ```
   reboot
   ```

   The restart process completes the upgrade. When the appliance restarts, the pre-database and post-database migrations are run automatically. This process also removes the pre-upgrade `avdf-pre-upgrade-12.2.0.10.0-1.x86_64.rpm` executable, so you do not need to manually remove this file.

   > **Note:**
   >
   > After restarting, the migration process can take several hours to complete. Please be patient. Do not restart the system while this is in progress.

3. If you have upgraded a Database Firewall, it may have regenerated the appliance certificate. In this scenario, you need to re-register the Database Firewall. To check this:
   a. Log in to the Audit Vault Server as an `administrator`.
   b. Click the **Database Firewalls** tab.
   c. If the upgraded Database Firewall indicates a certificate error, click on its name, and then click **Re-Register Firewall**.

> **See Also:**
>
> Registering a Database Firewall in the Audit Vault Server

> **Note:**
>
> Make sure that you upgrade all the components as mentioned in these sections:
>
> 1. Upgrade The Audit Vault Server (Standalone) Or Server Pair (High Availability) (page 6-11)
> 2. Automatic Upgrade Of The Audit Vault Agents And Host Monitors (page 6-13)
> 3. Upgrade The Database Firewall Or Firewall Pair (page 6-13)
>
> Once the upgrade is complete, perform the post-upgrade changes.

6.4 Post Upgrade Tasks

Post upgrade tasks for Oracle Audit Vault and Database Firewall (Oracle AVDF).

> **Note:**
>
> Apply the deprecated ciphers patch (`Deprecated-Cipher-Removal.zip`) to remove old ciphers, post AVS install or upgrade. Apply this patch on Audit Vault Server after installation or upgrade to 12.2.0.13.0 (or later). Before applying the patch, make sure that all the Audit Vault Agents and Host Monitor Agents are upgraded to 12.2.0.13.0.

The following topics describe some important post upgrade changes:

- Confirmation Of The Upgrade Process (page 6-20)
  Here are the symptoms that validate whether the upgrade was successful or not.
- Upon Successful Upgrade, Data Encryption Is Automatically Enabled (page 6-21)
  After upgrade, the newly created tablespaces are automatically encrypted.
- Changes Required To Existing Archive Locations (page 6-21)
  After the upgrade, new behavior is enforced on archive locations.
- Enable Archiving Functionality Post Upgrade From BP11 to Later Releases (page 6-22)
  Learn how to fix disabled archiving functionality post upgrade from Oracle AVDF 12.2.0.11.0 to later releases (12.2.0.12.0 or 12.2.0.13.0).
- Enable Archiving Functionality Post Upgrade From Release BP10 and Prior (page 6-24)
  Enable archiving functionality post upgrade from release 12.2.0.10.0 and prior. This is required only if the Audit Vault Server is deployed in a high availability environment.
- Recommended Post Upgrade Steps For Setting TLS Levels (page 6-25)
  After upgrading all of the appliances and Agents, Oracle recommends that you set the TLS level to Level-4.
- Post Upgrade Actions to Clear Unused Kernels From Oracle Audit Vault and Database Firewall (page 6-25)
  See MOS note (Doc ID 2458154.1) for complete instructions to clear unused kernels from Oracle Audit Vault and Database Firewall (Oracle AVDF).
- Scheduling Maintenance Job (page 6-26)
  There are some jobs on the Audit Vault Server that need to be scheduled for proper and effective functioning of the system.
- Resolve Missing Log Rotate File Post Upgrade (page 6-26)
  After upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), you will need to resolve a missing log rotate file.

6.4.1 Confirmation Of The Upgrade Process

Here are the symptoms that validate whether the upgrade was successful or not.

Symptoms when the upgrade is successful:

- The Audit Vault Server console can be launched without issues
- The home page on the Audit Vault Server console displays the actual version on the top right corner

- SSH connection to the Audit Vault Server is successful without any errors

Symptoms when the upgrade has failed:

- Unable to launch the Audit Vault Server console
- SSH connection to the Audit Vault Server displays an error that the upgrade has failed

6.4.2 Upon Successful Upgrade, Data Encryption Is Automatically Enabled

After upgrade, the newly created tablespaces are automatically encrypted.

However, tablespaces created before the system was upgraded to 12.2 continue to be in clear text.

> **See Also:**
>
> Data Encryption on Upgraded Instances in the *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed steps to encrypt existing tablespaces.

6.4.3 Changes Required To Existing Archive Locations

After the upgrade, new behavior is enforced on archive locations.

- New archive locations are owned by the user with administrator role who created them.
- The user with super administrator role can view all archive locations.
- Existing archive locations can only be accessed by the user with super administrator role. In order for the regular user with administrator role to access these locations, you must do the following task for each archive location:

  Log in to Audit Vault Server as `root` OS user, then perform the following commands:

  ```
  su - dvaccountmgr
  sqlplus /
  alter user avsys identified by <password> account unlock;
  exit;
  exit;
  su - oracle
  sqlplus avsys/<password>
  update avsys.archive_host set created_by=<adminuser> where name=<archive
  location name>;
  commit;
  exit;
  exit;
  su - dvaccountmgr
  sqlplus /
  alter user avsys account lock;
  exit;
  exit;
  ```

6.4.4 Enable Archiving Functionality Post Upgrade From BP11 to Later Releases

Learn how to fix disabled archiving functionality post upgrade from Oracle AVDF 12.2.0.11.0 to later releases (12.2.0.12.0 or 12.2.0.13.0).

Problem

Archiving functionality may be disabled after upgrading from Oracle AVDF 12.2.0.11.0 or 12.2.0.12.0, to 12.2.0.12.0 or 12.2.0.13.0.

Archiving functionality for high availability environment is supported starting Oracle AVDF release 12.2.0.11.0. This problem arises when you are upgrading from older releases where archiving functionality is supported only on the primary Audit Vault Server. Execute the steps only if you are upgrading from Oracle AVDF 12.2.0.11.0 to later releases.

> **Note:**
>
> If you are upgrading from any release prior to Oracle AVDF 12.2.0.11.0, then follow the steps documented in section Enable Archiving Functionality Post Upgrade.

Solution

If archive locations were present before upgrading to 12.2.0.13.0, execute the following steps to enable archiving functionality. These steps must be executed post upgrade process.

1. Create a new archive location using the Audit Vault Server console. While creating this new archive location enter the details of both the primary and standby location. This will mount the new archive location on the primary or standby Audit Vault Server and update the `fstab` with both archive locations.

2. SSH to the primary Audit Vault Server as *support* user and then unlock the *avsys* user by executing the following commands:

   ```
   su root
   ```

   ```
   su dvaccountmgr
   ```

   ```
   sqlplus /
   ```

   ```
   alter user avsys identified by <new password for avsys user> account
   unlock;
   ```

   ```
   exit;
   ```

   ```
   exit;
   ```

3. Execute the following commands as *avsys* user:

   ```
   su oracle
   ```

   ```
   sqlplus avsys
   ```

4. Enter the *avsys* password when prompted. Execute the following SQL commands:

   ```
   delete from avsys.system_configuration where property =
   '_ILM_ARCHIVING_DISABLED';
   ```

   ```
   COMMIT;
   ```

   ```
   insert into avsys.system_configuration values
   ('_ILM_HA_UPGRADE_COMPLETED', 'Y');
   ```

   ```
   COMMIT;
   ```

   ```
   exit;
   ```

   ```
   exit;
   ```

5. Execute the following command to lock the *avsys* user:

   ```
   su dvaccountmgr


   sqlplus /


   alter user avsys account lock;
   ```

6. Delete the new archive location that was created in the initial step. Navigate to **Settings** tab, then click **Manage Archive Locations** in the left navigation menu. Delete the specific archive location.

6.4.5 Enable Archiving Functionality Post Upgrade From Release BP10 and Prior

Enable archiving functionality post upgrade from release 12.2.0.10.0 and prior. This is required only if the Audit Vault Server is deployed in a high availability environment.

Archiving functionality for high availability environment is supported starting Oracle AVDF release 12.2.0.11.0. This problem arises when you are upgrading from older releases where archiving functionality is supported only on the primary Audit Vault Server. Execute the steps only if you are upgrading from Oracle AVDF 12.2.0.10.0 or prior releases to later releases where archiving functionality is supported for both primary and standby Audit Vault Servers.

In case there are NFS locations and archived data files, ensure all the data files are available in the respective NFS locations. Upon completion of the upgrade process, archiving is disabled. User must follow the below steps to enable archiving.

1. Connect to the primary Audit Vault Server using *SSH*.
2. Switch to *root* user and then to *oracle* user by executing the following commands:

   ```
   su - root
   ```

   ```
   su - oracle
   ```

3. Create new NFS locations using the Audit Vault Server console. These new locations created consider the newly mounted NFS points for both the primary and secondary Audit Vault Servers. Ensure there is sufficient space in the newly created NFS locations to store all the necessary data files archived.
4. Enter the `SQL*Plus` credentials as follows:

   ```
   sqlplus <super-admin>/<password>
   ```

5. Enable the archiving functionality by executing the following command:

   ```
   exec management.ar.run_hailm_job('<NFS location name defined>');
   ```

   This command triggers a back ground job. The status can be viewed under the **Jobs** page. The name of the job is `HAILM POST UPGRADE JOB`.

6. Once this functionality is enabled, all the archived data files are moved to the new NFS location. Archiving is enabled once this job completes successfully.

6.4.6 Recommended Post Upgrade Steps For Setting TLS Levels

After upgrading all of the appliances and Agents, Oracle recommends that you set the TLS level to Level-4.

Set the TLS level to *Level-4* by executing the following command:

```
/usr/local/dbfw/bin/priv/configure-networking --wui-tls-cipher-level 4 --
internal-tls-cipher-level 4 --agent-tls-cipher-level 4
```

> **Note:**
>
> - In case any single instance of an Agent is running on *IBM AIX*, then use `--agent-tls-cipher-level 3` instead of `--agent-tls-cipher-level 4` in the above command.
> - If any Agent is using `Java 1.6`, then upgrade the `Java` version to `1.8`.

Then, perform the following procedure to propagate cipher level change to all Agents:

1. Log in to the Audit Vault Server console as *root* user.
2. Change the directory by using the command:

   ```
   cd /usr/local/dbfw/bin/priv
   ```
3. Execute the following script using the command:

   ```
   ./send_agent_update_signal.sh
   ```

> **Note:**
>
> - This command must not be executed more than once in a period of one hour.
> - This will break communication with external systems if they do not support the strict TLS setting. See About Setting TLS Levels in the *Oracle Audit Vault and Database Firewall Administrator's Guide* for the appropriate level.

6.4.7 Post Upgrade Actions to Clear Unused Kernels From Oracle Audit Vault and Database Firewall

See MOS note (Doc ID 2458154.1) for complete instructions to clear unused kernels from Oracle Audit Vault and Database Firewall (Oracle AVDF).

6.4.8 Scheduling Maintenance Job

There are some jobs on the Audit Vault Server that need to be scheduled for proper and effective functioning of the system.

These jobs should run during a period when the Audit Vault server usage is low, such as night.

The user can schedule these jobs as per their time zone, through these procedures:

1. Log in to the Audit Vault Server as an *administrator*.
2. Click **Settings** tab, and then **Manage.**
3. To schedule a new maintenance job, select **Start Time.** Enter the time in hours and minutes for the maintenance job to start at a specific time. The time specified here is the time on the browser.
4. In the **Time Out (In hours)** field, enter the duration of the maintenance job in hours.

   > **Note:**
   >
   > In case the job does not complete within the duration specified, it is timed out.

5. In the **Repeat Frequency** field, select the frequency of the maintenance job to be repeated.

   > **Note:**
   >
   > This field cannot be edited, and by default the value remains *Daily.* The job runs at the specified start time daily.

   > **See Also:**
   >
   > Monitoring Jobs in the *Oracle Audit Vault and Database Firewall Administrator's Guide* to check the status of the job scheduled.

6.4.9 Resolve Missing Log Rotate File Post Upgrade

After upgrading Oracle Audit Vault and Database Firewall (Oracle AVDF), you will need to resolve a missing log rotate file.

This scenario is encountered while upgrading from Oracle Audit Vault and Database Firewall release `12.2.0.4.0` or prior, to release `12.2.0.5.0` and above. The `/etc/logrotate.d/dbfw-db` file may be missing after the upgrade.

To fix this issue, execute the following commands as *root* user:

```
install -o root -g root -m 0400 \
  /usr/local/dbfw/templates/template-logrotate.d_dbfw-db \
  /etc/logrotate.d/dbfw-db
```

Upgrade to Oracle Audit Vault and Database Firewall release `12.2.0.10.0` or later, to fix the following error:

```
error: /etc/logrotate.d/dbfw-db:10 duplicate log entry for /var/lib/oracle/
dbfw/av/log/apex_perf_patch.log
```

6.5 Migration of Expired Audit Records

Releases prior to Oracle Audit Vault and Database Firewall 12.2 did not automatically archive expired audit records (records that were older than the months online period specified in the data retention/archiving policy).

Expired audit records were stored in the `AVSPACE` schema of the Audit Vault Server.

After you upgrade to Oracle Audit Vault and Database Firewall 12.2, a migration job automatically kicks off to migrate expired audit data, and either archive it or delete it according to retention policies set for your secured targets. You can see the status of this migration job in the Jobs page (**Settings** tab, **System** menu, **Jobs**). In the event of an error (for example, not enough space for migration), the error appears in the job status. The expired records migration job runs every six hours until errors are fixed and the migration is complete.

> **Note:**
>
> Upon successfully upgrading to release 12.2.0.4.0 from 12.2.0.3.0, the user must run the encryption script prior to executing archive jobs.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information on archiving.

6.6 Recovering the Database in the Event of a Failed Upgrade

Always take back up Oracle Audit Vault and Database Firewall before upgrading in case the upgrade fails for an unforeseen reason.

If there is enough space in the Audit Vault Server's flash recovery area, you may be able to recover the database after a failed upgrade under the guidance of Oracle Support.

As a rule of thumb, to make recovery of the database possible, you should have the following amount of free space in the flash recovery area:

20 GB or 150% of the amount of data stored in the Audit Vault Server database, whichever is larger.

> **See Also:**
>
> - Back Up The Current Oracle Audit Vault And Database Firewall Installation (page 6-9)
> - *Oracle Audit Vault and Database Firewall Administrator's Guide* for information on monitoring the flash recovery area.

6.7 Uninstalling Audit Vault Agents Deployed on Target Host Machines

Uninstall the Audit Vault Server and the Database Firewall appliances, and the Audit Vault Agents, that are deployed on target host machines.

To remove the Audit Vault Agent from secured target host machines:

1. In the Audit Vault Server, stop all audit trails for the secured target host.
2. If the secured target host has a host monitor running, stop it.
3. In the Audit Vault Server, deactivate the Audit Vault Agent for the secured target host.
4. In the Audit Vault Server, delete the secured target host.
5. In the secured target host, delete the Audit Vault Agent install directory.

> **See Also:**
>
> *Oracle Audit Vault and Database Firewall Administrator's Guide*

To uninstall the Audit Vault Server or Database Firewall(s), turn off the computers on which they are installed, and follow the procedures for safely decomissioning the hardware.

6.8 Reimage Oracle Database Firewall and Restore from Audit Vault Server

About reimaging Oracle Database Firewall and to restore from Audit Vault Server.

Use this procedure to reimage the Oracle Database Firewall appliance and restore the configuration from the Audit Vault Server console.

1. Reinstall Database Firewall.
2. Complete the configuration steps for the Database Firewall instance. The configuration includes the IP address, proxy ports, bridges, and other settings similar to the previous Database Firewall instance.

3. Specify the Audit Vault Server certificate and IP address on the new Database Firewall instance.
4. Log in to the Audit Vault Server console as an administrator.
5. Click on **Database Firewalls** tab. The **Database Firewalls** tab on the left navigation menu is selected by default and a list of Database Firewall instances configured are displayed on the main page.
6. The newly installed Database Firewall displays red in the **Status** column.
7. Click on the name of the specific Database Firewall instance.
8. In the **Status** section on the main page, click on **Show details** against the **Status** field.
9. The **Diagnostic Status** section is displayed on the main page. There is a `Certificate Validation Failed` message displayed in the list.
10. Click on the **Back** button in the top right corner.
11. In the main page, click **Update Certificate** and wait for the page to load.
12. Check the status of the Database Firewall instance.
13. Click **Reset** button under **Reset Database Firewall** section and confirm the operation.
14. Verify the status of the Database Firewall is `Primary` and the status of the Enforcement Point is `Up`.

Index