Oracle® Audit Vault and Database Firewall

Installation Guide

Release 12.1.2

E27778-13

August 2014

ORACLE®

Oracle Audit Vault and Database Firewall Installation Guide Release 12.1.2

E27778-13

Primary Author: Sheila Moore

Contributing Author: Gigi Hanna

Contents

3 Installing Oracle Audit Vault and Database Firewall Software

4 Post-Install Configuration Tasks

5 Upgrading or Removing Oracle Audit Vault and Database Firewall

Index

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 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.

Related Documents

For more information about Oracle Database, see the following documents in the Oracle AVDF Release 12.1.2 documentation set:

- *Oracle Audit Vault and Database Firewall Release Notes*
- *Oracle Audit Vault and Database Firewall Administrator's Guide*
- *Oracle Audit Vault and Database Firewall Auditor's Guide*
- *Oracle Audit Vault and Database Firewall Developer's Guide*

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.

1

Overview of Oracle Audit Vault and Database Firewall Installation

This chapter gives an overview of Oracle Audit Vault and Database Firewall (Oracle AVDF) and its installation.

Topics

> **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 AVDF in a network and in special configurations

Downloading the Latest Version of This Manual

You can download the latest version of this manual from the following website:

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

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

`http://docs.oracle.com`

Platform Support

Topics

Supported Server Platforms

Oracle AVDF is delivered as software appliance images ready to be deployed on their own hardware, either directly or as virtual appliances. Oracle AVDF can be installed and run on the following platforms:

- **(Recommended)** Any Intel x86 64-bit hardware platform supported by Oracle Linux Release 5 Update 10.

  For a complete list of certified hardware that supports Oracle Linux, go to `https://linux.oracle.com/hardware.html`.

- Oracle VM Server for x86, version 3.x

Audit Collection: Supported Secured Target Types and Versions

Table 1–1 lists supported secured target types and versions for audit data collection for the current release of Oracle Audit Vault and Database Firewall.

Table 1–1 Audit Collection: Supported Secured Target Types and Versions

Category	Releases/Versions
DATABASE	
Oracle Database	10g, 11g
	12c
IBM DB2 for LUW (Linux, UNIX, Windows)	9.x
Microsoft SQL Server	2000, 2005, 2008, 2008 R2
	2012
SAP Sybase ASE	12.5.4 - 15.7
MySQL	5.5.29 - 5.6.12
OPERATING SYSTEM	
Oracle Solaris on SPARC64	10, 11
Oracle Solaris on x86-64	10, 11
Oracle Linux	OL5.8 (requires auditd 1.8)
	OL6.0 (requires auditd 2.0)
	OL 6.1-6.4 (requires auditd 2.2.2)
Microsoft Windows Server on x86-64	2008, 2008 R2
DIRECTORY SERVICE	
Microsoft Active Directory	2008, 2008 R2
FILE SYSTEM	
Oracle ACFS	12c
HADOOP SYSTEM	
Oracle Big Data Appliance*	2.3

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

Database Firewall Protection: Supported Secured Target Types and Versions

Table 1–2 lists supported secured target types and versions for Database Firewall protection for the current release.

Table 1–2 Database Firewall Protection: Supported Secured Target Types and Versions

Database Product	Releases/Versions
Oracle Database	9i
	10g, 11g
	12c
IBM DB2 for LUW (Linux, UNIX, Windows)	9.x
Microsoft SQL Server	2000, 2005, 2008, 2008 R2
	2012
SAP Sybase ASE	12.5.4 - 15.7
MySQL	5.0, 5.1, 5.5
	5.6
SAP Sybase SQL Anywhere	10.0.1

Audit Vault Agent: Supported Platforms and Versions

Table 1–3 lists supported platforms and versions for the Audit Vault Agent for the current release.

Table 1–3 Audit Vault Agent: Supported Platforms and Versions

Operating System	Releases/Versions
Linux x86-64	SLES11, RHEL5,6, Asianux 3, Oracle Linux 5,6
Microsoft Windows x64	7, 8, 8.1
Microsoft Windows Server on x86-64	2003, 2003 R2, 2008, 2008 R2
Oracle Solaris on SPARC64	10, 11
Oracle Solaris on x86-64	10, 11
IBM AIX on POWER Systems (64-bit)	6.1, 7.1
HP-UX on Itanium	11.31
Linux x86-32	SLES11 SP2, RHEL5,6, Asianux 3, Oracle Linux 5,6
Microsoft Windows 32-bit	7, 8, 8.1, 2003, 2003 R2, 2008

Host Monitor: Supported Platforms and Versions

Table 1–4 lists supported platforms and versions for the host monitor for the current release.

Table 1–4 Host Monitor: Supported Platforms and Versions

Operating System	Releases/Versions

Table 1–4 (Cont.) Host Monitor: Supported Platforms and Versions

Linux x86-64	SLES11, RHEL5,6, Asianux 3, Oracle Linux 5,6
Microsoft Windows Server x86-64	2008, 2008 R2

About Oracle AVDF

Topics

Oracle AVDF Features

Oracle Audit Vault and Database Firewall (AVDF) secures databases and other critical components of IT infrastructure (such as operating systems) in these key ways:

- Provides a database firewall that can monitor activity and/or block SQL statements on the network based on a firewall policy
- Collects audit data, and makes it available in audit reports
- Provides dozens of built-in, customizable activity and compliance reports, and lets you proactively configure alerts and notifications

See Also:

- *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information about Oracle AVDF administrative features
- *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed information about Oracle AVDF auditing features

Summary of Oracle AVDF Components and Users

This section briefly describes the Oracle AVDF components that you will install.

Topics

See Also: *Oracle Audit Vault and Database Firewall Administrator's Guide* for more information about Oracle AVDF components, including a diagram of how they work together

Audit Vault Server

An **Audit Vault Server** is a dedicated server that has:

- Tools to configure Oracle AVDF to collect audit data from secured targets, and/or apply firewall policies to secured targets.

  For more information about the secured targets, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

- An Oracle database, which provides a data repository for audit and firewall events.

> **Note:** You should not attempt to administer or set password policies for the Oracle Database embedded in the Audit Vault Server.

For more information about the Audit Vault Server, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Database Firewalls

A **Database Firewall** is a dedicated server that collects SQL data from network traffic going to and from a database and sends the data to the Audit Vault Server. Oracle AVDF can support one or more Database Firewalls, depending on your network scenario. For more information about Database Firewalls, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Audit Vault Agents

An **Audit Vault Agent** retrieves audit trail data from a secured target database or nondatabase (such as an operating system) and sends it to the Audit Vault Server. Each secured target is associated with an Audit Vault Agent, which retrieves data from one or more of its audit trails. For information about the Audit Vault Agent and deploying it on secured target computers, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Oracle AVDF Users

Oracle AVDF has the following users for the Audit Vault Server:

- **Administrator:** The administrator user can access the Audit Vault Server administration functions. A super administrator can create other super administrator or administrator users. Administrators perform all system configuration tasks including setting up connections to secured targets, audit trails, system and network services, maintenance, backup, high availablity, and third-party integrations. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information.
- **Auditor:** The auditor user can access the Audit Vault Server auditing functions. A super auditor can create other super auditor or auditor users. Auditors perform Oracle AVDF auditing functions such as setting up audit and firewall policies, generating reports, retrieving entitlement information, setting up alerts, and creating customer reports. See *Oracle Audit Vault and Database Firewall Auditor's Guide* for detailed information.
- **support:** This the Linux operating system user who does Audit Vault Server updates, and diagnostic or remedial tasks. Only use this account as documented, or as instructed by Oracle Support.
- **root:** This is the Linux operating system user with the highest system privileges, and can do the same tasks as the support user, as well as additional tasks as required by Oracle AVDF. Only use this account as documented, or as instructed by Oracle Support.

Oracle AVDF has the following users for the Database Firewall:

- **Administration User:** This user can the Database Firewall administration interface. The administration user can perform all configuration tasks on the

Database Firewall, including setting up system networking and services, traffic sources, proxy configuration, view diagnostic information, configuring high availablity, etc. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information.

- **support:** This the Linux operating system user who does Database Firewall updates, and diagnostic or remedial tasks. Only use this account as documented, or as instructed by Oracle Support.
- **root:** This is the Linux operating system user with the highest system privileges, and can do the same tasks as the support user, as well as additional tasks as required by Oracle AVDF. Only use this account as documented, or as instructed by Oracle Support.

About Oracle AVDF Installation

Briefly, the Oracle AVDF installation steps are:

1. Understand the Oracle AVDF components to be installed.

   For information about the components, see "Summary of Oracle AVDF Components and Users" on page 1-4.

2. Plan the system configuration that best suits your needs.

   For details, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

3. Ensure that your system meets the pre-install requirements.

   For details, see Chapter 2, "Oracle Audit Vault and Database Firewall Pre-Install Requirements."

4. Install the Oracle AVDF software.

   For details, see Chapter 3, "Installing Oracle Audit Vault and Database Firewall Software."

5. Do the post-install configuration tasks.

   For details, see Chapter 4, "Post-Install Configuration Tasks."

Periodically, you might need to update the Oracle AVDF software. For instructions, see "Upgrading or Removing Oracle Audit Vault and Database Firewall" on page 5-1

If you must remove Oracle AVDF software from your system, see the instructions in "Removing the Oracle AVDF Software" on page 5-2.

CAUTION: 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.

Supported Secured Targets

Secured targets are the systems (such as a database or operating system) that you will monitor using Oracle AVDF. Each type of supported secured target has a corresponding plug-in in Oracle AVDF. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for detailed information on plug-ins shipped out-of-the-box.

See these topics for secured targets supported for auditing and firewall functions:

- "Audit Collection: Supported Secured Target Types and Versions" on page 1-2
- "Database Firewall Protection: Supported Secured Target Types and Versions" on page 1-3

In addition, you can find supported platforms for prior releases in **Article 1536380.1** at the following website:

`https://support.oracle.com`

Compatible Third-Party Products

You can use Oracle AVDF with these third-party products:

- HP ArcSight Security Information Event Management (SIEM), which logs, analyzes, and manages network user activity that is recorded in syslog messages from different sources
- F5 BIG-IP ASM (Application Security Manager) (versions 9.5.*x* and 10.*x*), which provides protection against Web-based attacks

2

Oracle Audit Vault and Database Firewall Pre-Install Requirements

This chapter explains the requirements that your system must meet before you can install Oracle Audit Vault and Database Firewall (Oracle AVDF) on it.

Topics

Privileges Required to Install Oracle AVDF

Any user can install Oracle AVDF. You do not need administrative privileges to complete the installation.

Oracle AVDF Hardware Requirements

You must install each Audit Vault Server and each Database Firewall onto its own dedicated x86 64-bit server (or Oracle VM 3.x). Your hardware must be compatible with Oracle Linux, Release 5 Update 10.

> **Important:** Do not install an 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.

Topics

Memory Requirements

Each x86 64-bit server must have at least 2 GB of RAM.

Disk Space Requirements

Each x86 64-bit server must have a single hard drive with a minimum 125 GB of disk space.

Network Interface Cards

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)
- 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.

For information on Database Firewall modes and proxy configuration, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Oracle AVDF Software Requirements

Topics

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 6 or later.

Browser Requirements

The AVDF Administrator and Auditor GUIs support the following browsers:

- Mozilla Firefox 14 or later
- Microsoft Internet Explorer 8.0 or later
- Google Chrome 21 or later
- Apple Safari 5.0 or later

The following is required to view charts and interactive reports in the GUI:

- Latest version of Adobe Flash plug-in

Host Monitor Requirements

Host Monitor enables the Database Firewall to directly monitor SQL traffic in a database. Before deploying the host monitor, ensure that the computer on which the host monitor is to run has the required libraries. See *Oracle Audit Vault and Database Firewall Administrator's Guide* for host monitoring instructions and prerequisites.

3

Installing Oracle Audit Vault and Database Firewall Software

This chapter explains 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. Audit Vault Agent deployment and activation are covered in *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Topics

> **Important:** The Security Guidelines chapter of *Oracle Audit Vault and Database Firewall Administrator's Guide* contains important information about installing Oracle AVDF securely and protecting your data

About the Software Installation Procedure

The Oracle AVDF software is installed using two disks, each created from `.iso` or `.zip` file downloads:

- The Audit Vault installer disk (created from two files)
- The Database Firewall installer disk (created from one file)

During the installation, you create an installation passphrase that protects the newly installed component until it is fully configured. See "Installation Passphrase Requirements" on page 3-2.

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

Downloading and Verifying the Software

You can download the software from Oracle Software Delivery Cloud as Media Packs. A Media Pack is an electronic version of the software, which you can then transfer to disk.

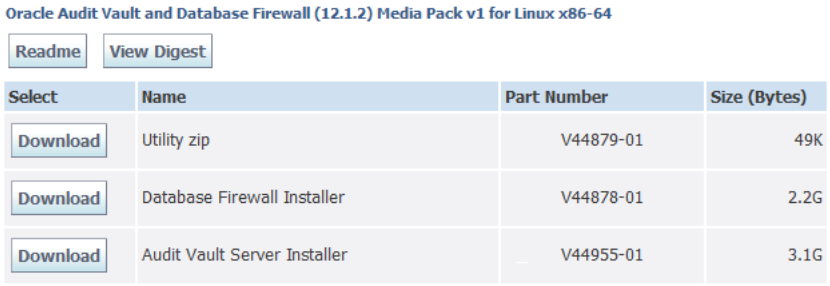
To download the software:

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

   https://edelivery.oracle.com

2. Complete the Export Validation process by completing the online form, and accepting the terms and conditions, and then click **Continue**.
3. In the Media Pack Search page, in the **Select a Product Pack** field, select **Oracle Database**, select a **Platform**, and click **Go**.
4. Select the required Oracle Audit Vault and Database Firewall media pack, and click **Continue**.
5. In the media pack downloads page, click **Readme** to review the Readme file for further instructions and product information.
6. After you review the Readme, click **Download** for the desired software to download the individual `.zip` or `.iso` files.

   Here is an example of the downloads section on this page. The number of files, part numbers, and file sizes may be different depending on the product version you selected:


Oracle Audit Vault and Database Firewall (12.1.2) Media Pack v1 for Linux x86-64

Readme View Digest

Select	Name	Part Number	Size (Bytes)
Download	Utility zip	V44879-01	49K
Download	Database Firewall Installer	V44878-01	2.2G
Download	Audit Vault Server Installer	V44955-01	3.1G

7. After you download the files, click **View Digest**, and then generate MD5 checksums for each `.iso` or `.zip` file downloaded to verify that they match the values listed in the View Digest page.

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 (described in Chapter 4, "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
- At least one of the following:
  - Comma (,)
  - Period (.)

  - Colon (:)
  - Plus sign (+)
  - Underscore (_)
- Space

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 installation step 12.

Installing an Audit Vault Server or Database Firewall

Topics

Step 1: Download the Installer Files and Create Disks

This step depends on which version of Oracle AVDF you are installing:

Oracle AVDF 12.1.2.2.0

Follow these instructions if you are downloading Oracle 12.1.2.2.0.

To download either the Audit Vault Server or the Database Firewall software:

1. Download and verify either the Audit Vault Server Installer file or the Database Firewall Installer file from the Oracle Software Delivery Cloud.

   See "Downloading and Verifying the Software" on page 3-1.

2. Create an installer disk from the downloaded installer file.

Oracle AVDF 12.1.2.1.0

Follow these instructions if you are downloading Oracle 12.1.2.1.0. Note in this version there are two installer files for the Audit Vault Server.

To download the Audit Vault Server software:

1. Download these two files from the Oracle Software Delivery Cloud:

   - Audit Vault Server Installer (Part 1 of 2)

   - Audit Vault Server Installer (Part 2 of 2)

   See "Downloading and Verifying the Software" on page 3-1.

2. Unzip the two Audit Vault Server files you downloaded. You will end up with two files:

   ```
   avs-installer-disc-12.1.2.1.0.iso00
   avs-installer-disc-12.1.2.1.0.iso01
   ```

3. Combine the two files to create a single `.iso` file using the appropriate command below (each command is on one line).

Windows:

```
copy /b avs-installer-disc-12.1.2.1.0.iso00+avs-installer-disc-12.1.2.1.0.iso01
avs-installer-disc-12.1.2.1.0.iso
```

Linux:

```
cat avs-installer-disc-12.1.2.1.0.iso00 avs-installer-disc-12.1.2.1.0.iso01 >
avs-installer-disc-12.1.2.1.0.iso
```

4. Generate an MD5 checksum for the combined `.iso` file to make sure it matches this value:

   ```
   29d6595de5467f70be9b3de502d80fed
   ```

5. Create an installer disk from the single `.iso` file.

To download the Database Firewall software:

1. Download and verify the Database Firewall Installer file from the Oracle Software Delivery Cloud.

   See "Downloading and Verifying the Software" on page 3-1.

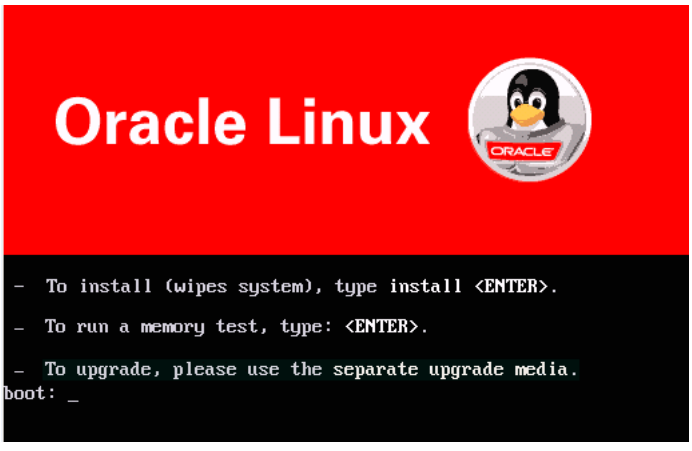
2. Create an installer disk from the downloaded Database Firewall Installer file.

Step 2: Install the Software

To install an Audit Vault Server or Database Firewall:

1. Insert either the installer disk for the Audit Vault Server or the 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:



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

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

   The installation proceeds. After some time, the screen displays this message:

   ```
   Please enter installation passphrase
   ```

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

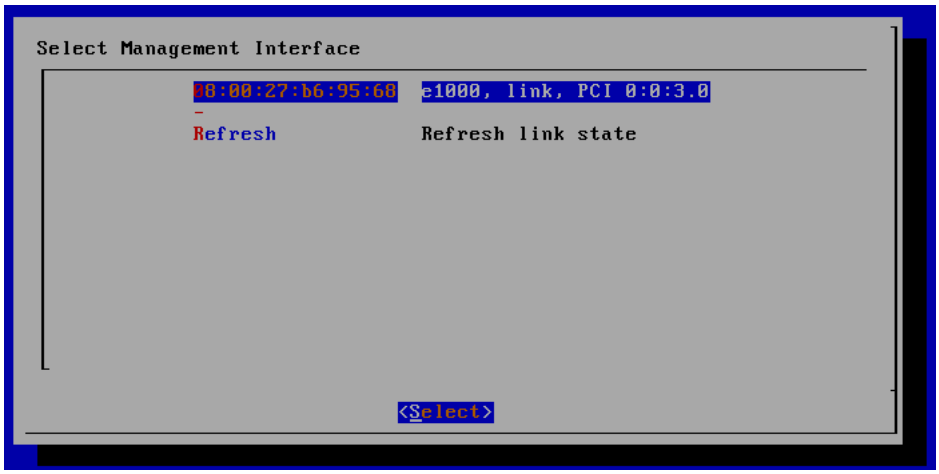
   See "Installation Passphrase Requirements" on page 3-2.

   The screen displays this message:

```
Installation passphrase was successfully configured
```

4. Press **Enter**.

   The Select Management Interface screen appears, listing the available interfaces.



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

   The management interface is the network interface used by the Audit Vault Server.

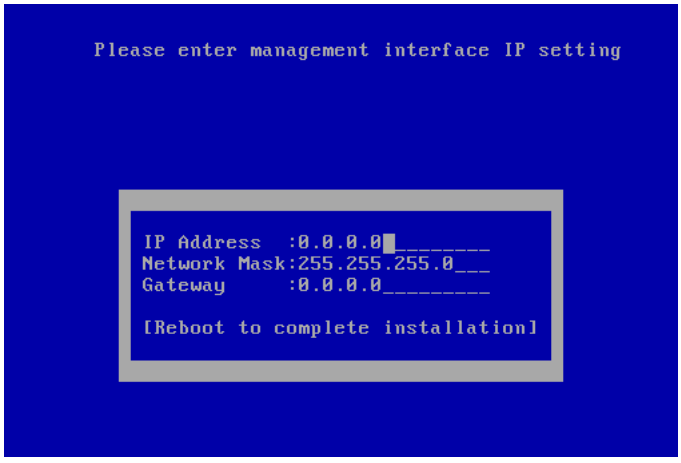
6. Press the key **Enter**.

   A screen appears with this option selected:

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

7. Press **Enter**.

   This screen appears:



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

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

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

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

10. 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**.

11. Press **Enter**.

    The computer reboots. This may take a long time. When rebooting has finished, the system displays your network settings.

12. Press **Enter**.

    Either the Audit Vault Server menu appears ...

    Or the Database Firewall menu appears:

13. Do the appropriate post-install configuration tasks, described in Chapter 4, "Post-Install Configuration Tasks."

    For these tasks, you need the passphrase that you created in step 3 and the IP address that you provided in step 8.

CAUTION: 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.

4

Post-Install Configuration Tasks

This chapter explains post-installation tasks for Oracle Audit Vault and Database Firewall (Oracle AVDF). Some of these tasks are mandatory.

Topics

Audit Vault Server Post-Install Tasks

After installing the Audit Vault Server, 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.

> **Note:** Oracle strongly recommends that you synchronize all Oracle AVDF components and secured targets with Network Time Protocol (NTP) servers. Without this synchronization, events might appear to be archived to the Audit Vault Server before they occur and alerts might appear to be sent before their triggering events occur.

Topics

Accessing the Audit Vault Server Post-Install Configuration Page

To access the Audit Vault Server Post-Install Configuration page:

1. Using any internet browser, go to the Audit Vault Server console:

   `https://ip_address`

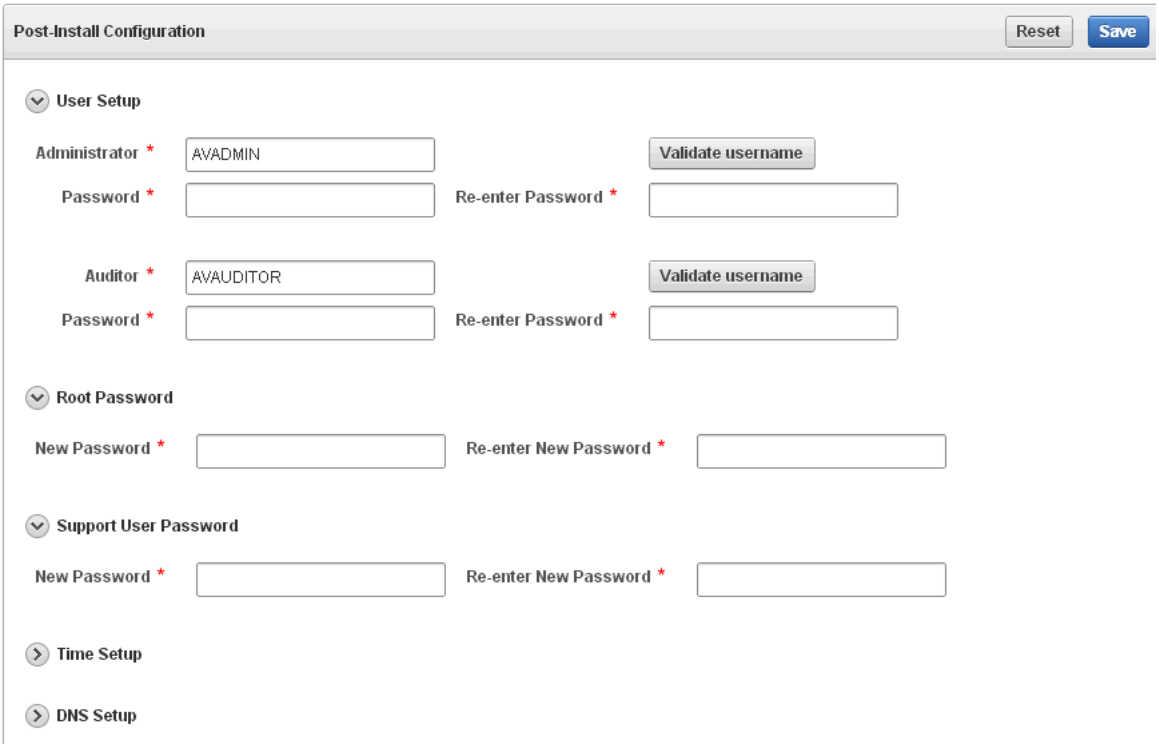
   For *ip_address*, use the IP address of the Audit Vault Server (see "Installing an Audit Vault Server or Database Firewall" on page 3-3, step 8).

   If you see a message saying that there is a problem with the Web site security certificate, this could be due to a self-signed certificate. Click the **Continue to this website** (or similar) link.

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" on page 3-3, step 3 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. For instructions, see:

- "Setting the Usernames and Passwords of Audit Vault Server Users (Required)" on page 4-2.
- "Setting the Audit Vault Server Time (Strongly Recommended)" on page 4-4
- "Setting the Audit Vault Server DNS Servers (Recommended)" on page 4-5

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

In the post-install configuration page, you set up usernames and passwords for the Oracle AVDF administrator, auditor, support, and root users. See "Oracle AVDF Users" on page 1-5 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.

Topics

- About Administrator and Auditor Usernames
- About Audit Vault Server User Passwords
- Setting the Passwords

About Administrator and Auditor Usernames

We recommend that you change the administrator and auditor usernames after installing Oracle AVDF. The administrator and auditor usernames 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 usernames are upshifted (that is, any lowercase alphabetic characters are replaced by their uppercase equivalents). Also, the Audit Vault Server does not support quoted usernames.

About Audit Vault Server User Passwords

Passwords need not be unique. However, Oracle recommends that passwords have the following characteristics, and enforces the first three listed below:

- Have at least one uppercase alphabetic, one alphabetic, one numeric, and one special character (plus sign, comma, colon, period, exclamation mark, 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(:), exclamation mark (!), 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.

Setting the Passwords

For a description of each user account, see "Oracle AVDF Users" on page 1-5.

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.

   For instructions, see "Accessing the Audit Vault Server Post-Install Configuration Page" on page 4-1.

2. Under **User Setup**:
   - In the **Administrator** field, replace the default user name (recommended).
   - Under the **Administrator**, field, enter the administrator **Password**, then confirm it in the **Re-enter Password** field.
   - Click **Validate username**.

The administrator username that you entered is validated.

- In the **Auditor** field, replace the default user name (recommended).
- Under the **Auditor**, field, enter the auditor **Password**, then confirm it in the **Re-enter Password** field.
- Click **Validate username**.

  The auditor username that you entered is validated.

3. Under the heading **Root Password**, in the fields labeled **New Password** and **Re-enter New Password**, type the password for root.
4. Under the heading **Support User Password**, in the fields labeled **New Password** and **Re-enter New Password**, type the password for the support user.
5. Click **Save**.
6. Proceed to "Setting the Audit Vault Server Time (Strongly Recommended)" on page 4-4.

Setting the Audit Vault Server Time (Strongly Recommended)

To set the Audit Vault Server time:

1. Access the Audit Vault Server Post-Install Configuration page.

   For instructions, see "Accessing the Audit Vault Server Post-Install Configuration Page" on page 4-1.
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 you selected **Use NTP**, then for each of the fields **Server 1 Address**, **Server 2 Address**, and **Server 3 Address**:

   1. 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.
   2. Click **Test Server**.

      The time from the specified server appears.

5. If in step 3 you selected **Set Manually**, then set the **Date** fields to your current local day and time.
6. Either click **Save** or proceed to "Setting the Audit Vault Server DNS Servers (Recommended)" on page 4-5.

Setting the Audit Vault Server DNS Servers (Recommended)

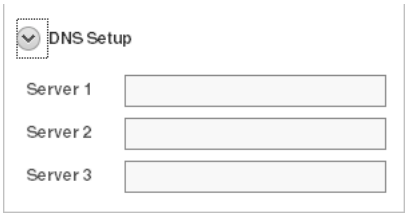
The Audit Vault Server DNS servers are used to resolve any host names that Audit Vault Server might use.

> **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.

   For instructions, see "Accessing the Audit Vault Server Post-Install Configuration Page" on page 4-1.
2. Expand the **DNS Setup** section.



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).

Database Firewall Post-Install Tasks

After you install the Database Firewall, you must set the passwords of its Administration User, root, and support user. The Administration User is the Web GUI user, while root and support user are the Linux system operating system user accounts on the Audit Vault Server.

Topics

Accessing the Database Firewall Post-Install Configuration Page

To access the Database Firewall Post-Install Configuration page:

1. Using any internet browser, go to the Database Firewall console:

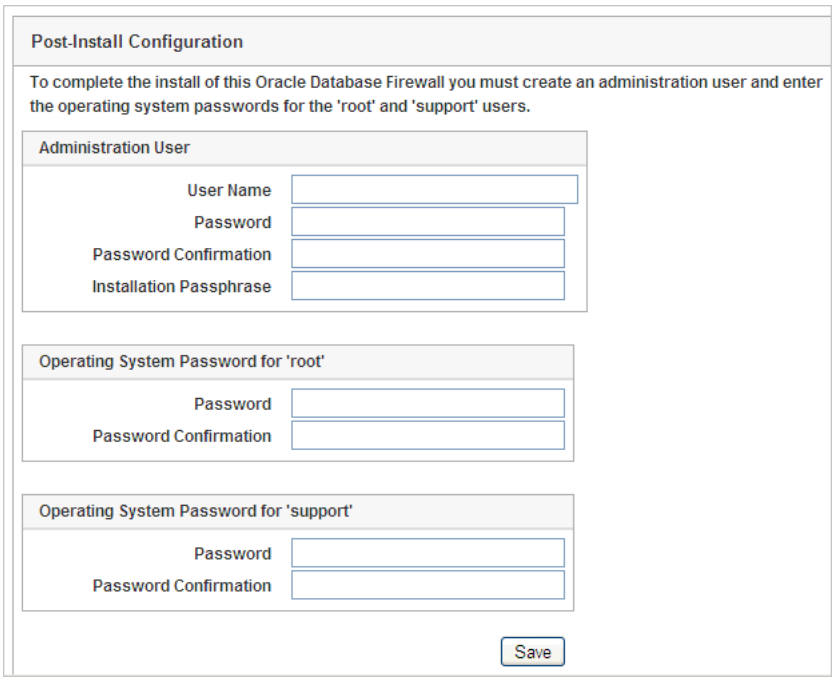
   `https://ip_address`

   For *ip_address*, use the IP address of the Database Firewall (see "Installing an Audit Vault Server or Database Firewall" on page 3-3, step 8).

   You are prompted to enter the installation passphrase.

2. Type the installation passphrase that you created in "Installing an Audit Vault Server or Database Firewall" on page 3-3, step 3) and click **Login**.

   The Post-Install Configuration page appears:



From this page, you can set the passwords of the Database Firewall users (for instructions, see "Setting the Passwords of Database Firewall Users (Required)" on page 4-7).

Setting the Passwords of Database Firewall Users (Required)

Topics

About 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.

Setting the Passwords

For a description of each user account, see "Oracle AVDF Users" on page 1-5.

To set the passwords of the Database Firewall administrator, root, and support user:

1. Under the heading **Administration User**:
   1. In the field **User Name**, type the user name of the Database Firewall Administration User.
   2. In the field **Password**, type the password of the Database Firewall Administration User.
   3. In the field **Password Confirmation**, retype the password.
   4. In the field **Installation Passphrase**, type the installation passphrase that you created in "Installing an Audit Vault Server or Database Firewall" on page 3-3, step 3.
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**.

5

Upgrading or Removing Oracle Audit Vault and Database Firewall

This chapter provides information on upgrades and Bundle Patch updates.

Topics

Downloading the Upgrade Software and Instructions

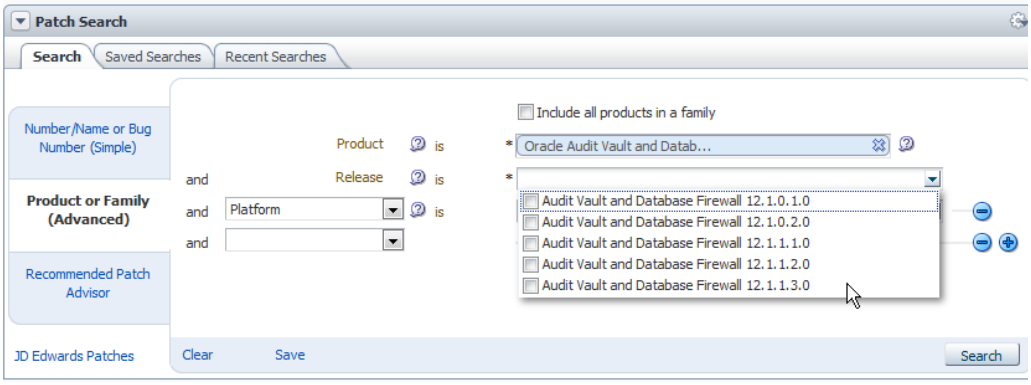
Be sure you have the latest upgrade software before starting the upgrade. This software is in the latest available Bundle Patch.

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

To download the upgrade software and README:

1. Go to the web site `https://support.oracle.com`, sign in, and click the **Patches & Updates** tab.
2. Use the **Patch Search** box to find the patch.

   The following image is an example only:



   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**.

3. In the search results page, in the **Patch Name** column, click the number for the latest Bundle Patch.

   A corresponding patch page appears.

4. In the page for this patch, click **Download**, and then save the `.zip` file in a selected location.

5. Unzip the downloaded file to access the upgrade software (a `.iso` file).

Upgrading Paired Audit Vault Servers and Database Firewalls

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

Follow the detailed instructions in the README file included with the upgrade software.

For detailed information about how Oracle AVDF works in a high-availability environment, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

Performing a Backup Before Upgrading the Oracle AVDF Software

Before upgrading or applying a patch update to Oracle Audit Vault and Database Firewall, back up the following:

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

Also back up your files, and keep these files until you have tested the update.

For guidance on how to back up and restore the Audit Vault Server, see My Oracle Support Document ID 1556200.1 at this web site: `https://support.oracle.com`.

Removing the Oracle AVDF Software

Oracle AVDF consists of the Audit Vault Server and the Database Firewall appliances, and the Audit Vault Agent, which is deployed on secured target host computers.

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

To remove the Audit Vault Agent from a secured target host computer:

1. In the Audit Vault Server, stop all audit trails for the secured target host.

   For instructions, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

2. If the secured target host has a host monitor running, stop it.

   For instructions, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

3. In the Audit Vault Server, deactivate the Audit Vault Agent for the secured target host.

   For instructions, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

4. In the Audit Vault Server, delete the secured target host.

   For instructions, see *Oracle Audit Vault and Database Firewall Administrator's Guide*.

5. In the secured target host, delete the Audit Vault Agent install directory.

Index

R

S

T

U

V

W