

Oracle® Audit Vault

Server Installation Guide

Release 10.2.3.2 for Microsoft Windows x64 (64-Bit)

E17379-02

September 2010

Oracle Audit Vault Server Installation Guide, Release 10.2.3.2 for Microsoft Windows x64 (64-Bit)

E17379-02

Copyright © 2007, 2010, Oracle and/or its affiliates. All rights reserved.

Primary Authors: Rod Ward, Tanaya Bhattacharjee

Contributing Authors: Sumit Jeloka, Nilima Kapoor, Robert Chang, Tammy Bednar, K Karun, Deborah Owens, Janet Blowney, Pat Huey

Contributors: Vipul Shah, Lok Sheung, Donna Keesling, Martin Widjaja, Trivikrama Samudrala, Luann Ho, Alan Galbreath, Sana Karam, Manish Chandra

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documents	viii
Conventions	viii
1 Overview of Oracle Audit Vault Server Installation	
1.1 Oracle Audit Vault Installation Components	1-1
1.2 Oracle Audit Vault Server Installation Methods	1-1
1.2.1 Interactive Installation Methods	1-1
1.2.2 Automated Installation Methods Using Response Files	1-2
1.3 Oracle Audit Vault Server Installation	1-2
1.4 Installation Considerations	1-3
1.4.1 Hardware and Software Considerations	1-3
1.4.2 Multiple Oracle Homes	1-3
2 Oracle Audit Vault Server Preinstallation Requirements	
2.1 Becoming Familiar with the Features of Oracle Audit Vault	2-1
2.2 Installing as a User Name in the Administrators Group	2-1
2.3 Checking the Hardware Requirements	2-1
2.3.1 Hardware Component Requirements	2-2
2.3.2 Hard Disk Space Requirements	2-2
2.3.3 Verifying Hardware Requirements	2-2
2.4 Checking the Operating System Requirements	2-3
2.5 Reviewing Oracle Audit Vault Server Hardware and Software Certification	2-4
2.5.1 Windows Terminal Services and Remote Desktop Support	2-5
2.5.2 Web Browser Support	2-5
2.6 Checking the Network Setup	2-5
2.6.1 Installing on DHCP Computers	2-5
2.6.2 Installing on Multi-homed Computers	2-6
2.6.3 Installing on Computers with Multiple Aliases	2-6
2.7 Creating Directories for Oracle Audit Vault Database Files	2-6
2.8 Setting the Correct Locale	2-7

3 Installing the Oracle Audit Vault Server

3.1	Accessing the Server Installation Software	3-1
3.2	Basic Installation – Performing the Single Instance Server Installation.....	3-1
3.3	Advanced Installation – Prerequisite Information for Installing in an Oracle Real Application Clusters Environment	3-4
3.4	Advanced Installation – Installing Single Instance and in an Oracle Real Application Clusters Environment	3-4
3.5	Performing a Silent Installation Using a Response File	3-8
3.6	Audit Vault Server Installation Details.....	3-9
3.6.1	Basic and Advanced Installation Details Screens.....	3-9
3.6.1.1	Audit Vault Name	3-10
3.6.1.2	Oracle Audit Vault Home	3-11
3.6.1.3	Oracle Audit Vault Server Accounts	3-11
3.6.2	Advanced Server Installation: Database Vault User Credentials Screen	3-14
3.6.2.1	Oracle Database Vault Owner and Oracle Database Vault Account Manager Accounts	3-15
3.6.2.2	Oracle Database Vault Owner and Oracle Database Vault Account Manager Passwords	3-15
3.6.3	Advanced Server Installation: Node Selection Screen	3-15
3.6.4	Advanced Server Installation: Specify Database Storage Options Screen	3-15
3.6.5	Advanced Server Installation: Specify Backup and Recovery Option Screen	3-16
3.6.6	Advanced Server Installation: Specify Database Schema Passwords Screen	3-17
3.7	Postinstallation Server Tasks.....	3-17
3.7.1	Download Patches	3-18
3.7.2	Download Critical Patch Updates	3-18
3.7.3	Reset User Passwords	3-19
3.7.3.1	Using SQL*Plus to Reset Passwords.....	3-19
3.7.4	Enable or Disable Connections with the SYSDBA Privilege	3-20
3.7.5	Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC Only)	3-20
3.7.6	Download JDBC Driver Files for Source Database Connectivity	3-21
3.7.6.1	Download Microsoft SQL Server JDBC Driver for SQL Server Connectivity ..	3-22
3.7.6.2	Download jConnect JDBC Driver for Sybase ASE Connectivity	3-22
3.7.6.3	Copy the DB2 JDBC and SQLJ Driver to the Audit Vault Homes	3-22
3.7.7	Log in to Oracle Audit Vault Console	3-23
3.7.8	Next Steps to Perform as an Oracle Audit Vault Administrator	3-23

4 Removing Audit Vault Server Software

4.1	Removing the Audit Vault Server Software	4-1
4.2	Manually Remove the Remaining Oracle Audit Vault Server Components	4-3
4.2.1	Removing the Oracle Net Service Registry Key	4-4
4.2.2	Removing All Oracle Audit Vault Server Registry Keys.....	4-4
4.2.3	Updating the PATH Environment Variable Path	4-6
4.2.4	Removing Oracle Audit Vault Server from the Start Menu	4-6
4.2.5	Removing Oracle Audit Vault Server Directories	4-6

Index

List of Tables

2-1	Hardware Requirements.....	2-2
2-2	Disk Space Requirements for NTFS	2-2
2-3	Software Requirements	2-3
3-1	Invalid Oracle Audit Vault Name and Oracle Audit Vault Account Name Characters	3-10
3-2	Special Characters Allowed in the Audit Vault Server Home Name	3-11
3-3	Valid Oracle Audit Vault Administrator and Oracle Audit Vault Auditor Password Characters	3-14

Preface

Oracle Audit Vault Server Installation Guide for Microsoft Windows x64 (64-Bit) explains how to prepare for, install, and configure Oracle Audit Vault Server (Audit Vault Server). It provides specific instructions for the operating system and Oracle software technology components that Audit Vault Server requires.

Audience

This document is intended for Oracle database administrators (DBAs) and system administrators and those who are involved in the installation of Oracle Audit Vault and its related components.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/support/contact.html> or visit <http://www.oracle.com/accessibility/support.html> if you are hearing impaired.

Related Documents

For more information, see the following documents:

- *Oracle Audit Vault Release Notes*
- *Oracle Audit Vault Collection Agent Installation Guide*
- *Oracle Audit Vault Licensing Information*
- *Oracle Audit Vault Administrator's Guide*
- *Oracle Audit Vault Auditor's Guide*
- *Oracle Database Installation Guide for Microsoft Windows (x64)*
- *Oracle Database Platform Guide for Microsoft Windows (x64)*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*
- *Oracle Database Vault Installation Guide for Microsoft Windows x64*
- *Oracle Database Vault Administrator's Guide*

To download free release notes, installation documentation, updated versions of this guide, white papers, or other collateral, visit the Oracle Technology Network (OTN). You must register online before using OTN. Registration is free. You can register at

<http://www.oracle.com/technology/membership/>

If you already have a user name and password for OTN, then you can go directly to the Oracle Audit Vault documentation section of the OTN Web site at

<http://www.oracle.com/technology/documentation/auditvault.html>

For OTN information specific to Oracle Audit Vault, visit

<http://www.oracle.com/technology/products/audit-vault/index.html>

For the Oracle Audit Vault Discussion Forums, visit

<http://forums.oracle.com/forums/forum.jspa?forumID=391>

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

Overview of Oracle Audit Vault Server Installation

Oracle Audit Vault is a powerful enterprisewide audit solution that efficiently consolidates, detects, monitors, alerts, and reports on audit data for security auditing and compliance. Oracle Audit Vault provides the ability to consolidate audit data and critical events into a centralized and secure audit warehouse.

This chapter provides an overview of the Oracle Audit Vault Server (Audit Vault Server) installation process. This chapter includes the following sections:

- [Oracle Audit Vault Installation Components](#)
- [Oracle Audit Vault Server Installation Methods](#)
- [Oracle Audit Vault Server Installation](#)
- [Installation Considerations](#)

1.1 Oracle Audit Vault Installation Components

Oracle Audit Vault Server software installation consists of two parts:

- Oracle Audit Vault Server installation that can be either:
 - Single Instance installation
 - Clustered using an Oracle Real Application Clusters (Oracle RAC) installation
- Oracle Audit Vault collection agent installation (see *Oracle Audit Vault Collection Agent Installation Guide*)

1.2 Oracle Audit Vault Server Installation Methods

You can choose different installation methods to install Audit Vault Server, as follows:

- [Interactive Installation Methods](#)
- [Automated Installation Methods Using Response Files](#)

1.2.1 Interactive Installation Methods

When you use the interactive method to install Oracle Audit Vault to perform a Basic, Advanced, or Upgrade installation, Oracle Universal Installer displays a series of screens that enable you to specify all of the required information to install the Oracle Audit Vault Server software.

1.2.2 Automated Installation Methods Using Response Files

Oracle Audit Vault provides a response file template for Audit Vault Server (`av.rsp`) and one for an upgrade installation (`upgrade_av.rsp`). These response template files can be found in the `AV_installer_location\response` directory on the Audit Vault Server installation media.

When you start Oracle Universal Installer and specify a response file, you can automate all of the Oracle Audit Vault Server installation. These automated installation methods are useful if you need to perform multiple installations on similarly configured systems.

For Audit Vault Server, Oracle Universal Installer can run in silent (non-interactive) mode. For silent mode, specify both the `-silent` and `-responseFile` options followed by the path of the response file on the command line when you invoke Oracle Universal Installer. For example:

```
setup.exe -silent -responseFile Path-of-response-file
```

Oracle Universal Installer runs in silent mode if you use a response file that specifies all required information. None of the Oracle Universal Installer screens are displayed, and all interaction (standard output and error messages) and installation logs appear on the command line.

Prepare the response file by entering values for all parameters that are missing in the first part of the response file, then save the file. Do not edit any values in the second part of either response file.

See [Section 3.5](#) for information about performing an Oracle Audit Vault Server silent installation.

Note: The basic installation is not supported in silent mode. Silent installation is only supported for the advanced installation.

1.3 Oracle Audit Vault Server Installation

The Oracle Audit Vault server installation consists of the following options:

- Basic installation – Simplifies the installation process and prompts for a minimal set of inputs from the user to perform a full installation. An Oracle RAC installation is not supported through this option; only a single instance installation is supported.
- Advanced installation – Offers the user more control and options for the installation process, including storage options and backup options. This option supports the installation of Audit Vault Server on a cluster and as a single instance.

After you complete the installation, you can configure secure communication at the management level between the Audit Vault Server and the Oracle Audit Vault collection agent. In this postinstallation step, you configure SSL for mutual authentication between the Oracle Audit Vault management service on the server side, and each collection agent over HTTPS.

After you check the requirements described in [Section 1.4](#), the general steps to install Oracle Audit Vault Server include these tasks:

1. Run Oracle Universal Installer to perform Audit Vault Server installation.

2. Run postinstallation and configuration tasks using Audit Vault Configuration Assistant (AVCA) utility.

1.4 Installation Considerations

This section contains information that you should consider before deciding how to install this product. It includes the following topics:

- [Hardware and Software Considerations](#)
- [Multiple Oracle Homes](#)

1.4.1 Hardware and Software Considerations

The platform-specific hardware and software requirements included in this installation guide were current at the time this guide was published. However, because new platforms and operating system versions might be certified after this guide is published, review the certification matrix on the My Oracle Support (formerly *OracleMetaLink*) Web site for the most up-to-date list of certified hardware platforms and operating system versions. The My Oracle Support Web site is available at

<https://support.oracle.com>

1.4.2 Multiple Oracle Homes

This product supports multiple Oracle homes. This means you can install this release of the software more than once on the same system, in different Oracle home directories See [Section 2.6.2](#) for more information.

Oracle Audit Vault Server Preinstallation Requirements

This chapter describes the following installation requirements for an x64-bit Windows installation of Oracle Audit Vault Server (Audit Vault Server). This chapter includes the following sections:

- [Becoming Familiar with the Features of Oracle Audit Vault](#)
- [Installing as a User Name in the Administrators Group](#)
- [Checking the Hardware Requirements](#)
- [Checking the Operating System Requirements](#)
- [Reviewing Oracle Audit Vault Server Hardware and Software Certification](#)
- [Checking the Network Setup](#)
- [Creating Directories for Oracle Audit Vault Database Files](#)
- [Setting the Correct Locale](#)

2.1 Becoming Familiar with the Features of Oracle Audit Vault

To plan the installation process, you must be familiar with the features of Oracle Audit Vault. *Oracle Audit Vault Administrator's Guide* discusses the basic features of Oracle Audit Vault.

2.2 Installing as a User Name in the Administrators Group

On Microsoft Windows, Audit Vault Server must be installed by a Windows username in the Administrators group. The username is automatically added to the Windows local group ORA_DBA.

2.3 Checking the Hardware Requirements

This section describes hardware component and hard disk space requirements.

- [Hardware Component Requirements](#)
- [Hard Disk Space Requirements](#)
- [Verifying Hardware Requirements](#)

2.3.1 Hardware Component Requirements

Table 2–1 lists the required hardware components for Oracle Audit Vault Server.

Table 2–1 Hardware Requirements

Requirement	Minimum Value
Physical memory (RAM)	1 GB minimum
Virtual memory	Double the amount of RAM
Hard disk space	3.19 GB Total See Table 2–2 for details.
Video adapter	256 colors
Processor	AMD64, or Intel Extended Memory 64 Technology (EM64T)

2.3.2 Hard Disk Space Requirements

This section lists system requirements for Windows platforms that use the NT File System (NTFS). Note that FAT32 File Systems are not supported. Oracle recommends installing Oracle components on NTFS.

The NTFS system requirements listed in this section are more accurate than the hard disk values reported by the Oracle Universal Installer Summary window. The Summary window does not include accurate values for disk space, the space required to create a database, or the size of compressed files that are expanded on the hard drive.

The hard disk requirements for Oracle Database components include 32 MB required to install Java Runtime Environment (JRE) and Oracle Universal Installer on the partition where the operating system is installed. If sufficient space is not detected, installation fails and an error message appears.

Table 2–2 lists the space requirements for NTFS.

Table 2–2 Disk Space Requirements for NTFS

TEMP Space	Oracle Home	Data Files	Total
108 MB	3.08 GB	1.49 GB	3.19 GB

See Also: "NTFS File System and Windows Registry Permissions" in *Oracle Database Platform Guide for Microsoft Windows (32-Bit)*

The 3.02 GB of disk space for the Oracle home is the disk space for the Oracle Audit Vault Server software files in the Oracle Base including 1.49 GB of disk space for the Oracle Audit Vault database files. The TEMP space required is 108 MB.

The 1.49 GB of disk space for the Oracle Audit Vault database files is only if the database storage option is on the file system. For other storage options, such as ASM, the database files will be stored elsewhere. Also, this 1.49 GB disk space is only the starting size. The Oracle Audit Vault administrator must take future growth of the database size into consideration, especially as the server collects more and more audit data.

2.3.3 Verifying Hardware Requirements

To ensure that the system meets these requirements, perform the following tasks:

1. Determine the physical RAM size. On a Microsoft Windows Server 2008 computer, click **System and Security** in the Windows Control Panel, then click **System**.

If the size of the physical RAM installed in the system is less than the required size, then you must install more memory before continuing.

2. Determine the size of the configured virtual memory (also known as paging file size). On a Microsoft Windows Server 2008 computer, click **System and Security**, then click **System**, click **Advanced System Settings**, click the **Advanced** tab on the System Properties page, and then click **Settings** in the Performance section. Then select the **Advanced** tab on the Performance Options page.

The virtual memory is listed in the Virtual Memory section.

If necessary, see your operating system documentation for information about how to configure additional virtual memory.

3. Determine the amount of free disk space on the system. On a Microsoft Windows Server 2008 computer, right click **My Computer** and click **Open**.
4. Determine the amount of disk space available in the `temp` directory. This is equivalent to the total amount of free disk space, minus what is required for the Oracle software to be installed.

If there is less than 100 MB of disk space available in the `temp` directory, then first delete all unnecessary files. If the temp disk space is still less than 100 MB, then set the `TEMP` or `TMP` environment variable to point to a different hard drive location.

On a Microsoft Windows Server 2008 computer, click **System and Security**, then click **System**, click **Advanced System Settings**, click the **Advanced** tab on the System Properties page, and then click **Environment Variables**.

2.4 Checking the Operating System Requirements

Table 2–3 lists the software requirements for Audit Vault Server.

Note: Oracle Universal Installer performs checks on your system to verify that it meets the listed requirements. To ensure that these checks pass, verify the requirements before you start Oracle Universal Installer.

Table 2–3 Software Requirements

Requirement	Value
System Architecture	Processor: AMD64, and Intel Extended Memory 64 Technology (EM64T) For additional information, visit My Oracle Support (formerly OracleMetaLink) at: https://support.oracle.com

Table 2–3 (Cont.) Software Requirements

Requirement	Value
Operating System	<p>Oracle Audit Vault Server for Windows x64 is supported on the following operating systems:</p> <ul style="list-style-type: none"> ▪ Microsoft Windows Server 2008 x64 - Standard, Enterprise, Datacenter, Web, Standard without Hyper-V, Enterprise without Hyper-V, and Datacenter without Hyper-V editions <p>The specific operating system components that are not supported are Microsoft Windows Server 2008 x64 Hyper-V and Server Core.</p> <p>Note: Oracle Audit Vault Server for Windows x64 cannot be installed on Microsoft Windows Server 2008 R2.</p> <p>The underlying file system must be NTFS. A FAT32 file system is not supported; if a FAT32 file system is detected, the installation will not proceed.</p> <p>Windows Multilingual User Interface Pack is supported on Microsoft Windows Server 2008.</p>
Network protocol	<p>The Oracle Net foundation layer uses Oracle protocol support to communicate with the following industry-standard network protocols:</p> <ul style="list-style-type: none"> ▪ TCP/IP ▪ TCP/IP with SSL ▪ Named Pipes

2.5 Reviewing Oracle Audit Vault Server Hardware and Software Certification

The platform-specific hardware and software requirements included in this installation guide were current at the time this guide was published. However, because new platforms and operating system software versions might be certified after this guide is published, review the certification matrix on the My Oracle Support Web site for the most up-to-date list of certified hardware platforms and operating system versions. This Web site also provides compatible client and database versions, patches, and workaround information for bugs. The My Oracle Support Web site is available at the following URL:

<https://support.oracle.com/>

You must register online before using My Oracle Support. After logging in, select the **More** tab and then select **Certifications**. Under **Find Certification Information**, fill in the following fields: **Product Line**, select **Oracle Database Products**. Under **Product Family**, **Product Area**, and **Product**, select **Oracle Audit Vault**. Under **Product Release**, select **10gR2**, and under **Product Version**, select **10.2.3.0**. Under **Tier**, **Tier Product**, and **Tier Product Version**, select the tier products that apply to your site. Under **Platform**, **Platform Version**, and **Certification Status**, select the platform information that applies to your site. Then click **Search**.

The following sections provide certification information:

- [Windows Terminal Services and Remote Desktop Support](#)
- [Web Browser Support](#)

2.5.1 Windows Terminal Services and Remote Desktop Support

Oracle supports installing, configuring, and running Oracle Database through Terminal Services on Microsoft Windows Server 2008. If you encounter problems with the installation through Terminal Server, Oracle recommends that you try connecting to the Terminal Services console session of the server (using `mstsc/console`).

You can have multiple Remote Desktop sessions on Microsoft Windows Server 2008.

Platform-specific support information is as follows:

See Also:

- The Microsoft Web site for more information about terminal services
<http://www.microsoft.com/>
- The My Oracle Support Web site for the latest Terminal Server certification information
<https://support.oracle.com/>

2.5.2 Web Browser Support

The following Web browsers are supported for iSQL*Plus and Oracle Enterprise Manager Database Control:

- Netscape Navigator 7.2 and later
- Microsoft Internet Explorer 6.0
- Mozilla version 1.7 and later
- Safari 1.2
- Firefox 1.0.4

2.6 Checking the Network Setup

Typically, the computer on which you want to install Oracle Audit Vault Server is connected to the network, has local storage to contain the Oracle Audit Vault Server installation, has a display monitor, and has a CD-ROM or DVD drive.

This section describes how to install Oracle Audit Vault on computers that do not meet the typical scenario. It covers the following cases:

- [Installing on DHCP Computers](#)
- [Installing on Multi-homed Computers](#)
- [Installing on Computers with Multiple Aliases](#)

2.6.1 Installing on DHCP Computers

Dynamic host configuration protocol (DHCP) assigns dynamic IP addresses on a network. Dynamic addressing enables a computer to have a different IP address each time it connects to the network. In some cases, the IP address can change while the computer is still connected. You can have a mixture of static and dynamic IP addressing in a DHCP system.

In a DHCP setup, the software tracks IP addresses, which simplifies network administration. This lets you add a new computer to the network without having to manually assign that computer a unique IP address.

Do not install Audit Vault Server in an environment where the IP addresses of the Audit Vault Server or the Oracle Audit Vault collection agent can change. If your environment uses DHCP, ensure that all Oracle Audit Vault systems use static IP addresses.

2.6.2 Installing on Multi-homed Computers

You can install Oracle Audit Vault on a multi-homed computer. A multiple-homed computer has multiple network cards, which in turn, allows it to have multiple IP addresses. Each IP address is associated with a host name. In addition, you can set up aliases for the host name. By default, Oracle Universal Installer uses the `ORACLE_HOSTNAME` environment variable setting to find the host name. If the `ORACLE_HOSTNAME` environment variable is not set and you are installing Oracle Audit Vault on a computer that has multiple network cards, then Oracle Universal Installer determines the host name by using the first entry in the `hosts` file, typically located in `SYSTEM_DRIVE:\WINDOWS\System32\drivers\etc`.

Clients must be able to access the computer using this host name, or by using aliases for this host name. To check, ping the host name from the client computers using the short name (host name only) and the full name (host name and domain name). Both must work.

Setting the `ORACLE_HOSTNAME` Environment Variable

To set the `ORACLE_HOSTNAME` environment variable:

1. From the **Start** menu, click **Control Panel**.
2. Click **System and Security**, then click **System**.
3. Click **Advanced System Settings**.
4. Click the **Advanced** tab on the System Properties page, and then click **Environment Variables**.
5. In the Environment Variables dialog box, under System Variables, click **New**.
6. In the New System Variable dialog box, enter the following information:
 - **Variable name:** `ORACLE_HOSTNAME`
 - **Variable value:** The host name of the computer that you want to use.
7. Click **OK**, then in the Environment Variables dialog box, click **OK**.
8. Click **OK** in the Environment Variables dialog box, then in the System Properties dialog box, click **OK**.

2.6.3 Installing on Computers with Multiple Aliases

A computer with multiple aliases is registered with the naming service under a single IP address, but with multiple aliases. The naming service resolves any of those aliases to the same computer. Before installing Oracle Audit Vault on such a computer, set the `ORACLE_HOSTNAME` environment variable to the computer whose host name you want to use.

2.7 Creating Directories for Oracle Audit Vault Database Files

If you choose to place the Oracle Audit Vault database files on a file system, then use the following guidelines when deciding where to place them:

- The default path suggested by Oracle Universal Installer for the database file directory is a subdirectory of the Oracle base directory.
- You can choose either a single file system or more than one file system to store the database files:
 - If you want to use a single file system, then choose a file system on a physical device that is dedicated to the database.

For best performance and reliability, choose a RAID device or a logical volume on more than one physical device and implement the stripe-and-mirror-everything (SAME) methodology.
 - If you want to use more than one file system, then choose file systems on separate physical devices that are dedicated to the database.

This method enables you to distribute physical I/O and create separate control files on different devices for increased reliability. It also enables you to fully implement the OFA guidelines.
- For optimum performance, the file systems that you choose should be on physical devices that are used only by the database.
- The user with Administrators privilege or who is a member of the ORA_DBA group performing the installation has write permissions to create the files in the path that you specify.

2.8 Setting the Correct Locale

Ensure that the `NLS_LANG` environment variable is not set. On a Microsoft Windows Server 2008 computer, click **System and Security**, then click **System**, click **Advanced System Settings**, click the **Advanced** tab on the System Properties page, and then click **Environment Variables**. Then under **System Variables** look for `NLS_LANG`. If `NLS_LANG` is set, remove the setting by selecting it and clicking **Delete**, and then click **OK** to save your change.

Installing the Oracle Audit Vault Server

This chapter describes how to install single instance Oracle Audit Vault Server (Audit Vault Server) and Audit Vault Server with Oracle Real Application Clusters (Oracle RAC).

Note: An upgrade option is not available on Microsoft Windows.

This chapter includes the following sections:

- [Accessing the Server Installation Software](#)
- [Audit Vault Server Installation Details](#)
- [Basic Installation – Performing the Single Instance Server Installation](#)
- [Advanced Installation – Prerequisite Information for Installing in an Oracle Real Application Clusters Environment](#)
- [Advanced Installation – Installing Single Instance and in an Oracle Real Application Clusters Environment](#)
- [Performing a Silent Installation Using a Response File](#)
- [Postinstallation Server Tasks](#)

3.1 Accessing the Server Installation Software

The Oracle Audit Vault Server software is available for download on Oracle Technology Network, <http://www.oracle.com/technology/index.html>

3.2 Basic Installation – Performing the Single Instance Server Installation

For an overview of requested information specific to the Audit Vault Server installation, see [Section 3.6](#).

See [Section 2.8](#) for important information about setting the correct locale.

To perform Audit Vault Server single instance basic installation:

1. Unset the ORACLE_HOME environment variable.

From the **Start Bar**, select **Settings**, then from the **Control Panel** double click **System**, select the **Advanced** tab, select **Environment Variables**, then under **System Variables** look for ORACLE_HOME. If ORACLE_HOME is set, remove the setting by selecting it and clicking **Delete**, and then click **OK** to save your change.

2. Invoke Oracle Universal Installer (OUI) to install Oracle Audit Vault release 10.2.2.1.0.

Log in as a member of the Administrators group to the computer on which to install Oracle Audit Vault Server.

If you are installing on a Primary Domain Controller (PDC) or a Backup Domain Controller (BDC), log on as a member of the Domain Administrators group.

3. Change your current directory to the directory containing the installation files. Start Oracle Universal Installer from the Oracle Audit Vault Server package by double-clicking `setup.exe`.

```
cd directory-containing-the-Oracle-Audit-Vault-installation-files
setup.exe
```

4. In the Welcome window, on the **Select Installation Type** page, select the **Basic Installation** option, then click **Next**.

5. Enter the following information on the **Basic Installation Details** page. See [Section 3.6](#) for more information about each of these topics.

- a. **Audit Vault Name** – A unique name for the Oracle Audit Vault database. The Oracle Audit Vault name is required. The name will be used as the database SID, and will be the first portion (*db_name*) of the database service name.
- b. **Audit Vault Home** – Specify or browse to find the path to the Oracle Audit Vault Home where you want to install Audit Vault Server. Install the Audit Vault Server into a new home directory.
- c. **Audit Vault Administrator** and **Audit Vault Auditor** – The account name of the Oracle Audit Vault Administrator and a separate, optional Oracle Audit Vault Auditor, respectively. The Oracle Audit Vault administrator and Oracle Audit Vault auditor account names must not be the same. The Oracle Audit Vault Administrator account name is required. For better security and to adhere to separation of duty guidelines, accept the selected **Create a Separate Audit Vault Auditor** check box to choose to create the Oracle Audit Vault Auditor account name. The check box is selected by default. Deselecting the check box disables the text fields for the Oracle Audit Vault Auditor user name and password. The Oracle Audit Vault Administrator in this case will also be granted the role of Oracle Audit Vault Auditor.

The Oracle Audit Vault Administrator user name will also be used for the following Oracle Database Vault users that are created to facilitate the separation of duties:

*AV_ADMIN*dv_o – The Oracle Database Vault Owner (granted DV_OWNER role) to manage Oracle Database Vault roles and configuration, where *AV_ADMIN* represents the Oracle Audit Vault Administrator user name.

*AV_ADMIN*dv_a – The Oracle Database Vault Account Manager (granted DV_ACCTMGR role) to manage database user accounts, where *AV_ADMIN* represents the Oracle Audit Vault Administrator user name.

- d. **Administrator Password** and **Auditor Password** – The password for the Oracle Audit Vault administrator account and the Oracle Audit Vault auditor account, respectively.

There cannot be repeating characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in [Table 3-3](#).

The password entered for the Oracle Audit Vault administrator account will also be used for the standard database accounts (*SYS*, *SYSTEM*, *SYSMAN*, *DBSNMP*).

The Oracle Audit Vault administrator password will also be used for the Oracle Database Vault users (Database Vault Owner and the Database Vault Account Manager users) that are created to facilitate the separation of duties.

- e. **Confirm Password** – The confirming password for the Oracle Audit Vault Administrator account and the Oracle Audit Vault auditor account, respectively.

Each password must be identical to its corresponding password confirmation.

Click **Next** to continue with the installation. The **Next** button is enabled only when information has been entered for all required fields. Validation of information occurs on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

- 6. If this is the first installation of an Oracle product on the system, the Oracle Universal Installer displays the **Specify inventory directory and credentials** page, enter the Inventory directory location and the OS group name, then click **Next**.
- 7. Review the installation prerequisite checks on the **Product-Specific Prerequisite Checks** page. This is when all installation prerequisite checks are performed and the results are displayed. Verify that all prerequisite checks succeed, then click **Next**.

Oracle Universal Installer checks the system to verify that it is configured correctly to run Oracle software. If you have completed all of the preinstallation steps in this guide, all of the checks should pass.

If a check fails, then review the cause of the failure listed for that check on the screen. If possible, rectify the problem and rerun the check. Alternatively, if you are satisfied that your system meets the requirements, then you can select the check box for the failed check to manually verify the requirement.

- 8. Review the installation summary information on the **Basic Installation Summary** page. The installation will copy files, link binaries, apply patches, run configuration assistants, including DBCA to create and start the Audit Vault Server, DVCA to secure the server, and AVCA to configure and start Oracle Audit Vault Console. After reviewing this installation information, click **Install** to begin the installation procedure.

At the end of running DBCA to configure the software and create the database, a message displays, click **OK** to continue.

- 9. Provide information or run scripts when prompted by Oracle Universal Installer. If there are scripts to be run, you need to run them on the remote node as the user who installed the Oracle Audit Vault database. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the Oracle Universal Installer actions recorded in the installation log file. The log file is located in the `Program Files\Oracle\Inventory` directory, in the following location:

```
SYSTEM DRIVE:\> Program Files\Oracle\Inventory\logs\installActionsdate_time.log
```

- 10. After the installation completes, take note of the Oracle Enterprise Manager Database Control URL and the Oracle Audit Vault Console URL. On the **Exit** page, click **Exit**. Then, on the **Confirmation** message box, click **Yes** to exit Oracle Universal Installer.

See [Section 3.7.8](#) for information about logging into Oracle Audit Vault Console and Oracle Enterprise Manager Database Control.

After you have completed the installation, proceed to [Section 3.7](#) to perform the postinstallation tasks.

3.3 Advanced Installation – Prerequisite Information for Installing in an Oracle Real Application Clusters Environment

This section assumes that you performed the initial installation procedures for installing Oracle Audit Vault with Oracle Real Application Clusters (Oracle RAC) as described in *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows*. These tasks include preinstallation tasks, configuring Oracle Clusterware and Oracle Database storage, installing Oracle Clusterware, and installing release 10.2.0.3 Patch set for Oracle Clusterware. You are now ready to install Audit Vault Server in an Oracle RAC environment as described in this section.

Verifying System Readiness for Installing Audit Vault Server with CVU

To help verify that your system is prepared to install Audit Vault Server with Oracle RAC successfully, use the Cluster Verification Utility (CVU) `runcvufy` command. See "Verifying System Readiness for Installing Oracle Database with CVU" in *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows* for more information.

If the cluster verification check fails, then review and correct the relevant system configuration steps, and run the test again. Use the system configuration checks described in "Troubleshooting Installation Setup for Windows" in *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows* to assist you.

3.4 Advanced Installation – Installing Single Instance and in an Oracle Real Application Clusters Environment

For an overview of requested information specific to the Audit Vault Server installation, see [Section 3.6](#).

This section describes the advanced installation for both the single instance installation and the Oracle RAC installation.

See [Section 2.8](#) for important information about setting the correct locale.

Perform the following procedures to install Audit Vault Server.

1. Unset the `ORACLE_HOME` environment variable.
From the **Start Bar**, select **Settings**, then from the **Control Panel** double click **System**, select the **Advanced** tab, select **Environment Variables**, then under **System Variables** look for `ORACLE_HOME`. If `ORACLE_HOME` is set, remove the setting by selecting it and clicking **Delete**, and then click **OK** to save your change.
2. Run Oracle Universal Installer (OUI) to install Audit Vault Server.
Log in as a member of the Administrators group to the computer on which to install Audit Vault Server.
If you are installing on a Primary Domain Controller (PDC) or a Backup Domain Controller (BDC), log on as a member of the Domain Administrators group

3. Change your current directory to the directory containing the installation files. Start Oracle Universal Installer from the Audit Vault Server package by double-clicking `setup.exe`.

```
cd directory-containing-the-Oracle-Audit-Vault-installation-files
setup.exe
```

4. In the Welcome window, on the **Select Installation Type** screen, select the **Advanced Installation** option, then click **Next**.
5. Enter the following information on the **Advanced Installation Details** screen. See [Section 3.6](#) for more information about each of these topics.
 - a. **Audit Vault Name** – A unique name for the Oracle Audit Vault database. The Oracle Audit Vault name is required. For a single instance installation, the name will be used as the database SID, and will be the first portion (*db_name*) of the database service name. For an Oracle RAC installation, the name will be used to derive the Oracle RAC database SID of each Oracle RAC node, and will be the first portion (*db_name*) of the database service name.
 - b. **Audit Vault Home** – Specify or browse to find the path to the Oracle Audit Vault home where you want to install Audit Vault Server. Install the Audit Vault Server into a new home directory.
 - c. **Audit Vault Administrator** and **Audit Vault Auditor** – The account name of the Oracle Audit Vault Administrator and a separate, optional Oracle Audit Vault Auditor, respectively. The Oracle Audit Vault Administrator and Oracle Audit Vault Auditor account names cannot be the same. The Oracle Audit Vault administrator account name is required. For better security and to adhere to separation of duty guidelines, accept the selected **Create a Separate Audit Vault Auditor** check box to choose to create the Oracle Audit Vault auditor account name. The check box is selected by default. Deselecting the check box disables the text fields for the Oracle Audit Vault auditor user name and password. The Oracle Audit Vault administrator in this case will also be granted the role of Oracle Audit Vault Auditor.
 - d. **Administrator Password** and **Auditor Password** – The password for the Oracle Audit Vault Administrator account and the Oracle Audit Vault auditor account, respectively.

There cannot be repeating characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in [Table 3–3](#).

- e. **Confirm Password** – The confirming password for the Oracle Audit Vault Administrator account and the Oracle Audit Vault Auditor account, respectively.

Each password must be identical to its corresponding password confirmation.

Click **Next** to continue with the installation. The **Next** button is enabled only when information has been entered for all required fields. Validation of information occurs on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

6. If this is the first installation of an Oracle product on the system, the Oracle Universal Installer displays the **Specify inventory directory and credentials** page, enter the Inventory directory location and the OS group name, then click **Next**.

7. Enter the following information on the **Database Vault User Credentials** screen. See [Section 3.6.2](#) for more information about each of these topics.
 - a. **Database Vault Owner** and **Database Vault Account Manager** – The account name of the Oracle Database Vault Owner and a separate, optional Oracle Database Vault Account Manager, respectively. The Oracle Database Vault Owner, Oracle Database Vault Account Manager, Oracle Audit Vault Administrator, and Oracle Audit Vault Auditor account names must not be the same (applicable when a separate Oracle Audit Vault Auditor or Oracle Database Vault Account Manager account is created). The Oracle Database Vault Owner name is required. Accept the selected **Create a Separate Database Vault Account Manager** check box to choose to create the Oracle Database Vault Account Manager account name. The check box is selected by default. Deselecting the check box disables the text fields for the Oracle Database Vault Account Manager user name and password. The Oracle Database Vault Owner in this case will also be granted the role of Database Vault Account Manager.
 - b. **Database Vault Owner Password** and **Database Vault Account Manager Password** – The password for the Database Vault Owner account and the Database Vault Account Manager account, respectively.

There cannot be repeating characters and space characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in [Table 3–3](#).
 - c. **Confirm Password** – The confirming password for the Database Vault Owner account and the Database Vault Account Manager account, respectively.

Each password must be identical to its corresponding password confirmation.

Click **Next** to continue with the installation. The **Next** button is enabled only when information has been entered for all required fields. Validation of information occurs on all user input after you click **Next**. The installation process will not continue until all required input passes validation.
8. If you are installing on a clustered system (Oracle Clusterware is installed and the system is already part of a cluster), the **Node Selection** screen appears from which to select the nodes on which Audit Vault Server will be installed. Local node will always be selected by default. If you are installing Audit Vault Server single instance on this local node only, select the **Local Only Installation** option, then click **Next**.

If installing on a clustered system (Oracle Clusterware is installed and the system is already part of a cluster), select the nodes on which on which Audit Vault Server will be installed, then click **Next**.
9. Review the installation prerequisite checks on the **Product-Specific Prerequisite Checks** screen. This is when all installation prerequisite checks are performed and the results are displayed. Verify that all prerequisite checks succeed, then click **Next**.

Oracle Universal Installer checks the system to verify that it is configured correctly to run Oracle Database software. If you have completed all of the preinstallation steps in this guide, all of the checks should pass.

If a check fails, then review the cause of the failure listed for that check on the screen. If possible, rectify the problem and rerun the check. Alternatively, if you are satisfied that your system meets the requirements, then you can select the check box for the failed check to manually verify the requirement.

10. On the **Specify Database Storage Options** screen, select one of the following storage options: **File system**, **Automatic Storage Management (ASM)**, or **Raw Devices**.

If you select **File System**, specify or browse to the database file location for the data files. If you select **Raw Devices**, specify the path or browse to the Raw Devices mapping file. If you select **Automatic Storage Management (ASM)**, you must have already installed ASM. Make a selection and click **Next**.

11. On the **Specify Backup and Recovery Options** page, choose either to not enable automated backups or to enable automated backups.

If you select the **Do not enable Automated backups** option, click **Next**.

If you select the **Enable Automated backups** option, then specify a **Recovery Area Storage**. You can choose either to use the **File System** option or the **Automatic Storage Management** option.

If you select the **File System** option, specify a path or browse to the recovery area location. Next, for **Backup Job Credentials**, enter the operating system credentials (user name and password) of the user account with administrative privileges to be used for the backup jobs, then click **Next**.

If you select the **Automatic Storage Management** option, then for **Backup Job Credentials**, enter the operating system credentials (user name and password) of the user account with administrative privileges to be used for the backup jobs, then click **Next**.

Next, select the disk group from the existing disk groups. This screen lets you select the disk groups. If the disk group selected has enough free space, by clicking **Next**, the **Specifying Database Schema Password** screen appears (see Step 12). If the disk group selected does not have enough free space, the **Configure Automatic Storage Management** page is displayed.

On the **Configure Automatic Storage Management** screen, select the disks to add from the **Add Member Disks** table by selecting the check box in the **Select** column for the corresponding disks. As you select the disks, the Required Storage Space area adjusts the sizes displayed. Ideally, the **Additional Space Needed** value is a negative number. Click **Next**.

12. On the **Specify Database Schema Passwords** screen, choose to enter different passwords for each privileged database account or select the **Use the same passwords for all accounts** option. If you choose to enter a set of valid passwords for each privileged database account, enter these passwords. If you select the **Use the same passwords for all accounts** option, then enter a single valid password. When you are finished, click **Next**.

13. Review the installation summary information on the **Advanced Installation Summary** screen. The installation will copy files, link binaries, apply patches, run configuration assistants, including DBCA to create and start the Audit Vault Server, DVCA to secure the server, and AVCA to configure and start Oracle Audit Vault Console. After reviewing this installation information, click **Install** to begin the installation procedure.

At the end of running DBCA to configure the software and create the database, a message displays, click **OK** to continue.

14. Run scripts when prompted by Oracle Universal Installer. If you need assistance during installation, click **Help**. If you encounter problems during installation, then examine the Oracle Universal Installer actions recorded in the installation log file.

The log file is located in the Program Files\Oracle\Inventory directory in the following location:

```
SYSTEM_DRIVE:\> Program Files\Oracle\Inventory\logs\installActionsdate_time.log
```

Note: The Oracle home name and path that you provide during Audit Vault Server installation *must be different* from the home that you used during the Oracle Clusterware installation. You **cannot** install Audit Vault Server with Oracle RAC software into the same home in which you installed the Oracle Clusterware software.

The following is a list of additional information to note about installation:

- If you are not using the ASM library driver (ASMLIB), and you select Automatic Storage Management (ASM) during installation, then ASM default discovery finds all disks that ASMLIB marks as ASM disks.
- If you are not using ASMLIB, and you select ASM during installation, then ASM default discovery finds all disks marked by the default discovery path for which the Oracle Software user has read/write permission. You can change the disk discovery path during the installation if the disks that you want to use for ASM are located elsewhere.
- On the **Select Database Management Option** page, if you have already completed the Grid Control Management Agent installation, then you can select either Grid or Local Database control. Otherwise, only Local Database control for database management is supported for Oracle RAC. When you use the local Database Control, you can choose the email option and enter the outgoing SMTP server name and e-mail address.

See Also: *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for details about installing Grid Control with OUI, and *Oracle Enterprise Manager Advanced Configuration Guide* for details about installing Database Control with Database Configuration Assistant (DBCA) and Enterprise Manager Configuration Assistant (EMCA)

15. After the installation completes, take note of the Oracle Enterprise Manager Database Control URL and the Oracle Audit Vault Console URL. On the **Exit** page, click **Exit**. Then, on the **Confirmation** message box, click **Yes** to exit Oracle Universal Installer.

See [Section 3.7.8](#) for information about logging into Oracle Audit Vault Console and Oracle Enterprise Manager Database Control.

After you have completed this part of the installation, proceed to [Section 3.7](#) to perform the postinstallation tasks.

3.5 Performing a Silent Installation Using a Response File

For an overview of requested information specific to the Audit Vault Server installation, see [Section 3.6](#).

Note: The basic installation is not supported in silent mode. Silent installation is only supported for the advanced installation.

Follow these brief steps to perform a silent installation using a response file:

1. Ensure that you have met the prerequisites for the installation of Audit Vault Server.
2. Prepare the Audit Vault Server response file. A template response file can be found at *AV-installer-location\response\av.rsp* on the Audit Vault Server installation media.

Prepare the response file by entering values for all parameters that are missing in the first part of the response file, then save the file. Note that for single instance installations, RAW storage is not used. Also note that the `CLUSTER_NODES` parameter must be specified for installing Audit Vault Server in an Oracle RAC environment. Do not edit any values in the second part of the response file.

3. Invoke Oracle Universal Installer using the following options:

```
setup.exe -silent -responseFile path-of-response-file
```

For more information about these options, see [Section 1.2.2](#). For general information about how to complete a database installation using response files, see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows*.

3.6 Audit Vault Server Installation Details

This section provides an overview of requested information specific to the Audit Vault Server installation.

An Audit Vault Server installation consists of three options:

- **Basic Installation** – Simplifies the installation process and prompts for a minimal set of inputs, including the name of the Oracle Audit Vault database, the Oracle Audit Vault administrator and optionally the auditor user names and passwords. An Oracle RAC installation is not supported through the **Basic Installation** option.
- **Advanced Installation** – Offers the user more control and options for the installation process, including storage options and backup options. The **Advanced Installation** option supports the installation of Audit Vault Server on a cluster.

This section covers the following topics:

- [Basic and Advanced Installation Details Screens](#)
- [Advanced Server Installation: Database Vault User Credentials Screen](#)
- [Advanced Server Installation: Node Selection Screen](#)
- [Advanced Server Installation: Specify Database Storage Options Screen](#)
- [Advanced Server Installation: Specify Backup and Recovery Option Screen](#)
- [Advanced Server Installation: Specify Database Schema Passwords Screen](#)

3.6.1 Basic and Advanced Installation Details Screens

This section describes the required fields in the **Basic Installation Details** screen and the **Advanced Installation Details** screen.

3.6.1.1 Audit Vault Name

The Audit Vault Name must be a unique name for the Oracle Audit Vault database. The name will be used for the database SID, and will be the first portion (*db_name*) of the database service name.

The name cannot exceed 8 characters and must begin with an alphabetic character. The name should only use ASCII characters.

The Oracle Audit Vault name cannot contain any of the characters shown in [Table 3–1](#).

Table 3–1 Invalid Oracle Audit Vault Name and Oracle Audit Vault Account Name Characters

Symbol	Character Name
!	Exclamation point
@	At sign
%	Percent sign
^	Circumflex
&	Ampersand
*	Asterisk
(Left parenthesis
)	Right parenthesis
-	Minus sign
+	Plus sign
=	Equal sign
"	Double quotation mark
	Vertical bar
`	grave
~	tilde
[Left bracket
{	Left brace
]	Right bracket
}	Right brace
;	Semicolon
:	Colon
'	Single quotation mark
<	Less than sign
>	Greater than sign
/	Slash
\	Backslash
?	Question mark
,	Comma
.	Period
#	Number sign

Table 3–1 (Cont.) Invalid Oracle Audit Vault Name and Oracle Audit Vault Account Name Characters

Symbol	Character Name
_	Underscore
\$	Dollar sign
	Space character

3.6.1.2 Oracle Audit Vault Home

The Oracle Audit Vault Home is the path that you must specify or browse to find the Audit Vault Server home where you want to install Audit Vault Server. The path can contain only alphanumeric characters (letters and numbers).

In addition, the special characters shown in [Table 3–2](#) are allowed.

Table 3–2 Special Characters Allowed in the Audit Vault Server Home Name

Symbol	Character Name
\	Backslash
/	Slash
-	hyphen
_	Underscore
.	Period
:	Colon

3.6.1.3 Oracle Audit Vault Server Accounts

The Audit Vault Server installation software prompts you for user names and passwords for the Oracle Audit Vault Administrator user and the separate, optional Oracle Audit Vault Auditor user. In addition, the installation creates an Oracle Database Vault Owner user and a separate Oracle Database Vault Account Manager user for you (basic installation) or the installation prompts you for these user names and passwords (advanced installation). Finally, the installation creates `sys`, `system`, `sysman`, and `dbsnmp` standard database users for you (basic installation) or the installation prompts for passwords for these users (advanced installation). For the basic installation, the installation creates an Oracle Database Vault Owner, Oracle Database Vault Account Manager, `SYS`, `SYSTEM`, `SYSMAN`, and `DBSNMP` accounts all with the same password as that of the Oracle Audit Vault Administrator.

You must supply a user name and password for the Oracle Audit Vault administrator user and optionally for the Oracle Audit Vault Auditor user during installation. The **Create a Separate Audit Vault Auditor** check box is selected by default, which means that a separate Oracle Audit Vault Auditor account will be created (and the corresponding user name and password are required). The Oracle Audit Vault administrator user will be granted the `AV_ADMIN` role and the Oracle Audit Vault auditor user will be granted the `AV_AUDITOR` role. For better security and separation of duty, Oracle recommends that you create the Audit Vault auditor account. Deselecting this check box means that the Oracle Audit Vault administrator user will be granted both roles because the separate Oracle Audit Vault auditor user will not be created.

Oracle Audit Vault Administrator and Oracle Audit Vault Auditor Accounts

The Oracle Audit Vault Administrator account is granted the AV_ADMIN role. The user granted the AV_ADMIN role can manage the postinstallation configuration. This role accesses Oracle Audit Vault services to administer, configure, and manage a running Oracle Audit Vault system. This role registers audit sources. This role has the ability to configure parameters that assist in populating the Oracle Audit Vault data warehouse. For the basic installation, the Oracle Audit Vault Administrator user name is used to generate the following Oracle Database Vault users to facilitate the separation of duties:

- AV_ADMINdvo – The Oracle Database Vault Owner (granted DV_OWNER role) to manage Oracle Database Vault roles and configuration
- AV_ADMINdva – The Oracle Database Vault Account Manager (granted DV_ACCTMGR role) to manage database user accounts

For the advanced installation, a **Database Vault User Credentials** page prompts for the Oracle Database Vault Owner account name and password and a separate, optional Oracle Database Vault Account Manager account name and password. For better security and separation of duty, Oracle recommends that you create the Oracle Database Vault Account Manager account.

The Oracle Audit Vault Auditor account is granted the AV_AUDITOR role. The user granted the AV_AUDITOR role accesses Oracle Audit Vault Reporting and Analysis services to monitor components, detect security risks, create and evaluate alert scenarios, create detail and summary reports of events across systems, and manage the reports. This role manages central audit settings. This role can use the data warehouse services to further analyze the audit data to assist in looking for trends, intrusions, anomalies, and other areas of interest.

The Oracle Audit Vault Administrator, Oracle Audit Vault Auditor, Oracle Database Vault Owner, and Oracle Database Vault Account Manager user names must not be the same. For the basic installation, the Oracle Audit Vault Administrator user name must be between 2 and 27 characters because the characters "dvo" and "dva" are appended to the Administrator name making the normal upper limit of 30 characters for the user names that are allowed to be 27 characters. For the advanced installation, the Oracle Audit Vault Administrator user name must be between 2 and 30 characters.

The length of the Oracle Audit Vault Auditor user name must be between 2 and 30 characters. Each user name must not be one of the following reserved names.

Names	Names	Names	Names	Names
ACCESS	ADD	ALL	ALTER	AND
ANONYMOUS	ANY	AQ_ADMINISTRATOR_ROLE	AQ_USER_ROLE	ARRAYLEN
AS	ASC	AUDIT	AUTHENTICATEDUSER	AV_ADMIN
AV_AGENT	AV_ARCHIVER	AV_AUDITOR	AV_SOURCE	AVSYS
BETWEEN	BY	CHAR	CHECK	CLUSTER
COLUMN	COMMENT	COMPRESS	CONNECT	CREATE
CTXAPP	CTXSYS	CURRENT	DATE	DBA
DBSNMP	DECIMAL	DEFAULT	DELETE	DELETE_CATALOG_ROLE
DESC	DIP	DISTINCT	DM_CATALOG_ROLE	DMSYS
DMUSER_ROLE	DROP	DV_ACCTMGR	DV_ADMIN	DVF
DV_OWNER	DV_PUBLIC	DV_REALM_OWNER	DV_REALM_RESOURCE	DV_SECANALYST
DVSYSD	EJBCCLIENT	ELSE	EXCLUSIVE	EXECUTE_CATALOG_ROLE

Names	Names	Names	Names	Names
EXFSYS	EXISTS	EXP_FULL_DATABASE	FILE	FLOAT
FOR	FROM	GATHER_SYSTEM_STATISTICS	GLOBAL_AQ_USER_ROLE	GRANT
GROUP	HAVING	HS_ADMIN_ROLE	IDENTIFIED	IMMEDIATE
IMP_FULL_DATABASE	IN	INCREMENT	INDEX	INITIAL
INSERT	INTEGER	INTERSECT	INTO	IS
JAVA_ADMIN	JAVADEBUGPRIV	JAVA_DEPLOY	JAVAIDPRIV	JAVASYSPRIV
JAVAUERPRIV	LBAC_DBA	LBACSYS	LEVEL	LIKE
LOCK	LOGSTDBY_ADMINISTRATOR	LONG	MAXEXTENTS	MDDATA
MDSYS	MGMT_USER	MGMT_VIEW	MINUS	MODE
MODIFY	NOAUDIT	NOCOMPRESS	NOT	NOTFOUND
NOWAIT	NULL	NUMBER	OEM_ADVISOR	OEM_MONITOR
OF	OFFLINE	OLAP_DBA	OLAPSYS	OLAP_USER
ON	ONLINE	ONT	OPTION	OR
ORDER	ORDPLUGINS	ORDSYS	OUTLN	OWF_MGR
PCTFREE	PRIOR	PRIVILEGES	PUBLIC	RAW
RECOVERY_CATALOG_OWNER	RENAME	RESOURCE	REVOKE	ROW
ROWID	ROWLABEL	ROWNUM	ROWS	SCHEDULER_ADMIN
SCOTT	SELECT	SELECT_CATALOG_ROLE	SESSION	SET
SHARE	SI_INFORMTN_SCHEMA	SIZE	SMALLINT	SQLBUF
START	SUCCESSFUL	SYNONYM	SYS	SYSDATE
SYSMAN	SYSTEM	TABLE	THEN	TO
TRIGGER	TSMYSYS	UID	UNION	UNIQUE
UPDATE	USER	VALIDATE	VALUES	VARCHAR
VARCHAR2	VIEW	WHENEVER	WHERE	WITH
WKPROXY	WKSYS	WK_TEST	WKUSER	WM_ADMIN_ROLE
WMSYS	XDB	XDBADMIN		

Each account name cannot contain any of the characters shown in [Table 3-1](#).

Oracle Audit Vault Administrator and Oracle Audit Vault Auditor Passwords

For the basic installation, the Oracle Audit Vault Administrator password you enter for the Oracle Audit Vault Administrator account is also used for the standard database accounts (*sys*, *system*, *sysman*, *dbnmp*). For the basic installation **Details** page, the Oracle Audit Vault Administrator user password is also used for the Oracle Database Vault Owner and Oracle Database Vault Account Manager user passwords.

For the advanced installation, the installer can choose individual passwords for each of these database accounts (*sys*, *system*, *sysman*, *dbnmp*) or select to use the same password as the Oracle Audit Vault Administrator for all of these accounts. In addition, a **Database Vault User Credentials** page prompts for the Oracle Database Vault Owner user password and for a separate, optional Oracle Database Vault Account Manager user password if that user is created.

The Oracle Audit Vault Administrator and Oracle Audit Vault Auditor password cannot be the name of the Oracle Audit Vault Administrator, Oracle Audit Vault Auditor, Oracle Database Vault Owner, or Oracle Database Vault Account Manager. The Oracle Audit Vault Administrator user password is required, while the Oracle Audit Vault Auditor user password is only required when creating the separate, optional Oracle Audit Vault Auditor user.

There cannot be repeating characters in each password. The length of each password must be between 8 and 30 characters. Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in [Table 3–3](#).

Table 3–3 Valid Oracle Audit Vault Administrator and Oracle Audit Vault Auditor Password Characters

Symbol	Character Name
%	Percent sign
^	Circumflex
-	Hyphen
[Left bracket
+	Plus sign
~	Tilde
,	Comma
#	Number sign
]	Right bracket
.	Period
_	Underscore

Each password must be identical to its corresponding password confirmation.

3.6.2 Advanced Server Installation: Database Vault User Credentials Screen

The Audit Vault Server installation software prompts you for two accounts that you create during installation. These are the Oracle Database Vault Owner account and the separate, optional Oracle Database Vault Account Manager account. You must supply an account name and password for the Oracle Database Vault Owner account, and optionally for the Oracle Database Vault Account Manager account during installation. For better security and separation of duty, Oracle recommends that you create the Oracle Database Vault Account Manager account.

The **Create a Separate Database Vault Account Manager** check box is selected by default, which means that a separate Oracle Database Vault Account Manager account will be created (and the corresponding user name and password are required). The Oracle Database Vault Owner user will be granted the `DV_OWNER` role and the Oracle Database Vault Account Manager user will be granted the `DV_ACCTMGR` role. Deselecting this check box means that the Oracle Database Vault Owner user will be granted both roles, because the separate Oracle Database Vault Account Manager user will not be created.

3.6.2.1 Oracle Database Vault Owner and Oracle Database Vault Account Manager Accounts

The Oracle Database Vault Owner, Oracle Database Vault Account Manager, Oracle Audit Vault Administrator, and Oracle Audit Vault Auditor account names must be different from each other (applicable when a separate Oracle Audit Vault Auditor or Oracle Database Vault Account Manager account is created). The Oracle Database Vault Owner name is required.

The length of each account name must be between 2 and 30 characters.

Each account name must not be one of the reserved names shown in the table in [Section 3.6.1.3](#).

Each account name cannot contain any of the characters shown in [Table 3-1](#).

3.6.2.2 Oracle Database Vault Owner and Oracle Database Vault Account Manager Passwords

The Oracle Database Vault Owner or Oracle Database Vault Account Manager password must not be the name of the Oracle Audit Vault Administrator, Oracle Audit Vault Auditor, Oracle Database Vault Owner, or Oracle Database Vault Account Manager. The Oracle Database Vault Owner user password is required, while the Oracle Database Vault Account Manager user password is only required when creating the separate, optional Oracle Database Vault Account Manager user.

Do not include repeating characters or space characters in the password.

The length of each password must be between 8 and 30 characters.

Each password must consist of at least one alphabetic character, one numeric character, and one of the special characters shown in [Table 3-3](#). All other characters are not allowed.

Each password must be identical to its corresponding password confirmation.

3.6.3 Advanced Server Installation: Node Selection Screen

The **Node Selection** screen appears if you are installing Audit Vault Server in an Oracle RAC environment and a clustered system (Oracle Clusterware) is installed and the system is already part of a cluster. On this screen, you can select the nodes on which they want to install Audit Vault Server, or you can select a local installation to install Audit Vault Server single instance. See *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows* for more information.

3.6.4 Advanced Server Installation: Specify Database Storage Options Screen

On the **Specify Database Storage Options** screen, you can select **File System**, **Automatic Storage Management**, or **Raw Storage**.

File System

If you choose the **File System** option, then Database Configuration Assistant creates the database files in a directory on a file system mounted on the computer. Oracle recommends that the file system you choose be separate from the file systems used by the operating system or the Oracle software. The file system that you choose can be any of the following:

- A file system on a disk that is physically attached to the system

If you are creating a database on basic disks that are not logical volumes or redundant arrays of independent disks (RAID) devices, then Oracle recommends that you follow the Optimal Flexible Architecture (OFA) recommendations and distribute the database files over more than one disk.

- A file system on a logical volume manager (LVM) volume or a RAID device

If you are using multiple disks in an LVM or RAID configuration, then Oracle recommends that you use the stripe and mirror everything (SAME) methodology to increase performance and reliability. Using this methodology, you do not need to specify more than one file system mounting point for database storage.

Automatic Storage Management

Automatic Storage Management (ASM) is a high-performance storage management solution for Oracle Audit Vault database files. It simplifies the management of a dynamic database environment, such as creating and laying out databases and managing disk space.

Note: An existing release 10.2.0.4 ASM instance must be installed to select the ASM option for database storage.

ASM can be used with a single instance Audit Vault Server installation, multiple Audit Vault Server installations, and in an Oracle Real Application Clusters (Oracle RAC) environment. ASM manages the storage of all Oracle Audit Vault database files, such as redo logs, control files, data pump export files, and so on.

See: *Oracle Database Administrator's Guide* for more information.

Raw Devices

Raw devices are disk partitions or logical volumes that have not been formatted with a file system. When you use raw devices for database file storage, Oracle Database writes data directly to the partition or volume, bypassing the operating system file system layer. For this reason, you can sometimes achieve performance gains by using raw devices. However, because raw devices can be difficult to create and administer, and because the performance gains over more modern file systems are minimal, Oracle recommends that you choose ASM or file system storage instead of raw devices.

3.6.5 Advanced Server Installation: Specify Backup and Recovery Option Screen

On the **Specify Backup and Recovery** screen, you can choose **Enable Automated Backups** or **Do Not Enable Automated Backups**.

If you choose **Enable Automated Backups**, then Oracle Enterprise Manager schedules a daily backup job that uses Oracle Recovery Manager (RMAN) to back up all of the database files to an on-disk storage area called the flash recovery area. The first time that the backup job runs, it creates a full backup of the database. Subsequent backup jobs perform incremental backups, which enable you to recover the database to its state at any point during the preceding 24 hours.

To enable automated backup jobs during installation, you must specify the following information:

- The location of the flash recovery area

You can choose to use either a file system directory or an ASM disk group for the flash recovery area. The default disk quota configured for the flash recovery area is 2 GB. For ASM disk groups, the required disk space depends on the redundancy level of the disk group that you choose. See *Oracle Database Installation Guide for Microsoft Windows (32-Bit)* for more information about how to choose the location of the flash recovery area and to determine its disk space requirements.

- An operating system user name and password for the backup job
- Oracle Enterprise Manager uses the operating system credentials that you specify when running the backup job. The user name that you specify must belong to the local group `ORA_DBA` that identifies database administrators who automatically receive the `SYSDBA` privilege. The user name belonging to the Administrator's group that you use to install the software is a suitable choice for this user.

Backup Job Default Settings

If you enable automated backups after choosing one of the preconfigured databases during the installation, then automated backup is configured with the following default settings:

- The backup job is scheduled to run nightly at 2:00 a.m.
- The disk quota for the flash recovery area is 2 GB.

If you enable automated backups by using Database Configuration Assistant after the installation, then you can specify a different start time for the backup job and a different disk quota for the flash recovery area.

For information about using Oracle Enterprise Manager Database Control to configure or customize automated backups or to recover a backed up database, see *Oracle Database 2 Day DBA*.

For more detailed information about defining a backup strategy and backing up and recovering Oracle databases, see *Oracle Database Backup and Recovery Advanced User's Guide*.

3.6.6 Advanced Server Installation: Specify Database Schema Passwords Screen

On the **Specify Database Schema Passwords** screen, provide the passwords for the four standard database accounts (`SYS`, `SYSTEM`, `SYSMAN`, and `DBSNMP`).

Either enter and confirm passwords for the privileged database accounts, or select the **Use the same passwords for all accounts** option. Make your selection, then click **Next**.

3.7 Postinstallation Server Tasks

Note: The use of the Database Configuration Assistant (DBCA) to configure additional components after an Audit Vault Server installation is not supported. Audit Vault Server installs with all of the components that it requires already configured, so no additional components need to be configured using DBCA.

Creation of additional databases in the Oracle Audit Vault home is not supported.

Cloning of Oracle Audit Vault homes is not supported.

This section includes the following topics:

- [Download Patches](#)
- [Download Critical Patch Updates](#)
- [Reset User Passwords](#)
- [Enable or Disable Connections with the SYSDBA Privilege](#)
- [Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions \(Oracle RAC Only\)](#)
- [Download JDBC Driver Files for Source Database Connectivity](#)
- [Log in to Oracle Audit Vault Console](#)
- [Next Steps to Perform as an Oracle Audit Vault Administrator](#)

3.7.1 Download Patches

You can find mandatory Oracle Audit Vault patchsets on the My Oracle Support (formerly Oracle*MetaLink*) Web site.

To find and download patchsets for Audit Vault Server:

1. Log in to My Oracle Support from the following URL:
<https://support.oracle.com>
2. Click the **Patches & Updates** tab.
3. Under **Patch Search**, click **Product or Family (Advanced Search)**.
4. Enter Oracle Audit Vault in the search field.
5. In the first **Select one or more** list, expand the Oracle Audit Vault list and select **Audit Vault 10.2.3.2.0**. Click **Close**.
6. In the second **Select one or more** list, select **Microsoft Windows (32-bit)**, then click **Close**.
7. Click **Search**. In a moment, the patches associated with your selection appear.
8. Select the patch you want from the list by clicking its Patch ID link.
9. Click **View Read Me** to read about the patch details, and then click **Download** to download the patch to your computer.
10. Repeat Step 8 through Step 9 for each patch listed in the Patch Search Results section.

Note: Do not apply any Oracle Database one-off patches to the Oracle Audit Vault database unless directed to do so by Oracle Support Services.

3.7.2 Download Critical Patch Updates

A critical patch update (CPU) is a collection of patches for security vulnerabilities. It includes non-security fixes required (because of interdependencies) by those security patches. Critical patch updates are cumulative, and they are provided quarterly on the Oracle Technology Network. You should periodically check My Oracle Support for critical patch updates.

To find and download critical patch updates for Audit Vault Server:

1. Follow Step 1 through Step 3 in [Section 3.7.1](#) to find the critical patch updates for Audit Vault Server.
2. In the list of articles that appears, search for the phrase `Oracle Critical Patch Update`.
3. Select the most recent critical patch update article, and then read its instructions.
Download the most recent critical patch update for Audit Vault Server. In most critical patch update articles, there is section entitled "Patch Download Procedure," which explains how to download the critical patch update.

For more information about critical patch updates, see:

<http://www.oracle.com/security/critical-patch-update.html>

For the latest information on whether a specific critical patch update is certified with Oracle Audit Vault, review the certification matrix on the My Oracle Support Web site, at:

<https://support.oracle.com>

3.7.3 Reset User Passwords

Audit Vault Server uses the password you enter for the Oracle Audit Vault Administrator as the password for core database accounts such as `SYS`, `SYSTEM`, `SYSMAN`, and `DBSNMP` in a basic installation. For an advanced installation, you are given the option of changing the password for each of these accounts.

For a basic installation, Audit Vault Server also uses the same Oracle Audit Vault administrator password for the `AV_ADMIN` account, the Oracle Database Vault Owner (granted `DV_OWNER` role), to manage Oracle Database Vault roles and configuration; and the `AV_ADMIN` account, the Oracle Database Vault Account Manager (granted `DV_ACCTMGR` role), to manage database user accounts. You must change these passwords according to your company policies.

For an advanced installation, Audit Vault Server uses the Oracle Database Vault Owner user password and the separate, optional Oracle Database Vault Account Manager user password you enter for these users. You must change these passwords according to your company policies.

3.7.3.1 Using SQL*Plus to Reset Passwords

To reset user account passwords using SQL*Plus:

1. Start SQL*Plus and log in as `AV_ADMIN` account.
2. Enter a command similar to the following, where *account* is the user account that you want and *password* is the new password:

```
SQL> ALTER USER account IDENTIFIED BY password;
```

In this example:

The `IDENTIFIED BY password` clause resets the password.

See Also: *Oracle Database Administrator's Guide* for more information about:

- Changing passwords after installation
- Oracle security procedures
- Best security practices

3.7.4 Enable or Disable Connections with the SYSDBA Privilege

Oracle Database Vault allows you to disable remote logins with the `SYSDBA` privilege. This enables enhanced security for your database.

To disable remote `SYSDBA` connections, re-create the password file with the `nosysdba` flag set to `y` (Yes). A user can still log in `AS SYSDBA` locally using Operating System (OS) authentication. However, remote connections `AS SYSDBA` will fail.

Use the following syntax to run the `orapwd` utility:

```
orapwd file=filename password=password [entries=users] force=y/n nosysdba=y/n
```

In this example:

- `file` is the name of password file (mandatory).
- `password` is the password for `SYS` (mandatory). Enter at least six alphanumeric characters.
- `entries` is the maximum number of distinct DBA users.
- `force` indicates whether to overwrite the existing file (optional). Enter `y` (for yes) or `n` (for no).
- `nosysdba` indicates whether to enable or disable the `SYS` login (optional for Oracle Database Vault only). Enter `y` (to disable `SYS` login) or `n` (to enable `SYS` login).

The default is `no`. If you omit this flag, the password file will be created enabling `SYSDBA` access for Oracle Database Vault instances.

For example:

```
orapwd file=ORACLE_HOME/dbs/orapworcl password=password force=y nosysdba=n
```

Note: Do not insert spaces around the equal sign (=).

See Also: *Oracle Database Administrator's Guide* for more information about using the `orapwd` utility

Enable or Disable Connecting with SYSDBA on Oracle Real Application Clusters Systems

Under a cluster file system and raw devices, you must update each node to enable or disable the `SYSDBA` connection privilege by using the `orapwd` utility.

Enable or Disable Connecting with SYSDBA on Automatic Storage Management Systems

For Automatic Storage Management systems, you must update each node to enable or disable the `SYSDBA` connection privilege by using the `orapwd` utility.

3.7.5 Run DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC Only)

After installing Audit Vault Server for an Oracle RAC instance, you must run Database Vault Configuration Assistant (DVCA) with the `-action optionrac` switch on all other Oracle RAC nodes. This sets instance parameters and disables `SYSDBA` operating system authentication.

You must run this command on all Oracle RAC nodes other than the node on which the Audit Vault Server installation is performed. This step is required to enable the enhanced security features provided by Oracle Database Vault.

Note: The listener and database instance should be running on the nodes on which you run DVCA.

Use the following syntax to run DVCA:

```
dvca -action optionrac -racnode host_name -oh oracle_home
-jdbc_str jdbc_connection_string -sys_passwd sys_password
[-logfile ./dvca.log] [-silent] [-nodecrypt] [-lockout]
```

In this example:

- `action` is the action to perform. The `optionrac` utility performs the action of updating the instance parameters for the Oracle RAC instance and optionally disabling SYSDBA operating system access for the instance.
- `racnode` is the host name of the Oracle RAC node on which the action is being performed. Do not include the domain name with the host name.
- `oh` is the Oracle home for the Oracle RAC instance.
- `jdbc_str` is the JDBC connection string used to connect to the database. For example, "jdbc:oracle:oci:@orcl1".
- `sys_password` is the password for the SYS user.
- `logfile` is optionally used to specify a log file name and location. You can enter an absolute path or a path that is relative to the location of the \$ORACLE_HOME/bin directory.
- `silent` is required if you are not running DVCA in an Xterm window.
- `nodecrypt` reads plain text passwords as passed on the command line.
- `lockout` is used to disable SYSDBA operating system authentication.

Note: You can reenable SYSDBA access by re-creating the password file with the `nosysdba` flag set to `n` (No). The `orapwd` utility enables you to do this.

After running DVCA, stop and restart the instance and database listener on all cluster nodes. This step is also applicable to the node on which Audit Vault Server was installed. Use the following commands:

```
srvctl stop instance -d sid -i instance_name -c "SYS/password AS SYSDBA"
srvctl stop nodeapps -n node_name
srvctl start nodeapps -n node_name
srvctl start instance -d sid -i instance_name -c "SYS/password AS SYSDBA"
```

3.7.6 Download JDBC Driver Files for Source Database Connectivity

Oracle Audit Vault enables you to collect audit trails from Microsoft SQL Server, Sybase Adaptive Server Enterprise, and IBM DB2 databases.

To allow connectivity between Audit Vault Server and Microsoft SQL Server source databases, Audit Vault Server and Sybase ASE source databases, and Audit Vault Server and IBM DB2 databases, you must download and copy the respective JDBC Driver jar file to the designated location.

[Section 3.7.6.1](#), [Section 3.7.6.2](#), and [3.7.6.3](#) describe this download process for each JDBC Driver.

3.7.6.1 Download Microsoft SQL Server JDBC Driver for SQL Server Connectivity

Oracle Audit Vault requires a JDBC connection to the SQL Server database. Audit Vault supports Microsoft SQL Server 2005 JDBC Driver 1.2.

This driver provides high performance native access to Microsoft SQL Server 2000 and SQL Server 2005 database data sources. Check the following Web sites for more information about the Microsoft SQL Server JDBC drivers and download.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c47053eb-3b64-4794-950d-81e1ec91c1ba&displaylang=en>

This Type 4 JDBC driver (`sqljdbc.jar`) provides highly scalable and reliable connectivity for the enterprise Java environment and provides JDBC access to SQL Server databases through any Java-enabled applet, application, or application server.

Download the JDBC driver (`sqljdbc.jar`) to the following Audit Vault Server home location:

```
ORACLE_HOME\jlib
```

3.7.6.2 Download jConnect JDBC Driver for Sybase ASE Connectivity

Download jConnect for JDBC, which provides high performance native access to Sybase ASE data sources, from the following link:

<http://www.sybase.com/products/allproductsa-z/softwaredeveloperkit/jconnect>

jConnect for JDBC (`jconn3.jar`) is a high performance JDBC Driver from Sybase that communicates directly to Sybase data sources.

Copy the `jconn3.jar` file to the Audit Vault Server home location:

```
ORACLE_HOME\jlib
```

3.7.6.3 Copy the DB2 JDBC and SQLJ Driver to the Audit Vault Homes

Copy the IBM Data Server Driver for JDBC and SQLJ (`db2jcc.jar`) to the `ORACLE_HOME\jlib` directory in the Audit Vault Server home. Oracle Audit Vault requires driver version 3.50 or later. This version of the `db2jcc.jar` file is available in either IBM DB2 UDB version 9.5 or IBM DB2 Connect version 9.5 or later.

This driver provides high performance native access to IBM DB2 database data sources. The DB2 collector uses this driver to collect audit data from IBM DB2 databases, so the driver must be present in Oracle Audit Vault OCFJ before you can start the collection agent.

You can verify the version of this `.jar` file that is currently installed as follows:

1. Ensure that the directory path to the `db2jcc.jar` file is included in the `CLASSPATH` environment variable setting.
2. Run the following command:

```
java com.ibm.db2.jcc.DB2Jcc -version
```

3.7.7 Log in to Oracle Audit Vault Console

Use the following instructions to log in to the Oracle Audit Vault Console:

1. On the node from which you installed the database, open a Web browser to access the Oracle Audit Vault Console URL, and use the following URL syntax:

```
http://host:port/av
```

In the preceding example:

- *host* is the name of the computer on which you installed Oracle Audit Vault Database.
- *port* is the port number reserved for the Oracle Audit Vault Console during installation.

If you do not know the correct port number to use, then perform the following steps in the Audit Vault Server home shell:

- a. Issue the AVCTL `show_av_status` command. The output displays the Oracle Audit Vault Console URL.
 - b. On any system, enter this URL in a Web browser and Oracle Enterprise Manager will display the Oracle Audit Vault Console login page.
2. Log in to the Oracle Audit Vault Console using the user name `AV_ADMIN` and the `AV_ADMIN` password that you created during the installation.

3.7.8 Next Steps to Perform as an Oracle Audit Vault Administrator

After Audit Vault Server installation is complete, see *Oracle Audit Vault Collection Agent Installation Guide* for information about installing Oracle Audit Vault collection agents and the collectors.

After an Oracle Audit Vault collection agent installation is complete, see *Oracle Audit Vault Administrator's Guide* for some Oracle Audit Vault Administration tasks to perform. These tasks include:

1. For collecting audit records from Oracle Database audit sources, see *Adding a Source and Collectors for an Oracle Database Source*.
2. For collecting audit records from SQL Server Database audit sources, see *Adding a Source and Collector for a SQL Server Database Source*.
3. For collecting audit records from Sybase ASE Database audit sources, see *Adding a Source and Collector for a Sybase ASE Database Source*.
4. For collecting audit records from IBM DB2 database audit sources, see the information about registering IBM DB2 sources and collector.
5. To start collecting audit records from a database audit source, see *Starting Up Collection Agents and Collectors*.
6. To perform other Oracle Audit Vault configuration tasks, see *Performing Additional Oracle Audit Vault Configuration Tasks*.
7. To manage and monitor an Oracle Audit Vault system, see *Managing Oracle Audit Vault*.

8. Before going into production be sure to secure management communications, see Oracle Advanced Security – Secure Management Communication.

Removing Audit Vault Server Software

This chapter describes the process of removing the Oracle Audit Vault Server (Audit Vault Server) software. It contains the following sections:

- [Removing the Audit Vault Server Software](#)
- [Manually Remove the Remaining Oracle Audit Vault Server Components](#)

4.1 Removing the Audit Vault Server Software

Before you can remove the Audit Vault Server software, you must stop all Oracle Audit Vault collection agents if the Oracle Audit Vault collection agent software is installed on the same system as the Audit Vault Server software. See *Oracle Audit Vault Collection Agent Installation Guide* for more information.

Use Oracle Universal Installer to remove Oracle Audit Vault Server software components from the inventory on the computer. Afterward, you need to manually remove the remaining components (see [Section 4.2](#)).

Do not delete Audit Vault Server home files or directories (for example, using Windows Explorer or the command prompt) without first using Oracle Universal Installer unless you exit Oracle Universal Installer during an installation. Otherwise, the components in the Audit Vault Server home remain registered in the Oracle Universal Installer inventory. If you manually delete Audit Vault Server home files and you attempt an installation in the same Oracle home, then some or all of the selected components may not be installed or properly configured.

Oracle Universal Installer does not register the installation in its inventory if the installation is unexpectedly interrupted. However, files may have been copied to your Oracle Audit Vault Server home. Remove these files manually and restart the installation.

Note: You can use Oracle Database Configuration Assistant to remove an Oracle Audit Vault instance and related services. For information about Oracle Database Configuration Assistant, see *Oracle Database 2 Day DBA* and see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows*.

Use the following procedure to uninstall the Audit Vault Server software.

1. Stop the Oracle Audit Vault Console using the `avctl stop_av` command.

For example:

```
$ avctl stop_av
```

In an Oracle RAC environment, run this command on all nodes where the Audit Vault Server is installed if you are removing Audit Vault Server from all nodes.

2. Start the Database Configuration Assistant to delete the Oracle Audit Vault database and then stop the listener.

Perform the following steps:

- a. Start the Database Configuration Assistant from the command-line.

```
$ dbca
```

The Welcome window appears.

- b. Click **Next**.

The Operations window appears.

- c. Select **Delete a Database**, then click **Next**.
- d. Select the Oracle Audit Vault database that you want to delete, then click **Finish**.
- e. In the window that appears, confirm that you want to delete the Oracle Audit Vault database.
- f. When the Database Configuration Assistant removes the Oracle Audit Vault database, you are prompted to choose whether you want to perform another operation. Click **No** to exit from the Database Configuration Assistant.

In an Oracle RAC environment, run the Database Configuration Assistant on all nodes where Oracle Audit Vault is installed if you are removing the Audit Vault Server from all nodes.

- g. Stop the listener.

Look in the `listener.ora` file to check the name of the listener. It might be `LISTENER1` or some other name, but usually it is `LISTENER`. For example:

```
$ lsnrctl stop listener-name
```

In an Oracle RAC environment, run this command on all nodes where Oracle Audit Vault is installed if you are removing the Audit Vault Server from all nodes.

3. Stop the Oracle Windows services before removing Oracle components or removing any registry entries.

See Also: Your Microsoft online help for more information about stopping services

To stop Windows services:

- a. Open the Windows **Services** utility: From the **Start** menu, choose **Programs**, then **Administrative Tools**, then **Services**.
- b. If the Oracle services named `OracleDBConsoleav`, `OracleJobSchedulerAV`, `OracleOraAV10g_home1TNSListener`, and `OracleServiceAV` exist and have the status *Started*, then select each service, and click **Stop**.
- c. Exit **Services**.

In an Oracle RAC environment, perform these operations on all the nodes where Audit Vault Server software is installed if you are removing Audit Vault Server software from all nodes.

4. Uninstall the Audit Vault Server software by running the following command in the home directory of Audit Vault Server. For example:

```
ORACLE_HOME\oui\bin\setup.exe
```

As an alternative, start Oracle Universal Installer. From the **Start** menu, select **Programs**, then **Oracle Server - HOME_NAME**, then **Oracle Installation Products**, and then **Universal Installer**. The Welcome window for Oracle Universal Installer appears.

5. Click **Deinstall Products** to bring up the Oracle Inventory screen.

Select the Oracle home directory and the products that you want to remove by selecting the desired check boxes, then click **Remove**. The **Confirmation** window appears. Click **Yes** to remove the selected components.

After the Oracle Audit Vault collection agent components are removed from your system, the Inventory window appears without the removed components. Click **Close** to close the **Inventory** window. Click **Cancel** to exit Oracle Universal Installer. Click **Yes** to confirm that you want to exit.

In an Oracle RAC environment, perform this operation on all the nodes where Audit Vault Server is installed if you are removing Audit Vault Server from all nodes.

6. Restart your computer.
7. Clean up the old Oracle directories.

On systems where Oracle Audit Vault Server is the only Oracle software installed, navigate to the directory for `oracle`, and remove the directory.

Otherwise, delete the Oracle Audit Vault Server home.

In an Oracle RAC environment, perform this operation on all the nodes where Audit Vault Server software is installed if you are removing Audit Vault Server software from all nodes.

Next, you must manually remove remaining registry keys, environment variables, Start menu options, and directories. See [Section 4.2](#) for details.

4.2 Manually Remove the Remaining Oracle Audit Vault Server Components

Oracle Universal Installer creates Windows services for Oracle Audit Vault Server components during installation but it does not delete all the services created by Oracle Net Configuration Assistant and Oracle Database Configuration Assistant during deinstallation. In addition, Oracle Universal Installer does not delete several other registry editor keys. You must remove any existing registry keys manually by following the instructions in one of the following sections:

- [Removing the Oracle Net Service Registry Key](#)
- [Removing All Oracle Audit Vault Server Registry Keys](#)
- [Updating the PATH Environment Variable Path](#)
- [Removing Oracle Audit Vault Server from the Start Menu](#)

- [Removing Oracle Audit Vault Server Directories](#)

Caution: Use Microsoft Registry Editor at your own risk. Incorrectly using the Registry Editor can cause serious problems and may require reinstallation of your operating system.

If you only had Oracle Audit Vault Server installed on the system and have no other Oracle databases installed on the same system, follow these steps as described in [Section 4.2.1](#) and [Section 4.2.2](#); otherwise, do not proceed with removing these registry entries.

4.2.1 Removing the Oracle Net Service Registry Key

To remove only the Oracle Net Service registry entry (if it exists):

1. Log in as a member of the Administrators group.
2. Ensure that you have stopped Oracle services by following the instructions in step 2 in [Section 4.1](#).
3. From a command prompt, enter the following command:

```
SYSTEM_DRIVE:\> regedit
```
4. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services and delete the `OracleAudit_Vault_HOME_NAME_TNSListener` registry entry. Oracle Universal Installer automatically deletes all other Oracle Net services.
5. Exit the Registry Editor.
6. Restart your computer.

4.2.2 Removing All Oracle Audit Vault Server Registry Keys

Caution: These instructions remove *all* Oracle Audit Vault Server components, services, and registry entries from your computer. Use extreme care when removing registry entries. Removing incorrect entries can break your system. Do not delete any database files under `ORACLE_BASE\ORACLE_HOME\DB_NAME` until you have completed these instructions.

To remove all Oracle Audit Vault Server registry keys from a computer:

1. Log in as a member of the Administrators group.
2. Make sure that you have stopped Oracle Audit Vault Server services by following the instructions in step 2 in [Section 4.1](#).
3. Start the Registry Editor at the command prompt:

```
SYSTEM_DRIVE:\> regedit
```
4. Go to HKEY_CLASSES_ROOT.
5. Delete keys that begin with `Ora`, `Oracle`, `Orcl`, or `EnumOra`.

This collection of keys includes those that begin with the following:

- `EnumOraHomes`

- OracleConfig
 - OracleDatabase
 - OracleHome
 - OracleInProcServer
 - OracleProcess
 - ORADC
 - ORAMMCCFG10
 - ORAMMCPMON10
 - OraOLEDB
 - OraPerfMon
 - ORCLMMC
 - ORCLSSO
 - ORG10SVR
6. Go to HKEY_CURRENT_USER.
 7. Delete the ORACLE key.
 8. Go to HKEY_CURRENT_USER\Software.
 9. Delete all Oracle keys, including *Oracle-Audit_Vault_Server_HOME_NAME* entries under:
Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu\Programs.
 10. Go to HKEY_LOCAL_MACHINE\SOFTWARE and search for the ORACLE group key.
Select ORACLE and note the value of the *inst_loc* key. This is the location of Oracle Universal Installer. The default location is *c:\Program Files\Oracle\Inventory*. If this value is different, make a note of it so that you can delete it later.
 11. Delete the ORACLE Group key.
 12. Go to HKEY_LOCAL_MACHINE\SOFTWARE\ODBC.
 13. Expand all the subkeys under ODBC and remove any Oracle-related ODBC driver keys, except for the Microsoft ODBC for Oracle key.
For example, the ODBC\ODBCINST.INI directory lists keys for each Oracle home. For example, delete *Oracle in Audit_Vault_Server_Home_Name*, such as *Oracle in OraAV10g_home1*.
 14. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services.
 15. Delete all keys under this branch that begin with Oracle or OraWeb. For example, delete the *OracleDBConsoleav*, *OracleJobSchedulerAV*, and *OracleServiceAV* registry entries.
 16. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application.
 17. Delete all keys under this branch that begin with Oracle. For example, delete *Oracle.av* and *OracleDBConsoleav* registry entries.
 18. Exit the Registry Editor.

19. Restart your computer.

Oracle Universal Installer does not remove all Audit Vault Server components. After using Oracle Universal Installer to remove Audit Vault Server components, you must manually remove the remaining registry keys, environment variables, Start menu options, and directories.

Note: In rare situations, you might want to correct serious system problems by completely removing Audit Vault Server components manually from the computer without first deinstalling with Oracle Universal Installer. Do this only as a last resort, and only if you want to remove all Audit Vault Server components from your system.

4.2.3 Updating the PATH Environment Variable Path

Check the `PATH` environment variable and remove any Oracle entries.

1. Display **System** in the Control Panel.
2. Select the **Advanced** tab and then click **Environment Variables**.
3. Select the system variable `PATH` and edit it to remove any Oracle entries.

For example, remove Oracle entries that contain `ORACLE_BASE\ORACLE_HOME` in the `Path` variable. You may see a `Path` variable that contains entries similar to the following:

```
ORACLE_BASE\ORACLE_HOME\product\10.2.2\av_1\bin
```

4. Save any changes and exit **System**.

4.2.4 Removing Oracle Audit Vault Server from the Start Menu

Check the **Start** menu for any Oracle Audit Vault collection agent entries and remove them.

Follow these steps:

1. Select **Start**, then **Programs**, then **Oracle - Server HOME_NAME**. For example, **Oracle - OraAV10g_home1**.
2. Right-click **Oracle - Server HOME_NAME**, and from the menu, select **Delete**.

You can also remove Oracle Audit Vault Server menu entries by using the following method:

1. Right click the **Start** button to display the pop-up menu.
2. Select the **Explore All Users** option.
3. Under Documents and Settings, expand the `\Start Menu\Programs` folder.
4. Right-click and delete the **Oracle - Server HOME_NAME** folder. For example, delete the **Oracle - OraAV10g_home1** folder.

4.2.5 Removing Oracle Audit Vault Server Directories

After removing all Audit Vault Server registry keys and restarting the computer, delete any existing Audit Vault Server directories and files.

1. Using My Computer or Windows Explorer, delete the `SYSTEM_DRIVE:\program files\oracle` directory.

2. Using My Computer or Windows Explorer, delete the Oracle Audit Vault *ORACLE_BASE* directory on your hard drive.

Index

A

aliases
 multiple on computers, 2-6
automatic storage management (ASM), 3-16

C

certification, hardware and software, 1-3
Cluster Verification Utility
 verifying readiness for database installation, 3-4
components
 removing database, Oracle Internet Directory, and
 Net Services services and registry entries, 4-3
 removing manually, 4-4
computers with multiple aliases, 2-6
critical patch updates for Oracle Audit Vault
 downloading, 3-18

D

data files
 recommendations for file system, 2-7
databases
 removing, 4-1 to 4-7
deinstalling. *See* removing
DHCP computers, installing on, 2-5
directories
 database file, 2-7
directories, removing Oracle Audit Vault Server, 4-6
disabling remote SYSDBA connections, 3-20
downloading Oracle Audit Vault critical patch
 updates, 3-18
downloading Oracle Audit Vault patches, 3-18
dynamic host configuration protocol
 See DHCP

E

enabling remote SYSDBA connections, 3-20
environment variables
 ORACLE_HOSTNAME, 2-6
 PATH, 4-6

F

file system

 using for data files, 2-7
Firefox Web browser, 2-5

H

hardware and software certifications, 1-3
hardware certification, 1-3
host name
 setting before installation, 2-6

I

installation
 computer aliases, multiple, 2-6
 non-interactive, 3-9
IP addresses, multiple, 2-6

M

Microsoft Internet Explorer, 2-5
Microsoft Registry Editor. *See* Registry Editor
Mozilla Web browser, 2-5
multihomed computers, installing on, 2-6
multiple aliases, computers with, 2-6
multiple Oracle homes, 1-3
 setting, 2-6

N

Net Services, removing, 4-3
Netscape Navigator, 2-5
network cards, multiple, 2-6
network setup
 about, 2-5
 computers with multiple aliases, 2-6
network topics
 DHCP computers, 2-5
 multiple network cards, 2-6

O

Oracle Audit Vault Agent
 removing, 4-6 to 4-7
Oracle Audit Vault Server directories, removing, 4-6
Oracle Audit Vault Server Service
 removing Registry Editor key, 4-4

- Oracle Database
 - Windows Terminal Services support, 2-5
- Oracle Database Vault roles
 - generating, 3-12
- Oracle home directory, 1-3
 - multiple homes
 - network considerations, 2-6
- Oracle homes, multiple, 1-3
- Oracle host name, setting before installation, 2-6
- Oracle Internet Directory
 - removing, 4-3
- ORACLE_HOSTNAME environment variable
 - about, 2-6
 - computers multiple homes, 2-6
 - computers with multiple aliases, 2-6
 - setting before installation, 2-6

P

- patches for Oracle Audit Vault
 - downloading, 3-18
- PATH environmental variable
 - removing Oracle Audit Vault Server entries, 4-6

R

- RAID
 - using for Oracle data files, 2-7
- raw devices, 3-16
- redundant array of independent disks
 - See* RAID
- Registry Editor
 - removing Oracle Audit Vault Server service
 - key, 4-4
- registry, care needed when using, 4-4
- remote SYSDBA connections
 - disabling, 3-20
 - enabling, 3-20
- removing
 - database, Oracle Internet Directory, and Net Services services and registry entries, 4-3
 - Oracle Audit Vault Agent components
 - manually, 4-6 to 4-7
 - Oracle Audit Vault Agent, overall
 - procedure, 4-6 to 4-7
 - Oracle Audit Vault Server directories, 4-6
 - Oracle Audit Vault Server Services Registry Editor
 - key, 4-4
 - Oracle components manually, 4-4
 - Oracle databases, 4-1 to 4-7
 - Oracle Registry Editor keys, 4-3, 4-4
 - Oracle software, 4-1 to 4-7
 - Registry Editor keys, 4-3, 4-4
 - Start menu Oracle Audit Vault Server entries, 4-6
- removing Oracle Audit Vault Server
 - Oracle Audit Vault Server from PATH
 - environment variable, 4-6
- removing, Oracle Software, 4-1
- requirements
 - Web browser support, 2-5

- Windows Remote Desktop Connection
 - support, 2-5
- Windows Terminal Services, 2-5

S

- Safari Web browser, 2-5
- silent installation, 3-9
- software and hardware certifications, 1-3
- software certification, 1-3
- software, removing, 4-1 to 4-7
- Start menu, removing Oracle Audit Vault Server
 - entries, 4-6

U

- unsupported components
 - on Windows Terminal Services, 2-5

W

- Web browser support, 2-5
- Web browsers
 - Firefox, 2-5
 - Microsoft Internet Explorer, 2-5
 - Mozilla, 2-5
 - Netscape Navigator, 2-5
 - Safari, 2-5
- Windows Terminal Services
 - support, 2-5
 - unsupported components, 2-5