Oracle® Audit Vault

Server Installation Guide

10*g* Release 2 (10.2.2.1) for Microsoft Windows (32-Bit)

E10252-01

August 2007

ORACLE®

Oracle Audit Vault Server Installation Guide, 10*g* Release 2 (10.2.2.1) for Microsoft Windows (32-Bit)

E10252-01

Contents

1 Overview of Oracle Audit Vault Server Installation

2 Oracle Audit Vault Server Preinstallation Requirements

3 Installing the Oracle Audit Vault Server

4   Removing Audit Vault Server Software

Index

List of Tables

Preface

Oracle Audit Vault Server Installation Guide for Microsoft Windows (32-Bit) explains how to prepare for, install, and configure Oracle 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 as well as 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, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following documents:

- *Oracle Audit Vault Release Notes*

- *Oracle Audit Vault 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 (32-Bit)*

- *Oracle Database Platform Guide for Microsoft Windows (32-Bit)*

- *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 (32-Bit)*

- *Oracle Database Vault Administrator's Guide*

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview of Oracle Audit Vault 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 installation process. This chapter includes the following sections:

- Audit Vault Installation Components
- Audit Vault Installation Methods
- Audit Vault Server Installation
- Installation Considerations

1.1 Audit Vault Installation Components

Oracle Audit Vault 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 Agent installation (see *Oracle Audit Vault Agent Installation Guide*)

1.2 Audit Vault Installation Methods

You can choose different installation methods to install Oracle 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, Oracle Universal Installer displays a series of screens that enable you to specify all of the required information to install the Oracle Audit Vault software.

1.2.2 Automated Installation Methods Using Response Files

Oracle Audit Vault provides a response file template for Audit Vault Server (`av.rsp`). The response template file 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 3.6 for information about performing an 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 Audit Vault Server Installation

The Audit Vault server installation consists of two 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.

The Audit Vault Console uses a wallet in the `ORACLE_HOME\network\admin\avwallet` directory. An Oracle wallet is a password-protected container that stores credentials, such as certificates, authentication credentials, and private keys, all of which are used by Secure Sockets Layer (SSL) for strong authentication. Oracle wallets are managed through Oracle Wallet Manager. Oracle Wallet Manager can perform tasks such as creating wallets, requesting certificate generation, and importing certificates into the wallet.

The wallet is used to store the user name and password of the user granted the `AV_ADMIN` role. This user name is used by the Audit Vault Console to allow communication with Oracle Audit Vault. The Audit Vault Console provides the management service that initiates the communication with agents using HTTP. The

Audit Vault Configuration Assistant (AVCA) modifies the Oracle Enterprise Manager Database Control console `server.xml` file and other related files to enable Audit Vault management through the Audit Vault Console.

If certificate-based authentication is used for communication with any agent, the Audit Vault administrator must acquire the necessary server-side certificates and set up Oracle Wallet for storing the certificates on the server. This server-side certificate is used for authenticating the Audit Vault Server to the agent. Similarly, agents must each have a certificate to authenticate each agent to the Audit Vault Server.

Communication at the management level between the Audit Vault Server and the Audit Vault Agent can be secured after the installation is complete. This is done as part of the postinstallation configuration, in which SSL is configured for the mutual authentication between the Audit Vault management service on the server side and each 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 AVCA.

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 Oracle*MetaLink* Web site for the most up-to-date list of certified hardware platforms and operating system versions. The Oracle*MetaLink* Web site is available at

`https://metalink.oracle.com`

If you do not have a current Oracle Support Services contract, then you can access the same information at

`http://www.oracle.com/technology/support/metalink/content.html`

1.4.2 Multiple Oracle Homes

This product supports multiple Oracle homes. This means that you can install this release of the software more than once on the same system, in different Oracle home directories See Section 2.5.2 for more information.

2

Oracle Audit Vault Server Preinstallation Requirements

This chapter describes the following Oracle Audit Vault Server preinstallation requirements. This chapter includes the following sections:

- Becoming Familiar with the Features of Oracle Audit Vault
- Checking the Hardware Requirements
- Checking the Operating System Requirements
- Reviewing Oracle Audit Vault Agent Hardware and Software Certification
- Checking the Network Setup
- Creating Directories for Oracle Audit Vault Database Files
- Setting the System Time Zone to GMT 00:00

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 Checking the Hardware 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)	512 MB
Virtual memory	Double the amount of RAM
Hard disk space	2.02 GB Total See Table 2–2 for details.
Video adapter	256 colors
Processor	550 MHz minimum

2.2.1 Hard Disk Space Requirements

This section lists system requirements for Windows platforms that use the NT File System (NTFS) file systems. FAT32 space requirements are slightly larger. 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 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 Client components include space 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, then 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
44 MB	0.976 GB	1.0 GB	2.02 GB

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

The 0.976 GB of disk space for the Oracle home is the disk space for the Oracle Audit Vault Server software files in the Oracle Base. The TEMP space required is 44 MB.

The 1.0 GB of disk space for the 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 1.0 GB disk space is only the starting size. The Audit Vault administrator must take future growth of the database size into consideration, especially as the server collects more and more audit data.

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

1. Determine the physical RAM size. For a computer using Windows 2003, for example, open **System** in the Windows Control Panel and select the **General** tab. 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). For a computer using Windows 2003, for example, open **System** in the Control Panel, select the **Advanced** tab, and click **Settings** in the **Performance** section. Then select the **Advanced** tab. 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. For a computer using Windows 2003, for example, open **My Computer**, right-click the drive where the Oracle software is to be installed, and choose **Properties**.

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 will be needed 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. For a computer using Windows 2003, for example, open **System** in the Control Panel, select the **Advanced** tab, and click **Environment Variables**.

2.3 Checking the Operating System Requirements

Table 2–3 lists the software requirements for Oracle 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: Intel (x86)
	For additional information, visit Oracle Metalink at:
	https://metalink.oracle.com
Operating System	Oracle Audit Vault Agent for Windows is supported on the following operating systems:
	■ Windows 2000 with service pack 1 or later. All editions, including Terminal Services and Microsoft Windows 2000 MultiLanguage Edition (MLE), are supported.
	■ Windows Server 2003 – all editions
	■ Windows Server 2003 R2 – all editions except Express edition
	■ Windows XP Professional (single instance only)
	Windows NT is not supported.
	Windows Multilingual User Interface Pack is supported on Windows XP Professional, and Windows Server 2003.
Network protocol	The Oracle Net foundation layer uses Oracle protocol support to communicate with the following industry-standard network protocols:
	■ TCP/IP
	■ TCP/IP with SSL
	■ Named Pipes

2.4 Reviewing Oracle Audit Vault Agent 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 Oracle*MetaLink* Web site for the most up-to-date list of certified hardware platforms and operating system versions. This Web site also provides compatible client an database versions, patches, and workaround information for bugs. The Oracle*MetaLink* Web site is available at the following URL:

https://metalink.oracle.com/

You must register online before using Oracle*MetaLink*. After logging in, select **Certify & Availability** from the left-hand column. From the Product Lifecycle page, select the **Certifications** button. Other Product Lifecycle options include **Product Availability**, **Desupport Notices**, and **Alerts**.

The following sections provide certification information:

- Windows Telnet Services Support
- Windows Terminal Services and Remote Desktop Support
- Windows Support
- Web Browser Support

2.4.1 Windows Telnet Services Support

Windows 2000, Windows 2003, and Windows XP include a Telnet Service that allows remote users to log on to the operating system and run console programs using the command line. Oracle supports database command line utilities such as `sqlplus`, `sqlldr`, `import`, and `export` using this feature, but does not support the database GUI tools such as Oracle Universal Installer, Database Configuration Assistant, and Oracle Net Configuration Assistant.

> **Note:** Ensure that the Telnet service is started on the Windows **Services** utility.

2.4.2 Windows Terminal Services and Remote Desktop Support

Oracle supports installing, configuring, and running Oracle Database through Terminal Services on Windows 2000, Windows 2003, and Windows XP. 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`).

Platform-specific support information is as follows:

- **Windows 2000**: Oracle supports installing, configuring, and running Oracle Database from a remote Terminal Services Client.

- **Windows 2003**: You can configure Windows 2003 to use Terminal Services in Remote Desktop for Administration Mode or Terminal Server Mode.

- **Windows XP**: The Remote Desktop is only available in Single User Mode.

> **See Also:**
>
> - The Microsoft Web site for more information about terminal services
>
>   http://www.microsoft.com/
>
> - The Oracle*MetaLink* Web site for the latest Terminal Server certification information
>
>   https://metalink.oracle.com/

2.4.3 Windows Support

The following components are not supported on Windows XP:

- DCE Adapter Support

- Entrust PKI Support

- Generic Connectivity

- Oracle Messaging Gateway

- Oracle Real Application Clusters, including Cluster File System and Server Management

- Oracle Clusterware

- nCipher Accelerator Support

- Oracle Fail Safe Server.

2.4.4 Web Browser Support

The following Web browsers are supported for *i*SQL*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

2.5 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 Computers with Multiple Homes

- Installing on Computers with Multiple Aliases

2.5.1 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.

Audit Vault Server cannot be installed in an environment where the IP addresses of the Audit Vault Server or the Audit Vault Agent can change. If your environment uses DHCP, ensure that all Audit Vault systems use static IP addresses.

2.5.2 Installing on Computers with Multiple Homes

You can install Oracle Audit Vault on a computer that has multiple homes. A multiple-homed computer is associated with multiple IP addresses. This is typically achieved by having multiple network cards on the computer. 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` on Windows 2003 and Windows XP, or on Windows 2000 *SYSTEM_DRIVE:*`\WINNIT\system32\drivers\etc`.

Clients must be able to access the computer either by using this host name or by using aliases for this host name. To verify this, 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 tests must be successful.

Setting the ORACLE_HOSTNAME Environment Variable

To set the `ORACLE_HOSTNAME` environment variable:

1. Display **System** in the Windows Control Panel.

2. In the System Properties dialog box, click **Advanced**.

3. In the **Advanced** tab, click **Environment Variables**.

4. In the Environment Variables dialog box, under System Variables, click **New**.

5. 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.

6. Click **OK**, then in the Environment Variables dialog box, click **OK**.

7. Click **OK** in the Environment Variables dialog box, then in the System Properties dialog box, click **OK**.

2.5.3 Installing on Computers with Multiple Aliases

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

2.6 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.

2.7 Setting the System Time Zone to GMT 00:00

Before installing Oracle Audit Vault Server on Windows (32-bit), you must make sure the system time zone is set with its original value of GMT 00:00. Setting the time zone to its original value will allow Oracle Universal Installer to automatically set the agentTZRegion property in the emd.properties file to its correct timezone value for the geographical location of the system during the installation. This will then allow the Audit Vault Console to show correct data on the **Overview** page. To perform this task, follow this procedure:

1. Change the Windows system time to GMT 00:00 using the **Control Panel** -> **Date and Time** -> **Time Zone tab** -> select the **(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London** option, click **Apply**, then click **OK**.

2. Install Oracle Audit Vault Server.

> **Note:** If Oracle Enterprise Manager has an issue with the time zone, then see Section 10.1.5 "Setting the Management Agent Time Zone" in *Oracle Enterprise Manager Advanced Configuration* as a workaround. After performing the Oracle Enterprise Manager workaround, restart Oracle Enterprise Manager.

3

Installing the Oracle Audit Vault Server

This chapter includes an overview of the major steps required to install single instance Oracle Audit Vault Server and to install Oracle Audit Vault Server with Oracle Real Application Clusters (Oracle RAC).

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 on digital video disk (DVD).

3.2 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 two options:

- **Basic Installation** – Simplifies the installation process and prompts for a minimal set of inputs, including the name of the Audit Vault database, the 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.

3.2.1 Basic and Advanced Installation Details Screens

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

3.2.1.1 Audit Vault Name

The Audit Vault Name must be a unique name for the 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 Audit Vault name cannot contain any of the characters shown in Table 3–1.

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

Symbol	Character Name
_	Underscore
$	Dollar sign
	Space character

3.2.1.2 Audit Vault Home

The Audit Vault Home is the path that you must specify or browse to find the Audit Vault home where you want to install Oracle Audit Vault. 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 Home Name

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

3.2.1.3 Audit Vault Server Accounts

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

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

Audit Vault Administrator and Audit Vault Auditor Accounts

The 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 manages the audit service including source creation and parameters, and sources and their channels. This role registers audit sources, defines plug-ins for translation, and manages central audit settings. For the

basic installation, the Audit Vault Administrator user name is used to generate the following Oracle Database Vault roles to facilitate the separation of duties:

- *AV_ADMIN*dvo – The Database Vault Owner (granted DV_OWNER role) to manage Database Vault roles and configuration

- *AV_ADMIN*dva – The 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 Database Vault Owner account name and password and a separate, optional Database Vault Account Manager account name and password.

The Audit Vault Auditor account is granted the AV_AUDITOR role. The user granted the AV_AUDITOR role accesses 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 has the ability to configure parameters that assist in populating the Audit Vault data warehouse. 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 Audit Vault Administrator, Audit Vault Auditor, Database Vault Owner, and Database Vault Account Manager user names must not be the same. For the basic installation, the 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 Audit Vault Administrator user name must be between 2 and 30 characters.

The length of the 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
DVSYS	EJBCLIENT	ELSE	EXCLUSIVE	EXECUTE_CATALOG_ROLE
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

Names	Names	Names	Names	Names
JAVA_ADMIN	JAVADEBUGPRIV	JAVA_DEPLOY	JAVAIDPRIV	JAVASYSPRIV
JAVAUSERPRIV	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	TSMSYS	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.

Audit Vault Administrator and Audit Vault Auditor Passwords

For the basic installation, the Audit Vault Administrator password entered for the Audit Vault Administrator account is also used for the standard database accounts (sys, system, sysman, dbsnmp). For the basic installation **Details** page, the 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, dbsnmp) or select to use the same password as the Audit Vault Administrator for all of these accounts. In addition, a **Database Vault User Credentials** page prompts for the Database Vault Owner user password and for a separate, optional Database Vault Account Manager user password if that user is created.

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

3.2.2 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 Database Vault Owner account and the separate, optional Database Vault Account Manager account. You must supply an account name and password for the Database Vault Owner account, and optionally for the Database Vault Account Manager account during installation.

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

3.2.2.1 Database Vault Owner and Database Vault Account Manager Accounts

The Database Vault Owner, Database Vault Account Manager, Audit Vault Administrator, and Audit Vault Auditor account names must be different from each other (applicable when a separate Audit Vault Auditor or Database Vault Account Manager account is created). The 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 3.2.1.3.

Each account name cannot contain any of the characters shown in Table 3–1.

3.2.2.2 Database Vault Owner and Database Vault Account Manager Passwords

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

There must be no repeating characters in each password. There must be no 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.

3.2.3 Advanced Server Installation: Node Selection Screen

The **Node Selection** screen will appear when you install Oracle Audit Vault in an Oracle RAC environment. On this screen, users can select the nodes on which they want to install Oracle Audit Vault, or they can select a local installation to install Oracle Audit Vault single instance.

3.2.4 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 10.2.0.3 ASM instance must be installed in order to select the ASM option for database storage.

ASM can be used with a single instance Audit Vault installation, multiple Audit Vault installations, and in an Oracle Real Application Clusters (Oracle RAC) environment. ASM manages the storage of all 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.

3.2.5 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*.

3.2.6 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**.

3.2.7 Default Audit Policy and Initialization Parameters

Oracle Audit Vault installs a baseline database auditing policy. This policy covers the access control configuration information stored in Audit Vault database tables, information stored in Oracle Catalog (rollback segments, tablespaces, and so on), the use of system privileges, and Oracle Label Security configuration.

> **See Also:** *Oracle Audit Vault Auditor's Guide* for more information about the database audit policy.

When you install Oracle Database Vault, the security-specific, database initialization parameters are initialized with default values. See the "Initialization Parameters" appendix in *Oracle Database Vault Installation Guide for Microsoft Windows (32-Bit)* for more information.

3.3 Basic Installation – Performing the Single Instance Server Installation

To perform Audit Vault Server single instance basic installation:

1. 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.

2. 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
```

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

4. Enter the following information on the **Basic Installation Details** page. See Section 3.2 for more information about each of these topics.

a. **Audit Vault Name** – A unique name for the Audit Vault database. The 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 Audit Vault Home where you want to install Oracle Audit Vault.

c. **Audit Vault Administrator** and **Audit Vault Auditor** – The account name of the Audit Vault Administrator and a separate, optional Audit Vault Auditor, respectively. The Audit Vault administrator and Audit Vault auditor account names must not be the same. The Audit Vault Administrator account name is required. Accept the selected **Create a Separate Audit Vault Auditor** check box to choose to create the Audit Vault Auditor account name. The check box is selected by default. Deselecting the check box disables the text fields for the Audit Vault Auditor user name and password. The Audit Vault Administrator in this case will also be granted the role of Audit Vault Auditor.

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

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

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

d. **Administrator Password** and **Auditor Password** – The password for the Audit Vault administrator account and the 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 Audit Vault administrator account will also be used for the standard database accounts (`sys`, `system`, `sysman`, `dbsnmp`).

The Audit Vault administrator password will also be used for the Oracle Database Vault roles (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 Audit Vault Administrator account and the Audit Vault auditor account, respectively.

Each password must be identical to its corresponding password confirmation.

After entering the required information, 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 is done on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

5. Review the installation prerequisite checks on the **Prerequisite Check** 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.

6. Review the installation summary information on the **Basic Installation Summary** page. After reviewing this installation information, click **Install** to begin the installation procedure.

7. 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 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 `cfgtoollogs/oui` directory, in the following location:

   `ORACLE_HOME/cfgtoollogs/oui/installActionsdate_time.log`

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

3.4 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 Oracle Audit Vault in an Oracle RAC environment.

This section describes the remaining installation procedures for installing Oracle Audit Vault with Oracle Real Application Clusters (Oracle RAC).

Verifying System Readiness for Installing Oracle Audit Vault with CVU

To help to verify that your system is prepared to install Oracle Audit Vault with Oracle RAC successfully, use the Cluster Verification Utility (CVU) `runcluvfy` 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.

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

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

Perform the following procedures to install Oracle Audit Vault.

1. Run Oracle Universal Installer (OUI) to install Oracle Audit Vault.

   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

2. 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
   ```

3. In the Welcome window, on the **Select Installation Type** screen, select the **Advanced Installation** option, then click **Next**.

4. Enter the following information on the **Advanced Installation Details** screen. See Section 3.2 for more information about each of these topics.

   a. **Audit Vault Name** – A unique name for the Audit Vault database. The 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 Audit Vault home where you want to install Oracle Audit Vault.

   c. **Audit Vault Administrator** and **Audit Vault Auditor** – The account name of the Audit Vault Administrator and a separate, optional Audit Vault Auditor, respectively. The Audit Vault Administrator and Audit Vault Auditor account names cannot be the same. The Audit Vault administrator account name is required. Accept the selected **Create a Separate Audit Vault Auditor** check box to choose to create the Audit Vault auditor account name. The check box is selected by default. Deselecting the check box disables the text fields for the Audit Vault auditor user name and password. The Audit Vault administrator in this case will also be granted the role of Audit Vault Auditor.

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

      Each password must be identical to its corresponding password confirmation.

After entering the required information, 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 is done on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

5. Enter the following information on the **Database Vault User Credentials** screen. See Section 3.2.2 for more information about each of these topics.

   a. **Database Vault Owner** and **Database Vault Account Manager** – The account name of the Database Vault Owner and a separate, optional Database Vault Account Manager, respectively. The Database Vault Owner, Database Vault Account Manager, Audit Vault Administrator, and Audit Vault Auditor account names must not be the same (applicable when a separate Audit Vault Auditor or Database Vault Account Manager account is created). The Database Vault Owner name is required. Accept the selected **Create a Separate Database Vault Account Manager** check box to choose to create the Database Vault Account Manager account name. The check box is selected by default. Deselecting the check box disables the text fields for the Database Vault Account Manager user name and password. The 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.

   After entering the required information, 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 is done on all user input after you click **Next**. The installation process will not continue until all required input passes validation.

6. 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 will be installed. Local node will always be selected by default. If you are installing Audit Vault 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 will be installed, then click **Next**.

7. Review the installation prerequisite checks on the **Prerequisite Check** 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.

8. On the **Specify Database Storage Options** screen, you can 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**.

9. On the **Specify Backup and Recovery Options** page, you can 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 you must 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 10). 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, you can 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**.

10. On the **Specify Database Schema Passwords** screen, you can 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**.

11. Review the installation summary information on the **Advanced Installation Summary** screen. After reviewing this installation information, click **Install** to begin the installation procedure.

12. 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 `cfgtoollogs\oui` directory in the following location:

SYSTEM_DRIVE:`\> `*ORACLE_HOME*`\cfgtoollogs\oui\installActions`*date_time*`.log`

> **Note:** The Oracle home name and path that you provide during
> database installation *must be different* from the home that you used
> during the Oracle Clusterware installation. You **cannot** install
> Oracle Audit Vault 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)

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

After you have completed this part of the installation, proceed to Section 3.7 to
perform the postinstallation tasks.

3.6 Performing a Silent Installation Using a Response File

> **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. Make sure all prerequisites are met for the installation of Audit Vault Server and
    Audit Vault Agent.

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*.

3.7 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 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 Audit Vault home is not supported.

This section includes the following topics:

- Unlocking and Resetting User Passwords
- Running DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC only)
- Logging In to Audit Vault Console

3.7.1 Unlocking and Resetting User Passwords

The password entered for the Audit Vault Administrator is used as the password for core database accounts such as `SYS`, `SYSTEM`, `SYSMAN`, and `DBSNMP` in a basic installation. For an advanced installation, the user is given the option of changing the password for each of these accounts.

For a basic installation, the same Audit Vault administrator password is also used for the `<AV_ADMIN>dvo` account, the Database Vault Owner (granted `DV_OWNER` role), to manage Database Vault roles and configuration; and the `<AV_ADMIN>dva` account, the 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, the Database Vault Owner user password and the separate, optional Database Vault Account Manager user password are entered for these users. You must change these passwords according to your company policies.

3.7.1.1 Using SQL*Plus to Unlock Accounts and Reset Passwords

To unlock and reset user account passwords using SQL*Plus:

1. Start SQL*Plus and log in as <AV_ADMIN>dva account.

2. Enter a command similar to the following, where `account` is the user account that you want to unlock and `password` is the new password:

    ```
    SQL> ALTER USER account [ IDENTIFIED BY password ] ACCOUNT UNLOCK;
    ```

    In this example:

    - The `ACCOUNT UNLOCK` clause unlocks the account.

    - The `IDENTIFED BY` password clause resets the password.

    > **Note:**   If you unlock an account but do not reset the password, then the password remains expired. The first time someone connects as that user, they must change the password.
    >
    > To permit unauthenticated access to your data through HTTP, unlock the ANONYMOUS user account.

    > **See Also:**   *Oracle Database Administrator's Guide* for more information about:
    >
    > - Unlocking and changing passwords after installation
    >
    > - Oracle security procedures
    >
    > - Best security practices

3.7.2 Running DVCA to Set Instance Parameters and Lock Out SYSDBA Sessions (Oracle RAC only)

After installing Audit Vault for a Oracle Real Application Clusters (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 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 Oracle Audit Vault 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"
```

3.7.3 Logging In to Audit Vault Console

To use the Audit Vault Console, you must access it on the node where you installed the Audit Vault database. If you want to log in to the Audit Vault Console from another cluster node, then you must reconfigure Enterprise Manager to start the Audit Vault Console interface on that other node.

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

1. On the node from which you installed the database, open a Web browser to access the 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 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 Audit Vault Console URL.

    b. On any system, enter this URL in a Web browser and Oracle Enterprise Manager will display the Audit Vault Console login page.

2. Log in to the Audit Vault Console using the user name <AV_ADMIN> and the <AV_ADMIN> password that you created during the installation to configure and manage Audit Vault.

Log in to Audit Vault Console using the user name <AV_AUDITOR> and the <AV_AUDITOR> password you created during the installation to view activity and alert reports and manage audit policies.

4

Removing Audit Vault Server Software

This chapter describes the process of removing the 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

To remove the Audit Vault Server software, all Audit Vault Agents must be stopped if the Audit Vault Agent software is installed on the same system as the Audit Vault Server software. See *Oracle Audit Vault 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 Oracle 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 Oracle Audit Vault Sever home remain registered in the Oracle Universal Installer inventory. If you manually delete Oracle 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 Audit Vault instance and related services. For information about Oracle Database Configuration Assistant, see the chapter "Installing Oracle and Building the Database" in *Oracle Database 2 Day DBA* and see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*.

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

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

   This command performs an emctl stop dbconsole operation. For example:

   ```
   $ avctl stop_av
   ```

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

2. Log in to the Audit Vault database and shut it down, as follows:

```
sqlplus /nolog
SQL> connect sys as sysoper
Enter password: <sysoperpassword>
Connected.
SQL> shutdown immediate;
SQL> exit
```

In an Oracle RAC environment, run the following command from any node where Audit Vault Server is installed:

```
ORACLE_HOME\bin\srvctl stop database -d <AV database name> -q
SQL> Connect String: sys as sysdba
Enter password: <sysdbapassword>
```

3. 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 that command on all nodes where Audit Vault is installed if you are removing the Audit Vault Server from all nodes.

4. 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` exists and has 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.

5. 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.

6. 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 Audit Vault 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 is installed if you are removing Audit Vault Server from all nodes.

7. Restart your computer.

8. 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 need to 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 need to 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.

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. Make sure 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 Oracle*Audit_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 Oracle Audit Vault Server components. After using Oracle Universal Installer to remove Oracle Audit Vault Server components, you need to 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 Oracle 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 Oracle 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 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 Oracle Audit Vault Server registry keys and restarting the computer, delete any existing Oracle 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