Oracle Database Audit Vault

Author	이규열
Creation Date	2011.5.26
Last Updated	
Version	1.0

Version	변경일자	변경자(작성자)	주요내용
1			
2			
3			

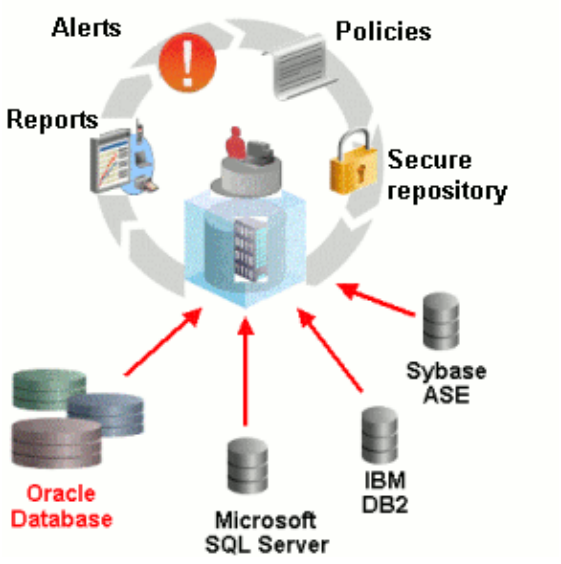
Goodus
Breathing Life into Technology

Contents

1. Introduction to Oracle Audit Vault

Oracle Audit Vault 는 다양한 데이터베이스들로부터 감사의 기초 정보를 수집해 통합 감사 정보를 구축함으로 관리의 편의성과 성능을 극대화 하며 다양한 보고서를 제공하고, 보안 위험에 대한 경고를 실시간으로 발생시킬 수 있는 강력한 보안 감사 관리 제품입니다.

1.1. Overview of Oracle Audit Vault



Oracle Audit Vault 를 사용함으로써 많은 장점들을 얻을 수 있습니다.

Oracle Audit Vault 는 중앙집중 통합 감사 솔루션으로 Oracle 은 물론 DB2, MS SQL, Sybase 등과 같은 다양한 데이터베이스를 지원하기 때문에 기업 환경에서 발생할 수 있는 다양한 감사 정보를 효율적으로 관리 할 수 있도록 도와 줍니다.

별도의 BI 툴과 연계해서 분석적인 정보를 추출 할 수 있으며 웹 기반의 콘솔화면을 제공하여 실시간으로 감사상황을 모니터링 하며 쉽게 리포트를 제공해 줍니다.

또한 시스템 운영에서 보안 관리자의 가장 큰 고민은 감사 정보의 대용량입니다. 이를 위해 감사 기초발생을 최소화하기 위한 기능인 FGA(Fine Grained Auditing) 기술을 제공 하며 별도의 서버에 구축되므로 수집된 이후에 감사 데이터 관리와 감사 데이터 관련 작업으로 인한 오버헤드를 줄 일 수 있습니다.

1.2. Why Use Oracle Audit Vault?

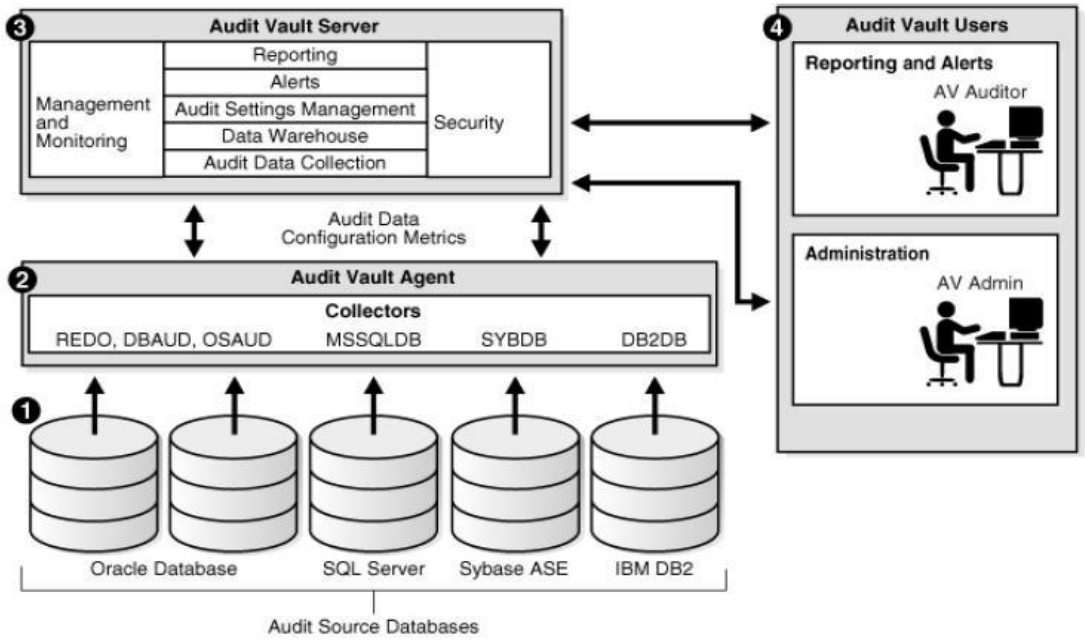
Sarbanes-Oxley 등의 법규를 준수하고 내부자 위협에 관련한 리스크를 경감하는 것은 오늘날의 기업이 당면한 가장 중요한 보안 문제의 하나입니다.

Oracle Audit Vault 는 감사 데이터를 핵심 보안 리소스로 활용함으로써 오늘날 기업의 보안, 컴플라이언스 문제를 해결할 수 있도록 지원합니다.

오늘날 감사 데이터를 보안 리소스로 활용하려면 많은 수작업 프로세스가 요구됩니다. IT 보안/감사 담당자가 데이터를 직접 수집하고 커스텀 스크립트 등을 이용하여 여러 서버에 분산되어 저장된 엄청난 양의 데이터를 처리해야 합니다. Oracle Audit Vault 는 감사 데이터의 수집, 분석 프로세스를 자동화 함으로써 기업에 신뢰와, 검증성 원칙을 투명하게 실현할 수 있게 합니다.

1.3. Oracle Audit Vault Architecture

Audit Vault 는 아래의 표와 같이 크게 1. 감사대상이 될 Source DB, 2 감사 수집 역할을 하는 Audit Vault Agent, 3 Audit Data 를 전송 받고 이를 관리하는 Audit Vault Server, 4 Audit Vault 전체를 관리 할 Audit Vault User 로 이루어져 있습니다.

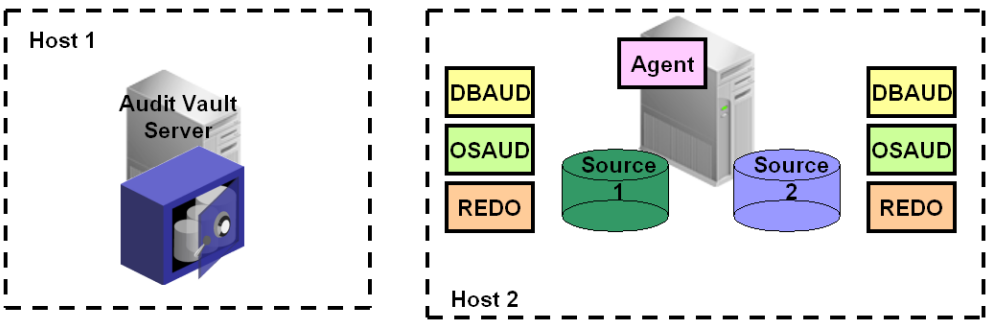


1.4. Oracle Audit Vault Collection Agents and Collectors

Oracle Audit Vault 는 Collector 를 통해 AV Collection Agent 와 연결된 source DB 의 감사데이터와 통신을 합니다. Collection Agent 는 Audit Vault Server, Source DB, 별도의 위치에 설치가 가능합니다.

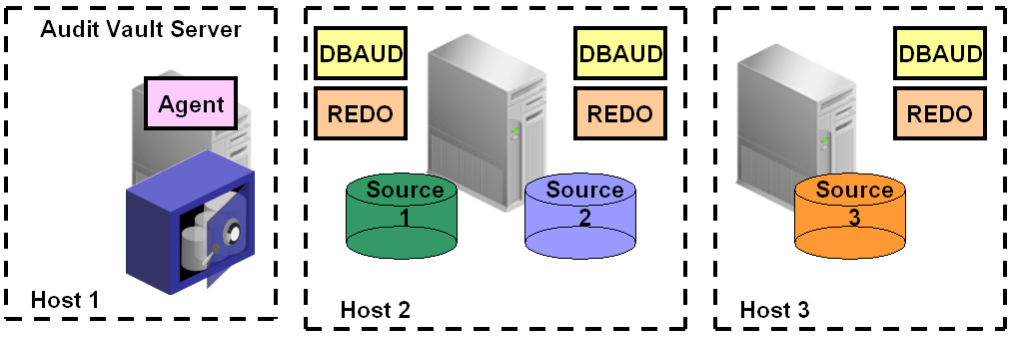
단, Collector type 이 DBAUD 와 REDO 인 경우에는 Source DB 를 연결해 감사정보를 수집하기 때문에 AV Collection Agent 를 별도의 server 에 설치되어 운영될 수 있으나 OSAUD 는 반드시 Source DB 와 AV Collection Agent 가 함께 설치되어야 합니다.

1.4.1. Oracle Audit Vault Collection Agents and Collectors Composition 1



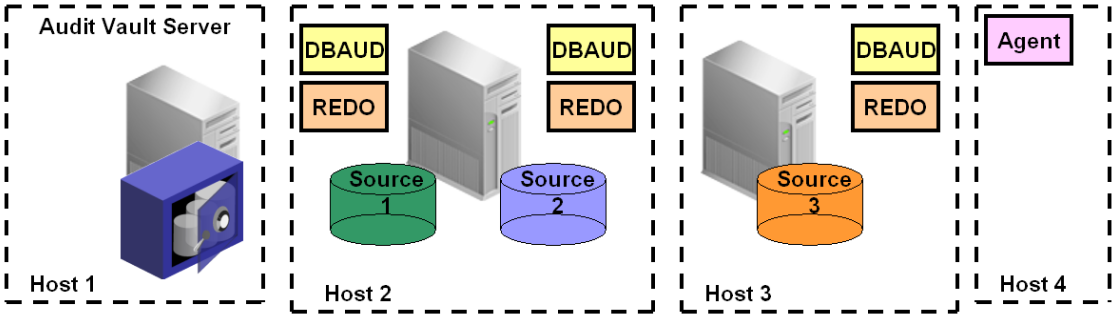
Source DB 에 AV Collection Agent 가 설치되어 DBAUD, OSAUD, REDO Collector 를 통해 감사정보를 수집하도록 구성한 예 입니다.

1.4.2. Oracle Audit Vault Collection Agents and Collectors Composition 2



AV Collection Agent 가 AV Server 에 설치되어 DBAUD,REDO collector 를 통해 감사정보를 수집하도록 구성한 예 입니다. **OSAUD Collector 는 구동 할 수 없습니다.**

1.4.3. Oracle Audit Vault Collection Agents and Collectors Composition 3

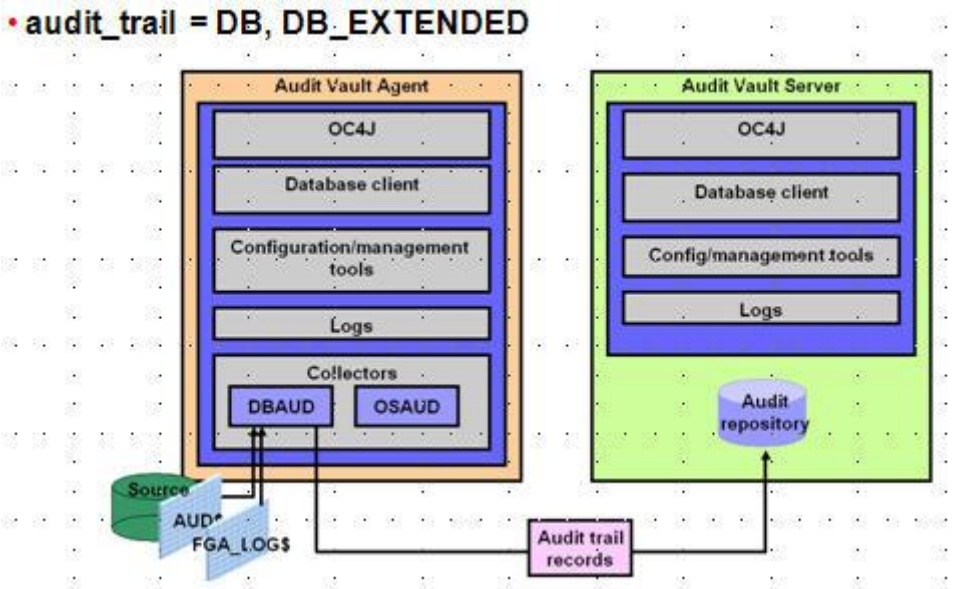


AV Collection Agent 가 별도의 server 에 위치해 DBAUD, REDO collector 를 통해 감사정보를 수집하도록 구성한 예 입니다. **OSAUD Collector 는 구동 할 수 없습니다.**

1.5. Oracle Audit Vault Collector Type

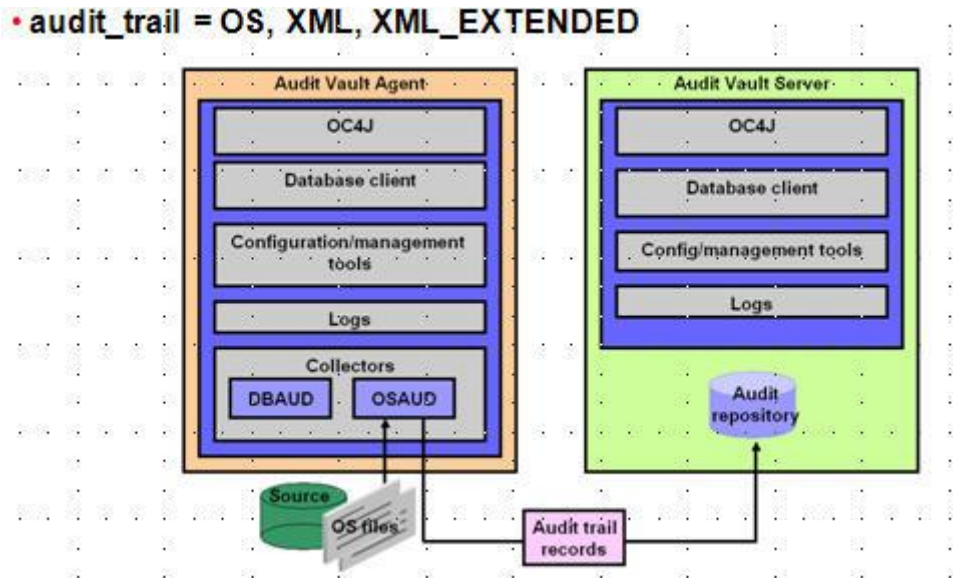
AV Agent 는 감사정보를 수집하기 위해 3 개의 Collector 를 가집니다.

1.5.1. DBAUD



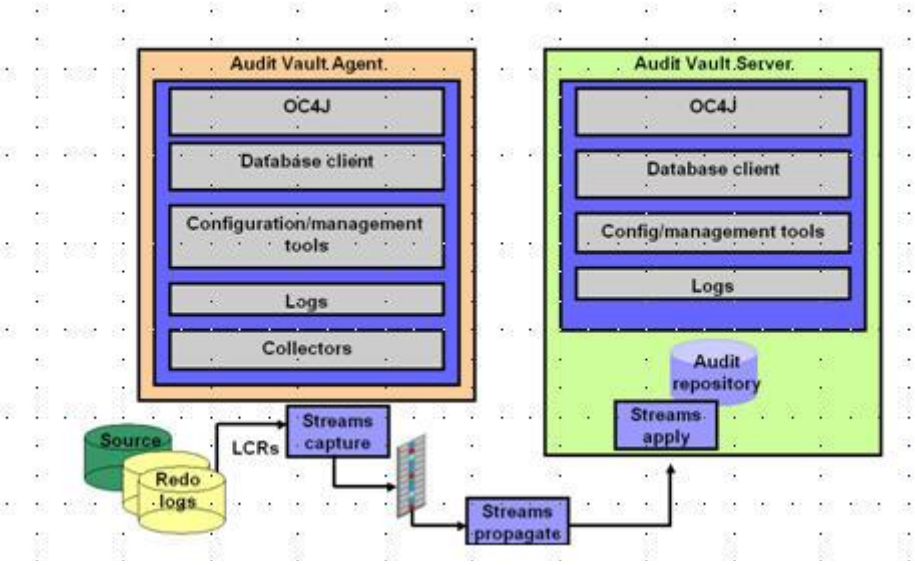
DBAUD Collector 는 감사정보는 SYS.AUD$ dictionary table 에 보관하고 fine-grained 감사 정보는 SYS.FGA_LOG$ dictionary table 에 저장합니다.

1.5.2. OSAUD



OSAUD Collector 는 감사정보를 audit_file_dest 에 위치한곳에 OSfile 형태로 저장됩니다. UNIX platforms 경우는 .aud 형태로 Windows platforms 경우는 .xml 형태로 저장됩니다.

1.5.3. REDO



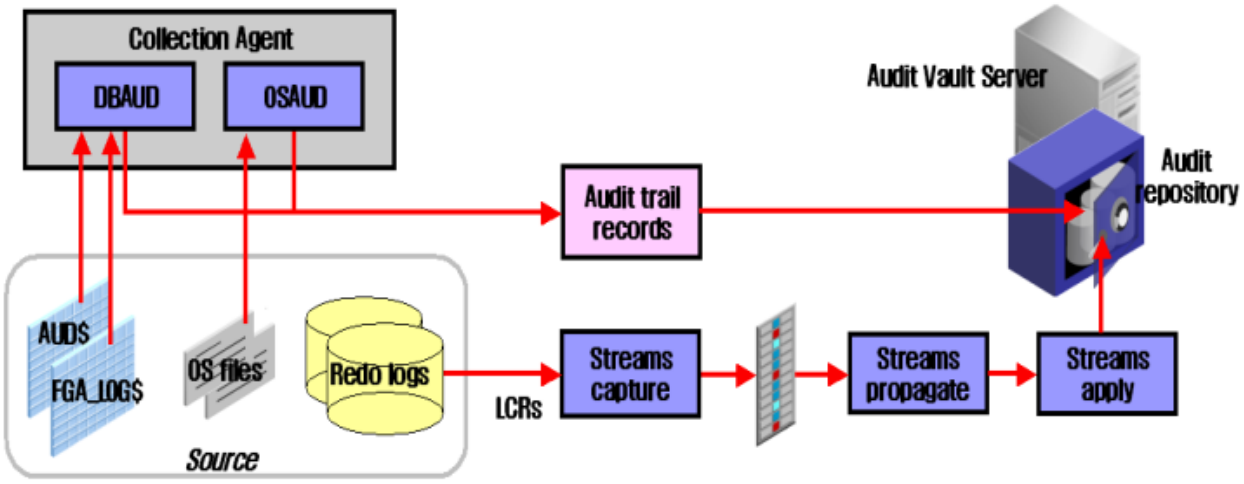
REDO Collector 는 Redo Log 의 정보들을(DML) LCRs(Logical Change Records)형태로 추출하여 Streams 기능을 통해 AV Server 에 전달합니다

1.5.4. Collector Property

아래의 표와 같이 각각의 Collector 별로 수집할 수 있는 특징들을 가집니다.

Characteristic	OSAUD	DBAUD	REDO
Select	✓	✓	
DML	✓	✓	✓
DDL	✓	✓	✓
Before and After Values			✓
Success and Failure	✓	✓	
SQL Text	✓*	✓	
SYS Auditing	✓		✓
Other considerations	Separation of Duties	FGA data	Supplemental logging may be required for values

1.5.5. Collector Process



위의 그림과 같이 AV Server 는 AV Agent 와 통신하여 감사정보를 수집하고 AV Agent 가 관리하는 Collector(DBAUD, OSAUD,)들은 각각의 감사정보를 수집하여 AV Server 에 전달합니다.

2. Oracle Audit Vault S/W Information

2.1. Oracle Audit Vault S/W Download

www.oracle.com 에서 해당 platform 에 맞는 Oracle Audit Vault Server 와 Oracle Audit Vault Collection Agent 를 다운받습니다.

Windows platform 은 Oracle Support (메타링크) => Patches and Updates 에서 9497849 선택

https://updates.oracle.com/download/9497849.html

3. Oracle Audit Vault Supported

아래의 표들을 통해서 각각 Audit Vault Server, Audit Vault Agent, Source DB 를 지원하는 내역을 확인 할 수 있습니다.

Supported 정보는 Oracle Metalink 에서도 확인 가능합니다.

3.1. Oracle Audit Vault Server Platform Support

아래의 표를 보시면 Audit Vault Server Version 별 지원할 수 있는 Platform 과 해당 OS 의 Version, 지원가능한 DBMS Version 을 확인 할 수 있습니다.

Oracle Audit Vault Server [ID 848408.1]

Oracle Audit Vault Server [ID 848408.1]

Oracle Audit Vault Server Platform Support

Audit Vault Server Release	Platform	Versions
10.2.3.2	HP Itanium	11.23, 11.31
10.2.3.2	IBM AIX	AIX 5.2, AIX 5.3, AIX 6.1
10.2.3.2	Linux x86	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.2	Linux x86	SLES-9, SLES-10, SLES-11
10.2.3.2	Linux x86-64	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.2	Linux x86-64	SLES-9, SLES-10, SLES-11
10.2.3.2	Solaris SPARC64	9, 10
10.2.3.2	Windows 32	2003, 2003 R2, XP
10.2.3.1	HP Itanium	11.23, 11.31
10.2.3.1	IBM AIX	AIX 5.2, AIX 5.3, AIX 6.1
10.2.3.1	Linux x86	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.1	Linux x86	SLES-9, SLES-10
10.2.3.1	Linux x86-64	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.1	Linux x86-64	SLES-9, SLES-10
10.2.3.1	Solaris SPARC64	9, 10

Oracle Audit Vault Source Database Support

DBMS	DBMS Release	Minimum Audit Vault Release for Support	Notes
IBM DB2 Unix, Linux, Windows	8.2 - 9.5	10.2.3.1	
Microsoft SQL Server	2000, 200, 2008	10.2.3.0	
Oracle	9.2.x., 10.1.x, 10.2.x, 11.1.x	10.2.2.0	The Oracle REDO collector only supports Oracle database versions 9.2.0.8, 10.2.0.3+, and 11.1.0.6+
	11.2	10.2.3.2	
Sybase ASE	12.5.4 ãl Ï 15.0.x	10.2.3.1	

3.2. Oracle Audit Vault Agent Platform Support

아래의 표를 보시면 Audit Vault Agent Version 별 지원할 수 있는 Platform 과 해당 OS 의 Version, 지원가능한 DBMS Version 을 확인 할 수 있습니다.

Oracle Audit Vault Server [ID 848402.1]

Oracle Audit Vault Agent [ID 848402.1]

Oracle Audit Vault Agent Platform Support

Audit Vault Server Release	Platform	Versions
10.2.3.2	HP Itanium	11.23, 11.31
10.2.3.2	HP-UX PA-RISC	11.11, 11.23, 11.31
10.2.3.2	IBM AIX	AIX 5.2, AIX 5.3, AIX 6.1
10.2.3.2	Linux x86	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.2	Linux x86	SLES-9, SLES-10, SLES-11
10.2.3.2	Linux x86-64	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.2	Linux x86-64	SLES-9, SLES-10, SLES-11
10.2.3.2	Solaris SPARC64	9, 10
10.2.3.2	Windows 32	2000, 2003, 2003 R2, XP
10.2.3.2	Windows 64	2003, 2003 R2 Note: 32bit code is certified on Windows 64bit
10.2.3.1	HP Itanium	11.23, 11.31
10.2.3.1	HP-UX PA-RISC	11.11, 11.23, 11.31
10.2.3.1	IBM AIX	AIX 5.2, AIX 5.3, AIX 6.1
10.2.3.1	Linux x86	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.1	Linux x86	SLES-9, SLES-10
10.2.3.1	Linux x86-64	Red Hat Enterprise AS/ES 3, Red Hat Enterprise AS/ES 4/Oracle VM, Red Hat Enterprise AS/ES 5/Oracle VM, OEL4/Oracle VM, OEL5/Oracle VM
10.2.3.1	Linux x86-64	SLES-9, SLES-10
10.2.3.1	Solaris SPARC64	9, 10
10.2.3.1	Windows 32	2000, 2003, 2003 R2, XP
10.2.3.1	Windows 64	2003, 2003 R2 Note: 32bit code is certified

Oracle Audit Vault Source Database Support

DBMS	DBMS Release	Minimum Audit Vault Release for Support	Notes
IBM DB2 Unix, Linux, Windows	8.2 - 9.5	10.2.3.1	
Microsoft SQL Server	2000, 200, 2008	10.2.3.0	
Oracle	9.2.x., 10.1.x, 10.2.x, 11.1.x	10.2.2.0	The Oracle REDO collector only supports Oracle database versions 9.2.0.8, 10.2.0.3+, and 11.1.0.6+
	11.2	10.2.3.2	
Sybase ASE	12.5.4 ãl ▯ 15.0.x	10.2.3.1	

3.3. Supported Source Database Products

아래 정보는 각각의 Collector 별로 지원하는 DBMS Version 을 나타내주고 있습니다.

Database Product	Supported Versions
Oracle Database	For the OSAUD and DBAUD collector types: Releases 9.2.x, 10.1.x, 10.2.x, and 11.x For the REDO collector type: Enterprise Edition Releases 9.2.0.8, 10.2.0.3, 10.2.0.4 and later, 11.1.0.6 and later, and 11.2 for the REDO collector type

4. Oracle Audit Vault Server Preinstallation Requirements

본 문서는 AV_SERVER 는 win 2003, AV_AGENT 는 win 2000, Source_DB 는 9.2.0.8 로구성합니다.

설치를 하기 전에 Audit Vault Server 와 Audit Vault Agent 의 host file 에 호스트 명을 등록합니다. UNIX/LINUX 경우 etc/hosts, Windows 는 C:₩WINDOWS₩system32₩drivers₩etc 위치의 hosts file 에 등록합니다.

```
###audit vault server
172.17.126.129    oldwasprod
###audit vault agent
172.17.126.191    goodus
```

4.1. Checking the Hardware Requirements

Requirement	Minimum Value
Physical memory (RAM)	256 MB minimum; 512 MB recommended
Virtual memory	Double the amount of RAM
Hard disk space	4.73 GB Total
Video adapter	256 colors
Processor	550 MHz minimum

4.2. Hard Disk Space Requirements

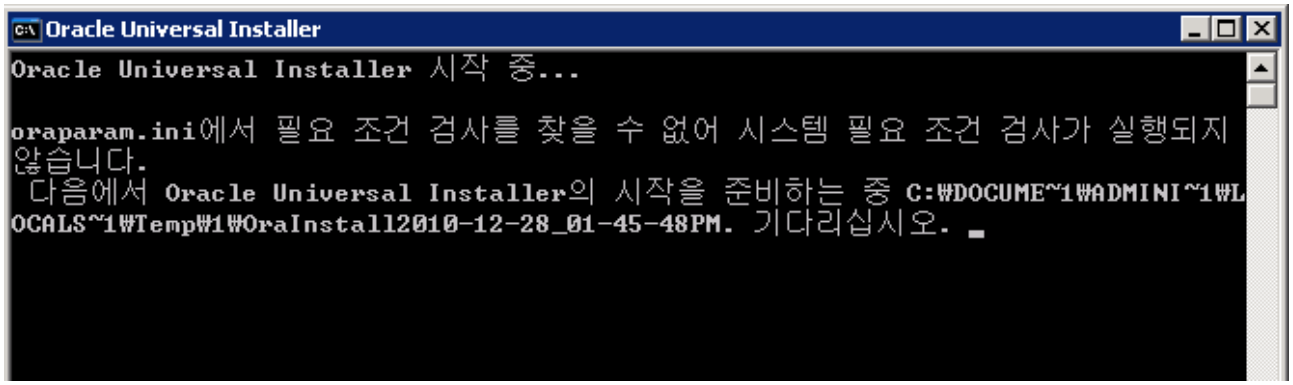
TEMP Space	Oracle Home	Data Files	Total
102 MB	3.38 GB	1.25 GB	4.73 GB

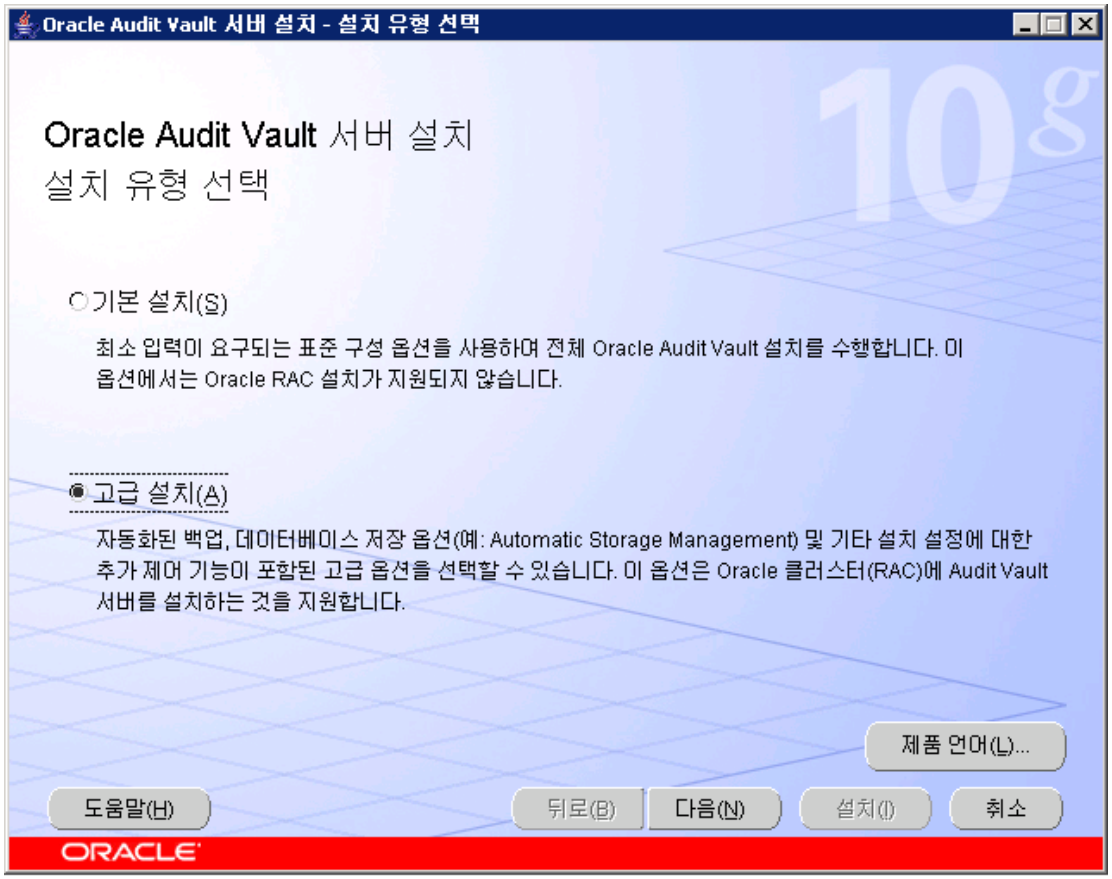
4.3. Checking the Operating System Requirements

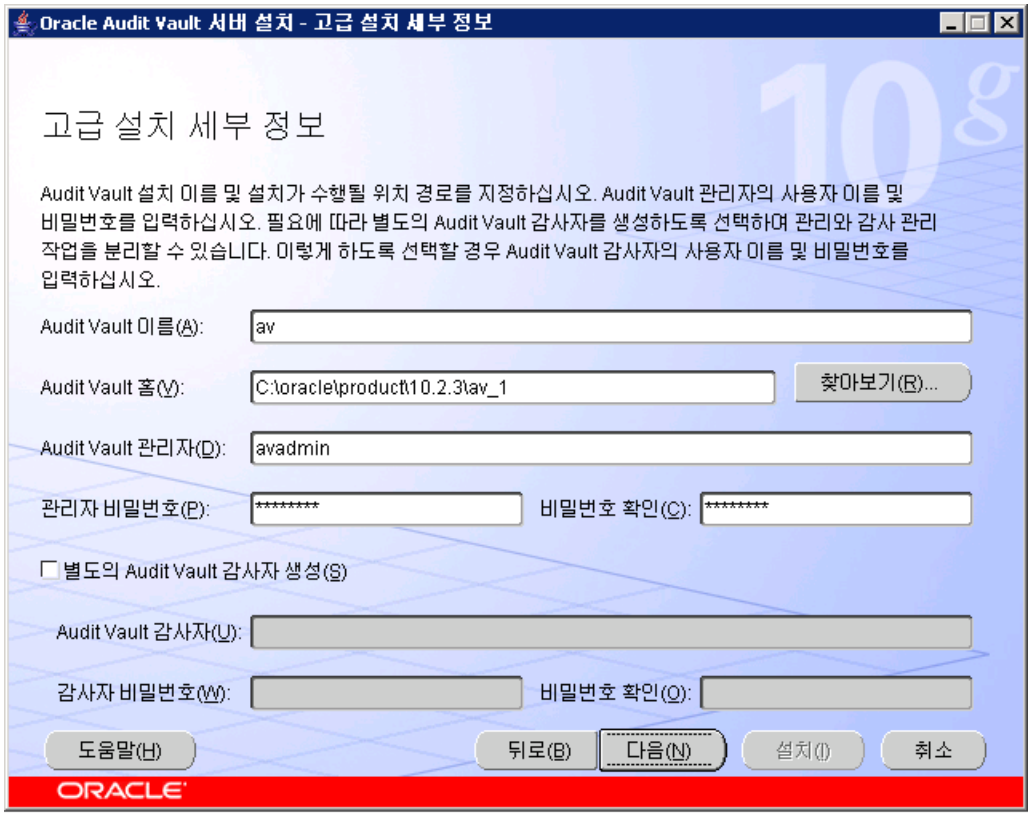
Requirement	Value
System Architecture	Processor: Intel (x86), AMD64, and Intel EM64T Note: The 32-bit Audit Vault version, which this installation guide describes, runs on the 32-bit version of Windows on either x86 or x64 hardware. For additional information, visit My Oracle Support (formerly OracleMetaLink)

Requirement	Value
	at: https://support.oracle.com
Operating System	Oracle Audit Vault collection agent for Windows is supported on the following operating systems: → 아래와 같은 OS System 들을 지원합니다. • **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** • **Windows XP Professional (single instance only)** 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. Windows NT is not supported. Windows Multilingual User Interface Pack is supported on Windows Server 2003, and Windows XP Professional.
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

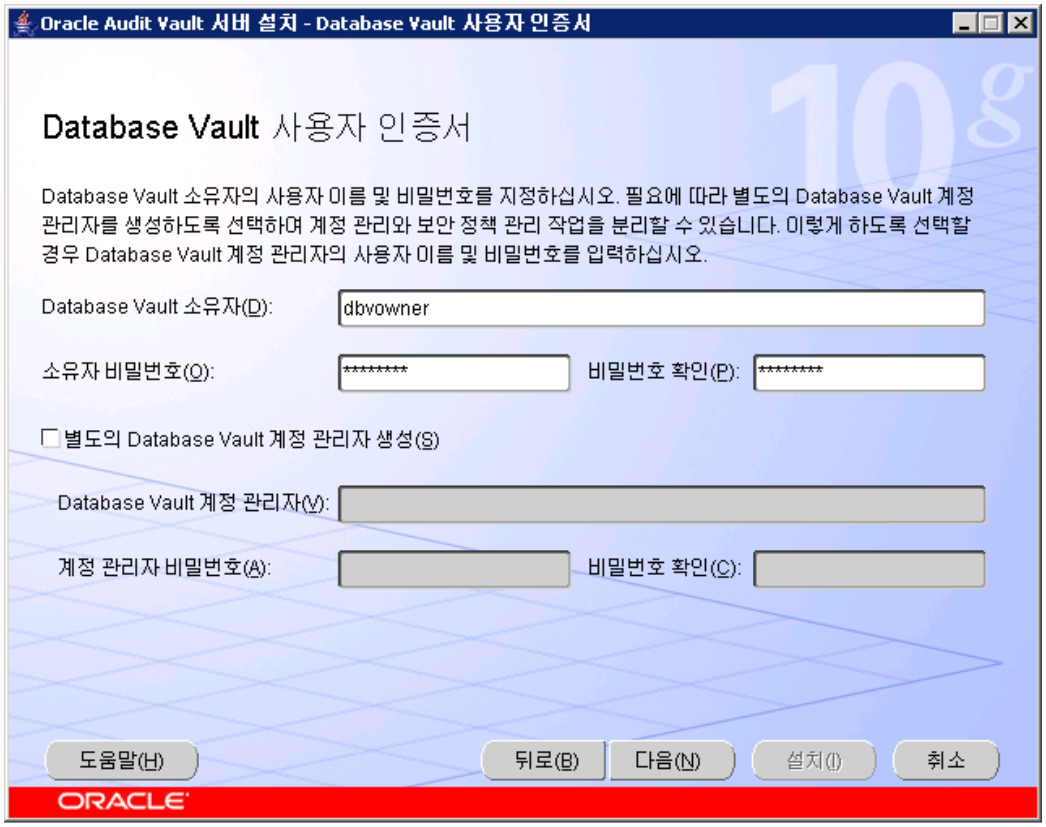
5. Installing the Oracle Audit Vault Server



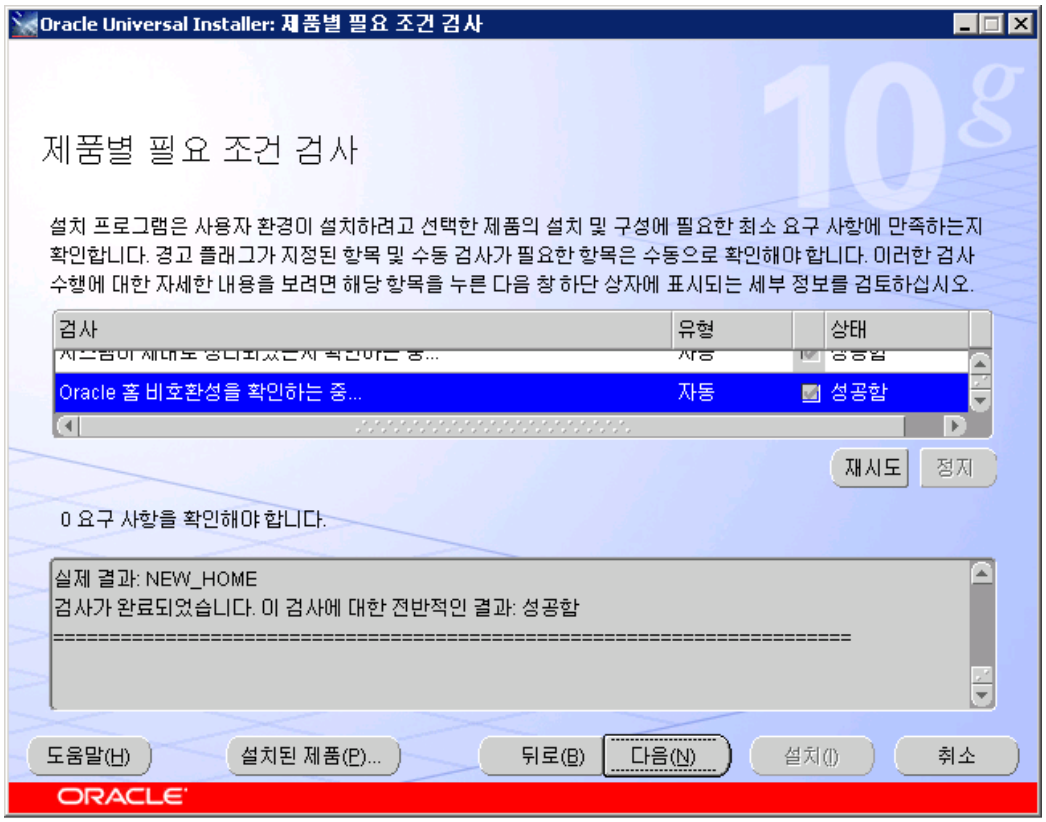


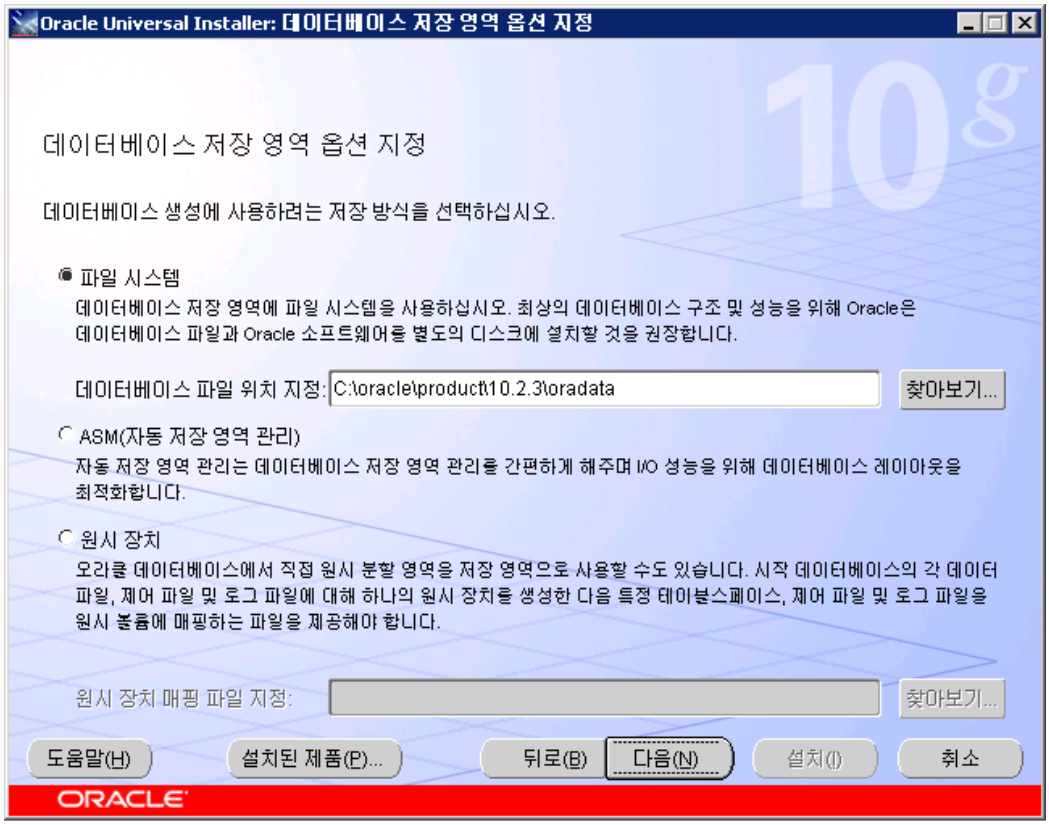


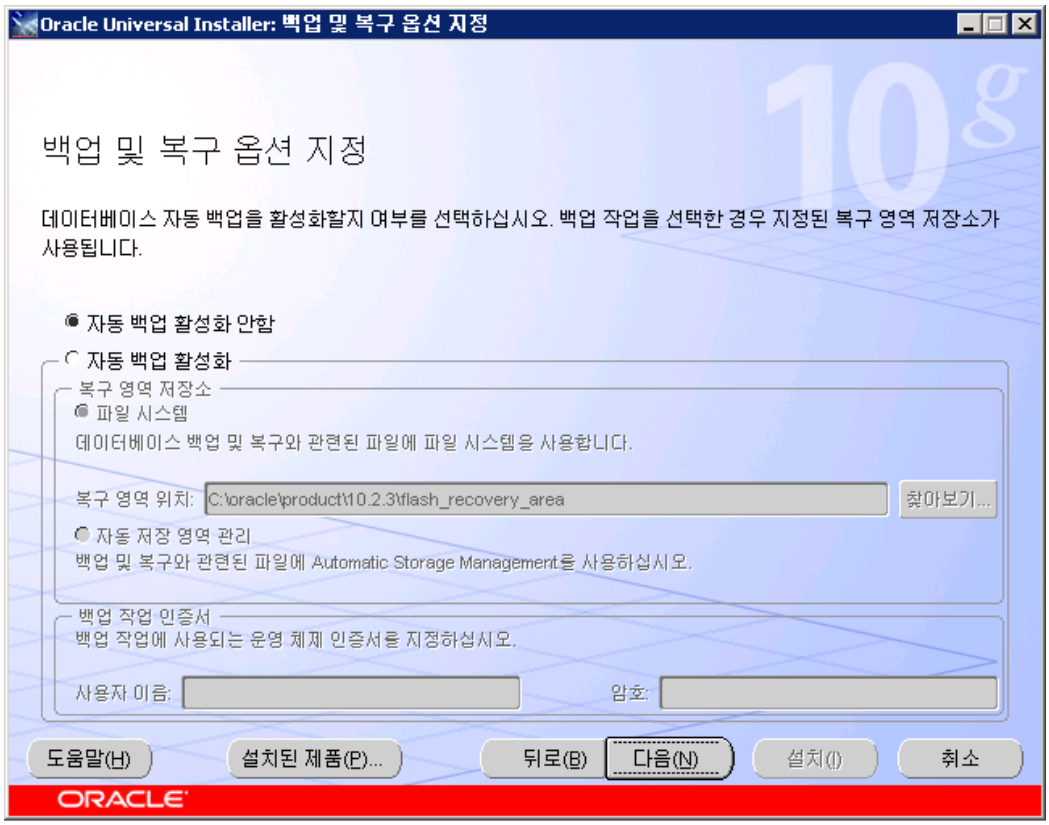
- Audit Vault 이름 : Audit Vault 를 설치하게 되면 DB 가 구성되며 해당 DB 이름
- Audit Vault 관리자 : Audit Vault 를 관리하기위해 별도의 user 가 필요

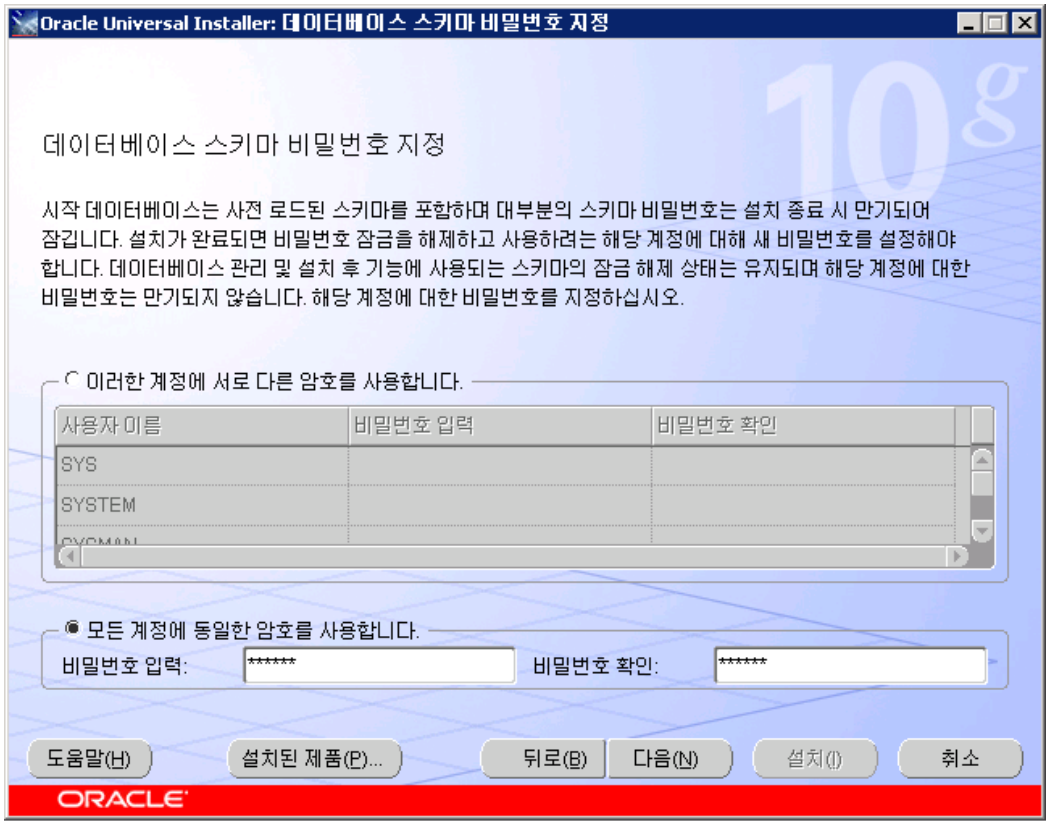


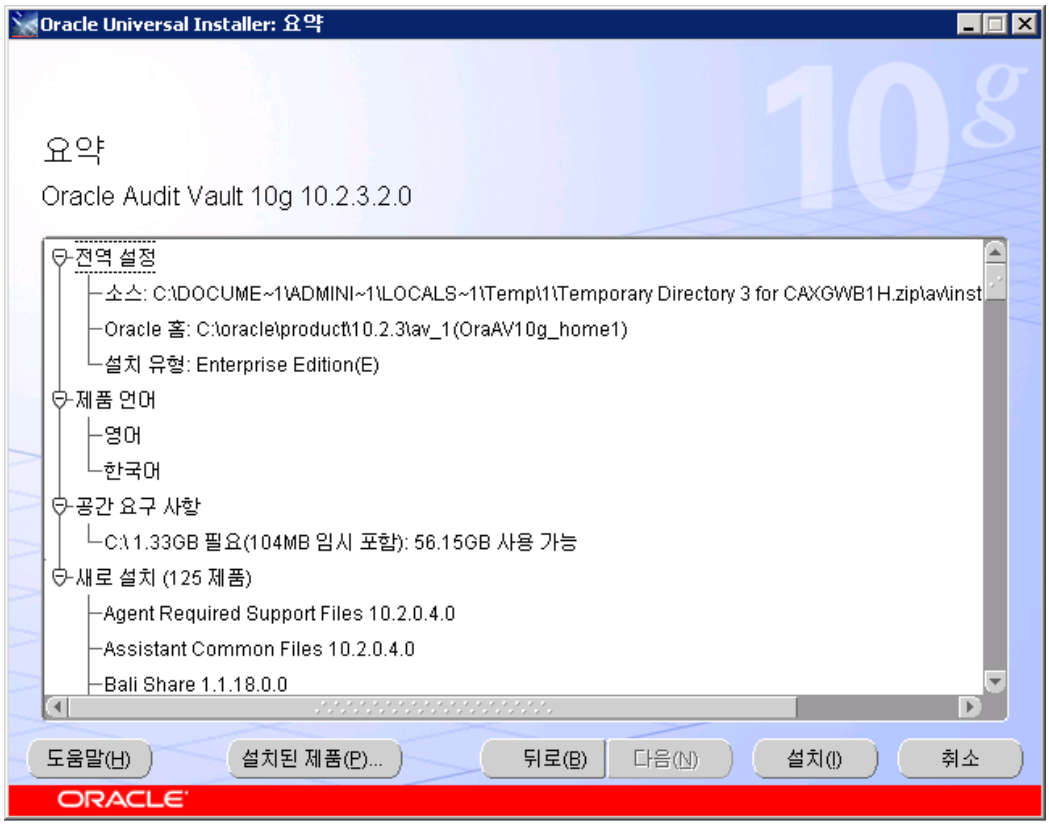
- Database Vault 소유자 : Audit Vault 를 설치하면 자동으로 DV 가 함께 설치됨

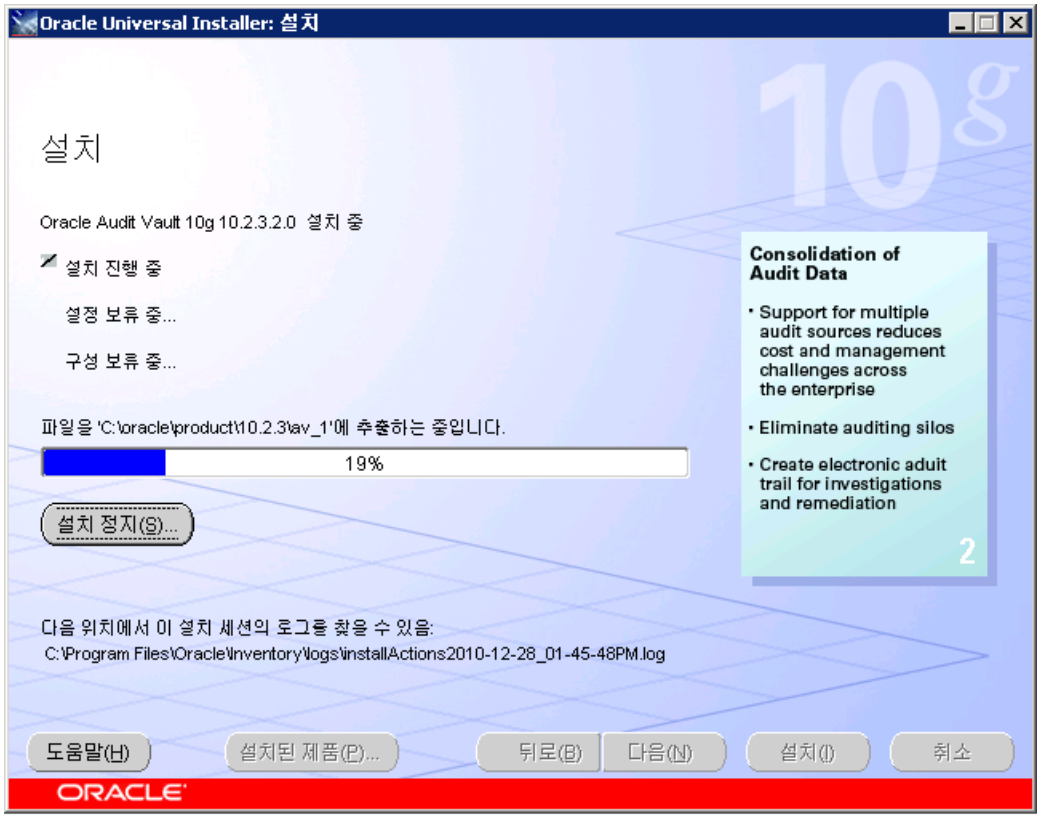

Oracle Universal Installer: 제품별 필요 조건 검사
제품별 필요 조건 검사
설치 프로그램은 사용자 환경이 설치하려고 선택한 제품의 설치 및 구성에 필요한 최소 요구 사항에 만족하는지 확인합니다. 경고 플래그가 지정된 항목 및 수동 검사가 필요한 항목은 수동으로 확인해야 합니다. 이러한 검사 수행에 대한 자세한 내용을 보려면 해당 항목을 누른 다음 창 하단 상자에 표시되는 세부 정보를 검토하십시오.
검사
유형
상태
Oracle 홈 비호환성을 확인하는 중...
자동
성공함
재시도
정지
0 요구 사항을 확인해야 합니다.
실제 결과: NEW_HOME
검사가 완료되었습니다. 이 검사에 대한 전반적인 결과: 성공함
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 데이터베이스 저장 영역 옵션 지정
데이터베이스 저장 영역 옵션 지정
데이터베이스 생성에 사용하려는 저장 방식을 선택하십시오.
파일 시스템
데이터베이스 저장 영역에 파일 시스템을 사용하십시오. 최상의 데이터베이스 구조 및 성능을 위해 Oracle은 데이터베이스 파일과 Oracle 소프트웨어를 별도의 디스크에 설치할 것을 권장합니다.
데이터베이스 파일 위치 지정:
C:\oracle\product\10.2.3\oradata
찾아보기...
ASM(자동 저장 영역 관리)
자동 저장 영역 관리는 데이터베이스 저장 영역 관리를 간편하게 해주며 I/O 성능을 위해 데이터베이스 레이아웃을 최적화합니다.
원시 장치
오라클 데이터베이스에서 직접 원시 분할 영역을 저장 영역으로 사용할 수도 있습니다. 시작 데이터베이스의 각 데이터 파일, 제어 파일 및 로그 파일에 대해 하나의 원시 장치를 생성한 다음 특정 테이블스페이스, 제어 파일 및 로그 파일을 원시 볼륨에 매핑하는 파일을 제공해야 합니다.
원시 장치 매핑 파일 지정:
찾아보기...
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 백업 및 복구 옵션 지정
백업 및 복구 옵션 지정
데이터베이스 자동 백업을 활성화할지 여부를 선택하십시오. 백업 작업을 선택한 경우 지정된 복구 영역 저장소가 사용됩니다.
자동 백업 활성화 안함
자동 백업 활성화
복구 영역 저장소
파일 시스템
데이터베이스 백업 및 복구와 관련된 파일에 파일 시스템을 사용합니다.
복구 영역 위치: C:\oracle\product\10.2.3\flash_recovery_area
찾아보기...
자동 저장 영역 관리
백업 및 복구와 관련된 파일에 Automatic Storage Management를 사용하십시오.
백업 작업 인증서
백업 작업에 사용되는 운영 체제 인증서를 지정하십시오.
사용자 이름:
암호:
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE

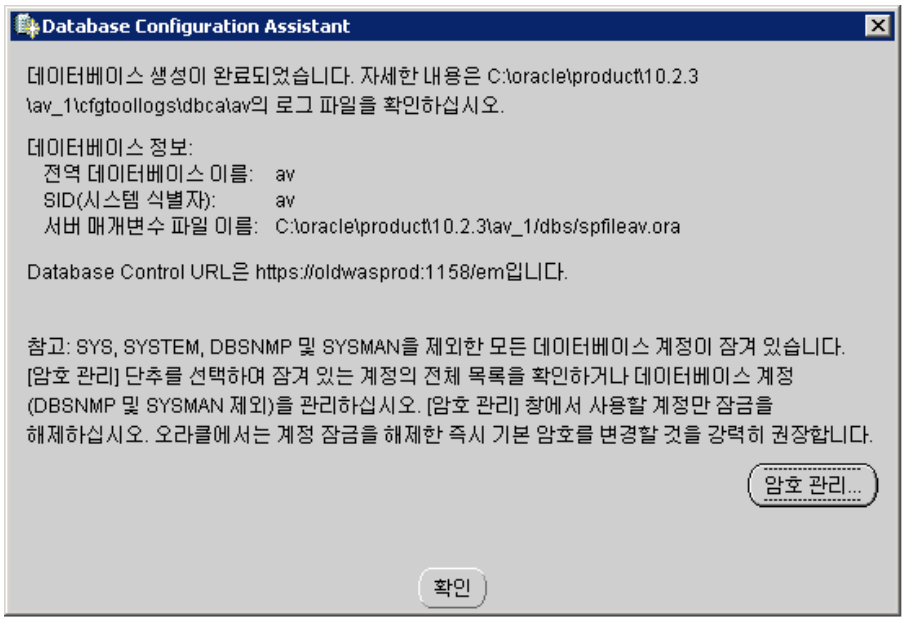

Oracle Universal Installer: 데이터베이스 스키마 비밀번호 지정
데이터베이스 스키마 비밀번호 지정
시작 데이터베이스는 사전 로드된 스키마를 포함하며 대부분의 스키마 비밀번호는 설치 종료 시 만기되어 잠깁니다. 설치가 완료되면 비밀번호 잠금을 해제하고 사용하려는 해당 계정에 대해 새 비밀번호를 설정해야 합니다. 데이터베이스 관리 및 설치 후 기능에 사용되는 스키마의 잠금 해제 상태는 유지되며 해당 계정에 대한 비밀번호는 만기되지 않습니다. 해당 계정에 대한 비밀번호를 지정하십시오.
이러한 계정에 서로 다른 암호를 사용합니다.
사용자 이름
비밀번호 입력
비밀번호 확인
SYS
SYSTEM
모든 계정에 동일한 암호를 사용합니다.
비밀번호 입력:
비밀번호 확인:
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 요약
요약
Oracle Audit Vault 10g 10.2.3.2.0
전역 설정
소스: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\Temporary Directory 3 for CAXGWB1H.zip\av\inst
Oracle 홈: C:\oracle\product\10.2.3\av_1(OraAV10g_home1)
설치 유형: Enterprise Edition(E)
제품 언어
영어
한국어
공간 요구 사항
C:\ 1.33GB 필요(104MB 임시 포함): 56.15GB 사용 가능
새로 설치 (125 제품)
Agent Required Support Files 10.2.0.4.0
Assistant Common Files 10.2.0.4.0
Bali Share 1.1.18.0.0
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE

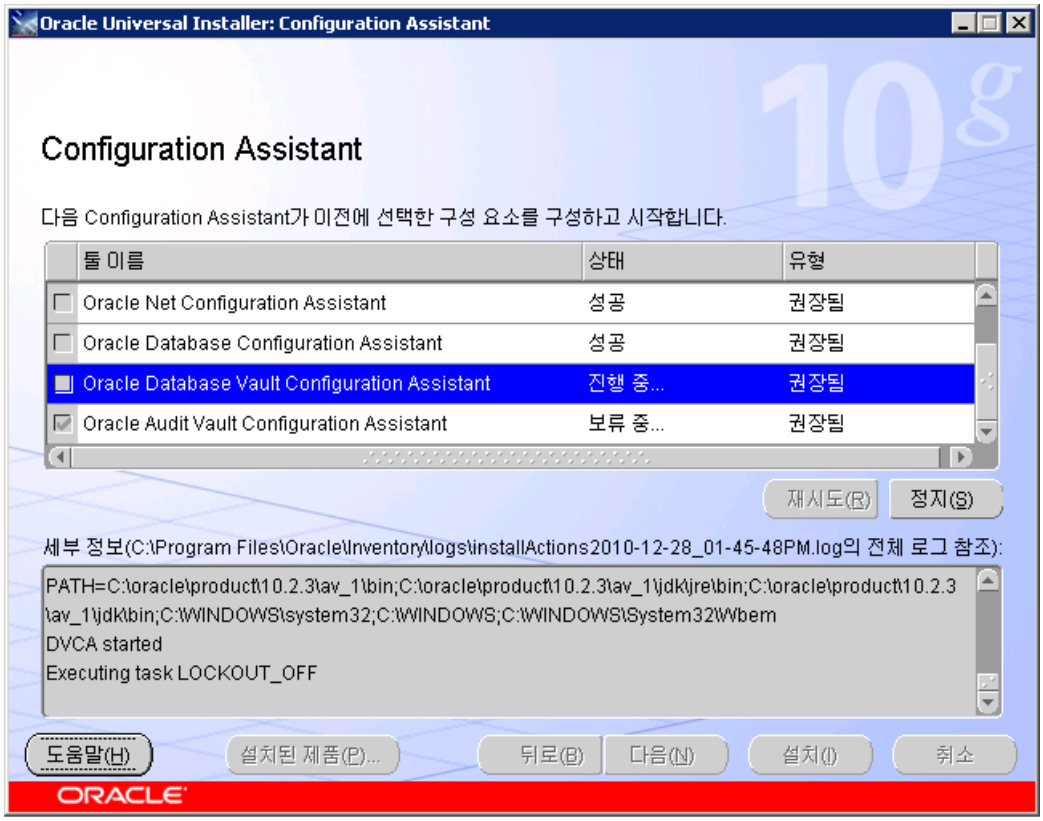

Oracle Universal Installer: 설치
설치
Oracle Audit Vault 10g 10.2.3.2.0 설치 중
설치 진행 중
설정 보류 중...
구성 보류 중...
파일을 'C:\oracle\product\10.2.3\av_1'에 추출하는 중입니다.
19%
설치 정지(S)...
Consolidation of Audit Data
• Support for multiple audit sources reduces cost and management challenges across the enterprise
• Eliminate auditing silos
• Create electronic adult trail for investigations and remediation
2
다음 위치에서 이 설치 세션의 로그를 찾을 수 있음:
C:\Program Files\Oracle\Inventory\logs\installActions2010-12-28_01-45-48PM.log
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE

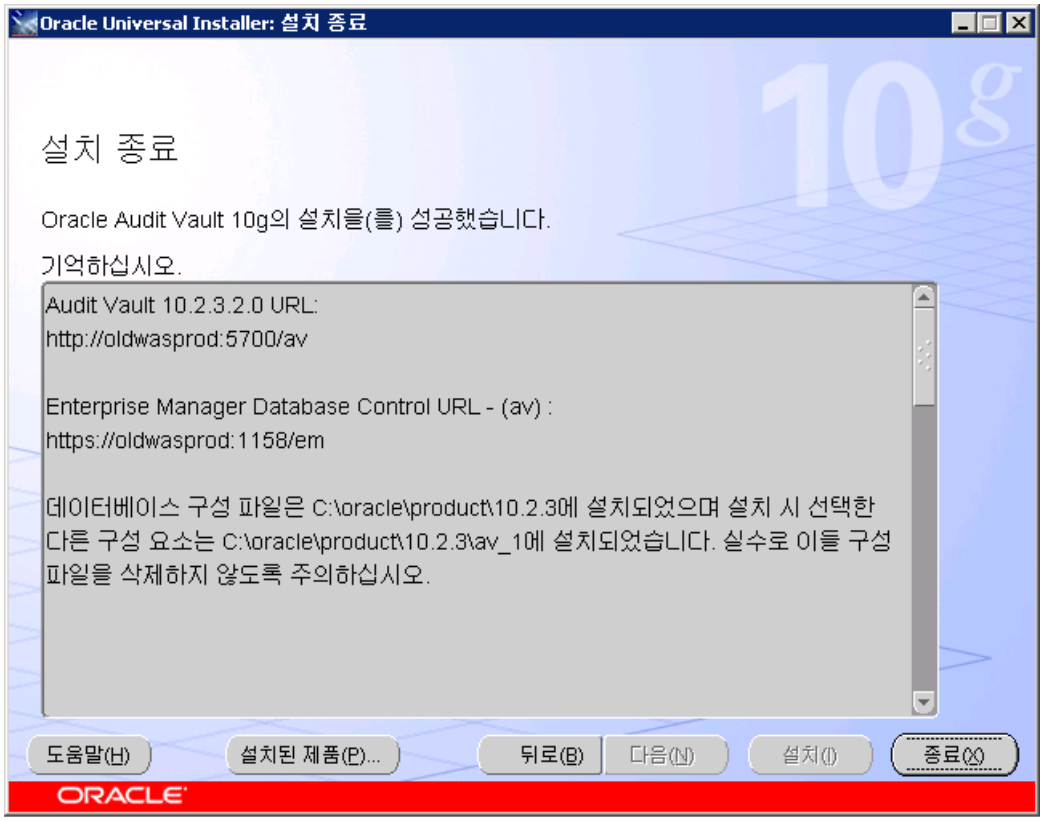
- AV Patch

- DBCA



- DVCA -> AVCA 단계를 거침




Oracle Universal Installer: 설치 종료
설치 종료
Oracle Audit Vault 10g의 설치을(를) 성공했습니다.
기억하십시오.
Audit Vault 10.2.3.2.0 URL:
http://oldwasprod:5700/av
Enterprise Manager Database Control URL - (av) :
https://oldwasprod:1158/em
데이터베이스 구성 파일은 C:\oracle\product\10.2.3에 설치되었으며 설치 시 선택한 다른 구성 요소는 C:\oracle\product\10.2.3\av_1에 설치되었습니다. 실수로 이들 구성 파일을 삭제하지 않도록 주의하십시오.
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
종료(X)
ORACLE

6. Oracle Audit Vault Agent Preinstallation Requirements

6.1. Hardware Requirements

Requirement	Minimum Value
Physical memory (RAM)	128 MB minimum, 512 MB recommended
Virtual memory	Double the amount of RAM
Hard disk space	797 MB (includes 167 MB temporary)
Video adapter	256 colors
Processor	550 MHz minimum

6.2. Hard Disk Space Requirements

TEMP Space	Oracle Home	Total
167 MB	630 MB	797 MB

6.3. Software Requirements

Requirement	Value
System architecture	Processor: Intel (x86) For additional information, visit My Oracle Support at https://support.oracle.com
Operating system	Oracle Audit Vault collection agent for Microsoft Windows is supported on the following operating systems: → 아래와 같은 OS System 들을 지원합니다. • **Microsoft Windows 2000 with service pack 1 or later. All editions, including Terminal Services and Microsoft Windows 2000 MultiLanguage Edition (MLE), are supported.** • **Microsoft Windows Server 2003 - all editions**

Requirement	Value
	• **Microsoft Windows XP Professional** 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. Microsoft Windows NT is not supported. Microsoft Windows Multilingual User Interface Pack is supported on Microsoft Windows Server 2003, and Microsoft Windows XP Professional.
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 Secure Sockets Layer (SSL) • Named Pipes

7. Installing the Oracle Audit Vault Agent

Agent 설치하기 전에 Audit Vault Server 에 아래와 같이 등록합니다.

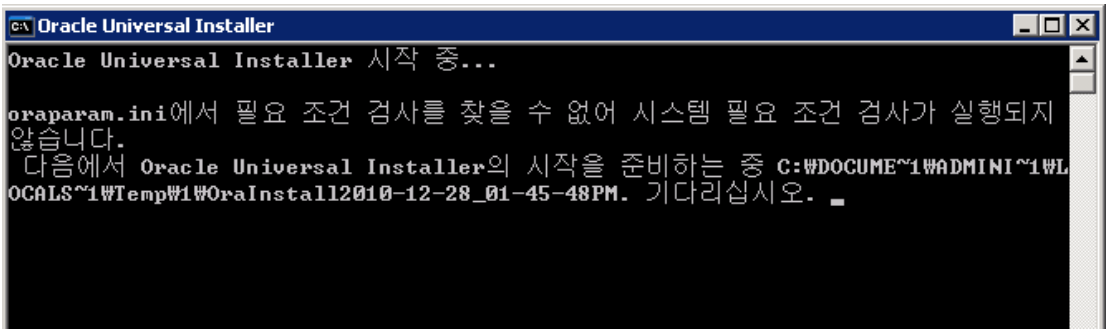
Source DB 서버와 Listener, Audit Vault Server 가 모두 구동 중인지 확인합니다.

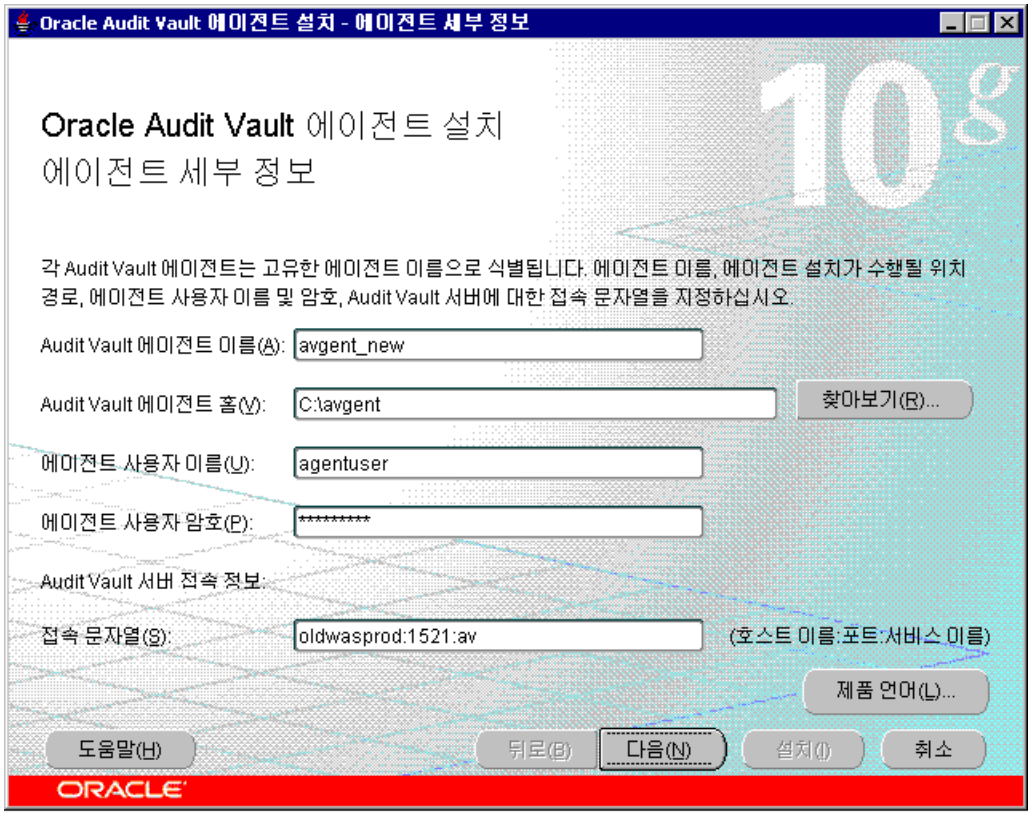
avca add_agent -agentname avgent_new -agenthost goodus

agentuser

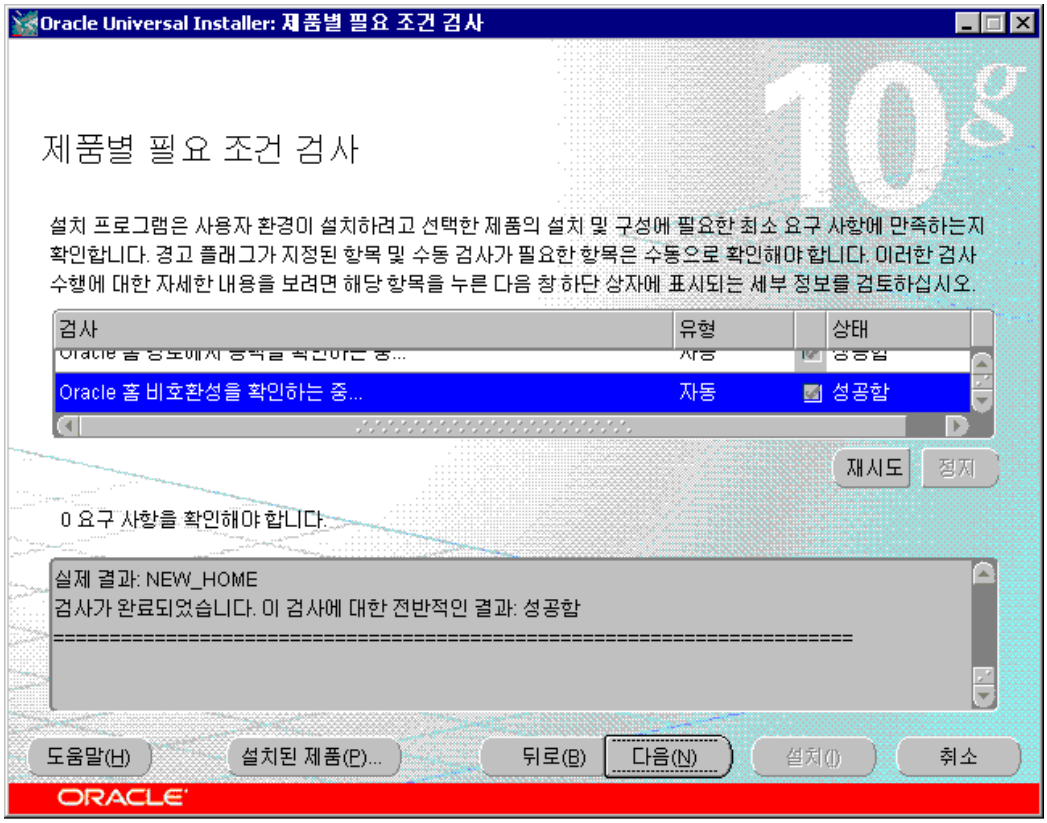
agentuser

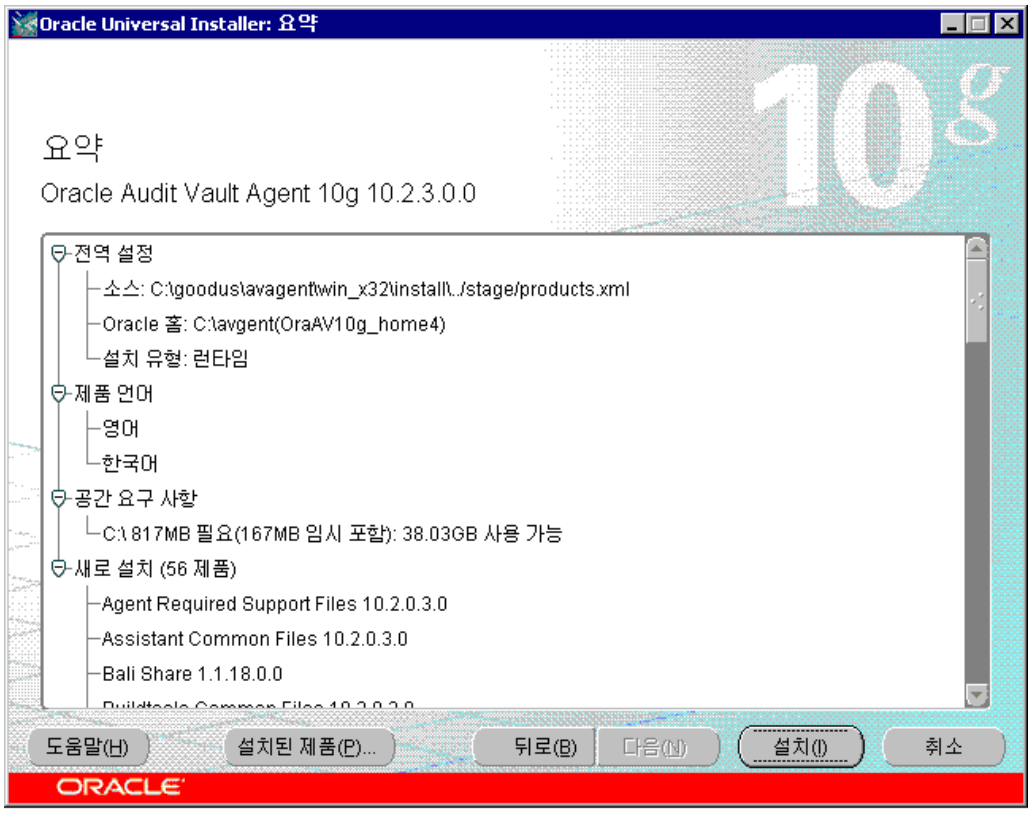
→ av_server em 화면 구성-에이전트 부분에 추가됨

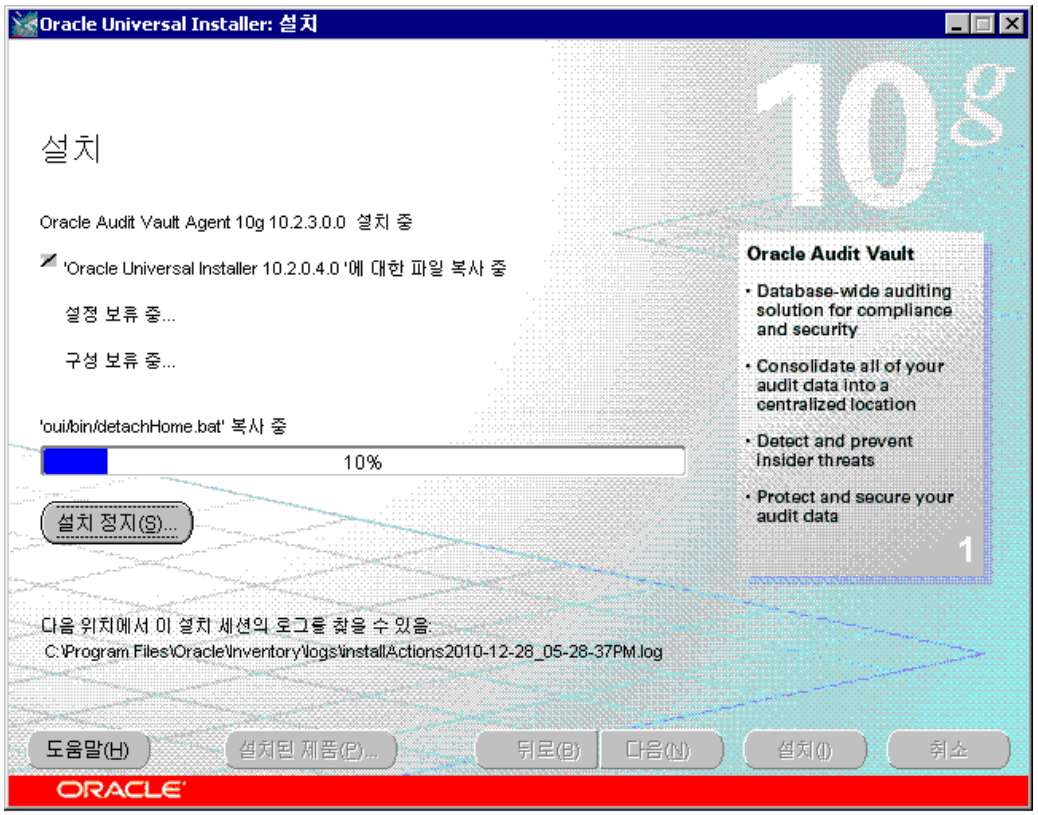


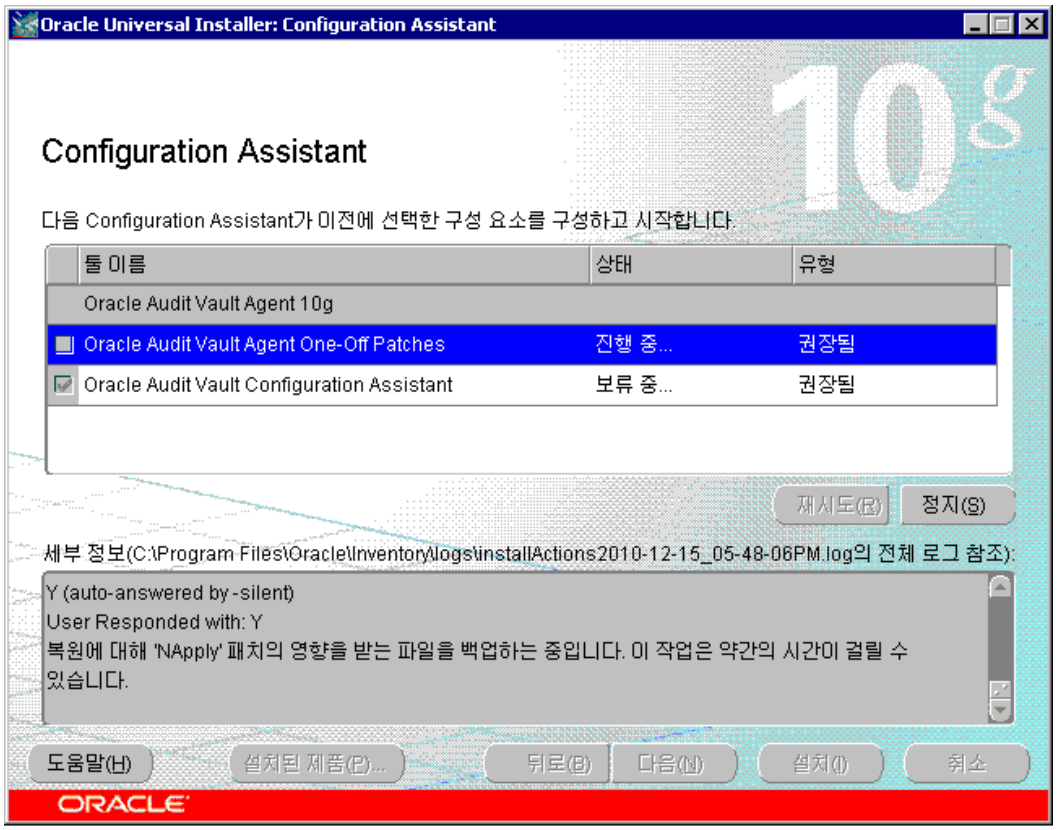


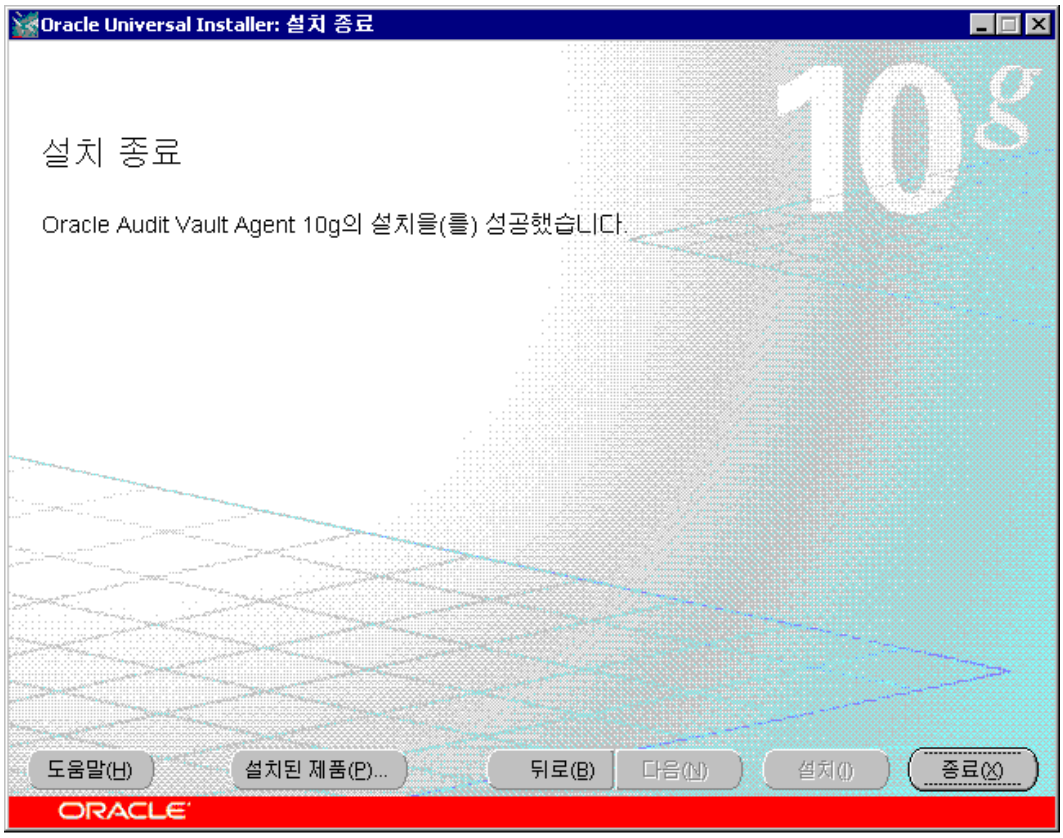
- Audit Vault 에이전트 이름 : AV_Server 에 등록한 agentname
- 에이전트 사용자 이름 : AV_Server 에 등록한 agentuser
- 접속문자열 : AV_Server 쪽의 호스트 이름:리스너포트:서비스이름


Oracle Universal Installer: 제품별 필요 조건 검사
제품별 필요 조건 검사
설치 프로그램은 사용자 환경이 설치하려고 선택한 제품의 설치 및 구성에 필요한 최소 요구 사항에 만족하는지 확인합니다. 경고 플래그가 지정된 항목 및 수동 검사가 필요한 항목은 수동으로 확인해야 합니다. 이러한 검사 수행에 대한 자세한 내용을 보려면 해당 항목을 누른 다음 창 하단 상자에 표시되는 세부 정보를 검토하십시오.
검사
유형
상태
Oracle 홈 비호환성을 확인하는 중...
자동
성공함
재시도
정지
0 요구 사항을 확인해야 합니다.
실제 결과: NEW_HOME
검사가 완료되었습니다. 이 검사에 대한 전반적인 결과: 성공함
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 요약
요약
Oracle Audit Vault Agent 10g 10.2.3.0.0
전역 설정
소스: C:\goodus\avagenttwin_x32\install\../stage/products.xml
Oracle 홈: C:\avgent(OraAV10g_home4)
설치 유형: 런타임
제품 언어
영어
한국어
공간 요구 사항
C:\ 817MB 필요(167MB 임시 포함): 38.03GB 사용 가능
새로 설치 (56 제품)
Agent Required Support Files 10.2.0.3.0
Assistant Common Files 10.2.0.3.0
Bali Share 1.1.18.0.0
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 설치
설치
Oracle Audit Vault Agent 10g 10.2.3.0.0 설치 중
'Oracle Universal Installer 10.2.0.4.0 '에 대한 파일 복사 중
설정 보류 중...
구성 보류 중...
'oui\bin\detachHome.bat' 복사 중
10%
설치 정지(S)...
Oracle Audit Vault
• Database-wide auditing solution for compliance and security
• Consolidate all of your audit data into a centralized location
• Detect and prevent insider threats
• Protect and secure your audit data
1
다음 위치에서 이 설치 세션의 로그를 찾을 수 있음:
C:\Program Files\Oracle\Inventory\logs\installActions2010-12-28_05-28-37PM.log
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE

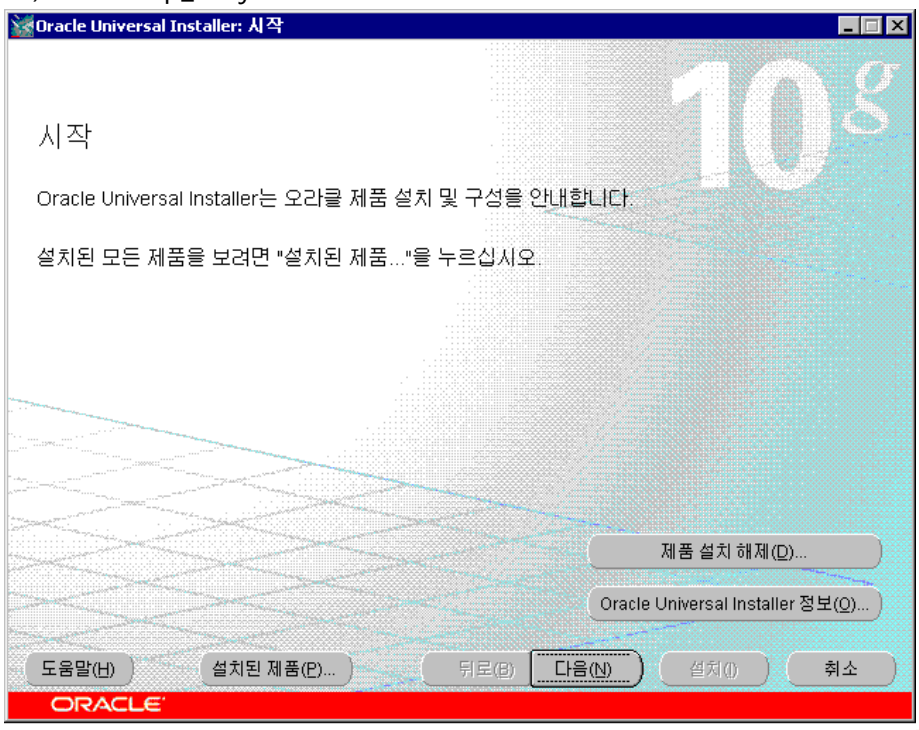

Oracle Universal Installer: Configuration Assistant
Configuration Assistant
다음 Configuration Assistant가 이전에 선택한 구성 요소를 구성하고 시작합니다.
툴 이름
상태
유형
Oracle Audit Vault Agent 10g
Oracle Audit Vault Agent One-Off Patches
진행 중...
권장됨
Oracle Audit Vault Configuration Assistant
보류 중...
권장됨
재시도(R)
정지(S)
세부 정보(C:\Program Files\Oracle\Inventory\logs\installActions2010-12-15_05-48-06PM.log의 전체 로그 참조):
Y (auto-answered by -silent)
User Responded with: Y
복원에 대해 'NApply' 패치의 영향을 받는 파일을 백업하는 중입니다. 이 작업은 약간의 시간이 걸릴 수 있습니다.
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE

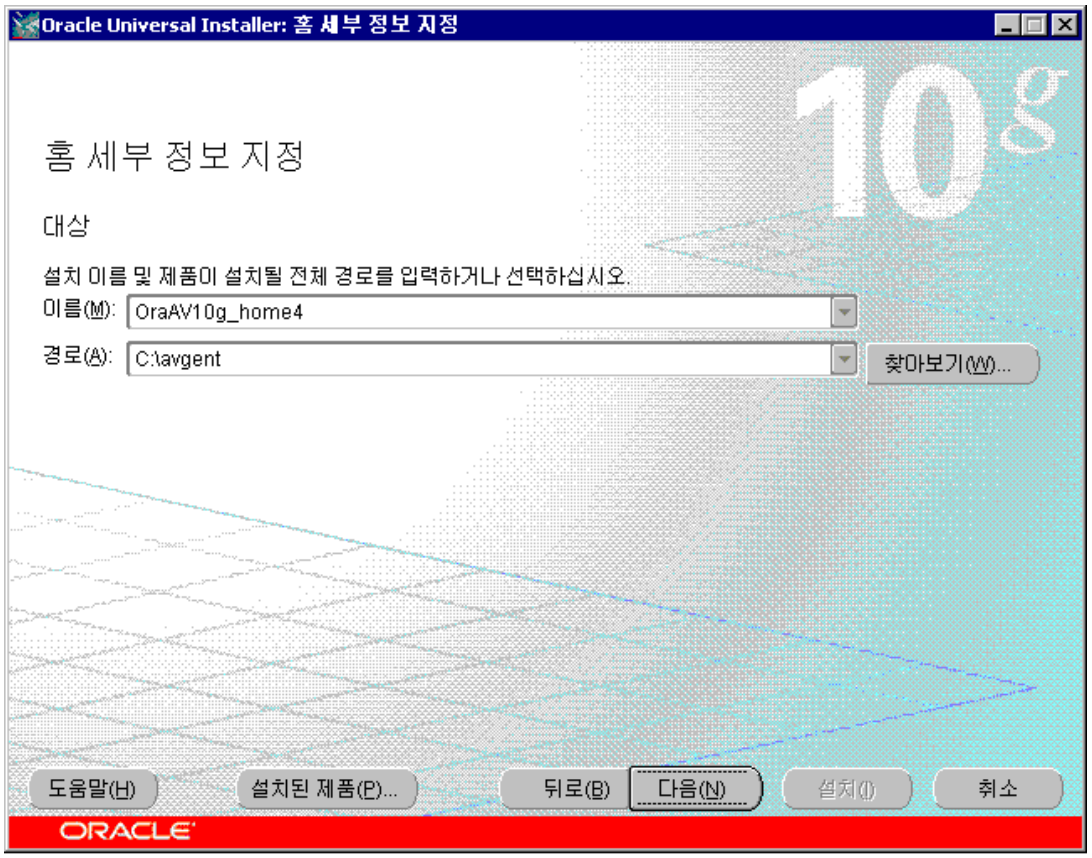


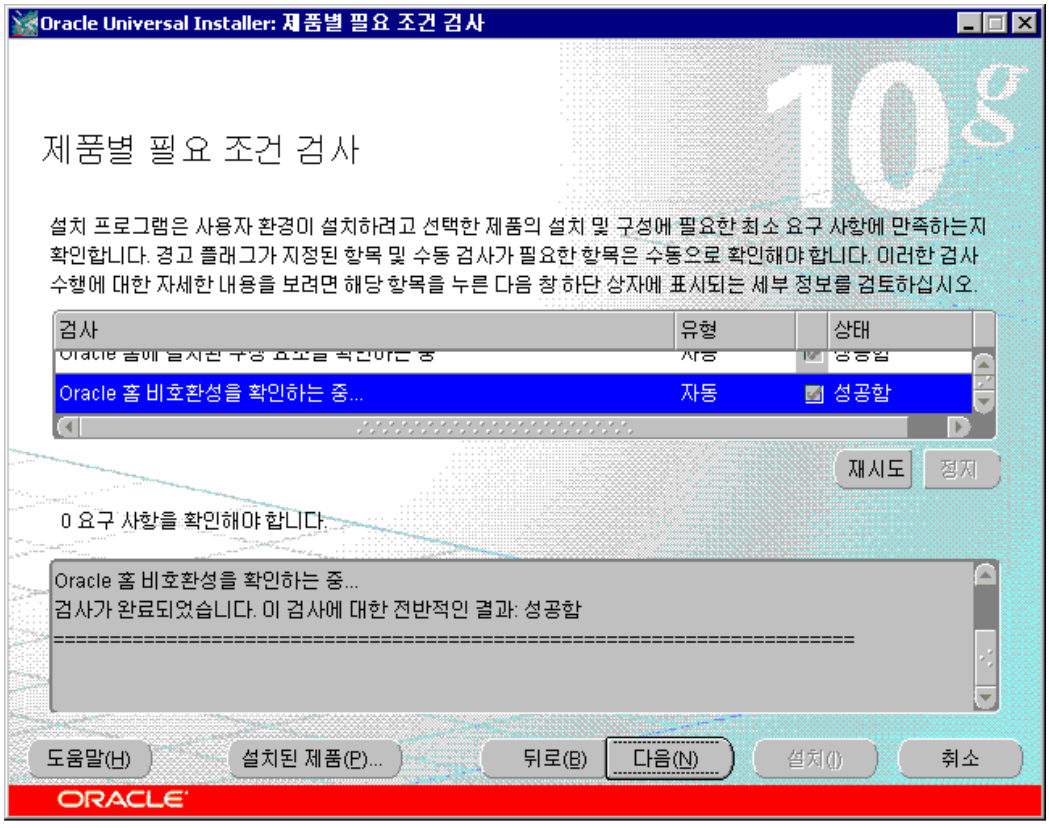
8. Installing the Oracle Audit Vault Patch Set on the Audit Vault Agent

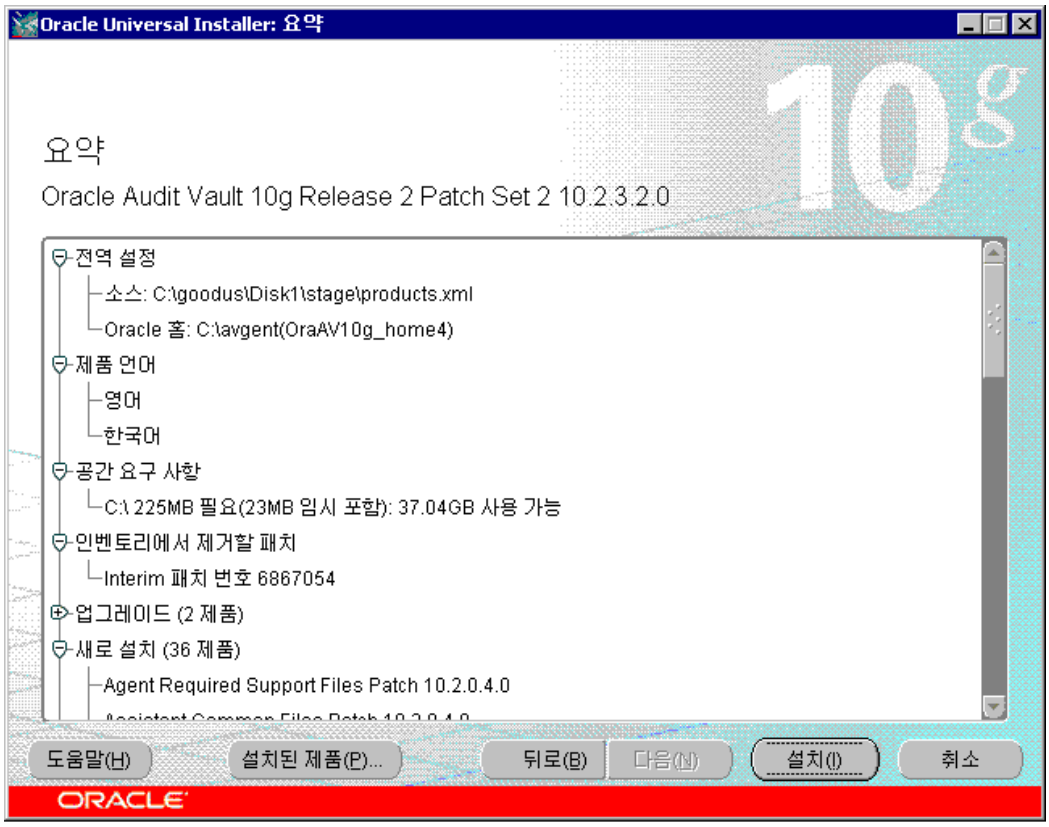
선행작업으로 Audit Vault Agent Service 를 정지 시키고 진행하여야 합니다.

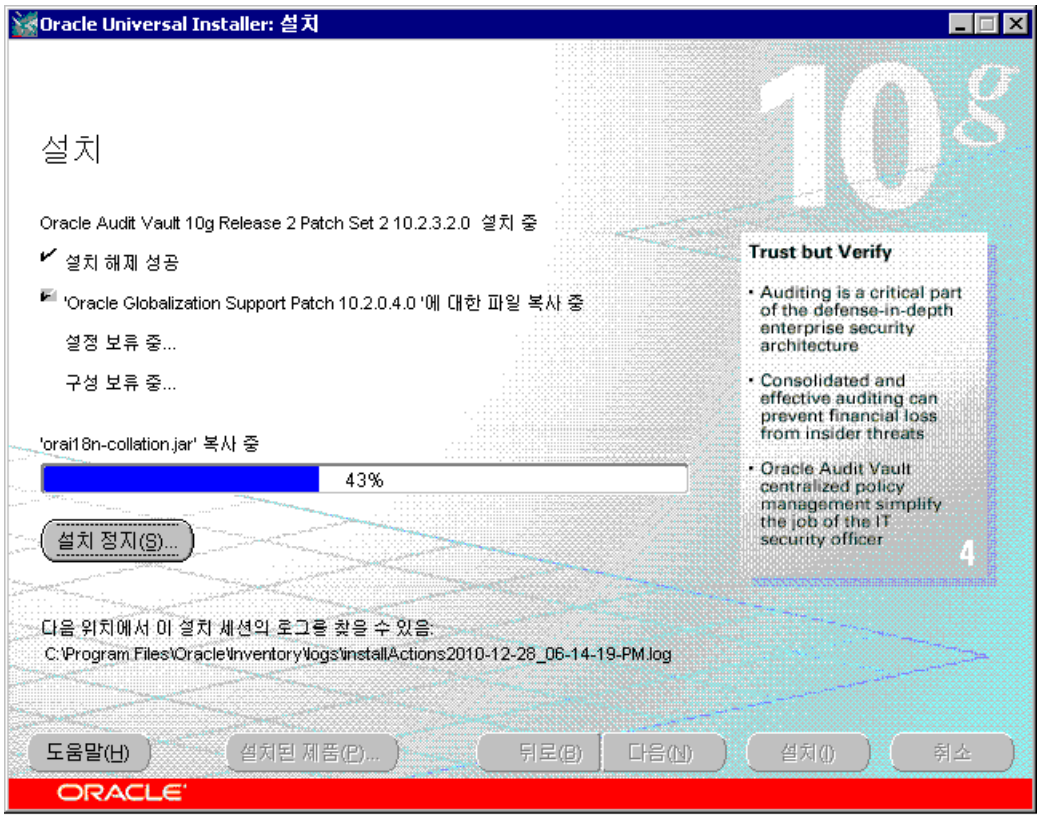
Ex) avctl stop_oc4j

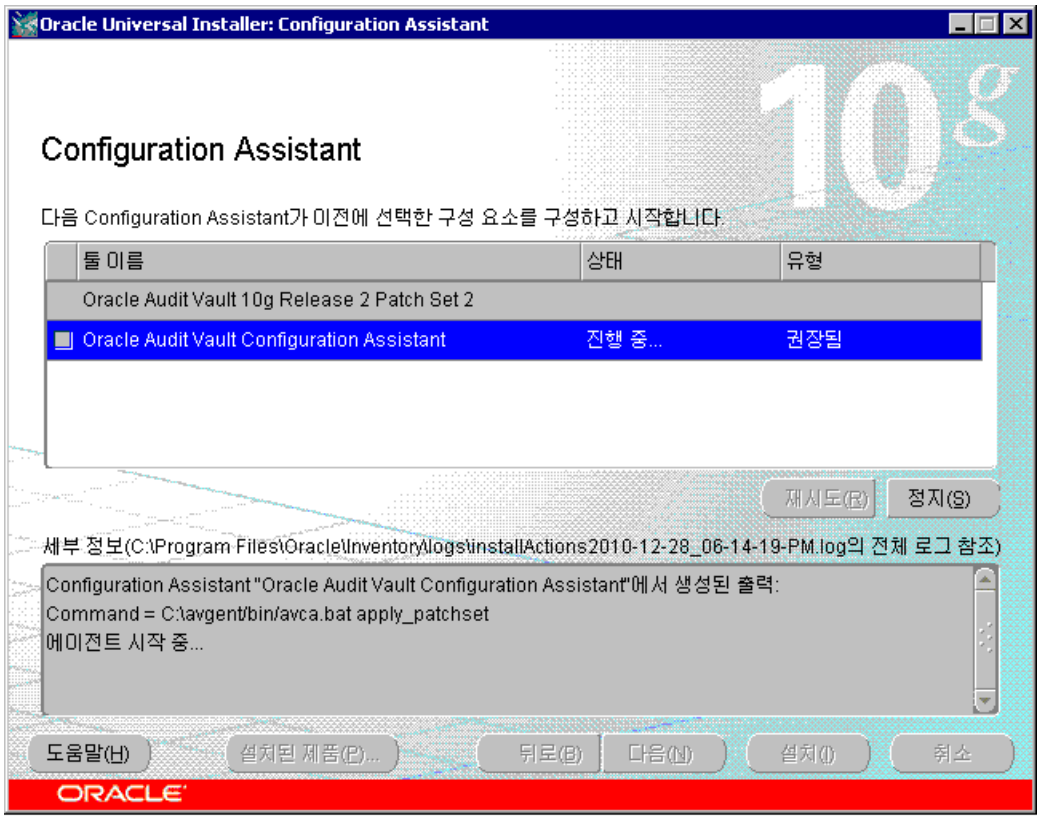


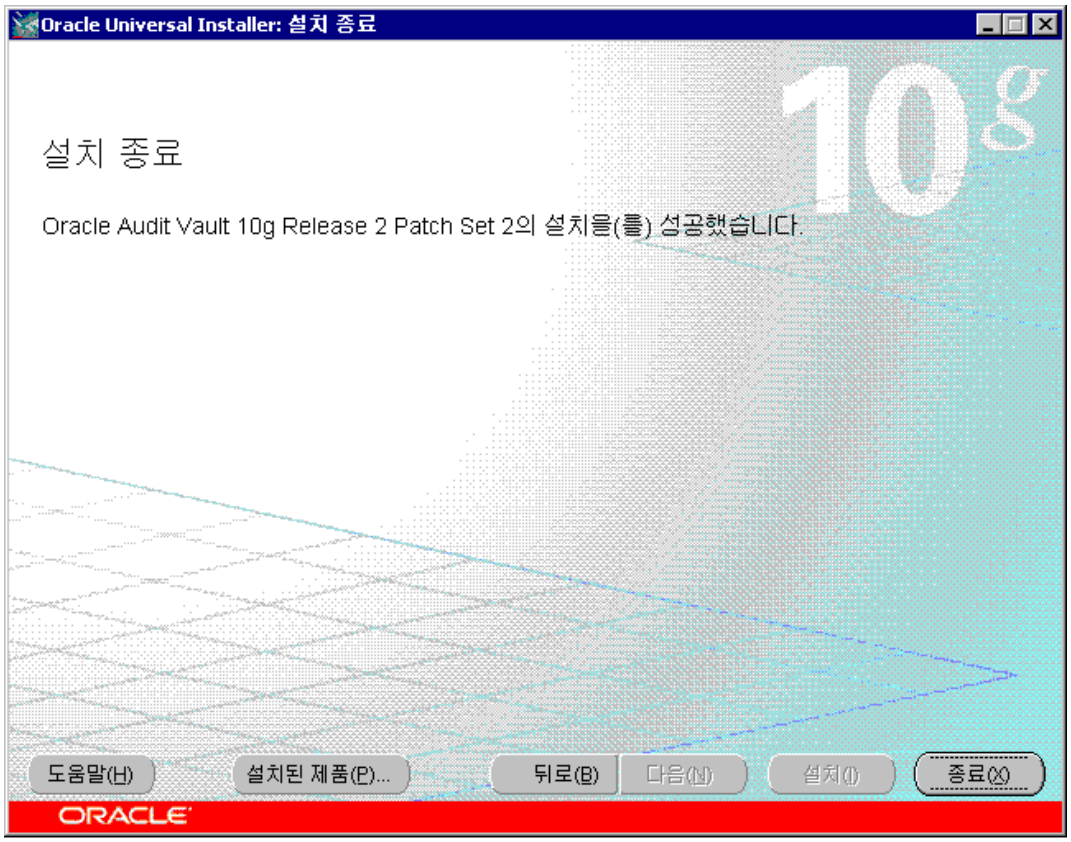

Oracle Universal Installer: 홈 세부 정보 지정
홈 세부 정보 지정
대상
설치 이름 및 제품이 설치될 전체 경로를 입력하거나 선택하십시오.
이름(M): OraAV10g_home4
경로(A): C:\avgent
찾아보기(W)...
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 제품별 필요 조건 검사
제품별 필요 조건 검사
설치 프로그램은 사용자 환경이 설치하려고 선택한 제품의 설치 및 구성에 필요한 최소 요구 사항에 만족하는지 확인합니다. 경고 플래그가 지정된 항목 및 수동 검사가 필요한 항목은 수동으로 확인해야 합니다. 이러한 검사 수행에 대한 자세한 내용을 보려면 해당 항목을 누른 다음 창 하단 상자에 표시되는 세부 정보를 검토하십시오.
검사
유형
상태
Oracle 홈 비호환성을 확인하는 중...
자동
성공함
재시도
정지
0 요구 사항을 확인해야 합니다.
Oracle 홈 비호환성을 확인하는 중...
검사가 완료되었습니다. 이 검사에 대한 전반적인 결과: 성공함
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 요약
요약
Oracle Audit Vault 10g Release 2 Patch Set 2 10.2.3.2.0
전역 설정
소스: C:\goodus\Disk1\stage\products.xml
Oracle 홈: C:\avgent(OraAV10g_home4)
제품 언어
영어
한국어
공간 요구 사항
C:\ 225MB 필요(23MB 임시 포함): 37.04GB 사용 가능
인벤토리에서 제거할 패치
Interim 패치 번호 6867054
업그레이드 (2 제품)
새로 설치 (36 제품)
Agent Required Support Files Patch 10.2.0.4.0
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 설치
설치
Oracle Audit Vault 10g Release 2 Patch Set 2 10.2.3.2.0 설치 중
설치 해제 성공
'Oracle Globalization Support Patch 10.2.0.4.0 '에 대한 파일 복사 중
설정 보류 중...
구성 보류 중...
'orai18n-collation.jar' 복사 중
43%
설치 정지(S)...
다음 위치에서 이 설치 세션의 로그를 찾을 수 있음:
C:\Program Files\Oracle\Inventory\logs\installActions2010-12-28_06-14-19-PM.log
Trust but Verify
Auditing is a critical part of the defense-in-depth enterprise security architecture
Consolidated and effective auditing can prevent financial loss from insider threats
Oracle Audit Vault centralized policy management simplify the job of the IT security officer
4
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: Configuration Assistant
Configuration Assistant
다음 Configuration Assistant가 이전에 선택한 구성 요소를 구성하고 시작합니다.
툴 이름
상태
유형
Oracle Audit Vault 10g Release 2 Patch Set 2
Oracle Audit Vault Configuration Assistant
진행 중...
권장됨
재시도(R)
정지(S)
세부 정보(C:\Program Files\Oracle\Inventory\logs\installActions2010-12-28_06-14-19-PM.log의 전체 로그 참조)
Configuration Assistant "Oracle Audit Vault Configuration Assistant"에서 생성된 출력:
Command = C:\avgent\bin\avca.bat apply_patchset
에이전트 시작 중...
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
취소
ORACLE


Oracle Universal Installer: 설치 종료
설치 종료
Oracle Audit Vault 10g Release 2 Patch Set 2의 설치을(를) 성공했습니다.
도움말(H)
설치된 제품(P)...
뒤로(B)
다음(N)
설치(I)
종료(X)
ORACLE

9. Registering Source Database and Collectors

이제 감사데이터 수집 및 레포팅을 위한 Source_DB + AV_Agent + AV_Server 의 설정 작업을 진행합니다.

9.1. Registering Oracle Database Sources and Collectors

9.1.1. Step 1 : Create a User Account on the Oracle Source Database

Source DB 에 연결할 사용자를 생성합니다. Source DB 에서 user 생성 후 SYS user 로 zarsspriv.sql 을 돌립니다. 이 script 는 source_db 사용자가 감사데이터의 수집 활성화 하는데 필요한 권한을 부여합니다. $ORACLE_HOME/av/scripts/streams/source 에 있습니다.
아래의 Enter value for 2 의 값은 Collector mode 로 SETUP 는 OSAUD,DBAUD Collectors 를 의미하고 REDO_COLL 는 REDO+SETUP MODE 를 의미 합니다.
입력은 대문자로 입력해야 합니다.

- source_db

```
create user srcuser_new identified by srcuser;
@zarsspriv.sql
Enter value for 1 : srcuser_new
Enter value for 2 : REDO_COLL or SETUP
```

DB vault 설치되어 있으면 Vault 계정으로 다음과 같은 추가 작업이 필요합니다.

```
EXEC DBMS_MACADM.ADD_AUTH_TO_REALM('Oracle Data Dictionary', 'SRCUSER_
NEW', null, dbms_macutl.g_realm_auth_participant);
commit;
grant dv_secanalyst to srcuser_new
```

9.1.2. Step 2 : Verify That the Source Database Is Compatible with the Collectors

Source DB 에서 감사데이터 수집에 이상이 있는지 AV Server or Collection agent 에서 검사 합니다.
아래의 과정에서 나오는 문제점들은 모두 적용 후 다음 Step 로 넘어가야 합니다.
-src 의 정보는 source_DB 의 정보입니다.

- av_server

```
avorcldb verify -src goodus:1521:audit -colltype ALL
소스 사용자 이름 입력: srcuser_new
소스 비밀번호 입력:
AV 소스가 OS File Audit Collector 수집기에 대해 확인되었습니다.
AV 소스가 Aud$/FGA_LOG$ Audit Collector 수집기에 대해 확인되었습니다.
```

매개변수 UNDO_RETENTION = 900 이(가) 권장 값 범위 [3600 - ANY_VALUE]에 있지 않습니다.
매개변수 GLOBAL_NAMES = false 이(가) 권장 값 true(으)로 설정되지 않았습니다.
AV 소스가 REDO Log Audit Collector 수집기에 대해 확인되었습니다.

9.1.3. Step 3 : Register the Oracle Source Database with Oracle Audit Vault

Audit 대상 source DB 와 agent 의 mapping 관계를 설정하면 AV Server 에서 작업합니다.
- av_server
avorcldb add_source -src goodus:1521:audit -srcname lee -agentname avgent_new
소스 사용자 이름 입력: **srcuser_new**
소스 비밀번호 입력:
소스 추가 중...
소스가 성공적으로 추가되었습니다.
avctl 에 사용할 수 있도록 다음 정보를 기억하십시오.
Source name (srcname): **lee**
인증서가 성공적으로 저장되었습니다.
에이전트에 소스 매핑 중...
-> srcname 나옴
-> srcname 부분 처음엔 안써도 되지만 다시 한다면 이름 지정해야 합니다
-> audit_vault em 구성-감사소스-소스 부분에 추가됩니다.
-> AV Server 의 tnsnames.ora 에 tnsalias 가 추가됩니다.
Alias for lee
SRCDB2 =
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=goodus)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=audit)))

9.1.4. Step 4 : Add the Oracle Collectors to Oracle Audit Vault

AV agent Collector 를 추가합니다. AV Server 에서 작업합니다.
DBAUD collector 추가하기(av_server)
- av_server
avorcldb add_collector -srcname lee -agentname avgent_new -colltype DBAUD
lee 소스가 Aud$/FGA_LOG$ Audit Collector 수집기에 대해 확인되었습니다.
수집기 추가 중...
수집기가 성공적으로 추가되었습니다.
avctl 에 사용할 수 있도록 다음 정보를 기억하십시오.

Collector name (collname): DBAUD_Collector

-> collname 나옴

-> audit_vault em 구성-감사소스-수집기 부분에 추가/관리-수집기 에도 추가됩니다.

9.1.5. Step 5 : Enagle the Audit Vault Agent to Run the Oracle Database Collectors

AV agent 와 Source DB 와 연결합니다. AV Agent 가 설치된 곳에서 작업합니다.

- av_agent

avorcldb setup -verbose -srcname lee

srcuser_new

srcuser1

인식할 수 없는 인수 -verbose 이(가) 무시되었습니다.

소스 사용자 이름 입력: **srcuser_new**

소스 암호 입력:

사용자 srcuser_new 에 대한 인증서를 [SRCDB2] 접속을 위해 추가하는 중입니다.

전자 지갑에 사용자 인증서 저장 중...

Create credential oracle.security.client.connect_string3

완료되었습니다.

[SRCDB2] 별칭을 사용하는 tnsnames.ora 를 소스 데이터베이스로 갱신했습니다.

전자 지갑을 사용하여 SRCDB2 접속을 확인하는 중입니다.

→ $AV_AGENT/network/admin/tnsnames.ora 에 [SRCDB2] alias 가 추가됨

9.1.6. Step 6: Collector start

- av_server

avctl start_collector -collname DBAUD_Collector -srcname lee

10. Oracle Audit Vault Start

10.1. Oracle Audit Vault Service start

1. Source DB

Lsnrctl start

DB startup

2. AV agent

Avctl start_agent

3. AV server

Lsnrctl start

DB startup

Avctl start_av

Oracle Audit Vault server 전체를 중단할 때는 반대의 순서로 명령어를 수행하면 됩니다.

10.2. Connection to Oracle Audit Vault

정상적으로 설치가 완료되고 위와 같이 정상적으로 Audit Vault service 를 시작했다면 다음과 같은 명령어를 통해 URL 확인 후 Internet Explorer 을 통해 접속 할 수 있습니다.

- av_server

C:₩Documents and Settings₩Administrator>**avctl show_av_status**

Oracle Audit Vault 10g Database Control Release 10.2.3.2.0

Copyright (c) 2006, 2009 Oracle Corporation. All rights reserved.

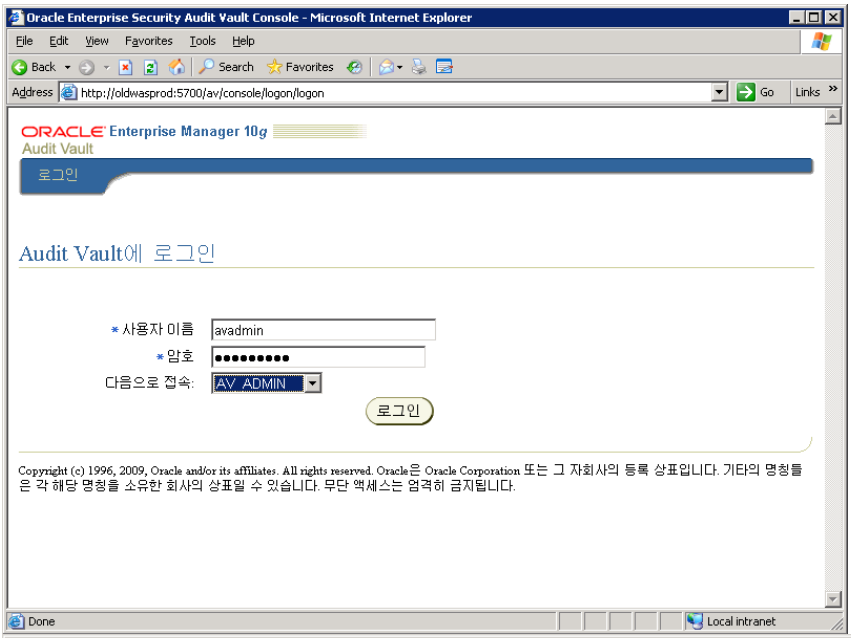
http://oldwasprod:5700/av --> AV server 용 web 관리화면

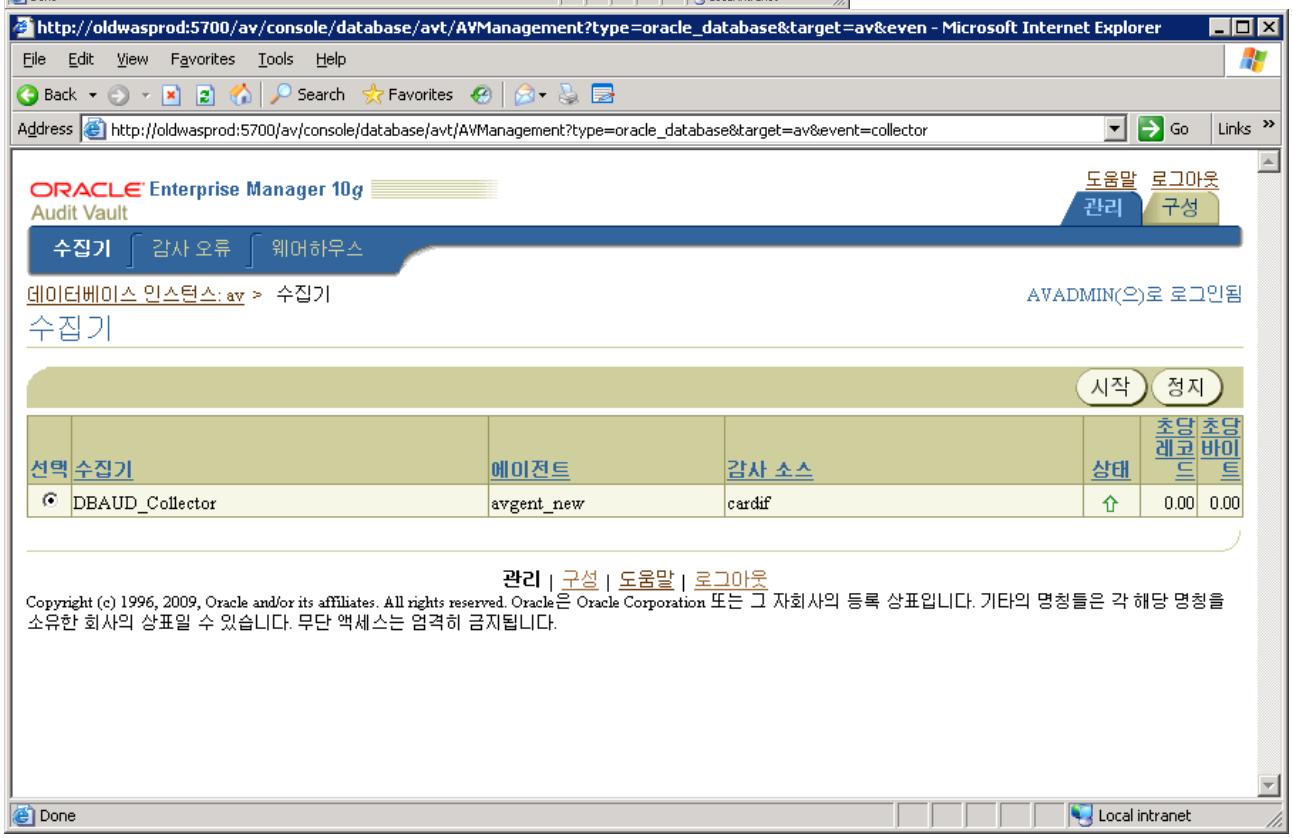
Oracle Audit Vault 10g is running.

로그는 디렉토리에 생성됩니다. C:₩oracle₩av₩log

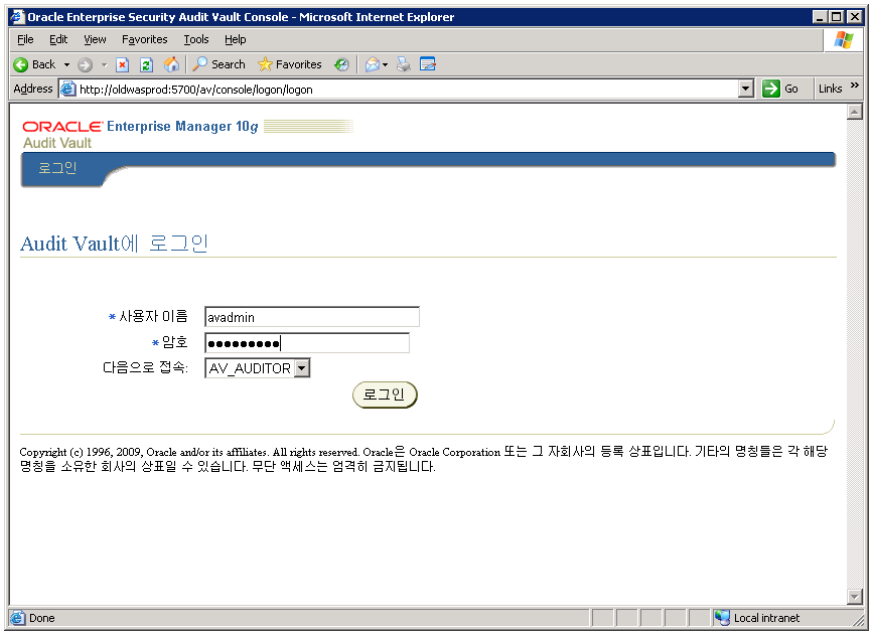
C:₩Documents and Settings₩Administrator>

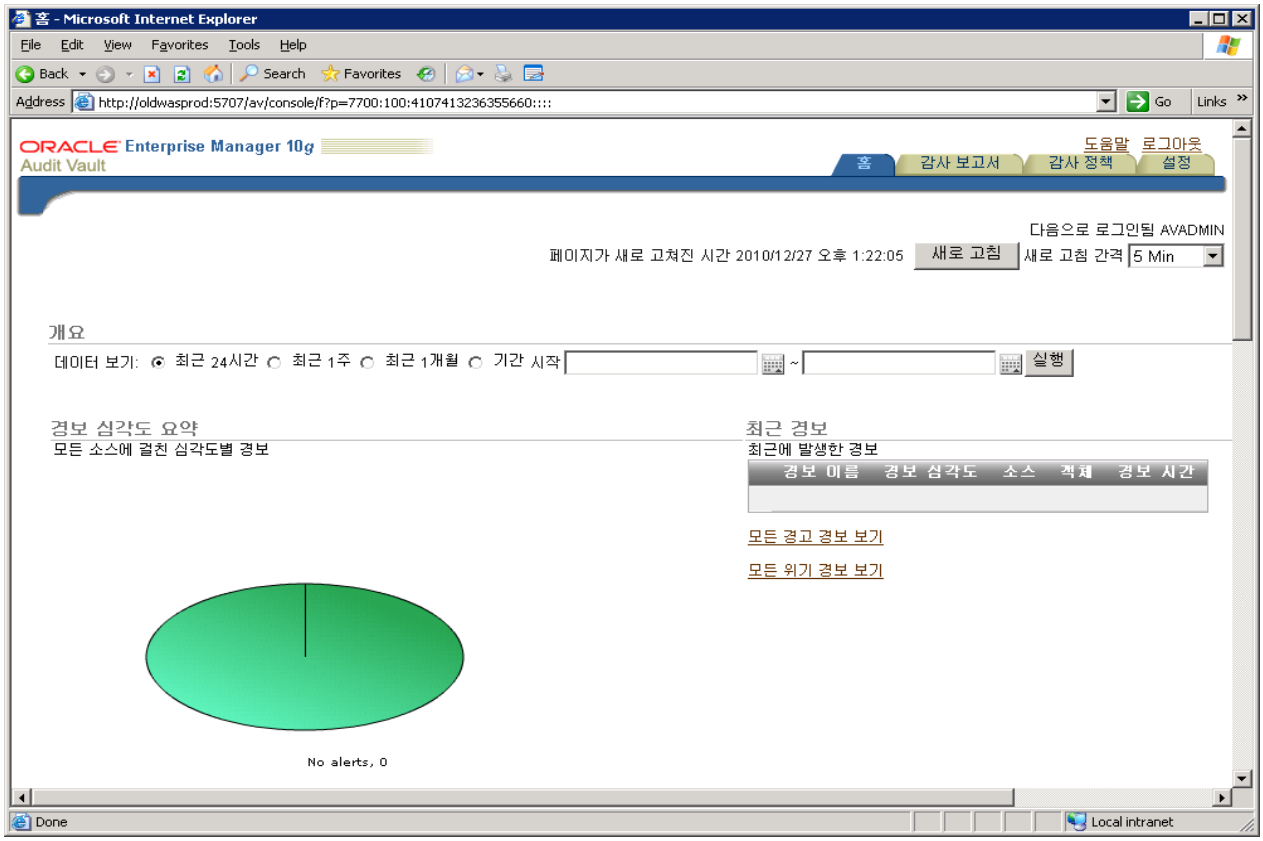
→**AV_ADMIN** 권한으로 접속하면 에이전트, 수집기, 감사오류, 웨어하우스등에 대한 관리/구성 작업을 할 수 있습니다.





→ **AV_AUDITOR** 권한으로 접속하면 감사보고서 확인, 감사정책 수립, 감사보고서 생성 등의 작업을 할 수 있습니다.





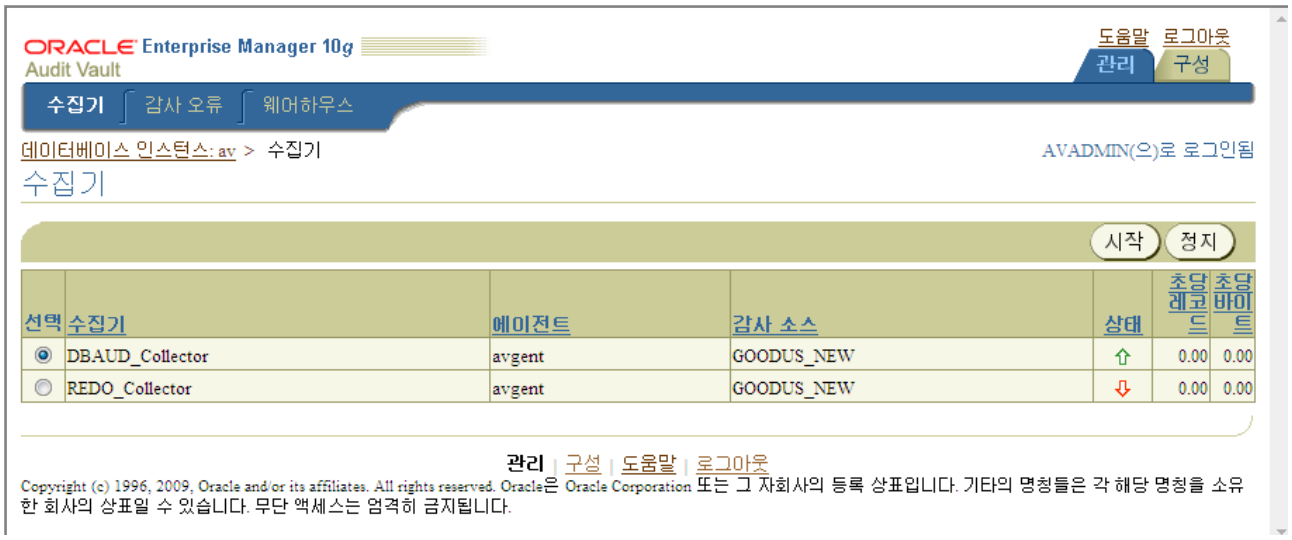
11. Creating Audit Vault Policies

Source DB 에서 감사정보를 생성하기 위해서는 다음 파라메터 값이 설정되어 있어야 합니다.

파라메터 값	설명
DB	시스템 감사 테이블 (AUD$, FGA_LOG$) 에 감사 정보 기록
DB, EXTENDED	DB 파라메터 설정과 동일 추가로, SQL Bind 내용과 전체 SQL 문장 감사 기록 추가
OS	운영체제 파일로 감사 정보 기록
XML	XML 파일 형태로 감사 정보 기록
XML, EXTENDED	XML 파라메터 설정과 동일 추가로, SQL Bind 내용과 전체 SQL 문장 감사 기록 추가
NONE	감사 정보 생성하지 않음

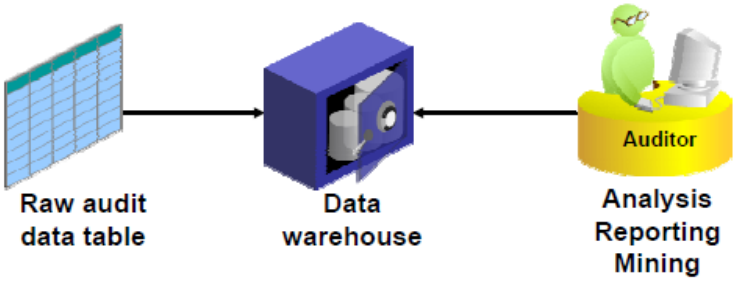
11.1. Step 1 : Collector Status Check

해당 Collector 가 running 상태인지 check 합니다. Down 상태일 시 시작버튼을 눌러 Collector 를 시작시킵니다.



11.2. Step 2 : Data Warehouse

Collector 가 수집한 감사정보는 물리적 형식과 포맷이 다르므로 사전에 이를 처리하는 과정이 필요합니다. 이러한 작업을 데이터웨어하우스 작업이라고 부릅니다.
로드작업에서 시작날짜, 일 수를 입력합니다.

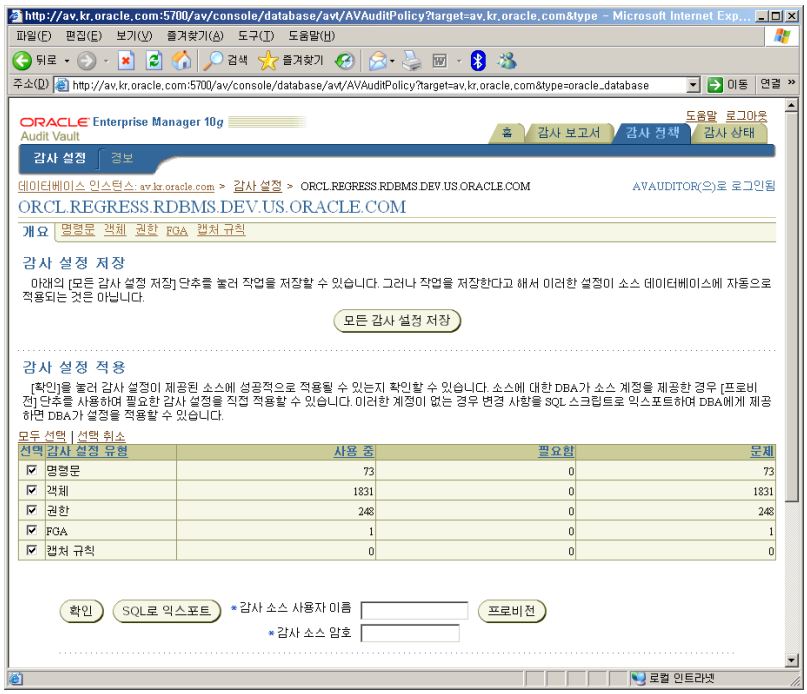


11.3. Step 3 : Audit Setup

Data warehouse 작업이 끝나면 아래와 같이 감사소스 링크가 활성화 됩니다.

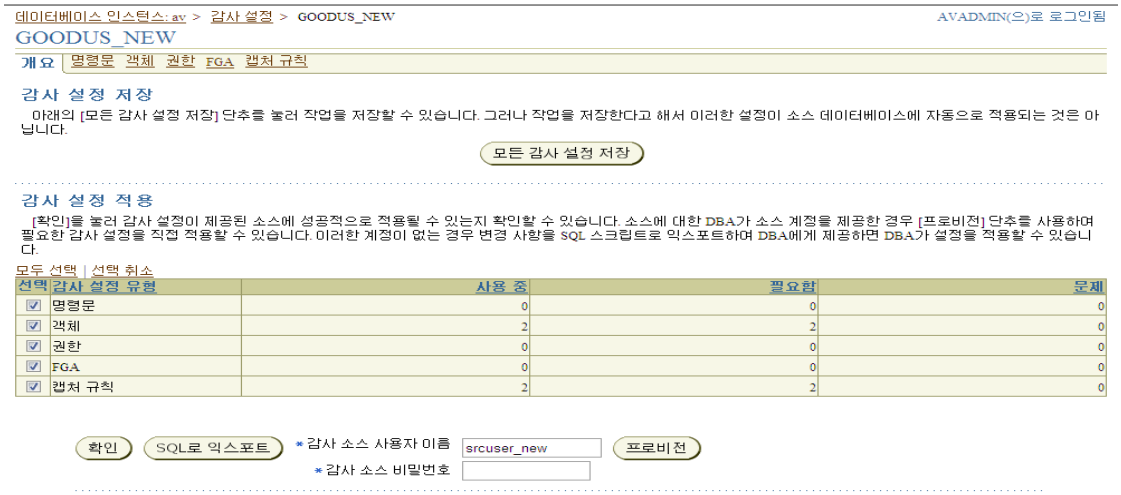
위 링크를 들어가면 아래 그림처럼 해당 Source DB 에 대한 감사 설정 사항들을 자세히 확인할 수 있습니다.

각각 명령문, 객체, 권한, FGA, 캡쳐규칙 등의 특성으로 감사 정책을 수립할 수 있습니다.



11.4. Step 4 : Audit Start

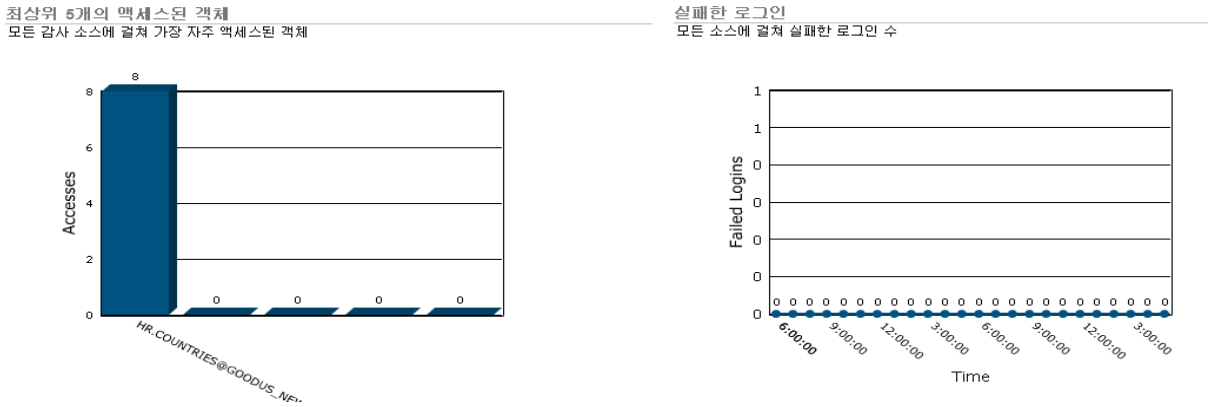
감사정책 생성이 끝난 후에 모든 감사 설정 저장 버튼과 감사 소스 사용자 이름과 비밀번호 입력 후 프로비전 버튼을 적용해야 활성화가 됩니다.



12. Using Audit Vault Reports

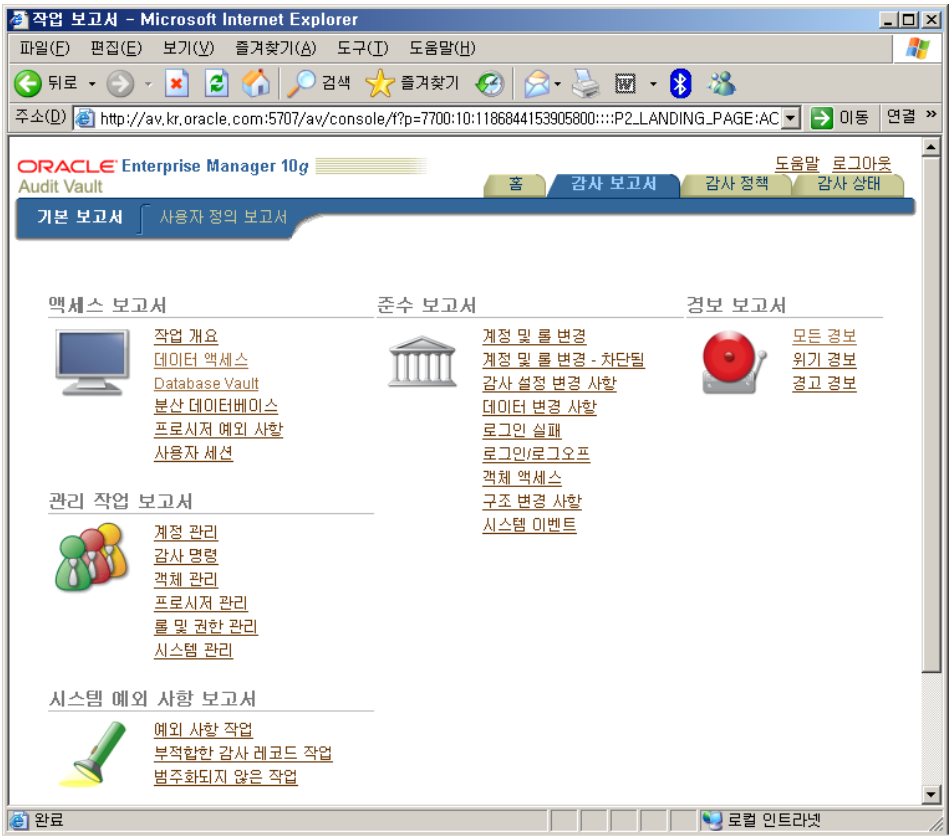
12.1. Enterprise Manager 메인화면에서 확인

실시간으로 audit 되는 정보들을 EM 을 통해서 확인할 수 있습니다.

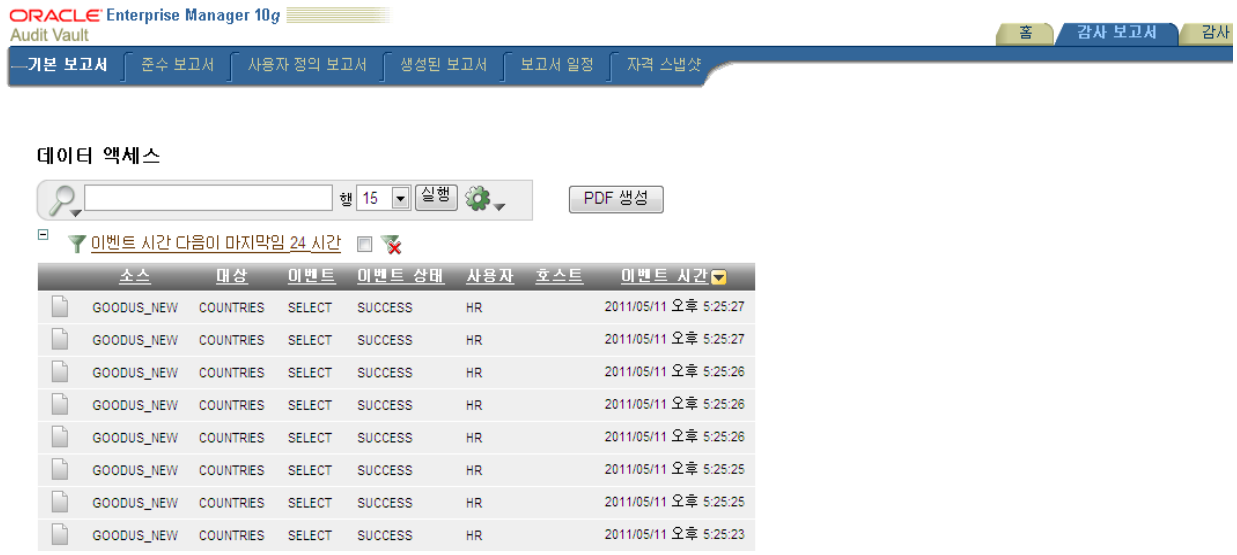


12.2. 감사데이터 조회

아래 그림과 같이 다양한 레포트 형태들을 제공합니다.



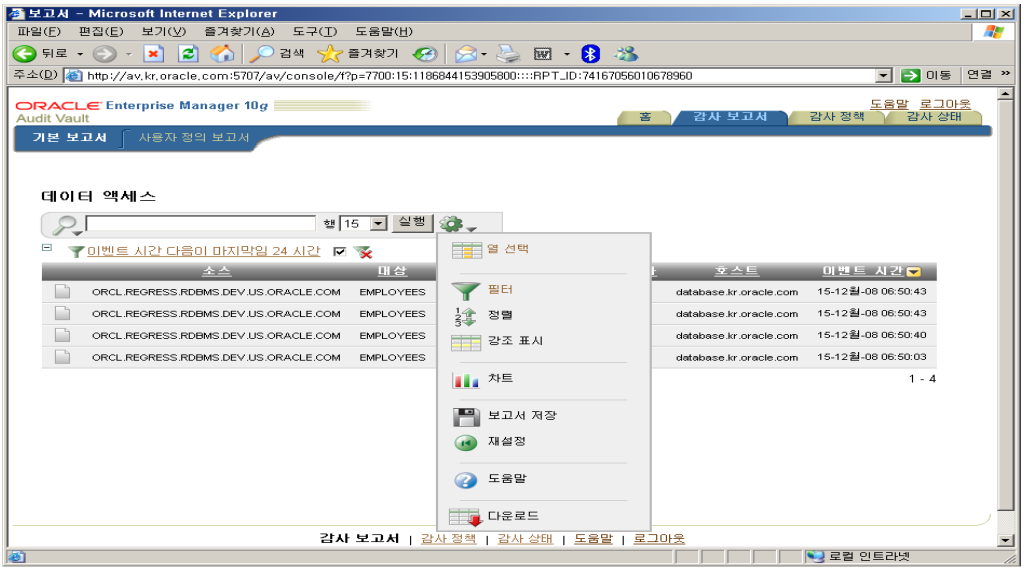
다음은 EM 화면의 감사보고서 – 기본보고서에서 확인된 감사 데이터 입니다.. 이 외 audit vault 에서 제공하는 여러 레포트 형식으로 감사데이터를 레포트 형태로 추출 가능합니다.

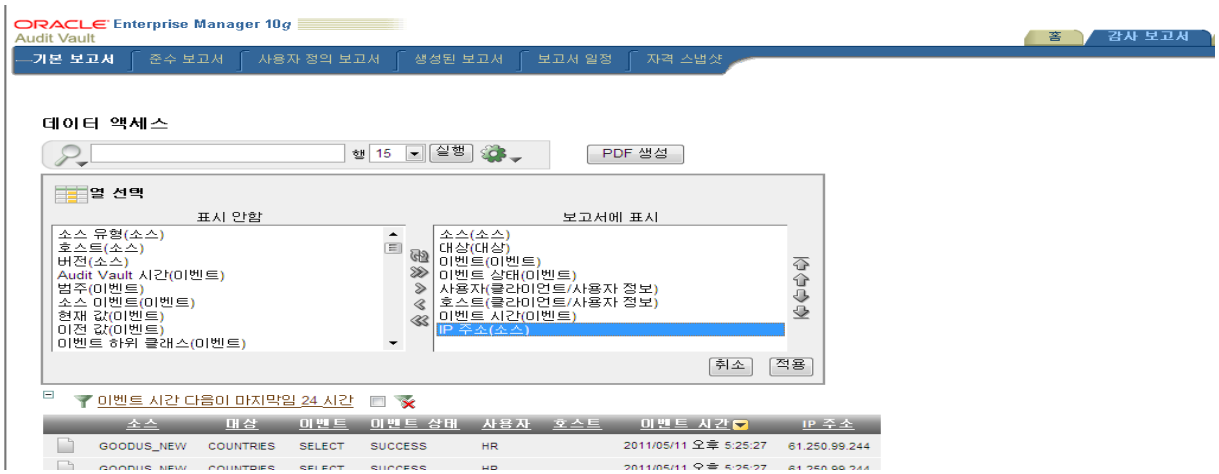


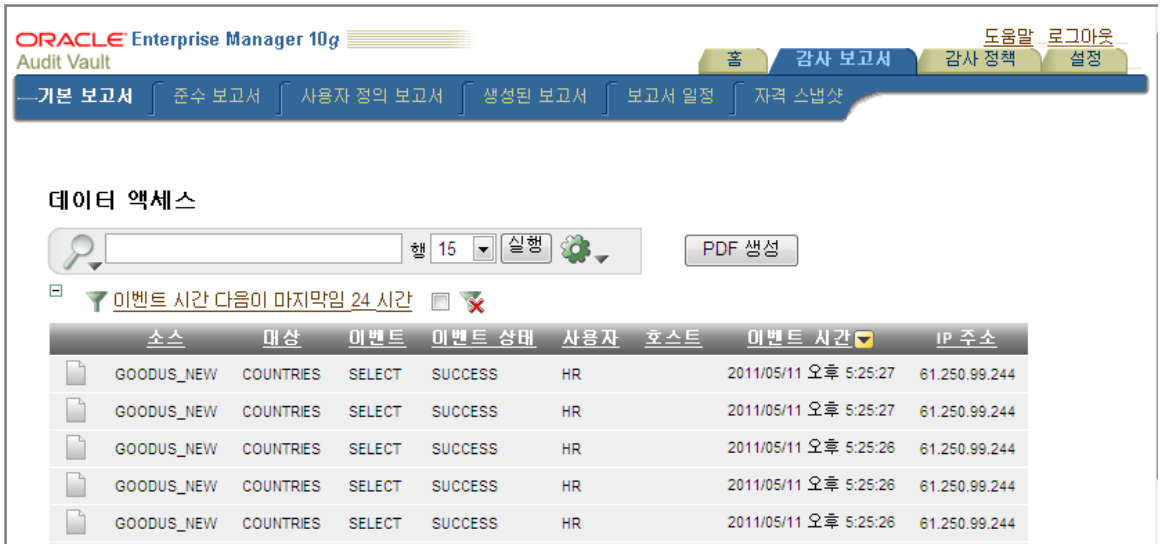
12.3. 추가 정보 조회

기본 정보 이외의 추가적인 정보를 조회할대는 아래와 같이 톱니바퀴 버튼 클릭 후 열선택 메뉴를 통해 원하는 정보를 추가할 수 있습니다.

아래의 예제는 IP 주소를 추가한 경우 입니다.







13. Audit Vault Logfile

Audit Vault Server 와 Agent 에서 생성되는 logfile 을 참고하여 Audit Vault 의 운영상황과 문제점, 오류등을 확인 할 수 있어 구성 및 운영 시 많은 도움을 줍니다.

13.1. Audit Vault Server Logfile

<Audit_Vault_Server_Home>/av/log. 디렉토리에 다음과 같은 log file 들로 관리 합니다.

Server Log File Names	Description	Maintenance
avorcldb.log	avorcldb 명령어를 통해 수행된 작업을 기록, 초기에 source, audit vault agents, collectors 구성 log 들	언제든지 삭제해도 무방함
avca.log	Audit vault agnet 와 collecotr 의 시작 및 정지에 대한 log 들	AV 서버가 shutdown 되어 있을 때에만 삭제해야 함
av_client-%g.log.n	수집기의 동작과 관련된 정보 기록 (%g 는 0 부터 시작되는 일련번호로 10MB 단위로 새롭게 생성)	언제든지 삭제해도 무방함

13.2. Audit Vault Collection Agent Logfile

<Audit_Vault_Collection_Agent_Home>/av/log. 디렉토리에 다음과 같은 log file 들로 관리 합니다.

Server Log File Names	Description	Maintenance
agent.err	에이전트 초기화 과정에서의 오류 기록	언제든지 삭제해도 무방함
agent.out	에이전트와 관련된 작업 및 수행 결과에 대한 정보 기록	AV Collection Agent 가 shutdown 되어 있을 때에만 삭제해야 함
avca.log	avca 명령어 수행과 결과를 기록	언제든지 삭제해도 무방함
avorcldb.log	avorcldb 명령어 수행과 결과를 기록	언제든지 삭제해도 무방함
<C><S><SID>.log C = 수집기명 S = 소스명 SID = 소스 아이디	DBAUD, OSAUD 수집기에 의한 작업 내용을 기록	AV Collection Agent 가 shutdown 되어 있을 때에만 삭제해야 함
av_client-%g.log.n	수집기의 동작 및 에러와 관련된 정보 기록	언제든지 삭제해도 무방함

	(%g 는 0 부터 시작되는 일련번호로 10MB 단위로 새롭게 생성)	
sqlnet.log	SQL*Net 정보에 대한 로그	-

14. Database Auditing Performance

Oracle Audit Vault Best Practices 의 auditing performance 결과에 따르면 아래처럼 초당 10 건 인 audit data 와 초동 100 건의 audit data 가 생성되는 동안 각각의 collector 의 부하정도는 5%내외 정도 였다. 하지만 audit vault server, source DB, audit vault agent 의 server spec 및 audit data 의 정도에 따라 performance 에 영향을 끼치므로 꾸준한 monitoring 이 필요합니다.

	10 audit/sec		100 audit/sec	
	Create;	Collect	Create;	Collect
OS Log	0.03%;	0.7% (c)	0.07%,	2.7% (c)
DB Audit	0.29%;	0.5% (c)	2.4%;	1.7% (c)
Redo	0;	3.7% (c)	0;	5.9% (c)

15. 맺음말

강력한 감사 기능의 구축은 데이터 암호화, 접근제어와 더불어 기업의 정보와 개인정보 보호를 위해 꼭 필요한 시스템 중 하나 입니다. 실제 보안 사고가 발생했다고 했을 때, 신속하고 신뢰성 있게 사고 원인과 과정을 파악할 수 있도록 해 줍니다.

또한 점점 강화되고 있는 보안 규제 준수에 효과적으로 대처하고 대내외적 위협 요소로 부터 기업의 자산을 안전하게 보호하기 위해서는 구현 비용이나 성능상 많은 문제점 및 어려움을 안고 있습니다

이에 오라클 데이터 베이스 보안 솔루션인 Audit Vault 는 기존 운영 환경 및 서비스와 호환성을 유지하며 성능 저하 및 과도한 비용 소모를 효과적으로 줄일 수 있는 방안을 제시하여 효율적인 정보 보호 조치를 구현 할 수 있습니다.

16. Reference Documents

Availability of Oracle Audit Vault Server on Windows [ID 753920.1]

Master Note For Oracle Audit Vault [ID 1199033.1]

Oracle® Audit Vault Administrator's Guide Release 10.2.3.2 Part Number E14459-10

Oracle® Audit Vault Auditor's Guide Release 10.2.3.2 Part Number E14460-05

Oracle® Audit Vault Server Installation Guide Release 10.2.3.2 for Microsoft Windows (32-Bit) Part Number E14467-03

Oracle® Audit Vault Collection Agent Installation Guide Release 10.2.3.2 Part Number E14457-05

Oracle® Audit Vault Release Notes Release 10.2.3.2 Part Number E11061-04