CAAT를 사용한 Oracle 데이터베이스 감사

Ian Cooke, CISA, CGEIT, COBIT-F, CFE, CPTS, DipFM, ITIL-F, Six Sigma Green Belt는 정보 시스템의 모든 사항에 있어서 25년의 경험을 가진 IT 감사 매니저로서 아일랜드의 더블린에 거주하고 있습니다. Cooke는 ISACA 지식 센터의 Oracle 데이터베이스, SQL 서버 데이터베이스 및 OS/400 주제 담당 리더로서 ISACA의 커뮤니티 위원회 회원입니다. *ian.j.cooke@gmail.com* 또는 ISACA 지식 센터의 Oracle 데이터베이스 주제 *(www.isaca.org/Groups/Professional-English/oracle-database/Pages/Overview.aspx)*를 통해 Cooke에게 의견이나 제안을 보낼 수 있습니다.

Oracle® 데이터베이스를 감사하기 위해 시장에는 다양한 보안 도구가 출시되어 있습니다.[1] 그러나, 이러한 도구가 실용적이지 않은 경우가 있습니다.

- 소규모 회사에는 비용이 걸림돌이 될 수 있습니다.
- 대형 지주 회사나 지리적으로 분산되어 있는 회사는 본사와 지사 사이에 완전한 네트워크 연결이 이루어져 있지 않을 수 있습니다.
- 외주 검토를 수행하는 컨설팅 회사에게는 완전한 데이터베이스 관리자(DBA) 권한과 이에 따른 관리자 암호를 필요로 하는 도구의 설치 또는 실행 권한이 부여되지 않을 수 있습니다. 또한, 감사를 받는 조직은 업무에 필수적인 데이터베이스에 어떠한 도구 또는 어떠한 영향이 발생할 것인지에 대한 관리를 못하고 있습니다.

이러한 경우에 Oracle 데이터베이스에서 직접 얻은 정보와 연계해서 컴퓨터 지원 감사 기술(CAAT)을 사용하여 Oracle 데이터베이스를 감사하는 것이 하나의 방법입니다.

ORACLE 데이터베이스

Oracle 데이터베이스는 메타데이터 또는 데이터를 위한 데이터를 포함하고 있습니다. 이것은 데이터 사전 및 데이터베이스 뷰에 포함되어 있습니다.

데이터 사전은 Oracle 데이터베이스 사용자, 이들의 권한, 역할 및 감사 정보 등을 포함하여, 데이터베이스의 모든 객체에 대한 정보를 제공합니다.

데이터 사전의 내용은 Oracle 데이터베이스 뷰를 통해 쿼리됩니다. 이러한 뷰는 기저의 테이블 데이터를 유용한 방법으로 표시합니다. 뷰 중에는 모든 데이터베이스 사용자가 접근 가능한 것이 있지만, 일부는 DBA로 제한됩니다. 이러한 뷰('DBA_' 접두어로 시작됨)는 데이터 사전에 저장되어 있는 정보를 포함하여 데이터베이스의 모든 관련 정보를 표시합니다. DBA 뷰의 전체 목록 및 이에 따른 세부적인 설명은 *Oracle Database Reference*에서 참조 가능합니다.[2]

Oracle 데이터베이스는 동적 성능 뷰도 관리하고 있습니다. 이것의 이름이 제시될 때마다 데이터베이스가 열려서 사용 중인 동안에 성능 정보가 지속적으로 업데이트됩니다. 동적 뷰의 이름은 'V$'로 시작됩니다. V$ 뷰의 전체 목록 및 이에 따른 세부적인 설명은 Oracle Database Reference에서 참조 가능합니다.

SQL*Plus는 모든 Oracle 데이터베이스 설치에 포함되어 있는 쿼리 도구입니다. 이것은 사용자가 SQL(Structured Query Language)을 사용해서 데이터베이스를 쿼리함으로써, 원하는 대로 출력 형식을 만들고 결과를 파일로 기록할 수 있도록 해줍니다(필요한 경우).

ORACLE 데이터베이스 뷰의 출력

그림 1에 있는 형식 및 구성 옵션을 사용하면 Oracle 쿼리 출력을 뷰의 내용과 함께 쉼표로 구분된 값(CSV) 텍스트 파일로 지정할 수 있습니다.

그림 1—SQL*Plus 형식 및 구성 명령

명령	설명
SPOOL	SPOOL은 쿼리 결과를 지정된 위치에 파일로 출력합니다. SPOOL OFF는 출력을 중지합니다.
SET LINES	새로운 행을 시작하기 전에 하나의 행에 표시될 수 있는 총 문자 수를 지정합니다.
SET TRIMSPOOL ON	스풀된 각 행의 끝에서 공백을 제거합니다.
SET PAGESIZE	출력되는 각 페이지에서 행의 수를 지정합니다. 제목은 각 '페이지'에 한 번만 나타납니다.
SET TIMING OFF	타이밍 정보가 출력되는 것을 방지합니다.
SET ECHO OFF	명령이 스크립트로 출력되는 것을 방지합니다.
SET FEEDBACK OFF	피드백 메시지를 방지합니다(예를 들어, 쿼리에 의해 반환된 레코드 수).
SET COLSEP	출력에서 열 사이에 인쇄되는 열 구분자를 설정합니다. CSV 형식 파일을 생성하는 경우, 이것은 일반적으로 쉼표(',')가 됩니다. 그러나, 출력에 쉼표가 포함되어 있는 경우, 이것은 출력에 나타나지 않는 다른 문자로 변경되어야 합니다(예를 들어, '|' 또는 '~').
SET UNDERLINE OFF	열 제목에 밑줄이 그어지는 것을 방지합니다.
SET NEWPAGE	0으로 설정되는 경우, 페이지 시작에서 0번 행을 건너 뜁니다.

그림 2는 스크립트의 출력 모양을 보여줍니다(전체 Oracle 스크립트는 ISACA® 지식 센터에서 다운로드 가능[3]). 생성된 스크립트는 DBA로 전달되어서 필요한 데이터베이스에 대해 실행될 수 있습니다. 각 뷰에 대해 하나의 CSV 파일이 생성됩니다.

그림 2—SQL 스크립트 형식 및 CSV 텍스트 파일로 출력

```
SET LINES 10000
SET TRIMSPOOL ON
SET PAGESIZE 10000
SET TIMING OFF
SET ECHO OFF
SET FEEDBACK OFF
SET COLSEP ","
SET UNDERLINE OFF
SET NEWPAGE 0

-- Get a list of profiles on the system
SPOOL dba_profiles.txt
SELECT *
FROM    dba_profiles;
SPOOL OFF

--Get a list of all users on the database
SPOOL dba_users.txt
SELECT *
FROM    dba_users;
SPOOL OFF

--Parameter file contains commas
SET COLSEP "!"

--Get a list of parameters
SPOOL V$PARAMETER.txt
SELECT *
FROM V$PARAMETER;
SPOOL OFF
```

ORACLE 데이터베이스 뷰의 분석

그 다음에 이러한 파일을 다음과 같은 CAAT 도구로 가져와서 분석 및 비교를 위해 다음과 같은 작업을 할 수 있습니다:

DBA_PROFILES

감사를 받는 실체는 암호를 설정하는 방법에 대한 정책을 가지고 있어야 합니다. Oracle 데이터베이스에서 암호 구성은 데이터베이스 프로파일(DBA_PROFILES) 뷰에 나타나 있습니다. 프로파일이란 사용자에 대한 데이터베이스 사용 및 인스턴스 리소스를 관리하는 자원의 한계와 암호 매개변수에 관해 명명된 세트입니다.[4] 즉, 지정된 프로파일은 사용자 계정에 적용되어 해당 사용자에 대한 실패한 로그인 시도 수, 암호 만료일 또는 암호 재사용 등과 같은 사항을 통제합니다.

전술한 바와 같이 이러한 뷰는 CSV 파일로 출력할 수 있습니다(**그림 2 참조**). DBA_PROFILES CSV 파일의 샘플 출력은 **그림 3**에 있습니다. 여기에서는 첫 번째 행이 Oracle 필드 이름을 보여줍니다. 이러한 필드 이름은 DBA_PROFILES 뷰에 대해 정의된 레이아웃과 관련이 있습니다(**그림 4**). 이러한 뷰에 대한 레이아웃 및 모든 Oracle 데이터베이스 뷰는 *Oracle Database Reference*에서 참조 가능합니다.

그림 3—DBA_PROFILES 샘플 출력

```
PROFILE..... ,RESOURCE_NAME.............,RESOURCE,LIMIT
DEFAULT..... ,COMPOSITE_LIMIT.............
,KERNEL..,UNLIMITED
DEFAULT..... ,SESSIONS_PER_USER...........
,KERNEL..,UNLIMITED
DEFAULT..... ,CPU_PER_SESSION.............
,KERNEL..,UNLIMITED
DEFAULT..... ,CPU_PER_CALL................
,KERNEL..,UNLIMITED
DEFAULT..... ,LOGICAL_READS_PER_SESSION....
,KERNEL..,UNLIMITED
DEFAULT..... ,LOGICAL_READS_PER_CALL.......
,KERNEL..,UNLIMITED
DEFAULT..... ,IDLE_TIME...................
,KERNEL..,UNLIMITED
DEFAULT..... ,CONNECT_TIME................
,KERNEL..,UNLIMITED
DEFAULT..... ,PRIVATE_SGA.................
,KERNEL..,UNLIMITED
DEFAULT..... ,FAILED_LOGIN_ATTEMPTS........,PASSWORD,5
DEFAULT..... ,PASSWORD_LIFE_TIME..........
,PASSWORD,UNLIMITED
DEFAULT..... ,PASSWORD_REUSE_TIME.........
,PASSWORD,UNLIMITED
DEFAULT..... ,PASSWORD_REUSE_MAX..........
,PASSWORD,UNLIMITED
DEFAULT..... ,PASSWORD_VERIFY_FUNCTION.....,PASSWORD,NULL
DEFAULT..... ,PASSWORD_LOCK_TIME..........
,PASSWORD,UNLIMITED
DEFAULT..... ,PASSWORD_GRACE_TIME.........
,PASSWORD,UNLIMITED
```

그림 4—DBA_PROFILES 뷰의 필드

열	데이터 유형	Null	설명
PROFILE	VARCHAR2(30)	NOT NULL	프로파일 이름
RESOURCE_ NAME	VARCHAR2(32)	NOT NULL	리소스 이름
RESOURCE_ TYPE	VARCHAR2(8)		리소스 프로파일이 KERNEL 또는 PASSWORD 매개변수인지 여부를 나타냅니다.
LIMIT	VARCHAR2(40)		이 프로파일의 리소스에 대해 설정된 제한을 나타냅니다.

모든 공통 CAAT 도구(그리고 Microsoft Excel과 Microsoft Access)는 CSV 파일의 가져오기를 허용합니다. DBA_PROFILES를 CAATs 도구로 가져와서 조직의 표준을 준수하는지 여부에 대해 분석할 수 있습니다. 이러한 표준은 ISACA의 Oracle Audit/Assurance Program and ICQ,[5] Defense Information System Agency의 Security Technical Implementation Guide,[6] Center for Internet Security 벤치마크,[7] 또는 조직이 개발한 문서에 기반을 둘 수 있습니다.

일단 조직이 하나의 데이터베이스를 분석해서 이것이 관련 표준을 준수한다고 확인한 경우에는 이러한 데이터베이스를 마스터 프로파일로 사용함으로써 모든 Oracle 데이터베이스에 전반에 걸쳐 관심있는 프로파일을 비교하기 위한 CAAT 도구로 설성한다는 것이 핵심적인 개념입니다. 이것은 필드 프로파일과 리소스를 연결해서(또는 단순히 리소스만), 제한 사항이 동일하지 않은 모든 레코드를 표시함으로써 가능합니다. 예를 들어, 실패한 로그인 시도 회수는 데이터베이스 샘플에 걸쳐 다를 수 있습니다. 이러한 방법을 통해 조직은 비준수 프로파일에 신속하게 플래그 표시해서 후속 조치 및 검토를 실시할 수 있습니다.

필요한 경우에, 조직은 Oracle 프로파일의 검토를 정기적으로 반복할 수도 있습니다. 이를 통해 변경 사항을 추적할 수 있으며 지속적인 모니터링 감사 프로그램의 일환으로 사용될 수 있습니다.

V$PARAMETER

감사를 받는 실체는 Oracle 데이터베이스를 설정하는 방법에 대한 정책도 가지고 있어야 합니다. 이러한 설정의 대부분은 Oracle 설치 매개변수에 반영되어 있는데, V$PARAMETER 뷰에서 검색 가능합니다. 이러한 매개변수의 예로는 DBA와 같은 특권 사용자가 실시한 작업에 대한 감사 활성화 또는 대소문자 구분 암호가 필요한지 여부에 대한 설정이 있습니다.

대략적으로 260개의 Oracle 초기화 매개변수가 있으며 전체 목록은 *Oracle Database Reference*에서 참조 가능합니다.[8] 그러나, 이러한 방법의 핵심 개념은 모든 데이터베이스에 대해 관심있는 모든 매개변수를 검토할 필요는 없다는 것입니다. 다시 말하자면, 하나의 데이터베이스가 표준을 준수하는 것으로 확인된 경우, 이 데이터베이스를 CAAT 도구에서 마스터로 사용하여 모든 데이터베이스에 걸쳐 관심있는 매개변수와 비교할 수 있습니다. 이것은 필드 이름을 연결하고(V$PARAMETER 레이아웃에서[9]), 값이 동일하지 않은 모든 레코드를 표시함으로써 가능합니다. 전술된 바와 같이, 이러한 방법을 통해 비준수 구성을 신속하게 플래그 표시해서 후속 조치 및 검토를 실시할 수 있습니다.

DBA_USERS

DBA_USERS는 Oracle 데이터베이스의 모든 사용자를 설명합니다. 여기에는 사용자 이름, 계정 상태가 포함되며 10.2.0.5 이하의 Oracle 데이터베이스에서는 암호 해시가 포함됩니다.

암호는 최대 30자의 길이이며 모든 문자는 해시 작업이 수행되기 전에 대문자로 변환됩니다. 또한 진정한 "변환"은 없습니다. 알고리즘은 단순히 사용자 이름을 사용합니다. 즉, 사용자 이름 암호 조합 sys/temp1 와 system/p1은 동일한 암호 해시값을 가집니다.[10] 또한, 서로 다른 Oracle 데이터베이스 상에 동일한 암호로 설치된 사용자 이름은 동일한 암호 해시를 가집니다. 이것은 데이터베이스 설치 과정에서 디폴트값이 적용되는 경우에 흔히 발생하기도 합니다. 디폴트 암호는 Oracle 데이터베이스 설치에서 실제적이고 흔한 위험을 내포하게 됩니다.

> 기본 암호는 Oracle 데이터베이스 설치에서 실제적이고 흔한 위험을 내포하게 됩니다.

이러한 위협은 너무 흔해서 디폴트 Oracle 암호의 해시 목록이 온라인으로 관리되고 있을 정도입니다.[11] 이것은 CSV 및 Excel을 비롯한 다양한 형식으로 관리되어 CAAT 도구로 쉽게 가져올 수 있습니다. 이러한 디폴트 암호 해시값 목록은 조직의 모든 데이터베이스에 걸쳐 DBA_USERS(필드 암호에서 연결[12]) 에 대해 비교됩니다. 암호 해시가 일치하는 것이 발견되는 경우 디폴트 암호가 사용되고 있음을 의미합니다. 이것은 즉시 검토되어야 합니다. DBA_USERS는 조직의 급여와 같이 다른 정보원과 비교되어 퇴사자와 이동자에 플래그를 설정할 수 있습니다. (유의사항: Oracle 11g부터 새로운 뷰인 DBA_USERS_WITH_DEFPWD는 디폴트 암호를 사용하고 있는 모든 사용자를 표시합니다.)

기타 뷰

Oracle 뷰에는 수 백가지가 있기 때문에 본 기사에서 모든 뷰를 설명하기는 불가능합니다. 상기에 언급된 뷰는 설명을 제공하기 위한 목적으로만 사용되었습니다. 사용되는 뷰는 감사 목적에 따라 달라지며, 여기에는 다음의 뷰가 포함될 수 있습니다:

- ISACA의 Oracle Audit/Assurance Program and ICQ에 설명되어 있는 뷰[13]
- 데이터베이스에 정의된 모든 역할을 나열하는 DBA_ROLES. 이것을 검토해서 역할이 적절하고 암호로 보호되는지 확인할 수 있습니다(해당되는 경우).
- 사용자에게 부여된 역할 또는 기타 역할을 식별하는 DBA_ROLE_PRIVS. 이것을 검토해서 사용자에게 부여된 역할 권한이 적절하고 최소 권한 원칙에 부합되는지 확인할 수 있습니다.
- 사용자 또는 역할에 부여된 모든 시스템 권한을 나열하는 DBA_SYS_PRIVS. 이것을 검토해서 사용자에게 부여된 시스템 권한이 적절하고 최소 권한 원칙에 부합되는지 확인할 수 있습니다.

기사가 흥미롭습니까?

- 지식 센터의 Oracle 데이터베이스 주제에서 본 기사의 저자이자 주제 리더인 Ian Cooke와 토의한 후 협업하는 방법에 대해 알아보십시오.

www.isaca.org/topic-oracle-database

- 사용자 또는 역할에 부여된 모든 테이블 권한을 나열하는 DBA_TAB_PRIVS. 이것을 검토해서 사용자에게 부여된 테이블 권한이 적절하고 최소 권한 원칙에 부합되는지 확인할 수 있습니다.
- 모든 객체에 대한 감사 옵션을 나열하는 DBA_OBJ_AUDIT_OPTS. 이것을 검토해서 활성화된 감사 기능이 데이터베이스에 있는 데이터 민감도에 적절한지 확인할 수 있습니다.
- 시스템 권한의 부여를 포착하는 DBA_PRIV_AUDIT_OPTS. 이것을 검토해서 최소 권한 원칙에 따라 시스템 권한이 적절한 사용자에게만 부여되었는지 확인할 수 있습니다.
- Statement를 포착하는 DBA_STMT_AUDIT_OPTS. 이것을 검토해서 적절한 사용자가 statement를 출력하고 최소 권한 원칙에 부합되는지 확인할 수 있습니다.
- 다른 데이터베이스로의 연결에 대한 정보를 나열하는 DBA_DB_LINKS. 이것을 검토해서 다른 데이터베이스에 대한 연결이 보안 유지되고 최소 권한 원칙에 부합되는지 확인할 수 있습니다.
- 컴포넌트 Oracle 제품에 대한 버전 및 상태 정보를 나열하는 V$VERSION. 이것을 검토해서 설치된 현재 버전이 완전히 지원되는지 확인할 수 있습니다.
- 데이터베이스 라이센스 정보를 나열하는 V$LICENSE. 이것을 검토해서 감사 대상 조직이 모든 Oracle 라이센스 요건을 충족하는지 확인할 수 있습니다.

Oracle 뷰의 전체 목록 및 이에 따른 세부적인 설명은 *Oracle Database Reference*에서 참조 가능합니다.[14] 그러나, 중요한 요점은 이러한 뷰를 CSV 파일로 출력해서 CAAT 도구로 가져올 수 있다는 사실입니다. 이렇게 가져온 후에는 다음 작업이 가능합니다.

- 표준을 준수하는 것으로 확인된 마스터를 비롯한 기타 Oracle 데이터베이스와 비교할 수 있습니다.
- 프로덕션 데이터베이스의 개발, 테스트 또는 품질 보증 버전과 비교할 수 있습니다(변경 통제에 유용함).
- 다른 데이터 소스와 비교할 수 있습니다. 여기에는 내부 또는 외부 기관의 데이터가 포함될 수 있습니다.

결론

CAAT는 Oracle 데이터베이스를 감사하기 위한 유용한 도구입니다. 많은 조직이 이미 CAAT 소프트웨어를 사용하고 있기 때문에 권장되는 CAAT를 사용하면 설정 비용이 거의 들지 않습니다. 또한, 이러한 방법을 통해 외부 컨설턴트와 지리적으로 분산되어 있는 회사는 관리자 암호를 노출할 필요 없이 쿼리를 로컬 DBA에 의해 실행되도록 할 수 있습니다. 또한, 감사 대상 조직의 DBA는 데이터베이스에 걸쳐 실행되는 SQL을 검토하여 프로덕션 환경에 아무런 영향이 없도록 보장할 수 있습니다.

일단 실행된 쿼리는 이메일 또는 기타 방법으로 보안 전송해서 분석을 받을 수 있습니다. 쿼리 결과를 이미 알려진 규정 준수 데이터베이스와 비교함으로써 감사 우려 사항을 식별할 수 있습니다. 또한, 쿼리 결과를 프리프로덕션 데이터베이스 및 기타 데이터 소스(예를 들어, 회사 급여)와도 비교할 수 있습니다. 결론적으로, 전체 프로세스는 반복되어 지속적인 모니터링 및/또는 감사의 일환으로 사용될 수 있습니다.

미주

[1] PeteFinnigan.com Limited, Commercial Oracle security tools, *www.petefinnigan.com/tools.htm*

[2] Oracle, *Oracle Database Reference 11g Release 2 (11.2)*, *http://docs.oracle.com/cd/E11882_01/server.112/e25513.pdf*

[3] ISACA, Knowledge Center, *www.isaca.org/Groups/Professional-English/oracle-database/GroupDocuments/Oracle.SQL*

[4] *Op cit*, Oracle, p. 17-3

[5] ISACA, *Security, Audit and Control Features Oracle Database, 3rd Edition*, 2009, USA, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Audit-Programs/Documents/Oracle_DB_3rd_Ed_Audit_Prog_ICQ_7Dec09.doc*

[6] Information Assurance Support Environment, 'Application Security—Database (Oracle7)', *http://iase.disa.mil/stigs/app_security/database/oracle.html*

[7] Center for Internet Security, 'Security Benchmarks', *http://benchmarks.cisecurity.org/downloads/browse/?category=benchmarks.servers.database.oracle*

[8] *Op cit*, Oracle, p. 1-4

[9] *Op cit*, Oracle, p. 8-52

[10] Red Data Base Security, 'Fact Sheet About Oracle Database Passwords', *www.red-database-security.com/whitepaper/oracle_passwords.html*

[11] PeteFinnigan.com Limited, 'Oracle Default Password List', *www.petefinnigan.com/default/default_password_list.htm*

[12] *Op cit*, Oracle, p. 5-49

[13] *Op cit*, ISACA, 2009

[14] *Op cit*, Oracle