Oracle® DIVAdirector

보안 설명서

릴리스 5.3

E71134-01

2015년 12월

ORACLE

Oracle® DIVAdirector
보안 설명서

E71134-01

차례

머리말

Oracle DIVAdirector 보안 설명서에서는 DIVAdirector 제품에 대한 정보를 제공하고 일반적인 응용 프로그램 보안 원칙에 대해 설명합니다.

대상

이 설명서는 DIVAdirector의 보안 설치/구성 및 보안 기능 사용과 관련된 모든 사람을 대상으로 합니다.

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

오라클 고객지원센터 액세스
지원 서비스를 구매한 오라클 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info를 참조하거나, 청각 장애가 있는 경우 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs를 방문하십시오.

1

1장. 개요

이 장에서는 DIVAdirector 제품의 개요를 제공하고 일반적인 응용 프로그램 보안 원칙에 대해 설명합니다.

1.1. 제품 개요

Oracle DIVAdirector는 기존 Oracle DIVArchive 시스템과의 상호 작용에 사용되는 도구입니다. UI(사용자 인터페이스)는 웹 브라우저를 통해 그래픽으로 제공됩니다. DIVAdirector의 주요 구성 요소는 다음과 같습니다.

1.1.1. DIVAdirector Server

DIVAdirector Server는 DIVAdirector Web에서 요청하는 모든 작업에 대해 C++ API를 통해 DIVArchive와의 인터페이스를 제공합니다. 또한 DIVArchive에 저장되어 있는 검색된 객체 정보를 고유 데이터베이스에 동기화합니다. 프록시, 메타데이터 및 작업에 대해 구성된 드롭 폴더를 모니터하고 모든 드롭 폴더 및 UI 작업의 내역을 유지 관리합니다.

1.1.2. DIVAdirector Web

DIVAdirector의 웹 모듈은 웹 기반 UI 인터페이스를 제공합니다. 이를 통해 사용자는 DIVArchive에서 검색된 객체를 찾고, 사용자 액세스 권한을 관리하고, 자산에 대한 메타데이터를 추가하고, 객체의 프록시 역할을 하고, 작업 공간 또는 샷 목록에 추가된 항목에 대해 작업(예: 복원, 부분 복원 및 삭제)을 수행할 수 있습니다. 또한 사용자에게 로컬에서 파일을 찾아보고 DIVArchive 시스템에 컨텐츠를 아카이브할 수 있는 기능을 제공합니다.

1.1.3. DIVAdirector Database

DIVAdirector는 PostgreSQL을 사용하여 모든 DIVArchive 자산 정보, 메타데이터, 프록시 정보, 사용자 정보, 작업 내역 및 구성 설정을 저장합니다.

1.1.4. DIVAdirector Transcoder Service

DIVAdirector Transcoder Service는 고해상도 클립을 저해상도 프록시로 트랜스코딩하여 DIVAdirector Web UI 내에 표시하기 위해 DIVAdirector가 호출하는 별도의 서비스입니다.

1.1.5. DIVAdirector Task Manager Service

DIVAdirector Task Manager Service는 표준 Services Control Manager 대화 상자에 표시되는 Windows 서비스 응용 프로그램입니다. 이 응용 프로그램은 백그라운드 프로세스로 잠재적 장기 실행 작업을 수행합니다.

1.1.6. DIVAdirector API Service

이 서비스는 일반적인 DIVAdirector 기능에 대한 끝점을 노출합니다. 처음에는 DIVAdirector 논리의 소수 하위 세트만 이 서비스에 포함됩니다. 이 서비스를 통해 노출된 끝점은 DIVAdirector Web에서 기능이 점진적으로 마이그레이션되면서 계속 증가됩니다.

1.2. 일반 보안 원칙

다음 절에서는 응용 프로그램을 안전하게 사용하는 데 필요한 기본적인 원칙을 설명합니다.

1.2.1. 소프트웨어를 최신 상태로 유지

실행하는 DIVAdirector를 항상 최신 버전으로 유지하십시오. 최신 버전의 소프트웨어는 Oracle Software Delivery Cloud에서 다운로드할 수 있습니다.

https://edelivery.oracle.com/

1.2.2. 중요한 서비스로 네트워크 액세스 제한

DIVAdirector에서는 다음 TCP/IP 포트를 사용합니다.

- tcp/7680 - 사용자 인터페이스 명령용
- tcp/8080 - HTTP Server용

5.3.0 이상의 DIVAdirector 릴리스에서는 세 가지 추가 포트가 필요합니다.

- tcp/9763 - DIVArchiveWS Service 통합
- tcp/9876 - DIVAtranscode Service 통합
- tcp/6543 - DIVAdirector API Service 통합

주:

위에 나열된 포트 번호는 최신이지만 나중에는 변경될 수도 있습니다.

1.2.3. ADMIN 사용자로 실행 및 가능한 최소 권한 원칙 사용

DIVAdirector는 첫번째 로그인 후 암호를 변경해야 하는 기본 수퍼 관리자 사용자를 제공합니다. 그러면 이 사용자는 액세스와 작업에 다른 그룹 권한을 사용하는 다른 사용자를 만들 수 있습니다.

기본 암호를 변경하지 않을 경우 시스템이 가능한 악의적인 작동에 노출됩니다. 수퍼 관리자 계정에 대한 설치와 구성이 끝난 후에는 즉시 기본 암호를 변경하고, 이후 최소 180일마다 암호를 변경해야 합니다. 변경을 완료한 후에는 필요한 경우 오라클 고객지원센터에 제공할 수 있도록 안전한 오프라인 장소에 암호를 보관해야 합니다.

1.2.4. 시스템 작동 모니터

시스템 작동을 모니터하여 DIVAdirector가 제대로 작동하고 있는지 확인할 수 있습니다. 로그는 C:/Program Files (x86)/DIVAdirector 5/cmg-server 및 C:/Program Files (x86)/DIVAdirector 5/www/logs에 있습니다.

1.2.5. 최신 보안 정보 유지

여러 소스의 보안 정보에 액세스할 수 있습니다. 다양한 소프트웨어 제품에 대한 보안 정보 및 경보는 다음을 참조하십시오.

http://www.us-cert.gov

보안 사항을 최신으로 유지하는 기본적인 방법은 최신 버전의 DIVAdirector 소프트웨어를 실행하는 것입니다.

2

2장. 보안 설치

이 장에서는 보안 설치 계획 프로세스의 개요를 살펴보고 권장되는 몇 가지 시스템 배치 토폴로지에 대해 설명합니다.

2.1. 사용자 환경 이해

보안 요구 사항을 더 잘 이해하려면 다음과 같은 질문을 해야 합니다.

2.1.1. 어떤 리소스를 보호해야 합니까?

프로덕션 환경의 다양한 리소스를 보호할 수 있습니다. 제공할 보안 레벨을 결정할 때 보호하고자 하는 리소스의 유형을 고려하십시오. DIVAdirector를 사용하는 경우 다음과 같은 리소스가 보호됩니다.

2.1.1.1. 기본 데이터 디스크

저해상도 클립이 포함된 프록시 폴더가 있습니다. 이러한 폴더는 주로 DIVAdirector 시스템에 연결되는 로컬 또는 원격 디스크에 있습니다. DIVAdirector를 사용하지 않고 개별적으로 해당 디스크에 액세스할 경우 보안 위험에 노출됩니다. 이 유형의 외부 액세스는 해당 디스크를 읽거나 쓰는 악의적인 시스템 또는 해당 디스크 장치에 대한 액세스를 실수로 제공하는 내부 시스템에서 발생할 수 있습니다.

2.1.1.2. 데이터베이스 디스크 및 백업 디스크

DIVAdirector를 빌드할 때 데이터베이스 디스크 및 백업 디스크 리소스가 사용됩니다. 일반적으로 이러한 리소스는 DIVAdirector 시스템에 연결되는 로컬 또는 원격 디스크입니다. DIVAdirector를 사용하지 않고 개별적으로 해당 디스크에 액세스할 경우 보안 위험에 노출됩니다. 이 유형의 외부 액세스는 해당 디스크를 읽거나 쓰는 악의적인 시스템 또는 해당 디스크 장치에 대한 액세스를 실수로 제공하는 내부 시스템에서 발생할 수 있습니다.

2.1.1.3. 구성 파일 및 설정

DIVAdirector 시스템 구성 설정은 OS(운영체제) 레벨의 관리자 외 사용자로부터 보호되어야 합니다. 일반적으로 해당 설정은 OS 레벨 관리 사용자에 의해 자동으로 보호됩니다. 비관리 OS 사용자에게 구성 파일을 쓸 수 있도록 허용할 경우 보안 위험에 노출됩니다. 다음을 비롯하여 설치 디렉토리에 들어 있는 모든 응용 프로그램 구성 파일이 중요한 파일에 해당합니다.

- www/Web.config

- Api/Oracle.DIVAdirector.Api.exe.config
- TaskManager/Oracle.DIVAdirector.TaskManager.exe.config
- cmgserver/cmgserver.ini

2.1.2. 누구로부터 리소스를 보호합니까?

일반적으로 이전 절에서 설명된 리소스는 구성된 시스템의 모든 비관리자 액세스나 WAN 또는 FC 패브릭으로 이러한 리소스에 액세스할 수 있는 악의적인 외부 시스템으로부터 반드시 보호되어야 합니다.

2.1.3. 전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?

전략적 리소스에 대한 보호 실패는 부적절한 액세스(정상적인 DIVAdirector 작동을 벗어나는 데이터에 대한 액세스)부터 데이터 손상(정상적인 권한을 벗어나는 디스크나 테이프에 쓰기)에 이르기까지 다양합니다.

3

3장. 보안 기능

잠재적인 보안 위협이 발생하지 않도록 DIVAdirector 작동 고객은 시스템 인증 및 권한 부여를 고려해야 합니다.

이러한 보안 위협은 적절한 구성 및 부록 A. 보안 배치 점검 목록의 설치 후 점검 목록을 준수하여 최소화할 수 있습니다.

3.1. 보안 모델

보안 위협으로부터 보호하는 중요 보안 기능은 다음과 같습니다.

- 인증 - 권한이 부여된 개인만 시스템 및 데이터에 액세스할 수 있도록 합니다.
- 권한 부여 - 시스템 권한 및 데이터에 대한 액세스 제어입니다. 이 기능은 인증을 기반으로 사용자가 적절한 액세스 권한만 가지도록 합니다.

부록 A

부록 A. 보안 배치 점검 목록

1. 관리자 계정 및 DIVArchive나 DIVAdirector 관리자 또는 서비스 역할이 지정된 기타 모든 OS 계정에 대해 강력한 암호를 설정합니다.
2. 로컬 관리자 OS 계정을 사용하는 대신 필요에 따라 다른 사용자 계정에 역할을 지정합니다.
3. DIVAdirector 관리자 사용자에 대해 강력한 암호를 설정합니다. 기본적으로 설치된 암호를 즉시 강력한 암호로 변경합니다. DIVAdirector **Admin**, **Personal** settings 화면에서 변경 작업을 수행할 수 있습니다.
4. 시스템에 방화벽을 설치하고 기본 DIVAdirector 포트 규칙을 적용합니다.
5. 보안 패치가 포함된 OS 및 DIVAdirector 업데이트를 주기적으로 설치합니다.
6. 바이러스 백신을 설치하고 성능을 위해 DIVAdirector 프로세스 및 스토리지를 제외합니다.