Oracle® DIVArchive

보안 설명서

릴리스 7.3

E70866-01

2015년 12월

ORACLE

Oracle® DIVArchive
보안 설명서

E70866-01

차례

머리말

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

대상

이 설명서는 DIVArchive의 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 DIVArchive 제품의 개요를 제공하고 일반적인 응용 프로그램 보안 원칙에 대해 설명합니다.

1.1. 제품 개요

Oracle DIVArchive는 컨텐츠 스토리지 관리 시스템으로 배포되었습니다. DIVArchive의 주요 구성 요소는 다음과 같습니다.

1.1.1. DIVArchive Manager

DIVArchive Manager는 DIVArchive 시스템의 주요 구성 요소입니다. 모든 아카이브 작업은 DIVArchive Manager를 통해 제어 및 처리됩니다. 개시자 응용 프로그램이 DIVArchive 클라이언트 API를 통해 작업 요청을 전송합니다. DIVArchive는 구매 가능한 옵션으로 Main DIVArchive Manager와 Backup DIVArchive Manager도 지원합니다. DIVArchive에 대한 자세한 내용은 DIVArchive 소프트웨어 릴리스 7.3 고객 설명서 라이브러리를 참조하십시오.

https://docs.oracle.com/en/storage/#csm

1.1.2. DIVArchive Actor

DIVArchive Actor는 프로덕션 시스템에서 장치 간 데이터 이동 도구입니다. 다른 유형의 여러 장치 간 데이터 전송을 지원하며, Telestream 트랜스코딩 소프트웨어(선택사항)와의 트랜스코드 작업도 처리합니다.

모든 Actor 작업은 DIVArchive Manager를 통해 시작 및 조정됩니다. 하나의 DIVArchive Manager가 하나 이상의 Actor를 구성 및 제어할 수 있습니다.

1.1.3. DIVArchive Robot Manager

DIVArchive는 디스크 스토리지 관리에만 사용될 수 있지만, 하나 이상의 테이프 라이브러리를 추가하여 스토리지 용량을 더 확장할 수 있습니다. 이러한 경우 DIVArchive Robot Manager 모듈은 DIVArchive Manager가 다른 유형의 여러 테이프 라이브러리와 상호 작용할 수 있도록 중간 소프트웨어 계층을 제공합니다. DIVArchive Robot Manager는 TCP/IP를 통해 DIVArchive Manager에 연결되며, 고유 SCSI 또는 SCSI over Fiber Channel을 통해 라이브러리 자체에 대한 직접 인터페이스를 사용하거나 제조업체의 고유 라이브러리 제어 소프트웨어에 대한 중간 이더넷 연결을 통해 라이브러리에 연계됩니다.

1.1.4. DIVArchive Backup Service

Oracle 데이터베이스 및 메타데이터 데이터베이스 백업의 안정성과 모니터링을 위해 DIVArchive Backup Service가 도입되었습니다.

DIVArchive Backup Service 구성 요소는 표준 DIVArchive 시스템 설치의 필수 요소로 설치됩니다. 일반적으로 이 구성 요소는 DIVArchive Manager 및 Oracle 데이터베이스와 동일한 서버에 설치됩니다. DIVArchive Backup Service는 구성 파일을 통해 예약된 백업의 구성을 고려하며, 전체 백업 프로세스를 관리 및 모니터합니다.

데이터베이스 및 메타데이터 데이터베이스 파일 백업 프로세스로 인해 발생하는 문제를 전자 메일로 전송할 수 있는 기능이 DIVArchive Backup Service에 포함되었습니다. 이 기능을 사용하려면 SMTP 메일 공급자에 연결하도록 DIVArchive를 구성해야 합니다. 전자 메일 통지는 Manger Setting 탭의 DIVArchive Configuration Utility를 통해 구성됩니다.

DIVArchive Backup Service 설치 및 구성에 대한 자세한 내용은 DIVArchive 소프트웨어 릴리스 7.3 고객 설명서 라이브러리를 참조하십시오.

https://docs.oracle.com/en/storage/#csm

1.1.5. Oracle Avid 연결

Avid와 DIVArchive 간 연결의 목적은 특정 비디오 형식으로 아카이브 데이터를 DIVArchive에서(로) 전송하고 단일 클립 또는 일련의 클립을 아카이브 및 검색할 수 있도록 하는 것입니다. AMC 및 TMC 관련 구성 요소가 주요 DIVArchive 설치와 함께 설치됩니다. AMC 및 TMC용 특정 플러그인은 추가로 설치해야 합니다.

1.1.6. DIVArchive Drop Folder Monitor

DIVArchive DFM(Drop Folder Monitor)은 최대 20개의 로컬 폴더 또는 FTP 폴더(또는 로컬 폴더와 FTP 폴더의 조합)에서 새로 만들어진 파일을 자동으로 모니터할 수 있는 기능을 제공합니다. DIVArchive 객체당 파일 하나 또는 여러 개(FTP 폴더 내)가 지원됩니다. 새 파일(또는 FTP 폴더)이 식별되면 DFM은 자동으로 DIVArchive에 새 파일 또는 폴더 아카이브 요청을 실행합니다. 해당 파일은 성공적으로 아카이브된 후 자동으로 소스에서 삭제됩니다.

1.1.7. DIVArchive SNMP

DIVArchive SNMP(Simple Network Management Protocol) 에이전트 및 MIB(Management Information Base)는 SNMP 프로토콜을 사용하는 타사 모니터링 응용 프로그램을 통해 DIVArchive와 관련 부속 시스템의 상태 및 작동 모니터링을 지원합니다.

1.1.8. DIVArchive SPM

DIVArchive SPM(Storage Plan Manager)은 SPM 구성에 정의된 규칙 및 정책을 기반으로 아카이브 내 자료의 자동 마이그레이션 및 수명 주기 기능을 제공합니다.

SPM 구성 요소는 디스크 공간 워터마크를 기반으로 SPM 관리 대상 어레이에서 자료 삭제를 트리거하는 데도 사용됩니다.

1.1.9. DIVArchive Migrate Service

DIVArchive에는 마이그레이션 서비스가 포함되어 있습니다. 이 서비스는 DIVArchive 내부의 새로운 별도 서비스로, 사용자가 DIVArchive 시스템 내 다른 매체 간에 컨텐츠를 마이그레이션하는 작업을 예약하고 실행할 수 있도록 도와줍니다. Control GUI 또는 명령줄 클라이언트를 사용할 수 있습니다.

1.1.10. DIVArchive VACP

VACP(Video Archive Command Protocol)는 Harris Automation에서 아카이브 시스템과의 연계를 위해 개발한 프로토콜입니다. DIVArchive에는 DIVArchive Manager와의 통신을 위한 고유 API가 있지만 VACP와 호환되지 않습니다.

1.1.11. DIVArchive Control GUI

DIVArchive Control GUI(그래픽 사용자 인터페이스)는 DIVArchive 내 작업을 모니터, 제어 및 감독하는 데 사용됩니다. 동시에 여러 DIVArchive GUI를 실행할 수 있으며 동일한 DIVArchive 시스템에 연결할 수 있습니다.

1.1.12. DIVArchive Configuration Utility

DIVArchive Configuration Utility는 DIVArchive 시스템 구성에 사용됩니다. 주로 DIVArchive 구성에 사용되지만, Configuration Utility에서 일부 작업 기능이 수행되기도 합니다.

1.1.13. DIVArchive Access Gateway

Access Gateway는 한 대의 컴퓨터에서 별도의 여러 DIVArchive 시스템이 작동 및 상호 작용할 수 있도록 해줍니다. 이는 컨텐츠 배포를 위한 글로벌 솔루션입니다. 미러 사이트에 파일이 자동으로 복제되면 간편하게 로컬 배포, 백업 및 재해 복구에 보안, 대역폭 제어 및 체크섬 확인 기능이 제공됩니다. 네트워크가 모니터되며 DIVAnet을 통해 컨텐츠가 최종적으로 전달됩니다.

1.1.14. DIVArchive Lynx Local delete

LYNXLocalDelete는 하나의 로컬 DIVArchive 시스템(예: LYNXlocal)과 하나(또는 하나 이상)의 원격 DIVArchive 시스템(예: LYNXdr) 간 객체 복제 기능을 모니터하는 서비스입니다. 객체가 원격 DIVArchive 시스템에 성공적으로 복제되면 로컬 DIVArchive 시스템에서의 삭제에 적격한 것으로 플래그가 지정됩니다.

1.2. 일반 보안 원칙

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

1.2.1. 소프트웨어를 최신 상태로 유지

실행하는 DIVArchive를 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

DIVArchive에서는 다음 TCP/IP 포트를 사용합니다.

- tcp/8500: DIVArchive Robot Manager에 사용
- tcp/9000: DIVArchive Manager에 사용
- tcp/9300: DIVArchive Backup Service에 사용
- tcp/9500: DIVArchive Access Gateway에 사용
- tcp/9900: DIVArchive Actor에 사용
- tcp/9191: DIVArchive Migrate Service에 사용

1.2.3. DIVA 사용자로 실행 및 가능한 최소 권한 원칙 사용

모든 DIVArchive 서비스는 DIVA 사용자로 실행됩니다. DIVArchive Control GUI에서는 세 가지 고정 사용자 프로파일(Administrator, Operator 및 User)을 제공합니다. 관리자 및 운영자 계정의 경우 액세스 권한을 얻으려면 암호가 필요합니다. DIVArchive 시스템은 기본 암호를 사용하여 설치된 상태로 제공되며, 기본 암호는 DIVArchive Configuration Utility를 통해 언제든지 변경할 수 있습니다. 기본 암호를 변경하지 않을 경우 DIVArchive 시스템이 가능한 악의적인 작동에 노출됩니다. **관리자 및 운영자 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 DIVArchive가 제대로 작동하고 있는지 여부 및 비정상적인 작업이 기록되고 있는지 여부를 확인합니다. /Program/log/의 설치 디렉토리에 있는 로그 파일을 확인하십시오.

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 DIVArchive 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.

DIVArchive를 사용하는 경우 다음과 같은 리소스가 보호됩니다.

2.1.1.1. 기본 데이터 디스크

DIVArchive 시스템을 빌드할 때 데이터 디스크 및 캐시 디스크 리소스가 사용됩니다. 일반적으로 이러한 리소스는 DIVArchive 시스템에 연결되는 로컬 또는 원격 디스크입니다. DIVArchive를 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, 메타데이터 디스크 및 백업 디스크

복합 객체를 사용하여 DIVArchive 시스템을 빌드할 때 데이터베이스 디스크, 메타데이터 디스크 및 백업 디스크 리소스가 사용됩니다. 일반적으로 이러한 리소스는 DIVArchive 시스템에 연결되는 **로컬 또는 원격** 디스크입니다. DIVArchive를 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. DIVArchive 테이프

일반적으로 DIVArchive 시스템을 통해 제어되는 테이프 라이브러리에서 데이터가 기록되는 테이프에 대해 개별 액세스를 허용할 경우 보안 위험에 노출됩니다.

2.1.1.4. 테이프 메타데이터 내보내기

내보내기 작업으로 만들어지는 테이프 메타데이터 덤프에는 데이터와 메타데이터가 포함됩니다. 이 데이터와 메타데이터는 일상적인 내보내기 또는 가져오기 작업 중 OS 관리자 이외의 다른 사용자가 액세스하지 못하도록 보호되어야 합니다.

2.1.1.5. 구성 파일 및 설정

DIVArchive 시스템 구성 설정은 OS 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.

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 DIVArchive 작동을 벗어나는 데이터에 대한 액세스)부터 데이터 손상(정상적인 권한을 벗어나는 디스크나 테이프에 쓰기)에 이르기까지 다양합니다.

2.2. 권장되는 배치 토폴로지

이 절에서는 기반구조 구성 요소를 안전하게 설치 및 구성하는 방법에 대해 설명합니다. DIVArchive 설치에 대한 자세한 내용은 DIVArchive 소프트웨어 릴리스 7.3 고객 설명서 라이브러리를 참조하십시오.

https://docs.oracle.com/en/storage/#csm

DIVArchive를 설치 및 구성할 때는 다음 사항을 고려하십시오.

2.2.1. 별도의 메타데이터 네트워크

DIVArchive 서비스 구성 요소 간 연결, 메타데이터 데이터베이스로의 연결 및 클라이언트로부터의 연결을 위해 WAN에 연결되지 않은 별도의 TCP/IP 네트워크 및 스위치 하드웨어를 제공하십시오. 메타데이터 트래픽은 TCP/IP를 사용하여 구현되므로 이론적으로 이 트래픽에 대한 외부 공격이 가능합니다. 별도의 메타데이터 네트워크를 구성하면 이 위험이 줄어들고 성능도 향상됩니다. 별도의 네트워크가 불가능한 경우 적어도 외부 WAN 및 네트워크의 신뢰할 수 없는 모든 호스트로부터 DIVArchive 포트에 대한 트래픽을 거부하십시오. 1.2.2 절. “중요한 서비스로 네트워크 액세스 제한”을 참조하십시오.

2.2.2. FC 영역 분할

FC 영역 분할을 사용하면 광 섬유 채널을 통해 디스크에 대한 액세스가 필요하지 않은 서버로부터 연결된 DIVArchive 디스크에 대한 액세스를 거부할 수 있습니다. 가능하면 별도의 FC 스위치를 사용하여 액세스가 필요한 서버에만 물리적으로 연결하는 것이 좋습니다.

2.2.3. SAN 디스크 구성 액세스 보호

일반적으로 SAN RAID 디스크는 주로 HTTP, 아니면 TCP/IP를 통해 관리 목적으로 액세스할 수 있습니다. SAN RAID 디스크에 대한 관리 액세스를 신뢰할 수 있는 도메인 내의 시스템으로만 제한하여 외부 액세스로부터 디스크를 보호해야 합니다. 또한 디스크 어레이에 대한 기본 암호를 변경하십시오.

2.2.4. DIVArchive 패키지 설치

먼저 필요한 DIVArchive 서비스만 설치하십시오. 예를 들어, 시스템에서 GUI 또는 Configuration Utility를 실행하지 않으려는 경우 설치 중 표시되는 설치할 구성 요소 목록에서 해당 항목의 선택을 취소하십시오. 설치 후 기본 DIVArchive 설치 디렉토리 권한과 소유자를 변경하려면 반드시 해당 변경이 보안에 끼치는 영향을 고려해야 합니다.

2.2.5. DIVArchive 테이프 보안

DIVArchive 시스템을 통해 제어되는 테이프 라이브러리 내 DIVArchive 테이프에 대한 외부 액세스를 방지하십시오. DIVArchive 테이프에 대해 허용되지 않은 액세스는 사용자 데이터를 조작하거나 삭제할 수 있습니다.

2.2.6. 백업

DIVArchive Backup Service를 통해 데이터베이스 백업을 설정 및 수행하십시오. OS 레벨 관리자 사용자로만 백업 덤프에 대한 액세스를 제한하십시오.

2.3. 설치 후 구성

DIVArchive를 설치한 후에는 부록 A. 보안 배치 점검 목록의 보안 점검 목록을 확인하십시오.

3

3장. 보안 기능

잠재적인 보안 위협이 발생하지 않도록 DIVArchive 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.

3.2. 인증

DIVArchive Control GUI에서는 세 가지 고정 사용자 프로파일(Administrator, Operator 및 User)을 제공합니다. 관리자 및 운영자 계정의 경우 액세스 권한을 얻으려면 암호가 필요합니다. DIVArchive 시스템은 기본 암호를 사용하여 설치된 상태로 제공되며, 기본 암호는 DIVArchive Configuration Utility를 통해 언제든지 변경할 수 있습니다. 기본 암호를 변경하지 않을 경우 DIVArchive 시스템이 가능한 악의적인 작동에 노출됩니다. **관리자 및 운영자 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.**

3.3. 액세스 제어

DIVArchive의 액세스 제어는 세 가지 프로파일로 구분됩니다.

User - DIVArchive Manager에 대한 연결이 설정된 후 Control GUI에서 사용자만 DIVArchive 작업을 모니터하고 데이터베이스에서 데이터를 검색할 수 있습니다. 이를 User 프로파일이라고 합니다. User 프로파일 모드에서는 DIVArchive에 명령을 실행하는 일부 기능에 액세스할 수 없습니다. 따라서 모니터링이 필요하지만 DIVArchive로 명령을 전송할 수 없는 경우가 발생합니다.

Administrator - DIVArchive에 요청(예: 아카이브 또는 복원 요청)을 실행하거나 라이브러리에서 테이프를 꺼내려면 Administrator 프로파일로 변경해야 합니다. Administrator 프

로파일은 암호로 보호되어 있습니다. 이 프로파일의 기본 암호는 diva이지만 Configuration Utility에서 변경할 수 있습니다(이미 변경되었을 수 있음). 자세한 내용은 DIVArchive 소프트웨어 릴리스 7.3 고객 설명서 라이브러리를 참조하십시오.

https://docs.oracle.com/en/storage/#csm

Operator - Operator 프로파일은 User 프로파일 권한과 함께 Object Transfer Utility에 대한 액세스 권한을 제공합니다. 이 프로파일을 사용하려면 Administrator 프로파일과 동일한 암호를 입력해야 합니다.

부록 A

부록 A. 보안 배치 점검 목록

1. 관리자 계정 및 다음을 비롯하여 DIVArchive 관리자 또는 서비스 역할이 지정된 기타 모든 OS 계정에 대해 강력한 암호를 설정합니다.
   - DIVA, Oracle 사용자 ID(사용되고 있을 경우)
   - 모든 디스크 어레이 관리 계정
2. 로컬 관리자 OS 계정을 사용하는 대신 필요에 따라 다른 사용자 계정에 역할을 지정합니다.
3. Control GUI의 관리자 및 운영자에 대해 강력한 암호를 설정합니다. 기본적으로 설치된 암호를 즉시 강력한 암호로 변경합니다. Tools의 Configuration Utility에서 변경 작업을 수행할 수 있습니다.
4. Oracle 데이터베이스 로그인에 대해 강력한 암호를 설정합니다. 설치된 기본값에서 기본 Oracle 데이터베이스 사용자 암호를 변경합니다.
5. 모든 시스템에 방화벽을 설치하고 기본 DIVArchive 포트 규칙을 적용합니다. 방화벽 규칙을 사용하여 액세스해야 하는 IP로 DIVArchive API(tcp 9000)에 대한 액세스를 제한합니다.
6. 보안 업데이트가 포함된 OS 및 DIVArchive 업데이트를 주기적으로 설치합니다.
7. 바이러스 백신을 설치하고 성능을 위해 DIVArchive 프로세스 및 스토리지를 제외합니다.
8. 디스크와 테이프 장치가 동일한 HBA 포트를 공유하지 않도록 물리적으로 또는 FC 영역 분할을 통해 FC 디스크와 FC 테이프 드라이브를 분리하는 것이 좋습니다. 관리 대상 디스크의 경우 DIVArchive Actor만 디스크 및 테이프 드라이브에 대한 액세스 권한을 가져야 합니다. 이 보안 방식은 테이프나 디스크의 우발적 덮어쓰기로 인한 데이터 손실 사고를 예방하는 데 도움이 됩니다.
9. DIVArchive 구성 및 데이터베이스의 적절한 백업 세트를 설정합니다. 백업은 보안의 일부이며 실수나 침입으로 손실된 데이터를 복원하는 방법을 제공합니다. 멀리 떨어진 위치로 전송되는 경우 백업에 특정 정책이 포함되어야 합니다. 백업은 DIVArchive 테이프 및 디스크와 동일한 수준으로 보호되어야 합니다.