Oracle® DIVAnet

보안 설명서

릴리스 2.2

E86309-01

2017년 1월

ORACLE®

Oracle® DIVAnet
보안 설명서

E86309-01

목차

머리말

Oracle의 DIVAnet 보안 설명서에서는 Oracle DIVAnet 제품에 대한 정보를 제공하고 응용 프로그램 보안에 대한 일반적인 원칙을 설명합니다.

대상

이 설명서는 DIVAnet의 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 Oracle DIVAnet 2.2 제품에 대한 개요와 응용 프로그램 보안에 대한 일반적인 원칙을 설명합니다.

1.1. 제품 개요

Oracle DIVAnet은 여러 분산된 Oracle DIVArchive 시스템에 걸쳐 있는 아카이브 컨텐츠에 대한 통합 보기를 제공합니다. Oracle의 DIVArchive는 테이프 라이브러리 및 디스크 시스템에 아카이브를 지원하는 확장성 높은 컨텐츠 스토리지 관리 시스템입니다. DIVAnet은 DIVArchive 사이트 간, 그리고 고객 소스와 대상 서버 및 디스크에서 컨텐츠 이동을 원활하게 해줍니다. 이러한 작업은 재해 복구, 컨텐츠 분산, 액세스 제어, 성능 및 컨텐츠 가용성을 목적으로 수행됩니다.

DIVAnet의 주요 구성요소는 다음과 같습니다.

1.1.1. DIVAnet ClientAdapter 서비스

DIVArchive API 또는 DIVAnet GUI를 사용하고자 하는 응용 프로그램 클라이언트는 **DIVAnet ClientAdapter Service**에 연결합니다. 이 DIVAnet 서비스는 응용 프로그램으로부터 웹 및 소켓 연결을 수락하고 요청을 처리합니다. **ClientAdapter**는 DIVArchive 및 DIVAnet이 설치된 사이트에 로컬 응용 프로그램이 있는 각 사이트에서 구성됩니다.

1.1.2. DIVAnet ManagerAdapter 서비스

DIVAnet ManagerAdapter Service는 DIVAnet과 Oracle DIVArchive Manager 사이에서 다리 역할을 합니다. 다른 DIVAnet 시스템에서 원격 액세스를 제공하려면 구성해야 합니다.

1.1.3. DIVAnet DbSync 서비스

DIVAnet DbSync Service는 여러 DIVArchive 사이트의 자산 정보 동기화 및 DIVAnet 데이터베이스에 정보 저장을 담당합니다. **DbSync**는 여러 사이트의 **ManagerAdapter** 서비스와 원격으로 통신하여 아카이브 객체 정보를 동기화합니다. **DbSync**는 일반적으로 **ClientAdapter**와 함께 배치됩니다. **DbSync** 서비스 및 **ClientAdapter**는 모두 DIVAnet 데이터베이스에 대한 직접 액세스가 필요합니다.

1.1.4. DIVAnet 사용자 인터페이스(DIVAnetUI)

DIVAnetUI는 여러 DIVArchive 사이트에 걸쳐 DIVAnet 요청을 모니터하고, DIVAnet 자산(DIVA 아카이브 객체)을 확인, 복사 및 삭제할 수 있는 GUI 응용 프로그램입니다. API 또는 UI 자체를 통해 실행되었는지 여부에 관계없이 모든 DIVAnet 레벨 요청을 모니터할 수 있습니다. 또한 자산이 DIVAnet을 통해 아카이브되었는지 여부와 상관 없이 모든 구성된 DIVArchive 사이트에 대한 자산 정보를 볼 수 있습니다. **DIVAnetUI**는 요청 정보와 자산 정보를 모두 질의할 수 있는 유연한 방법을 제공합니다.

1.2. 일반 보안 원칙

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

1.2.1. 소프트웨어를 최신 상태로 유지

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

`https://edelivery.oracle.com/`

1.2.2. 중요 서비스에 대한 네트워크 액세스 제한

DIVAnet은 기본적으로 다음 TCP/IP 포트를 사용합니다.

- *`tcp/9801`*은 DIVAnet **ClientAdapter**에서 사용하는 기본 **WebService** 포트입니다.
- *`tcp/7101`*은 DIVAnet **ClientAdapter**에서 사용하는 기본 API 소켓 포트입니다(다른 포트 구성 가능).
- *`tcp/9800`*은 DIVAnet **ManagerAdapter**에서 사용하는 기본 **WebService** 포트입니다.

주:

이러한 포트 중 일부는 외부에 노출되어서는 안 되며, 구성 및 사용을 기반으로 합니다.

1.2.3. 가능한 최소 권한 원칙 사용

DIVAnet 서비스는 *`admin`* 또는 *`root`*로 실행하면 안됩니다. 응용 프로그램을 관리하는 데 사용되는 사용자가 아닌 다른 운영체제 사용자를 사용하여 서비스를 실행하면 전체적인 시스템 보안이 향상됩니다.

DIVanet Linux 설치 프로그램이 DIVAnet 설치를 수행하려면 두 명의 사용자(*`diva`* 및 운영체제 사용자)가 필요합니다. 관리자 및 운영자는 *`diva`* 계정을 사용하여 DIVAnet을 설치하고 모니터합니다. 운영체제 사용자는 DIVAnet 서비스를 제어합니다.

방화벽은 필요한 서비스로만 포트를 제한해야 합니다. DIVAnet에는 가능한 최소 권한으로 사용자 및 시스템을 제한하는 데 사용되는 액세스 제어 기능(액세스 제어의 간략한 설명 참조)이 포함되어 있습니다.

1.2.4. 시스템 작업 모니터

시스템 작업을 모니터하여 DIVAnet이 제대로 작동하고 있는지 및 비정상적인 작업이 기록되고 있는지 여부를 확인해야 합니다. *`$DIVANET_HOME/Program/log`* 폴더에 있는 로그 파일을 확인합니다.

1.2.5. 최신 보안 정보 유지

다양한 소프트웨어 제품에 대한 보안 정보 및 경보의 여러 소스에 액세스할 수 있습니다.

`http://www.us-cert.gov`

보안 사항을 최신으로 유지하는 기본적인 방법은 최신 릴리스의 DIVAnet 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 요구사항을 더 잘 이해하려면 다음과 같은 질문을 해야 합니다.

2.1.1. 어떤 리소스를 보호해야 합니까?

운영 환경의 다양한 리소스를 보호할 수 있습니다. 제공할 보안 레벨을 결정할 때 보호할 리소스의 유형을 고려하십시오.

DIVAnet을 사용할 때 다음과 같은 리소스를 보호해야 합니다.

2.1.1.1. DIVAnet 서버

DIVAnet은 하나 이상의 디스크(DIVAnet 시스템에 직접 연결된 로컬 또는 원격 디스크)에 연결된 서버에 설치됩니다. DIVAnet을 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

DIVAnet 시스템을 만드는 데 사용되는 데이터베이스 소프트웨어 및 데이터 리소스가 있습니다. 데이터는 대개 DIVAnet 시스템에 연결된 로컬 또는 원격 디스크에 있습니다. DIVAnet을 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 소스, 대상 및 아카이브 매체

DIVAnet은 요청 충족 프로세스에서 DIVArchive 소스와 대상 및 DIVA 아카이브 시스템(디스크 또는 테이프)을 사용합니다. 대개 DIVArchive 시스템으로 제어되는 이러한 서버 디스크 및 시스템 매체에 대한 승인되지 않은 개별적인 액세스는 보안 위험을 가져옵니다. DIVAnet 복사 작업에 대한 임시 데이터 저장소로 사용되는 **Source/Destinations**에는 액세스가 제한되어야 하고, 이러한 **Source/Destinations**를 DIVAnet 작업 전용으로 지정을

고려해야 합니다. 또한 전송이 암호화되고 신뢰할 수 있는 네트워크를 통해 이루어지도록 해야 합니다.

2.1.1.4. 구성 파일 및 설정

DIVAnet 시스템 구성 설정은 운영체제 레벨 관리자 이외의 사용자로부터 보호되어야 합니다. 일반적으로 이러한 설정은 운영체제 레벨 관리 사용자에 의해 자동으로 보호됩니다. 비관리 운영체제 사용자에게 구성 파일을 쓸 수 있도록 허용할 경우 보안 위험에 노출됩니다.

2.1.2. 누구로부터 리소스를 보호합니까?

일반적으로 위의 절에서 설명한 리소스는 구성된 시스템의 모든 비관리자 액세스나 WAN 또는 FC 패브릭을 통해 이러한 리소스에 액세스할 수 있는 악의적인 외부 시스템으로부터 반드시 보호해야 합니다.

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

전략 리소스에 대한 보호 실패는 부적절한 액세스(즉, 정상적인 DIVAdirector 작업을 벗어나는 데이터에 대한 액세스)부터 데이터 손상(실수로 자산 삭제 또는 정상적인 권한을 벗어나는 디스크나 테이프에 쓰기)에 이르기까지 다양합니다.

2.2. 권장되는 배치 토폴로지

이 절에서는 안전한 기반구조 구성요소의 설치 및 구성에 대해 설명합니다.

DIVAnet 설치에 대한 자세한 내용은 *DIVAnet 2.2* 설명서 라이브러리에서 *Oracle DIVAnet* 설치, 구성 및 작업 설명서를 참조하십시오.

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

DIVAnet을 설치 및 구성할 때는 다음 사항을 고려하십시오.

2.2.1. DIVAnet 설치

필요한 DIVAnet 구성요소만 설치해야 합니다. 예를 들어, 클라이언트 컴퓨터에서 **DIVAnetUI**만 실행하려는 경우 설치 중 설치할 구성요소 목록에서 **DIVAnet Services** 확인란을 선택 해제합니다. 설치 후 기본 DIVAnet 설치 디렉토리 권한과 소유자를 변경하려면 반드시 해당 변경이 보안에 끼치는 영향을 고려해야 합니다.

2.2.2. DIVArchive에 연결

Oracle은 시스템 보안 향상을 위해 DIVArchive Manager 시스템에 **ManagerAdapter** 구성요소를 설치할 것을 권장합니다. DIVArchive Manager 포트에 대한 외부 액세스가 필요하지 않은 경우 방화벽 소프트웨어를 사용하여 포트를 차단할 것을 권장합니다. 또한 대개 **DIVAnet DbSync WebService** 포트에 대한 외부 네트워크 액세스를 허용할 필요가 없습니다.

WAN을 통해 원격 DIVArchive 인스턴스에 연결하는 경우 신뢰할 수 있는 네트워크를 통해 연결합니다. 또한 *SSL/TLS*를 사용하여 원격 사이트의 **ManagerAdapter** 포트에 연결을 고려하십시오.

2.2.3. 디스크 시스템 보호

FC 영역 지정을 사용하여 디스크에 대한 액세스가 필요하지 않은 모든 서버로부터 광 섬유 채널을 통해 연결된 DIVAnet 디스크에 대한 액세스를 거부합니다. 가능하면 별도의 FC 스위치를 사용하여 액세스가 필요한 서버에만 물리적으로 연결하는 것이 좋습니다.

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.

2.3. 설치 후 구성

DIVAnet 설치 후 부록 A. 보안 배치 점검 목록의 보안 점검 목록으로 이동합니다.

3

3장. 보안 기능

잠재적인 보안 위협이 발생하지 않도록 DIVAnet 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

DIVAnet 서비스는 여러 방법을 사용하여 인증을 수행할 수 있습니다.

- **SSL/TLS 인증서** - DIVAnet이 원격 DIVAnet 서비스에 대한 아웃바운드 연결을 만들 때 DIVAnet은 인증서 보안 저장소를 질의합니다. 이 방법은 DIVAnet이 올바른 DIVAnet 서비스에 연결되는지 확인하는 데 도움이 됩니다. DIVAnet **ClientAdapter**에서 DIVArchive 인스턴스로 보안 연결을 만들려면 **WebServices**로 식별된 *`ConnectionType`*을 사용하여 **ManagerAdapter**를 통해 연결해야 합니다.
- **액세스 규칙** - 기술적으로는 액세스 제어의 형식이지만 액세스 규칙은 인바운드 IP 주소를 기준으로 인바운드 연결을 필터링할 수 있습니다. 이 기능은 승인된 시스템만 DIVAnet 서비스에 대한 적절한 액세스 권한을 가지도록 하는 데 필요합니다.

> **주의:**
>
> DIVAnet 서비스는 데이터베이스 암호를 구성의 일부로 사용합니다. 암호는 설치 후 즉시 그리고 이후 최소 180일마다 변경해야 합니다. 암호를 변경한 후에는 오라클 고객지원센터에서 필요한 경우 사용할 수 있는 안전한 오프라인 위치에 저장해 두어야 합니다.

3.3. 액세스 제어

액세스 규칙은 특정 사용자나 시스템이 분산된 아카이브 시스템에서 수행할 수 있는 작업을 제한하기 위해 만들 수 있습니다. 액세스 규칙은 다음 방식으로 실행할 수 있습니다.

- **ClientAdapter/MultiDiva 모드** - 실행할 수 있는 DIVAnet 요청의 유형을 제한합니다.
- **ManagerAdapter** - DIVAnet 요청(원격 시스템의 요청 등)을 충족하기 위해 실행할 수 있는 DIVArchive 요청의 유형을 제한합니다.

액세스 규칙은 **DIVAnetUI** 또는 API 소켓 연결(MAM 또는 자동화 시스템에서 시작 등)에서 시작된 요청에 영향을 줄 수 있습니다.

DIVAnet 요청에는 DIVAnet 레벨 또는 DIVArchive 레벨에서 실행되는 액세스 규칙이 있을 수 있습니다. DIVAnet 레벨의 경우, **ClientAdapter**는 요청이 수신된 위치에서 요청을 처리합니다. DIVArchive 레벨의 경우, 원격 **ManagerAdapter**는 DIVAnet 요청을 충족하기 위해 실행된 DIVArchive 요청을 처리합니다.

Oracle은 응용 프로그램 요구사항을 충족하는 가장 엄격한 규칙 세트를 만들 것을 권장합니다. 예를 들어, 관리자만 전역 삭제를 수행해야 하는 경우 다른 사람은 이 기능에 대한 액세스가 거부되도록 합니다. 시스템 사용자 그룹이 제한된 소스 및 대상 목록에만 액세스가 필요한 경우 사용자들이 해당하는 특정 소스 및 대상에 대해서만 요청을 실행할 수 있도록 합니다.

또한 요청을 충족하는 데 사용되는 사이트를 고려합니다. 예를 들어, 로컬 사이트의 사용자가 소스 또는 대상 사이트가 로컬 사이트가 아닌 위치에서 복사를 수행할 이유가 없다면(DIVAnet을 사용하여 가능), **ClientAdapter** 구성에서 이러한 규칙을 구성합니다.

마지막으로, 전체적으로 제외시킬 요청에서 특정 구성을 고려합니다. 예를 들어, 범주 없이 객체 이름만 있는 객체를 지정할 필요가 없는 경우 범주가 비어 있는 모든 요청을 제외시킵니다.

또한 각 ClientAdapter WorkflowProfile에는 WorkflowProfile에 지정된 요청에서 처리할 수 있는 유효한 메시지 목록이 포함되어 있습니다. **MultiDiva 모드**의 경우, 정보 메시지를 포함하여 특정 메시지가 처리되지 않도록 제외할 수 있는 방법을 제공합니다.

Oracle은 고유한 액세스 규칙을 정의하지 않더라도 *`AccessRules.xml.ini`* 파일에 정의된 기본 규칙부터 시작할 것을 권장합니다. DIVAnet 액세스 제어 기능에 대한 자세한 내용은 다음 사이트에서 제공하는 *Oracle DIVAnet 설치, 구성 및 작업 설명서*를 참조하십시오.

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

3.4. SSL/TLS 구성

DIVAnet에는 로컬 시스템에서 호스트되는 웹 서비스에 사용되는 개인 키 저장소 및 원격으로 호출되는 웹 서비스를 확인하는 데 사용되는 공개 키 저장소의 두 위치에 인증서 데이터가 있습니다. **Java Keytool 유틸리티**를 사용하여 키 저장소 암호를 변경하고 인증서를 추가 및 삭제할 수 있습니다.

키 저장소 만들기에 대한 자세한 내용은 다음을 참조하십시오.

`http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#CreateKeystore`

DIVAnet 웹 서비스 연결만 *SSL/TLS*를 사용합니다. 이 릴리스에서 DIVArchive API 소켓 연결을 사용한 DIVArchive 또는 DIVAnet 연결은 *SSL/TLS*를 사용하지 않습니다.

3.4.1. 개인 키 저장소

DIVAnet 개인 키 인증서 데이터가 저장되는 위치:

$DIVANET_HOME/Program/divanet/lib/diva129.jks

정확하게 하나의 인증서만 이 키 저장소에 나타나야 합니다. 이 인증서는 이 *$DIVANET_HOME* 디렉토리에서 실행 중인 서비스에서 호스트하는 웹 서비스에 사용됩니다. 제공된 인증서를 새 인증서로 교체하고, 네트워크의 각 DIVAnet 사이트에 대해 서로 다른 인증서를 사용할 것을 권장합니다.

이 키 저장소의 암호를 변경해야 합니다. 암호 정보를 *$DIVANET_HOME/Program/divanet/lib/diva129.properties*라는 새 파일에 저장하고, DIVAnet 서비스(Linux의 경우 *divanetsvc* 사용자)에서는 이 파일을 읽을 수 있지만 시스템의 일반 사용자(예: Linux의 경우 *diva* 사용자)는 읽을 수 없도록 합니다. 파일에 대해 다음 형식을 사용합니다.

keystorePassword=newpassword

3.4.2. 공개 키 저장소

보안 저장소라고도 하는 이 데이터는 다음 위치에 있습니다.

$DIVANET_HOME/Java/lib/security/cacerts2

이 인증서 데이터는 아웃바운드 웹 서비스 호출(**DIVAnetUI** 포함)에서 사용됩니다. 여러 공개 키를 이 키 저장소에 로드할 수 있습니다.

새 자체 서명된 인증서를 DIVAnet 개인 키 저장소에 추가한 경우 keytool 유틸리티를 사용하여 인증서를 내보냅니다. 그런 다음 이 사이트에서 **WebServices**를 호출하는 모든 응용 프로그램(DIVAnet 서비스, DIVAnetUI 등)은 내보낸 인증서를 고유의 공개 키 저장소에 추가해야 합니다.

부록 A

부록 A. 보안 배치 점검 목록

1. DIVAnet 관리자 또는 서비스 역할이 지정된 관리자 및 기타 모든 운영체제 계정에 대해 강력한 암호를 설정합니다. 여기에는 다음이 포함됩니다.
   - *diva*, *divanetsvc* 및 Oracle 사용자 ID(사용하는 경우)
   - 모든 디스크 관리 계정
2. 로컬 관리자 운영체제 계정을 사용하지 않습니다. 대신 필요에 따라 다른 사용자 계정에 역할을 지정합니다.
3. 각 DIVAnet 설치에 대해 사이트별 인증서를 사용하고 Oracle 데이터베이스 및 개인 키 저장소에 대해 강력한 암호를 정의합니다. Oracle 데이터베이스 운영체제 로그인에 대해 강력한 암호를 설정합니다.
4. 모든 DIVAnet 시스템에 방화벽 소프트웨어를 설치하고 기본 DIVAnet 포트 규칙을 적용합니다. 방화벽 규칙을 사용하여 액세스가 필요한 IP의 DIVAnet API 소켓(*tcp 7101*)에 대한 액세스를 제한합니다. DIVAnet의 액세스 규칙에서 이 단계를 수행합니다.
5. 보안 패치가 포함된 운영체제 및 DIVAnet 업데이트를 정기적으로 설치합니다.
6. 바이러스 백신을 설치하고 성능을 위해 DIVAdirector 프로세스 및 스토리지를 제외시킵니다.
7. 디스크와 테이프 장치가 동일한 HBA 포트를 공유하지 않도록 FC 디스크 및 FC 테이프 드라이브를 물리적으로 또는 FC 영역 지정을 통해 분리합니다. 이 보안 방식은 중요 데이터의 우발적 덮어쓰기로 인한 데이터 손실 사고를 예방하는 데 도움이 됩니다.
8. DIVAnet 구성 및 데이터베이스에 대해 포괄적인 백업 세트를 구성합니다. 백업은 보안의 일부이며 실수나 침입으로 손실된 데이터를 복원하는 방법을 제공합니다. 멀리 떨어진 위치로 전송되는 경우 백업에 특정 정책이 포함되어야 합니다. 백업은 DIVAnet 디스크와 동일한 수준으로 보호해야 합니다.