Oracle® Key Manager 3

보안 설명서

릴리스 3.1

E52203-02

2016년 4월

ORACLE

Oracle® Key Manager 3
보안 설명서

E52203-02

Copyright © 2007, 2016, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이센스 합의서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이센스 합의서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이센스, 전송, 배포, 진열, 실행, 발행 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이센스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이센스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이센스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제3자로부터 제공되는 컨텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. 사용자와 오라클 간의 합의서에 별도로 규정되어 있지 않는 한 Oracle Corporation과 그 자회사는 제3자의 컨텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제3자의 컨텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다. 단, 사용자와 오라클 간의 합의서에 규정되어 있는 경우는 예외입니다.

차례

표 목록

머리말

이 문서에서는 OKM 3(Oracle Key Manager 3)의 보안 기능에 대해 설명합니다.

대상

이 설명서는 OKM 3의 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 절에서는 제품의 개요를 살펴보고 애플리케이션 보안의 일반적인 원칙에 대해 설명합니다.

1.1. 제품 개요

OKM(Oracle Key Manager)은 암호화 키를 만들고 저장 및 관리합니다. 구성 요소는 다음과 같습니다.

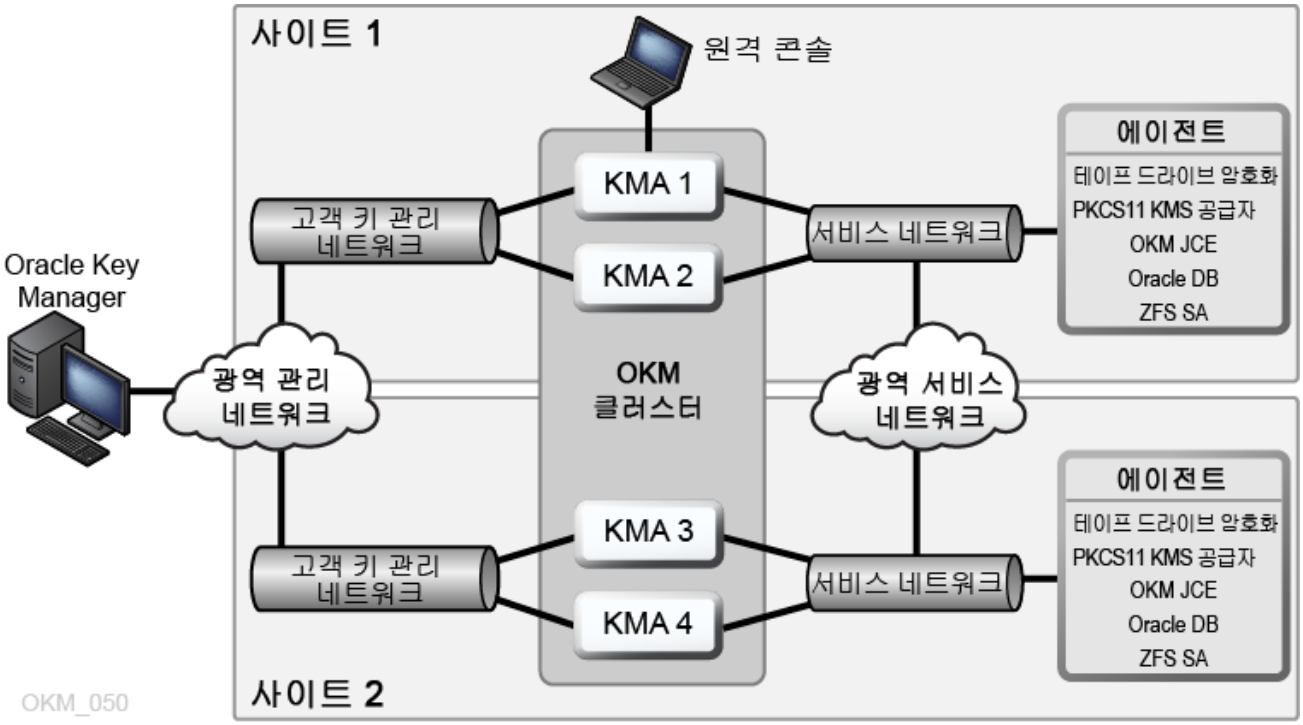
- KMA(키 관리 어플라이언스) – 정책 기반 수명 주기 키 관리, 인증, 액세스 제어 및 키 프로비저닝 서비스를 제공하는 보안 강화 장비입니다. 스토리지 네트워크에 대해 신뢰된 기관으로서 KMA는 모든 스토리지 장치가 등록 및 인증되었으며 모든 암호화 키 생성, 프로비전 및 삭제가 규정된 정책을 준수함을 보장합니다.
- Oracle Key Manager GUI – 워크스테이션에서 실행되며 IP 네트워크를 통해 KMA와 통신하여 OKM을 구성 및 관리하는 그래픽 사용자 인터페이스입니다. Oracle Key Manager GUI는 고객이 제공한 워크스테이션에 설치해야 합니다.
- Oracle Key Manager CLI – 워크스테이션에서 실행되며 IP 네트워크를 통해 KMA와 통신하여 공통적으로 실행되는 관리 작업을 자동화하는 2개의 명령줄 인터페이스입니다. Oracle Key Manager CLI는 고객이 제공한 워크스테이션에 설치해야 합니다.
- OKM 클러스터 – 시스템의 전체 KMA 세트입니다. 모든 KMA는 서로 인식하고 상호 간에 정보를 복제합니다.
- 에이전트 – OKM 클러스터에서 관리되는 키를 사용하여 암호화를 수행하는 장치나 소프트웨어입니다. 에이전트로는 테이프 드라이브를 암호화하는 StorageTek이 있습니다. 에이전트는 KMS 에이전트 프로토콜을 사용하여 KMA와 통신합니다. 에이전트 API는 에이전트 하드웨어 또는 소프트웨어에 통합된 소프트웨어 인터페이스 세트입니다.

OKM은 KMA와 에이전트, Oracle Key Manager GUI 및 CLI가 실행되고 있는 워크스테이션 간의 연결에 TCP/IP 네트워킹을 사용합니다. 유연한 네트워크 연결을 제공하기 위해 각 KMA의 네트워크 연결용으로 3개의 인터페이스가 제공됩니다.

- 관리 연결 – 고객 네트워크에 대한 연결에 사용됩니다.
- 서비스 연결 – 에이전트에 대한 연결에 사용됩니다.
- ILOM/ELOM 연결 – KMA의 ILOM 또는 ELOM에 대한 연결에 사용됩니다.

다음 그림의 예를 참조하십시오.

그림 1.1.



1.2. 일반 보안 원칙

다음 원칙은 애플리케이션을 안전하게 사용하는 데 반드시 필요한 사항입니다.

1.2.1. 소프트웨어를 최신 상태로 유지

올바른 보안 실행 원칙 중 하나는 모든 소프트웨어 버전 및 패치를 최신 상태로 유지하는 것입니다. My Oracle Support 웹 사이트(http://support.oracle.com)에서 최신 Oracle Key Manager 업그레이드 패키지 및 설치 프로그램이 제공됩니다.

1.2.2. 중요 서비스에 대한 네트워크 액세스 제한

비즈니스 애플리케이션은 방화벽으로 보호하십시오. 방화벽으로 보호하면 시스템에 대한 액세스가 알려진 네트워크 경로로 제한되며 필요한 경우 모니터링하고 제한할 수 있습니다. 또는 방화벽 라우터가 여러 개의 독립된 방화벽을 대체할 수 있습니다.

1.2.3. 최소 권한 원칙 준수

최소 권한 원칙이란 사용자에게 작업을 수행할 수 있는 최소한의 권한을 부여해야 한다는 것입니다. 인력은 부족하고 업무는 빨리 처리해야 하는 상황에서 책임, 역할, 권한 등의 과도한 부여(특히 조직의 수명 주기 초기)는 시스템 오용으로 이어질 수 있습니다. 사용자 권한을 정기적으로 검토하여 현재 작업 책임에 따라 권한이 적절한지 확인해야 합니다.

1.2.4. 시스템 작동 모니터

시스템 보안은 적합한 보안 프로토콜, 적절한 시스템 구성 및 시스템 모니터링을 기반으로 합니다. 감사 및 감사 레코드 검토는 세번째 요구 사항과 관련됩니다. 시스템 내의 각 구성 요소에는 일정 수준의 모니터링 기능이 있습니다. 이 문서에 있는 감사 권고 사항을 따르고 감사 레코드를 정기적으로 모니터합니다.

1.2.5. 최신 보안 정보 유지

오라클은 지속적으로 소프트웨어 및 설명서를 개선하고 있습니다. 매년 My Oracle Support 웹 사이트에서 개정이 있는지 확인하십시오.

2

2장. 보안 설치 및 구성

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

2.1. 사용자 환경 이해

보안 요구 사항을 제대로 파악하기 위해 다음과 같은 질문에 스스로 답해보십시오.

2.1.1. 어떤 리소스를 보호해야 합니까?

프로덕션 환경의 다양한 리소스를 보호할 수 있습니다. 제공해야 할 보안 레벨을 결정할 때는 보호할 리소스를 고려하십시오.

일반적으로 보호할 기본 리소스는 데이터입니다. 여기서는 다른 리소스에 대해서도 개략적으로 설명되는데, 이러한 리소스가 데이터 관리 및 보호와 연관되어 있기 때문입니다. 데이터 보호와 관련된 다양한 문제로는 데이터 손실(데이터를 사용할 수 없음)과 데이터 손상 또는 허용되지 않은 대상으로의 데이터 공개가 있습니다.

허용되지 않은 공개로부터 데이터를 보호하기 위해 암호화 키가 사용되는 경우가 많습니다. 따라서 암호화 키도 보호할 리소스에 해당합니다. 데이터의 고가용성을 유지하려면 안정성이 뛰어난 키 관리가 중요합니다. 보호할 다른 리소스 계층으로는 Oracle Key Manager 클러스터 자체 내의 자산(Key Management Appliance 등)이 있습니다.

2.1.2. 누구로부터 리소스를 보호해야 합니까?

액세스 권한이 없는 모든 사람들로부터 리소스를 보호해야 합니다. 이러한 리소스는 물리적으로 보호해야 합니다. 이러한 리소스에 대한 액세스 권한을 부여할 직원을 결정해야 합니다. 그런 다음 각 직원이 Oracle Key Manager 환경에서 실행할 수 있어야 할 작업의 유형을 파악하십시오.

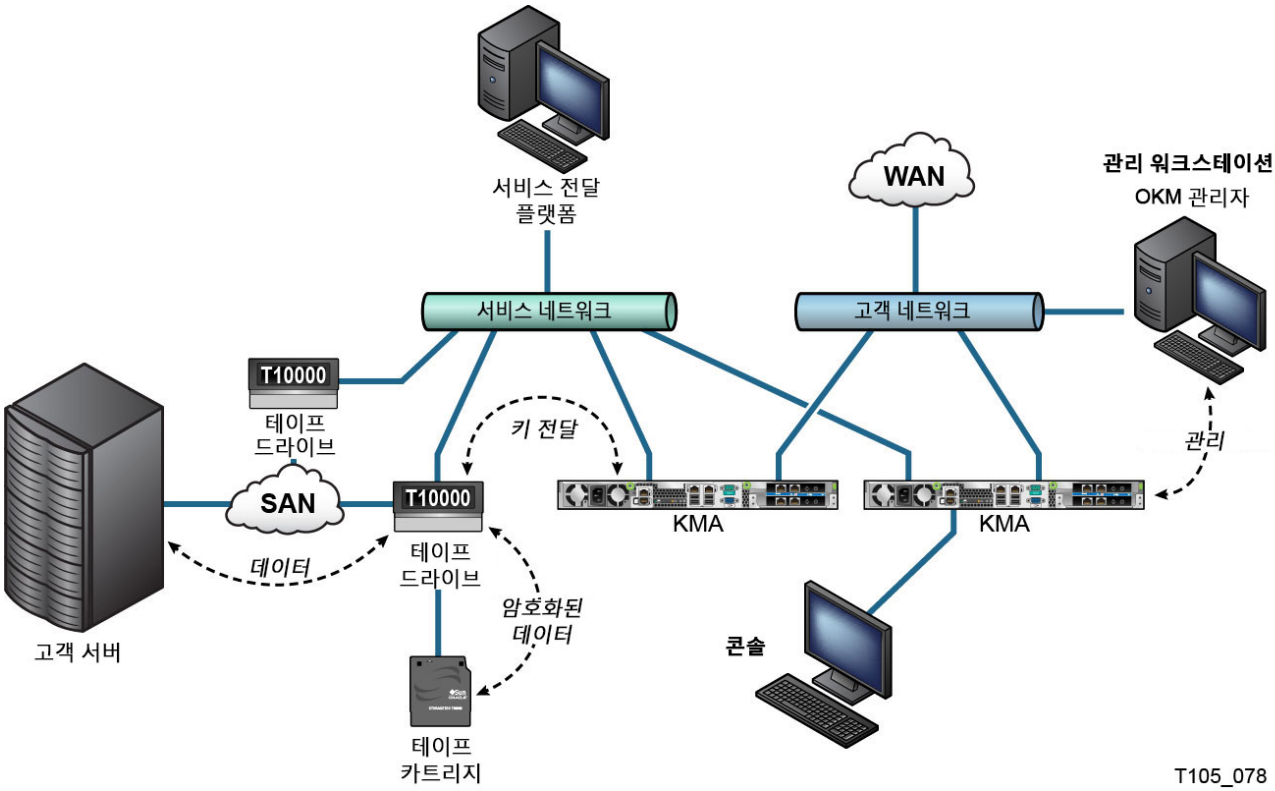
2.1.3. 전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?

어떤 경우에는 보안 체계의 결함이 쉽게 감지되고 불편함 정도로만 간주됩니다. 경우에 따라서는 결함으로 인해 리소스를 사용하는 회사 또는 개별 클라이언트에 막대한 피해가 발생할 수 있습니다. 각 리소스의 보안이 미치는 영향을 이해하면 해당 리소스를 적절하게 보호할 수 있습니다.

2.2. 권장되는 배치 토폴로지

다음 그림에서는 Oracle Key Manager 솔루션의 일반적인 배치를 보여줍니다.

그림 2.1. 일반적인 OKM 솔루션 배치



2.3. Key Management Appliance 설치

이 절에서는 OKM Key Management Appliance를 안전하게 설치 및 구성하는 방법에 대해 설명합니다.

KMA는 Oracle Key Manager 기능을 내장한 강화된 어플라이언스로 제조되었습니다.

OKM 클러스터에서 KMA를 설치 및 구성하는 단계는 다음과 같습니다.

1. 각 KMA를 랙에 설치합니다.
2. 각 KMA의 해당 ILOM을 보안 설정합니다.
3. OKM 클러스터에서 첫번째 KMA를 구성합니다.
4. OKM 클러스터에 KMA를 더 추가합니다.

OKM 클러스터 배치 계획에 대한 자세한 내용은 OKM 개요 및 계획 설명서를 참조하십시오.

2.3.1. 랙에 KMA 설치

Oracle 고객 서비스 센터 엔지니어가 *Oracle Key Manager Installation and Service Manual*에 설명된 절차에 따라 랙에 KMA를 설치합니다. Oracle 서비스 담당자는 이 설명서에서 자세한 내용을 참조할 수 있습니다.

2.3.2. KMA의 ILOM 보안

Oracle Key Manager KMA는 최신 ILOM 펌웨어를 사용하여 제조되었습니다. KMA의 ILOM은 Oracle 고객 서비스 센터 엔지니어 또는 고객에 의해 보안되어야 합니다. ILOM은 ILOM 펌웨어가 업그레이드된 후에도 보안되어야 합니다.

ILOM 보안은 보안을 손상시킬 수 있는 ILOM 변경을 방지하기 위해 특정 ILOM 설정을 지정하는 작업으로 구성됩니다. 지침은 OKM 관리 설명서의 서비스 프로세서 절차 부록에서 "ILOM 보안 강화"를 참조하십시오.

2.3.3. OKM 클러스터에서 첫번째 KMA 구성

첫번째 KMA를 구성하기 전에 먼저 이 OKM 클러스터에서 정의할 키 분할 자격 증명과 사용자 ID, 문장암호를 식별하십시오. 이를 위해 워크시트(예: OKM *Installation and Service Manual*(내부 전용)에 있는 워크시트)를 사용할 수 있습니다. 오라클 고객지원센터 담당자에게 문의하십시오.

적절한 담당자에게 해당 키 분할 자격 증명과 사용자 ID, 문장암호를 제공하십시오. 자세한 내용은 본 문서의 뒤쪽에 나오는 "쿼럼 보호"를 참조하십시오.

주:

해당 키 분할 자격 증명과 사용자 ID, 문장암호는 안전하게 보관하십시오!

웹 브라우저를 열고 원격 콘솔을 시작한 다음 원격 콘솔에서 OKM QuickStart 유틸리티를 시작하십시오. 이 KMA에서 OKM 클러스터를 초기화하려면 Oracle Key Manager 설명서 라이브러리에 포함된 *Oracle Key Manager* 관리 설명서에 설명된 클러스터 초기화 절차를 따르십시오.

이 절차에서는 키 분할 자격 증명 및 보안 관리자 권한을 갖는 사용자가 정의됩니다. QuickStart 절차가 완료되면 보안 관리자는 KMA에 로그인하여 추가 OKM 사용자를 정의해야 합니다.

2.3.4. 키 분할 자격 증명 정의 시 고려 사항

키 분할 사용자 ID와 문장암호를 더 적게 정의하고 임계값을 낮게 설정하면 편리성은 높아지지만 보안 수준은 낮아집니다. 키 분할 사용자 ID와 문장암호를 더 많이 정의하고 임계값을 높게 설정하면 편리성은 낮아지지만 보안 수준은 높아집니다.

2.3.5. 추가 OKM 사용자 정의 시 고려 사항

OKM 사용자를 적게 정의하면 일부 사용자에게 여러 역할이 지정되므로 편리성은 높아지지만 보안 수준은 낮아집니다. OKM 사용자를 많이 정의하면 대부분의 사용자에게 하나의 역할만 지정되므로 편리성은 낮아지지만 보안 수준은 높아집니다. 지정된 OKM 사용자가 수행하는 작업이 원활하게 추적됩니다.

2.3.6. OKM 클러스터에 KMA 추가

웹 브라우저를 열고 원격 콘솔을 시작한 다음 원격 콘솔에서 OKM QuickStart 유틸리티를 시작하십시오. OKM 클러스터에 이 KMA를 추가하려면 *Oracle Key Manager* 관리 설명서에 설명된 "클러스터 결합" 절차를 따르십시오.

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

2.3.7. KMA 추가 시 고려 사항

Oracle Key Manager에서는 편의를 위해 각 KMA에 대한 자율 잠금 해제 옵션을 제공합니다. 이 옵션은 클러스터에서 첫번째 및 추가 KMA에 대한 QuickStart를 실행하는 동안 정의되며 나중에 보안 관리자가 수정할 수 있습니다.

자율 잠금 해제가 사용으로 설정되면 KMA는 시작 시 자동으로 자체 잠금을 해제하며 쿼럼 승인 없이 키를 제공하려고 준비합니다. 자동 잠금 해제가 사용 안함으로 설정되면 KMA는 시작 시 잠금 상태를 유지하고 보안 관리자가 잠금 해제 요청을 실행하여 쿼럼에서 이 요청을 승인하기 전까지 키를 제공하지 않습니다.

보안을 극대화하기 위해 자율 잠금 해제는 사용 안함으로 설정하는 것이 좋습니다. 자율 잠금 해제 옵션에 대한 자세한 내용은 다음 링크의 *Oracle Key Manager Version 2.x Security and Authentication White Paper*를 참조하십시오.

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

2.3.8. 강화된 KMA의 특성

앞서 설명된 대로 KMA는 Oracle Key Manager 기능이 제공되는 강화된 어플라이언스로 제조되었습니다. 강화된 어플라이언스로서 KMA는 다음과 같은 특성을 갖습니다.

- Solaris 이미지에 불필요한 Solaris 패키지가 포함되지 않습니다. 예를 들어, FTP 및 Telnet 서비스와 유틸리티가 Solaris 이미지에 나타나지 않습니다.
- KMA는 코어 파일을 생성하지 않습니다.
- 표준 Solaris login(1) 유틸리티가 OKM 콘솔로 대체되었습니다. 따라서 사용자는 Solaris 콘솔에 로그인할 수 없습니다.
- SSH 서비스가 기본적으로 사용 안함으로 설정되어 있습니다. 고객 지원을 위해 보안 관리자는 SSH 서비스를 사용으로 설정하고 제한된 시간 동안의 지원 계정을 정의할 수 있습니다. 이 지원 계정은 유일하게 사용 가능한 계정이며 액세스 및 권한이 제한됩니다. Solaris 감사를 통해 지원 계정이 호출하는 명령이 추적됩니다.
- 루트 계정이 사용 안함으로 설정되어 있으며 역할로 구성됩니다.
- KMA에는 DVD 드라이브가 장착되어 있지 않습니다.
- USB 포트가 효과적으로 사용 안함으로 설정되어 있습니다.
- 사용되지 않는 네트워크 포트가 닫혀 있습니다.

- 실행 불가능 스택이 사용으로 설정되어 있습니다.
- 주소 공간 조회 임의 지정이 구성되어 있습니다.
- 실행 불가능 힙이 사용으로 설정되어 있습니다.
- 보안에 민감한 파일 시스템에 ZFS 암호화가 사용됩니다.
- SCAP PCI-DSS 벤치마크를 준수하도록 Solaris가 구성되어 있습니다.
- 불필요한 SMF 서비스가 사용 안함으로 설정되어 있습니다.
- 시스템 부트 프로세스를 보안 설정하여 커널 모듈 손상, 루트 키트 삽입 또는 기타 악의적인 프로그램으로부터 보호할 수 있도록 SPARC T7-1 기반 KMA에서 Oracle Solaris 확인된 부트를 구성할 수 있습니다.
- SPARC T7-1 및 Netra SPARC T4-1 서버 기반의 최신 KMA는 전원이 공급되는 동안 섀시 도어가 열리면 변경 증거(ILOM 결함)가 감지됩니다.
- ILOM 3.2 펌웨어가 이제 FIPS 140-2 레벨 1 인증을 획득하여 FIPS 모드로 구성할 수 있습니다.
- 포렌식을 지원하기 위해 기본 감사 및 보고서 도구가 정기적으로 실행됩니다. 이러한 보고서는 OKM 시스템 덤프에 포함되어 있습니다.
- 하드웨어 보안 모듈을 사용하거나 사용하지 않고 FIPS 140-2 레벨 1 보안 원칙(Solaris 11.1용으로 설명됨)에 따라 Solaris 암호화 보안 프레임워크가 구성되어 있습니다.

2.4. TCP/IP 연결 및 KMA

엔티티(OKM Manager, 에이전트 및 동일 클러스터의 다른 KMA)와 KMA 사이에 방화벽이 존재할 경우 다음 포트에서 엔티티가 KMA와 TCP/IP 연결을 설정할 수 있도록 허용해야 합니다.

- OKM Manager-KMA 통신을 위해서는 3331, 3332, 3333, 3335 포트가 필요합니다.
- 에이전트-KMA 통신을 위해서는 3331, 3332, 3334, 3335 포트가 필요합니다.
- KMA-KMA 통신을 위해서는 3331, 3332, 3336 포트가 필요합니다.

주:

KMA에서 IPv6 주소를 사용하도록 구성하는 사용자의 경우, IPv4 기반 경계면 방화벽에서 IPv6-over-IPv4 터널링 트래픽이 내부 호스트에 도달할 수 없도록 모든 아웃바운드 IPv4 프로토콜 41 패킷과 UDP 포트 3544 패킷을 삭제하도록 구성해야 합니다.

자세한 내용은 방화벽 구성 설명서를 참조하십시오. 표 2.1. “KMA 포트 연결 ”은 KMA에서 명시적으로 사용하는 포트 또는 KMA에서 서비스를 제공하는 포트를 나열하고 있습니다.

표 2.1. KMA 포트 연결

포트 번호	프로토콜	방향	설명
22	TCP	수신	SSH(기술 지원이 사용으로 설정된 경우에만)
123	TCP/UDP	수신	NTP
3331	TCP	수신	OKM CA 서비스
3332	TCP	수신	OKM 인증 서비스

포트 번호	프로토콜	방향	설명
3333	TCP	수신	OKM 관리 서비스
3334	TCP	수신	OKM 에이전트 서비스
3335	TCP	수신	OKM 복구 서비스
3336	TCP	수신	OKM 복제 서비스

표 2.2. “기타 서비스 ”는 사용되지 않을 수 있는 포트에서 수신되는 기타 서비스를 보여줍니다.

표 2.2. 기타 서비스

포트 번호	프로토콜	방향	설명
53	TCP/UDP	연결	DNS(KMA가 DNS를 사용하도록 구성된 경우에만)
68	UDP	연결	DHCP(KMA가 DHCP를 사용하도록 구성된 경우에만)
111	TCP/UDP	수신	RPC(KMA가 rpcinfo 질의에 응답). 이 포트는 KMS 2.1 이전 버전에서만 외부 요청에 열려 있습니다.
161	UDP	연결	SNMP(SNMP Manager가 정의된 경우에만)
161	UDP	수신	SNMP(Hardware Management Pack이 사용으로 설정된 경우에만)
514	TCP	연결	원격 syslog(암호화되지 않은 TCP를 사용하도록 원격 syslog 서버가 정의 및 구성된 경우에만)
546	UDP	연결	DHCPv6(KMA가 DHCP 및 IPv6을 사용하도록 구성된 경우에만)
4045	TCP/UDP	수신	NFS 잠금 데몬(KMS 2.0만 해당)
6514	TLS over TCP	연결	원격 syslog(TLS를 사용하도록 원격 syslog 서버가 정의 및 구성된 경우에만)

주:

포트 443은 고객이 방화벽을 통해 서비스 프로세서 웹 인터페이스 및 OKM 콘솔에 액세스할 수 있도록 열어 두어야 합니다. ELOM 및 ILOM 포트는 *Oracle Key Manager Installation and Service Manual*을 참조하십시오.

표 2.3. “ELOM/ILOM 포트 ”은 KMA ELOM/ILOM 포트를 보여줍니다. 방화벽 외부에서 ELOM/ILOM에 액세스해야 하는 경우 이러한 포트가 사용으로 설정됩니다. 그렇지 않은 경우에는 ELOM/ILOM IP 주소에 대해 사용으로 설정할 필요가 없습니다.

표 2.3. ELOM/ILOM 포트

포트 번호	프로토콜	방향	설명
22	TCP	수신	SSH(ELOM/ILOM 명령줄 인터페이스의 경우)
53	TCP/UDP	연결	DNS(DNS가 구성된 경우에만 필요함)
68	UDP	연결	ELOM/ILOM에 DHCP가 필요한 경우 주: DHCP 및 ELOM/ILOM에 대한 설명서는 제공되지 않지만, 이들은 지원됩니다.

포트 번호	프로토콜	방향	설명
80	TCP	수신	HTTP(ELOM/ILOM 웹 인터페이스의 경우) HTTP가 필요한 경우. 그렇지 않은 경우 사용자가 다음 위치에 있는 원격 콘솔에 연결하는 방법에 대한 지침을 참조할 수 있습니다. ELOM: http://docs.oracle.com/cd/E19121-01/sf.x2100m2/819-6588-14/819-6588-14.pdf ILOM: http://docs.oracle.com/cd/E19860-01/index.html
161	UDP	수신/연결	SNMPv3(구성 가능, 기본 포트)
443	TCP/TLS	수신	Embedded/Integrated Lights Out Manager TLS(Transport Layer Security)를 통한 관리 프로토콜(WS-Man)용 DMTF (Desktop Management Task Force) 웹 서비스
623	UDP	수신	IPMI(Intelligent Platform Management Interface)

3

3장. 보안 기능

이 절에서는 제품에서 제공하는 구체적인 보안 메커니즘의 개요를 살펴봅니다.

3.1. 잠재적 위협

암호화 기반 에이전트를 사용하는 고객의 주된 문제는 다음과 같습니다.

- 정책 위반 시 정보 공개
- 데이터 손실 또는 삭제
- 비즈니스 연속성 사이트 등에서의 심각한 오류 발생 시 허용할 수 없는 데이터 복원 지연
- 감지되지 않은 데이터 수정.

3.2. 보안 기능의 목표

Oracle Key Manager 보안 기능의 목표는 다음과 같습니다.

- 암호화된 데이터가 공개되지 않도록 보호.
- 공격에 대한 노출 최소화.
- 뛰어난 안정성 및 가용성 제공.

3.3. 보안 모델

보안 설명서의 이 절에서는 시스템이 대응해야 할 위협에 대해 대략적인 개요를 설명하며 각 보안 기능을 결합하여 공격에 대비하는 방법을 제공합니다.

이러한 보호를 제공하는 중요 보안 기능은 다음과 같습니다.

- 인증 – 권한이 부여된 개인만 시스템 및 데이터에 액세스할 수 있도록 합니다.
- 권한 부여 – 시스템 권한 및 데이터에 대한 액세스 제어로, 개인이 적절한 액세스 권한을 얻도록 하는 인증에 기초합니다.
- 감사 – 관리자가 인증 메커니즘 침해 시도와 액세스 제어 침해 시도나 성공을 감지할 수 있습니다.

Oracle Key Manager의 보안 및 인증 요소에 대한 자세한 내용은 다음 링크의 *Oracle Key Manager Version 2.x Security and Authentication White Paper*를 참조하십시오.

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

3.4. 인증

Oracle Key Manager 구조는 사용자 작업을 위해 시스템의 모든 요소 간(KMA와 KMA, 에이전트와 KMA, Oracle Key Manager GUI 또는 CLI와 KMA 간)에 상호 인증을 제공합니다.

시스템의 각 요소(예: 새 암호화 에이전트)는 OKM에서 ID 및 문장암호를 만들어 시스템에 등록됩니다. 해당 ID 및 문장암호는 추가될 요소에 입력됩니다. 예를 들어, 시스템에 테이프 드라이브가 추가되는 경우 에이전트와 KMA는 공유 문장암호를 기반으로 시도/응답 프로토콜을 자동 실행합니다. 이를 통해 에이전트는 에이전트에 대한 루트 CA(인증 기관) 인증서, 새 키 쌍 및 서명된 인증서를 얻습니다. 현재 위치에서 루트 CA 인증서, 에이전트 인증서 및 키 쌍을 사용하여 에이전트는 KMA와의 모든 후속 통신을 위해 TLS(Transport Layer Security) 프로토콜을 실행할 수 있습니다. 모든 인증서는 X.509 인증서입니다.

OKM은 루트 인증 기관으로 작동하여 루트 인증서를 생성하고, KMA는 이 루트 인증서를 사용하여 에이전트, 사용자 및 새 KMA에 사용되는 인증서를 파생(자체 서명)합니다.

3.5. 액세스 제어

액세스 제어 유형은 다음과 같습니다.

- 사용자 및 역할 기반 액세스 제어
- 쿼럼 보호

3.5.1. 사용자 및 역할 기반 액세스 제어

Oracle Key Manager는 각각 사용자 ID와 문장암호를 가진 여러 사용자를 정의할 수 있는 기능을 제공합니다. 각 사용자에게는 하나 이상의 미리 정의된 역할이 지정됩니다. 이러한 역할에 따라 사용자가 Oracle Key Manager 시스템에서 수행할 수 있는 작업이 결정됩니다. 역할은 다음과 같습니다.

- 보안 관리자 – Oracle Key Manager 설정 및 관리를 수행합니다.
- 운영자 – 에이전트 설정 및 일상적인 작업을 수행합니다.
- 준수 관리자 – 키 그룹을 정의하고 키 그룹에 대한 에이전트 액세스를 제어합니다.
- 백업 운영자 – 백업 작업을 수행합니다.
- 감사자 – 시스템 감사 추적을 확인합니다.
- 쿼럼 구성원 – 보류 중인 쿼럼 작업을 확인 및 승인합니다.

보안 관리자는 OKM 클러스터에서 KMA를 설정하는 QuickStart 프로세스를 수행할 때 정의됩니다. 나중에 추가 사용자를 정의하려면 사용자가 Oracle Key Manager GUI를 사용하여 보안 관리자로 클러스터에 로그인해야 합니다. 보안 관리자는 특정 사용자에게 여러 역할을 지정하도록 선택할 수도 있고, 여러 명의 사용자에게 하나의 특정 역할을 지정하도록 선택할 수도 있습니다.

각 역할에서 허용되는 작업 및 보안 관리자가 사용자를 만들고 해당 사용자에게 역할을 지정하는 방법에 대한 자세한 내용은 다음 링크의 Oracle Key Manager 설명서 라이브러리에 포함된 *Oracle Key Manager* 관리 설명서를 참조하십시오.

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

이 역할 기반 액세스 제어는 운영 기능을 구분할 수 있도록 NIST(National Institute of Standards and Technology) SP(Special Publication) 800-60 운영 역할을 지원합니다.

3.5.2. 쿼럼 보호

경우에 따라 중요한 작업을 수행하기 위해 추가적인 보안 레벨이 필요할 수 있습니다. OKM 클러스터에 KMA를 추가하고, KMA의 잠금을 해제하고, 사용자를 만들고, 사용자에게 역할을 추가하는 작업이 이에 해당합니다. 이러한 보안을 구현하기 위해 시스템에서는 앞서 설명된 역할 기반 액세스와 함께 일련의 키 분할 자격 증명을 사용합니다.

키 분할 자격 증명은 특정 작업을 완료할 수 있도록 시스템에 필요한 최소 개수의 쌍과 함께 일련의 사용자 ID와 문장암호 쌍으로 구성됩니다. 키 분할 자격 증명을 "쿼럼", 최소 개수를 "쿼럼 임계값"이라고도 합니다.

Oracle Key Manager에서는 최대 10개의 키 분할 사용자 ID/문장암호 쌍과 임계값을 정의할 수 있습니다. 이는 QuickStart 프로세스 중 OKM 클러스터에서 첫번째 KMA가 구성될 때 정의됩니다. 키 분할 사용자 ID 및 문장암호는 시스템에 로그인할 때 사용되는 사용자 ID 및 문장암호와 다릅니다. 사용자가 쿼럼 승인이 필요한 작업을 시도하면 정의된 키 분할 사용자 및 문장암호 임계값을 통해 이 작업이 승인되어야만 시스템에서 이 작업이 수행됩니다.

3.6. 감사

각 KMA는 OKM 클러스터에서 에이전트, 사용자 및 피어 KMA가 실행한 작업을 비롯하여 직접 수행하는 작업에 대한 감사 이벤트를 기록합니다. 또한 KMA는 에이전트, 사용자 또는 피어 KMA가 인증을 실패할 때마다 감사 이벤트를 기록합니다. 보안 위반을 나타내는 감사 이벤트에 유의해야 합니다. 보안 위반을 나타내는 감사 이벤트로는 인증 실패가 있습니다. OKM 클러스터에서 SNMP 에이전트가 식별되면 KMA는 보안 위반이 발생하는 경우 해당 SNMP 에이전트로 SNMP INFORM을 전송합니다. 원격 Syslog가 구성된 경우 KMA는 또한 이러한 감사 메시지를 구성된 서버로 전달합니다. "원격 *Syslog* "를 참조하십시오.

사용자는 OKM 클러스터에 올바른 방식으로 로그인해야 하며 역할을 지정 받아야만 감사 이벤트를 확인할 수 있습니다.

KMA는 감사 이벤트를 관리하며, 보존 기간 및 제한(개수)을 기반으로 오래된 감사 이벤트를 제거합니다. 보안 관리자는 필요에 따라 이러한 보존 기간 및 제한을 수정할 수 있습니다.

3.7. 기타 보안 기능

Oracle Key Manager는 기타 보안 기능도 제공합니다. 기타 OKM 기능에 대한 자세한 내용은 다음 링크의 *Oracle Key Manager Overview*를 참조하십시오.

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf

3.7.1. 보안 통신

에이전트와 KMA, 사용자와 KMA, KMA와 피어 KMA 간의 통신 프로토콜은 동일합니다. 각각의 경우에 시스템에서는 통신을 시작하는 엔티티에 문장암호를 사용하여 시도/응답 프로토콜을 수행합니다. 성공하면 엔티티에 인증서 및 해당하는 개인 키가 제공됩니다. 이 인증서와 개인 키는 TLS(Transport Layer Security)(보안 소켓) 채널을 설정할 수 있습니다. 연결의 양쪽 끝이 서로 인증하는 상호 인증이 수행됩니다. OKM 3.1+ KMA는 피어 투 피어 복제 트래픽에 항상 TLS 1.2를 사용합니다.

3.7.2. 하드웨어 보안 모듈

KMA에서는 하드웨어 보안 모듈(별도로 주문 가능)을 사용할 수 있습니다. 이 하드웨어 보안 모듈, 즉 SCA(Sun Cryptographic Accelerator) 6000 카드는 FIPS 140-2 레벨 3 인증을 받았으며 AES(Advanced Encryption Standard) 256비트 암호화 키를 제공합니다. (이 인증서는 2015년 12월 31일에 만료된 후 갱신되지 않아 이후 릴리스에서는 대체 HSM이 제공될 예정입니다.) SCA 6000 카드는 FIPS 140-2 레벨 3 작동 모드를 지원하며 OKM은 항상 이 방식으로 카드를 사용합니다. OKM 클러스터가 FIPS 준수 모드로 작동하면 암호화 키가 SCA 6000 카드의 암호화 경계를 언래핑 형식으로 유지하지 않습니다. SCA 6000 카드는 SHA-1을 사용하여 암호화 키를 생성하는 FIPS 186-2 DSA 난수 생성기에 지정된 대로 FIPS에서 승인한 난수 생성기를 사용합니다.

KMA가 SCA 6000 카드를 사용하도록 구성되지 않은 경우 SCF(Solaris Cryptographic Framework) PKCS#11 소프트 토큰을 사용하여 암호화가 수행됩니다. SCF는 최근에 게시된 Solaris FIPS 140-2 보안 정책에 따라 FIPS 140 모드로 구성됩니다.

3.7.3. AES 키 래핑

Oracle Key Manager는 키를 암호화하는 256비트 키와 함께 AES 키 래핑(RFC 3994)을 사용하여 만들어진 후 KMA에 저장되고 에이전트로 전송되거나 키 전송 파일 내에서 전송되는 대칭 키를 보호합니다.

3.7.4. 키 복제

OKM 클러스터의 첫번째 KMA가 초기화되면 KMA는 대용량 키 풀을 생성합니다. 클러스터에 KMA가 더 추가되면 새 KMA에 키가 복제되고 데이터 암호화에 사용되도록 준비됩니다. 클러스터에 추가된 각 KMA는 키 풀을 생성하여 클러스터의 피어 KMA에 복제합니다. 모든 KMA는 에이전트에 대해 항상 준비 키를 사용할 수 있도록 키 풀 크기를 관리하기 위해 필요에 따라 새 키를 생성합니다. 새 키가 필요할 경우 에이전트는 클러스터의 KMA에 연락하여 새 키를 요청합니다. KMA는 키 풀에서 준비 키를 인출하여 에이전트의 기본 키 그룹과 데이터 단위에 이 키를 지정합니다. 그런 다음 KMA는 네트워크를 통해 클러스터의 다른 KMA에 해당 데이터베이스 업데이트를 복제합니다. 나중에 에이전트는 클러스터의 다른 KMA에 연락하여 키를 검색할 수 있습니다. 일반 텍스트의 키 자료는 네트워크를 통해 전송되지 않습니다.

3.7.5. Solaris FIPS 140-2 보안 정책

2013년 12월, NIST(National Institute of Standards and Technology)에서는 Solaris 11의 Oracle Solaris 커널 암호화 프레임워크 모듈에 대해 FIPS 140-2 레벨 1 검증 인증서 #2061을 수여했습니다. 2014년 1월, NIST에서는 Oracle Solaris Userland 암호화 프레임워크(SPARC T4 및 SPARC T5 사용)에 대해 FIPS 140-2 레벨 1 검증 인증서 #2076을 수여했습니다. Oracle Key Manager 3.1.0 KMA는 FIPS 140-2 검증 테스트가 아직 진행 중인 Solaris 11.3을 기반으로 합니다. Oracle Key Manager 3.1.0 KMA의 Oracle Solaris 커널 암호화 프레임워크는 *Oracle* 커널 암호화 프레임워크 보안 정책에 따라 구성되었습니다. 마찬가지로, KMA도 *Oracle Solaris Userland* 암호화 프레임워크*(SPARC T4* 및 *SPARC T5* 사용*)* 보안 정책에 따라 구성되었습니다. OKM은 출시될 때 최신 Solaris 보안 정책으로 업데이트될 예정입니다.

3.7.6. 소프트웨어 업그레이드

모든 KMA 소프트웨어 업그레이드 번들은 승인되지 않은 소스에서의 악의적인 소프트웨어 로드를 방지하기 위해 디지털 방식으로 서명되었습니다.

4

4장. 끝점

OKM은 다양한 암호화 끝점을 지원합니다. 지원되는 끝점은 다음과 같습니다.

- 암호화 가능 테이프 드라이브
- Oracle TDE(Transparent Database Encryption) 11g 이상
- Oracle ZFS Storage Appliance
- Oracle Solaris 11 ZFS File System

또한 끝점 도구는 애플리케이션 개발자가 사용할 수 있거나, PKCS#11의 경우 Oracle Database의 TDE(Transparent Database Encryption)에서 사용할 수 있습니다.

4.1. Linux PKCS#11 KMS 공급자

Linux PKCS#11 KMS 공급자는 PKCS#11을 사용하여 OKM과 통신하려는 고객이 사용할 수 있습니다. 관리자는 My Oracle Support 웹 사이트에서 Linux PKCS#11 KMS 공급자를 다운로드하여 Oracle Enterprise Linux Server에 설치할 수 있습니다. Linux PKCS#11 KMS 공급자는 같은 보안 특성을 제공하며 다른 에이전트와 동일한 방식으로 Oracle Key Manager 어플라이언스를 인증합니다. Linux PKCS#11 KMS 공급자는 */var/opt/kms/username* 디렉토리에 로그 파일 및 프로파일 정보를 저장합니다. 사용자 및/또는 관리자는 수동으로 또는 logrotate와 같은 유틸리티를 사용하여 이 로그 파일을 관리해야 합니다. */var/opt/kms/username* 디렉토리에 대한 액세스 제어는 적절한 권한을 통해 제한해야 합니다. 프로파일 디렉토리 내에서 에이전트에 대한 인증 자격 증명은 PKCS#12 파일에 보존됩니다. PKCS#12 파일은 암호로 보안됩니다. Linux PKCS#11 KMS 공급자에 대한 자세한 내용은 다음 링크의 Oracle Key Manager 설명서 라이브러리에 포함된 *Oracle Key Manager* 관리 설명서를 참조하십시오.

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#mainframeswncs

4.2. Solaris용 PKCS#11 KMS 공급자

유사한 PKCS#11 KMS 공급자를 Solaris 10 및 Solaris 11에서 사용할 수 있습니다.

4.3. JCE KMS 공급자

Java Cryptographic Environment 공급자는 OKM에서 키를 얻을 수 있는 Java 클라이언트 애플리케이션을 구현하려는 개발자가 사용할 수 있습니다. 이 제품은 다양한 Oracle 제품과 통합되었으며 Oracle Technology Network에서 제공합니다.

4.4. Oracle Enterprise Manager용 OKM 플러그인

OEM(Oracle Enterprise Manager) Cloud Control용 OKM(Oracle Key Manager) 어플라이언스 플러그인은 OKM 클러스터에 대한 모니터링을 제공합니다. 클러스터에 속한 각 KMA를 이 플러그인에서 모니터합니다. 이 도구에 대한 보안 설명서가 제공됩니다.

5

5장. 원격 Syslog

Oracle Key Manager는 원격 syslog를 지원합니다. 암호화되지 않은 TCP 또는 TLS(Transport Layer Security)를 통해 RFC 3164 또는 RFC 5424 메시지 형식의 메시지를 원격 syslog 서버로 전송하도록 KMA를 구성할 수 있습니다. RFC 5425는 RFC 5424 메시지 형식의 syslog 메시지를 전송하기 위해 보안 연결을 제공하는 TLS 사용에 대해 설명합니다.

보안 관리자는 암호화되지 않은 TCP 또는 TLS를 통해 메시지를 전송하도록 KMA를 구성할 수 있습니다. TLS를 사용하여 KMA와 원격 syslog 서버 간의 통신을 인증하고 암호화하는 것이 더 안전합니다. KMA는 인증서와 공개 키를 요청하는 방식으로 원격 syslog 서버를 인증합니다. 선택적으로 원격 syslog 서버가 상호 인증을 사용하도록 구성할 수 있습니다. 상호 인증을 사용할 경우 원격 syslog 서버는 권한이 부여된 클라이언트(예: KMA)에서 보내는 메시지만 수락합니다. 상호 인증을 사용하도록 구성된 경우 원격 syslog 서버는 KMA의 신원을 확인하기 위해 KMA로부터 인증서를 요청합니다.

6

6장. Hardware Management Pack

Oracle Key Manager는 SPARC T7-1, Netra SPARC T4-1 및 Sun Fire X4170 M2 KMA에서 Oracle HMP(Hardware Management Pack)를 지원합니다. HMP 제품은 ILOM과 함께 Oracle 단일 시스템 관리 제품군입니다. 보안 관리자는 KMA에 있는 HMP가 Solaris에서 관리 에이전트를 사용하여 SNMP를 통해 KMA의 인밴드 모니터링을 사용하도록 설정할 수 있습니다. HMP 소프트웨어는 사전 설치되어 있지만 SNMP 에이전트 구성과 함께 사용 안함으로 설정되어 있습니다. 따라서 HMP가 사용으로 설정될 때까지 SNMP 에이전트 수신 포트가 열리지 않습니다. HMP는 기본적으로 사용 안함으로 설정되어 있습니다.

HMP를 사용으로 설정할 경우 다음과 같이 기능이 제공됩니다.

- 하드웨어 문제가 Oracle Key Manager 관련 SNMP 알림 또는 KMA 중단으로 표시되기 전에 이 문제에 대한 알림이 제공됩니다.
- OKM 클러스터의 지원되는 임의 또는 모든 KMA에서 HMP를 사용으로 설정할 수 있습니다.
- MIB-II, SUN-HW-MONITORING-MIB, SUN-STORAGE-MIB를 비롯한 KMA에 있는 SNMP MIB에 대해 읽기 전용 SNMP Get 작업을 사용할 수 있습니다.
- SNMP Receivelet 및 SNMP Fetchlet을 통해 Oracle Red Stack을 Oracle Enterprise Manager와 통합할 수 있습니다.

KMA에서 HMP를 사용으로 설정할 때 다음과 같은 보안 고려 사항을 염두에 두어야 합니다. 사용으로 설정할 경우 HMP는 다음과 같이 동작합니다.

- Oracle Key Manager 클러스터에서 구성되어 사용으로 설정된 프로토콜 v2c SNMP 관리자를 사용합니다. SNMP v2c 프로토콜은 SNMP v3 프로토콜의 향상된 보안 기능을 제공하지 않습니다.
- KMA에 있는 SNMP 관리 에이전트가 사용으로 설정되므로 해당 KMA에서 SNMP MIB 정보에 대한 읽기 전용 네트워크 액세스가 허용됩니다.
- *Oracle Hardware Management Pack* 보안 설명서(http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf)에서 식별된 보안 위험이 다음 방법에 따라 완화됩니다.
  - "시스템 관리 제품을 사용하여 부트 가능한 루트 환경을 얻을 수 있습니다." - KMA를 강화하면 시스템 사용자가 루트 액세스를 사용할 수 없습니다. SNMP는 읽기 전용 액세스를 사용하도록 구성됩니다. 따라서 SNMP Put 작업이 거부됩니다.
  - "시스템 관리 제품에는 관리자나 루트 권한으로 실행해야 하는 강력한 도구가 있습니다." - KMA에 대한 루트 액세스를 사용할 수 없습니다. 따라서 시스템 사용자가 이 도구를 실행할 수 없습니다.

부록 A

부록 A. 보안 배치 점검 목록

다음 보안 점검 목록에는 키 관리 시스템 보안에 유용한 지침이 포함되어 있습니다.

1. 물리적으로 보안된 환경에 각 KMA를 설치합니다.
2. 각 KMA에서 OpenBoot PROM 또는 BIOS를 보안 설정합니다.
3. 각 KMA에서 Lights Out Manager를 보안 설정합니다.
4. 이 Oracle Key Manager 클러스터에 대한 키 분할 구성을 정의합니다.
5. 적절한 경우 각 KMA에 대한 자율 잠금 해제 설정을 구성합니다.
6. Oracle Key Manager 사용자 및 연관된 역할을 정의합니다.
7. 최소 권한 원칙을 따릅니다.
   a. 필요에 따라 각 Oracle Key Manager 사용자에게만 해당 역할을 부여합니다.
8. Oracle Key Manager 클러스터에서 작동을 모니터합니다.
   a. Oracle Key Manager 감사 로그에 기록된 오류, 특히 보안 위반을 조사합니다.
9. 키 분할 구성이 처음 정의될 때, 그리고 키 분할 구성이 수정될 때마다 핵심 보안을 백업합니다.
10. 정기적으로 Oracle Key Manager 백업을 수행합니다.
11. 핵심 보안 백업 파일 및 Oracle Key Manager 백업 파일을 보안 위치에 저장합니다.

부록 B

부록 B. 참조

- Oracle Key Manager 고객 설명서

  http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle Key Manager Security Guide*
- *Oracle Key Manager Installation and Service Manual*(내부 전용)
- *Oracle Key Manager Overview*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf
- *Oracle Key Manager Version 2.X Security and Authentication White Paper*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf
- Oracle ILOM(Integrated Lights Out Manager) 설명서

  http://docs.oracle.com/cd/E37444_01/
- SPARC T7-1 서버 설명서(https://docs.oracle.com/cd/E54976_01/)
- Netra SPARC T4-1 서버 설명서

  http://docs.oracle.com/cd/E23203_01/
- Oracle Hardware Management Pack 설명서
  - Oracle Hardware Management Pack 설명서 라이브러리

    http://docs.oracle.com/cd/E20451_01/
  - Oracle Single System Management

    http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- NIST 설명서:
  - *National Institute of Standards and Technology Special Publication 800-60 Volume I Revision 1*

    http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

- Oracle 제품용 보안 정책 설명서:
  - *Oracle Solaris Kernel Cryptographic Framework Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *Oracle Solaris Kernel Cryptographic Framework with SPARC T4 and T5 Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2060.pdf
  - *Sun Cryptographic Accelerator 6000 FIPS 140-2 Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Oracle StorageTek T9480D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- Oracle 제품용 FIPS 검증 인증서:
  - Sun Crypto Accelerator 6000 - Certificate #1026(만료됨)

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1026.pdf