Netra Modular System 보안 설명서

부품 번호: E68382-01
2015년 8월

부품 번호: E68382-01

Copyright © 2015, 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 공지사항이 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.

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.

목차

보안 개요

Oracle의 Netra Modular System은 완전히 가상화할 수 있는 사전 통합되고 미리 케이블이 연결된 플랫폼으로서 데이터 센터에서 비용 및 배치 시간을 절감할 수 있습니다. 모듈식 시스템에는 고객이 주문한 대로 공장에서 조립하여 배송되는 하드웨어가 포함됩니다.

다음 항목에서는 모듈식 시스템에 대한 보안 개념 및 기능을 설명합니다.

기본 보안 원칙

모든 모듈식 시스템 소프트웨어 및 하드웨어에 대해 다음 기본 보안 원칙을 따르십시오.

- 인증 - 인증은 일반적으로 기밀 정보(예: 사용자 이름 및 암호 또는 공유 키)를 통해 사용자가 식별되는 방식입니다. 인증을 통해 하드웨어 또는 소프트웨어 사용자가 실제로 등록된 사용자인지 확인됩니다. 기본적으로 로컬 사용자 이름과 암호가 인증에 사용됩니다. 공유 키 기반 인증도 사용할 수 있습니다.
- 계정 및 감사 - 계정 및 감사는 시스템에서의 사용자 작업 레코드를 유지 관리합니다. 모듈식 시스템 소프트웨어 및 하드웨어 기능을 통해 관리자는 로그인 작업을 모니터하고 하드웨어 인벤토리를 유지 관리할 수 있습니다.
  - 사용자 로그인은 시스템 로그를 통해 모니터됩니다. 시스템 관리자 및 서비스 계정은 잘못 사용되면 피해 및 데이터 손실이 발생할 수 있는 명령에 대한 액세스 권한을 가집니다.
  - 하드웨어 자산은 일련 번호를 통해 추적됩니다. Oracle 부품 번호는 모든 카드, 모듈 및 마더보드에 전자적으로 기록되어 인벤토리 용도로 사용할 수 있습니다.

고급 보안 고려 사항

기본 보안 원칙과 함께 모듈식 시스템은 회복성 및 심층 방어 기능을 제공합니다. 모듈식 시스템은 중요 보안 요구 사항 및 문제를 충족할 수 있도록 잘 통합된 보안 기능을 제공합니다. 다음 절에서는 이러한 원칙에 대해 설명합니다.

- 미션 크리티컬 작업 로드의 회복성 - 미션 크리티컬 작업 로드를 위해 하드웨어 및 소프트웨어 플랫폼을 선택하는 조직의 경우 모듈식 시스템은 내부 사용자나 외부 상대방이 실수 및 악의적인 작업으로 인한 피해를 방지하거나 최소화할 수 있습니다. Oracle 최대 가용성 아키텍처 방식의 일부로 다음 방식은 회복성을 높입니다.
  - 사용된 구성 요소가 보안 배치 아키텍처를 지원하면서 함께 잘 작동하도록 설계, 엔지니어링 및 테스트되었는지 확인합니다. 모듈식 시스템은 보안 격리, 액세스 제어, 서비스 품질 및 보안 관리를 지원합니다.
  - 구성 제품의 기본 공격 범위를 줄여 전체적인 시스템 노출을 최소화합니다.
  - 공개 및 검증된 프로토콜의 보완과 전통적인 보안 목표(강력한 인증, 액세스 제어, 기밀성, 무결성 및 가용성)를 지원할 수 있는 API를 사용하여 운영 및 관리 인터페이스를 포함한 전체 시스템을 보호합니다.
  - 오류가 발생하더라도 소프트웨어 및 하드웨어에 서비스 가용성을 유지하는 기능이 포함되어 있는지 확인합니다. 이러한 기능은 공격자가 시스템에서 하나 이상의 개별 구성 요소를 무력화하려는 경우 유용합니다.
- 운영 환경 보안을 위한 심층 방어 - 모듈식 시스템은 다중, 개별 및 상호 보완 보안 컨트롤을 채택하여 작업 로드 및 데이터에 대한 안전한 운영 환경을 만듭니다. 모듈식 시스템은 다음과 같이 심층 방어 원칙을 지원합니다.
  - 전송, 사용 및 보관 중인 정보 보안을 위해 강력한 보호 기능을 제공합니다. 보안 컨트롤은 서버 및 네트워크 층에서 사용할 수 있습니다. 각 층의 고유한 보안 컨트롤은 다른 층의 보안 컨트롤과 통합되어 강력한 계층형 보안 아키텍처를 만들 수 있습니다.
  - 잘 정의된 공개 표준, 프로토콜 및 인터페이스 사용을 지원합니다. 모듈식 시스템은 기존 보안 정책, 아키텍처, 방식 및 표준과 통합할 수 있습니다.

보안 기능

모듈식 시스템 하드웨어 및 소프트웨어는 견고합니다. 또한 Oracle은 NTP 및 SSH와 같은 서비스에 대한 권장 보안 구성을 제공합니다. 더불어 모듈식 시스템의 아키텍처는 핵심 구성 요소에 대한 보안 기능을 제공합니다. 이러한 보안 기능은 계층형 보안 전략을 배치하는 조직에서 주로 적용합니다. 기능은 다음 범주로 그룹화됩니다.

- “네트워크 트래픽 격리” [9]
- “보안 관리를 위한 Oracle ILOM” [9]

네트워크 트래픽 격리

IT 기반구조 통합, 공유 서비스 아키텍처 구현 및 보안 다중 테넌트 서비스 제공을 원하는 경우 네트워크 트래픽 격리를 고려하십시오. 모듈식 시스템은 필요에 따른 격리 정책 및 전략 구현을 위한 유연성을 제공합니다.

물리적 네트워크 레벨에서는 클라이언트 액세스가 장치 관리 및 장치간 통신으로부터 격리됩니다. 클라이언트 및 관리 네트워크 트래픽은 별도의 네트워크에서 격리됩니다. 클라이언트 액세스는 시스템에서 실행 중인 서비스에 대한 안정적인 고속 액세스를 위해 중복된 10Gbps 이더넷 네트워크를 통해 제공됩니다. 관리 액세스는 물리적으로 분리된 1Gbps 이더넷 네트워크를 통해 제공됩니다. 이를 통해 운영 및 관리 네트워크가 분리됩니다.

조직에서는 VLAN(가상 LAN)을 구성하여 클라이언트 액세스 이더넷 네트워크를 통한 네트워크 트래픽을 한층 더 분리하도록 선택할 수 있습니다. VLAN은 요구 사항을 기준으로 네트워크 트래픽을 분리합니다. Oracle은 통신의 기밀성 및 무결성을 위해 VLAN을 통한 암호화된 프로토콜 사용을 권장합니다.

보안 관리를 위한 Oracle ILOM

보안 컨트롤 및 기능 모음은 개별 응용 프로그램 및 서비스를 적절히 보호하는 데 필요합니다. 배치된 서비스 및 시스템의 보안 유지를 위한 포괄적인 관리 기능을 갖추는 것도 마찬가지로 중요합니다. 모듈식 시스템은 Oracle ILOM의 보안 관리 기능을 사용합니다.

Oracle ILOM은 모듈식 시스템의 계산 노드에 내장된 SP입니다. Oracle ILOM은 다음과 같은 아웃오브밴드 관리 작업을 수행하는 데 사용됩니다.

- 데이터베이스 및 저장소 서버의 보안 lights-out 관리를 수행하기 위한 보안 액세스를 제공합니다. 액세스에는 SSL로 보호되는 웹 기반 액세스, 보안 셸과 IPMI v2.0 및 SNMPv3 프로토콜을 사용하는 명령줄 액세스가 포함됩니다.
- 역할 기반 액세스 제어 모델을 사용하여 임무 요구 사항을 구분합니다. 개별 사용자에게는 수행 가능한 기능을 제한하는 특정 역할이 지정됩니다.
- 모든 로그인 및 구성 변경사항에 대한 감사 레코드를 제공합니다. 각 감사 로그 항목은 작업을 수행하는 사용자를 시간 기록과 함께 나열합니다. 감사 레코드를 통해 조직에서는 허용되지 않은 작업이나 변경을 감지하고 이러한 작업의 책임을 특정 사용자로 지목할 수 있습니다.

Oracle ILOM 보안에 대한 자세한 내용은 `http://www.oracle.com/goto/ILOM/docs`에서 *Oracle ILOM* 보안 설명서를 참조하십시오.

보안 환경 계획

Netra Modular System 도착 전에 보안 지침을 마련해 둡니다. 시스템이 설치된 후에는 조직의 최신 보안 요구 사항이 반영되도록 보안 지침을 주기적으로 검토 및 조정합니다.

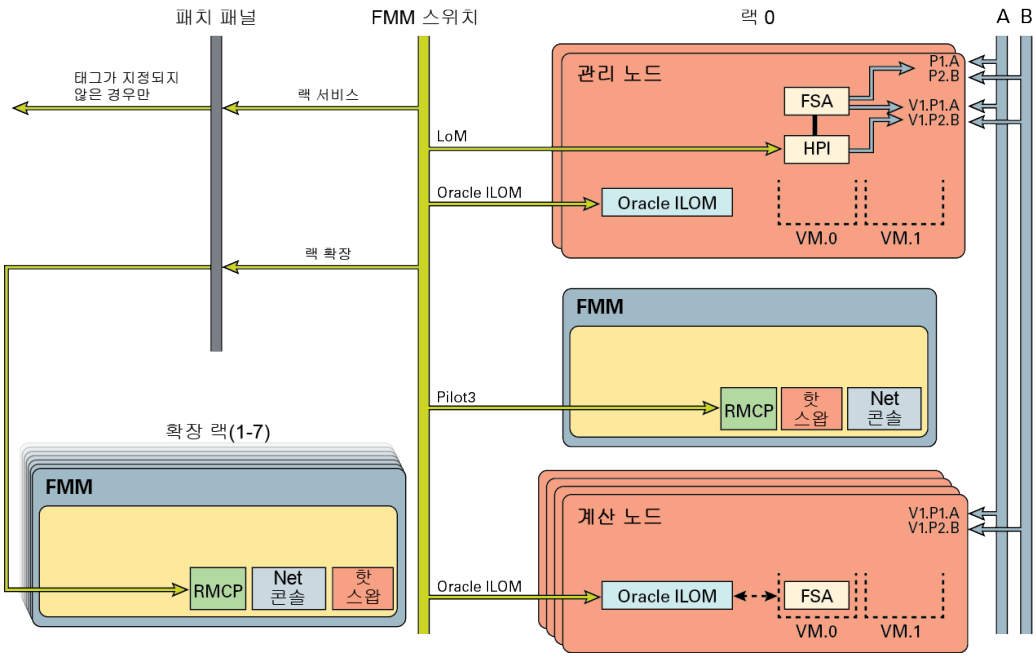
다음 항목에서는 Netra Modular System의 설치 보안 지침을 제공합니다.

사용 중인 시스템 및 특정 환경과 관련된 추가 보안 요구 사항은 IT 보안 관리자에게 문의하십시오.

기본 네트워크

다음 그림과 설명은 Netra Modular System에 대한 기본 네트워크를 보여줍니다.

- 시스템/원격 측정 네트워크(연녹색 네트워크)에는 FMM 스위치를 통한 VLAN 4090의 관리 노드 LoM 포트가 포함됩니다.
- FMM과 함께 내부 VLAN 4094의 원격 측정 ILOM 네트워크에는 계산 노드 Oracle ILOM 및 FMM 스위치를 통한 네트워크 노드 Oracle ILOM이 포함됩니다.
- 패치 패널은 원격 측정 네트워크를 랙 1-7로 확장합니다. 다중 랙 구성은 동일 서브넷 및 다른 랙 ID를 가진 VLAN을 지원합니다.
- VLAN(1)은 적절한 인증을 통해 원격 측정 네트워크에 다른 서비스를 제공합니다.
- 데이터 네트워크(A 및 B)는 FSA 노드에 대한 인밴드 액세스를 제공합니다.
- HA 응용 프로그램은 모듈식 시스템의 노출된 인터페이스(JMX, C- API 등)를 통해 랙을 관리할 수 있습니다.



사용자 계정

이 표는 모듈식 시스템 구성 요소에 대한 기본 사용자 및 암호를 나열합니다. Netra Modular System 설치 후 모든 기본 암호를 변경하십시오.

구성 요소	사용자 이름 및 암호
이더넷 스위치	`root/changeme` **주** - `admin` 사용자에 대한 `enable mode password` 및 `secret` 값을 보호하십시오.
관리 및 계산 노드	`root/changeme`

기본 보안 설정

모듈식 시스템은 많은 기본 보안 설정으로 설치됩니다. 가능하면 언제나 안전한 보안 설정을 구성하십시오. http://www.oracle.com/goto/ILOM/docs에서 해당 버전의 Oracle ILOM에 대한 기본 설정을 참조하십시오.

하드웨어 보안

물리적 격리 및 액세스 제어를 기반으로 보안 아키텍처를 구축해야 합니다. 물리적 시스템이 안전한 환경에 설치되면 허용되지 않은 액세스로부터 시스템이 보호됩니다. 마찬가지로, 일련 번호를 모두 기록해 두면 허용되지 않은 하드웨어 구성 요소의 사용을 방지할 수 있습니다.

다음 절에서는 모듈식 시스템에 대한 일반적인 하드웨어 보안 지침을 제공합니다.

액세스 제한

- 시스템 및 관련 장비는 잠겨 있으며 액세스가 제한된 공간에 설치합니다.
- 장비가 잠금 문이 있는 랙에 설치된 경우 랙의 구성 요소를 서비스해야 할 때까지 항상 랙 문을 잠급니다. 문을 잠그면 핫 플러그 또는 핫 스왑 장치에 대한 액세스도 제한됩니다.
- 모든 예비 교체 부품은 잠겨 있는 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 액세스할 수 있도록 제한합니다.
- 랙 및 예비 장치 캐비닛에 대한 잠금 상태 및 무결성을 주기적으로 확인하여 변조 또는 사고로 인한 문 잠금 해제 상태 유지를 방지하거나 감지합니다.
- 액세스가 제한된 안전한 위치에 캐비닛 키를 보관합니다.
- USB 콘솔에 대한 액세스를 제한합니다. 시스템 컨트롤러, PDU, 네트워크 스위치 등의 장치가 USB 연결을 제공할 수 있습니다. 물리적 액세스는 네트워크 기반 공격에 노출되지 않으므로 구성 요소에 액세스할 수 있는 보다 안전한 방법입니다.
- 원격 콘솔에 액세스할 수 있도록 외부 KVM에 콘솔을 연결합니다. KVM 장치는 두 단계 인증, 중앙화된 액세스 제어 및 감사를 지원하는 경우가 많습니다. KVM 보안 지침 및 모범 사례에 대한 자세한 내용은 KVM 장치와 함께 제공된 설명서를 참조하십시오.

일련 번호

구성 요소를 받아 인벤토리에 보관할 때 모든 일련 번호를 기록하여 허용되지 않은 하드웨어 구성 요소의 사용을 방지합니다. 구성 요소를 설치 또는 사용하기 전에 해당 일련 번호를 구성 요소를 받을 때 기록한 일련 번호와 비교하여 신뢰성을 확인합니다. 하드웨어를 보호하려면 다음 방법에 따르십시오.

- 모든 하드웨어의 일련 번호를 기록해 둡니다.
- 교체 부품과 같은 컴퓨터 하드웨어의 모든 중요한 항목에 보안 표시를 합니다. 특수 자외선 펜 또는 돌출된 레이블을 사용합니다.
- 시스템 긴급 상황 시 시스템 관리자가 쉽게 액세스할 수 있는 보안 위치에 하드웨어 활성화 키 및 라이센스를 보관합니다. 인쇄된 문서가 유일한 소유권 증명이 될 수도 있습니다.

무선 RFID(Radio Frequency Identification) 판독기는 자산 추적을 더욱 간소화할 수 있습니다. Oracle 백서 *How to Track Your Oracle Sun System Assets by Using RFID*(http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf)을 참조하십시오.

하드 드라이브

하드 드라이브는 중요한 정보를 저장하는 데 사용되는 경우가 많습니다. 이 정보가 무단으로 공개되지 않도록 보호하려면 하드 드라이브를 재사용하거나 구성 해제하거나 폐기하기 전에 정리합니다.

- 관련 데이터 보호 정책을 참조하여 가장 적절한 하드 드라이브 정리 방법을 결정합니다.
- 필요한 경우 Oracle의 고객 데이터 및 장치 보존 서비스를 활용합니다.

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

소프트웨어 보안

대부분의 하드웨어 보안은 소프트웨어 조치를 통해 구현됩니다. 다음 절에서는 Netra Modular System에 대한 일반적인 소프트웨어 보안 지침을 제공합니다.

▼ 허용되지 않은 액세스 방지(Oracle Linux)

- **소프트웨어에 대한 액세스를 제한하는 Oracle Linux OS 명령을 사용하여 OS를 강화하고 보안 기능을 사용하며 응용 프로그램을 보호합니다.**

  http://docs.oracle.com/cd/E37670_01/E36387/html/index.html에서 *Oracle Linux* 보안 설명서*(*릴리스 *6*용*)*를 참조하십시오.

▼ 허용되지 않은 액세스 방지(Oracle ILOM)

- **Oracle ILOM 펌웨어에 대한 액세스를 제한하는 Oracle ILOM 명령을 사용하여 출하 시 설정된 암호를 변경하고 루트 수퍼 유저 계정 사용을 제한하며 SP에 대한 개인 네트워크를 보호합니다.**

  http://www.oracle.com/goto/ILOM/docs에서 해당 버전의 *Oracle ILOM* 보안 설명서를 참조하십시오.

▼ 허용되지 않은 액세스 방지(Oracle Linux의 Oracle VM Server)

- **Oracle VM Server 소프트웨어에 대한 액세스를 제한하는 Oracle Linux 명령을 사용하여 보안 기능을 사용하고 응용 프로그램을 보호합니다.**

  http://docs.oracle.com/cd/E50245_01/E50254/html/index.html에서 *Oracle VM* 보안 설명서*(*릴리스 *3.3*용*)*를 참조하십시오.

Oracle Hardware Management Pack 보안

Oracle Hardware Management Pack에는 SNMP 모니터링 에이전트 및 시스템 관리를 위한 교차 운영 체제 CLI 도구(명령줄 인터페이스 도구) 모음의 두 구성 요소가 있습니다.

- Hardware Management Agent SNMP 플러그인 - SNMP는 시스템을 모니터하거나 관리하는 표준 프로토콜입니다. Hardware Management Agent SNMP 플러그인과 함께 SNMP를 사용하면 데이터 센터에서 Oracle 시스템을 모니터할 수 있으며 2개의 관리 지점인 호스트와 Oracle ILOM에 연결하지 않아도 된다는 장점이 있습니다. 이 기능을 통해 단일 IP 주소(호스트의 IP 주소)를 사용하여 여러 시스템을 모니터할 수 있습니다.

  SNMP 플러그인은 Oracle 시스템의 호스트 OS에서 실행됩니다. SNMP 플러그인은 호스트 OS에서 고유 SNMP 에이전트를 확장하여 추가 Oracle MIB 기능을 제공합니다. Oracle Hardware Management Pack 자체에는 SNMP 에이전트가 포함되어 있지 않습니다. Oracle Linux의 경우 `net-snmp` 에이전트에 모듈이 추가됩니다. Microsoft Windows의 경우 플러그인이 고유 SNMP 서비스를 확장합니다. Oracle Hardware Management Pack의 경우 SNMP와 관련된 보안 설정은 플러그인이 아닌 고유 SNMP 에이전트나 서비스의 설정에 따라 결정됩니다.

  SNMPv1 및 SNMPv2c는 암호화를 제공하지 않으며 커뮤니티 문자열을 인증 형식으로 사용합니다. SNMPv3은 암호화를 사용하여 보안 채널과 개별 사용자 이름 및 암호를 제공하므로 보다 안전합니다. 따라서 이 버전을 사용하는 것이 좋습니다.
- Oracle Hardware Management Pack 설명서 - Oracle Hardware Management Pack과 관련된 보안 지침은 `http://www.oracle.com/goto/OHMP/docs`에서 *Oracle Hardware Management Pack* 보안 설명서를 참조하십시오.

관련 보안 설명서 찾기

보안 설명서

다음 설명서에서는 관련 제품의 보안 유지를 위한 정책 및 절차를 설명합니다.

- *Oracle Server X5-2 Security Guide*
- *Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide*
- *Oracle Linux* 보안 설명서*(*릴리스 *6*용*)*(http://docs.oracle.com/cd/E37670_01/E36387/html/index.html)
- *Oracle ILOM* 보안 설명서(http://www.oracle.com/goto/ILOM/docs)
- *Oracle VM* 보안 설명서*(*릴리스 *3.3*용*)*(http://docs.oracle.com/cd/E50245_01/E50254/html/index.html)
- *Oracle Hardware Management Pack* 보안 설명서(http://www.oracle.com/goto/OHMP/docs)