# Oracle® Server X5-4 보안 설명서

보안 설명서

**부품 번호: E64500**
2015년 6월

**부품 번호: E64500**

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=docacc`에서 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=info`를 참조하거나, 청각 장애가 있는 경우 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`를 방문하십시오.

# 목차

**기본 보안** ..... 7

**서버 구성 및 관리 도구 사용** ..... 9
- Oracle System Assistant 보안 ..... 9
- Oracle ILOM 보안 ..... 10
- Oracle Hardware Management Pack 보안 ..... 11

**보안 환경 계획** ..... 13
- 운영 체제 보안 지침 ..... 13
- 네트워크 포트 및 스위치 ..... 14
- VLAN 보안 ..... 14
- Infiniband 보안 ..... 15
- 하드웨어 물리적 보안 ..... 15
- 소프트웨어 보안 ..... 15

**보안 환경 유지 관리** ..... 17
- 하드웨어 전원 제어 ..... 17
- 자산 추적 ..... 17
- 소프트웨어 및 펌웨어 업데이트 ..... 18
- 네트워크 보안 ..... 18
- 데이터 보호 및 보안 ..... 19
- 로그 유지 관리 ..... 19

# 기본 보안

이 문서에서는 Oracle 서버, 서버 네트워크 인터페이스 및 연결된 네트워크 스위치를 보호하는 데 유용한 일반적인 보안 지침을 제공합니다.

---

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

---

이 절에서는 모든 하드웨어 및 소프트웨어를 사용할 때 준수해야 하는 네 가지 보안 원칙인 액세스, 인증, 권한 부여 및 계정에 대해 설명합니다.

- **액세스**

  액세스란 하드웨어에 대한 물리적 액세스나 소프트웨어에 대한 물리적 또는 가상 액세스를 의미합니다.

  - 침입으로부터 하드웨어와 데이터를 보호하려면 물리적 제어 및 소프트웨어 제어를 사용하십시오.
  - 소프트웨어에 사용 가능한 보안 기능을 사용으로 설정하려면 소프트웨어와 함께 제공된 설명서를 참조하십시오.
  - 서버 및 관련 장비는 잠겨 있으며 접근이 제한된 공간에 설치합니다.
  - 잠금 문이 있는 랙에 장비가 설치된 경우 랙의 구성 요소를 수리해야 하는 경우를 제외하고는 문을 잠가 둡니다.
  - SSH 연결보다 강력한 액세스를 제공할 수 있는 커넥터 또는 포트에 대한 접근을 제한하십시오. 시스템 컨트롤러, PDU(전원 분배 장치), 네트워크 스위치 등의 장치가 커넥터 및 포트를 제공합니다.
  - 특히 핫 플러그 또는 핫 스왑 장치는 쉽게 분리될 수 있으므로 접근을 제한하십시오.
  - 스페어 FRU(현장 교체 가능 장치) 및 CRU(자가 교체 가능 장치)는 잠긴 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 접근할 수 있도록 제한합니다.

- **인증**

  인증이란 하드웨어 또는 소프트웨어 사용자가 실제로 등록된 사용자인지 확인하는 것을 의미합니다.

  - 사용자가 실제로 등록된 사용자인지 확인할 수 있도록 사용 중인 플랫폼 운영 체제에서 암호 시스템 등의 인증 기능을 설정하십시오.
  - 담당자가 컴퓨터실에 출입할 때는 사원 명찰을 사용하도록 하십시오.
  - 사용자 계정에 대해서는 필요한 경우 액세스 제어 목록을 사용하고, 확장된 세션에 대한 시간 초과를 설정하고, 사용자에 대한 권한 레벨을 설정하십시오.

- **권한 부여**

권한 부여란 하드웨어 또는 소프트웨어를 사용할 담당자를 제한하는 것을 의미합니다.

- 담당자가 사용 교육 및 자격을 받은 하드웨어와 소프트웨어만 사용할 수 있도록 하십시오.
- 읽기/쓰기/실행 권한 시스템을 설정하여 명령, 디스크 공간, 장치 및 응용 프로그램에 대한 사용자 액세스 권한을 제어합니다.

- **계정**

  계정이란 로그인 작업과 하드웨어 인벤토리 유지 관리를 모니터하는 데 사용되는 소프트웨어 및 하드웨어 기능을 의미합니다.

  - 시스템 로그를 사용하여 사용자 로그인을 모니터할 수 있습니다. 특히 시스템 관리자 및 서비스 계정은 강력한 명령에 액세스할 수 있으므로 모니터합니다.
  - 모든 하드웨어의 일련 번호를 기록해 두십시오. 구성 요소 일련 번호를 사용하여 시스템 자산을 추적할 수 있습니다. Oracle 부품 번호는 카드, 모듈 및 마더보드에 전자적으로 기록되어 인벤토리 용도로 사용할 수 있습니다.
  - 구성 요소를 감지 및 추적하려면 컴퓨터 하드웨어의 모든 중요한 품목(예: FRU)에 보안 표시를 해두십시오. 특수 자외선 펜 또는 돌출된 레이블을 사용할 수 있습니다.

# 서버 구성 및 관리 도구 사용

소프트웨어 및 펌웨어 도구를 사용하여 서버를 구성하고 관리할 때는 다음 보안 지침을 따르십시오.


- "Oracle System Assistant 보안" [9]
- "Oracle ILOM 보안" [10]
- "Oracle Hardware Management Pack 보안" [11]


## Oracle System Assistant 보안

Oracle System Assistant는 로컬 또는 원격으로 서버 하드웨어를 구성 및 업데이트하고 지원되는 운영 체제를 설치할 수 있도록 지원하기 위해 사전 설치되는 도구입니다. Oracle System Assistant 사용 방법에 대한 자세한 내용은 다음 웹 사이트의 *Oracle X5* 시리즈 서버 관리 설명서를 참조하십시오.

http://www.oracle.com/goto/x86AdminDiag/docs

다음 정보를 통해 Oracle System Assistant와 관련된 보안 문제를 파악할 수 있습니다.

- **Oracle System Assistant에는 부트 가능한 루트 환경이 있음**

  Oracle System Assistant는 사전 설치된 내부 USB 플래시 드라이브에서 실행되는 응용 프로그램입니다. 이 응용 프로그램은 부트 가능한 Linux 루트 환경에 구축됩니다. Oracle System Assistant는 기본 루트 셸에 액세스할 수 있는 기능도 제공합니다. 시스템에 대해 물리적 액세스 권한을 가지거나 시스템에 대해 Oracle ILOM을 통한 원격 KVMS(키보드, 비디오, 마우스 및 저장소) 액세스 권한을 가진 사용자는 Oracle System Assistant 및 루트 셸에 액세스할 수 있습니다.

  루트 환경에서는 시스템 구성 및 정책을 변경하고 다른 디스크의 데이터에 액세스할 수 있습니다. 서버에 대한 물리적 액세스를 보호하고 Oracle ILOM 사용자에 대한 관리자 및 콘솔 권한을 제한적으로 지정하는 것이 좋습니다.

- **Oracle System Assistant는 운영 체제에서 액세스할 수 있는 USB 저장 장치를 마운트함**

  부트 가능한 환경 외에 Oracle System Assistant는 설치 후 호스트 운영 체제에서 액세스할 수 있는 USB 저장 장치(플래시 드라이브)로도 마운트됩니다. 이 기능은 유지 관리와 재구성을 위해 도구 및 드라이버에 액세스할 때 유용합니다. Oracle System Assistant USB 저장 장치는 읽기/쓰기가 가능하므로 바이러스에 의해 악용될 수 있습니다.

  따라서 일반적인 바이러스 검사 및 무결성 검사를 비롯하여 디스크를 보호하는 것과 동일한 방식을 Oracle System Assistant 저장 장치에 적용하는 것이 좋습니다.

- **Oracle System Assistant를 사용 안함으로 설정할 수 있음**

  Oracle System Assistant는 서버 설정, 펌웨어 업데이트 및 구성, 호스트 운영 체제 설치에 유용한 도구입니다. 하지만 앞서 설명된 보안 문제가 발생하지 않도록 하려는 경우 또는 도구가 필요하지 않은 경우 Oracle System Assistant를 사용 안함으로 설정할 수 있습니다. Oracle System Assistant를 사용 안함으로 설정하면 호스트 운영 체제에서 더 이상 USB 저장 장치에 액세스할 수 없게 됩니다. 또한 Oracle System Assistant를 부트할 수 없습니다.

  도구 자체에서 또는 BIOS에서 Oracle System Assistant를 사용 안함으로 설정할 수 있습니다. 사용 안함으로 설정한 후에는 BIOS Setup Utility를 통해서만 Oracle System Assistant를 다시 사용으로 설정할 수 있습니다. 권한이 부여된 사용자만 Oracle System Assistant를 다시 사용으로 설정할 수 있도록 BIOS 설정을 암호로 보호하는 것이 좋습니다. Oracle System Assistant를 사용 안함으로 설정한 후 다시 사용으로 설정하는 방법은 다음 사이트의 Oracle X4 시리즈 서버 관리 설명서를 참조하십시오.

  http://www.oracle.com/goto/x86AdminDiag/docs

# Oracle ILOM 보안

이 서버, 기타 Oracle x86 기반 서버 및 일부 Oracle SPARC 기반 서버에 사전 설치된 Oracle ILOM(Integrated Lights Out Manager) 관리 펌웨어를 사용하여 시스템 구성 요소를 보안, 관리 및 모니터할 수 있습니다.

일반 네트워크와 구분되도록 SP(서비스 프로세서)에 전용 내부 네트워크를 사용합니다. Oracle ILOM은 시스템 관리자에게 서버 제어 및 모니터링 기능을 제공합니다. 관리자에게 부여된 권한 부여 레벨에 따라 이러한 기능에 서버 끄기, 사용자 계정 만들기, 원격 저장 장치 마운트 등의 기능이 포함될 수 있습니다. 따라서 Oracle ILOM에서 가장 안전한 보안 환경을 유지하기 위해서는 서버의 전용 네트워크 관리 포트 또는 사이드밴드 관리 포트가 항상 신뢰할 수 있는 내부 네트워크 또는 전용 보안 관리/개인 네트워크에 연결되어 있어야 합니다.

기본 관리자 계정(`root`)은 Oracle ILOM에 처음 로그인할 때만 사용합니다. 이 기본 관리자 계정은 초기 서버 설치를 지원할 목적으로만 제공됩니다. 따라서 가장 안전한 환경을 보장하려면 시스템 초기 설정의 일부로 이 기본 관리자 암호(`changeme`)를 변경해야 합니다. 기본 관리자 계정의 암호를 변경하는 것 이외에도, 고유한 암호와 지정된 권한 부여 레벨을 사용하는 새로운 사용자 계정을 새로운 Oracle ILOM 사용자마다 설정해야 합니다.

SSH(보안 셸), SSL(Secure Socket Layer) 및 RADIUS 인증을 비롯한 보안 관련 기능 적용과 암호 설정, 사용자 관리에 대해 자세히 알아보려면 Oracle ILOM 설명서를 참조하십시오. Oracle ILOM과 관련된 보안 지침은 사용 중인 Oracle ILOM 릴리스에 대해 Oracle ILOM 설명서 라이브러리에 포함된 *Oracle ILOM(Integrated Lights Out Manager)* 보안 설명서를 참조하십시오. Oracle ILOM 설명서는 다음 위치에서 확인할 수 있습니다.

http://www.oracle.com/goto/ILOM/docs

# Oracle Hardware Management Pack 보안

Oracle Hardware Management Pack은 서버, 기타 여러 x86 기반 서버 및 일부 SPARC 서버에 사용할 수 있습니다. Oracle Hardware Management Pack은 두 가지 구성 요소로 SNMP 모니터링 에이전트와 서버 관리용 운영 체제 간 CLI(명령줄 인터페이스) 도구 제품군을 제공합니다.

Hardware Management Agent SNMP 플러그인을 사용하면 호스트 및 Oracle ILOM의 두 관리 지점에 연결할 필요 없이 SNMP를 통해 데이터 센터의 Oracle 서버 및 서버 모듈을 모니터링할 수 있습니다. 이 기능을 통해 단일 IP 주소(호스트의 IP 주소)를 사용하여 여러 서버 및 서버 모듈을 모니터할 수 있습니다. SNMP 플러그인은 Oracle 서버의 호스트 운영 체제에서 실행됩니다.

Oracle Server CLI 도구를 사용하여 Oracle 서버를 구성할 수 있습니다. CLI 도구는 Oracle Solaris, Oracle Linux, Oracle VM, 기타 Linux 변형 및 Microsoft Windows 운영 체제와 연동됩니다.

이러한 기능에 대한 자세한 내용은 Oracle Hardware Management Pack 설명서를 참조하십시오. Oracle Hardware Management Pack과 관련된 보안 지침은 Oracle Hardware Management Pack 설명서 라이브러리에 포함된 *Oracle Hardware Management Pack* 보안 설명서를 참조하십시오. Oracle Hardware Management Pack 설명서는 다음 사이트에서 확인할 수 있습니다.

http://www.oracle.com/goto/OHMP/docs

# 보안 환경 계획

서버 및 관련 장비를 설치하고 구성하기 전과 도중에 다음 사항을 참고하십시오.

다음 항목을 다룹니다.


- "운영 체제 보안 지침" [13]
- "네트워크 포트 및 스위치" [14]
- "VLAN 보안" [14]
- "Infiniband 보안" [15]
- "하드웨어 물리적 보안" [15]
- "소프트웨어 보안" [15]


## 운영 체제 보안 지침

다음 사항에 대한 자세한 내용은 Oracle OS(운영 체제) 문서를 참조하십시오.

- 시스템 구성 시 보안 기능을 사용하는 방법
- 응용 프로그램 및 사용자를 시스템에 추가할 때 안전하게 작업하는 방법
- 네트워크 기반 응용 프로그램을 보호하는 방법

지원되는 Oracle 운영 체제에 대한 보안 설명서 문서는 운영 체제 설명서 라이브러리에 포함되어 있습니다. Oracle OS에 대한 보안 설명서 문서를 확인하려면 다음 웹 사이트의 Oracle OS 설명서 라이브러리로 이동하십시오.

| 운영 체제 | 링크 |
|---|---|
| Oracle Solaris OS | http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html |
| Oracle Linux OS | http://linux.oracle.com |
| Oracle VM OS | http://www.oracle.com/technetwork/documentation/vm-096300.html |

다른 공급업체에서 제공하는 운영 체제(예: Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows, VMware ESXi)에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

# 네트워크 포트 및 스위치

서로 다른 스위치는 다른 레벨의 포트 보안 기능을 제공합니다. 다음 작업을 수행하는 방법에 대해 알아보려면 스위치 설명서를 참조하십시오.

- 로컬 및 원격으로 스위치에 액세스하기 위해 인증, 권한 부여 및 계정 관리 기능을 사용합니다.
- 기본적으로 여러 사용자 계정 및 암호를 가질 수 있는 네트워크 스위치에서 모든 암호를 변경합니다.
- 스위치를 아웃오브밴드(데이터 트래픽에서 분리)로 관리합니다. 아웃오브밴드 관리가 가능하지 않으면 인밴드 관리를 위해 별도의 VLAN(가상 LAN) 번호를 지정합니다.
- IDS(침입 방지 시스템) 액세스를 위해 네트워크 스위치의 포트 미러링 기능을 사용합니다.
- 스위치 구성 파일을 오프라인으로 유지 관리하고 권한이 부여된 관리자로만 액세스를 제한합니다. 구성 파일에는 각 설정에 대한 세부 설명이 포함되어 있어야 합니다.
- MAC 주소를 기반으로 액세스를 제한하려면 포트 보안을 구현합니다. 모든 포트에서 오토트렁킹을 사용 안함으로 설정합니다.
- 스위치에서 사용 가능한 경우 다음 포트 보안 기능을 사용합니다.
  - **MAC 잠금**: 하나 이상의 연결된 장치의 MAC(Media Access Control) 주소를 스위치의 물리적 포트와 연관시키는 것과 관련됩니다. 특정 MAC 주소로 스위치 포트를 잠그면 수퍼 유저가 허위 액세스 포인트가 있는 네트워크로의 백도어를 만들 수 없습니다.
  - **MAC 잠금**: 지정된 MAC 주소가 스위치에 연결되지 않도록 합니다.
  - **MAC 학습**: 네트워크 스위치에서 현재 연결을 기반으로 보안을 설정할 수 있도록 각 스위치 포트의 직접 연결에 대한 정보를 사용합니다.

# VLAN 보안

VLAN(가상 LAN)을 설정한 경우 VLAN은 네트워크의 대역폭을 공유하므로 추가 보안 조치가 필요합니다.

- 시스템의 중요한 클러스터가 나머지 네트워크에서 분리되도록 VLAN을 정의합니다. 그러면 사용자가 해당 클라이언트 및 서버의 정보에 대한 액세스 권한을 얻을 가능성이 줄어듭니다.
- 고유한 VLAN 번호를 트렁크 포트에 지정합니다.
- 트렁크를 통해 전송할 수 있는 VLAN을 엄격하게 요구되는 VLAN으로만 제한합니다.
- 가능한 경우 VTP(VLAN Trunking Protocol)를 사용 안함으로 설정합니다. 그렇지 않은 경우 VTP에 대해 관리 도메인, 암호 및 제거를 설정합니다. 그런 다음 VTP를 투명 모드로 설정합니다.

# Infiniband 보안

Infiniband 호스트 보안을 유지합니다. Infiniband 패브릭은 최소한의 보안 Infiniband 호스트만큼만 안전합니다.

- 분할은 Infiniband 패브릭을 보호하지 않습니다. 분할은 호스트의 가상 시스템 간에 Infiniband 트래픽 격리만 제공합니다.
- 가능한 경우 정적 VLAN 구성을 사용합니다.
- 사용되지 않은 스위치 포트를 사용 안함으로 설정하여 사용되지 않은 VLAN 번호를 지정합니다.

# 하드웨어 물리적 보안

물리적 하드웨어는 하드웨어에 대한 액세스 제한 및 일련 번호 기록을 통해 매우 간단하게 보안을 설정할 수 있습니다.

- **액세스 제한**
  - 서버 및 관련 장비는 잠겨 있으며 접근이 제한된 공간에 설치합니다.
  - 잠금 문이 있는 랙에 장비가 설치된 경우 랙의 구성 요소를 수리해야 하는 경우를 제외하고는 문을 잠가 둡니다. 장비를 서비스한 후에는 문을 잠급니다.
  - SSH 연결보다 강력한 액세스를 제공할 수 있는 USB 콘솔에 대한 접근을 제한합니다. 시스템 컨트롤러, PDU(전력 분배 장치), 네트워크 스위치 등의 장치가 USB 연결을 제공할 수 있습니다.
  - 특히 핫 플러그 또는 핫 스왑 장치는 쉽게 분리될 수 있으므로 접근을 제한하십시오.
  - 예비 FRU(현장 교체 가능 장치) 또는 CRU(자가 교체 가능 장치)는 잠긴 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 접근할 수 있도록 제한합니다.
- **일련 번호 기록**
  - 컴퓨터 하드웨어의 모든 중요한 품목(예: FRU)에 보안 표시를 해두십시오. 특수 자외선 펜 또는 돌출된 레이블을 사용할 수 있습니다.
  - 모든 하드웨어의 일련 번호를 기록해 두십시오.
  - 시스템 긴급 상황 시 시스템 관리자가 쉽게 액세스할 수 있는 보안 위치에 하드웨어 활성화 키 및 라이센스를 보관합니다. 인쇄된 문서만 소유권 증명이 될 수 있습니다.

# 소프트웨어 보안

대부분의 하드웨어 보안은 소프트웨어 조치를 통해 구현됩니다.

- 시스템을 새로 설치할 때 기본 암호를 모두 변경합니다. 대부분의 장비 유형은 널리 알려지고 허용되지 않은 장비 액세스를 허가하는 기본 암호(예: changeme)를 사용합니다.

- 기본적으로 사용자 계정과 암호가 여러 개 있을 수 있는 네트워크 스위치에서 모든 암호를 변경합니다.
- 기본 관리자 계정(root)은 관리자 사용자 한 명만 사용합니다. 새 사용자의 경우 항상 Oracle ILOM 계정을 새로 만듭니다. 각 Oracle ILOM 사용자 계정에 항상 고유한 암호와 적절한 레벨의 권한 부여 권한(운영자, 관리자 등)이 지정되도록 합니다.
- 일반 네트워크와 구분되도록 서비스 프로세서에 전용 네트워크를 사용합니다.
- USB 콘솔에 대한 액세스를 보호합니다. 시스템 컨트롤러, PDU(전력 분배 장치) 및 네트워크 스위치와 같은 장치는 USB 연결을 제공할 수 있으며 이를 통해 SSH 연결보다 더 강력한 액세스를 제공될 수 있습니다.
- 소프트웨어에 사용 가능한 보안 기능을 사용으로 설정하려면 소프트웨어와 함께 제공된 설명서를 참조하십시오.
- MAC 주소를 기반으로 액세스를 제한하려면 포트 보안을 구현합니다. 모든 포트에서 오토트렁킹을 사용 안함으로 설정합니다.

# 보안 환경 유지 관리

초기 설치 및 설정 후 계속해서 Oracle 하드웨어 및 소프트웨어 보안 기능을 사용하여 하드웨어를 제어하고 시스템 자산을 추적할 수 있습니다.


- "하드웨어 전원 제어" [17]
- "자산 추적" [17]
- "소프트웨어 및 펌웨어 업데이트" [18]
- "네트워크 보안" [18]
- "데이터 보호 및 보안" [19]
- "로그 유지 관리" [19]


## 하드웨어 전원 제어

소프트웨어를 사용하여 일부 Oracle 시스템의 전원을 켜고 끌 수 있습니다. 일부 시스템 캐비닛의 PDU(전원 분배 장치)도 원격으로 사용 및 사용 안함으로 설정할 수 있습니다. 이러한 명령에 대한 권한 부여는 일반적으로 시스템 구성 중 설정되며 시스템 관리자 및 서비스 담당자로 제한됩니다.

자세한 내용은 시스템 또는 캐비닛 설명서를 참조하십시오.

## 자산 추적

일련 번호를 사용하여 인벤토리를 추적할 수 있습니다. Oracle 일련 번호는 옵션 카드 및 시스템 마더보드에 있는 펌웨어에 포함되어 있습니다. LAN 연결을 통해 이러한 일련 번호를 확인할 수 있습니다.

또한 무선 RFID(Radio Frequency Identification) 판독기를 사용하여 자산 추적을 추가로 간소화할 수 있습니다. Oracle 백서 *How to Track Your Oracle Sun System Assets by Using RFID*는 다음 사이트에서 확인할 수 있습니다.

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

# 소프트웨어 및 펌웨어 업데이트

서버 장비의 소프트웨어 및 펌웨어 버전을 최신으로 유지합니다.

- 정기적으로 업데이트를 확인합니다.
- 장비에 항상 소프트웨어 또는 펌웨어의 최신 릴리스 버전을 설치합니다.
- 소프트웨어에 필요한 보안 패치를 설치합니다.
- 네트워크 스위치, 익스프레스 모듈 등의 장치에는 펌웨어가 포함되어 있어 패치 및 펌웨어 업데이트가 필요할 수 있습니다.

# 네트워크 보안

시스템에 대한 로컬 및 원격 액세스를 보안하려면 다음 지침을 따르십시오.

- 텔넷 대신 SSH를 사용하여 원격 구성을 특정 IP 주소로 제한합니다. 텔넷은 사용자 이름 및 암호를 일반 텍스트로 전달하여 잠재적으로 LAN 세그먼트에 있는 모든 사용자가 로그인 자격 증명을 볼 수 있습니다. SSH에 대해 강력한 암호를 설정합니다.
- SNMP(Simple Network Management Protocol)의 버전 3을 사용하여 보안 전송을 제공합니다. 이전 버전의 SNMP는 보안되지 않아 암호화되지 않은 텍스트로 인증 데이터를 전송합니다.
- SNMP가 필요한 경우 기본 SNMP 커뮤니티 문자열을 강력한 커뮤니티 문자열로 변경합니다. 일부 제품에는 기본 SNMP 커뮤니티 문자열로 PUBLIC이 설정되어 있습니다. 공격자는 커뮤니티를 질의하여 거의 완전한 네트워크 맵을 작성하고 MIB(Management Information Base) 값을 수정할 수 있습니다.
- 시스템 컨트롤러에 브라우저 인터페이스가 사용되는 경우 시스템 컨트롤러를 사용한 후 항상 로그아웃합니다.
- TCP(Transmission Control Protocol) 또는 HTTP(Hypertext Transfer Protocol)와 같이 불필요한 네트워크 서비스는 사용 안함으로 설정합니다. 필요한 네트워크 서비스를 사용으로 설정하고 이러한 서비스를 안전하게 구성합니다.
- LDAP를 사용하여 시스템에 액세스할 경우 LDAP 보안 조치를 따릅니다. Oracle ILOM 보안 설명서(`http://www.oracle.com/goto/ILOM/docs`)를 참조하십시오.
- 허용되지 않은 액세스는 금지된다는 배너를 만듭니다.
- 필요한 경우 액세스 제어 목록을 사용합니다.
- 확장된 세션에 대해 시간 초과를 설정하고 권한 레벨을 설정합니다.
- 로컬 및 원격으로 스위치에 액세스하기 위한 인증, 권한 부여 및 계정(AAA) 기능을 사용합니다.
- 가능한 경우 RADIUS 및 TACACS+ 보안 프로토콜을 사용합니다.
  - RADIUS(Remote Authentication Dial In User Service)는 허용되지 않은 액세스에 대해 네트워크를 보호하는 클라이언트/서버 프로토콜입니다.
  - TACACS+(Terminal Access Controller Access-Control System)는 사용자에게 네트워크에 대한 액세스 권한이 있는지 확인하기 위해 원격 액세스 서버가 인증 서버와 통신하도록 하는 프로토콜입니다.

- IDS(침입 방지 시스템) 액세스를 위해 스위치의 포트 미러링 기능을 사용합니다.
- MAC 주소를 기반으로 액세스를 제한하려면 포트 보안을 구현합니다. 모든 포트에서 오토트렁킹을 사용 안함으로 설정합니다.

# 데이터 보호 및 보안

데이터 보호 및 보안을 최대화하려면 다음 지침을 따르십시오.

- 외장 하드 드라이브 또는 USB 저장 장치 등의 장치를 사용하여 중요한 데이터를 백업합니다. 안전한 별도의 오프사이트 위치에 백업된 데이터를 보관합니다.
- 데이터 암호화 소프트웨어를 사용하여 기밀 정보를 하드 드라이브에 안전하게 보관합니다.
- 이전 하드 드라이브를 폐기할 때는 물리적으로 드라이브를 파괴하고 드라이브의 모든 데이터를 완전히 지웁니다. 파일이 삭제되거나 드라이브가 다시 포맷된 후에도 드라이브에서 정보를 복구할 수 있습니다. 파일을 삭제하거나 드라이브를 다시 포맷하면 드라이브의 주소 테이블만 제거됩니다. 따라서 드라이브의 모든 데이터를 완전히 지우려면 디스크 완전 삭제 소프트웨어를 사용합니다.

# 로그 유지 관리

정기적으로 로그 파일을 검사하고 유지 관리합니다. 다음 방법으로 로그 파일을 보안할 수 있습니다.

- 로깅을 사용으로 설정하고 전용 보안 로그 호스트로 로그를 보냅니다.
- NTP(Network Time Protocol) 및 시간 기록을 사용하여 정확한 시간 정보가 포함되도록 로깅을 구성합니다.
- 발생 가능한 문제에 대비하여 로그를 검토하고 보안 정책에 따라 아카이브합니다.
- 로그 파일이 적당한 크기를 초과할 경우 주기적으로 로그 파일을 처분합니다. 나중에 참조하거나 통계 분석에 사용할 수 있도록 처분할 파일의 복사본을 유지 관리합니다.