SPARC 및 Netra SPARC T5 시리즈 서버

보안 설명서

Part No: E40473-01
2013년 4월

저작권 © 2013 , Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이센스 계약서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이센스 계약서 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 등록 상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제 3자로부터 제공되는 컨텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. Oracle Corporation과 그 자회사는 제 3자의 컨텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제 3자의 컨텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다.

차례

• • • 1 장

SPARC 및 Netra SPARC T5 시리즈 서버 보안

이 문서는 SPARC T5-1B, T5-2, T5-4, T5-8 및 Netra SPARC T5-1B 서버에 대한 일반 보안 지침을 제공합니다. 이 설명서는 네트워크 스위치, 네트워크 인터페이스 카드 등의 Oracle 하드웨어 제품과 함께 이 서버를 사용할 경우 보안을 유지하는 데 유용한 정보를 제공합니다.

이 장은 다음 절로 구성됩니다.

보안 원칙 이해

액세스, 인증, 권한 부여 및 계정 관리의 네 가지 기본 보안 원칙이 있습니다.

- **액세스**

  물리적 제어 및 소프트웨어 제어를 통해 침입으로부터 하드웨어 또는 데이터를 보호합니다.
  - 하드웨어의 경우 액세스 제한은 일반적으로 물리적 액세스 제한을 의미합니다.
  - 소프트웨어의 경우 액세스는 물리적 수단 및 가상 수단을 통해 제한됩니다.
  - 펌웨어는 Oracle 업데이트 프로세스를 통해서만 변경할 수 있습니다.
- **인증**

  모든 플랫폼 운영 체제에서는 사용자가 자신들에 대해 말하는 정보를 확인하기 위해 설정할 수 있는 인증 기능을 제공합니다.

  인증은 배지 및 암호와 같은 수단을 통해 다양한 수준의 보안을 제공합니다.
- **권한 부여**

  권한 부여를 통해 회사 직원이 자신들이 사용하기 위해 교육 받고 인증 받은 하드웨어 및 소프트웨어만 작업하도록 할 수 있습니다. 읽기/쓰기/실행 권한 시스템을 설정하여 명령, 디스크 공간, 장치 및 응용 프로그램에 대한 사용자 액세스 권한을 제어할 수 있습니다.
- **계정 관리**

  Oracle 소프트웨어 및 하드웨어 계정 관리 기능을 사용하여 로그인 작업을 모니터하고 하드웨어 인벤토리를 유지 관리할 수 있습니다.

- 사용자 로그인은 시스템 로그를 통해 모니터링할 수 있습니다. 특히 시스템 관리자 및 서비스 계정은 강력한 명령에 대한 액세스 권한이 있기 때문에 시스템 로그를 통해 주의 깊게 모니터링해야 합니다. 일반적으로 로그는 오랜 시간 동안 유지 관리되므로 고객 회사 정책에 따라 적정 크기를 초과하면 주기적으로 로그 파일을 폐기하는 것이 중요합니다.
- 고객 IT 자산은 일반적으로 일련 번호를 통해 추적됩니다. Oracle 부품 번호는 전자적으로 모든 카드, 모듈 및 마더보드에 기록되어 인벤토리 용도로 사용할 수 있습니다.

보안 환경 계획

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

하드웨어 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.
  - 장비가 잠금 문이 있는 랙에 설치된 경우 랙의 구성 요소를 서비스해야 하기 전까지는 항상 랙 문을 잠급니다.
  - SSH 연결보다 강력한 액세스를 제공할 수 있는 USB 콘솔에 대한 액세스를 제한합니다. 시스템 컨트롤러, PDU(전력 분배 장치), 네트워크 스위치 등의 장치가 USB 연결을 제공할 수 있습니다.
  - 핫 플러그 또는 핫 스왑 장치는 쉽게 분리될 수 있으므로 접근을 제한합니다.
  - 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**
  - 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.

소프트웨어 보안

대부분의 하드웨어 보안은 소프트웨어 수단을 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. 또한 네트워크 스위치와 같은 장치는 기본적으로 여러 사용자 계정이 있을 수 있습니다. 모든 계정 암호를 변경해야 합니다.
- `root` 수퍼 유저 계정의 사용을 제한합니다. 가능하면 `operator` 및 `administrator`와 같은 Oracle ILOM(Oracle Integrated Lights Out Manager) 사용자 프로파일을 대신 사용해야 합니다.
- 일반 네트워크와 구분하려면 서비스 프로세서의 전용 네트워크를 사용합니다.
- 소프트웨어에 사용 가능한 보안 기능을 사용으로 설정하려면 소프트웨어와 함께 제공된 설명서를 참조하십시오.
- 서버는 WAN 부트 또는 iSCSI 부트를 사용하여 안전하게 부트할 수 있습니다.
  - Oracle Solaris 10 릴리스의 경우 Oracle Solaris 설치 설명서: 네트워크 기반 설치를 참조하십시오

- Oracle Solaris 11 릴리스의 경우 WAN 부트 정보는 Oracle Solaris 11 시스템 설치를 참조하고, iSCSI 부트 정보는 시스템 관리 설명서: 기본 관리를 참조하십시오.

Oracle Solaris 보안 지침 문서는 다음에 대한 정보를 제공합니다.

- Oracle Solaris를 강화하는 방법
- 시스템을 구성할 때 Oracle Solaris 보안 기능을 사용하는 방법
- 응용 프로그램 및 사용자를 시스템에 추가할 때 안전하게 작동하는 방법
- 네트워크 기반 응용 프로그램을 보호하는 방법

사용 중인 버전에 대한 Oracle Solaris 보안 지침 문서는 다음 위치에 있습니다.

- http://www.oracle.com/goto/Solaris11/docs
- http://www.oracle.com/goto/Solaris10/docs

펌웨어 보안

Oracle 시스템 펌웨어의 모든 하위 구성 요소는 함께 업데이트할 수 있습니다. Oracle 시스템 펌웨어는 제어된 펌웨어 업데이트 프로세스를 사용하여 인증되지 않은 펌웨어 수정을 방지합니다. 수퍼유저 또는 적절한 권한을 보유한 인증된 사용자만 업데이트 프로세스를 사용할 수 있습니다.

Oracle OpenBoot 보안

Oracle OpenBoot 펌웨어 명령줄 인터페이스에 대한 액세스는 OpenBoot 보안 변수를 사용하여 암호로 보호할 수 있습니다.

OpenBoot 보안 변수 설정에 대한 자세한 내용은 다음 위치에 있는 OpenBoot 4.x Command Reference Manual을 참조하십시오.

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM 펌웨어

Oracle ILOM(Integrated Lights Out Manager)은 서버, 서버 모듈, 모듈식 시스템 및 기타 Oracle 하드웨어에 사전 설치된 시스템 관리 펌웨어입니다. Oracle ILOM을 사용하면 시스템에 설치된 구성 요소를 적극적으로 관리 및 모니터링할 수 있습니다. Oracle ILOM을 사용하는 방법은 시스템의 보안에 영향을 미칩니다. 암호 설정, 사용자 관리 및 보안 셸(Secure Shell, SSH), SSL(Secure Socket Layer), RADIUS 인증을 비롯한 보안 관련 기능을 적용할 때 이 펌웨어 사용에 대해 좀 더 자세하게 이해하려면 다음 Oracle ILOM 설명서를 참조하십시오.

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

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 제어

일부 Oracle 시스템은 소프트웨어 명령에 의해 설정되고 해제되도록 설정할 수 있습니다. 또한 일부 시스템 캐비닛의 PDU(전력 분배 장치)도 소프트웨어 명령을 통해 원격으로 사용 및 사용 안함으

로 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

Oracle 일련 번호는 옵션 카드 및 시스템 마더보드에 있는 펌웨어에 포함되어 있습니다. 인벤토리 추적을 위해 이러한 일련 번호는 LAN(Local Area Network) 연결을 통해 읽을 수 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 RFID는 다음 사이트에서 확인할 수 있습니다.

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

소프트웨어 및 펌웨어 업데이트

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

로컬 및 원격 액세스

시스템에 대한 로컬 및 원격 액세스 보안을 유지하려면 다음 지침을 따르십시오.

- 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 인증 서버와 통신하도록 원격 액세스 서버를 허용하는 프로토콜입니다.
- IDS(침입 방지 시스템) 액세스를 위해 스위치의 포트 미러링 기능을 사용합니다.
- MAC 주소를 기반으로 액세스를 제한하려면 포트 보안을 구현합니다. 모든 포트에서 자동 트렁킹을 사용 안함으로 설정합니다.
- Telnet 대신 SSH를 사용하여 원격 구성을 특정 IP 주소로 제한합니다. Telnet은 사용자 이름 및 암호를 일반 텍스트로 전달하여 잠재적으로 LAN 세그먼트에 있는 모든 사용자가 로그인 자격 증명을 볼 수 있습니다. SSH에 대해 강력한 암호를 설정합니다.
- 이전 버전의 SNMP는 보안이 설정되지 않아 암호화되지 않은 텍스트로 인증 데이터를 전송합니다. SNMP 3 버전만 보안 전송을 제공할 수 있습니다.
- 일부 제품은 공장 출하 시 기본 SNMP 커뮤니티 문자열로 설정된 PUBLIC과 함께 제공됩니다. 공격자는 커뮤니티를 질의하여 거의 완전한 네트워크 맵을 작성하고 MIB(Management Information Base) 값을 수정할 수 있습니다. SNMP가 필요한 경우 기본 SNMP 커뮤니티 문자열을 강력한 커뮤니티 문자열로 변경합니다.

- 로깅을 사용으로 설정하고 전용 보안 로그 호스트로 로그를 보냅니다.
- NTP 및 시간 기록을 사용하여 정확한 시간 정보가 포함되도록 로깅을 구성합니다.
- 발생 가능한 사고를 위해 로그를 검토하고 보안 정책에 따라 아카이브합니다.
- 시스템 컨트롤러가 브라우저 인터페이스를 사용하는 경우 사용 후에 반드시 로그아웃합니다.

데이터 보안

데이터 보안을 최대화하려면 다음 지침을 따르십시오.

- 외부 하드 드라이브, 펜 드라이브 또는 메모리 스틱과 같은 장치를 사용하여 중요한 데이터를 백업합니다. 외부의 안전한 별도의 위치에 백업된 데이터를 보관합니다.
- 데이터 암호 소프트웨어를 사용하여 기밀 정보를 하드 드라이브에 안전하게 보관합니다.
- 이전 하드 드라이브를 폐기할 때는 물리적으로 드라이브를 완전히 제거하고 드라이브의 모든 데이터를 완전히 지웁니다. 모든 파일을 삭제하거나 드라이브를 재포맷하면 드라이브의 주소 테이블만 제거되기 때문에 파일을 삭제하거나 드라이브를 재포맷한 후에도 여전히 드라이브에서 정보를 복구할 수 있습니다. 따라서 드라이브의 모든 데이터를 완전히 지우려면 디스크 완전 삭제 소프트웨어를 사용하십시오.

네트워크 보안

네트워크 보안을 최대화하려면 다음 지침을 따르십시오.

- 대부분의 스위치를 통해 VLAN(Virtual Local Area Network)을 정의할 수 있습니다. 스위치를 사용하여 VLAN을 정의하는 경우 네트워크의 나머지에서 시스템의 중요한 클러스터를 분리합니다. 그러면 사용자가 이러한 클라이언트 및 서버의 정보에 대한 액세스 권한을 얻을 가능성이 줄어듭니다.
- 스위치를 아웃오브밴드(데이터 트래픽에서 분리)로 관리합니다. 아웃오브밴드 관리가 가능하지 않으면 인밴드 관리를 위해 별도의 VLAN 번호를 지정합니다.
- 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.
- 스위치 구성 파일을 오프라인으로 유지 관리하고 권한이 부여된 관리자로만 액세스를 제한합니다. 구성 파일에는 각 설정에 대한 세부 설명이 포함되어 있어야 합니다.
- 가능한 경우 정적 VLAN 구성을 사용합니다.
- 사용하지 않는 스위치 포트는 사용 안함으로 설정하고 이 포트에 사용하지 않는 VLAN 번호를 지정합니다.
- 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.
- TCP 소형 서버 또는 HTTP와 같이 필요 없는 네트워크 서비스를 사용 안함으로 설정합니다. 필요한 네트워크 서비스를 사용으로 설정하고 이러한 서비스를 안전하게 구성합니다.
- 서로 다른 스위치는 다른 레벨의 포트 보안 기능을 제공합니다. 스위치에서 사용 가능한 경우 다음 포트 보안 기능을 사용합니다.
  - MAC 잠금(Locking): 하나 이상의 연결된 장치의 MAC(매체 액세스 제어) 주소를 스위치의 물리적 포트에 연결시키는 것과 관련됩니다. 특정 MAC 주소로 스위치 포트를 잠그면 수퍼 유저가 허위 액세스 포인트가 있는 네트워크로의 백도어를 만들 수 없습니다.
  - MAC 잠금(Lockout): 스위치에 연결된 특정한 MAC 주소를 사용 안함으로 설정합니다.

- MAC 학습(Learning): 각 스위치 포트의 직접 연결에 대한 지식을 사용하므로 스위치에서 현재 연결에 기반한 보안을 설정할 수 있습니다.