SPARC M5-32 및 SPARC M6-32 서버

보안 설명서

부품 번호: E49760-02
2014년 7월

차례

1 장

하드웨어 보안 이해

물리적 격리 및 접근 제어를 기반으로 보안 아키텍처를 구축해야 합니다. 물리적 서버가 안전한 환경에 설치되면 허용되지 않은 액세스로부터 보호됩니다. 마찬가지로 모든 일련 번호를 기록해 두면 도난, 재판매 또는 공급망 위험(위조 또는 손상된 구성 요소의 조직 공급망 침투)을 방지할 수 있습니다.

이 장에서는 SPARC M5-32 및 M6-32 서버에 대한 일반적인 하드웨어 보안 지침을 제공합니다.

이 장은 다음 절로 구성됩니다.

접근 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. 문을 잠그면 핫 플러그 또는 핫 스왑 장치에 대한 접근도 제한됩니다.
- 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.
- 랙 및 예비 장치 캐비닛에 대한 잠금 상태 및 무결성을 주기적으로 확인하여 변조 또는 문 잠금 해제 상태 유지를 방지하거나 감지합니다.
- 접근이 제한된 안전한 위치에 캐비닛 키를 보관합니다.
- USB 콘솔에 대한 접근을 제한합니다. 시스템 컨트롤러, PDU(전원 분배 장치), 네트워크 스위치 등의 장치가 USB 연결을 제공할 수 있습니다. 물리적 접근은 네트워크 기반 공격에 노출되지 않으므로 구성 요소에 접근할 수 있는 보다 안전한 방법입니다.
- 원격 콘솔에 접근할 수 있도록 외부 KVM에 콘솔을 연결합니다. KVM 장치는 두 단계 인증, 중앙화된 접근 제어 및 감사를 지원하는 경우가 많습니다. KVM 보안 지침 및 모범 사례에 대한 자세한 내용은 KVM 장치와 함께 제공된 설명서를 참조하십시오.

일련 번호

- 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 접근할 수 있는 안전한 위치에 하드웨어 활성화 키 및 라이센스를 보관합니다. 인쇄된 문서가 유일한 소유권 증명이 될 수도 있습니다.

무선 RFID 판독기를 통해 추가로 자산 추적을 간소화할 수 있습니다. 자세한 내용은 다음 사이트의 *How to Track Your Oracle Sun System Assets by Using RFID*를 참조하십시오.

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

하드 드라이브

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

- Oracle Solaris **format** (1M) 명령 등 디스크 완전 삭제 도구를 사용하여 디스크 드라이브에서 모든 데이터를 완전히 지웁니다. 적절하며 사용 가능한 경우 물리적 소자 도구를 사용할 수도 있습니다.
- 하드 드라이브에 포함된 정보가 매우 중요하여 분쇄 또는 소각을 통해 하드 드라이브를 물리적으로 폐기하는 것만이 적절한 정리 방법인 경우도 있습니다.

조직에서는 관련 데이터 보호 정책을 참조하여 가장 적절한 하드 드라이브 정리 방법을 결정해야 합니다.

주의

데이터 액세스 관리 방식으로 인해 디스크 완전 삭제 소프트웨어를 사용하여 최신 하드 드라이브(특히 SSD)의 일부 데이터를 삭제하지 못할 수도 있습니다.

• • • 2 장

2 소프트웨어 보안 이해

대부분의 하드웨어 보안은 소프트웨어 수단을 통해 구현됩니다. 이 장에서는 SPARC M5-32 및 SPARC M6-32 서버에 대한 일반적인 소프트웨어 보안 지침을 제공합니다.

이 장은 다음 절로 구성됩니다.

▼ 허용되지 않은 액세스 방지(Oracle Solaris OS)

- Oracle Solaris 소프트웨어에 대한 액세스를 제한하는 Oracle Solaris OS 명령을 사용하여 OS를 강화하고 보안 기능을 사용하며 응용 프로그램을 보호합니다.
  다음 사이트에서 사용 중인 OS 버전에 대한 Oracle Solaris 보안 지침 문서를 얻습니다.
  http://www.oracle.com/goto/Solaris11/docs
  http://www.oracle.com/goto/Solaris10/docs

▼ 허용되지 않은 액세스 방지(Oracle ILOM)

1. Oracle ILOM 소프트웨어에 대한 사용자 액세스를 제한하는 Oracle ILOM 명령을 사용하여 출하 시 설정된 암호를 변경하고 루트 수퍼 유저 계정 사용을 제한하며 서비스 프로세서에 대한 개인 네트워크를 보안합니다.
   다음 사이트에서 *Oracle ILOM* 보안 설명서를 얻습니다.
   http://www.oracle.com/goto/ILOM/docs
2. 특정 물리적 도메인에 적용되는 역할을 가지는 사용자 계정을 만들어 플랫폼별 Oracle ILOM 명령으로 개별 도메인을 보안합니다.
   물리적 도메인에 사용자 역할을 지정하는 경우 해당 도메인에 대한 기능은 플랫폼에 대해 지정된 사용자 역할의 기능을 미러링하지만, 제공된 구성 요소에 대해 실행된 명령으로 제한됩니다.

참고

관리자(a), 콘솔(c) 및 재설정(r) 사용자 역할만 개별 물리적 도메인에 대해 지정할 수 있습니다.

다음 사이트에서 *SPARC M5-32* 및 *SPARC M6-32* 서버 관리 설명서를 얻습니다.
http://www.oracle.com/goto/M6-32/docs

▼ 허용되지 않은 액세스 방지(Oracle VM Server for SPARC)

- Oracle VM for SPARC 소프트웨어에 대한 액세스를 제한하는 Oracle VM for SPARC 명령을 사용합니다.
  다음 사이트에서 *Oracle VM for SPARC* 보안 설명서를 얻습니다.
  http://www.oracle.com/goto/VM-SPARC/docs

액세스 제한(OpenBoot)

다음 항목에서는 OpenBoot 프롬프트에서 액세스를 제한하는 방법에 대해 설명합니다.

- 암호 보호 구현(OpenBoot) [8]
- 실패한 로그인 확인(OpenBoot) [8]
- 전원 켜기 배너 제공(OpenBoot) [9]

관련 정보

- OpenBoot 보안 변수 설정에 대한 자세한 내용은 *OpenBoot 4.x Command Reference Manual*(http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069)을 참조하십시오.

▼ 암호 보호 구현(OpenBoot)

- security-mode 매개변수를 **full** 또는 **command**로 설정합니다.
  full로 설정하는 경우 부트 등 일반 작업을 비롯한 모든 작업을 수행하는 데 암호가 필요합니다. **command**로 설정하는 경우 **boot** 또는 **go** 명령에는 암호가 필요하지 않지만 기타 모든 명령에는 암호가 필요합니다. 비즈니스 연속성을 위해서는 다음 예와 같이 security-mode 매개변수를 command로 설정합니다.

```
ok password
ok setenv security-mode command
ok password
```

▼ 실패한 로그인 확인(OpenBoot)

1. 다음 예와 같이 **security-#badlogins** 매개변수를 사용하여 OpenBoot 환경에 대해 시도된 액세스 및 실패한 액세스가 있는지 확인합니다.

```
ok printenv security-#badlogins
```

   이 명령으로 0보다 큰 값이 반환되면 OpenBoot 환경에 대해 실패한 액세스 시도가 기록된 것입니다.

2. 다음 명령을 입력하여 **security-#badlogins** 매개변수를 재설정합니다.

```
ok setenv security-#badlogins 0
```

▼ 전원 켜기 배너 제공(OpenBoot)

- 다음 명령을 통해 사용자 정의 경고 메시지를 사용으로 설정합니다.

```
ok setenv oem-banner banner-message
ok setenv oem-banner? true
```

Oracle 시스템 펌웨어

Oracle 시스템 펌웨어는 제어된 업데이트 프로세스를 사용하여 허용되지 않은 수정을 방지합니다. 수퍼 유저 또는 적절한 권한이 부여된 인증된 사용자만 업데이트 프로세스를 사용할 수 있습니다.

최신 업데이트 또는 패치를 얻는 방법은 사용 중인 서버의 제품 안내서를 참조하십시오.

보안 WAN 부트

WAN 부트는 다양한 보안 레벨을 지원합니다. WAN 부트로 지원되는 다양한 보안 기능을 사용하여 네트워크 요구 사항을 충족시킬 수 있습니다. 보다 안전한 구성을 위해서는 추가적인 관리가 필요하지만 이를 통해 더 많은 시스템 데이터가 보호됩니다.

- Oracle Solaris 10 OS의 경우 *Oracle Solaris* 설치 설명서*:* 네트워크 기반 설치의 "보안 WAN 부트 설치 구성"을 참조하십시오.

  http://www.oracle.com/goto/Solaris10/docs
- Oracle Solaris 11 OS의 경우 *Securing the Network in Oracle Solaris 11.1*을 참조하십시오.

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