SPARC T8 시리즈 서버 보안 설명서

부품 번호: **E91691-01**
2017년 9월

ORACLE

부품 번호: E91691-01

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

하드웨어 보안 이해 7
- 접근 제한 7
- 일련 번호 8
- 하드 드라이브 8

소프트웨어 보안 이해 9
- ▼ 허용되지 않은 액세스 방지(Oracle Solaris OS) 9
- ▼ 허용되지 않은 액세스 방지(Oracle ILOM) 9
- ▼ 허용되지 않은 액세스 방지(Oracle VM Server for SPARC) 9
- 액세스 제한(OpenBoot) 10
  - ▼ 암호 보호 구현 10
  - ▼ 보안 모드 사용 10
  - ▼ 보안 모드 사용 안함 11
  - ▼ 실패한 로그인 확인 11
  - ▼ 전원 켜기 배너 제공 12
- Oracle 시스템 펌웨어 12
- 보안 WAN 부트 12

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 구성요소의 조직 공급망 침투)을 방지할 수 있습니다.

다음 절에서는 SPARC T8-1, T8-2 및 T8-4 서버에 대한 일반적인 하드웨어 보안 지침을 제공합니다.

- “접근 제한” [7]
- “일련 번호” [8]
- “하드 드라이브” [8]

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 사고로 인한 문 잠금 해제 상태 유지를 방지하거나 감지합니다.
- 접근이 제한된 안전한 위치에 캐비닛 키를 보관합니다.
- USB 콘솔에 대한 접근을 제한합니다. 시스템 컨트롤러, PDU(전력 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 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*는 다음 사이트에서 확인할 수 있습니다.

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 정리합니다.

- Oracle Solaris format (1M) 명령 등 디스크 완전 삭제 도구를 사용하여 디스크 드라이브에서 모든 데이터를 완전히 지웁니다.
- 조직에서는 관련 데이터 보호 정책을 참조하여 가장 적절한 하드 드라이브 정리 방법을 결정해야 합니다.
- 필요한 경우 Oracle의 고객 데이터 및 장치 보존 서비스를 활용합니다.

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

소프트웨어 보안 이해

대부분의 하드웨어 보안은 소프트웨어 수단을 통해 구현됩니다. 다음 절에서는 SPARC T8-1, T8-2 및 T8-4 서버에 대한 일반적인 소프트웨어 보안 지침을 제공합니다.

- 허용되지 않은 액세스 방지(Oracle Solaris OS) [9]
- 허용되지 않은 액세스 방지(Oracle ILOM) [9]
- 허용되지 않은 액세스 방지(Oracle VM Server for SPARC) [9]
- “액세스 제한(OpenBoot)” [10]
- “Oracle 시스템 펌웨어” [12]
- “보안 WAN 부트” [12]

▼ 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 버전에 대한 *Oracle Solaris Security Guidelines* 문서를 얻습니다.

  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

▼ 허용되지 않은 액세스 방지(Oracle ILOM)

- **Oracle ILOM 소프트웨어에 대한 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`

▼ 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 [10]
- 보안 모드 사용 [10]
- 보안 모드 사용 안함 [11]
- 실패한 로그인 확인 [11]
- 전원 켜기 배너 제공 [12]

OpenBoot 보안 변수 설정에 대한 자세한 내용은 다음 위치에 있는 OpenBoot 설명서를 참조하십시오.

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

▼ 암호 보호 구현

- **아직 암호를 설정하지 않았으면 이 단계를 수행합니다.**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

암호는 1~8개 사이의 문자일 수 있습니다. 8개 이상의 문자를 입력한 경우 처음 8개 문자만 사용됩니다. 모든 인쇄 가능한 문자가 허용됩니다. 제어 문자는 허용되지 않습니다.

주 - 암호를 0개 문자로 설정하면 보안이 해제되고 `security-mode` 매개변수가 `none`으로 설정된 것처럼 취급됩니다. 하지만 설정이 변경되지는 않습니다.

▼ 보안 모드 사용

1. **`security-mode` 매개변수를 `full` 또는 `command`로 설정합니다.**

   `full`로 설정하는 경우 `boot` 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 `command`로 설정합니다.

```
{0} ok setenv security-mode command
{0} ok
```

2. **보안 모드 프롬프트를 가져옵니다.**

   위의 설명에 따라 보안 모드를 설정한 다음에는 두 가지 방법으로 보안 모드 프롬프트를 가져올 수 있습니다.

주 - HOST 콘솔이 시작되면 HUP가 콘솔로 전송됩니다. `security-mode`가 OpenBoot에서 설정된 경우 HUP로 인해 로그아웃 동작이 발생합니다. 따라서 HOST 콘솔이 다시 시작되면 사용자가 로그인하여 OpenBoot OK 프롬프트에 액세스해야 합니다.

- **`logout` 및 `login` 단어를 사용합니다.**

  ```
  {0} ok logout
  Type boot , go (continue), or login (command mode)
  >
  > login
  Firmware Password: password
  Type help for more information
  {0} ok
  ```

  보안 모드를 종료하려면 예에서와 같이 `logout` 및 `login` 이름을 사용합니다.

- **`reset-all` 단어를 사용합니다.**

  ```
  {0} ok reset-all
  ```

  이 단어는 시스템을 재설정합니다. 시스템이 다시 작동되면 OpenBoot가 보안 모드 프롬프트로 이동합니다. 명령 프롬프트에 다시 로그인하려면(또는 보안 모드에서 로그아웃하려면) `logout` 및 `login` 이름을 사용한 후 위 설명에 따라 암호를 입력합니다.

▼ 보안 모드 사용 안함

1. **`security-mode` 매개변수를 `none`으로 설정합니다.**

   ```
   {0} ok setenv security-mode none
   ```

2. **두 암호 프롬프트 다음에 Return을 입력해서 암호를 0 길이로 설정합니다.**

▼ 실패한 로그인 확인

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

   ```
   {0} ok printenv security-#badlogins
   ```

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

2. **이 명령을 입력해서 매개변수를 재설정합니다.**

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

▼ 전원 켜기 배너 제공

직접적인 방지책이나 감지 제어 방법은 아니지만 다음과 같은 이유로 배너를 사용할 수 있습니다.

- 소유권 이전
- 사용자에게 허용되는 서버 사용에 대해 경고
- OpenBoot 매개변수에 대한 액세스나 수정을 허가된 사용자만으로 제한

- **다음 명령을 통해 사용자정의 경고 메시지를 사용으로 설정합니다.**

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

배너 메시지는 68자까지 지정할 수 있습니다. 모든 인쇄 가능한 문자가 허용됩니다.

Oracle 시스템 펌웨어

Oracle 시스템 펌웨어는 제어된 업데이트 프로세스를 사용하여 허용되지 않은 수정을 방지합니다. 수퍼 유저 또는 적절한 권한을 보유한 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 요구사항을 충족시킬 수 있습니다. 보다 안전한 구성을 위해서는 추가적인 관리가 필요하지만 이를 통해 시스템 데이터가 더 많이 보호됩니다.

- Oracle Solaris 10 OS의 경우 *Oracle Solaris* 설치 설명서*:* 네트워크 기반 설치 문서에서 WAN 부트 설치 구성 보안에 대한 정보를 참조하십시오.
- Oracle Solaris 11 OS의 경우 Oracle Solaris 11.3 시스템 설치를 참조하십시오.