Oracle® VM Server for SPARC 3.0 보안 설명서

부품 번호: E37594
2012년 11월

ORACLE

130417@25097

목차

머리말

Oracle VM Server for SPARC 3.0 보안 설명서는 Oracle VM Server for SPARC 3.0 소프트웨어를 안전하게 설치, 구성 및 사용하는 방법에 대한 내용을 다룹니다.

관련 문서

다음 표는 Oracle VM Server for SPARC 3.0 릴리스와 관련된 사용 가능한 설명서를 보여줍니다.

표 P–1 관련 문서

응용 프로그램	제목
Oracle VM Server for SPARC 3.0 소프트웨어	**Oracle VM Server for SPARC 3.0 관리 설명서** **Oracle VM Server for SPARC 3.0 보안 설명서** **Oracle VM Server for SPARC 3.0 Reference Manual** **Oracle VM Server for SPARC 3.0 릴리스 노트**
Oracle VM Server for SPARC 3.0 `drd`(1M) 및 `vntsd`(1M) 매뉴얼 페이지	Oracle Solaris OS 참조 설명서: ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
Oracle Solaris OS: 설치 및 구성	Oracle Solaris OS 설치 및 구성 설명서: ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
Oracle VM Server for SPARC 및 Oracle Solaris OS 보안	Oracle VM Server for SPARC 백서 및 Oracle Solaris OS 보안 설명서: ■ **Secure Deployment of Oracle VM Server for SPARC** (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf`) ■ **Oracle Solaris 10 Security Guidelines** ■ **Oracle Solaris 11 Security Guidelines**

사용 중인 서버, 소프트웨어 또는 Oracle Solaris OS 관련 설명서는 http://www.oracle.com/technetwork/indexes/documentation/index.html에서 찾을 수 있습니다. 검색 상자를 이용하여 필요한 문서와 정보를 찾으십시오.

Oracle VM Server for SPARC 토론 포럼은 http://forums.oracle.com/forums/forum.jspa?forumID=1047에서 액세스할 수 있습니다.

Oracle Support에 액세스

Oracle 고객은 My Oracle Support를 통해 전자 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.

활자체 규약

다음 표는 이 책에서 사용되는 활자체 규약에 대해 설명합니다.

표 P–2 활자체 규약

활자체	설명	예
`AaBbCc123`	명령 및 파일, 디렉토리 이름; 컴퓨터 화면에 출력되는 내용입니다.	`.login` 파일을 편집하십시오. 모든 파일 목록을 보려면 `ls -a` 명령을 사용하십시오. `machine_name% you have mail.`
`AaBbCc123`	사용자가 입력하는 내용으로 컴퓨터 화면의 출력 내용과 대조됩니다.	`machine_name%` **`su`** `Password:`
aabbcc123	새로 나오는 용어, 강조 표시할 용어입니다. 명령줄 변수를 실제 이름이나 값으로 바꾸십시오.	파일을 제거하는 명령은 `rm` *filename*입니다.
AaBbCc123	책 제목, 장, 절	**사용자 설명서**의 6장을 읽으십시오. **캐시**는 로컬로 저장된 복사본입니다. 파일을 저장하면 **안 됩니다**. **주:** 일부 강조된 항목은 온라인에서 굵은체로 나타납니다.

명령 예의 셸 프롬프트

다음 표에는 Oracle Solaris OS에 포함된 셸의 UNIX 시스템 프롬프트 및 수퍼유저 프롬프트가 나와 있습니다. 명령 예제에서 셸 프롬프트는 일반 사용자 또는 권한 있는 사용자가 명령을 실행해야 하는지 여부를 나타냅니다.

표 P–3 쉘 프롬프트

셸	프롬프트
Bash 셸, Korn 셸 및 Bourne 셸	`$`
수퍼유저용 Bash 셸, Korn 셸 및 Bourne 셸	`#`
C 셸	`machine_name%`
수퍼유저용 C 셸	`machine_name#`

◆ ◆ ◆ 1 장

1 Oracle VM Server for SPARC 보안 개요

이 장에서는 Oracle VM Server for SPARC 소프트웨어에서 사용하는 다음과 같은 보안 기능에 대해 설명합니다.

Oracle VM Server for SPARC에서 사용하는 보안 기능

Oracle VM Server for SPARC 소프트웨어는 각각에 Oracle Solaris 10 또는 Oracle Solaris 11 OS가 설치된 둘 이상의 Oracle Solaris VM(가상 시스템)이 하나의 물리적 시스템에서 실행될 수 있도록 하는 가상화 제품입니다. 각 VM은 **논리적 도메인**이라고도 합니다. 도메인은 독립 인스턴스이므로 다른 응용 프로그램 소프트웨어는 물론 다른 버전의 Oracle Solaris OS도 실행할 수 있습니다. 예를 들어 도메인에서 다른 패키지 개정판을 설치하고, 다른 서비스를 사용으로 설정하며, 다른 암호를 사용하는 시스템 계정을 사용할 수 있습니다. Oracle Solaris 보안에 대한 자세한 내용은 **Oracle Solaris 10 Security Guidelines** 및 **Oracle Solaris 11 Security Guidelines**를 참조하십시오.

논리적 도메인을 구성하고 상태 정보를 검색하려면 `ldm` 명령을 컨트롤 도메인에서 실행해야 합니다. 컨트롤 도메인 및 `ldm` 명령에 대한 액세스를 제한하는 것은 시스템에서 실행되는 도메인의 보안에 중요합니다. 도메인 구성 데이터에 대한 액세스를 제한하려면 콘솔 및 `solaris.ldoms` 권한 부여에 대해 Oracle Solaris의 RBAC(역할 기반 액세스 제어)와 같은 Oracle VM Server for SPARC 보안 기능을 사용하십시오. **Oracle VM Server for SPARC 3.0 관리 설명서**의 “Logical Domains Manager 프로파일 컨텐츠”를 참조하십시오.

Oracle VM Server for SPARC 소프트웨어에서 사용하는 보안 기능은 다음과 같습니다.

- Oracle Solaris 10 OS와 Oracle Solaris 11 OS에서 사용 가능한 보안 기능은 Oracle VM Server for SPARC 소프트웨어를 실행하는 도메인에서도 사용 가능합니다. **Oracle Solaris 10 Security Guidelines** 및 **Oracle Solaris 11 Security Guidelines**를 참조하십시오.
- Oracle Solaris OS 보안 기능은 Oracle VM Server for SPARC 소프트웨어에 적용할 수 있습니다. Oracle VM Server for SPARC 보안에 대한 종합적인 내용은 **Secure Deployment of Oracle VM Server for SPARC**를 참조하십시오.
- Oracle Solaris 10 OS 및 Oracle Solaris 11 OS에는 시스템에 사용 가능한 보안 수정 프로그램이 포함되어 있습니다. Oracle Solaris 10 OS 수정 프로그램은 보안 패치나 업데이트로 제공되고, Oracle Solaris 11 OS 수정 프로그램은 SRU(Support Repository Update)로 제공됩니다.
- Oracle VM Server for SPARC 관리 명령 및 도메인 콘솔에 대한 액세스를 제한하고 Oracle VM Server for SPARC 감사 기능을 사용으로 설정하려면 **Oracle VM Server for SPARC 3.0 관리 설명서**의 3 장, “Oracle VM Server for SPARC 보안”를 참조하십시오.

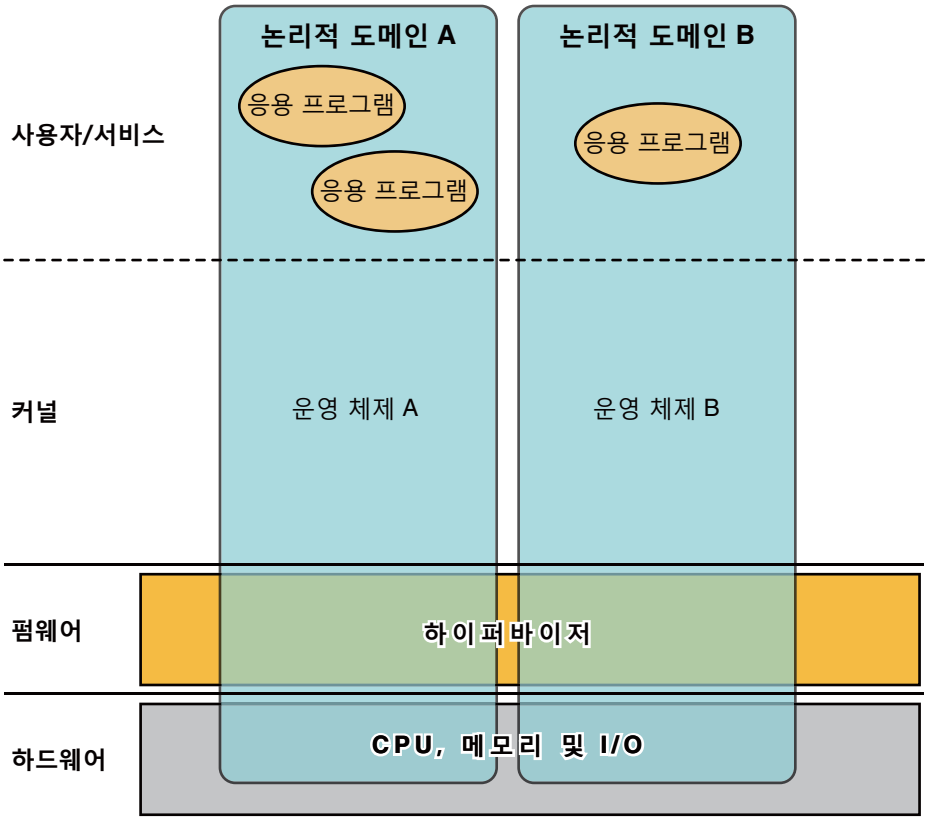
Oracle VM Server for SPARC 제품 개요

Oracle VM Server for SPARC는 Oracle's SPARC T-Series 서버에 매우 효율적인 엔터프라이즈급 가상화 기능을 제공합니다. Oracle VM Server for SPARC 소프트웨어를 사용하여 단일 시스템에 논리적 도메인이라는 가상 서버를 최대 128개까지 만들 수 있습니다. 이러한 종류의 구성을 통해 SPARC T-Series 서버와 Oracle Solaris OS에서 제공한 대규모 스레드를 활용할 수 있습니다.

논리적 도메인은 별도의 논리적 리소스 그룹을 포함하는 가상 시스템입니다. 논리적 도메인은 단일 컴퓨터 시스템 안에 자체 운영 체제와 신원을 가지고 있습니다. 각 논리적 도메인은 서버의 전원을 껐다가 켤 필요 없이 개별적으로 생성, 삭제, 재구성 및 재부트할 수 있습니다. 여러 논리적 도메인에서 다양한 응용 프로그램 소프트웨어를 실행하고 성능과 보안을 위해 이들을 독립적으로 유지할 수 있습니다.

Oracle VM Server for SPARC 소프트웨어 사용에 대한 자세한 내용은 **Oracle VM Server for SPARC 3.0 관리 설명서** 및 **Oracle VM Server for SPARC 3.0 Reference Manual** 을 참조하십시오. 필요한 하드웨어 및 소프트웨어에 대한 자세한 내용은 **Oracle VM Server for SPARC 3.0 릴리스 노트**를 참조하십시오.

그림 1–1 두 개의 논리적 도메인을 지원하는 하이퍼바이저



시스템 가상화를 제공하기 위해 Oracle VM Server for SPARC 소프트웨어에서 사용하는 구성 요소는 다음과 같습니다.

- **하이퍼바이저**: 하이퍼바이저는 운영 체제를 설치할 수 있는 안정적인 가상화 시스템 아키텍처를 제공하는 소형 펌웨어 계층입니다. 하이퍼바이저를 사용하는 Oracle Sun 서버는 논리적 도메인에서 운영 체제 작업에 대한 하이퍼바이저 제어를 지원하는 하드웨어 기능을 제공합니다.

  특정 SPARC 하이퍼바이저가 지원하는 도메인 수 및 각 도메인의 기능은 서버 종속 기능입니다. 하이퍼바이저는 서버의 CPU, 메모리 및 I/O 리소스의 일부분을 지정된 로컬 도메인에 할당할 수 있습니다. 이와 같이 할당하면 각 운영 체제가 자체 논리적 도메인 내에 있는 여러 운영 체제를 동시에 지원할 수 있습니다. 원하는 정밀도로 리소스를 개별 논리적 도메인 간에 재배열할 수 있습니다. 예를 들어, CPU 스레드의 세분성으로 논리적 도메인에 CPU를 지정할 수 있습니다.

  SC(**시스템 제어기**)라고도 하는 SP(서비스 프로세서)는 물리적 시스템을 모니터링하고 실행하지만 논리적 도메인을 관리하지는 않습니다. 논리적 도메인은 Logical Domains Manager에서 관리합니다.

- **컨트롤 도메인.** Logical Domains Manager는 이 도메인에서 실행되어 사용자가 다른 논리적 도메인을 만들고 관리하며, 가상 리소스를 다른 도메인에 할당할 수 있도록 해줍니다. 서버당 하나의 컨트롤 도메인만 가질 수 있습니다. 컨트롤 도메인은 Oracle VM Server for SPARC 소프트웨어를 설치할 때 가장 먼저 만들어지는 도메인으로, `primary`로 이름이 지정됩니다.
- **서비스 도메인**: 서비스 도메인은 가상 스위치, 가상 콘솔 집중기, 가상 디스크 서버 등의 가상 장치 서비스를 다른 도메인에 제공합니다. 임의 도메인을 서비스 도메인으로 구성할 수 있습니다.
- **I/O 도메인.** I/O 도메인은 PCIe(PCI EXPRESS) 제어기에 있는 네트워크 카드와 같은 물리적 I/O 장치에 직접 액세스할 수 있습니다. I/O 도메인은 PCIe 루트 컴플렉스를 소유하거나, 직접 I/O(DIO) 기능을 사용하여 PCIe 슬롯 또는 온보드 PCIe 장치를 소유할 수 있습니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "PCIe 끝점 장치 지정"를 참조하십시오.

  I/O 도메인은 서비스 도메인으로 사용될 경우 물리적 I/O 장치를 가상 장치 형태로 다른 도메인과 공유할 수 있습니다.
- **루트 도메인**: 루트 도메인에는 PCIe 루트 컴플렉스가 지정됩니다. 이 도메인은 PCIe 패브릭을 소유하며 패브릭 오류 처리와 같은 모든 패브릭 관련 서비스를 제공합니다. 루트 도메인은 물리적 I/O 장치를 소유하고 직접 액세스를 제공하므로 I/O 도메인이기도 합니다.

  플랫폼 구조에 따라 지정할 수 있는 루트 도메인 수가 다릅니다. 예를 들어 Oracle의 Sun SPARC Enterprise T5440 서버를 사용하는 경우 루트 도메인을 네 개까지 지정할 수 있습니다.
- **게스트 도메인.** 게스트 도메인은 하나 이상의 서비스 도메인에서 제공하는 가상 장치 서비스를 이용하는 비I/O 도메인으로, 물리적 I/O 장치가 없습니다. 디스크 장치 및 가상 네트워크 인터페이스와 같은 가상 I/O 장치만 있습니다.

대개 Oracle VM Server for SPARC 시스템에는 I/O 도메인과 서비스 도메인에서 수행하는 서비스를 제공하는 컨트롤 도메인이 한 개만 있습니다. 중복성 및 플랫폼 서비스 가용성을 높이려면 Oracle VM Server for SPARC 시스템에 I/O 도메인을 두 개 이상 구성하십시오.

Oracle VM Server for SPARC에 일반 보안 원칙 적용

게스트 도메인을 다양한 방식으로 구성하여 다양한 레벨의 게스트 도메인 격리, 하드웨어 공유 및 도메인 연결을 제공할 수 있습니다. 이러한 요소는 전반적인 Oracle VM Server for SPARC 구성의 보안 레벨에 기여하므로, 다음과 같은 몇 가지 일반 보안 원칙을 이 구성에 적용할 수 있습니다.

- **공격 영역을 최소화합니다.**
  - 시스템의 보안을 정기적으로 평가할 수 있는 운영 지침을 마련하여 의도하지 않은 구성 오류를 최소화합니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Counter Measure #1: Operational Guidelines"를 참조하십시오.
  - 도메인 격리를 최대화하도록 가상 환경의 아키텍처를 신중하게 계획합니다. **Secure Deployment of Oracle VM Server for SPARC**의 "Threat #2: Errors in the Architecture of the Virtual Environment"에 설명된 대책을 참조하십시오.
  - 지정할 리소스 및 리소스의 공유 여부를 신중하게 계획합니다. **Secure Deployment of Oracle VM Server for SPARC**의 "Counter Measure #7: Carefully Assigning Hardware Resources" 및 "Counter Measure #8: Careful Assignment of Shared Resources"를 참조하십시오.
  - **Secure Deployment of Oracle VM Server for SPARC**의 "Threat #4: Manipulation of the Execution Environment" 및 "Counter Measure #28: Securing the Guest OS"에 설명된 대책을 적용하여 논리적 도메인이 조작으로부터 보호되도록 합니다.
  - 필요한 **경우에만** 게스트 도메인을 네트워크에 노출합니다. 가상 스위치를 사용하여 게스트 도메인의 네트워크 연결을 **오직** 적합한 네트워크로만 제한할 수 있습니다.
  - **Oracle Solaris 10 Security Guidelines** 및 **Oracle Solaris 11 Security Guidelines**에 설명된 내용에 따라 Oracle Solaris 10 및 Oracle Solaris 11에 대한 공격 영역을 최소화하는 단계를 수행합니다.
  - **Secure Deployment of Oracle VM Server for SPARC**의 "Counter Measure #15: Validating Firmware and Software Signatures" 및 "Counter Measure #16: Validating Kernel Modules"에 설명된 내용에 따라 하이퍼바이저 코어를 보호합니다.
  - 서비스 거부 공격에 대비하여 컨트롤 도메인을 보호합니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Counter Measure #17: Console Access"를 참조하십시오.
  - 권한이 없는 사용자가 Logical Domains Manager를 실행하지 못하도록 합니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Threat #8: Unauthorized Use of Configuration Utilities"를 참조하십시오.
  - 권한이 없는 사용자나 프로세스가 서비스 도메인에 액세스하지 못하도록 합니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Threat #9: Manipulation of a Service Domain"을 참조하십시오.

- 서비스 거부 공격에 대비하여 I/O 도메인 또는 서비스 도메인을 보호합니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Threat #10: Denial-of-Service of IO Domain or Service Domain"을 참조하십시오.
- 권한이 없는 사용자나 프로세스가 I/O 도메인에 액세스하지 못하도록 합니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Threat #11: Manipulation of an IO Domain"을 참조하십시오.
- 불필요한 도메인 관리 서비스를 사용 안함으로 설정합니다. Logical Domains Manager는 도메인 액세스, 모니터링 및 마이그레이션을 위한 네트워크 서비스를 제공합니다. 다음 네트워크 서비스를 사용하지 않는 경우 사용 안함으로 설정합니다.
  - TCP 포트 `8101`의 마이그레이션 서비스

    이 서비스를 사용 안함으로 설정하려면 `ldmd(1M)` 매뉴얼 페이지에서 `ldmd/incoming_migration_enabled` 및 `ldmd/outgoing_migration_enabled` 등록 정보에 대한 설명을 참조하십시오.
  - TCP 포트 `6482`의 XMPP(확장성 메시징 및 프레즌스 프로토콜) 지원

    이 서비스를 사용 안함으로 설정하려면 **Oracle VM Server for SPARC 3.0 관리 설명서**의 "XML 전송"를 참조하십시오.
  - UDP 포트 `161`의 SNMP(Simple Network Management Protocol)

    Oracle VM Server for SPARC MIB(Management Information Base)를 사용하여 도메인을 관찰할지 여부를 확인합니다. 이 기능을 사용하려면 SNMP 서비스를 사용으로 설정해야 합니다. 선택 사항에 따라 다음 중 하나를 수행합니다.
    - **SNMP 서비스가 Oracle VM Server for SPARC MIB를 사용하도록 설정합니다.** Oracle VM Server for SPARC MIB를 안전하게 설치합니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "Oracle VM Server for SPARC MIB 소프트웨어 패키지를 설치하는 방법" 및 **Oracle VM Server for SPARC 3.0 관리 설명서**의 "보안 관리"를 참조하십시오.
    - **SNMP 서비스를 사용 안함으로 설정합니다.** 이 서비스를 사용 안함으로 설정하려면 **Oracle VM Server for SPARC 3.0 관리 설명서**의 "Oracle VM Server for SPARC MIB 소프트웨어 패키지를 제거하는 방법"를 참조하십시오.
  - 멀티캐스트 주소 `239.129.9.27` 및 `64535` 포트의 검색 서비스

    Logical Domains Manager 데몬 `ldmd`가 실행 중인 동안에는 이 서비스를 사용 안함으로 설정할 수 **없습니다**. 대신 Oracle Solaris의 IP 필터 기능을 사용하여 이 서비스에 대한 액세스를 차단합니다. 그러면 Logical Domains Manager의 공격 영역이 최소화됩니다. 액세스를 차단하면 유틸리티를 무단으로 사용할 수 없게 되어 결과적으로 서비스 거부 공격과 이러한 네트워크 서비스를 잘못 사용하려는 시도를 방어할 수 있습니다. **Oracle Solaris Administration: IP Services**의 20 장, "IP Filter in Oracle Solaris (Overview)" 및 **Oracle Solaris Administration: IP Services**의 "Using IP Filter Rule Sets"를 참조하십시오.

또한 **Secure Deployment of Oracle VM Server for SPARC**에서 "Counter Measure #14: Securing the ILOM" 및 "Counter Measure #20: Hardening LDoms Manager"도 참조하십시오.

- **작업을 수행할 수 있는 최소한의 권한을 제공합니다.**
  - 같은 보안 요구 사항과 권한을 공유하는 개별 게스트 시스템의 그룹인 **보안 클래스**에 시스템을 격리합니다. 단일 보안 클래스의 게스트 도메인만 단일 하드웨어 플랫폼에 지정하면 격리 위반이 발생하여 도메인이 다른 보안 클래스에 접근할 수 없게 됩니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Counter Measure #2: Carefully Assigning Guests to Hardware Platforms"를 참조하십시오.
  - RBAC를 사용하여 `ldm` 명령으로 도메인 관리 기능을 제한합니다. 도메인을 관리해야 하는 사용자**에게만** 이 기능이 제공됩니다. 모든 `ldm` 하위 명령에 액세스해야 하는 사용자에게는 LDoms 관리 권한 프로파일을 사용하는 역할을 지정합니다. 목록 관련 `ldm` 하위 명령에만 액세스해야 하는 사용자에게는 LDoms 검토 권한 프로파일을 사용하는 역할을 지정합니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "권한 프로파일 및 역할 사용"를 참조하십시오.
  - RBAC를 사용하여 Oracle VM Server for SPARC의 관리자가 액세스해야 하는 도메인의 콘솔**로만** 액세스를 제한합니다. 모든 도메인에 대한 일반 액세스는 허용하지 **마십시오**. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "권한 프로파일 및 역할 사용"를 참조하십시오.
- **시스템 작업을 모니터링합니다.**

  Oracle VM Server for SPARC 감사를 사용으로 설정합니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "감사를 사용으로 설정한 후 사용"를 참조하십시오.

보안 방식으로 Oracle VM Server for SPARC 소프트웨어를 배포하는 작업에 대한 권장 사항은 **Secure Deployment of Oracle VM Server for SPARC**에서 "Recommended Deployment Options"를 참조하십시오.

◆ ◆ ◆ 2 장

2 Oracle VM Server for SPARC 보안 설치 및 구성

이 장에서는 Oracle VM Server for SPARC 설치 및 구성과 관련된 보안 고려 사항에 대해 설명합니다.

설치

Oracle VM Server for SPARC 소프트웨어는 자동으로 Oracle Solaris 10 또는 Oracle Solaris 11 패키지로 안전하게 설치됩니다. 설치가 완료되면 관리자 권한이 있어야 RBAC(역할 기반 액세스 제어), 감사 및 권한 부여를 사용하여 도메인을 구성할 수 있습니다. 이러한 기능은 기본적으로 사용으로 설정되어 있지 않습니다.

설치 후 구성

리소스 사용을 최대화하려면 Oracle VM Server for SPARC 소프트웨어를 설치한 후 다음 작업을 수행하십시오.

- 필요한 가상 I/O 서비스(예: 가상 스위치, 가상 디스크 서버 및 가상 콘솔 집중기 서비스)로 컨트롤 도메인을 구성합니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 4 장, "서비스 및 컨트롤 도메인 설정"를 참조하십시오.
- 게스트 도메인을 구성합니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 5 장, "게스트 도메인 설정"를 참조하십시오.

  가상 스위치를 사용하여 관리 네트워크 및 프로덕션 네트워크를 통해 게스트 도메인을 구성할 수 있습니다. 이 경우 프로덕션 네트워크 인터페이스를 가상 스위치 네트워크 장치로 사용하면 가상 스위치가 생성됩니다. **Secure Deployment of Oracle VM Server for SPARC**에서 "Counter Measure #13: Dedicated Management Network"를 참조하십시오.

  가상 디스크가 손상되면 게스트 도메인의 보안도 손상됩니다. 따라서 가상 디스크(네트워크 연결 저장소, 로컬에 저장된 디스크 이미지 파일 또는 물리적 디스크)는 안전한 위치에 저장해야 합니다.

vntsd 데몬은 기본적으로 사용 안함으로 설정되어 있습니다. 이 데몬이 사용으로 설정되면 컨트롤 도메인에 로그인한 사용자가 게스트 도메인의 콘솔에 연결할 수 있습니다. 이 유형의 액세스를 방지하려면 vntsd 데몬이 사용 안함으로 설정되었는지 확인하거나, RBAC를 사용하여 콘솔 연결 액세스를 **오직** 허용된 사용자로 제한하십시오.

- SP(서비스 프로세서)는 기본적으로 안전하게 구성됩니다. ILOM(Integrated Lights Out Management) 소프트웨어를 사용하여 SP를 관리하는 방법은 http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html에서 사용 중인 플랫폼용 설명서를 참조하십시오.

◆ ◆ ◆ 3 장

3 Oracle VM Server for SPARC 보안 기능

이 장에서는 Oracle VM Server for SPARC 소프트웨어에서 사용하는 보안 기능의 개요에 대해 다룹니다.

인증, 액세스 제어 및 감사에 대한 자세한 내용은 **Oracle VM Server for SPARC 3.0 관리 설명서**의 3 장, "Oracle VM Server for SPARC 보안"를 참조하십시오.

보안 모델

Oracle VM Server for SPARC 소프트웨어는 Oracle Solaris OS에 내장된 보안 모델과 기능을 기반으로 합니다. Oracle Solaris OS 보안 지침은 **Oracle Solaris 11 Security Guidelines** 및 **Oracle Solaris 10 Security Guidelines**를 참조하십시오.

인증 구성 및 사용

베어 메탈 Oracle Solaris 설치와 마찬가지로, 계정이 있는 사용자라면 논리적 도메인, 컨트롤 도메인에 로그인할 수 있습니다. Oracle VM Server for SPARC 소프트웨어는 사용자 계정을 만들지 않습니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "Logical Domains Manager 설치"를 참조하십시오. Oracle Solaris 사용자 보안 방법은 **Oracle Solaris 11 Security Guidelines**의 "Securing Users"를 참조하십시오.

Logical Domains Manager를 사용하여 컨트롤 도메인에서 도메인 관리 작업을 수행하려면 구성 데이터를 읽고 쓸 수 있는 특수 권한을 사용자에게 부여해야 합니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "Logical Domains Manager 프로파일 컨텐츠" 및 **Oracle VM Server for SPARC 3.0 관리 설명서**의 "권한 프로파일 및 역할 사용"을 참조하십시오.

RBAC 구성 및 사용

Oracle Solaris OS의 RBAC(역할 기반 액세스 제어) 기능을 사용하여 권한 부여 및 권한 프로파일을 관리하고 역할을 사용자 계정에 지정할 수 있습니다. RBAC에 대한 자세한 내용은 **System Administration Guide: Security Services**의 9 장, "Using Role-Based Access Control (Tasks)"를 참조하십시오.

Logical Domains Manager를 설치하면 필요한 권한 부여 및 권한 프로파일이 로컬 파일에 추가됩니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 "권한 프로파일 및 역할 사용"를 참조하십시오.

이름 지정 서비스에서 사용자, 권한 부여, 권한 프로파일 및 역할을 구성하려면 **System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)**를 참조하십시오.

감사 구성 및 사용

베어 메탈 시스템에서 실행 중인 Oracle Solaris OS의 경우와 동일하게 게스트 도메인에서 Oracle Solaris 인스턴스를 관리 및 감사해야 합니다. 사용 환경에 중요한 기능과 시스템 서비스만 감사하도록 Oracle Solaris OS 감사 기능을 사용자 정의할 수 있습니다. Oracle VM Server for SPARC의 경우, 가상화 소프트웨어 클래스를 감사해야 합니다. 기타 감사 관련 작업도 수행할 수 있습니다. **Oracle Solaris 11 Security Guidelines**의 "Using the Audit Service" 및 **Oracle Solaris 11 Security Guidelines**의 "How to Audit Significant Events in Addition to Login/Logout"를 참조하십시오.

Logical Domains Manager는 감사 이벤트를 만들어 저장 후 나중에 검사할 수 있도록 이 이벤트를 Oracle Solaris 감사 부속 시스템에 전달합니다. 내역은 수행된 작업, 수행 시기 및 수행자 및 영향을 받는 대상에 대한 로그에 보존됩니다. 컨트롤 도메인에서는 시스템의 모든 도메인에 대한 감사 정보를 볼 수 **없습니다**.

따라서 시스템의 각 도메인에 대해 다음과 같이 시스템에서 실행되는 Oracle Solaris OS의 버전에 따라 감사 기능을 사용 및 사용 안함으로 설정할 수 있습니다.

- **Oracle Solaris 10 OS.** `bsmconv` 및 `bsmunconv` 명령을 사용합니다. `bsmconv(1M)` 및 `bsmunconv(1M)` 매뉴얼 페이지와 **System Administration Guide: Security Services**의 Oracle Solaris 10 버전을 참조하십시오.
- **Oracle Solaris 11 OS.** `audit` 명령을 사용합니다. `audit(1M)` 매뉴얼 페이지 및 **System Administration Guide: Security Services**의 Oracle Solaris 11 버전을 참조하십시오.

자세한 내용은 **Oracle VM Server for SPARC 3.0 관리 설명서**의 "감사를 사용으로 설정한 후 사용"를 참조하십시오.

기타 보안 기능 구성 및 사용

Oracle VM Server for SPARC는 특정 가상화 기능 사용에 보안을 설정합니다. 사용으로 설정된 경우 `vntsd` 데몬이 기본적으로 가장 안전한 구성에 구성됩니다. 네트워크를 통해서가 **아니라** 컨트롤 도메인을 통해서만 연결이 허용됩니다. 필요한 경우 덜 안전한 옵션을 구성하여 네트워크 연결을 허용할 수 있습니다. `vntsd(1M)` 매뉴얼 페이지에서 `vntsd/listen_addr` 등록 정보에 대한 설명을 참조하십시오.

`vntsd`를 사용하여 네트워크 연결을 허용할 경우 주의하십시오. 최적의 보안을 위해 컨트롤 도메인의 연결만 허용하거나 `vntsd`를 사용 안함으로 설정하는 것이 가장 좋습니다. 13 페이지 “Oracle VM Server for SPARC에 일반 보안 원칙 적용”을 참조하십시오.

Oracle VM Server for SPARC 도메인 마이그레이션 기능은 보안 수단을 사용합니다. 소스 시스템의 Logical Domains Manager는 도메인 마이그레이션 요청을 수락하고 대상 시스템에서 실행되는 Logical Domains Manager에 대한 보안 네트워크 연결을 설정합니다. 마이그레이션은 이 연결이 설정된 후 발생합니다. 이러한 보안 연결은 인증 및 암호화 기능을 사용하여 생성됩니다. **Oracle VM Server for SPARC 3.0 관리 설명서**의 “마이그레이션 작업 보안”를 참조하십시오.

특히, 도메인 마이그레이션 작업은 기본적으로 SSL(Secure Sockets Layer)을 사용하여 네트워크를 통해 보내고 받는 모든 트래픽을 암호화합니다. 암호화 장치를 지원하는 시스템의 컨트롤 도메인에 암호화 장치를 지정하면 마이그레이션 성능이 향상됩니다.

도메인 마이그레이션이 필요하지 않은 경우 `ldmd` 프로세스가 마이그레이션 포트에서 수신되지 않도록 마이그레이션 기능을 사용 안함으로 설정할 수 있습니다.

도메인 마이그레이션을 사용하는 경우 `ldmd` 데몬이 마이그레이션 중 암호 인증을 요구하도록 구성되었는지 확인하십시오. 이 옵션이 기본 동작입니다.

◆ ◆ ◆ 4 장

4 개발자를 위한 보안 고려 사항

이 장은 Oracle VM Server for SPARC 소프트웨어용 응용 프로그램을 생성하는 개발자에게 유용한 정보를 제공합니다.

Oracle VM Server for SPARC XML 인터페이스

XML(확장성 마크업 언어) 통신 방식을 통해 Oracle VM Server for SPARC 소프트웨어와 연결되는 외부 프로그램을 만들 수 있는데, 이 프로그램은 XMPP(확장성 메시징 및 프레즌스 프로토콜)를 사용합니다.

공격자들은 이 네트워크 프로토콜을 악용하여 시스템에 액세스할 수 있으므로, XMPP를 사용 안함으로 설정하십시오. XMPP를 사용 안함으로 설정하는 방법은 **Oracle VM Server for SPARC 3.0 관리 설명서**의 "XML 전송"를 참조하십시오. Logical Domains Manager가 사용하는 보안 방식에 대한 자세한 내용은 **Oracle VM Server for SPARC 3.0 관리 설명서**의 "XMPP 서버"를 참조하십시오.

XMPP를 사용 안함으로 설정하면 도메인 마이그레이션, 메모리 동적 재구성, `ldm init-system` 명령과 같은 주요 Oracle VM Server for SPARC 기능을 사용할 수 없습니다.

◆ ◆ ◆ 부 록 A

보안 배포 점검 목록

이 점검 목록은 Oracle VM Server for SPARC 환경을 강화하기 위해 수행할 수 있는 단계를 요약하여 보여줍니다. 자세한 내용은 다음과 같은 다른 문서에서 다룹니다.

- **Oracle VM Server for SPARC 3.0 관리 설명서**
- **Oracle Solaris 10 Security Guidelines**
- **Oracle Solaris 11 Security Guidelines**
- **Secure Deployment of Oracle VM Server for SPARC**

Oracle VM Server for SPARC 보안 점검 목록

- ❒ 가상화되지 않은 환경에서처럼 게스트 도메인에 대해 Oracle Solaris 강화 단계를 수행합니다.
- ❒ LDoms 관리 및 LDoms 검토 권한 프로파일을 사용하여 적합한 권한을 사용자에게 위임합니다.
- ❒ RBAC(역할 기반 액세스 제어)를 사용하여 Oracle VM Server for SPARC의 관리자가 액세스해야 하는 도메인의 콘솔**로만** 액세스를 제한합니다.
- ❒ Oracle VM Server for SPARC에 대한 Oracle Solaris OS 감사 기능을 사용으로 설정합니다.
- ❒ 불필요한 도메인 관리 서비스를 사용 안함으로 설정합니다.
- ❒ 같은 보안 클래스의 게스트 시스템은 한 물리적 플랫폼에만 배포합니다.
- ❒ 실행 환경 관리와 게스트 도메인 간 네트워크 연결이 없는지 확인합니다.
- ❒ 필요한 리소스만 게스트 시스템에 지정합니다.