Oracle® VM Server for SPARC 3.4 보안 설명서

부품 번호: **E71815**
2016년 5월

ORACLE

부품 번호: E71815

Copyright © 2007, 2016, 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=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

이 설명서 사용

- **개요** – Oracle VM Server for SPARC 3.4 소프트웨어를 안전한 방식으로 사용하는 방법에 대해 설명합니다.
- **대상** – 가상화된 SPARC 서버의 보안을 관리하는 시스템 관리자를 대상으로 합니다.
- **필요한 지식** – 이러한 서버의 시스템 관리자는 UNIX 시스템 및 Oracle Solaris OS (Oracle Solaris 운영 체제)를 사용할 수 있는 실제적인 지식을 보유하고 있어야 합니다.

제품 설명서 라이브러리

이 제품과 관련 제품들에 대한 설명서 및 리소스는 http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html에서 사용할 수 있습니다.

피드백

http://www.oracle.com/goto/docfeedback에서 이 설명서에 대한 피드백을 보낼 수 있습니다.

♦ ♦ ♦ 1 장

1 Oracle VM Server for SPARC 보안 개요

이 문서에 있는 보안 권장 사항의 수로 인해 인식이 바뀔 수도 있지만 일반적인 Oracle VM Server for SPARC 설치는 이미 허용되지 않은 사용에 대한 높은 보안을 제공합니다. 악용의 가능성은 낮지만 소규모 공격의 여지가 존재하고 어느 정도의 위험은 남아 있습니다. 대문의 자물쇠와 같은 일반적인 보호 장치를 보완하기 위해 주거 침입 경보 장치를 추가하는 것과 마찬가지로 추가적인 네트워크 보안 방법은 예상치 못한 문제 발생 가능성을 줄이고 잠재적인 피해를 최소화하는 데 도움이 될 수 있습니다.

이 장에서는 다음 Oracle VM Server for SPARC 보안 항목을 다룹니다.

Oracle VM Server for SPARC에서 사용하는 보안 기능

Oracle VM Server for SPARC 소프트웨어는 각각에 Oracle Solaris 10 또는 Oracle Solaris 11 OS가 설치된 여러 Oracle Solaris VM(가상 시스템)이 하나의 물리적 시스템에서 실행될 수 있도록 하는 가상화 제품입니다. 각 VM은 논리적 도메인이라고도 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.

`ldm` 명령은 Logical Domains Manager를 호출하며, 도메인을 구성하고 상태 정보를 검색하려면 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 Solaris 권한과 같은 Oracle VM Server for SPARC 보안 기능을 사용하십시오. *Oracle VM Server for SPARC 3.4* 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 보안 강화에 대한 자세한 내용은 "가상화 환경의 보안" [14] 및 "공격 방어" [15]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 제한하는 방법에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4* 관리 설명서 의 2 장, "Oracle VM Server for SPARC 보안"을 참조하십시오.

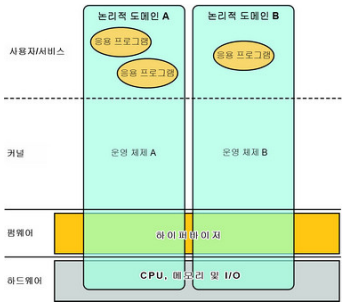
Oracle VM Server for SPARC 제품 개요

Oracle VM Server for SPARC는 Oracle의 SPARC T-Series 서버, SPARC M5 서버 및 Fujitsu M10 서버에 매우 효율적인 엔터프라이즈급 가상화 기능을 제공합니다. Oracle VM Server for SPARC 소프트웨어를 사용하여 단일 시스템에 논리적 도메인이라는 가상 서버를 많이 만들 수 있습니다. 이러한 종류의 구성을 통해 SPARC 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 3.4* 관리 설명서 및 *Oracle VM Server for SPARC 3.4 Reference Manual*를 참조하십시오. 필요한 하드웨어 및 소프트웨어에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4* 설치 설명서를 참조하십시오.

그림 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.

  시스템 컨트롤러*(SC)*라고도 하는 서비스 프로세서*(SP)*는 물리적 시스템을 모니터링하고 실행합니다. 논리적 도메인은 SP가 아닌 Logical Domains Manager에서 관리합니다.
- **컨트롤 도메인**: Logical Domains Manager는 이 도메인에서 실행되고 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) 컨트롤러에 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 3.4* 관리 설명서 의 “PCIe 끝점 장치를 지정하여 I/O 도메인 만들기”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 해당 루트 컴플렉스의 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 SPARC T4-4 서버를 사용하는 경우 루트 도메인을 4개까지 지정할 수 있습니다.
- **게스트 도메인**: 게스트 도메인은 하나 이상의 서비스 도메인에서 제공하는 가상 장치 서비스를 이용하는 비I/O 도메인으로, 물리적 I/O 장치가 없습니다. 가상 디스크 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 요인은 전체적인 Oracle VM Server for SPARC 구성의 보안 레벨에 기여합니다. 안전한 방식으로 Oracle VM Server for SPARC 소프트웨어 배포를 위한 권장 사항은 “가상화 환경의 보안” [14] 및 “공격 방어” [15]를 참조하십시오.

다음 중 몇 가지 일반적인 보안 원칙을 적용할 수 있습니다.

- **공격 영역을 최소화합니다.**
  - 시스템의 보안을 정기적으로 평가할 수 있는 운영 지침을 마련하여 의도하지 않은 구성 오류를 최소화합니다. “대처 방법: 운영 기준 만들기” [17]를 참조하십시오.
  - 도메인 격리를 최대화하도록 가상 환경의 아키텍처를 신중하게 계획합니다. “위협: 가상 환경 아키텍처의 오류” [18]에 대해 설명된 대처 방법을 참조하십시오.
  - 지정할 리소스 및 리소스의 공유 여부를 신중하게 계획합니다. “대처 방법: 하드웨어 리소스를 주의하여 지정” [20] 및 “대처 방법: 공유 리소스를 주의하여 지정” [20]을 참조하십시오.
  - “위협: 실행 환경의 조작” [21] 및 “대처 방법: 게스트 도메인 OS 보안” [32]에 대해 설명된 대처 방법을 적용하여 조작으로부터 논리적 도메인을 보호합니다.
    - “대처 방법: 대화식 액세스 경로 보안” [21].
    - “대처 방법: Oracle Solaris OS 최소화” [22].
    - “대처 방법: Oracle Solaris OS 강화” [22].
    - “대처 방법: Logical Domains Manager 강화” [27].

    - "대처 방법: 역할 구분 및 응용 프로그램 격리 사용" [22]에서는 다양한 도메인에 기능 역할 지정 및 컨트롤 도메인에서 게스트 도메인을 호스트하는 데 필요한 기반 구조를 제공하는 소프트웨어 실행의 중요성을 설명합니다. 이 목적으로 설계된 게스트 도메인에서 다른 시스템에 의해 실행될 수 있는 응용 프로그램을 실행해야 합니다.
    - "대처 방법: 전용 관리 네트워크 구성" [22]에서는 SP가 있는 서버를 전용 관리 네트워크에 연결하여 네트워크 액세스로부터 SP를 보호하는 고급 네트워크 구성에 대해 설명합니다.
- 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.
- "대처 방법: 펌웨어 및 소프트웨어 서명 검증" [25] 및 "대처 방법: 커널 모듈 검증" [25]에서 설명한 대로 하이퍼바이저의 코어를 보호합니다.
- 서비스 거부 공격에 대비하여 컨트롤 도메인을 보호합니다. "대처 방법: 콘솔 액세스 보안" [26]를 참조하십시오.
- 권한이 없는 사용자가 Logical Domains Manager를 실행하지 못하도록 합니다. "위협: 구성 유틸리티의 허용되지 않은 사용" [27]을 참조하십시오.
- 권한이 없는 사용자나 프로세스가 서비스 도메인에 액세스하지 못하도록 합니다. "위협: 서비스 도메인의 조작" [29]을 참조하십시오.
- 서비스 거부 공격에 대비하여 I/O 도메인 또는 서비스 도메인을 보호합니다. "위협: I/O 도메인 또는 서비스 도메인의 서비스 거부 경험" [30]을 참조하십시오.
- 권한이 없는 사용자나 프로세스가 I/O 도메인에 액세스하지 못하도록 합니다. "위협: I/O 도메인의 조작" [31]을 참조하십시오.
- 불필요한 도메인 관리 서비스를 사용 안함으로 설정합니다. Logical Domains Manager는 도메인 액세스, 모니터링 및 마이그레이션을 위한 네트워크 서비스를 제공합니다. "대처 방법: Logical Domains Manager 강화" [27] 및 "대처 방법: Oracle ILOM 보안" [24]을 참조하십시오.
- **작업을 수행할 수 있는 최소한의 권한을 제공합니다.**
    - 같은 보안 요구 사항과 권한을 공유하는 개별 게스트 시스템의 그룹인 보안 클래스에 시스템을 격리합니다. 단일 보안 클래스의 게스트 도메인만 단일 하드웨어 플랫폼에 지정하면 격리 장벽을 만들어 도메인이 다른 보안 클래스에 접근할 수 없게 됩니다. "대처 방법: 게스트를 하드웨어 플랫폼에 주의하여 지정" [18]을 참조하십시오.
    - 권한을 사용하여 `ldm` 명령으로 도메인 관리 기능을 제한합니다. 도메인을 관리해야 하는 사용자에게만 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 3.4* 관리 설명서 의 "권한 프로파일 및 역할 사용"를 참조하십시오.

- 권한을 사용하여 Oracle VM Server for SPARC의 관리자가 관리하는 도메인의 콘솔로만 액세스를 제한합니다. 모든 도메인에 대한 일반 액세스는 허용하지 마십시오. *Oracle VM Server for SPARC 3.4* 관리 설명서 의 "권한을 사용하여 도메인 콘솔에 대한 액세스 제어"를 참조하십시오.

가상화 환경의 보안

Oracle VM Server for SPARC 가상화 환경을 효율적으로 보호하려면 각 도메인에서 실행되는 운영 체제 및 각 서비스를 보호합니다. 침입으로 인한 영향을 줄이려면 서비스를 서로 다른 도메인에 배포하여 격리합니다.

Oracle VM Server for SPARC 환경에서는 하이퍼바이저를 사용하여 논리적 도메인에 대한 CPU, 메모리 및 I/O 리소스를 가상화합니다. 각 도메인은 잠재적인 공격으로부터 보호해야 하는 독립적인 가상화 서버입니다.

가상화 환경에서는 하드웨어 리소스 공유를 통해 여러 서버를 하나의 서버로 통합할 수 있습니다. Oracle VM Server for SPARC에서 CPU 및 메모리 리소스는 각 도메인에 배타적으로 할당되어 과도한 CPU 사용이나 메모리 할당을 통한 남용을 막습니다. 디스크 및 네트워크 리소스는 대개 서비스 도메인에서 여러 게스트 도메인으로 제공됩니다.

보안을 평가할 때는 항상 환경에 공격자가 악용할 수 있는 결함이 있다고 가정하십시오. 예를 들어, 공격자는 하이퍼바이저의 약점을 악용하여 게스트 도메인을 포함한 전체 시스템을 가로챌 수 있습니다. 따라서 항상 침입에 대비하여 피해 위험을 최소화하도록 시스템을 배포하십시오.

실행 환경

실행 환경에는 다음 구성 요소가 포함됩니다.

- **하이퍼바이저 –** 하드웨어를 가상화하고 CPU에 내장된 하드웨어 지원에 크게 의존하는 플랫폼별 펌웨어입니다.
- **컨트롤 도메인 –** 하이퍼바이저를 구성하고, 논리적 도메인을 관리하는 Logical Domains Manager를 실행하는 특수 도메인입니다.
- **I/O 도메인 또는 루트 도메인 –** 플랫폼의 사용 가능한 I/O 장치를 일부 또는 전부 소유하고 다른 도메인과 공유하는 도메인입니다.
- **서비스 도메인 –** 서비스를 다른 도메인에 제공하는 도메인입니다. 서비스 도메인은 다른 도메인에 콘솔 액세스를 제공하거나 가상 디스크를 제공할 수 있습니다. 다른 도메인에 가상 디스크 액세스를 제공하는 서비스 도메인도 I/O 도메인입니다.

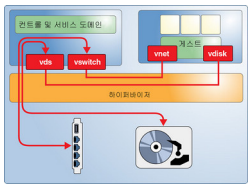
이러한 구성 요소에 대한 자세한 내용은 그림 1 및 자세한 구성 요소 설명을 참조하십시오.

보조 I/O 도메인을 구성하여 중복 I/O 구성에 대한 서비스 제공 능력을 높일 수 있습니다. 또한 보조 I/O 도메인을 사용하여 보안 침입으로부터 하드웨어를 격리할 수 있습니다. 구성 옵션에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4 관리 설명서*를 참조하십시오.

실행 환경 보안

Oracle VM Server for SPARC에는 실행 환경에서 여러 공격 대상이 있습니다. 그림 2는 컨트롤 도메인이 게스트 도메인에 네트워크 및 디스크 서비스를 제공하는 단순한 Oracle VM Server for SPARC 구성을 보여줍니다. 이러한 서비스는 컨트롤 도메인에서 실행되는 데몬 및 커널 모듈로 구현됩니다. Logical Domains Manager는 각 서비스 및 클라이언트에 대해 논리적 도메인 채널(LDC)을 지정하여 지점간 통신을 구현합니다. 공격자는 구성 요소 중에 있는 오류를 악용하여 게스트 도메인의 격리를 무력화할 수 있습니다. 예를 들어, 공격자는 서비스 도메인에서 임의의 코드를 실행하거나 플랫폼에서 정상적인 작업을 방해할 수 있습니다.

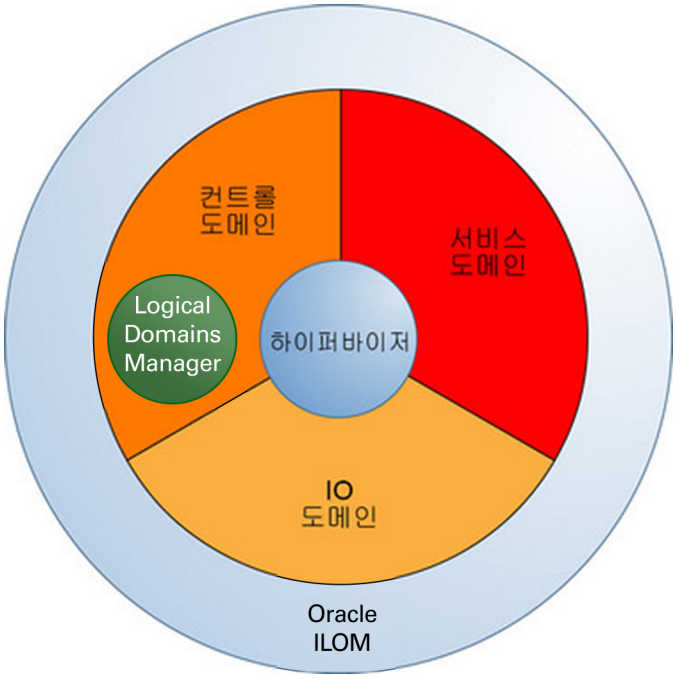
그림 **2** Oracle VM Server for SPARC 환경의 예



공격 방어

다음 그림은 Oracle VM Server for SPARC “실행 환경”을 구성하는 가상 구성 요소를 나타냅니다. 이러한 구성 요소는 엄격하게 구분되지 않았습니다. 가장 단순한 구성은 이러한 모든 기능을 단일 도메인에서 결합하는 것입니다. 컨트롤 도메인은 다른 도메인에 대한 I/O 도메인 및 서비스 도메인의 역할을 수행할 수도 있습니다.

그림 3 실행 환경의 구성 요소



공격자가 시스템 격리를 무효화한 다음 실행 환경의 하이퍼바이저나 다른 구성 요소를 조작하여 게스트 도메인에 접근을 시도한다고 가정해 보겠습니다. 독립형 서버와 마찬가지로 각 게스트 도메인을 보호해야 합니다.

이 장의 나머지 부분에서는 위협 가능성 및 이러한 위협에 대처할 수 있는 다양한 방법을 소개합니다. 이러한 각 공격에서는 단일 플랫폼에서 실행되는 여러 도메인의 격리를 무효화하거나 제거하려고 시도합니다. 다음 절에서는 Oracle VM Server for SPARC 시스템의 각 부분에 대한 위협을 설명합니다.

- “운영 환경” [17]
- “실행 환경” [21]
- “Oracle ILOM” [23]
- “하이퍼바이저” [24]
- “컨트롤 도메인” [26]
- “Logical Domains Manager” [26]
- “I/O 도메인” [30]
- “서비스 도메인” [28]

- “게스트 도메인” [32]

운영 환경

운영 환경에는 물리적 시스템과 해당 구성 요소, 데이터 센터 설계자, 관리자 및 IT 조직의 구성원이 포함됩니다. 보안 침입은 운영 환경의 어느 지점에서나 발생할 수 있습니다.

가상화는 실제 하드웨어와 운용 서비스를 실행하는 게스트 도메인 사이에 소프트웨어 층을 두며, 이 구조는 점점 더 복잡해지고 있습니다. 따라서 가상 시스템을 주의 깊게 계획하고 구성해야 하며, 사람의 실수 가능성을 염두에 두어야 합니다. 또한 “소셜 엔지니어링”을 사용하여 운영 환경에 액세스하려는 공격자의 시도를 유의해야 합니다.

다음 절에서는 운영 환경 레벨에서 대처할 수 있는 고유한 위협을 설명합니다.

위협: 의도하지 않은 잘못된 구성

가상화 환경에 대한 기본적인 보안 고려 사항은 네트워크 세그먼트를 구분하고, 관리 액세스 권한을 차별화하며, 서버를 보안 클래스(동일한 보안 요구 사항 및 권한을 가지는 도메인 그룹)에 배포하여 서버 격리를 유지하는 것입니다.

다음 오류를 피하도록 가상 리소스를 세심하게 구성하십시오.

- 운용 게스트 도메인과 실행 환경 사이에 불필요한 통신 채널 만들기
- 네트워크 세그먼트에 대한 불필요한 액세스 권한 만들기
- 각 보안 클래스 사이에 의도하지 않은 연결 만들기
- 의도하지 않게 게스트 도메인을 잘못된 보안 클래스로 마이그레이션
- 예상치 않은 리소스 오버로드로 이어질 수 있는 불충분한 하드웨어 할당
- 디스크나 I/O 장치를 잘못된 도메인에 지정

대처 방법: 운영 기준 만들기

시작하기 전에 Oracle VM Server for SPARC 환경에 대한 운영 기준을 주의 깊게 정의하십시오. 이러한 기준에서는 수행할 다음 작업 및 수행 방법을 설명합니다.

- 환경의 모든 구성 요소에 대한 패치 관리
- 잘 정의되고 추적 가능한 변경 사항의 안전한 구현 사용
- 정기적으로 로그 파일 확인
- 환경의 무결성 및 가용성 모니터링

이러한 기준이 최신이고 충분하며, 일상 작업에서 이러한 기준을 따르고 있는지 정기적으로 확인합니다.

이러한 기준 이외에도 여러 가지 더욱 기술적인 방법을 사용하여 의도하지 않은 작업의 위험을 줄일 수 있습니다. “Logical Domains Manager” [26]를 참조하십시오.

위협: 가상 환경 아키텍처의 오류

물리적 시스템을 가상화 환경으로 이동하는 경우 대개 원래 LUN을 재사용하여 저장소 구성을 그대로 유지할 수 있습니다. 하지만 네트워크 구성은 가상화 환경에 맞추어야 하므로 결과적인 아키텍처는 물리적 시스템에서 사용된 아키텍처와 상당히 다를 수 있습니다.

각 보안 클래스의 격리 유지 방법 및 필요성을 고려해야 합니다. 또한 네트워크 스위치 및 SAN 스위치와 같은 플랫폼의 공유 하드웨어 및 공유 구성 요소를 고려합니다.

환경에 대한 보안을 극대화하기 위해서는 게스트 도메인과 보안 클래스의 격리를 유지해야 합니다. 아키텍처를 설계할 때 가능한 오류 및 공격을 예측하고 방어망을 구현합니다. 좋은 설계는 복잡성과 비용을 관리하면서 잠재적인 보안 문제를 파악하는 데 도움을 줍니다.

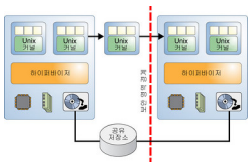
대처 방법: 게스트를 하드웨어 플랫폼에 주의하여 지정

동일한 보안 요구 사항과 권한을 가지는 도메인 그룹인 보안 클래스를 사용하여 개별 도메인을 서로 격리합니다. 동일한 보안 클래스에 있는 게스트 도메인을 특정 하드웨어 플랫폼에 지정하면 격리 무효화가 발생하더라도 다른 보안 클래스로 공격이 넘어오는 것을 막을 수 있습니다.

대처 방법: Oracle VM Server for SPARC 도메인 마이그레이션 계획

실시간 도메인 마이그레이션 기능은 다음 그림에 나온 대로 게스트 도메인이 다른 보안 클래스에 지정된 플랫폼으로 잘못 마이그레이션될 경우 격리 무효화를 유발할 수 있습니다. 따라서 보안 클래스 경계 사이에는 마이그레이션이 허용되지 않도록 게스트 도메인 마이그레이션을 주의해서 계획하십시오.

그림 **4** 보안 경계 사이의 도메인 마이그레이션



마이그레이션 작업 중에 노출되는 보안 취약성을 최소화하거나 없애려면 각 소스 시스템 및 대상 시스템 쌍 사이에서 `ldmd`로 생성한 호스트 인증서 아웃오브밴드를 수동으로 교환하고 설치

해야 합니다. SSL 인증서 설치 방법에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4* 관리 설명서 의 “마이그레이션용 SSL 인증서 구성”을 참조하십시오.

대처 방법: 올바른 가상 연결 구성

모든 가상 네트워크 연결 추적을 잃으면 도메인이 네트워크 세그먼트에 대한 잘못된 액세스 권한을 얻을 수 있습니다. 예를 들어, 이러한 액세스 권한은 방화벽이나 보안 클래스를 우회할 수 있습니다.

구현 오류의 위험을 줄이려면 환경의 모든 가상 및 물리적 연결을 주의 깊게 계획하고 문서화하십시오. 도메인 연결 계획은 단순성과 관리 용이성으로 최적화하십시오. 계획을 명확하게 문서화하고 운용으로 들어가기 전에 계획에 대해 구현의 정확성을 확인하십시오. 가상 환경이 운용 중인 상태 이후에도 정기적으로 계획에 대해 구현을 확인하십시오.

대처 방법: VLAN 태그 지정 사용

VLAN 태그 지정을 사용하여 여러 이더넷 세그먼트를 단일 물리적 네트워크로 통합할 수 있습니다. 이 기능은 가상 스위치에 대해서도 사용할 수 있습니다. 가상 스위치의 구현에서 소프트웨어 오류와 관련된 위험을 완화하려면 물리적 NIC 및 VLAN당 하나의 가상 스위치를 구성합니다. 이더넷 드라이버의 오류에 대해 추가적으로 보호하려면 태그 지정된 VLAN 사용을 피합니다. 하지만 이 태그 지정된 VLAN 취약점은 잘 알려져 있으므로 이러한 오류의 가능성은 낮습니다. Oracle VM Server for SPARC 소프트웨어를 사용하는 Oracle의 Sun SPARC T-Series 서버에 대한 침입 테스트에서는 이 취약점이 나타나지 않았습니다.

대처 방법: 가상 보안 장치 사용

패킷 필터 및 방화벽과 같은 보안 장치는 격리 수단이며 보안 클래스의 격리를 보호합니다. 이러한 장치는 다른 게스트 도메인과 마찬가지로 동일한 위협에 노출되므로 이를 사용한다고 해서 격리 무효화로부터 완전한 보호가 보장되는 것은 아닙니다. 따라서 이러한 서비스의 가상화를 결정하기 전에 위험 및 보안의 모든 측면을 주의 깊게 고려하십시오.

위협: 리소스 공유의 부작용

가상화 환경에서 리소스 공유는 다른 구성 요소(다른 도메인 등)에 악영향을 줄 때까지 리소스를 오버로드하는 서비스 거부(DoS) 공격으로 이어질 수 있습니다.

Oracle VM Server for SPARC 환경에서는 일부 리소스만 DoS 공격의 영향을 받을 수 있습니다. CPU 및 메모리 리소스는 각 게스트 도메인에 배타적으로 지정되어 대부분의 DoS 공격을 막을 수 있습니다. 이러한 리소스의 배타적 지정에서도 다음 방법으로 게스트 도메인의 성능을 저하시킬 수 있습니다.

- 스트랜드 사이에 공유되고 두 게스트 도메인에 지정된 캐시 영역 스래싱

- 메모리 대역폭 오버로드

CPU 및 메모리 리소스와 달리 디스크 및 네트워크 서비스는 대개 게스트 도메인 사이에 공유됩니다. 이러한 서비스는 하나 이상의 서비스 도메인에 의해 게스트 도메인에 제공됩니다. 이러한 리소스를 게스트 도메인에 지정하고 분산시키는 방법을 주의 깊게 고려하십시오. 최대 성능 및 리소스 활용률을 동시에 허용하는 구성은 부작용의 위험을 최소화합니다.

평가: 공유 리소스를 통한 부작용

도메인에 배타적으로 지정되거나 도메인 사이에 공유되든지 네트워크 연결은 포화되고 디스크는 오버로드될 수 있습니다. 이러한 공격은 공격 시간 동안 서비스의 가용성에 영향을 줍니다. 공격 대상은 손상되지 않고 데이터는 손실되지 않습니다. 이 위협의 영향을 쉽게 최소화할 수 있지만, Oracle VM Server for SPARC에서는 네트워크 및 디스크 리소스로 제한되더라도 항상 염두에 두어야 합니다.

대처 방법: 하드웨어 리소스를 주의하여 지정

필요한 하드웨어 리소스만 게스트 도메인에 지정해야 합니다. 리소스가 더 이상 필요하지 않을 때는 사용되지 않는 리소스를 지정 해제하십시오. 예를 들어, 네트워크 포트나 DVD 드라이브는 설치 중에만 필요합니다. 이 방식을 따르면 공격자에게 가능한 진입 지점 수를 최소화할 수 있습니다.

대처 방법: 공유 리소스를 주의하여 지정

물리적 네트워크 포트와 같은 공유 하드웨어 리소스는 DoS 공격 대상이 될 수 있습니다. DoS 공격의 영향을 단일 게스트 도메인 그룹으로 제한하려면 어떤 게스트 도메인에서 어떤 하드웨어 리소스를 공유할지 주의 깊게 결정하십시오.

예를 들어, 하드웨어 리소스를 공유하는 게스트 도메인은 동일한 가용성 또는 보안 요구 사항으로 그룹화할 수 있습니다. 그룹화 이외에도 서로 다른 종류의 리소스 제어를 적용할 수 있습니다.

디스크 및 네트워크 리소스를 어떻게 공유할지 고려해야 합니다. 전용 물리적 액세스 경로 또는 전용 가상 디스크 서비스를 통해 디스크 액세스를 구분함으로써 문제를 완화할 수 있습니다.

요약: 공유 리소스를 통한 부작용

이 절에서 설명한 모든 대처 방법에는 배포 및 보안 구현에 대한 기술적 세부 정보의 이해가 필요합니다. 주의 깊게 계획하고, 올바르게 문서화하며, 가능한 단순하게 아키텍처를 유지하십시오. 가상화 하드웨어의 구현을 이해해야만 Oracle VM Server for SPARC 소프트웨어의 안전한 배포를 준비할 수 있습니다.

CPU 및 메모리는 실제로 거의 공유가 발생하지 않으므로 논리적 도메인은 CPU 및 메모리 공유의 영향에 비교적 안전합니다. 그래도 게스트 도메인 내에서 Solaris 리소스 관리와 같은 리소스 제어를 적용하는 것이 가장 좋습니다. 이러한 제어를 사용하면 가상 또는 비가상화 환경에 대한 잘못된 응용 프로그램 동작으로부터 보호할 수 있습니다.

실행 환경

그림 3은 실행 환경의 구성 요소를 나타냅니다. 각 구성 요소는 운용 게스트 도메인 실행을 위한 전체적인 플랫폼을 함께 구성하는 특정 서비스를 제공합니다. 구성 요소를 올바르게 구성하는 것은 시스템의 무결성에 매우 중요합니다.

모든 실행 환경 구성 요소는 공격자의 잠재적 대상입니다. 이 절에서는 실행 환경의 각 구성 요소에 영향을 줄 수 있는 위협에 대해 설명합니다. 일부 위협 및 대처 방법은 여러 구성 요소에 적용될 수 있습니다.

위협: 실행 환경의 조작

실행 환경을 조작하면 여러 가지 방법으로 제어 권한을 얻을 수 있습니다. 예를 들어, 조작된 펌웨어를 Oracle ILOM에 설치하면 I/O 도메인 내에서 모든 게스트 도메인 I/O를 스누핑할 수 있습니다. 이러한 공격은 시스템의 구성에 액세스하고 변경할 수 있습니다. Oracle VM Server for SPARC 컨트롤 도메인에 대한 제어 권한을 얻은 공격자는 시스템을 마음대로 재구성할 수 있으며, I/O 도메인에 대한 제어 권한을 얻은 공격자는 연결된 저장소(부트 디스크 등)를 변경할 수 있습니다.

평가: 실행 환경의 조작

Oracle ILOM 또는 실행 환경의 도메인에 성공적으로 침입한 공격자는 해당 도메인에서 사용 가능한 모든 데이터를 읽고 조작할 수 있습니다. 이 액세스 권한은 네트워크를 통해 또는 가상화 스택의 오류로 부여될 수 있습니다. 대개 Oracle ILOM 및 도메인은 직접 공격할 수 없으므로 이러한 공격은 감행하기가 어렵습니다.

실행 환경의 조작으로부터 보호하기 위한 대처 방법은 표준 보안 방식이며 모든 시스템에서 구현되어야 합니다. 표준 보안 방식은 실행 환경에 대한 추가 보호망을 제공하여 침입 및 조작의 위험을 줄여줍니다.

대처 방법: 대화식 액세스 경로 보안

시스템에서 실행되는 응용 프로그램에 필요한 계정만 만들어야 합니다.

관리에 필요한 계정은 키 기반 인증 또는 강력한 암호로 보안을 유지해야 합니다. 이러한 키 또는 암호는 다른 도메인과 공유해서는 안됩니다. 또한 특정 작업 수행을 위해 두 단계 인증 또는 “두 사람 규칙”을 구현하는 것이 좋습니다.

시스템에서 명령 실행의 완전한 추적 및 책임을 확보하려면 `root`와 같은 계정에 대해 익명 로그인을 사용하지 마십시오. 대신 권한을 사용하여 개별 관리자에게 수행이 허용된 기능에 대한 액세스 권한만 부여하십시오. 관리 네트워크 액세스에서는 항상 SSH와 같은 암호화를 사용하고 관리자의 워크스테이션은 최상위 보안 시스템으로 취급하십시오.

대처 방법: Oracle Solaris OS 최소화

시스템에 설치된 모든 소프트웨어가 악용될 수 있으므로 필요한 소프트웨어만 설치하여 침입 가능성을 최소화하십시오.

대처 방법: Oracle Solaris OS 강화

최소한의 Oracle Solaris OS 설치와 함께, 공격에 대해 소프트웨어를 “강화”하도록 소프트웨어 패키지를 구성하십시오. 먼저, 제한된 네트워크 서비스를 실행하여 SSH를 제외한 모든 네트워크 서비스를 효과적으로 사용 안함으로 설정합니다. 이 정책은 Oracle Solaris 11 시스템에서 기본 동작입니다. Oracle Solaris OS 보안 방법에 대한 자세한 내용은 *Oracle Solaris 10 Security Guidelines* 및 *Oracle Solaris 11 Security Guidelines*을 참조하십시오.

대처 방법: 역할 구분 및 응용 프로그램 격리 사용

필요에 따라 운용 응용 프로그램은 다른 시스템에 연결되며 결과적으로 외부 공격에 더 많이 노출됩니다. 실행 환경의 일부인 도메인에 운용 응용 프로그램을 배포하지 마십시오. 대신 추가 권한이 없는 게스트 도메인에만 배포하십시오.

실행 환경은 이러한 게스트 도메인에 대해 필요한 기반구조만 제공해야 합니다. 실행 환경을 운용 응용 프로그램에서 분리하면 관리 권한에서 세밀도를 구현할 수 있습니다. 운용 게스트 도메인 관리자는 실행 환경에 대한 액세스 권한이 필요하지 않으며, 실행 환경 관리자는 운용 게스트 도메인에 대한 액세스 권한이 필요하지 않습니다. 가능하다면 컨트롤 도메인 및 I/O 도메인 등 실행 환경의 서로 다른 역할을 서로 다른 도메인에 지정하십시오. 이러한 유형의 구성은 도메인 중 하나가 공격 당할 경우 피해를 줄일 수 있습니다.

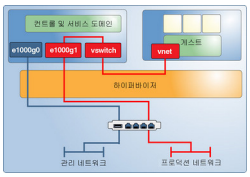
또한 서로 다른 서버를 연결하는 데 사용되는 네트워크 환경으로 역할 구분을 확장할 수도 있습니다.

대처 방법: 전용 관리 네트워크 구성

서비스 프로세서(SP)가 있는 모든 서버를 전용 관리 네트워크에 연결합니다. 이 구성은 실행 환경의 도메인에도 권장됩니다. 모두 네트워크에 연결된 경우 자신의 전용 네트워크에서 해당 도메인을 호스트합니다. 실행 환경 도메인을 운용 도메인에 지정된 네트워크에 직접 연결하지 마십시오. Oracle ILOM SP로 사용할 수 있는 단일 콘솔 연결을 통해 모든 관리 작업을 수행할 수 있지만 이 구성은 관리를 매우 어렵게 만듭니다. 운용 및 관리 네트워크를 구분하면 감청 및

조작 모두로부터 보호할 수 있습니다. 또한 이와 같은 유형의 구분은 공유 네트워크를 통해 게스트 도메인에서 실행 환경에 대한 공격 가능성도 없앱니다.

그림 **5** 전용 관리 네트워크



Oracle ILOM

모든 최신 Oracle SPARC 시스템에는 다음 기능을 갖춘 내장 시스템 컨트롤러(Oracle ILOM)가 포함됩니다.

- 팬 속도 및 섀시 전원과 같은 기본적인 환경 컨트롤 관리
- 펌웨어 업그레이드 사용
- 컨트롤 도메인에 대한 시스템 콘솔 제공

직렬 연결을 통해 Oracle ILOM에 액세스하거나 SSH, HTTP, HTTPS, SNMP 또는 IPMI를 사용하여 네트워크 포트를 통해 액세스할 수 있습니다. Fujitsu M10 서버에서는 Oracle ILOM 대신 XSCF를 사용하여 유사한 기능을 수행합니다.

위협: 전체 시스템 서비스 거부

Oracle ILOM에 대한 제어 권한을 얻은 공격자는 다음을 포함한 여러 가지 방법으로 시스템을 손상시킬 수 있습니다.

- 모든 실행 중인 게스트에서 전원 제거
- 조작된 펌웨어를 설치하여 최소 하나의 게스트 도메인에 대한 액세스 권한 획득

이러한 시나리오는 이 컨트롤러 장치가 있는 모든 시스템에 적용됩니다. 가상화 환경에서는 동일한 시스템 인클로저에 들어 있는 많은 도메인이 위험에 노출될 수 있으므로 물리적 환경보다 피해가 더 클 수 있습니다.

마찬가지로 컨트롤 도메인이나 I/O 도메인에 대한 제어 권한을 얻은 공격자는 해당하는 I/O 서비스를 종료함으로써 모든 종속 게스트 도메인을 쉽게 사용 안함으로 설정할 수 있습니다.

평가: 전체 시스템 서비스 거부

일반적으로 Oracle ILOM는 잘 보호되고 일반 프로덕션 네트워크로부터 격리되어야 하는 관리 네트워크에 연결됩니다.

마찬가지로 공격자는 네트워크에서 또는 가상화 스택의 오류를 통해 서비스 도메인에 침입한 다음 게스트 I/O를 차단하거나 시스템 종료를 실행할 수 있습니다. 데이터가 손실되거나 손상되지 않으므로 피해는 제한적이지만, 많은 수의 게스트 도메인에 영향을 줄 수 있습니다. 따라서 이 위협의 발생 가능성에 대비하여 잠재적인 피해를 막으십시오.

대처 방법: Oracle ILOM 보안

시스템 서비스 프로세서인 Oracle ILOM는 섀시 전원, Oracle VM Server for SPARC 시작 구성 및 컨트롤 도메인에 대한 콘솔 액세스와 같은 중요 기능을 제어합니다. 다음 방법을 통해 Oracle ILOM의 보안을 유지할 수 있습니다.

- Oracle ILOM의 네트워크 포트를 실행 환경의 도메인에 사용되는 관리 네트워크와 구분된 네트워크 세그먼트에 둡니다.
- HTTP, IPMI, SNMP, HTTPS, SSH 등 운영에 필요하지 않은 모든 서비스를 사용 안함으로 설정합니다.
- 필요한 권한만 부여하는 전용 및 개인별 관리자 계정을 구성합니다. 관리자가 수행한 작업의 책임을 분명하게 하기 위해 개인별 관리자 계정을 만드십시오. 이와 같은 유형의 액세스 권한은 콘솔 액세스, 펌웨어 업그레이드 및 시작 구성 관리에 특히 중요합니다.

하이퍼바이저

하이퍼바이저는 실제 하드웨어의 가상화를 구현하고 제어하는 펌웨어 층입니다. 하이퍼바이저에는 다음 구성 요소가 포함됩니다.

- 펌웨어로 구현되고 시스템의 CPU로 지원되는 실제 하이퍼바이저
- 컨트롤 도메인에서 실행되어 하이퍼바이저를 구성하는 커널 모듈
- I/O 도메인 및 서비스 도메인에서 실행되어 가상화 I/O를 제공하는 커널 모듈 및 데몬과 LDC(Logical Domain Channels)로 통신하는 커널 모듈
- 게스트 도메인에서 실행되어 가상화 I/O 장치에 액세스하는 커널 모듈 및 장치 드라이버와 LDC로 통신하는 커널 모듈

위협: 격리 무효화

공격자는 하이퍼바이저가 제공하는 격리된 런타임 환경에서 빠져 나와 게스트 도메인이나 전체 시스템을 가로챌 수 있습니다. 잠재적으로 이 위협은 시스템에 가장 심각한 피해를 줄 수 있습니다.

평가: 격리 무효화

모듈식 시스템 설계는 게스트 도메인, 하이퍼바이저 및 컨트롤 도메인에 서로 다른 레벨의 권한을 부여함으로써 격리를 향상시킬 수 있습니다. 각 기능별 모듈은 구분되고 구성 가능한 커널 모듈, 장치 드라이버 또는 데몬에서 구현됩니다. 이 모듈성에는 전체적인 오류의 위험을 줄일 수 있도록 명료한 API 및 단순한 통신 프로토콜이 필요합니다.

오류의 악용 가능성은 낮더라도 잠재적 피해는 공격자의 전체 시스템 제어로 이어질 수 있습니다.

대처 방법: 펌웨어 및 소프트웨어 서명 검증

시스템 펌웨어 및 OS 패치를 Oracle 웹 사이트에서 직접 다운로드할 수 있더라도 이러한 패치는 조작될 수 있습니다. 소프트웨어를 설치하기 전에 소프트웨어 패키지의 MD5 체크섬을 확인하십시오. 모든 다운로드 가능한 소프트웨어의 체크섬은 Oracle에 의해 게시됩니다.

대처 방법: 커널 모듈 검증

Oracle VM Server for SPARC에서는 여러 드라이버 및 커널 모듈을 사용하여 전체 가상화 시스템을 구현합니다. Oracle Solaris OS에서 배포되는 모든 커널 모듈 및 대부분의 바이너리에는 디지털 서명이 있습니다. `elfsign` 유틸리티를 사용하여 각 커널 모듈 및 드라이버에 대한 디지털 서명을 확인하십시오. Oracle Solaris 11 `pkg verify` 명령을 사용하면 Oracle Solaris 바이너리의 무결성을 확인할 수 있습니다. `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`를 참조하십시오.

먼저, `elfsign` 유틸리티의 무결성을 설정해야 합니다. 기본적인 감사 및 보고 도구(BART)를 사용하여 디지털 서명 확인 프로세스를 자동화하십시오. Integrating BART and the Solaris Fingerprint Database in the Solaris 10 Operating System (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf`)에서는 BART 및 Solaris 지문 데이터베이스를 결합하여 유사한 무결성 검사를 자동으로 수행하는 방법을 설명합니다. 지문 데이터베이스가 연결되어 있지 않더라도 이 문서에 설명된 개념은 `elfsign` 및 BART를 유사한 방식으로 사용하도록 전달할 수 있습니다.

확인된 부트 기능을 커널 모듈 검증 대처 방법으로 사용할 수 있습니다. 부트 시 자동 커널 모듈 검증을 구성하려면 Oracle ILOM에서 확인된 부트 정책을 설정하십시오. `http://docs.oracle.com/en/hardware/`에서 사용 중인 플랫폼용 설명서를 참조하십시오. 컨트롤 도메인에서 커널 모듈을 검증하려면 Oracle ILOM에서 확인된 부트 정책을 설정하십시오. 게스트 도메인에서 커널 모듈을 검증하려면 Logical Domains Manager에서 확인된 부트 정책을 설정하십시오.

컨트롤 도메인

종종 I/O 도메인 및 서비스 도메인의 역할도 수행하는 컨트롤 도메인은 모든 연결된 하드웨어 리소스를 제어하는 하이퍼바이저의 구성을 수정할 수 있으므로 가능한 안전하게 유지해야 합니다.

위협: 컨트롤 도메인 서비스 거부

컨트롤 도메인이 종료되면 구성 도구의 서비스 거부가 발생할 수 있습니다. 컨트롤 도메인은 구성 변경을 위해서만 필요하므로 게스트 도메인은 다른 서비스 도메인을 통해 자신의 네트워크 및 디스크 리소스에 액세스한다면 영향을 받지 않습니다.

평가: 컨트롤 도메인 서비스 거부

네트워크를 통한 컨트롤 도메인 공격은 제대로 보호된 다른 Oracle Solaris OS 인스턴스를 공격하는 것과 같습니다. 컨트롤 도메인의 종료 또는 유사한 서비스 공격의 피해는 비교적 적습니다. 하지만 컨트롤 도메인이 게스트 도메인에 대한 서비스 도메인의 역할도 수행하는 경우 게스트 도메인이 영향을 받습니다.

대처 방법: 콘솔 액세스 보안

실행 환경의 도메인에 대한 관리 네트워크 액세스 구성을 피하십시오. 이 시나리오의 경우 컨트롤 도메인에 대해 Oracle ILOM 콘솔 서비스를 사용하여 모든 관리 작업을 수행해야 합니다. 다른 모든 도메인에 대한 콘솔 액세스는 컨트롤 도메인에서 실행되는 `vntsd` 서비스를 사용하여 여전히 가능합니다.

이 옵션은 주의 깊게 고려하십시오. 이 옵션은 관리 네트워크를 통해 공격 받을 위험을 줄이지만 한 번에 한 명의 관리자만 콘솔에 액세스할 수 있습니다.

`vntsd`의 안전한 구성에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4* 관리 설명서의 "가상 네트워크 터미널 서버 데몬을 사용으로 설정하는 방법"을 참조하십시오.

Logical Domains Manager

Logical Domains Manager는 컨트롤 도메인에서 실행되고 하이퍼바이저를 구성하는 데 사용되며, 모든 도메인 및 해당 하드웨어 리소스를 만들고 구성합니다. Logical Domains Manager 사용은 기록 및 모니터링되어야 합니다.

위협: 구성 유틸리티의 허용되지 않은 사용

공격자가 관리자의 사용자 ID를 도용하거나 다른 그룹의 관리자가 다른 시스템에 대해 허용되지 않은 액세스 권한을 얻을 수 있습니다.

평가: 구성 유틸리티의 허용되지 않은 사용

적절한 ID 관리를 통해 관리자가 시스템에 대한 불필요한 액세스 권한을 보유하지 않도록 하십시오. 또한 엄격하고 세밀한 액세스 제어 및 기타 방법(두 사람 규칙 등)을 구현하십시오.

대처 방법: 두 사람 규칙 적용

권한을 사용하여 Logical Domains Manager 및 기타 관리 도구에 대해 두 사람 규칙 구현을 고려하십시오. Enforcing a Two Man Rule Using Solaris 10 RBAC (`https://blogs.oracle.com/gbrunett/entry/enforcing_a_two_man_rule`). 이 규칙은 소셜 엔지니어링 공격, 유출된 관리 계정 및 사람의 실수로부터 보호합니다.

대처 방법: Logical Domains Manager에 대해 권한 사용

`ldm` 명령에 대해 권한을 사용하면 세밀한 액세스 제어를 구현하고 완전한 추적 기능을 유지할 수 있습니다. 권한 구성에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4 관리 설명서*를 참조하십시오. 권한을 사용하면 `ldm` 명령의 일부 기능을 모든 관리자가 사용할 수 없게 되므로 사람의 실수로부터 보호하는 데 도움이 됩니다.

대처 방법: Logical Domains Manager 강화

불필요한 도메인 관리 서비스를 사용 안함으로 설정합니다. Logical Domains Manager는 도메인 액세스, 모니터링 및 마이그레이션을 위한 네트워크 서비스를 제공합니다. 네트워크 서비스를 사용 안함으로 설정하면 Logical Domains Manager의 공격 범위가 일반적으로 운영하는 데 필요한 최소 범위로 줄어듭니다. 이 시나리오를 통해 서비스 거부 공격 및 이러한 네트워크 서비스를 오용하려는 기타 시도에 대비할 수 있습니다.

주 - 도메인 관리자 서비스를 사용 안함으로 설정하면 공격 범위가 최소화되지만, 특정 구성에서 이로 인한 모든 부작용은 사전에 알 수가 없습니다.

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 6482의 XMPP(확장성 메시징 및 프레즌스 프로토콜) 지원

  이 서비스를 사용 안함으로 설정하는 방법에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4 개발자 설명서* 의 "XML 전송"을 참조하십시오.

  XMPP를 사용 안함으로 설정하면 일부 관리 도구 및 핵심 Oracle VM Server for SPARC 기능이 작동하지 않습니다. "Oracle VM Server for SPARC XML 인터페이스" [35]를 참조하십시오.
- UDP 포트 161의 SNMP(Simple Network Management Protocol)

  Oracle VM Server for SPARC MIB(Management Information Base)를 사용하여 도메인을 관찰할지 여부를 결정합니다. 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 Management Information Base 사용자 설명서* 의 "Oracle VM Server for SPARC MIB 소프트웨어 패키지를 설치하는 방법" 및 *Oracle VM Server for SPARC Management Information Base 사용자 설명서* 의 3 장, "보안 관리"를 참조하십시오.
  - **SNMP 서비스를 사용 안함으로 설정합니다.** 이 서비스를 사용 안함으로 설정하는 방법에 대한 자세한 내용은 *Oracle VM Server for SPARC Management Information Base 사용자 설명서* 의 "Oracle VM Server for SPARC MIB 소프트웨어 패키지를 제거하는 방법"을 참조하십시오.
- 멀티캐스트 주소 239.129.9.27 및 64535 포트의 검색 서비스

  주 - 이 검색 방식은 ldmd 데몬에서도 사용되어 MAC 주소를 자동으로 지정할 때 충돌을 감지합니다. 검색 서비스를 사용 안함으로 설정할 경우 MAC 주소 충돌 감지가 작동하지 않으며, 이에 따라 자동 MAC 주소 할당이 올바르게 작동하지 않습니다.

  Logical Domains Manager 데몬 ldmd가 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"을 참조하십시오.

"대처 방법: Oracle ILOM 보안" [24]도 참조하십시오.

서비스 도메인

서비스 도메인은 시스템의 게스트 도메인에 몇 가지 가상 서비스를 제공합니다. 서비스에는 가상 스위치, 가상 디스크 또는 가상 콘솔 서비스가 포함될 수 있습니다.

그림 6은 콘솔 서비스를 제공하는 서비스 도메인의 예를 나타냅니다. 컨트롤 도메인은 종종 콘솔 서비스를 호스트하므로 서비스 도메인이기도 합니다. 실행 환경 도메인은 컨트롤 도메인, I/O 도메인 및 서비스 도메인의 기능을 하나 또는 두 개의 도메인에서 결합하기도 합니다.

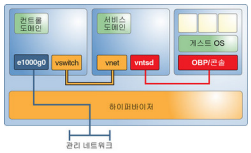
위협: 서비스 도메인의 조작

서비스 도메인에 대한 제어 권한을 얻은 공격자는 제공된 서비스를 통해 데이터를 조작하거나 통신을 감청할 수 있습니다. 이 제어에는 게스트 도메인에 대한 콘솔 액세스, 네트워크 서비스에 대한 액세스 또는 디스크 서비스에 대한 액세스가 포함될 수 있습니다.

평가: 서비스 도메인의 조작

공격 전략은 컨트롤 도메인에 대한 공격과 같지만, 공격자가 시스템 구성을 수정할 수 없으므로 발생 가능한 피해가 훨씬 적습니다. 결과적인 피해에는 데이터 소스의 조작이 아닌 서비스 도메인으로 제공되는 데이터의 도난이나 조작이 포함될 수 있습니다. 서비스에 따라 공격자가 커널 모듈을 교환해야 할 수 있습니다.

그림 **6** 서비스 도메인의 예



대처 방법: 서비스 도메인을 세밀하게 구분

가능한 경우 각 서비스 도메인이 하나의 서비스만 클라이언트에 제공하도록 하십시오. 이 구성은 서비스 도메인이 공격을 받을 경우 하나의 서비스만 침해되도록 합니다. 하지만 이와 같은 유형의 구성에 대한 중요성을 추가적인 복잡성과 비교하십시오. 이 구성에서는 중복 I/O 도메인을 구성할 것을 권장합니다.

대처 방법: 서비스 도메인과 게스트 도메인 격리

Oracle Solaris 10 및 Oracle Solaris 11 서비스 도메인을 게스트 도메인에서 격리할 수 있습니다. 다음 솔루션은 구현의 선호 순서로 나열한 것입니다.

- 서비스 도메인 및 게스트 도메인이 동일한 네트워크 포트를 공유하지 않도록 하십시오. 또한 서비스 도메인에서 가상 스위치 인터페이스를 건드리지 마십시오. Oracle Solaris 11

서비스 도메인의 경우, 가상 스위치에 사용되는 물리적 포트에서 VNIC를 건드리지 마십시오.

- Oracle Solaris 10 OS 및 Oracle Solaris 11 OS에 대해 동일한 네트워크 포트를 사용해야 하는 경우 I/O 도메인 트래픽을 게스트 도메인에서 사용되지 않는 VLAN에 두십시오.
- 위의 솔루션 중 하나도 구현할 수 없는 경우 Oracle Solaris 10 OS에서 가상 스위치를 건드리지 말고 Oracle Solaris 11 OS에서 IP 필터를 적용하십시오.

대처 방법: 가상 콘솔에 대한 액세스 제한

개별 가상 콘솔에 대한 액세스는 액세스해야 하는 사용자로만 제한하십시오. 이 구성은 한 명의 관리자가 모든 콘솔에 대한 액세스 권한을 보유하지 않도록 하여 유출된 계정에 지정된 콘솔 이외의 다른 콘솔에 대한 액세스를 막습니다. *Oracle VM Server for SPARC 3.4* 관리 설명서 의 “기본 서비스를 만드는 방법”을 참조하십시오.

I/O 도메인

네트워크 포트나 디스크와 같이 물리적인 I/O 장치에 대한 직접 액세스 권한을 가지는 모든 도메인이 I/O 도메인입니다. I/O 도메인 구성에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4* 관리 설명서 의 6 장, “I/O 도메인 구성”을 참조하십시오.

하드웨어에 대한 도메인 액세스를 제공하는 I/O 서비스를 게스트 도메인에 적용하는 경우 I/O 도메인은 서비스 도메인이 되기도 합니다.

위협: I/O 도메인 또는 서비스 도메인의 서비스 거부 경험

I/O 도메인의 I/O 서비스를 차단하는 공격자는 모든 종속 게스트 도메인도 차단되도록 합니다. 백엔드 네트워크 또는 디스크 기반구조를 오버로드하거나 도메인에 결함을 주입함으로써 DoS 공격을 성공할 수 있습니다. 두 공격 모두 도메인이 작동을 멈추거나 패닉을 발생시킵니다. 마찬가지로 서비스 도메인의 서비스를 일시 중지하는 공격자는 이러한 서비스에 의존하는 모든 게스트 도메인의 작동을 즉시 멈출 수 있습니다. 게스트 도메인의 작동이 멈출 경우 I/O 서비스가 재개되면 작업을 재개합니다.

평가: I/O 도메인 또는 서비스 도메인의 서비스 거부 경험

DoS 공격은 일반적으로 네트워크를 통해 이루어집니다. 이러한 공격은 네트워크 포트가 통신을 위해 열려 있고 네트워크 트래픽으로 과부하를 일으킬 수 있으므로 성공합니다. 서비스 중단으로 인해 종속 게스트 도메인은 차단됩니다. 디스크 리소스에 대한 유사한 공격은 SAN 기반구조를 통해 또는 I/O 도메인 공격으로 이루어집니다. 유일한 피해는 모든 종속 게스트 도메인의 일시 중지입니다. DoS 작업의 영향이 클 수 있지만, 데이터는 손상되거나 손실되지 않으며 시스템 구성은 그대로 유지됩니다.

대처 방법: I/O 도메인을 세밀하게 구성

여러 I/O 도메인을 구성하면 한 도메인에서 장애가 발생하거나 손상되는 영향이 줄어듭니다. 개별 PCIe 슬롯을 게스트 도메인에 지정하여 I/O 도메인 기능을 부여할 수 있습니다. PCIe 버스를 소유하는 루트 도메인에서 장애가 발생하면 해당 버스는 재설정되고 개별 슬롯이 지정된 도메인의 다음 장애 발생으로 이어집니다. 이 기능이 있다고 해서 각각 별도의 PCIe 버스를 소유하는 두 루트 도메인에 대한 필요성이 완전히 없어지는 것은 아닙니다.

대처 방법: 중복 하드웨어 및 루트 도메인 구성

고가용성도 서비스가 서비스 거부 공격에 견딜 수 있도록 하여 보안 향상에 기여합니다. Oracle VM Server for SPARC는 중복 I/O 도메인에서 중복 디스크 및 네트워크 리소스 사용과 같은 고가용성 방법을 구현합니다. 이 구성 옵션은 I/O 도메인의 롤링 업그레이드를 가능하게 하고 DoS 공격 성공으로 인해 장애가 발생한 I/O 도메인의 영향으로부터 보호합니다. SR-IOV의 출현으로 게스트 도메인은 개별 I/O 장치에 대한 직접 액세스 권한을 가질 수 있습니다. 하지만 SR-IOV가 옵션이 아닌 경우 중복 I/O 도메인 생성을 고려하십시오. “대처 방법: 서비스 도메인을 세밀하게 구분” [29]을 참조하십시오.

위협: I/O 도메인의 조작

I/O 도메인은 가상화한 다음 게스트 도메인에 제공하는 백엔드 장치(대개 디스크)에 직접 액세스할 수 있습니다. 성공한 공격자는 이러한 장치에 대한 전체 액세스 권한을 얻고 게스트 도메인의 부트 디스크에서 민감한 데이터를 읽거나 소프트웨어를 조작할 수 있습니다.

평가: I/O 도메인의 조작

I/O 도메인 공격은 서비스 도메인이나 컨트롤 도메인에 대한 공격만큼 성공할 수 있습니다. I/O 도메인은 많은 수의 디스크 장치에 대한 잠재적인 액세스를 감안할 때 매력적인 대상입니다. 따라서 가상화 디스크에서 실행되는 게스트 도메인에서 민감한 데이터를 다룰 때는 이 위협을 고려하십시오.

대처 방법: 가상 디스크 보호

I/O 도메인이 손상될 경우 공격자는 게스트 도메인의 가상 디스크에 대한 전체 액세스 권한을 얻습니다.

다음을 수행하여 가상 디스크의 컨텐츠를 보호하십시오.

- **가상 디스크의 컨텐츠 암호화.** Oracle Solaris 10 시스템에서는 자신의 데이터를 암호화할 수 있는 응용 프로그램(예: `pgp`/`gpg`) 또는 Oracle 11g 암호화된 테이블스페이스를 사용할 수 있습니다. Oracle Solaris 11 시스템에서는 파일 시스템에 저장된 모든 데이터의 투명한 암호화를 제공하는 ZFS 암호화된 데이터 세트를 사용할 수 있습니다.

- **서로 다른 I/O 도메인에 걸쳐 여러 가상 디스크에 데이터 분산.** 게스트 도메인은 두 I/O 도메인에서 가져온 여러 가상 디스크를 묶는 스트라이프(RAID 1/RAID 5) 볼륨을 만들 수 있습니다. 이러한 I/O 도메인 중 하나가 손상될 경우 공격자는 사용 가능한 데이터의 일부를 활용하는 데 어려움을 겪습니다.

게스트 도메인

게스트 도메인은 실행 환경의 일부가 아니지만 네트워크에 연결되어 있으므로 주요 공격 대상입니다. 가상화 시스템에 침입한 공격자는 실행 환경에 대한 공격을 감행할 수 있습니다.

대처 방법: 게스트 도메인 OS 보안

게스트 도메인의 운영 체제는 공격에 대한 첫번째 방어망인 경우가 많습니다. 데이터 센터 내부에서 시작된 공격을 제외하고 공격자는 게스트 도메인 격리 무효화 및 전체 환경 장악을 시도하기 전에 외부와 연결된 게스트 도메인에 침입해야 합니다. 따라서 게스트 도메인의 OS를 강화할 필요가 있습니다.

OS를 더욱 강화하기 위해 Solaris 영역에 응용 프로그램을 배포할 수 있습니다. 그러면 응용 프로그램의 네트워크 서비스와 게스트 도메인의 운영 체제 사이에 격리 층이 추가됩니다. 서비스에 대한 공격이 성공하더라도 기본 운영 체제가 아닌 영역만 손상되어 공격자가 영역에 할당된 리소스 이외에는 제어 권한을 확장할 수 없게 됩니다. 결과적으로 게스트 격리 무효화 공격이 더욱 어려워집니다. 게스트 OS 보안에 대한 자세한 내용은 *Oracle Solaris 10 Security Guidelines* 및 *Oracle Solaris 11 Security Guidelines*를 참조하십시오.

♦ ♦ ♦ 2 장

2 Oracle VM Server for SPARC 보안 설치 및 구성

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

설치

Oracle VM Server for SPARC 소프트웨어는 자동으로 Oracle Solaris 11 패키지로 안전하게 설치됩니다. 설치가 완료되면 관리자 권한이 있어야 권한 및 권한 부여 기능을 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 3.4* 관리 설명서 의 3 장, "서비스 및 컨트롤 도메인 설정"을 참조하십시오.
- 게스트 도메인을 구성합니다. *Oracle VM Server for SPARC 3.4* 관리 설명서 의 4 장, "게스트 도메인 설정"을 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. "대처 방법: 전용 관리 네트워크 구성" [22]을 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, 권한을 사용하여 콘솔 연결 액세스를 오직 허용된 사용자로 제한하십시오.

- SP(서비스 프로세서)는 기본적으로 안전하게 구성됩니다. Oracle ILOM(Oracle 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 개발자를 위한 보안 고려 사항

이 장은 Oracle VM Server for SPARC 소프트웨어용 응용 프로그램을 제작하는 개발자를 위한 정보를 제공합니다.

Oracle VM Server for SPARC XML 인터페이스

XML(확장성 마크업 언어) 통신 방식을 통해 Oracle VM Server for SPARC 소프트웨어와 상호 작용하는 외부 프로그램을 만들 수 있습니다. XML은 XMPP(Extensible Messaging and Presence Protocol)를 사용합니다. XML 인터페이스는 TLS(전송 계층 보안) 프로토콜 버전 1.2만 지원합니다.

공격자들은 이 네트워크 프로토콜을 악용하여 시스템에 액세스할 수 있으므로, XMPP를 사용 안함으로 설정하십시오. XMPP를 사용 안함으로 설정하는 방법은 *Oracle VM Server for SPARC 3.4* 개발자 설명서 의 "XML 전송"을 참조하십시오. Logical Domains Manager에서 사용하는 보안 방식에 대한 자세한 내용은 *Oracle VM Server for SPARC 3.4* 개발자 설명서 의 "XMPP 서버"를 참조하십시오.

XMPP를 사용 안함으로 설정하면 Oracle VM Manager 또는 Ops Center가 시스템을 관리하지 못하게 되어 다음 명령과 같은 일부 핵심 Oracle VM Server for SPARC 기능을 사용할 수 없게 됩니다.

- `ldm migrate-domain`
- `ldm init-system`
- `ldm remove-core -g`
- `ldm add-memory`
- `ldm set-memory`
- `ldm remove-memory`
- `ldm grow-socket`
- `ldm shrink-socket`
- `ldm set-socket`
- `ldm list-socket`

♦ ♦ ♦ 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 3.4 관리 설명서*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*

Oracle VM Server for SPARC 보안 점검 목록

- 가상화되지 않은 환경에서처럼 게스트 도메인에 대해 Oracle Solaris OS 강화 단계를 수행합니다.
- LDoms 관리 및 LDoms 검토 권한 프로파일을 사용하여 적합한 권한을 사용자에게 위임합니다.
- 권한을 사용하여 Oracle VM Server for SPARC의 관리자만 액세스해야 하는 도메인의 콘솔로 액세스를 제한합니다.
- 불필요한 도메인 관리 서비스를 사용 안함으로 설정합니다.
- 같은 보안 클래스의 게스트 도메인은 한 물리적 플랫폼에만 배포합니다.
- 실행 환경 관리 네트워크와 게스트 도메인 간 네트워크 연결이 없는지 확인합니다.
- 필요한 리소스만 게스트 도메인에 지정합니다.