Oracle® VM Server for SPARC 3.2 安全指南

文件号码 E56430
2015 年 3 月

ORACLE

文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

获得 Oracle 支持

购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

目录

使用本文档

- **概述** – 提供了有关以安全方式使用 Oracle VM Server for SPARC 3.2 软件的信息。
- **目标读者** – 负责管理虚拟化 SPARC 服务器安全的系统管理员
- **必需的知识** – 这些服务器的系统管理员必须具有 UNIX® 系统和 Oracle Solaris 操作系统 (Oracle Solaris operating system, Oracle Solaris OS) 的实际应用知识。

产品文档库

有关本产品的最新信息和已知问题均包含在文档库中，网址为：http://www.oracle.com/pls/topic/lookup?ctx=E56447。

获得 Oracle 支持

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

反馈

可以在 http://www.oracle.com/goto/docfeedback 上提供有关本文档的反馈。

♦ ♦ ♦ 第 1 章

1 Oracle VM Server for SPARC 安全概述

虽然本文档中的安全建议数量会让人有异样的感觉，但典型的 Oracle VM Server for SPARC 安装已经可以很好的防止未经授权的使用。即使不可能受到破坏，但仍存在小的攻击面，仍会有一定程度的风险。就像您可能会在标准的防护措施（如门锁）以外再增设居家防盗警报一样，额外的网络安全措施有助于降低意外问题发生的机率，或者最大程度地减少可能的损坏。

本章包含以下 Oracle VM Server for SPARC 安全主题：

Oracle VM Server for SPARC 使用的安全功能

Oracle VM Server for SPARC 软件是一个虚拟化产品，允许在一个物理系统上运行多个 Oracle Solaris 虚拟机 (virtual machine, VM)，每个虚拟机均安装有自己的 Oracle Solaris 10 或 Oracle Solaris 11 OS。每个 VM 也称为逻辑域。这些域都是独立的实例，可运行不同版本的 Oracle Solaris OS 以及不同的应用程序软件。例如，这些域可能安装有不同的软件包版本，启用了不同的服务以及存在密码不同的系统帐户。有关 Oracle Solaris 安全的信息，请参见《Oracle Solaris 10 Security Guidelines》和《Oracle Solaris 11 Security Guidelines》。

`ldm` 命令会调用 Logical Domains Manager，并且必须在控制域上运行该命令来配置域和检索状态信息。对于保证系统上运行的域的安全而言，限制对控制域和 `ldm` 命令的访问至关重要。要限制对域配置数据的访问，可使用 Oracle VM Server for SPARC 安全功能，例如控制台的 Oracle Solaris 权限和 `solaris.ldoms` 授权。请参见《Oracle VM Server for SPARC 3.2 管理指南》中的“Logical Domains Manager 配置文件内容”。

Oracle VM Server for SPARC 软件使用以下安全功能：

- Oracle Solaris 10 OS 和 Oracle Solaris 11 OS 中可用的安全功能在运行 Oracle VM Server for SPARC 软件的域中也是可用的。请参见《Oracle Solaris 10 Security Guidelines》和《Oracle Solaris 11 Security Guidelines》。

- Oracle Solaris OS 安全功能可应用于 Oracle VM Server for SPARC 软件。有关确保 Oracle VM Server for SPARC 安全的全面信息，请参见“虚拟化环境中的安全性” [14]和“防御攻击” [15]。
- Oracle Solaris 10 OS 和 Oracle Solaris 11 OS 包含可用于您的系统的安全修复。Oracle Solaris 10 OS 修复作为安全修补程序或更新提供。Oracle Solaris 11 OS 修复作为支持系统信息库更新 (Support Repository Updates, SRU) 提供。
- 有关如何限制对 Oracle VM Server for SPARC 管理命令和域控制台的访问以及如何启用 Oracle VM Server for SPARC 审计功能的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的第 2 章 “Oracle VM Server for SPARC 安全”。

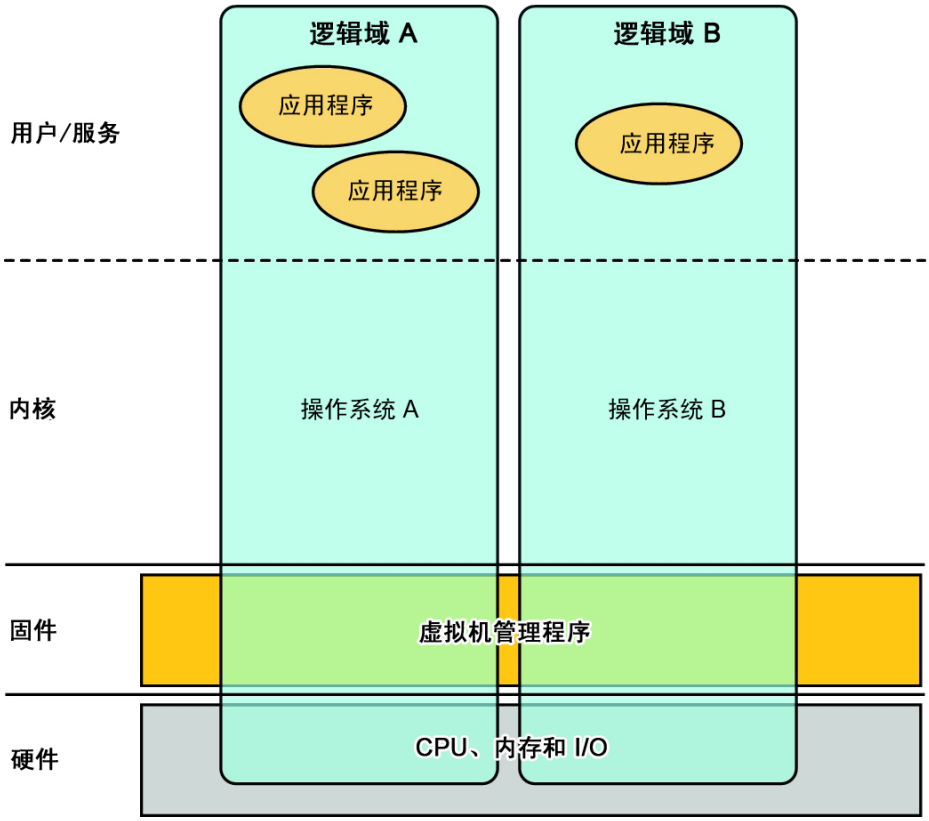
Oracle VM Server for SPARC 产品概述

Oracle VM Server for SPARC 为 Oracle 的 SPARC T 系列服务器以及 SPARC M5 服务器和 Fujitsu M10 服务器提供高效的企业级虚拟化功能。使用 Oracle VM Server for SPARC 软件，可以在单个系统上创建许多虚拟服务器（称为逻辑域）。通过这种配置，可以利用由这些 SPARC 服务器和 Oracle Solaris OS 提供的海量线程规模。

逻辑域是一种包含离散的逻辑资源分组的虚拟机。逻辑域在单个计算机系统内具有自己的操作系统和身份。可以单独创建、销毁、重新配置及重新引导每个逻辑域，而无需对服务器执行关开机循环。可以在不同的逻辑域中运行各种应用程序软件，并使其保持相互独立，以获得相应的性能和安全。

有关使用 Oracle VM Server for SPARC 软件的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》和《Oracle VM Server for SPARC 3.2 Reference Manual 》。有关所需硬件和软件的信息，请参见《Oracle VM Server for SPARC 3.2 安装指南 》。

图 1-1 支持两个逻辑域的虚拟机管理程序



Oracle VM Server for SPARC 软件使用以下组件提供系统虚拟化：

- **虚拟机管理程序。**虚拟机管理程序是一个小固件层，提供了一种稳定的虚拟机体系结构，可在其中安装操作系统。使用虚拟机管理程序的 Oracle Sun 服务器提供了一些硬件功能，通过这些功能可支持虚拟机管理程序在逻辑域中控制操作系统活动。

  特定的 SPARC 虚拟机管理程序所支持的域数量和每个域的功能是与服务器相关的特性。虚拟机管理程序可以向给定的逻辑域分配服务器的 CPU、内存和 I/O 资源的子集。通过此分配便可以同时支持多个操作系统，每个操作系统均位于自己的逻辑域内。资源可在不同的逻辑域之间以任意粒度重新排列。例如，可以按 CPU 线程为粒度将 CPU 分配给逻辑域。

  服务处理器 (service processor, SP) 也称为系统控制器 (system controller, SC)，用于监视和运行物理计算机。管理逻辑域本身的是 Logical Domains Manager，而不是 SP。

- **控制域。**Logical Domains Manager 在此域中运行，支持您创建和管理其他逻辑域，以及向其他域分配虚拟资源。每台服务器只能有一个控制域。控制域是在安装 Oracle VM Server for SPARC 软件时创建的第一个域。控制域名为 `primary`。
- **服务域。**服务域为其他域提供虚拟设备服务（例如，虚拟交换机、虚拟控制台集中器和虚拟磁盘服务器）。任何域都可以配置为服务域。
- **I/O 域。**I/O 域对物理 I/O 设备（例如 PCI EXPRESS (PCIe) 控制器中的网卡）具有直接访问权限。I/O 域可以拥有 PCIe 根联合体，也可以通过使用直接 I/O (direct I/O, DIO) 功能拥有 PCIe 插槽或板载 PCIe 设备。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“通过分配 PCIe 端点设备创建 I/O 域”。

  当 I/O 域也用作服务域时，I/O 域能够以虚拟设备形式与其他域共享物理 I/O 设备。
- **根域。**根域分配有 PCIe 根联合体。此域拥有该根联合体的 PCIe 结构，并提供所有与结构相关的服务，如结构错误处理。根域也是 I/O 域，因为它拥有对物理 I/O 设备的直接访问权限。

  您可以拥有的根域的数量取决于您的平台体系结构。例如，如果使用的是 Oracle SPARC T4-4 服务器，最多可以有四个根域。
- **来宾域。**来宾域是非 I/O 域，它使用由一个或多个服务域提供的虚拟设备服务。来宾域不具有任何物理 I/O 设备。来宾域只有虚拟 I/O 设备（例如虚拟磁盘和虚拟网络接口）。

通常，Oracle VM Server for SPARC 系统只有一个控制域，用于提供由 I/O 域和服务域执行的服务。要提高冗余和平台可维护性，请在 Oracle VM Server for SPARC 系统上配置多个 I/O 域。

将常规安全原则应用到 Oracle VM Server for SPARC

您可以通过各种方式配置来宾域，从而提供各种级别的来宾域隔离、硬件共享和域连接。这些因素会影响 Oracle VM Server for SPARC 整体配置的安全级别。有关以安全方式部署 Oracle VM Server for SPARC 软件的建议，请参见“虚拟化环境中的安全性” [14]和“防御攻击” [15]。

可以应用下列某些一般安全原则：

- **将攻击面减小到最低限度。**
  - 通过创建用于定期评估系统安全的运行准则，将意外配置错误减少到最低限度。请参见“对策：建立操作准则” [17]。
  - 谨慎规划虚拟环境的体系结构以最大限度地隔离域。请参见针对“威胁：虚拟环境体系结构中的错误” [18]介绍的对策。
  - 谨慎规划要分配的资源以及是否要对其进行共享。请参见“对策：仔细分配硬件资源” [20]和“对策：仔细分配共享资源” [21]。
  - 通过应用针对“威胁：操纵执行环境” [21]和“对策：保护来宾域 OS 安全” [32]介绍的对策，确保逻辑域受保护，可防止对其进行处理。
    - “对策：保护交互式访问路径” [22]。
    - “对策：最小化 Oracle Solaris OS” [22]。

  - “对策：强化 Oracle Solaris OS” [22]。
  - “对策：强化 Logical Domains Manager” [27]。
  - “对策：使用角色划分和应用程序隔离” [22]描述了为各个域分配功能角色并确保控制域运行的软件提供托管来宾域所需的基础结构的重要性。应该运行的应用程序可以由其他系统在为此目的设计的来宾域上运行。
  - “对策：配置专用管理网络” [23]描述了一种更高级的网络配置，可以将包含 SP 的服务器连接到专用管理网络以防止对 SP 的网络访问。
- 仅在必要时才向网络公开来宾域。您可以使用虚拟交换机限制来宾域的网络连接，以便为仅连接合适的网络。
- 按照《Oracle Solaris 10 Security Guidelines 》和《Oracle Solaris 11 Security Guidelines 》中所述执行步骤以将 Oracle Solaris 10 和 Oracle Solaris 11 的攻击面减小到最低限度。
- 保护虚拟机管理程序的核心，如“对策：验证固件和软件签名” [25]和“对策：验证内核模块” [25]中所述。
- 保护控制域免遭拒绝服务攻击。请参见“对策：保护控制台访问安全” [26]。
- 确保未授权用户无法运行 Logical Domains Manager。请参见“威胁：未经授权使用配置实用程序” [26]。
- 确保未授权用户或进程无法访问服务域。请参见“威胁：操纵服务域” [29]。
- 保护 I/O 域或服务域免遭拒绝服务攻击。请参见“威胁：遇到 I/O 域或服务域拒绝服务” [30]。
- 确保未授权用户或进程无法访问 I/O 域。请参见“威胁：操纵 I/O 域” [31]。
- 禁用不必要的域管理器服务。Logical Domains Manager 为域访问、监视和迁移提供网络服务。请参见“对策：强化 Logical Domains Manager” [27]和“对策：保护 ILOM 安全” [24]。
- **为执行操作提供最小特权。**
  - 将系统划分为不同安全类，安全类是共享相同安全要求和特权的单个来宾系统构成的组。通过将同一安全类中的来宾域仅分配到一个硬件平台，可创建隔离屏障，从而防止域跨不同的安全类。请参见“对策：仔细将来宾域分配到硬件平台” [18]。
  - 使用权限来限制使用 `ldm` 命令管理域的功能。仅应向那些必须管理域的用户提供此功能。将使用 "LDoms Management"（LDoms 管理）权限配置文件的角色分配给需要访问所有 `ldm` 子命令的用户。将使用 "LDoms Review"（LDoms 查看）权限配置文件的角色分配给只需访问 `ldm` 列出方面的子命令的用户。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“使用权限配置文件和角色”。
  - 使用权限来限制对域的控制台访问：只能访问 Oracle VM Server for SPARC 管理员管理的域的控制台。请勿对所有域提供通用访问。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“通过使用权限控制对域控制台的访问”。
- **监视系统活动。**

  启用 Oracle VM Server for SPARC 审计。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“启用并使用审计”。

虚拟化环境中的安全性

要有效地保护 Oracle VM Server for SPARC 虚拟化环境，需要保护操作系统以及在每个域中运行的每项服务的安全。要降低违规行为成功得逞的影响，需要将服务部署到不同的域来隔离服务。

Oracle VM Server for SPARC 环境使用虚拟机管理程序对逻辑域的 CPU、内存和 I/O 资源进行虚拟化。每个域就是一个独立的虚拟化服务器，必须保护其免受可能的攻击。

利用虚拟化环境，可以通过硬件资源共享，将多个服务器整合到一个服务器中。在 Oracle VM Server for SPARC 中，CPU 和内存资源以独占方式分配给每个域，这样可防止过度使用 CPU 或过度分配内存造成的滥用。磁盘和网络资源通常由服务域提供给许多来宾域。

在评估安全性时，始终假定环境中存在攻击者可利用的缺陷。例如，攻击者可能会利用虚拟机管理程序中的弱点劫持整个系统（包括其来宾域）。因此，请始终部署系统以最大程度地降低发生违规时的损坏风险。

执行环境

执行环境包含以下组件：

- **虚拟机管理程序** – 特定于平台的固件，可以虚拟化硬件，并严重依赖内置于 CPU 的硬件支持。
- **控制域** – 一种专门的域，可以配置虚拟机管理程序以及运行管理逻辑域的 Logical Domains Manager。
- **I/O 域或根域** – 一种域，拥有平台的全部或部分可用 I/O 设备，并将这些设备与其他域共享。
- **服务域** – 一种域，可以向其他域提供服务。服务域可能会提供对其他域的控制台访问权限，或者提供虚拟磁盘。提供对其他域的虚拟磁盘访问权限的服务域也是一种 I/O 域。

有关这些组件的更多信息，请参见图 1-1 “支持两个逻辑域的虚拟机管理程序” 以及更详细的组件说明。

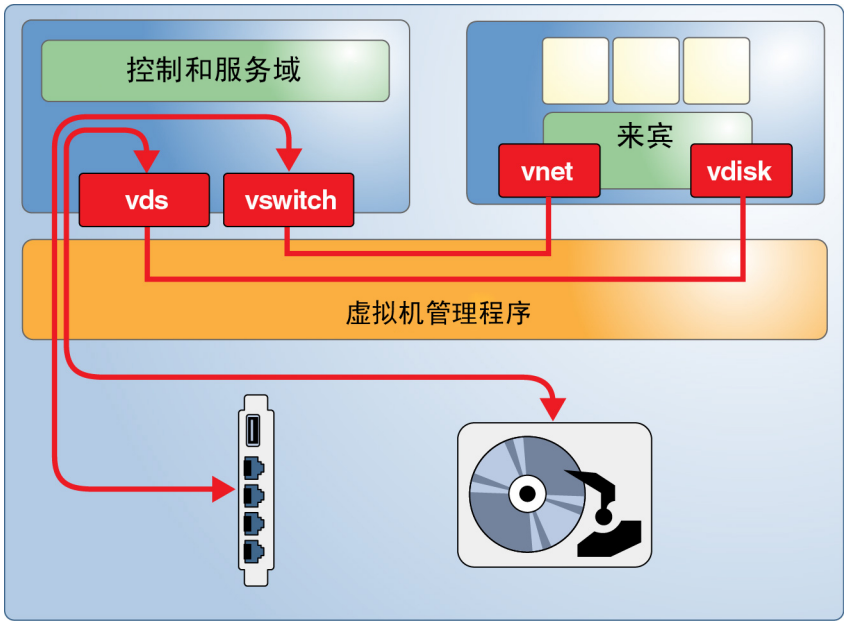
通过再配置一个 I/O 域，可以提高冗余 I/O 配置的可维护性。也可以使用第二个 I/O 域来隔离硬件以防安全违规。有关配置选项的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》。

保护执行环境

Oracle VM Server for SPARC 在执行环境中有多个攻击目标。图 1-2 “Oracle VM Server for SPARC 环境样例” 显示了一个简单的 Oracle VM Server for SPARC 配置；

在该配置中，由控制域向来宾域提供网络和磁盘服务。这些服务是通过在控制域中运行的守护进程和内核模块实现的。Logical Domains Manager 为每项服务分配逻辑域通道 (Logical Domain Channel, LDC)，并指定一个客户机来简化这些通道间的点到点通信。攻击者可能会利用任何组件中的错误来突破对来宾域的隔离。例如，攻击者可能会在服务域中执行任意代码，也可能会中断平台上的正常操作。

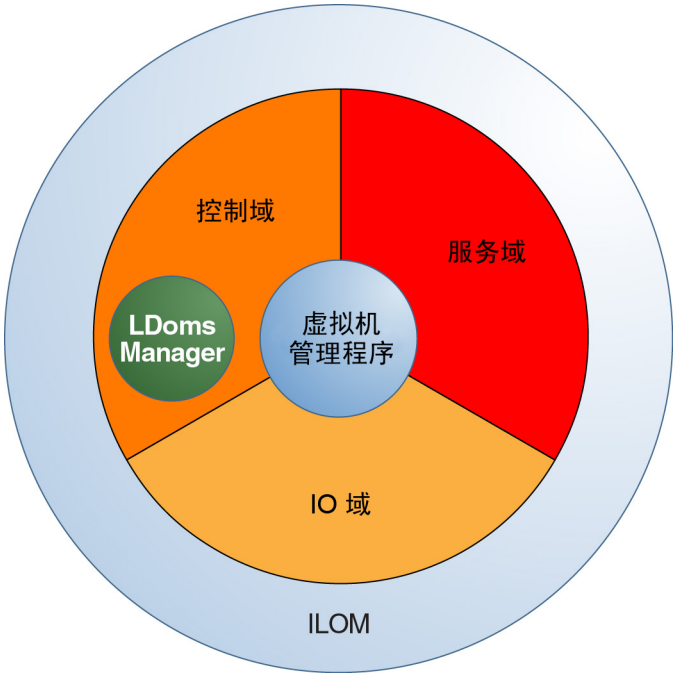
图 1-2 Oracle VM Server for SPARC 环境样例



防御攻击

下图显示了形成 Oracle VM Server for SPARC 的“执行环境”的虚拟化组件。这些组件并未严格分隔。最简单的配置是将所有这些功能组合到一个域中。控制域还可能用作 I/O 域以及其他域的服务域。

图 1-3 执行环境的组件



假定一个攻击者试图突破系统隔离，然后操纵虚拟机管理程序或者执行环境的另一个组件到达来宾域。必须像保护任何独立服务器一样保护每个来宾域。

本章的其余部分将介绍一些可能的威胁，以及可以用于应对这些威胁的各种措施。其中的每种攻击都试图攻克或消除对在单个平台上运行的不同域的隔离。以下各部分将介绍对 Oracle VM Server for SPARC 系统的每个部分的威胁：

操作环境

操作环境包括物理系统及其组件、数据中心架构师、管理员以及 IT 组织的成员。安全违规可能发生在操作环境中的任何点上。

虚拟化会将一个软件层放在实际硬件与运行生产服务的来宾域之间，这将增加复杂性。因此，必须仔细地规划和配置虚拟系统，注意人为错误。此外，还要注意攻击者利用“社交工程”获取操作环境访问权限的企图。

以下各部分介绍了可能在操作环境级别遇到的各种威胁。

威胁：意外错误配置

虚拟化环境的主要安全问题是通过划分网段、隔离管理访问权限以及将服务器部署到安全类（具有相同安全要求和特权的域组），保持服务器隔离。

仔细配置虚拟资源以避免以下某些错误：

- 在生产来宾域和执行环境之间建立不必要的信道
- 创建不必要的网段访问权限
- 在独立的安全类之间建立意外连接
- 将来宾域意外迁移到错误的安全类
- 分配的硬件不足，这可能导致意外的资源过载
- 将磁盘或 I/O 设备分配到错误的域

对策：建立操作准则

在开始之前，仔细地制定适合您的 Oracle VM Server for SPARC 环境的操作准则。这些准则说明以下要执行的任务以及执行任务的方式：

- 管理所有环境组件的修补程序
- 支持定义完善并且可跟踪的安全更改实现
- 定期检查日志文件
- 监视环境的完整性和可用性

定期执行检查以确保这些准则保持最新并适当，并验证在日常操作中是否遵循了这些准则。

除了这些准则以外，还可以采取若干其他技术措施来降低意外操作的风险。请参见“Logical Domains Manager” [26]。

威胁：虚拟环境体系结构中的错误

将物理系统转移到虚拟化环境中时，通常可以重复使用原来的 LUN，原样保留存储配置。但是，必须针对虚拟化环境调整网络配置，得到的体系结构可能与物理系统上使用的体系结构有很大的不同。

必须考虑如何保持独立安全类的隔离及其需求。此外，还要考虑平台的共享硬件以及网络交换机和 SQN 交换机等共享组件。

为了最大程度地提高环境的安全性，要确保保持来宾域与安全类的隔离。设计体系结构时，预知可能的错误和攻击，并实施防御措施。良好的设计有助于压制可能的安全问题，同时管理好复杂性和成本。

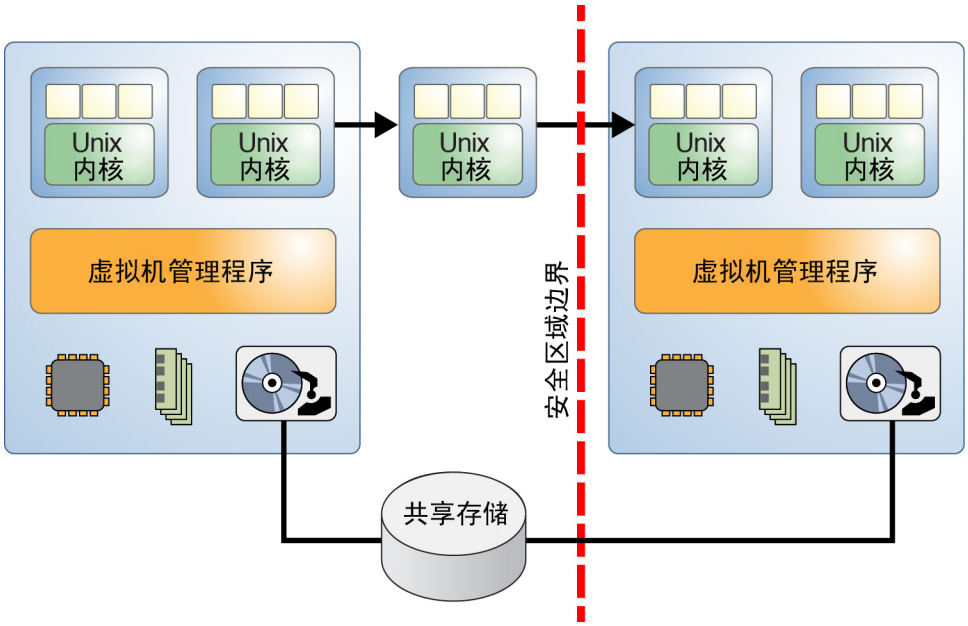
对策：仔细将来宾域分配到硬件平台

使用安全类（具有相同安全要求和特权的域组）将各个域互相隔离。通过将同一个安全类中的来宾域分配到特定的硬件平台，即使在突破隔离的情况下，也能防止攻击跨界进入其他安全类。

对策：规划 Oracle VM Server for SPARC 域迁移

如果无意间将来宾域迁移到分配给不同安全类的平台，则实时域迁移功能可能会突破隔离，如下图中所示。因此，要仔细规划来宾域迁移，确保不允许跨安全类边界进行迁移。

图 1-4 跨安全边界的域迁移



要最大限度地减少或消除迁移操作导致的安全漏洞，必须在每个源计算机和目标计算机对之间手动交换并安装 `ldmd` 生成的带外主机证书。有关如何设置 SSL 证书的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“为迁移配置 SSL 证书”。

对策：正确配置虚拟连接

失去对所有虚拟网络连接的跟踪可能会导致域获得对网段的错误访问权限。例如，可能绕过防火墙或安全类的访问权限。

为了降低出现实现错误的风险，要仔细地规划并记录环境中的所有虚拟连接和物理连接。优化域连接规划以获得简单性和易管理性。清晰地记录规划，并在投入生产前对照规划验证实现是否正确。即使在虚拟环境投入生产之后，也可对照规划定期验证实现内容。

对策：使用 VLAN 标记

可以使用 VLAN 标记将多个以太网段整合到一个物理网络上。此功能也可用于虚拟交换机。为了减轻虚拟交换机实现中涉及软件错误的风险，要为每个物理 NIC 和 VLAN

配置一个虚拟交换机。为了进一步防备以太网驱动程序方面的错误，要避免使用标记的 VLAN。但是，由于这是一个众所周知的标记 VLAN 漏洞，因此发生此类错误的可能性很低。对采用 Oracle VM Server for SPARC 软件的 Oracle Sun SPARC T 系列平台的入侵测试没有显示此漏洞。

对策：使用虚拟安全设备

诸如包过滤器和防火墙之类的安全设备是一些隔离工具，可以保护对安全类的隔离。这些设备也会面临与其他任何来宾域一样的威胁，因此使用它们不能保证完全防范隔离违规。所以，要仔细考虑风险和安全的所有方面，然后再决定对此类服务进行虚拟化。

威胁：共享资源的副作用

在虚拟化环境中共享资源可能会导致拒绝服务 (denial-of-service, DoS) 攻击，就是过量加载资源，直到对其他组件（例如其他域）产生负面影响。

在 Oracle VM Server for SPARC 环境中，只有部分资源可能会受 DoS 攻击影响。CPU 和内存资源是以独占方式分配给每个来宾域的，这样可防止大多数 DoS 攻击。即使以独占方式分配这些资源，也可能会因为以下几方面的原因降低来宾域速度：

- 挤占在导线束间共享并且分配给两个来宾域的高速缓存区域
- 内存带宽过载

与 CPU 和内存资源不同，磁盘和网络服务通常在来宾域之间共享。这些服务是通过一个或多个服务域提供给来宾域的。需要仔细考虑如何向来宾域分配和分发这些资源。请注意，可以最大程度地提高性能和资源利用率的任何配置，都能同时最大程度地降低副作用的风险。

评估：共享资源带来的副作用

不管是以独占方式分配给域，还是在域之间共享，网络链路都可能会饱和，磁盘也可能会过载。此类攻击会影响服务在攻击期间的可用性。攻击的目标不会受损，数据不会丢失。可以轻松地将此威胁的影响降到最低，但是，即使将其限制到 Oracle VM Server for SPARC 上的网络和磁盘资源，也应对其保持警惕。

对策：仔细分配硬件资源

确保仅将所需的硬件资源分配到来宾域。确保取消分配不再需要的未使用资源；例如，仅在安装过程中需要网络端口或 DVD 驱动器。通过遵循这种做法，可以最大程度地减少攻击者的可能入口点数量。

对策：仔细分配共享资源

物理网络端口之类的共享硬件资源会提供可能的 DoS 攻击目标。为了将 DoS 攻击的影响局限于一组来宾域，要仔细确定哪些来宾域共享哪些硬件资源。

例如，共享硬件资源的来宾域可以按相同的可用性或安全要求分组。在分组以外，可以应用各种不同的资源控制。

必须考虑如何共享磁盘和网络资源。通过分隔经由专用的物理访问路径或者专用的虚拟磁盘服务的磁盘访问，可以减轻问题。

摘要：共享资源带来的副作用

本部分介绍的所有对策都需要了解部署的技术细节及其安全意义。需要仔细规划，认真记录，并让体系结构尽可能地简单。确保了解虚拟化硬件的意义，从而可以做好安全部署 Oracle VM Server for SPARC 软件的准备。

逻辑域可以稳健地承受共享 CPU 和内存的影响，因为实际上很少发生共享。虽然如此，最好还是要应用资源控制，如在来宾域内部进行 Solaris 资源管理。利用这些控制可以防止虚拟化环境或非虚拟化环境的不良应用程序行为。

执行环境

图 1-3 “执行环境的组件” 显示了执行环境的组件。每个组件提供特定的服务，这些服务共同形成运行生产来宾域的整个平台。正确地配置组件对系统的完整性至关重要。

所有执行环境组件都是攻击者的潜在目标。本部分介绍了可能影响执行环境中每个组件的威胁。有些威胁和对策可能适于多个组件。

威胁：操纵执行环境

通过操纵执行环境，可以从多个方面获取控制权。例如，可以在 ILOM 中安装受操纵的固件，对来自 I/O 域内部的所有来宾域 I/O 进行侦听。这样的攻击可以访问并更改系统的配置。获取了 Oracle VM Server for SPARC 控制域的控制权的攻击者可以随意重新配置系统；获取了 I/O 域控制权的攻击者可以更改连接的存储（如引导磁盘）。

评估：操纵执行环境

成功侵入 ILOM 或执行环境中任何域的攻击者可以读取和操纵该域可用的所有数据。这种访问权限可通过网络获取，也可通过虚拟化堆栈中的错误获取。由于通常无法直接攻击 ILOM 和域，因此此类攻击难以执行。

防止操纵执行环境的对策是采用标准安全措施，并且应该在任何系统上都实施这些对策。标准安全措施在执行环境周围增加了一个保护层，可以进一步降低入侵和操纵的风险。

对策：保护交互式访问路径

确保仅创建在系统上运行的应用程序所需的帐户。

确保使用基于密钥的验证或强口令保护进行管理所需的帐户。不应在不同的域之间共享这些密钥或口令。此外，还要考虑实施双重验证或“两人规则 (two-person rule)”以采取特定的操作。

不要对 `root` 之类的帐户使用匿名登录，确保可以完整地追溯系统上运行的命令并可确定责任。应使用权限向个别管理员仅授予对允许其执行的功能的访问权限。确保管理网络访问始终使用 SSH 之类的加密，并确保将管理员的工作站视为高安全性系统。

对策：最小化 Oracle Solaris OS

系统上安装的任何软件都可能会受破坏，因此要确保仅安装必需的软件，最大程度地缩小违规窗口。

对策：强化 Oracle Solaris OS

除了安装最小化的 Oracle Solaris OS 以外，还要配置软件包来“强化”软件以防御攻击。首先，运行有限的网络服务，以便有效地禁用除 SSH 以外的所有网络服务。此策略是 Oracle Solaris 11 系统上的缺省行为。有关如何保护 Oracle Solaris OS 的信息，请参见《Oracle Solaris 10 Security Guidelines》和《Oracle Solaris 11 Security Guidelines》。

对策：使用角色划分和应用程序隔离

生产应用程序必然要连接到其他系统，因此更容易受到外部攻击。不要将生产应用程序部署到属于执行环境的域，而是要确保仅将其部署到没有进一步特权的来宾域。

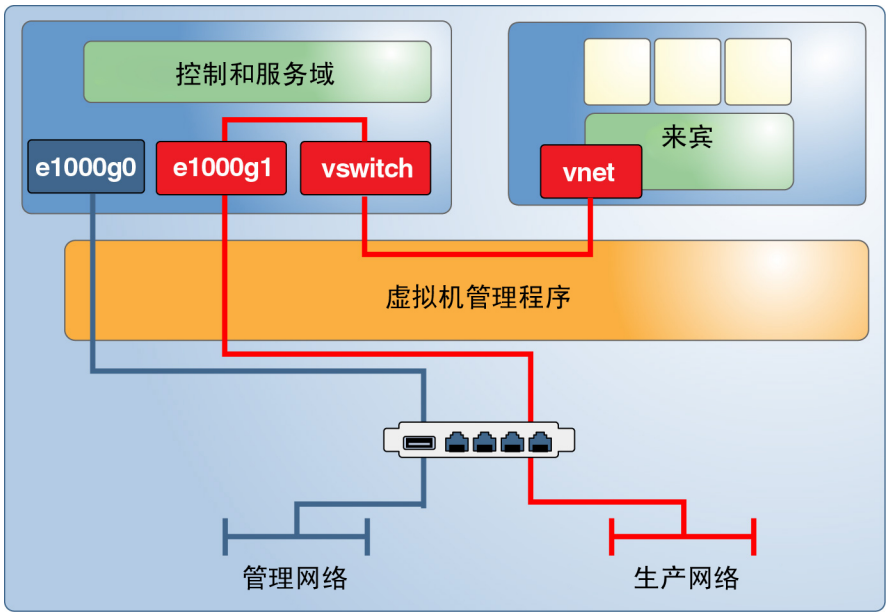
执行环境应该仅提供这些来宾域必需的基础结构。通过将执行环境与生产应用程序分开，可以在管理特权上实现细分。生产来宾域管理员不需要访问执行环境，而执行环境管理员则不需要访问生产来宾域。如有可能 ，为不同的域分配不同的执行环境角色，如控制域和 I/O 域。这种类型的配置可减少万一其中某个域受破坏时可能造成的损害。

还可以将角色划分延伸到用于连接不同服务器的网络环境。

对策：配置专用管理网络

将所有配备了服务处理器 (service processor, SP) 的服务器连接到专用管理网络。此配置也推荐用于执行环境的域。如果已经联网，则在这些域自己的专用网络上托管这些域。不要将执行环境域直接连接到分配给生产域的那些网络。虽然可以通过 ILOM SP 提供的单个控制台连接执行所有管理工作，但此配置会让管理变得很繁琐，以致不切实际。通过划分生产网络和管理网络，可以防止窃听和操纵。这种类型的分隔还可以防止通过共享网络从来宾域攻击执行环境。

图 1-5 专用管理网络



ILOM

所有当前的 Oracle SPARC 系统都包括一个内置系统控制器 (ILOM)，该控制器具有以下功能：

- 管理基本环境控制，如风扇转速和机箱电源
- 支持固件升级
- 为控制域提供系统控制台

可以通过串行连接访问 ILOM，也可以使用 SSH、HTTP、HTTPS、SNMP 或 IPMI 通过网络端口访问 ILOM。Fujitsu M10 服务器使用 XSCF（而不是 ILOM）执行类似功能。

威胁：完全的系统拒绝服务

获取了 ILOM 控制权的攻击者可以通过多种方式破坏系统，其中包括以下方式：

- 断开所有正在运行的来宾的电源
- 安装受操纵的固件以获取至少一个来宾域的访问权限

这些情形适用于具有此类控制器设备的任何系统。在虚拟化环境中，损害可能远大于物理环境，因为同一个系统附件中承载的许多域都将面临风险。

同样，获取了控制域或 I/O 域的控制权的攻击者可以通过关闭对应的 I/O 服务，轻松地禁用所有依赖的来宾域。

评估：完全的系统拒绝服务

虽然 ILOM 通常连接到管理网络，但还可以通过将 IPMI 与 BMC 访问模块配合使用，从控制域访问 ILOM。因此，这两种连接类型都应得到妥善保护，并与正常生产网络隔离。

同样，攻击者通过网络或者通过虚拟化堆栈中的错误破坏服务域，然后阻止来宾 I/O 或者执行系统关闭操作。虽然由于数据不会丢失或受损而损坏有限，但这种损坏可能会影响大量的来宾域。因此，请确保防止出现这种威胁的可能性以限制潜在的损坏。

对策：保护 ILOM 安全

作为系统服务处理器，ILOM 控制了一些重要的功能，如机箱电源、Oracle VM Server for SPARC 启动配置以及对控制域的控制台访问权限。通过以下措施，可以保护 ILOM 的安全：

- 将 ILOM 的网络端口放在与用于执行环境中的域的管理网络分隔的网段中。
- 禁用操作不需要的所有服务，如 HTTP、IPMI、SNMP、HTTPS 和 SSH。
- 配置专用的个人管理员帐户，这些帐户仅授予必需的权限。为了尽可能明确管理员所执行的操作的责任，应确保创建个人管理员帐户。对于控制台访问、固件升级和启动配置管理，这种类型的访问权限尤其重要。

虚拟机管理程序

虚拟机管理程序是实现并控制实际软件虚拟化的固件层。虚拟机管理程序包含以下组件：

- 在固件中实现并由系统的 CPU 支持的实际虚拟机管理程序。
- 在控制域中运行以配置虚拟机管理程序的内核模块。
- 在 I/O 域和服务器中运行以提供虚拟化 I/O 的内核模块和守护进程，以及通过逻辑域通道 (Logical Domain Channel, LDC) 通信的内核模块。
- 在来宾域中运行以访问虚拟化 I/O 设备的内核模块和设备驱动程序，以及通过 LDC 通信的内核模块。

威胁：突破隔离

攻击者可以突破虚拟机管理程序提供的隔离的运行时环境，劫持来宾域或整个系统。这种威胁可能会导致最严重的系统损坏。

评估：突破隔离

模块化的系统设计可以向来宾域、虚拟机管理程序和控制域授予不同级别的特权，从而加强隔离。每个功能模块都是在独立的可配置内核模块、设备驱动程序或守护进程中实现的。这种模块化要求干净的 API 以及简单的通信协议，以此降低整体错误风险。

即使利用某个错误的可能性看起来不存在，可能的损坏也可能导致攻击者控制整个系统。

对策：验证固件和软件签名

即使可以直接从 Oracle Web 站点下载系统固件和 OS 修补程序，这些修补程序也可能被操纵。在安装软件之前，请确保验证软件包的 MD5 校验和。所有可下载软件的校验和都是由 Oracle 发布的。

对策：验证内核模块

Oracle VM Server for SPARC 使用多个驱动程序和内核模块来实现整个虚拟化系统。随 Oracle Solaris OS 分发的所有内核模块和大多数二进制文件都带有数字签名。使用 `elfsign` 实用程序可以检查每个内核模块和驱动程序的数字签名。可以使用 Oracle Solaris 11 `pkg verify` 命令检查 Oracle Solaris 二进制文件的完整性。请参见 `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`。

首先，必须建立 `elfsign` 实用程序的完整性。使用基本审计和报告工具 (basic audit and reporting tool, BART) 实现数字签名验证过程自动化。《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`)（《将 BART 与 Solaris 10 操作系统中的 Solaris 指纹数据库集成》）介绍了如何结合 BART 与 Solaris 指纹数据库以自动执行类似的完整性检

查。虽然该指纹数据库已经停用，但可以继承本文档中描述的概念，以类似的方式使用 `elfsign` 和 BART。

控制域

经常承担 I/O 域和服务域角色的控制域必须保持安全，因为控制域可以修改虚拟机管理程序的配置，而后者可控制所有连接的硬件资源。

威胁：控制域拒绝服务

关闭控制域可能导致配置工具拒绝服务。因为只有配置更改需要控制域，因此，如果来宾域通过其他服务域访问其网络和磁盘资源，则来宾域不受影响。

评估：控制域拒绝服务

通过网络攻击控制域等效于攻击其他任何受正当保护的 Oracle Solaris OS 实例。控制域关闭或类似拒绝服务之类的损坏相对较小。但是，如果控制域还承担来宾域的服务域角色，则这些来宾域会受影响。

对策：保护控制台访问安全

避免配置对执行环境的域的管理网络访问权限。这种情形需要使用针对控制域的 ILOM 控制台服务来执行所有管理任务。通过使用在控制域上运行的 `vntsd` 服务，仍可对其他所有域进行控制台访问。

请认真考虑此选项。虽然此选项可降低通过管理网络攻击的风险，但一次只有一个管理员可以访问控制台。

有关安全配置 `vntsd` 的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“如何启用虚拟网络终端服务器守护进程”。

Logical Domains Manager

Logical Domains Manager 在控制域中运行，可用于配置虚拟机管理程序，以及创建和配置所有域及其硬件资源。确保记录并监视 Logical Domains Manager 使用情况。

威胁：未经授权使用配置实用程序

攻击者可能会获取管理员用户 ID 的控制权，其他组中的管理员也可能获取对其他系统的未经授权访问权限。

评估：未经授权使用配置实用程序

确保通过实施妥善维护的身份管理，使管理员不会拥有不必要的系统访问权限。此外，还要实施严格的精细访问控制及其他措施（如两人规则）。

对策：应用两人规则

考虑使用权限对 Logical Domains Manager 和其他管理工具实施两人规则。Enforcing a Two Man Rule Using Solaris 10 RBAC (`https://blogs.oracle.com/gbrunett/entry/enforcing_a_two_man_rule`)（使用 Solaris 10 RBAC 强制实施双人规则）。此规则可防御社交工程攻击、管理帐户受损和人为错误。

对策：使用 Logical Domains Manager 权限

通过使用 `ldm` 命令的权限，可以实现精细访问控制，并维护完整的可跟踪性。有关配置权限的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》。使用权限可帮助防止人为错误，因为并非所有管理员都能使用 `ldm` 命令的所有功能。

对策：强化 Logical Domains Manager

禁用不必要的域管理器服务。Logical Domains Manager 为域访问、监视和迁移提供网络服务。禁用网络服务可将 Logical Domains Manager 的攻击面减少到其正常操作所需的最低水平。这种情形会遇到拒绝服务攻击以及其他滥用这些网络服务的企图。

注 - 虽然禁用域管理器服务有助于减少攻击面，但在任何特定的配置中，无法预料这样做的全部副作用。

不使用以下任一网络服务时，请将其禁用：

- TCP 端口 `8101` 上的迁移服务

  要禁用此服务，请参见 `ldmd`(1M) 手册页中的 `ldmd/incoming_migration_enabled` 和 `ldmd/outgoing_migration_enabled` 属性说明。
- TCP 端口 `6482` 上的可扩展消息处理现场协议 (Extensible Messaging and Presence Protocol, XMPP) 支持

  有关如何禁用此服务的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“XML 传输”。

  请注意，禁用 XMPP 会阻止您使用某些关键 Oracle VM Server for SPARC 功能，例如域迁移、内存动态重新配置以及 `ldm init-system` 命令。禁用 XMPP 也会阻止 Oracle VM Manager 或 Ops Center 管理系统。
- UDP 端口 `161` 上的简单网络管理协议 (Simple Network Management Protocol, SNMP)

确定是否要使用 Oracle VM Server for SPARC 管理信息库 (Management Information Base, MIB) 观察域。此功能需要启用 SNMP 服务。根据您的选择，执行以下操作之一：

- 启用 SNMP 服务以使用 Oracle VM Server for SPARC MIB。安全地安装 Oracle VM Server for SPARC MIB。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“如何安装 Oracle VM Server for SPARC MIB 软件包”和《Oracle VM Server for SPARC 3.2 管理指南 》中的“管理安全性”。
- 禁用 SNMP 服务。有关如何禁用此服务的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“如何删除 Oracle VM Server for SPARC MIB 软件包”。

- 多播地址 `239.129.9.27` 和端口 `64535` 上的发现服务

注 - 请注意，`ldmd` 守护进程也会使用此搜索机制来检测自动分配 MAC 地址时的冲突。如果禁用搜索服务，则 MAC 地址冲突检测将失效，自动 MAC 地址分配也将因此失效。

您无法在 Logical Domains Manager 守护进程 `ldmd` 运行时禁用此服务。不过，使用 Oracle Solaris 的 IP 过滤器功能可阻止访问此服务，这可将 Logical Domains Manager 的攻击面减小到最低限度。阻止访问可防止对实用程序的未授权使用，这可以有效地计算拒绝服务攻击次数和误用这些网络服务的其他尝试次数。请参见《Oracle Solaris Administration: IP Services 》中的第 20 章 “IP Filter in Oracle Solaris (Overview)”和《Oracle Solaris Administration: IP Services 》中的“Using IP Filter Rule Sets”。

另请参见“对策：保护 ILOM 安全” [24]。

对策：审计 Logical Domains Manager

保护 Logical Domains Manager 对整个系统的安全至关重要。必须记录对 Oracle VM Server for SPARC 配置的任何更改以便跟踪恶意操作。定期扫描审计日志，并将日志复制到独立的系统进行安全归档。有关更多信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的第 2 章 “Oracle VM Server for SPARC 安全”。

服务域

服务域可以为系统上的来宾域提供一些虚拟服务。这些服务可能包括虚拟交换机、虚拟磁盘或虚拟控制台服务。

图 1-6 “服务域示例” 显示了提供控制台服务的服务域示例。控制域经常会承载控制台服务，因此也是一种服务域。执行环境域经常会组合一个或两个域中的控制域、I/O 域和服务域的功能。

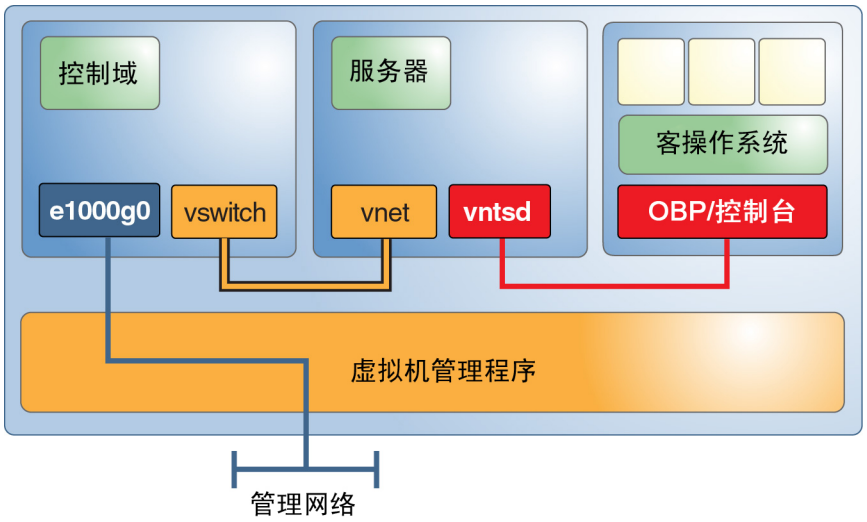
威胁：操纵服务域

获取了服务域控制权的攻击者可以操纵数据或者侦听通过提供的服务发生的任何通信。这种控制权可能包括对来宾域的控制台访问、对网络服务的访问或者对磁盘服务的访问。

评估：操纵服务域

虽然与针对控制域的攻击的攻击策略相同，但可能造成的损害更小，因为攻击者无法修改系统配置。产生的损害可能包括服务域正在提供的数据被盗或受操纵，但不包括对任何数据源的操纵。根据具体的服务，攻击者可能需要交换内核模块。

图 1-6 服务域示例



对策：精细划分服务域

如有可能，让每个服务域仅为其客户机提供一项服务。此配置可保证在服务域遭破坏时，只能损坏一项服务。但是，请确保权衡好此类型配置的重要性与增加的复杂性。请注意，强烈推荐拥有冗余 I/O 域。

对策：隔离服务域和来宾域

可以同时将 Oracle Solaris 10 和 Oracle Solaris 11 服务域与来宾域隔离。以下解决方案按实现的首选顺序显示：

- 确保服务域和来宾域不共享同一个网络端口。此外，也不要在服务域上检测任何虚拟交换机接口。对于 Oracle Solaris 11 服务域，不要在用于虚拟交换机的物理端口上检测任何 VNIC。
- 如果必须将同一个网络端口同时用于 Oracle Solaris 10 OS 和 Oracle Solaris 11 OS，则可将 I/O 域通信流量放在来宾域未使用的 VLAN 中。
- 如果不能实现以前的任一解决方案，则不要在 Oracle Solaris 10 OS 中检测虚拟交换机，并在 Oracle Solaris 11 OS 中应用 IP 过滤器。

对策：限制对虚拟控制台的访问

确保将单个虚拟控制台的访问权限仅限于必须访问这些虚拟控制台的用户。此配置可确保单个管理员不能访问所有控制台，从而可防止访问分配给受损帐户的控制台以外的其他控制台。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“如何创建默认服务”。

I/O 域

可直接访问物理 I/O 设备（如网络端口或磁盘）的任何域都是 I/O 域。有关配置 I/O 域的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的第 5 章 “配置 I/O 域”。

如果某个 I/O 域向来宾域提供 I/O 服务（这将授予域访问硬件的权限），则该 I/O 域也可能是服务域。

威胁：遇到 I/O 域或服务域拒绝服务

阻止 I/O 域的 I/O 服务的攻击者可确保同等阻止所有依赖的来宾域。通过让后端网络或磁盘基础结构过载，或者向域中注入错误，可能成功实现 DoS 攻击。攻击可能会强制将域挂起，或者使域出现紧急情况。同样，暂挂了某个服务域的服务的攻击者会导致依赖于这些服务的任何来宾域立即挂起。如果来宾域挂起，则将在 I/O 服务恢复时恢复操作。

评估：遇到 I/O 域或服务域拒绝服务

DoS 攻击通常通过网络进行。因为网络端口开放用于通信，可能会不堪网络通信流量的重负，因此此类攻击可能会成功。因此而导致的服务丢失会阻止依赖的来宾域。对磁盘

资源的类似攻击可以通过 SAN 基础结构或者通过攻击 I/O 域进行。造成的唯一损害是暂时停止所有依赖的来宾域。虽然 DoS 任务造成的影响可能会很严重，但是数据既不会丢失，也不会受损，系统配置保持不变。

对策：精细配置 I/O 域

配置多个 I/O 域可减轻一个域发生故障或受损造成的影响。可以将单个 PCIe 插槽分配给来宾域，为其提供 I/O 域功能。如果拥有 PCIe 总线的根域崩溃，则将重置该总线，从而导致随后分配有单个插槽的域崩溃。有了此功能，并不意味着完全不需要两个各自拥有独立 PCIe 总线的根域。

对策：配置冗余硬件和根域

高可用性也有助于增强安全性，因为可以确保服务能承受拒绝服务攻击。Oracle VM Server for SPARC 实现了一些高可用性方法，例如，使用冗余磁盘以及冗余 I/O 域中的网络资源。利用此配置选项，可以滚动升级 I/O 域，防止受到由于成功的 DoS 攻击而发生故障的 I/O 域的影响。随着 SR-IOV 的出现，来宾域可以直接访问单个 I/O 设备。但是，当不能选择 SR-IOV 时，可考虑创建冗余 I/O 域。请参见“对策：精细划分服务域” [29]。

威胁：操纵 I/O 域

I/O 域可以直接访问后端设备（通常是磁盘）；I/O 域将这些设备虚拟化，然后将其提供给来宾域。成功的攻击者拥有这些设备的完全访问权限，可以读取来宾域的引导磁盘上的敏感数据或操纵其上的软件。

评估：操纵 I/O 域

在成功攻击了服务域或控制域后，可能会发生 I/O 域攻击。I/O 域是一个有吸引力的目标，因为成功攻击 I/O 域就可以访问大量的磁盘设备。因此，在处理虚拟化磁盘上运行的来宾域中的敏感数据时，要考虑这种威胁。

对策：保护虚拟磁盘

在 I/O 域受损时，攻击者将拥有对来宾域的虚拟磁盘的完全访问权限。

可通过以下措施保护虚拟磁盘的内容：

- **将虚拟磁盘内容加密。**在 Oracle Solaris 10 系统上，可以使用能将自己的数据加密的应用程序，如 `pgp`/`gpg` 或 Oracle 11g 加密表空间。在 Oracle Solaris 11 系统上，可以使用 ZFS 加密数据集，为文件系统中存储的所有数据提供透明的加密。

- **将数据分布在跨不同 I/O 域的多个虚拟磁盘上。**来宾域可以创建条带化的 (RAID 1/RAID 5) 卷；该卷在从两个 I/O 域获取的多个虚拟磁盘上条带化。当其中一个 I/O 域受损时，攻击者将难以利用可用数据部分。

来宾域

虽然来宾域不属于执行环境，但是，由于它们连接到网络，因此最可能成为攻击目标。破坏了虚拟化系统的攻击者可以发起对执行环境的攻击。

对策：保护来宾域 OS 安全

来宾域上的操作系统常常是防御攻击的第一条防线。除了源自数据中心内部的攻击以外，攻击者必须攻入具有外部连接的来宾域，然后才能尝试突破来宾域隔离，攻占整个环境。因此，必须强化来宾域的 OS。

要进一步强化 OS，可以将应用程序部署在 Solaris 区域中，这将在应用程序的网络服务与来宾域的操作系统之间增加一个隔离层。成功攻击服务将仅破坏该区域，而不会破坏底层操作系统，从而可以防止攻击者将控制权扩大到分配给该区域的资源以外。因此，最终将增加突破来宾域隔离的难度。有关如何保护客操作系统的更多信息，请参见《Oracle Solaris 10 Security Guidelines》和《Oracle Solaris 11 Security Guidelines》。

♦ ♦ ♦ 第 2 章

2 安全安装和配置 Oracle VM Server for SPARC

本章介绍了与安装和配置 Oracle VM Server for SPARC 软件相关的安全注意事项。

安装

Oracle VM Server for SPARC 软件作为 Oracle Solaris 10 或 Oracle Solaris 11 软件包自动安全安装。安装完成后，必须拥有管理员特权才能为域配置权限、审计和授权功能。默认情况下不启用这些功能。

安装后配置

安装 Oracle VM Server for SPARC 软件之后，请执行以下任务以确保软件使用尽可能安全：

- 使用所需的虚拟 I/O 服务（例如，虚拟交换机、虚拟磁盘服务器和虚拟控制台集中器服务）配置控制域。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的第 3 章 “设置服务和控制域”。
- 配置来宾域。请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的第 4 章 “设置来宾域”。

  您可以使用虚拟交换机通过管理网络和生产网络配置来宾域。在这种情况下，使用生产网络接口创建的虚拟交换机将作为虚拟交换机网络设备。请参见“对策：配置专用管理网络” [23]。

  如果来宾域的任何虚拟磁盘受到影响，则该来宾域的安全也会受到影响。因此，确保将虚拟磁盘（与网络连接的存储、本地存储的磁盘映像文件或物理磁盘）存储在安全位置。

  默认情况下禁用 `vntsd` 守护进程。启用此守护进程后，任何登录到控制域的用户均有权连接到来宾域的控制台。要防止发生此类型的访问，请确保禁用 `vntsd` 守护进程，或使用权限限制控制台连接，仅允许批准的用户访问控制台。
- 默认情况下的服务处理器 (service processor, SP) 配置是安全的。有关使用 Integrated Lights Out Management (ILOM) 软件管理 SP 的信息，请参见以下网页中适用于您平台的文档：`http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html`。

♦ ♦ ♦ 第 3 章

3 开发者需要注意的安全事项

本章提供的信息适用于为 Oracle VM Server for SPARC 软件创建应用程序的开发者。

Oracle VM Server for SPARC XML 接口

可以创建外部程序，这些程序通过可扩展标记语言 (Extensible Markup Language, XML) 与 Oracle VM Server for SPARC 软件交互。XML 使用可扩展消息处理现场协议 (Extensible Messaging and Presence Protocol, XMPP)。

攻击者可能会尝试使用此网络协议访问系统，因此，应考虑禁用 XMPP。有关禁用 XMPP 的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“XML 传输”。有关 Logical Domains Manager 所使用的安全机制的信息，请参见《Oracle VM Server for SPARC 3.2 管理指南 》中的“XMPP 服务器”。

请注意，禁用 XMPP 会阻止您使用某些关键 Oracle VM Server for SPARC 功能，例如域迁移、内存动态重新配置以及 `ldm init-system` 命令。禁用 XMPP 也会阻止 Oracle VM Manager 或 Ops Center 管理系统。

♦ ♦ ♦ 附 录 A

安全部署核对表

此核对表汇总了强化 Oracle VM Server for SPARC 环境可采取的步骤。在其他文档中提供了详细信息，这些文档如下：

- 《Oracle VM Server for SPARC 3.2 管理指南》
- 《Oracle Solaris 10 Security Guidelines》
- 《Oracle Solaris 11 Security Guidelines》

Oracle VM Server for SPARC 安全核对表

- 对来宾域执行 Oracle Solaris OS 强化步骤，就像您在非虚拟化环境中所做的一样。
- 使用 "LDoms Management"（LDoms 管理）和 "LDoms Review"（LDoms 查看）权限配置文件将合适的特权委派给用户。
- 使用权限来限制对域的控制台访问：只能对 Oracle VM Server for SPARC 管理员必须访问的域提供控制台访问。
- 为 Oracle VM Server for SPARC 启用 Oracle Solaris OS 审计功能。
- 禁用不必要的域管理器服务。
- 仅将安全类相同的来宾域部署到一个物理平台。
- 确保在执行环境的管理网络与来宾域之间没有网络连接。
- 仅将必需的资源分配给来宾域。