Oracle® VM Server for SPARC 3.0 安全指南

文件号码 E37593
2012 年 12 月

ORACLE

130417@25097

目录

前言

《Oracle VM Server for SPARC 3.0 安全指南》介绍了如何安全安装、配置和使用 Oracle VM Server for SPARC 3.0 软件的信息。

相关文档

下表显示了 Oracle VM Server for SPARC 3.0 发行版可用的相关文档。

表 P–1 相关文档

应用	书名
Oracle VM Server for SPARC 3.0 软件	《Oracle VM Server for SPARC 3.0 管理指南》 《Oracle VM Server for SPARC 3.0 安全指南》 《Oracle VM Server for SPARC 3.0 Reference Manual》 《Oracle VM Server for SPARC 3.0 发行说明》
Oracle VM Server for SPARC 3.0 `drd`(1M) 和 `vntsd`(1M) 手册页	Oracle Solaris OS 参考手册： ■ Oracle Solaris 10 Documentation（Oracle Solaris 10 文档） ■ Oracle Solaris 11 Documentation（Oracle Solaris 11 文档）
Oracle Solaris OS：安装和配置	Oracle Solaris OS 安装和配置指南： ■ Oracle Solaris 10 Documentation（Oracle Solaris 10 文档） ■ Oracle Solaris 11 Documentation（Oracle Solaris 11 文档）
Oracle VM Server for SPARC 和 Oracle Solaris OS 安全	Oracle VM Server for SPARC 白皮书和 Oracle Solaris OS 安全指南： ■ 《Secure Deployment of Oracle VM Server for SPARC》(`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf`)（《Oracle VM Server for SPARC 安全部署》） ■ 《Oracle Solaris 10 Security Guidelines》 ■ 《Oracle Solaris 11 Security Guidelines》

可以从 http://www.oracle.com/technetwork/indexes/documentation/index.html 查找与您的服务器、软件或 Oracle Solaris OS 相关的文档。使用 "Search"（搜索）框查找所需的文档和信息。

可以访问 Oracle VM Server for SPARC 的论坛，地址为 http://forums.oracle.com/forums/forum.jspa?forumID=1047。

获取 Oracle 支持

Oracle 客户可以通过 My Oracle Support 访问电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info，或者，如果您有听力障碍，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

印刷约定

下表介绍了本书中的印刷约定。

表 P–2 印刷约定

字体或符号	含义	示例
`AaBbCc123`	命令、文件和目录的名称；计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`
`AaBbCc123`	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name%` **`su`** `Password:`
aabbcc123	要使用实名或值替换的命令行占位符	删除文件的命令为 `rm` *filename*。
AaBbCc123	保留未译的新词或术语以及要强调的词	这些称为 *Class* 选项。 **注意**：有些强调的项目在联机时以粗体显示。
新词术语强调	新词或术语以及要强调的词	**高速缓存**是存储在本地的副本。 请**勿**保存文件。
《书名》	书名	阅读《用户指南》的第 6 章。

命令中的 shell 提示符示例

下表显示了 Oracle Solaris OS 中包含的缺省 UNIX shell 系统提示符和超级用户提示符。请注意，在命令示例中显示的缺省系统提示符可能会有所不同，具体取决于 Oracle Solaris 发行版。

表 P–3 shell 提示符

shell	提示符
Bash shell、Korn shell 和 Bourne shell	`$`
Bash shell、Korn shell 和 Bourne shell 超级用户	`#`
C shell	`machine_name%`
C shell 超级用户	`machine_name#`

◆ ◆ ◆ 第 1 章

Oracle VM Server for SPARC 安全概述

本章介绍了 Oracle VM Server for SPARC 软件使用的以下安全功能：

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，可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》。

必须在控制域中运行 `ldm` 命令才能配置逻辑域和检索状态信息。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，请使用 Oracle VM Server for SPARC 安全功能，例如，Oracle Solaris 中针对控制台的基于角色的访问控制 (role-based access control, RBAC) 功能和 `solaris.ldoms` 授权。请参见《Oracle VM Server for SPARC 3.0 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 安全性的完整信息，请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）。

- 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。
- 要限制对 Oracle VM Server for SPARC 管理命令和域控制台的访问并启用 Oracle VM Server for SPARC 审计功能，请参见《Oracle VM Server for SPARC 3.0 管理指南》中的第 3 章 “Oracle VM Server for SPARC 安全”。

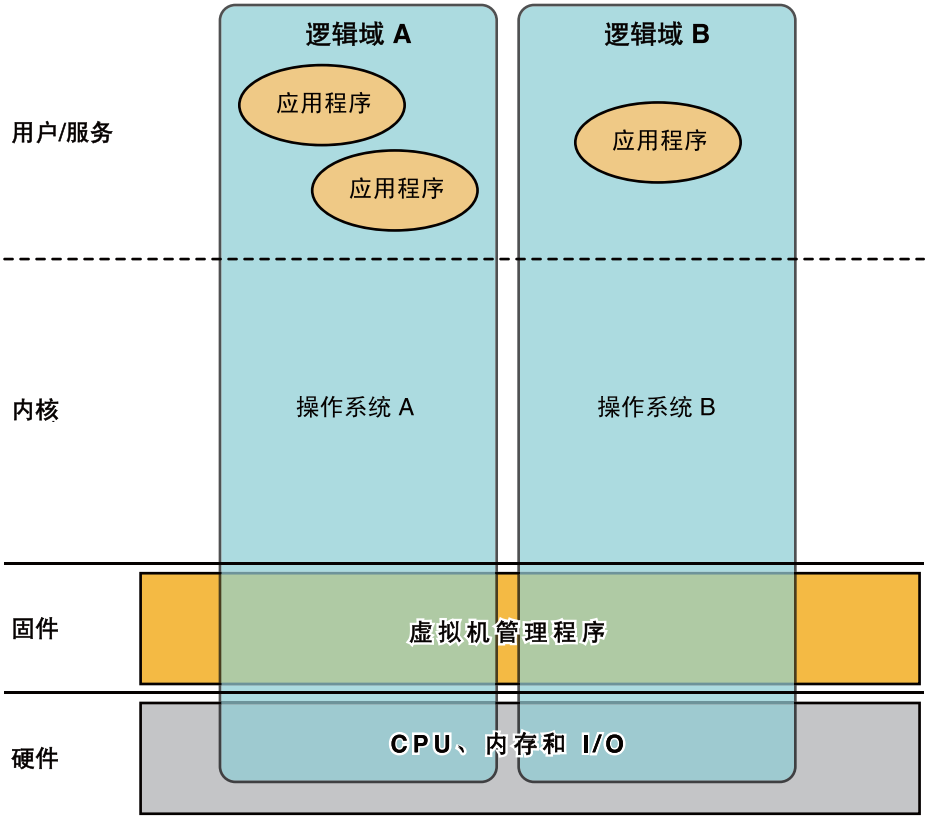
Oracle VM Server for SPARC 产品概述

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最多 128 个虚拟服务器（称为逻辑域）。这种配置使您能够利用由 SPARC T 系列服务器和 Oracle Solaris OS 提供的海量线程缩放。

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，而无需关闭再打开服务器电源。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 3.0 管理指南》和《Oracle VM Server for SPARC 3.0 Reference Manual》。有关必需硬件和软件的信息，请参见《Oracle VM Server for SPARC 3.0 发行说明》。

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，但不管理逻辑域。Logical Domains Manager 管理逻辑域。

- **控制域。**Logical Domains Manager 在此域中运行，以便您可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，或可以通过使用直接 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 3.0 管理指南》中的“分配 PCIe 端点设备”。

  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 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 Sun SPARC Enterprise T5440 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。它只有虚拟 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。这些因素构成了总体 Oracle VM Server for SPARC 配置的安全级别，可对此配置应用以下常规安全原则中的部分原则：

- **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《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 "Counter Measure #1: Operational Guidelines"（“第 1 项计数器措施：运行准则”）。
  - 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《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Threat #2: Errors in the Architecture of the Virtual Environment”（“第 2 项威胁：虚拟环境体系结构中的错误”）介绍的计数器措施。
  - 谨慎规划要分配的资源以及是否要对其进行共享。请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Counter Measure #7: Carefully Assigning Hardware Resources” 和 “Counter Measure #8: Careful Assignment of Shared Resources”（“第 7 项计数器措施：谨慎分配硬件资源”和“第 8 项计数器措施：谨慎分配共享资源”）。

- 通过应用《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Threat #4: Manipulation of the Execution Environment” 和 “Counter Measure #28: Securing the Guest OS”（“第 4 项威胁：操控执行环境”和“第 28 项计数器措施：确保客操作系统安全”）介绍的计数器措施，确保逻辑域免受操控。
- 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。
- 按照《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Counter Measure #15: Validating Firmware and Software Signatures” 和 “Counter Measure #16: Validating Kernel Modules”（“第 15 项计数器措施：验证固件和软件签名”和“第 16 项计数器措施：验证内核模块”）所述保护虚拟机管理程序的核心。
- 保护控制域免遭拒绝服务攻击。请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Counter Measure #17: Console Access”（“第 17 项计数器措施：控制台访问”）。
- 确保未授权用户无法运行 Logical Domains Manager。请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Threat #8: Unauthorized Use of Configuration Utilities”（“第 8 项威胁：未经授权使用配置实用程序”）。
- 确保未授权用户或进程无法访问服务域。请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Threat #9: Manipulation of a Service Domain”（“第 9 项威胁：操控服务域”）。
- 保护 I/O 域或服务域免遭拒绝服务攻击。请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Threat #10: Denial-of-Service of IO Domain or Service Domain”（“第 10 项威胁：I/O 域或服务域拒绝服务”）。
- 确保未授权用户或进程无法访问 I/O 域。请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Threat #11: Manipulation of an IO Domain”（“第 11 项威胁：操控 I/O 域”）。
- 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。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

要禁用此服务，请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“XML 传输”。

- 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 3.0 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 3.0 管理指南》中的“管理安全性”。
  - **禁用 SNMP 服务**。要禁用此服务，请参见《Oracle VM Server for SPARC 3.0 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

  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《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Counter Measure #14: Securing the ILOM” 和 “Counter Measure #20: Hardening LDoms Manager”（“第 14 项计数器措施：保护 ILOM”和“第 20 项计数器措施：强化 LDoms Manager”）。

- **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，可创建隔离违规，从而防止域跨不同的安全类。请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Counter Measure #2: Carefully Assigning Guests to Hardware Platforms”（“第 2 项计数器措施：为来宾域谨慎分配硬件平台”）。
  - 使用 RBAC 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 3.0 管理指南》中的“使用权限配置文件和角色”。

- 使用 RBAC 限制对域的控制台访问：只对 Oracle VM Server for SPARC 管理员必须访问的域提供控制台访问。请勿对所有域提供通用访问。请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“使用权限配置文件和角色”。
- **监视系统活动。**

  启用 Oracle VM Server for SPARC 审计。请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“启用并使用审计”。

有关安全部署 Oracle VM Server for SPARC 软件的建议，请参见《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的“Recommended Deployment Options”（“建议的部署选项”）。

◆ ◆ ◆ 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 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，您必须具有管理员特权才能使用基于角色的访问控制 (role-based access control, RBAC)、审计和授权功能来配置域。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 3.0 管理指南》中的第 4 章 “设置服务和控制域”。
- 配置来宾域。请参见《Oracle VM Server for SPARC 3.0 管理指南》中的第 5 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《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）中的 “Counter Measure #13: Dedicated Management Network”（“第 13 项计数器措施：专用管理网络”）。

  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 RBAC 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 Oracle VM Server for SPARC 安全功能

本章概述了 Oracle VM Server for SPARC 软件使用的安全功能。

有关验证、访问控制和审计的信息，请参见《Oracle VM Server for SPARC 3.0 管理指南》中的第 3 章 “Oracle VM Server for SPARC 安全”。

安全模型

Oracle VM Server for SPARC 软件建立在 Oracle Solaris OS 内置的安全模型和功能之上。有关 Oracle Solaris OS 安全准则的信息，请参见《Oracle Solaris 11 Security Guidelines》和《Oracle Solaris 10 Security Guidelines》。

配置并使用验证

与裸机 Oracle Solaris 安装一样，任何具有帐户的用户均可登录到逻辑域，甚至是控制域。Oracle VM Server for SPARC 软件不会创建任何用户帐户。请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“安装 Logical Domains Manager”。有关如何保护 Oracle Solaris 用户的信息，请参见《Oracle Solaris 11 Security Guidelines》中的“Securing Users”。

要在控制域上使用 Logical Domains Manager 执行域管理活动，必须授予用户读取和写入配置数据的特定特权。请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“Logical Domains Manager 配置文件内容”和《Oracle VM Server for SPARC 3.0 管理指南》中的“使用权限配置文件和角色”。

配置并使用 RBAC

可以使用 Oracle Solaris OS 基于角色的访问控制 (role-based access control, RBAC) 功能来管理授权和权限配置文件并为用户帐户分配角色。有关 RBAC 的信息，请参见《System Administration Guide: Security Services》中的第 9 章 “Using Role-Based Access Control (Tasks)”。

安装 Logical Domains Manager 会向本地文件中添加必需的授权和权限配置文件。请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“使用权限配置文件和角色”。

要在命名服务中配置用户、授权、权限配置文件和角色，请参见《System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)》。

配置并使用审计

您应在来宾域中管理和审计 Oracle Solaris 实例，就像您在裸机系统上运行的 Oracle Solaris OS 中所做的一样。您可以定制 Oracle Solaris OS 审计功能，以便仅审计那些对您的环境至关重要的功能和系统服务。对于 Oracle VM Server for SPARC，确保审计虚拟化软件类。您可以执行其他审计相关的任务。请参见《Oracle Solaris 11 Security Guidelines》中的“Using the Audit Service”和《Oracle Solaris 11 Security Guidelines》中的“How to Audit Significant Events in Addition to Login/Logout”。

Logical Domains Manager 创建审计事件并将其传送给 Oracle Solaris 审计子系统以供存储和日后检查。这些历史记录保存在日志中，其中包括执行的操作、完成时间、执行者以及产生的后果。请注意，您**无法**从系统的控制域查看其所有域的审计信息。

因此，对于系统中的每个域，您可以基于系统上运行的 Oracle Solaris OS 的版本，按如下方式启用和禁用审计功能：

- **Oracle Solaris 10 OS**。使用 `bsmconv` 或 `bsmunconv` 命令。请参见 `bsmconv(1M)` 和 `bsmunconv(1M)` 手册页，以及 Oracle Solaris 10 版的《系统管理指南：安全性服务》。
- **Oracle Solaris 11 OS**。使用 `audit` 命令。请参见 `audit(1M)` 手册页，以及 Oracle Solaris 11 版的《系统管理指南：安全性服务》。

有关更多信息，请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“启用并使用审计”。

配置并使用其他安全功能

Oracle VM Server for SPARC 保护特定虚拟化功能的使用。如果启用了 `vntsd`，默认情况下将以最安全的配置来配置该守护进程。它只接受来自控制域的连接，而不接受通过网络的连接。如果需要，您可以配置一个安全性较低的选项，以允许网络连接。请参见 `vntsd(1M)` 手册页中 `vntsd/listen_addr` 属性的说明。

配置 `vntsd` 接受网络连接时要谨慎。为达到最佳安全性，最好仅允许来自控制域的连接，或禁用 `vntsd`。请参见第 12 页中的 “将常规安全原则应用到 Oracle VM Server for SPARC”。

Oracle VM Server for SPARC 域迁移功能使用安全措施。源计算机上的 Logical Domains Manager 接受迁移域的请求，并建立与目标计算机上运行的 Logical Domains Manager 的安全网络连接。在建立此连接之后，将进行迁移。这些安全连接使用验证和加密功能创建。请参见《Oracle VM Server for SPARC 3.0 管理指南》中的“迁移操作安全性”。

需要特别指出的是，域迁移操作在默认情况下使用安全套接字层 (Secure Sockets Layer, SSL) 加密通过网络发送和接收的所有通信流量。您可以通过将加密单元分配给支持加密单元的系统控制域来提高迁移性能。

不需要域迁移时，可禁用迁移功能以阻止 `ldmd` 进程在迁移端口上侦听。

如果您使用域迁移，请确保 `ldmd` 守护进程配置为在迁移期间要求密码验证。这是默认行为。

◆ ◆ ◆ 第 4 章

4 开发者需要注意的安全事项

本章介绍了有助于开发者针对 Oracle VM Server for SPARC 软件创建应用程序的信息。

Oracle VM Server for SPARC XML 接口

您可创建通过可扩展标记语言 (Extensible Markup Language, XML) 通信机制与 Oracle VM Server for SPARC 软件衔接的外部程序，该机制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，您需要考虑禁用 XMPP。有关禁用 XMPP 的信息，请参见《Oracle VM Server for SPARC 3.0 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 3.0 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。

◆ ◆ ◆ 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 3.0 管理指南》
- 《Oracle Solaris 10 Security Guidelines》
- 《Oracle Solaris 11 Security Guidelines》
- 《Secure Deployment of Oracle VM Server for SPARC》（《Oracle VM Server for SPARC 安全部署》）

Oracle VM Server for SPARC 安全核对表

- ❒ 对来宾域执行 Oracle Solaris 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。
- ❒ 使用基于角色的访问控制 (role-based access control, RBAC) 限制对域的控制台访问：只对 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。
- ❒ 在一个物理平台上仅部署同一安全类中的来宾系统。
- ❒ 确保在管理执行环境与来宾域时，两者之间无任何网络连接。
- ❒ 仅将必需的资源分配给来宾系统。