SPARC 和 Netra SPARC T5 系列服务器

安全指南

文件号码： E40472-01
2013 年 4 月

目录

• • • 第 1 章

SPARC 和 Netra SPARC T5 系列服务器安全

本文档提供了有关 SPARC T5-1B、T5-2、T5-4、T5-8 和 Netra SPARC T5-1B 等服务器的一般安全准则。此指南可帮助您在将以上服务器与其他 Oracle 硬件产品（如网络交换机和网络接口卡）一起使用时，确保安全性。

本章包含以下几节：

了解安全原则

有四个基本安全原则：访问、验证、授权和记帐。

- 访问

  物理和软件控件可保护硬件或数据免遭入侵。
  - 对于硬件，访问限制通常意味着物理访问限制。
  - 对于软件，将通过物理和虚拟方法来限制访问。
  - 除非通过 Oracle 更新过程，否则无法更改固件。
- 验证

  所有平台操作系统都提供可设置的验证功能，以确保用户为他们所声明的身份。

  验证通过诸如标记和密码之类的措施提供不同程度的安全性。
- 授权

  授权使公司职员只能使用他们经过培训并有资格使用的硬件和软件。建立一套读/写/执行权限制度，以控制用户对命令、磁盘空间、设备和应用程序的访问。
- 记帐

  使用 Oracle 的软件和硬件记账功能监视登录活动和维护硬件清单。
  - 可通过系统日志监视用户登录。尤其是系统管理员和服务帐户可以访问许多功能强大的命令，应当通过系统日志进行仔细监视。日志通常会被维护较长的一段时间，因此，当日志文件超出合理大小时，有必要根据公司客户的政策定期弃用一些日志文件。

- 通常通过序列号跟踪客户 IT 资产。Oracle 部件号以电子方式记录在所有卡、模块和主板上，并可用于库存目的。

规划安全环境

在安装和配置服务器及相关设备之前和期间内，请遵循以下注意事项。

硬件安全

物理硬件的保护相当简单，只需限制接近硬件并记录序列号即可。

- 限制接近
  - 将服务器和相关设备安装在带锁的房间内并限制随意出入。
  - 如果设备安装在带有门锁的机架中，则除非必须在机架内维修组件，否则应始终锁上机架门。
  - 限制人员接近 USB 控制台，该控制台可提供比 SSH 连接更强大的访问功能。系统控制器、配电设备 (Power Distribution Unit, PDU) 和网络交换机之类的设备都可能有 USB 连接。
  - 限制人员接近热插拔或热交换设备，因为这些设备可以轻易移除。
  - 在带锁的机柜中存储备用现场可更换单元 (Field-Replaceable Unit, FRU) 或客户可更换单元 (Customer-Replaceable Unit, CRU)。仅限经授权的人员接近带锁机柜。
- 记录序列号
  - 保留所有硬件的序列号记录。
  - 为计算机硬件的所有重要物项（如更换部件）添加安全标记。使用特殊的紫外线笔或压纹标签。
  - 将硬件激活密钥和许可证保存在一个安全位置，在系统出现紧急状况时系统管理员可以轻松访问该位置。打印的文档可能是证明所有权的唯一证据。

软件安全

大多数硬件安全都通过软件方法实现。

- 安装新系统时更改所有默认密码。大多数类型的设备都使用默认密码（如 changeme），这些密码广为人知，从而有可能对设备进行未经授权的访问。此外，默认情况下，一些设备（如网络交换机）可能有多个用户帐户。请确保更改所有帐户密码。
- 限制 `root` 超级用户帐户的使用。而应尽可能使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 用户配置文件（如 `operator` 和 `administrator`）。
- 对服务处理器使用专用网络，从而将其与常规网络隔离。
- 请参阅软件随附的文档以启用可用于该软件的任何安全功能。
- 可以使用 WAN Boot 或 iSCSI Boot 安全地引导服务器。
  - 对于 Oracle Solaris 10 发行版，请参阅《*Oracle Solaris* 安装指南：基于网络的安装》一书。
  - 对于 Oracle Solaris 11 发行版，请参阅《安装 *Oracle Solaris 11* 系统》一书了解 WAN Boot 相关信息，参阅《系统管理指南：基本管理》一书了解 iSCSI Boot 相关信息。

《*Oracle Solaris* 安全准则》文档提供有关以下内容的信息：

- 如何强化 Oracle Solaris
- 配置系统时如何使用 Oracle Solaris 安全功能

- 将应用程序和用户添加到系统时如何安全操作
- 如何保护基于网络的应用程序

适用于您要使用的版本的《*Oracle Solaris* 安全准则》文档位于：

- http://www.oracle.com/goto/Solaris11/docs
- http://www.oracle.com/goto/Solaris10/docs

固件安全

Oracle System Firmware 的所有子组件必须一起更新。Oracle System Firmware 使用受控的固件更新过程来防止未经授权的固件修改。只有超级用户或具有相应授权的授权用户才可以使用该更新过程。

Oracle OpenBoot 安全

对 Oracle OpenBoot 固件命令行界面的访问可以使用 OpenBoot 安全变量进行密码保护。

有关设置 OpenBoot 安全变量的信息，请参阅《*OpenBoot 4.x Command Reference Manual*》，网址为：

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM 固件

Oracle Integrated Lights Out Manager (Oracle ILOM) 是预先安装在服务器、服务器模块、模块化系统以及其他 Oracle 硬件上的系统管理固件。借助 Oracle ILOM，可以有效管理和监视系统中安装的组件。您使用 Oracle ILOM 的方式将影响系统的安全性。要了解有关设置密码、管理用户以及应用与安全相关的功能（包括安全 Shell (Secure Shell, SSH)、安全套接字层 (Secure Socket Layer, SSL) 和 RADIUS 验证）时如何使用该固件的更多信息，请参阅 Oracle ILOM 文档：

- http://www.oracle.com/goto/ILOM/docs

维护安全环境

初始安装和设置之后，可以使用 Oracle 硬件和软件安全功能继续控制硬件和跟踪系统资产。

硬件控制

某些 Oracle 系统可设置为通过软件命令打开和关闭。此外，某些系统机柜的配电设备 (Power Distribution Unit, PDU) 也可以通过软件命令远程启用和禁用。这些命令的授权通常在系统配置期间设置，并且通常仅限系统管理员和服务人员使用这些命令。有关详细信息，请参阅系统或机柜文档。

资产跟踪

Oracle 序列号嵌入在位于选件卡和系统主板上的固件中。可以通过局域网连接读取这些序列号以进行库存跟踪。

无线射频识别 (Radio Frequency Identification, RFID) 读取器可以进一步简化资产跟踪。 可从以下位置获取 Oracle 白皮书《*How to Track Your Oracle Sun System Assets by Using RFID*》（《如何使用 RFID 跟踪 Oracle Sun 系统资产》）：

- http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

软件和固件更新

- 定期检查更新。
- 始终在设备上安装软件或固件的最新发行版本。
- 为您的软件安装任何必要的安全修补程序。
- 请记住，网络交换机之类的设备也包含固件，因此也可能需要修补程序和固件更新。

本地和远程访问

请遵循以下准则以确保对系统的本地和远程访问的安全性：

- 创建标题以指出禁止未经授权的访问。
- 在适用的情况下使用访问控制列表。
- 设置扩展会话的超时时间，并设置特权级别。
- 针对交换机的本地和远程访问，使用验证、授权和记帐 (Authentication, Authorization, and Accounting, AAA) 功能。
- 如果可能，使用 RADIUS 和 TACACS+ 安全协议：
  - RADIUS（Remote Authentication Dial In User Service，远程验证拨入用户服务）是一种客户机/服务器协议，可保护网络免受未经授权的访问。
  - TACACS+（Terminal Access Controller Access-Control System，终端访问控制器访问控制系统）是一种协议，它允许远程访问服务器与验证服务器通信，以确定用户是否有权访问网络。
- 对入侵检测系统 (Intrusion Detection System, IDS) 访问使用交换机的端口镜像功能。
- 实施端口安全，以基于 MAC 地址限制访问。对所有端口禁用自动中继。
- 使用 SSH 而非 Telnet 限制只有特定的 IP 地址才可以进行远程配置。Telnet 以明文形式传递用户名和密码，可能使 LAN 段上的每个人都能看到登录凭据。为 SSH 设置强密码。
- SNMP 的早期版本不安全（以未加密的文本形式传输验证数据）。只有 SNMP 的版本 3 可以提供安全传输。
- 某些产品出厂时便将 PUBLIC 设置为默认 SNMP 团体字符串。攻击者可以查询团体以绘制非常完整的网络图，并可能修改管理信息库 (Management Information Base, MIB) 值。如果 SNMP 是必需的，请将默认的 SNMP 团体字符串改为加强的团体字符串。
- 启用日志记录并向专用安全日志主机发送日志。
- 使用 NTP 和时间戳配置日志记录以包含准确的时间信息。
- 查看日志以发现可能的事件，并根据安全策略将其归档。
- 如果系统控制器使用浏览器界面，请确保在使用后注销。

数据安全

请遵循以下准则以最大限度地确保数据安全：

- 使用外部硬盘驱动器、笔式驱动器或记忆棒等设备备份重要数据。将备份的数据存储在另一个不在现场的安全位置。
- 使用数据加密软件确保硬盘驱动器上的机密信息安全。
- 处置旧硬盘驱动器时，请物理销毁该驱动器或彻底清除该驱动器上的所有数据。删除所有文件或重新格式化驱动器将仅删除驱动器上的地址表 – 删除文件或重新格式化驱动器后，仍然可以恢复驱动器中的信息。（使用磁盘擦除软件彻底清除驱动器上的所有数据。）

网络安全

请遵循以下准则以最大限度地确保网络安全：

- 大多数交换机允许您定义虚拟局域网 (Virtual Local Area Network, VLAN)。如果您使用交换机定义 VLAN，请将系统的敏感群集与网络的其余部分隔离。这样可以降低用户访问这些客户机和服务器上信息的可能性。
- 带外管理交换机（与数据通信隔开）。如果带外管理不可行，则专门使用一个单独的 VLAN 号进行带内管理。
- 确保 Infiniband 主机安全。Infiniband 光纤网络的安全程度取决于其安全程度最低的 Infiniband 主机。
- 请注意，分区不会保护 Infiniband 光纤网络。分区只会使主机上各虚拟机之间的 Infiniband 通信相互隔离。
- 脱机维护交换机配置文件，并且仅限授权的管理员访问。该配置文件应包含每个设置的描述性注释。
- 如果可能，使用静态 VLAN 配置。
- 禁用未使用的交换机端口，并为其指定未使用的 VLAN 号。
- 为中继端口指定唯一本机 VLAN 号。
- 将可通过中继传输的 VLAN 仅限于绝对必需的那些 VLAN。
- 如果可能，禁用 VLAN 中继协议 (VLAN Trunking Protocol, VTP)。否则，为 VTP 设置以下内容：管理域、密码和删改。然后将 VTP 设置为透明模式。
- 禁用不必要的网络服务，如 TCP 小型服务器或 HTTP。启用必要的网络服务并以安全方式配置这些服务。
- 不同的交换机将提供不同级别的端口安全功能。如果您的交换机具有以下端口安全功能，请使用这些功能：
  - MAC 绑定 (MAC Locking)：这涉及将一个或多个连接设备的介质访问控制 (Media Access Control, MAC) 地址绑定到交换机上的物理端口。如果将交换机端口绑定到特定的 MAC 地址，超级用户将无法利用非法接入点在您的网络中创建后门。
  - MAC 锁定 (MAC Lockout)：这将禁止指定的 MAC 地址连接到交换机。
  - MAC 学习 (MAC Learning)：使用有关每个交换机端口的直接连接的知识，以便交换机可以基于当前连接设置安全性。