Sun Server X4-8

安全指南

文件号码 E55447-01
2014 年 6 月

目录

基本安全

本文档提供了若干一般安全准则，来帮助您保护 Oracle 服务器、服务器网络接口及其连接的网络交换机。

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

在使用所有硬件和软件时，应遵循一些基本安全原则。本节介绍了以下四个基本安全原则：

访问

访问是指对硬件的物理访问，或对软件的物理或虚拟访问。

- 使用物理和软件控制措施来保护硬件和数据免遭入侵。
- 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，从而可能允许对硬件或软件进行未经授权的访问。
- 参阅软件随附的文档，以启用可用于软件的任何安全功能。
- 将服务器和相关设备安装在带锁并限制随意出入的房间内。
- 如果设备安装在带有门锁的机架中，除非必须维修机架内的组件，否则请始终锁上机架门。
- 限制对 USB 端口、网络端口和系统控制台的物理访问。服务器和网络交换机都有端口和控制台连接，通过这些连接可直接访问系统。
- 限制通过网络重新启动系统的能力。
- 尤其要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被移除。
- 在带锁的机柜中存储备用的现场可更换单元 (field-replaceable unit, FRU) 和客户可更换单元 (customer-replaceable unit, CRU)。仅限经授权的人员接近带锁机柜。

验证

验证就是识别用户的身份，通常是通过用户名和密码等保密信息来进行。验证可确保硬件或软件的用户与其表明的身份相符。

- 在平台操作系统中设置验证功能（如密码系统）以确保用户与其表明的身份相符。
- 确保员工正确使用员工胸卡进入机房。
- 对于用户帐户：酌情使用访问控制列表；对扩展会话设置超时；为用户设置特权级别。

授权

管理员可以通过授权来控制用户可执行或使用哪些任务或权限。用户只能执行为其分配的任务，并使用为其分配的权限。授权是指对用户使用硬件和软件所施加的限制。

- 只允许用户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。

记帐和审计

记帐和审计指的是维护用户在系统中执行的活动的记录。利用 Oracle 服务器的相关软件和硬件功能，管理员可以监视登录活动并维护硬件清单。

- 使用系统日志来监视用户登录。尤其要监视系统管理员和服务帐户，因为这些帐户可以访问一些特定的命令，如果这些命令使用不当，可能导致系统损坏或造成数据丢失。访问活动和命令应该通过系统日志进行细致监控。
- 记录所有硬件的序列号。使用组件序列号来跟踪系统资产。Oracle 部件号以电子方式记录在卡、模块和主板上，并可用于盘点目的。
- 为了检测和跟踪组件，为计算机硬件的所有重要物项（如 FRU）提供安全标记。使用特殊的紫外线笔或压纹标签。

安全使用服务器配置和管理工具

在使用软件和固件工具来配置和管理服务器时，请遵循以下安全准则：

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

Oracle System Assistant 安全性

Oracle System Assistant 是一种预安装的工具，可帮助您配置和更新服务器硬件，以及安装支持的操作系统。有关如何使用 Oracle System Assistant 的信息，请参阅《*Oracle X4* 系列服务器管理指南》，网址为：

http://www.oracle.com/goto/x86AdminDiag/docs

以下信息介绍了与 Oracle System Assistant 相关的安全问题。

- **Oracle System Assistant 包含可引导的根环境。**

  Oracle System Assistant 是一款在预安装的内部 USB 闪存驱动器上运行的应用程序。Oracle System Assistant 建立在可引导的 Linux 根环境基础之上。Oracle System Assistant 还具有访问其底层 root shell 的能力。对系统具有物理访问权限的用户或通过 Oracle ILOM 对系统具有远程 KVMS（keyboard, video, mouse, and storage，键盘、视频、鼠标和存储）访问权限的用户，可以访问 Oracle System Assistant 和 root shell。

  根环境可以用来更改系统配置和策略，还可以用来访问其他磁盘上的数据。为了提高安全性，请对服务器的物理访问采取保护措施，并慎重为 Oracle ILOM 用户分配管理员和控制台特权。

  Oracle System Assistant shell 的设计目的是，允许具有相应权限的用户使用 Oracle Hardware Management Pack CLI Tools 进行系统管理。该 shell 不是设计用来提供网络服务。为确保拥有最高级别的安全性，默认情况下会禁用网络服务且不应启用网络服务。

- **Oracle System Assistant 会挂载一个操作系统可访问的 USB 存储设备。**

  除作为可引导环境外，Oracle System Assistant 还作为 USB 存储设备（闪存驱动器）挂载，安装后主机操作系统可访问此设备。这在访问工具和驱动程序以进行维

护和重新配置时很有用。Oracle System Assistant USB 存储设备既可读取又可写入，因而可能会被病毒利用。

为了提高安全性，请使用保护磁盘的方法来保护 Oracle System Assistant 存储设备，包括定期扫描病毒和检查完整性。

- **可以禁用 Oracle System Assistant。**

  Oracle System Assistant 是一种有用的工具，可帮助设置服务器、更新和配置固件以及安装主机操作系统。但是，如果您不能接受上述安全风险，或不需要此工具，可以禁用 Oracle System Assistant。禁用 Oracle System Assistant 后，主机操作系统将不能再访问此 USB 存储设备，而用户将无法引导至 Oracle System Assistant。

  您可以通过 Oracle System Assistant 工具本身或通过 BIOS 禁用该工具。一旦禁用了 Oracle System Assistant，只能从 BIOS 设置实用程序重新启用它。建议使用密码保护 BIOS 设置实用程序，以便只有授权用户才能重新启用 Oracle System Assistant。

- **参阅 Oracle System Assistant 文档。**

  有关 Oracle System Assistant 各种特性和功能的更多信息，请参阅《*Oracle X4* 系列服务器管理指南》，网址为：

  http://www.oracle.com/goto/x86AdminDiag/docs

Oracle ILOM 安全性

您可以使用 Oracle Integrated Lights Out Manager (ILOM) 管理固件（已嵌入到基于 x86 的 Oracle 服务器以及基于 SPARC 的 Oracle 服务器上）来主动保护、管理和监视系统组件。根据授予系统管理员的授权级别，这些功能可能包括关闭服务器电源、创建用户帐户、挂载远程存储设备等。

- **使用安全的内部可信网络。**

  无论通过本地串行端口、专用网络管理端口还是标准数据网络端口与 Oracle ILOM 建立物理管理连接，服务器上的此物理端口要始终连接到内部的可信网络或者专用安全管理或专用网络，这一点至关重要。

  绝不要将 Oracle ILOM 服务处理器 (service processor, SP) 连接到公共网络，比如 Internet。应确保 Oracle ILOM SP 管理通信始终位于单独的管理网络上并仅授予系统管理员访问权限。

- **限制对默认管理员帐户的使用。**

  默认管理员帐户 (`root`) 只能用于 Oracle ILOM 初始登录。提供此默认管理员帐户只是为了帮助进行服务器初始安装。因此，为了确保环境最安全，必须在最初设置系统的过程中更改此默认管理员的密码 (`changeme`)。如果获得了访问默认管理员帐户的权限，用户将可以无限制地访问 Oracle ILOM 的所有功能。此外，还要为每个新的 Oracle ILOM 用户设立新用户帐户并指定唯一密码和授权级别（用户角色）。

- **仔细考虑将串行端口连接到终端服务器的风险。**

终端设备并不能始终提供适当级别的用户验证或授权，而这些是保护网络免受恶意入侵所需的。为了保护系统免受意外的网络入侵，请不要通过任何类型的网络重定向设备（比如终端服务器）与 Oracle ILOM 建立串行连接（通过串行端口），除非服务器具有足够的访问控制能力。

此外，诸如密码重置和 "Preboot" 菜单等某些 Oracle ILOM 功能只能通过物理串行端口使用。如果使用未经验证的终端服务器将串行端口连接到网络，则无需进行物理访问，并且会降低与这些功能相关的安全性。

- **访问 "Preboot" 菜单需要对服务器进行物理访问。**

  Oracle ILOM 的 "Preboot" 菜单是一个强大的实用程序，可将 Oracle ILOM 重置为默认值，或者在 Oracle ILOM 不响应时重置闪存固件。在 Oracle ILOM 重置之后，用户将需要按下服务器上的按钮（默认方式）或键入密码才能访问。Oracle ILOM 的 "Physical Presence" 属性可控制此行为 (`check_physical_presence= true`)。为了在访问 "Preboot" 菜单时实现最高的安全性，请不要更改该属性的默认设置 (`true`)，以便访问 "Preboot" 菜单时始终需要对服务器进行物理访问。

- **参阅 Oracle ILOM 文档。**

  请参阅 Oracle ILOM 文档，详细了解如何设置密码、管理用户以及应用安全相关的功能。有关特定于 Oracle ILOM 的安全准则，请参阅 Oracle ILOM 文档库中的《*Oracle ILOM* 安全指南》。您可以在以下位置找到 Oracle ILOM 文档：

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

Oracle Hardware Management Pack 安全性

Oracle Hardware Management Pack 可用于您的服务器，以及许多基于 x86 的其他 Oracle 服务器和某些基于 SPARC 的 Oracle 服务器。Oracle Hardware Management Pack 采用两种组件（即 SNMP 监视代理和一系列跨操作系统的命令行界面工具 (CLI Tools)）来管理您的服务器。

- **使用 Hardware Management Agent SNMP Plugins。**

  SNMP 是用于监视或管理系统的标准协议。通过 Hardware Management Agent SNMP Plugins，您可以使用 SNMP 来监视数据中心中的 Oracle 服务器，其优点是不必连接到两个管理点，即主机和 Oracle ILOM。通过此功能，可以使用单个 IP 地址（主机的 IP 地址）来监视多个服务器。

  SNMP Plugins 在 Oracle 服务器的主机操作系统上运行。SNMP Plugin 模块可扩展主机操作系统中的本机 SNMP 代理，以提供其他 Oracle MIB 功能。Oracle Hardware Management Pack 本身不包含 SNMP 代理。对于 Linux，模块将添加到 net-snmp 代理。对于 Oracle Solaris，模块将添加到 Oracle Solaris Management Agent。对于 Microsoft Windows，该插件可扩展本机 SNMP 服务。与 Oracle Hardware Management Pack 的 SNMP 相关的任何安全性设置均由本机 SNMP 代理或服务的设置（而不是插件）来决定。

请注意，SNMPv1 和 SNMPv2c 不提供加密，并且使用团体字符串作为验证形式。相比之下，SNMPv3 更为安全，是建议使用的版本，因为它使用加密来提供安全的通道并使用单独的用户名和密码。

- 参阅 Oracle Hardware Management Pack 文档。

  有关这些功能的更多信息，请参阅 Oracle Hardware Management Pack 文档。有关特定于 Oracle Hardware Management Pack 的安全准则，请参阅 Oracle Hardware Management Pack 文档库中的《*Oracle Hardware Management Pack (HMP) Security Guide*》。您可以在以下位置找到 Oracle Hardware Management Pack 文档：

  http://www.oracle.com/goto/OHMP/docs

规划安全环境

安全准则应在系统到位之前制定就绪。系统到位之后，应定期审核和调整安全准则，以便与组织当前的安全要求保持同步。在对服务器及相关设备进行安装和配置之前和期间，请利用本节中提供的信息。

本节包括以下主题：

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

密码保护

密码是安全性的一个重要方面，因为如果选择的密码不安全，可能会导致有人未经授权便访问公司资源。实施密码管理最佳做法可以确保用户遵守创建和保护密码的一组准则。密码策略典型的几个部分应该定义以下内容：

- 密码长度和强度
- 密码期限
- 密码的常见做法

强制实施以下标准做法以创建强安全性的复杂密码：

- 不要创建包含用户名、员工姓名或家庭成员姓名的密码。
- 不要选择易于猜测的密码。
- 不要创建包含连续数字字符串（例如 12345）的密码。
- 创建的密码不得包含通过简单的 Internet 搜索便可轻松发现的单词或字符串。
- 不允许用户在多个系统中重复使用相同的密码。
- 不允许用户重复使用旧密码。

定期更改密码。这样有助于防止恶意行为，并且可以确保密码符合当前的密码策略。

操作系统安全指南

有关下列内容的信息，请参阅 Oracle 操作系统 (operating system, OS) 文档：

- 配置系统时如何使用安全功能
- 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

受支持的 Oracle 操作系统的安全指南文档包含在该操作系统的文档库中。要获得某个 Oracle 操作系统的安全指南文档，请转到该 Oracle 操作系统文档库：

操作系统	链接
Oracle Solaris OS	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Oracle Linux OS	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

有关其他供应商提供的操作系统（例如 Red Hat Enterprise Linux、SUSE Linux Enterprise Server、Microsoft Windows 和 VMware ESXi）的信息，请参阅相应供应商的文档。

网络交换机和端口

网络交换机提供不同级别的端口安全功能。请参阅交换机文档，了解如何执行下列操作：

- 针对交换机的本地和远程访问，使用验证、授权和记帐功能。
- 对于默认情况下可能有多个用户帐户和密码的网络交换机，更改其上的每个密码。
- 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虚拟局域网 (Virtual Local Area Network, VLAN) 号进行带内管理。
- 对入侵检测系统 (Intrusion Detection System, IDS) 访问使用网络交换机的端口镜像功能。
- 脱机维护一份交换机配置文件，并且只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。
- 实施端口安全性，以基于 MAC 地址限制访问。对所有端口禁用自动中继。
- 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) 涉及将一个或多个连接设备的介质访问控制 (Media Access Control, MAC) 地址与交换机的物理端口相关联。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) 会禁止将指定的 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，以便网络交换机可以基于当前连接设置安全性。

VLAN 安全

如果设置了虚拟局域网 (Virtual Local Area Network, VLAN)，请记住，VLAN 会共享网络带宽，且需要其他安全措施。

- 使用 VLAN 时，请将敏感的系统群与网络的其余部分隔开。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。
- 为中继端口指定唯一的本机 VLAN 号。
- 限制使用可通过中继传输的 VLAN，只有绝对需要时才使用。
- 如果可能，禁用 VLAN 中继协议 (VLAN Trunking Protocol, VTP)。否则，为 VTP 设置以下项：管理域、密码和修剪。然后将 VTP 设置为透明模式。
- 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。

Infiniband 安全

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。

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软件资产。

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

电源控制

可以使用软件来打开和关闭某些 Oracle 系统的电源。某些系统机柜的配电设备 (Power Distribution Unit, PDU) 可以远程进行启用和禁用。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

可使用序列号来跟踪清单。Oracle 在选件卡和系统主板上的固件中嵌入了序列号。可以通过局域网 (local area network, LAN) 连接读取这些序列号。

还可以使用无线射频识别 (Wireless Radio Frequency Identification, RFID) 读取器来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*》：

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

软件和固件更新

安全增强功能是通过新的软件发行版和修补程序引入的。有效、主动的修补程序管理是系统安全的重要部分。最佳的安全措施是，使用最新的软件发行版以及所有必要的安全修补程序对系统进行更新。

- 定期检查是否有软件更新和安全修补程序。
- 始终安装软件或固件的最新发行版本。
- 为您的软件安装所有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，可能需要修补程序和固件更新。

网络安全

在根据安全原则对网络进行配置后，需要定期进行检查和维护。

请遵循以下准则来保护对系统的本地和远程访问：

- 限制只能使用 SSH（而非 Telnet）对特定 IP 地址进行远程配置。Telnet 以明文形式传递用户名和密码，这可能使局域网 (local area network, LAN) 段上的每个人都能看到登录凭据。为 SSH 设置强密码。
- 使用简单网络管理协议 (Simple Network Management Protocol, SNMP) 版本 3 来提供安全传输。SNMP 的早期版本不安全，它们以未加密文本形式传输验证数据。
- 如果必须使用 SNMP，请将默认的 SNMP 团体字符串更改为加强的团体字符串。某些产品将 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。
- 如果系统控制器使用浏览器界面，请始终在使用后进行注销。
- 禁用不必要的网络服务，如传输控制协议 (Transmission Control Protocol, TCP) 或超文本传输协议 (Hypertext Transfer Protocol, HTTP)。启用必要的网络服务并以安全方式配置这些服务。
- 创建在登录时显示的标题消息，声明禁止未经授权的访问。您可以向用户告知任何重要的策略或规则。可以使用标题向用户警示给定系统的特殊访问限制，或者向用户提醒密码策略及正确使用方式。
- 在适用情况下，使用访问控制列表实施限制。
- 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。

- 使用 LDAP 访问系统时，遵循 LDAP 安全措施。
- 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。

有关网络安全的更多信息，请参阅 Oracle ILOM 文档库中的《*Oracle ILOM* 安全指南》。您可以在以下位置找到 Oracle ILOM 文档：

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

数据保护和安全

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或 USB 存储设备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，请以物理方式销毁该驱动器或彻底清除该驱动器上的所有数据。删除驱动器中的文件或重新格式化驱动器后，仍可从该驱动器恢复信息。删除文件或重新格式化驱动器只会删除该驱动器中的地址表。使用磁盘擦除软件可彻底清除驱动器上的所有数据。

日志维护

定期检查和维护日志文件。使用以下方法来保证日志文件的安全：

- 启用日志记录并将系统日志发送至专用安全日志主机。
- 使用网络时间协议 (Network Time Protocol, NTP) 和时间戳配置日志记录以包含准确的时间信息。
- 对网络设备日志执行定期调度的扫描，查看有无异常的网络活动或访问。
- 查看日志以发现可能的事件，并根据安全策略将它们归档。
- 定期将超出合理大小的日志文件作废。保留已作废文件的副本，以备用于将来参考或统计分析。