Netra Server X3-2（以前称为 Sun Netra X4270 M3 Server）

安全指南

文件号码 E35611–01
2012 年 7 月

ORACLE

130427@25097

目录

Netra Server X3-2 安全指南

本文档提供了若干一般安全准则，来帮助您保护 Oracle Netra Server X3-2（以前称为 Sun Netra X4270 M3 Server）、其网络接口及其连接的网络交换机。

本章包含以下几节：

系统概述

Netra Server X3-2 是符合 NEBS 的企业级 2U 服务器，它有两个处理器，并支持十六个 DDR3 DIMM（每个处理器八个）、六个 PCIe Gen3 插槽以及八个或六个 SAS/SATA 存储驱动器。六驱动器机型还提供了一个 DVD。

该服务器包含一个板载 Oracle Integrated Lights Out Manager (Oracle ILOM) 服务处理器 (service processor, SP)。在预先安装的 USB 驱动器上，作为服务器配置的一部分还嵌入了一个名为 Oracle System Assistant 的服务器设置工具。

安全原则

有四个基本安全原则：访问、验证、授权和记帐。

- **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。
  - 请参阅软件随附的文档，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。
  - 限制人员接近连接器或端口，这些位置可以提供比 SSH 连接更强大的访问。一些设备（如系统控制器、配电设备和网络交换机）提供了连接器和端口。

- 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或客户可更换单元。仅限经授权的人员接近带锁机柜。

- **验证**

  验证是指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。
  - 确保人员正确使用员工胸卡进入计算机室。
  - 对于用户帐户，根据需要使用访问控制列表。设置扩展会话的超时，并为用户设置特权级别。

- **授权**

  授权是指对人员使用硬件或软件施加的限制。

  - 只允许员工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**

  记帐是指用于监视登录活动和维护硬件清单的软件和硬件功能。

  - 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功能强大的命令。
  - 保留所有硬件的序列号记录。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插卡、模块和主板中。
  - 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。

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。

Oracle System Assistant 安全性

Oracle System Assistant 是一种预安装的工具，可帮助您从本地或远程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，请参阅服务器管理指南，网址为：

`http://docs.oracle.com/cd/E27124_01`

下列信息有助于您了解与 Oracle System Assistant 相关的安全问题。

- **Oracle System Assistant 包含一个可引导的根环境。**

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。它构建于可引导的 Linux 根环境之上。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。建议保护对服务器的物理访问权限，慎重为 Oracle ILOM 用户分配管理员和控制台特权。

- **Oracle System Assistant 挂载了可供操作系统访问的一个 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 存储设备可读取且可写入，有可能被病毒利用。

建议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。此外，也无法引导 Oracle System Assistant。

您可以通过工具自身或通过 BIOS 禁用 Oracle System Assistant。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，以便只有授权用户才能重新启用 Oracle System Assistant。有关如何禁用和重新启用 Oracle System Assistant 的信息，请参阅服务器管理指南。

Oracle ILOM 安全性

您可以使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 管理固件（已预先安装到服务器、基于 x86 的其他 Oracle 服务器以及某些基于 SPARC 的 Oracle 服务器上）来主动保护、管理和监视系统组件。

对服务处理器使用专用网络，以将其与常规网络隔开。限制 `root` 超级用户帐户的使用。尽可能分配 Oracle ILOM 帐户，如 `ilom-operator` 和 `ilom-admin`。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`），这些密码广为人知并允许对设备进行未经授权的访问。

请参阅 Oracle ILOM 文档，以更详细地了解如何设置密码、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。有关特定于 Oracle ILOM 的安全准则，请参阅 Oracle ILOM 3.1 文档库中的《Oracle Integrated Lights Out Manager (ILOM) 3.1 安全指南》。您可以在以下位置找到 Oracle ILOM 3.1 文档：

http://docs.oracle.com/cd/E24707_01

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 的其他服务器和某些 SPARC 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。

通过 Hardware Management Agent SNMP Plugins，您可以使用 SNMP 来监视数据中心中的 Oracle 服务器和服务器模块，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）来监视多个服务器和服务器模块。SNMP Plugins 在 Oracle 服务器的主机操作系统上运行。

您可以使用 Oracle Server CLI Tools 来配置 Oracle 服务器。CLI Tools 适用于 Oracle Solaris、Oracle Linux、Oracle VM、其他 Linux 变体以及 Microsoft Windows 操作系统。

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://docs.oracle.com/cd/E20451_01

规划安全环境

在安装和配置服务器及相关设备时请使用下列信息。

Oracle 操作系统准则

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：

- **Oracle Solaris** – http://docs.oracle.com/cd/E23824_01
- **Oracle Linux** – http://linux.oracle.com/documentation/
- **Oracle VM** – http://www.oracle.com/technetwork/documentation/vm-096300.html

网络端口和交换机

不同的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。

- 对交换机进行本地和远程访问时，使用验证、授权和记帐功能。

- 在默认情况下可能有多个用户帐户和密码的网络交换机上，更改每个密码。
- 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具有访问权限。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访问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 安全性

如果设置了虚拟局域网 (virtual local area network, VLAN)，请记住，VLAN 会分享网络带宽，并需要其他安全措施。

- 定义 VLAN 以将系统的敏感群集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。

Infiniband 安全性

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。
- 如果可能，使用静态 VLAN 配置。
- 禁用未使用的交换机端口，并为它们指定未使用的 VLAN 号。

维护安全环境

初始安装和配置之后，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。

硬件电源控制

可以使用软件来打开和关闭某些 Oracle 系统。可以远程启用和禁用某些系统机柜的配电设备 (power distribution unit, PDU)。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

使用序列号跟踪清单。Oracle 将序列号嵌入到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。

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》（《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
```

更新软件和固件

保持服务器设备上的软件和固件为最新版本。

- 定期检查更新。
- 始终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，可能需要修补程序和固件更新。

网络访问

请遵循以下准则来保护对系统的本地和远程访问。

- 使用 SSH 而非 Telnet 限制只有特定的 IP 地址可以进行远程配置。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。
- 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 SNMP 是必需的，请将默认 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，请始终在使用后将其注销。
- 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安全地配置这些服务。

数据保护

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完全清除该驱动器上的所有数据。删除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完全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。
- 查看日志以发现可能的事件，并根据安全策略将它们归档。
- 当日志文件超出合理大小时，定期对这些日志文件进行归档，然后重置日志。您可以使用归档后的文件来进行参考或统计分析。