Oracle 双端口 EDR InfiniBand 适配器安全指南

文件号码 E76129-01
2016 年 9 月

文件号码 E76129-01

版权所有 © 2016, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，则适用以下注意事项：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。除非您与 Oracle 签订的相应协议另行规定，否则对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的保证，亦不对其承担任何责任。除非您和 Oracle 签订的相应协议另行规定，否则对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

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

Oracle 双端口 EDR InfiniBand 适配器安全

本文档提供 Oracle 双端口 EDR InfiniBand 适配器的一般安全准则。本指南适用于有经验的网络管理员，并提供了一般准则和特定说明来增强安全性。

本文档包括以下主题：

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，访问限制通常是指物理访问限制。
  - 对于软件，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

  在平台操作系统中设置授权功能（如密码系统）可确保用户与其声明的身份相符。确保人员正确使用员工胸卡进入机房。
- 授权

  只允许员工使用他们经过培训且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 的软件和硬件功能监视登录活动和维护硬件清单。

  - 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功能强大的命令。
  - 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。

规划安全环境

在安装和配置服务器及相关设备时，请遵循以下注意事项。

硬件安全

保护物理硬件的方式非常简单：限制对硬件的接近并记录序列号。

- 限制接近
  - 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 控制台的访问，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。
  - 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。
- 记录序列号
  - 对计算机硬件的所有重要物项（如 FRU）添加安全标记。使用特殊的紫外线笔或压纹标签。
  - 记录所有硬件的序列号。
  - 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

大多数硬件和软件安全都通过软件方法实施。

- 请参阅软件随附的文档，启用可用于软件的任何安全功能。
- 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。
- 对服务处理器使用专用网络，从而将其与常规网络隔离。
- 可以通过广域网 (Wide Area Network, WAN) 或存储区域网络 (Storage Area Network, SAN) 安全地引导系统。有关使用 WAN Boot 或 iSCSI Boot 进行安全引导的信息，请参阅适用于相应 Oracle Solaris 操作系统发行版的《Oracle Solaris 安装指南：基于网络的安装》一书。
- 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，从而有可能导致对设备进行未经授权的访问。
- 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。

Oracle Solaris OS 准则

有关以下内容的信息，请参阅 Oracle Solaris 安全准则文档：

- 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

  可在以下位置找到 Oracle Solaris 安全准则文档 http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

Oracle Linux OS 准则

使用 Oracle Linux OS 命令限制对软件的访问、强化 OS、使用安全功能以及保护应用程序。请参阅《Oracle Linux Security Guide for Release 6》（《Oracle Linux 发行版 6 安全指南》），网址为 http://docs.oracle.com/cd/E37670_01/E36387/html/index.html。

网络交换机

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。

- 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。
- 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。
- 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绑定。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。

Oracle 固件安全

使用超级用户帐户设置和更新 OpenBoot PROM (OBP) 或其他 Oracle 固件。普通用户帐户允许用户查看固件但不允许编辑固件。Oracle Solaris OS 固件更新过程可防止进行未经授权的固件修改。

有关设置 OBP 安全变量的信息，请参阅《OpenBoot 4.x Command Reference Manual》（《OpenBoot 4.x 命令参考手册》），网址为：http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM 固件

您可以使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 管理固件（已预先安装到某些 SPARC 服务器上）来主动保护、管理和监视系统组件。

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，网址为：http://docs.oracle.com/cd/E37444_01/index.html

VLAN 安全

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。

- 定义虚拟局域网 (Virtual Local Area Network, 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 设置以下内容：管理域、密码和删改。然后将 VTP 设置为透明模式。

Infiniband 安全

Infiniband (IB) 安全是指使用 IB 网状结构网络以及其中运行的子网管理器 (Subnet Manager, SM) 的功能。确保连接到 IB 网状结构网络的所有 IB 主机都是安全的。IB 网状结构网络的安全性与连接到它的最低安全性 IB 主机相同。对主机具有 root 访问权限的攻击者能够攻陷整个 IB 网状结构网络。（就此而言，物理访问还是很重要的 – 能够将自己主机连接到 IB 交换机的攻击者能够损坏 IB 网状结构网络的安全性。）

在虚拟化环境中使用 Oracle 双端口 EDR InfiniBand 适配器或 Oracle 双端口 QDR InfiniBand 适配器 M4 时，要特别注意物理域的安全，因为受影响的物理域可能会导致所有虚拟机被暴露并易受攻击。

有关保护 InfiniBand 以及受支持交换机（还运行 SM）的安全的更多信息，请参见适用于相应交换机的 InfiniBand 交换机安全指南：

- 对于 Sun Datacenter InfiniBand Switch 36，请参见《Sun Datacenter InfiniBand Switch 36 Hardware Security Guide》（《Sun Datacenter InfiniBand Switch 36 硬件安全指南》），网址为：http://docs.oracle.com/cd/E36265_01/
- 对于 Sun Network QDR InfiniBand Gateway Switch，请参见《Sun Network QDR InfiniBand Gateway Switch Hardware Security Guide》（《Sun Network QDR InfiniBand Gateway Switch 安全指南》），网址为：http://docs.oracle.com/cd/E36256_01/
- 对于 IB 交换机和 Oracle 虚拟网络 InfiniBand 交换机上的 SM，请参见：http://docs.oracle.com/cd/E38500_01/

用户帐户

- 如果可能，设置 RADIUS 和 TACACS+ 访问协议：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。
- 限制超级用户帐户 (root) 的使用。该帐户拥有特权，如果被误用，会对安全造成不利影响。尽可能改用特权较低的其他用户帐户。这适用于主机操作系统 (Solaris, Linux) 以及 Oracle ILOM。
- 在适用的情况下使用访问控制列表。

- 针对长期会话设置超时。
- 设置特权级别。
- 创建一个系统标题以提醒用户未经授权的访问是被禁止的。

系统日志

- 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。

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。

硬件电源控制

可以使用软件来打开和关闭某些 Oracle 系统的电源。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

可使用序列号来跟踪清单。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 (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》），网址为：http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

软件和固件更新

请保持服务器设备上的固件以及相关主机软件（驱动程序、用户空间工具）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，因此也可能需要修补程序和固件更新。

检查更新和修补程序的可用性，网址为 https://support.oracle.com

网络访问

请遵循以下准则以保护对系统的本地和远程访问：

- 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。
- 只允许使用 SSH（而非 Telnet）从特定 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 LAN 段上的每个人都能看到登录凭据。为 SSH 设置强密码。
- 使用 SNMP 的版本 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，请始终在使用后将其注销。
- 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

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。

日志安全

定期检查和维护日志文件。

- 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。