**Oracle® EDR InfiniBand 交换机和虚拟化 I/
O 系统硬件安全指南**

ORACLE®

文件号码 E75984-01
2016 年 9 月

文件号码 E75984-01

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

使用本文档	7
产品文档库	7
反馈	7
Oracle InfiniBand Switch IS2-46 安全指南	9
了解安全原则	9
规划安全环境	10
硬件安全	10
软件安全	10
Oracle ILOM 固件	11
VLAN 安全	11
用户帐户	11
系统日志	12
维护安全环境	12
硬件电源控制	12
资产跟踪	12
软件和固件更新	12
网络访问	13
数据保护	13
日志安全	14

使用本文档

- 概述—介绍如何在 Oracle 的交换机上实施安全策略。
- 目标读者—技术人员、系统管理员和授权服务提供商
- 所需知识—管理网络硬件的丰富经验

产品文档库

可从以下网址获得有关该产品及相关产品的文档和资源：<http://www.oracle.com/goto/is2-46/docs>。

反馈

可以通过以下网址提供有关本文档的反馈：<http://www.oracle.com/goto/docfeedback>。

Oracle InfiniBand Switch IS2-46 安全指南

本文档提供一般的安全准则，以帮助保护 Oracle IS2-46 交换机机箱。

讨论的主题包括：

- [“了解安全原则” \[9\]](#)
- [“规划安全环境” \[10\]](#)
- [“维护安全环境” \[12\]](#)

了解安全原则

4A (AAAA) 基本安全准则是：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**

在交换机中设置验证功能（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数据中心。
- **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。

 - 使用系统日志和 Oracle ILOM 日志监视用户登录。尤其要监视 root 帐户和 root 特权帐户，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 序列号以物理方式标记在机箱上，并以电子方式记录在所有 SP、SCP 和主板上。

规划安全环境

请在安装和配置交换机之前及过程中查阅这些主题。

- “硬件安全” [10]
- “软件安全” [10]
- “Oracle ILOM 固件” [11]
- “VLAN 安全” [11]
- “用户帐户” [11]
- “系统日志” [12]

硬件安全

保护物理硬件的方式很简单：限制接近硬件并记录序列号。

- 限制接近
 - 在上锁的限制接近区域安装交换机。
 - 如果设备安装在有带锁门的机架中，请始终保持门的安全。
 - 限制接近交换机光纤结构和网络连接。除了保护交换机，这也会保护对等节点。
 - 限制接近交换机本身的串行控制台，不越过安全边界。不使用终端服务器或端口集线器。串行控制台允许更大的用户管理以及错误和调试消息传递特权。这些消息会无意中提供线索，促成恶意侵入及破坏安全。串行控制台未加密，在该方面的安全性弱于 SSH 连接。
 - 尤其要限制接近电源、风扇模块和收发器，因为这些东西可以轻松拆卸。
 - 在上锁的机柜内存储备用的可更换组件。仅允许授权人员接近上锁的机柜。
- 记录序列号
 - 对包括可更换组件在内的所有重要物品进行安全标记。使用特殊的紫外线笔或压纹标签。
 - 保存所有硬件的序列号记录。
 - 将发票、采购记录和许可证副本保存在系统出现紧急状况时系统管理员容易获取的安全位置。这些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。

- 有关在固件中实施安全功能的其他准则，请参阅交换机文档。
- 请参阅 OFOS 和 OFM 文档，启用可用于软件套件的任何安全功能。
- 通过 SER MGT 端口进行交换机带外管理。此端口独立于数据通信流量和常规网络。
- 如果带外管理不可行，则专门使用一个唯一的 VLAN 号进行带内管理。

- 在安装新交换机时，尽快更改所有默认密码。交换机有一个默认用户帐户 root。root 用户有超级用户特权。默认密码为 changeme。使用 Oracle ILOM `set /SP/users/root password=password` 命令更改密码，最好在交换机连接到网络之前更改。
- 计划并定期更改交换机上的每个密码，尤其在使用其他用户帐户配置时。

Oracle ILOM 固件

可以通过交换机上预安装的 Oracle ILOM 固件主动保护、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)、Active Directory 和 LDAP 验证协议。有关特定于 Oracle ILOM 的安全准则，请参阅 Oracle ILOM 3.2 文档库中的《*Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*》（《Oracle ILOM 安全指南（固件发行版 3.0、3.1 和 3.2）》）。您可以在以下位置找到 Oracle ILOM 3.2 文档：

http://docs.oracle.com/cd/E37444_01

VLAN 安全

例如，如果配置虚拟局域网 (virtual local area network, VLAN) 进行带内网络管理，请记住 VLAN 在一个网络上共享带宽，需要额外的安全措施。

- 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 设置以下内容：管理域、密码和删改。然后将 VTP 设置为透明模式。

用户帐户

- 实施安全的验证协议，如 Active Directory、LDAP 和 RADIUS。集中管理验证和授权。
- 限制使用 root 超级用户帐户。代之以创建特权较小的 Oracle ILOM 帐户仅用于管理。一般准则是：创建并使用具有足以执行特定任务的最小特权的用户帐户。
- 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” [12]
- “资产跟踪” [12]
- “软件和固件更新” [12]
- “网络访问” [13]
- “数据保护” [13]
- “日志安全” [14]

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

可使用序列号来跟踪清单。Oracle 在 SP 和 SCP 上的固件中以及主板中嵌入了序列号。有关如何查阅这些序列号的说明，请参见交换机文档。

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》）：

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

软件和固件更新

保持交换机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。
- 为软件安装任何必要的安全修补程序。

检查更新和修补程序的可用性：

<http://support.oracle.com>

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：

- 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。
- 配置并使用第 3 版 (v3) 的 SNMP 来提供安全传输。v1 和 v2c 版的 SNMP 不安全（以未加密的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 (PUBLIC) 更改为加强的团体字符串。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。
- 除非绝对必要，否则不要启用 SNMP set 请求。如果启用，请创建具有只读和读写权限的单独的 SNMP v3 用户。
- 始终在通过 Web 接口访问 SP 或 SCP 后注销。
- 禁用不使用的或不必要的服务，如 TCP 小服务器。仅启用必要的服务并安全地配置这些服务。
- 禁用不使用的 IPMI 服务。IPMI 协议是一种不安全的 SP 访问方式。
- 禁用 HTTP 服务，代之以使用 HTTPS。在有些情况下，可能必须临时启用 HTTP 以兼容 Java。请根据情况慎重进行此操作。
- 禁用不使用的交换机端口。

数据保护

请遵循以下准则以最大限度地确保数据安全：

- 将交换机配置文件备份到安全的远程位置，并仅限授权管理员可对其访问。配置文件应包含每个设置的描述性注释。
- 使用数据加密软件确保硬盘驱动器上的机密信息安全。
- SP、SCP 和 SSD 是包含等效于系统硬盘的数据的交换机组件。在更换交换机时，请物理销毁这些组件，或者彻底清除相应文件系统中的所有数据。使用磁盘擦除软件可彻底清除文件系统上的所有数据。

日志安全

定期检查和维护日志文件。

- 检查系统日志和 Oracle ILOM 日志以发现可能的事件，并根据安全政策将它们归档。
- 在日志文件超过合理大小时，定期归档并清除日志文件。将归档文件保存在安全位置以供将来需要时参考或用于统计分析。