

Sun Storage 16 Gb 光纤通道 PCIe 通用主机 总线适配器 (Emulex) 安全指南

适用于 HBA 型号 7101684

ORACLE®

文件号码 E41468-02
2015 年 7 月

文件号码 E41468-02

版权所有 © 2014, 2015, 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，并按许可证的规定使用。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=dacc>。

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
Sun Storage 16 Gb FC PCIe 通用 HBA (Emulex) 安全性	9
通用 HBA 概述	9
安全原则	10
规划安全环境	11
硬件安全	11
软件安全	12
固件安全	12
Oracle ILOM 固件	12
系统日志	12
维护安全环境	13
资产跟踪	13
固件更新	13
软件更新	13
日志安全	14
模块安全	14

使用本文档

- 概述 - 描述了如何安全地使用通用主机总线适配器
- 目标读者 - 技术人员、系统管理员和授权服务提供商
- 必备知识 - 对故障排除和硬件更换具有丰富经验

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://docs.oracle.com/cd/E24649_01/index.html。

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>。

Sun Storage 16 Gb FC PCIe 通用 HBA (Emulex) 安全性

本文档介绍了使用 Sun Storage 16 Gb FC PCIe 通用 HBA (Emulex) 时要注意的一般安全原则和准则。

本文档未包含以下安全信息：

- 有关 BIOS、Open Boot Prom (OBP) 和虚拟机管理程序的特定平台固件安全性
- 有关操作系统安全性的问题
- 硬件系统的物理安全性
- 外部联网基础结构的网络安全性
- 可信平台模块信息

有关上述任何安全领域的安全信息，请参见随具体产品提供的安全文档。

本文档包含以下主题：

- [“通用 HBA 概述” \[9\]](#)
- [“安全原则” \[10\]](#)
- [“规划安全环境” \[11\]](#)
- [“维护安全环境” \[13\]](#)

通用 HBA 概述

Oracle Sun Storage 16 Gb FC PCIe 通用 HBA (Emulex) (销售部件号 7101684) 是一个独立的 PCIe 窄版型通用主机总线适配器。该 HBA 被视为通用适配器是因为该适配器是可配置的板卡，即可根据插入并连接到 HBA 的光纤收发器和光缆将其运行协议模式从双端口 16 Gb FC HBA 更改为双端口 10 GbE CNA。

该板卡的接口是一个八通道 PCI Express 总线，其中八个通道支持两个光纤通道 (Fibre Channel, FC) 光学介质端口或以太网光纤通道 (Fibre Channel over Ethernet, FCoE) 光学介质端口。每个独立的 FC 端口以 16 Gb/秒的速度运行，并具有 16/8/4 自动协商功能。每个 FCoE 端口以 10 Gb/秒的速度运行。您可以配置以下三种选项：

- **10 GbE FCoE 选项** – 该版本的卡提供双轴（或铜质）10 GbE FCoE ExpressModule 聚合网络适配器功能。此聚合网络适配器上未安装任何光纤模块。

- **16 Gb FC 光纤选项** – 该版本的卡在卡的 SFP+ 连接器中安装了 16 Gb FC 光纤模块（光纤模块销售部件号：7101686），可提供短波 16 Gb 光纤通道 ExpressModule 主机总线适配器功能。
- **10 Gb FCoE 光纤选项** – 该版本的卡在卡的 SFP+ 连接器中安装了 10 GbE 光纤模块（光纤模块销售部件号：7101688），可提供短波 10 GbE FCoE ExpressModule 聚合网络适配器功能。

下图显示了 Sun Storage 16 Gb FC PCIe 通用 HBA (Emulex)：



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。
 - 除非执行 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计算机室。
- **授权**

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**

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。在所有插卡、模块和主板上以电子方式记录了 Oracle 部件号。

规划安全环境

在安装和配置服务器和 Sun Storage 16 Gb 光纤通道 PCIe 通用 HBA (Emulex) 之前和过程中，请查看本部分中的内容。

本部分包含以下主题：

- [“硬件安全” \[11\]](#)
- [“软件安全” \[12\]](#)
- [“固件安全” \[12\]](#)
- [“Oracle ILOM 固件” \[12\]](#)
- [“系统日志” \[12\]](#)

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**
 - 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。
 - 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)。仅限经授权的人员操作带锁机柜。
- **记录序列号**

记录所有通用 HBA 卡的序列号。

软件安全

软件组件的安全注意事项包括：

- 参阅软件随附的文档，启用可用于软件的任何安全功能。
- 使用超级用户帐户设置和更新通用 HBA 驱动程序。
- 大多数硬件安全都通过软件方法实现。
- 支持通用 HBA 的软件组件依靠系统安全功能来提供安全访问。

固件安全

通用 HBA 在交付时已安装了所有固件。除了更新以外，不需要实地安装固件。

- 如果需要更新固件，请从 Emulex Web 站点的 Oracle 支持区域获取固件更新：<http://www.emulex.com/downloads/oem-qualified/oracle/>
还可以联系 Oracle 技术支持部门安排支持，或访问 Oracle 技术支持站点获取产品最近的更新和最新的过程。
<https://support.oracle.com>
- 使用超级用户帐户设置和更新通用 HBA 固件管理实用程序。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。
- 有关最新发布的信息、固件更新要求信息或其他安全信息，请参阅位于 Oracle Web 站点的通用 HBA 安装指南。
- 有关设置 SPARC OpenBootPROM (OBP) 安全变量的信息，请参阅《*OpenBoot 4.x Command Reference Manual*》。

Oracle ILOM 固件

您可以使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 固件（已预先安装到某些 x86 服务器上）来主动保护、管理和监视系统组件。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/pls/topic/lookup?ctx=ilom31>

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

初始安装和设置通用 HBA 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。

其中包括以下部分：

- “资产跟踪” [13]
- “固件更新” [13]
- “软件更新” [13]
- “日志安全” [14]
- “模块安全” [14]

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。请参阅 Oracle 白皮书《*How to Track Your Oracle Sun System Assets by Using RFID*》。

固件更新

保持设备上的固件为最新版本。

- 定期检查更新。
- 一般而言，所有操作系统，特别是 Oracle Solaris 要求您使用 root 凭证登录来管理卡和升级驱动程序或固件。
- 始终安装固件的最新发行版本。

软件更新

保持设备上的软件为最新版本。

- 可通过 Oracle Solaris 修补程序和更新获取 Oracle Solaris 驱动程序的软件更新。

- 可从以下位置获取其他操作系统的驱动程序软件更新：<http://www.emulex.com/downloads/oem-qualified/oracle/>。
- 有关最新发布的信息、软件更新要求信息或其他安全信息，请参阅位于 Oracle Web 站点的通用 HBA 文档。
- 始终安装软件的最新发行版本。
- 为您的软件安装任何必要的安全修补程序。
- 设备还包含固件，可能需要固件更新。

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。您可以复制要作废的文件，将副本用于将来参考或统计分析。

模块安全

通用 HBA 可通过 Emulex OneCommand Manager 命令行界面 (command-line interface, CLI) 或图形用户界面 (graphical user interface, GUI) 实用程序管理。这两个实用程序支持执行以下操作：

- 监视通用 HBA 运行。
- 更改通用 HBA 的运行协议模式配置。
- 更新通用 HBA 固件。

OneCommand Manager 实用程序仅允许具有 root 凭证的用户访问。因此，无此特权的用户无法通过使用这两个实用程序来更改 SAN 环境。

有关 OneCommand Manager CLI 和 GUI 的信息，请参见位于以下 Web 站点的 Emulex OneCommand Manager 文档：<http://www.emulex.com>