Sun Storage 16 Gb 光纤通道 PCIe 通用主机总线适配器

安全指南（适用于 HBA 型号 7101674）

文件号码： E41429-01
2013 年 7 月

目录

• • • 第 1 章

Sun Storage 16 Gb FC PCIe 通用 HBA 安全性

本文档介绍了使用 Sun Storage 16 Gb FC PCIe 通用 HBA 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。

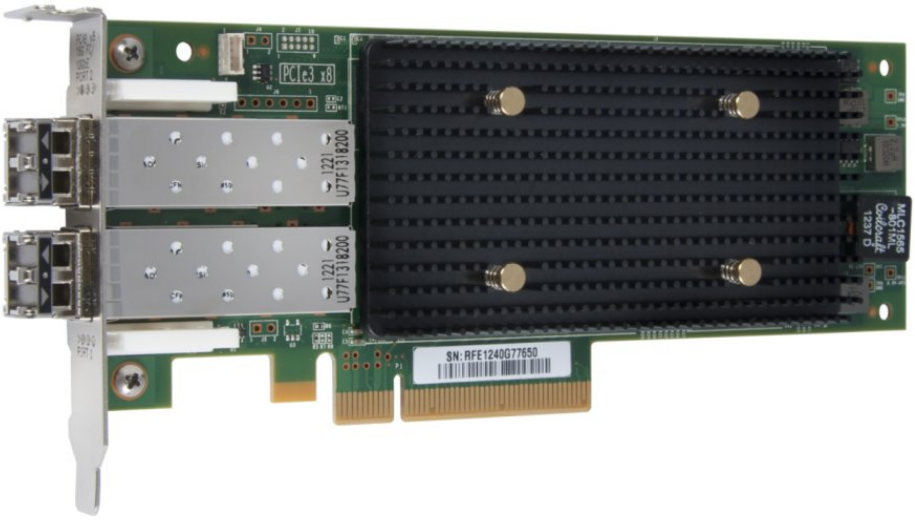
本文档包含以下主题：

通用 HBA 概述

Oracle Sun Storage 16 Gb 光纤通道 PCIe 通用 HBA（部件号 7101674）是一个独立的 PCIe 窄板型通用主机总线适配器，该适配器使用 QLogic 技术。该 HBA 被视为通用适配器是因为该适配器是可配置的板卡，允许将其运行协议模式从双端口 16 Gb 光纤通道 HBA 改为双端口 10 GbE 以太网光纤通道 (Fibre Channel over Ethernet, FCoE) 聚合网络适配器。该通用 HBA 具有以下四种可能的配置：

- 10 GbE FCoE 铜缆 – 此配置提供双轴铜质电缆连接和 10 GbE FCoE 通用 HBA 功能。通用 HBA 的此配置未安装光纤模块，也未提供此模块。
- 16 Gb FC SW（shortwave，短波）光纤 – 此配置要求在通用 HBA 的 SFP+ 连接器中安装 16 Gb FC 短波光纤收发器模块，可支持 16 Gb 光纤通道 HBA 功能。
- 10 Gb FCoE SR（short-range，短程）光纤 – 此配置要求在通用 HBA 的 SFP+ 连接器中安装 10 GbE 短程光纤收发器模块，可支持 10 GbE FCoE 聚合网络适配器功能。
- 16 Gb FC LW（longwave，长波）光纤 – 此配置要求在通用 HBA 的 SFP+ 连接器中安装 16 Gb FC 长波光纤收发器模块，可支持 16 Gb 光纤通道 HBA 功能。

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



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 之前和过程中，请查看本节中的内容。

本节包含以下主题：

硬件安全

保护物理硬件的方式非常简单：限制对硬件的接近和记录序列号。

- 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)。仅限经授权的人员接近带锁机柜。
- 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。

- 如果需要固件更新，请从以下 QLogic Web 站点的 Oracle 支持区域获取固件更新： http://www.driverdownloads.qlogic.com/QLogicDriverDownloads/Oracle_Search.aspx

  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” [8]
- “固件更新” [8]
- “软件更新 ” [8]
- “日志安全” [9]
- “模块安全” [9]

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。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.driverdownloads.qlogic.com/QLogicDriverDownloads/Oracle_Search.aspx。

- 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 QLogic QConvergeConsole 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。

QConvergeConsole 实用程序只允许具有 **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 QConvergeConsole CLI 和 GUI 的信息，请参见位于以下 Web 站点的 QLogic QConvergeConsole 文档： http://www.qlogic.com