Sun Flash Accelerator F40 PCIe 卡

安全指南

文件号码： E39698-02
2013 年 10 月

目录

• • • 第 1 章

Sun Flash Accelerator F40 PCIe 卡安全

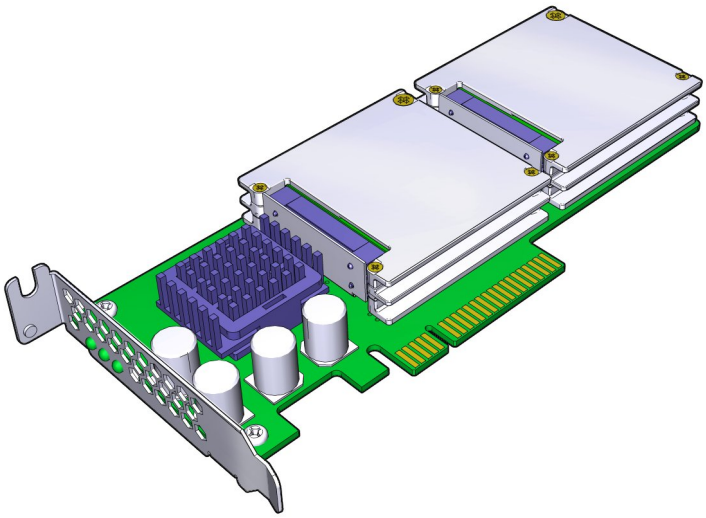
本文档介绍了一些常规安全准则，用于帮助您保护 Oracle x86 硬件产品，例如 Sun Flash Accelerator F40 PCIe 卡。

其中包括以下部分：

Sun Flash Accelerator F40 PCIe 卡说明

其中包括以下部分：

Sun Flash Accelerator F40 PCIe 卡是一款现成可用的 PCI-E 2.0 HBA 闪存存储卡，外形规格为窄板型。下图显示了 Sun Flash Accelerator F40 PCIe 卡：



有关详细的产品信息，请参阅《*Sun Flash Accelerator F40 PCIe* 卡用户指南》。

硬件组件

Sun Flash Accelerator F40 PCIe 卡包含以下硬件组件：

- 四个 SSD 闪存模块：卡上直接装配了总共 400 GB 的 32 nm eMLC NAND 闪存。
- 到 SAS 协议控制器的 PCI-E 接口：Sun Flash Accelerator F40 PCIe 卡到协议控制器的 SATA 接口具有连接 LSI 2008 SAS/SATA 2 x4 6 Gbps 协议控制器的 PCI-E 2.0 x8 主机接口。
- 能量存储组件：如果系统或 PCIe 插槽发生电源故障，未完成的写入将刷新到闪存中。

有关详细信息，请参阅《*Sun Flash Accelerator F40 PCIe* 卡用户指南》。

软件和固件组件

Sun Flash Accelerator F40 PCIe 卡中包含以下模块：

组件	请参见
MegaRAID Storage Manager (MSM)	第 7 页中的“MSM 应用程序安全”
诊断服务	第 8 页中的“诊断服务安全”
Linux 诊断驱动程序	第 9 页中的“Linux 诊断驱动程序安全”
SNMP	第 9 页中的“SNMP 安全”
WarpDrive 控制器 FW	第 10 页中的“WarpDrive 控制器固件安全”
SSDFW	第 10 页中的“SSDFW 安全”
DDCLI	第 11 页中的“DDCLI 安全”

有关详细信息，请参阅《*Sun Flash Accelerator F40 PCIe* 卡用户指南》。

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，访问限制通常表示物理访问限制。
  - 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及 Sun Flash Accelerator F40 PCIe 卡之前和期间，请遵循以下注意事项。

其中包括以下部分：

硬件安全

确保物理硬件安全的方式非常简单：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
  - 安全标记所有 Sun Flash Accelerator F40 PCIe 卡。使用特殊的紫外线笔或压纹标签。
  - 保留所有 Sun Flash Accelerator F40 PCIe 卡的序列号记录。
  - 将硬件激活密钥和许可证保留在一个安全位置，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

软件组件的安全注意事项包括：

- 请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 Sun Flash Accelerator F40 PCIe 卡驱动程序。
- 大多数硬件安全都通过软件方法实现。
- 支持 Sun Flash Accelerator F40 PCIe 卡的软件组件依赖系统安全功能来提供安全的访问。

固件安全

Sun Flash Accelerator F40 PCIe 卡附带的所有固件都已安装。除了更新以外，不需要实地安装固件。

- 如果需要更新固件，请联系 Oracle 技术支持来安排支持服务，或访问 Oracle 技术支持网站来获取有关产品的最新更新和过程。

  https://support.oracle.com

- 使用超级用户帐户设置和更新 Sun Flash Accelerator F40 PCIe 卡固件管理实用程序。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，请参阅随 Sun Flash Accelerator F40 PCIe 卡一起提供的产品说明。
- 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 Sun Flash Accelerator F40 PCIe 卡之后，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。

其中包括以下部分：

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.lsi.com。
- 有关最新发布的信息、软件更新要求信息或其他安全信息，请参阅随 Sun Flash Accelerator F40 PCIe 卡一起提供的产品说明。
- 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，将这些副本用于将来参考或统计分析。

模块安全

软件和固件模块包括：

- “MSM 应用程序安全” [9]
- “诊断服务安全” [10]
- “Linux 诊断驱动程序安全” [10]
- “SNMP 安全” [11]
- “SSDFW 安全” [11]
- “DDCLI 安全” [12]

注

文中的术语 WarpDrive 指 Sun Flash Accelerator F40 PCIe 卡。

MSM 应用程序安全

MegaRAID Storage Manager (MSM) 是一款软件应用程序，提供了通过驱动程序配置 WarpDrive 固件和与之交互的图形用户界面。MSM 还监视和维护 LSI® MegaRAID、SAS 和 WarpDrive 控制器上的存储配置。

Sun Flash Accelerator F40 PCIe 卡中 MSM 模块的安全注意事项包括：

- MegaRAID Storage Manager 兼容性：Linux 64 位、Solaris X86。
- 请参阅 LSI 提供的用户指南、MSM 中内置的联机帮助和安装程序提供的自述文件。访问 http://www.lsi.com。
- 需要先验证用户身份，然后才会允许用户进行访问。
  - 如果用户验证为 root 用户，则允许访问所有硬件。
  - 如果验证为一般用户，则仅允许查看。

- 通常，日志文件具有写权限，二进制文件具有执行权限，其他文件为只读文件。
- 每次只有一个用户具有管理权限。其他用户仅拥有查看权限。Java 内置随机数生成器用于在客户机-服务器验证时生成会话 ID。
- 客户机和服务器以 Java 实施。客户机和服务器使用 TCP/IP 来相互通信。服务器使用 JNI 与库进行通信。
- MSM 可与 Internet 进行交互，但不支持 IPv6。
- MSM 使用 SSL 在客户机和服务器之间进行通信。
- 系统的防火墙设置取决于执行的安装类型。
  - 在除本地安装以外的所有安装中，需要配置防火墙来控制对 MSM 客户机和服务器的访问。
  - 本地安装将使用 localhost IP。
- 需要有 root 用户访问权限来配置/修改设置。要限制潜在攻击者访问，请遵循以下指导准则。
  - 选择一个安全的密码。
  - 对所有运行 MSM 组件的系统（客户机和服务器）使用不同的密码。
- 或者，可以使用 LDAP 验证对服务器的访问。
- 可通过以下方式安装 MegaRAID Storage Manager (MSM)：
  - 完整版：安装所有组件。
  - 客户机版：仅安装远程查看和配置服务器所需的组件。需要打开端口 3071 和 5571。
  - 服务器版：仅安装远程服务器管理所需的组件。

    除了单播地址以外，MSM 服务器还使用多播 IP 地址 229.111.112.12 以及 TCP/UDP 端口 3071 和 5571。

    对于 SNMP，需要打开端口 161 和 162。如果配置了 LDAP，则需要打开端口 389。
  - 单机版：仅安装本地服务器管理所需的组件。
  - 本地版：仅安装本地服务器配置所需的组件。

诊断服务安全

诊断服务是一种服务守护进程应用程序，用于侦听由驱动程序发出的与 WarpDrive 关联的触发事件。当发生报告的事件或当用户请求时，诊断服务会从 WarpDrive 收集诊断信息。

Sun Flash Accelerator F40 PCIe 卡中诊断服务模块的安全注意事项包括：

- 诊断服务守护进程使用 storelib 库 API 来配置关注的触发事件以及获取事件通知。
- 诊断服务事件和日志信息仅通过 storelib 库 API 获取，并保存在日志文件中。
- 诊断服务使用 UDP 端口 162。
- 默认情况下会安装示例用户事件脚本文件，但不会使用此文件，除非出于调试目的对其进行了配置。
- 诊断服务配置和日志文件对于所有人均为只读，但 root 用户对其具有写权限。二进制文件对于所有人均为只读，但 root 用户对其具有写权限和执行权限。
- 诊断服务（如果配置）会在发生事件时发送 SNMP 陷阱消息。内部使用管道进行监视。

Linux 诊断驱动程序安全

Linux 诊断驱动程序是 MPT2SAS SAS2 6 Gb 驱动程序，可在启动时自动发布主机跟踪缓冲区 (2MB)，实施诊断服务触发器，并使用管理接口应用程序支持多种功能。该驱动程序基于触发器属性监视错误并添加新的诊断服务事件以供将来参考。

Sun Flash Accelerator F40 PCIe 卡中 Linux 诊断驱动程序的安全注意事项包括：

- Linux 诊断驱动程序在内核空间中运行。如果 OS 虚拟化，则驱动程序在父操作系统中运行。
- 发生一组触发事件时，Linux 诊断驱动程序会从固件中捕获跟踪缓冲区。这些触发事件由系统管理员指定，并在内核中通过 Sysfs 接口传入驱动程序。
- 只有具有权限的 root 用户才可以向 Linux 诊断驱动程序 Sysfs 属性文件写入数据。
- Linux 诊断驱动程序 SAS2 生成产品支持 EEDP（End-to-End Data Protection, 端到端数据保护）。
- Linux 诊断驱动程序位于硬件、固件和操作系统中间层之间。Linux 诊断驱动程序在底部使用已确立的行业 SAS2 和 SATA 协议以及 LSI 消息传递技术，在顶部使用 OS 调用来处理存储数据流。
- Linux 诊断驱动程序源代码是开源的，由 Linux 内核社区进行检查。
- Linux 诊断驱动程序对其管理的所有硬件具有完全访问权限，并对其运行所需的所有内核结构具有访问权限。Linux 诊断驱动程序对用于管理 SCSI IO 的所有内核接口具有完全访问权限。

SNMP 安全

通过 SNMP 代理，您可以使用简单网络管理协议 (Simple Network Management Protocol, SNMP) 管理和监视 LSI SAS 控制器。SNMP 支持的控制器系列包括 LSI MR、IR、IR2 和 WarpDrive。可以使用 MIB 浏览器或创建您自己的浏览器来监视和配置 LSI SNMP 代理公开的拓扑。

Sun Flash Accelerator F40 PCIe 卡中 SNMP 模块的安全注意事项包括：

- SNMP 子代理使用简单网络管理协议向 SNMP 客户机提供系统监视信息。
- SNMP 客户机可以是支持 SNMPv1 的任何 MIB 浏览器。
- MR/IR SNMP 子代理使用 storelib API 从 storelib 库中检索信息。Storelib 对驱动程序执行 IOCTL（input-output control，输入/输出控制）以获取该信息。
- SNMP 日志文件具有写权限，二进制文件具有执行权限，其他文件为只读文件。
- 对于任何 SNMP 访问，必须使用支持 Net-SNMP 验证机制的验证。

WarpDrive 控制器固件安全

WarpDrive 控制器固件在 WarpDrive 控制器板上运行。它向连接到 WarpDrive 控制器板的 SATA 固态驱动器 (SSD) 提供 6 Gbps 或传统的 3 Gbps 的传输速率。通过 PCIe 2.0 连接支持到 WarpDrive 控制器的主机连接。

Sun Flash Accelerator F40 PCIe 卡中 WarpDrive 控制器固件的安全注意事项包括：

- WarpDrive 控制器固件在位于控制器板上的处理器上执行操作。
- WarpDrive OS 驱动程序位于 WarpDrive 控制器固件的上方，使用 MPI（Message Passing Interface，消息传递接口）通过 PCIe 进行通信。
- WarpDrive 控制器固件使用 SAS/SATA 与其下方的 SSD 驱动器模块进行交互。
- 只允许将具有正确签名和校验和的 WarpDrive 控制器固件映像上载到板上。

SSDFW 安全

SSDFW 固件模块为 SF-2500 闪存存储处理器系列提供固件。

Sun Flash Accelerator F40 PCIe 卡中 SSDFW 模块的安全注意事项包括：

- SSDFW 固件模块一端连接 NAND 闪存接口，另一端连接 SATA AHCI 接口。
- 主机端通信通过 SATA 接口连接，在串行 ATA 规格和 ATA 命令集 (ACS-2) 规范中定义了该接口。
- SSDFW 固件模块默认具有管理权限。
- 日志文件已加密。通过串行端口支持日志记录。
- SSDFW 模块是驻留在 SF-2500 闪存存储处理器 ASIC 中的嵌入式固件。
- SSDFW 固件模块存储系统数据（例如驱动器状态）和用户数据，并将其放置在非易失性 NAND 介质中。所有系统数据均使用驱动器唯一密钥进行加密。
- 系统和用户密码用于获取权限。
- SSDFW 固件内嵌在 LSI-ASD 子系统中。
- AES-128 或 AES-256 用于对数据（纯文本）进行加密。SHA 引擎对固件进行验证。密钥和计数器值在存储到闪存之前会进行加密。

DDCLI 安全

DDCLI 是用户应用程序。DDCLI 是单机版 CLI，可用于监视任何连接系统的 WarpDrive。可以使用 ddcli 实用程序检索 WarpDrive 各个组件的重要信息。

Sun Flash Accelerator F40 PCIe 卡中 DDCLI 应用程序的安全注意事项包括：

- 提供的初始 DDCLI 不具有可执行权限。root 用户需要添加此权限。
- ddcli 文件需要更改其权限才能执行。为了尽可能减少安全问题，请将权限设置为 0744。该文件应归 root 用户所有。这样就允许所有人查看该文件，但只有 root 用户可以执行。
- 支持 MPT（Message Processing Technology，消息处理技术）API 的库静态链接到 DDCLI。该库将 IOCTL 发送到驱动程序以获取所需信息。
- DDCLI 应用程序是具有可执行权限的二进制文件。