Sun Flash Accelerator F40 PCIe Card

安全指南

文件號碼： E39699-02
2013 年 10 月

版權所有 © 2013 Oracle 和 (或) 其關係公司。 保留一切權利。

本軟體與相關說明文件是依據含有用途及保密限制事項的授權合約所提供，且受智慧財產法的保護。除了授權合約中或法律明文允許的部份外，不得以任何形式或方法使用、複製、重製、翻譯、廣播、修改、授權、傳送、散佈、展示、演出、出版或陳列本軟體的任何部份。除非依法需要取得互通性操作 (interoperability)，否則嚴禁對本軟體進行還原工程 (reverse engineering)、反向組譯 (disassembly) 或解編 (decompilation)。

本文件中的資訊如有變更恕不另行通知，且不保證沒有任何錯誤。如果您發現任何問題，請來函告知。

如果本軟體或相關說明文件是提供給美國政府或代表美國政府授權使用本軟體者，適用下列條例：

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.

本軟體或硬體是針對各類資訊管理應用程式的一般使用所開發。不適用任何原本就具危險性的應用上，包含會造成人身傷害風險的應用。如果您將本軟體或硬體應用於危險用途，則應採取適當的防範措施，包括保全、備份、儲備和其他措施以確保使用安全。Oracle Corporation 和其關係公司聲明對將本軟體或硬體應用於危險用途所造成之損害概不負任何責任。

Oracle 和 Java 是 Oracle 和 (或) 其關係公司的註冊商標。其他名稱為各商標持有人所擁有之商標。

Intel 和 Intel Xeon 是 Intel Corporation 的商標或註冊商標。所有 SPARC 商標的使用皆經過授權，且是 SPARC International, Inc. 的商標或註冊商標。AMD、Opteron、AMD 標誌與 AMD Opteron 標誌是 Advanced Micro Devices 的商標或註冊商標。UNIX 是 The Open Group 的註冊商標。

本軟體或硬體與說明文件可能提供第三方內容、產品和服務的存取途徑與資訊。Oracle Corporation 和其關係公司明文聲明對第三方網站所提供的內容、產品與服務不做保證，且不負任何責任。Oracle Corporation 和其關係公司對於您存取或使用第三方的內容、產品或服務所引起的任何損失、費用或損害亦不負任何責任。

目錄

1. Sun Flash Accelerator F40 PCIe Card 安全 5
    Sun Flash Accelerator F40 PCIe Card 描述 5
        硬體元件 6
        軟體與韌體元件 6
    安全性原則 6
    規劃安全的環境 7
        硬體安全 7
        軟體安全 7
        韌體安全 7
        Oracle ILOM 韌體 8
        系統記錄 8
    維護安全的環境 8
        資產追蹤 8
        韌體更新 8
        軟體更新 9
        記錄安全 9
        模組安全 9
        MSM 應用程式安全 9
        診斷服務安全 10
        Linux 診斷驅動程式安全 10
        SNMP 安全 11
        WarpDrive 控制器韌體安全 11
        SSDFW 安全 11
        DDCLI 安全 12

• • • 第 1 章

Sun Flash Accelerator F40 PCIe Card 安全

本文件提供一般性的安全指導方針，協助您保護 Sun Flash Accelerator F40 PCIe Card 之類的 Oracle x86 硬體產品。

內容包含下列小節：

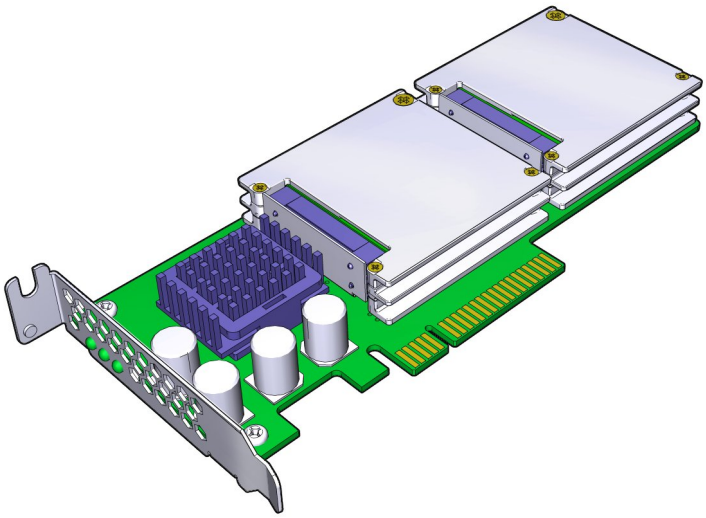
- 第 5 頁的 「Sun Flash Accelerator F40 PCIe Card 描述」
- 第 6 頁的 「安全性原則」
- 第 7 頁的 「規劃安全的環境」
- 第 8 頁的 「維護安全的環境」

Sun Flash Accelerator F40 PCIe Card 描述

內容包含下列小節：

- 第 6 頁的 「硬體元件」
- 第 6 頁的 「軟體與韌體元件」

Sun Flash Accelerator F40 PCIe Card 是一種整合式 PCI-E 2.0、HBA、短版外觀尺寸的快閃記憶體儲存卡。下圖為 Sun Flash Accelerator F40 PCIe Card：



如需詳細的產品資訊，請參閱 *Sun Flash Accelerator F40 PCIe Card User Guide*。

硬體元件

Sun Flash Accelerator F40 PCIe Card 包含下列硬體元件：

- 四個 SSD 快閃模組：介面卡上直接內建共 400 GB 的 32 nm eMLC NAND 快閃記憶體。
- PCI-E to SAS 協定控制器：Sun Flash Accelerator F40 PCIe Card SATA 協定控制器介面具有連接至 LSI 2008 SAS/SATA 2 x4 6 Gbps 協定控制器的 PCI-E 2.0 x8 主機介面。
- 儲能元件：系統或 PCIe 插槽斷電時，可將未完成的寫入資料送至快閃記憶體。

如需詳細資訊，請參閱 *Sun Flash Accelerator F40 PCIe Card User Guide*。

軟體與韌體元件

Sun Flash Accelerator F40 PCIe Card 包含下列模組：

元件	請參閱
MegaRAID Storage Manager (MSM)	MSM 應用程式安全，第 7 頁
診斷服務	診斷服務安全，第 8 頁
Linux 診斷驅動程式	Linux 診斷驅動程式安全，第 9 頁
SNMP	SNMP 安全，第 9 頁
WarpDrive 控制器韌體	WarpDrive 控制器韌體安全，第 10 頁
SSDFW	SSDFW 安全，第 10 頁
DDCLI	DDCLI 安全，第 11 頁

如需詳細資訊，請參閱 *Sun Flash Accelerator F40 PCIe Card User Guide*。

安全性原則

有四項安全性原則：存取、認證、授權及資料記錄。

- **存取**

  實體與軟體控制可保護您的硬體或資料避免遭受入侵。
  - 若為硬體，存取限制通常是指實體存取限制。
  - 若為軟體，則是透過實體和虛擬方式限制存取。
  - 除非透過 Oracle 更新程序，否則無法變更韌體。
- **認證**

  設定認證功能 (例如平台作業系統中的密碼系統功能) 來確認使用者的身分是否真實無誤。

  確認您的工作人員需正確配戴識別證才能進入電腦機房。
- **授權**

  僅允許受過訓練並符合使用資格的工作人員使用相應的硬體及軟體。設定系統的讀取/寫入/執行 (Read/Write/Execute) 權限，以控制使用者對指令、磁碟空間、裝置及應用程式的存取。
- **資料記錄**

  使用 Oracle 軟體和硬體功能，監視登入活動以及維護硬體資產。

- 使用系統記錄來監視使用者登入。尤其是監視系統管理員及服務帳號，因為這些帳號可以存取功能強大的指令。
- 使用元件序號來追蹤系統資產。所有介面卡、模組及主機板都有 Oracle 零件編號的電子記錄。

規劃安全的環境

安裝與配置伺服器及 Sun Flash Accelerator F40 PCIe Card 之前和期間，請參考下列注意事項。

內容包含下列小節：

- 第 7 頁的 「硬體安全 」
- 第 7 頁的 「軟體安全 」
- 第 7 頁的 「韌體安全」
- 第 8 頁的 「Oracle ILOM 韌體」
- 第 8 頁的 「系統記錄」

硬體安全

實體硬體的保護相當簡單：限制對於硬體的存取，並記錄序號。

- **限制存取**
  - 如果設備安裝在有門可以上鎖的機架內，除非必須維護或操作機架內的元件，否則請將機架門保持上鎖狀態。
  - 將備用的現場可更換單元 (FRU) 或客戶可更換單元 (CRU) 存放在上鎖的機櫃中。限制只有獲得授權的人員才能使用上鎖的機櫃。
- **記錄序號**
  - 為所有 Sun Flash Accelerator F40 PCIe Card 加上安全標誌。使用特殊的紫外線筆或浮水印標籤來加註安全標誌。
  - 保留所有 Sun Flash Accelerator F40 PCIe Card 的序號記錄。
  - 將硬體啟動金鑰與授權文件存放在安全的位置。發生系統緊急狀況時，系統管理人員必須能輕易地存取此位置。書面文件可能將成為擁有權的唯一證明。

軟體安全

軟體元件的安全考量如下：

- 參考軟體隨附的文件，啟用軟體提供的安全性功能。
- 使用超級使用者帳號，設定與更新 Sun Flash Accelerator F40 PCIe Card 驅動程式。
- 大部分硬體安全性是透過軟體的方式來實作。
- 支援 Sun Flash Accelerator F40 PCIe Card 的軟體元件，必須仰賴系統安全功能才能提供安全的存取。

韌體安全

Sun Flash Accelerator F40 PCIe Card 出廠時已安裝所有韌體。現場不需要安裝韌體，但可能需要更新。

- 若需要韌體更新，請洽詢 Oracle Support 安排支援人員，或查看 Oracle Support 有關產品的最新更新與程序。

https://support.oracle.com

- 使用超級使用者帳號，設定與更新 Sun Flash Accelerator F40 PCIe Card 韌體管理公用程式。一般使用者帳號僅允許使用者檢視韌體，但無法編輯韌體。Oracle Solaris OS 韌體更新處理作業禁止未經授權的韌體修改。
- 請參閱 Sun Flash Accelerator F40 PCIe Card 隨附的產品注意事項，瞭解最新資訊、韌體更新需求相關資訊，或其他安全資訊。
- 如需設定 SPARC OpenBootPROM (OBP) 安全變數的相關資訊，請參閱 *OpenBoot 4.x Command Reference Manual*。

Oracle ILOM 韌體

您可以使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 韌體，主動保護、管理及監視系統元件，此韌體已預先安裝在部分 x86 伺服器上。若要深入瞭解如何在進行設定密碼、管理使用者與套用 Secure Shell (SSH)、安全通訊端層 (SSL) 與 RADIUS 認證等安全相關功能時使用此韌體，請參閱 Oracle ILOM 文件：

http://www.oracle.com/pls/topic/lookup?ctx=ilom31

系統記錄

- 開啟記錄功能，並將記錄傳送至專用的安全記錄主機。
- 使用 NTP 與時戳設定記錄功能，以包含正確的時間資訊。

維護安全的環境

完成 Sun Flash Accelerator F40 PCIe Card 初始安裝及設定後，請使用 Oracle 硬體和軟體安全性功能來繼續控制硬體及追蹤系統資源。

內容包含下列小節：

- 第 8 頁的 「資產追蹤」
- 第 8 頁的 「韌體更新」
- 第 9 頁的 「軟體更新 」
- 第 9 頁的 「記錄安全」
- 第 9 頁的 「模組安全」

資產追蹤

可使用序號追蹤資產。Oracle 會在選項卡及系統主機版的韌體中嵌入序號。您可以透過區域網路連線看到這些序號。

您也可以使用無線電頻率識別 (RFID) 讀取器，進一步簡化資產的追蹤。請參閱 Oracle 白皮書「如何使用 *RFID* 追蹤您的 *Oracle Sun* 系統資產」。

韌體更新

請讓設備的韌體版本維持在最新狀態。

- 請定期檢查更新。
- 一般而言，所有作業系統 (特別是 Oracle Solaris) 會要求您以 root 證明資料登入，才能管理介面卡與升級驅動程式或韌體。
- 請務必安裝最新的韌體版本。

軟體更新

請讓設備的軟體版本維持在最新狀態。

- 您可以透過 Oracle Solaris 修補程式與更新，進行 Oracle Solaris 驅動程式的軟體更新。
- http://www.lsi.com 可能有其他作業系統的驅動程式軟體更新。
- 請參閱 Sun Flash Accelerator F40 PCIe Card 隨附的產品注意事項，瞭解最新資訊、軟體更新需求相關資訊，或其他安全資訊。
- 務必安裝最新的軟體版本。
- 安裝軟體任何必要的安全修補程式。
- 裝置也包含韌體，因此可能需要更新韌體。

記錄安全

定期檢查及維護您的記錄檔。

- 複查記錄以找出可能的未預期事件，然後依據安全性原則將它們歸檔。
- 當記錄檔超過合理的大小後，定期汰換記錄檔。保留汰換的檔案，以供日後參考或用於統計分析。

模組安全

軟體與韌體模組如下：

- 第 9 頁的 「MSM 應用程式安全」
- 第 10 頁的 「診斷服務安全」
- 第 10 頁的 「Linux 診斷驅動程式安全」
- 第 11 頁的 「SNMP 安全」
- 第 11 頁的 「SSDFW 安全」
- 第 12 頁的 「DDCLI 安全」



注意

內文中的 WarpDrive 一詞是指 Sun Flash Accelerator F40 PCIe Card。

MSM 應用程式安全

MegaRAID Storage Manager (MSM) 是一個軟體應用程式，它提供圖形使用者介面，經由驅動程式配置 WarpDrive 韌體並與之互動。MSM 亦監視與維護 LSI® MegaRAID、SAS 與 WarpDrive 控制器上的儲存配置。

Sun Flash Accelerator F40 PCIe Card 中 MSM 模組的安全考量如下：

- MegaRAID Storage Manager 相容性：Linux 64 位元、Solaris X86。
- 請參閱 LSI 提供的使用者指南、MSM 內建的線上說明，以及安裝程式提供的讀我檔案。請至 http://www.lsi.com。
- 使用者必須通過認證，才能進行存取。
  - 若使用者認證為 root，則允許存取所有硬體。
  - 若認證為使用者，則僅允許檢視的權限。

- 一般而言，記錄檔具有寫入權限、二進位檔案具有執行權限，其他檔案則為唯讀。
- 同一時間只能有一個使用者具備管理權限。其他使用者僅具備檢視權限。用戶端-伺服器認證時，會使用 Java 內建亂數產生器，產生一個階段作業 ID。
- 用戶端與伺服器是以 Java 實作。用戶端與伺服器使用 TCP/IP 彼此相互通訊。伺服器使用 JNI 與程式庫通訊。
- MSM 可與網際網路互動，但不支援 IPv6。
- MSM 使用 SSL 在用戶端與伺服器之間通訊。
- 系統的防火牆設定取決於執行的安裝類型。
  - 除了本機安裝之外，所有安裝必須將防火牆配置為控制 MSM 用戶端與伺服器的存取。
  - 本機安裝將會使用 Localhost IP。
- 需要 Root 使用者存取權，才能配置/修改設定。若要限制潛在攻擊者的存取，請遵循下列指示。
  - 選擇安全的密碼。
  - 在執行 MSM 元件 (包括用戶端與伺服器) 的所有系統使用不同的密碼。
- 也可以選擇使用 LDAP 來認證伺服器的存取權。
- MegaRAID Storage Manager (MSM) 可以使用下列方式來安裝：
  - 完整：安裝所有元件。
  - 用戶端：僅安裝遠端檢視與配置伺服器所需的元件。必須開啟連接埠 3071 與 5571。
  - 伺服器：僅安裝遠端伺服器管理所需的元件。

    除了單點傳送位址之外，MSM 伺服器亦使用多點傳送 IP 位址 229.111.112.12 以及 TCP/UDP 連接埠 3071 與 5571。

    針對 SNMP，必須開啟連接埠 161 與 162。若配置了 LDAP，則必須開啟連接埠 389。
  - 獨立：僅安裝本機伺服器管理所需的元件。
  - 本機：僅安裝本機伺服器配置所需的元件。

診斷服務安全

「診斷服務」是一個服務常駐應用程式，監聽驅動程式所發出的 WarpDrive 關聯觸發事件。當發生報告事件或使用者要求時，「診斷服務」會從 WarpDrive 收集診斷資訊。

Sun Flash Accelerator F40 PCIe Card 中「診斷服務」模組的安全考量如下：

- 「診斷服務」常駐程式使用 storelib 程式庫 API，配置所要的觸發事件並取得事件通知。
- 只有透過 storelib 程式庫 API 才能取得「診斷服務」事件與記錄資訊，並儲存在記錄檔中。
- 「診斷服務」使用 UDP 連接埠 162。
- 預設會安裝一個範例使用者事件命令檔，但是除非配置供除錯之用，否則不會使用該命令檔。
- 「診斷服務」配置與記錄檔對於所有人為唯讀，root 使用者則有寫入權限。二進位檔案對於所有人為唯讀，但是 root 使用者則有寫入與執行權限。
- 若配置了「診斷服務」，則可能在事件發生時傳送 SNMP 設陷訊息。內部將會使用管線來監視。

Linux 診斷驅動程式安全

「Linux 診斷驅動程式」為 MPT2SAS SAS2 6 Gb 驅動程式，可在啟動時自動宣告 Host Trace Buffer (2MB)、實作診斷服務觸發程式，並使用管理介面應用程式支援多功能。根據觸發程式的屬性，驅動程式可監視錯誤，並新增新的診斷服務事件以供日後參考。

Sun Flash Accelerator F40 PCIe Card 中「Linux 診斷驅動程式」的安全考量如下：

- 「Linux 診斷驅動程式」是在核心空間中執行。若是虛擬化作業系統，驅動程式會在上層空間中執行。
- 一組觸發事件發生時，「Linux 診斷驅動程式」會從韌體擷取追蹤緩衝區。這些觸發事件是由系統管理員指定，經由核心的 Sysfs 介面送入驅動程式。
- 只有具備 root 權限的使用者可以寫入「Linux 診斷驅動程式」Sysfs 屬性檔。
- 「Linux 診斷驅動程式」SAS2 這一代的產品支援 EEDP (點對點資料保護)。
- 「Linux 診斷驅動程式」是介於硬體、韌體與作業系統之間的中間層。「Linux 診斷驅動程式」在底端使用業界通用的 SAS2 與 SATA 協定及 LSI 訊息傳遞技術，頂端則是作業系統呼叫，以處理儲存資料流程。
- 「Linux 診斷驅動程式」為開放程式碼，由 Linux 核心社群所核可。
- 「Linux 診斷驅動程式」可完整存取它所管理的所有硬體，以及存取功能運作所需的所有核心架構。「Linux 診斷驅動程式」可完整存取用於管理 SCSI IO 的所有核心介面。

SNMP 安全

SNMP 代理程式可使用 Simple Network Management Protocol (SNMP) 管理與監視 LSI SAS 控制器。SNMP 支援的控制器系列為 LSI MR、IR、IR2 與 WarpDrive。您可以使用 MIB 瀏覽器或自行建立以監視與配置 LSI SNMP 代理程式公開的拓樸。

Sun Flash Accelerator F40 PCIe Card 中 SNMP 模組的安全考量如下：

- SNMP 子代理程式使用 Simple Network Management Protocol，提供監視系統的資訊給 SNMP 用戶端。
- SNMP 用戶端可以是支援 SNMPv1 的任何 MIB 瀏覽器。
- MR/IR SNMP 子代理程式使用 storelib API 擷取 storelib 程式庫的資訊。Storelib 藉由驅動程式 IOCTL (輸入-輸出控制) 取得該資訊。
- SNMP 記錄檔具有寫入權限、二進位檔案具有執行權限，其他檔案則為唯讀。
- SNMP 存取需要使用支援 Net-SNMP 認證機制的認證。

WarpDrive 控制器韌體安全

「WarpDrive 控制器」韌體是在 WarpDrive 控制器板上執行。它對連接至 WarpDrive 控制器板的 SATA 固態硬碟 (DFF)，提供 6 Gbps 或舊式 3 Gbps 的傳輸率。WarpDrive 控制器的主機連線是透過 PCIe 2.0 連線。

Sun Flash Accelerator F40 PCIe Card 中「WarpDrive 控制器」韌體的安全考量如下：

- 「WarpDrive 控制器」韌體是在 WarpDrive 控制器板上的處理器中執行。
- WarpDrive 作業系統驅動程式位於「WarpDrive 控制器」韌體之上，使用 MPI (訊息傳遞介面) 透過 PCIe 來通訊。
- 「WarpDrive 控制器」韌體使用 SAS/SATA 介面，與其下的 SSD 磁碟機模組互動。
- 只有具有正確簽章與總和檢驗的「WarpDrive 控制器」韌體影像才能上傳至機板上。

SSDFW 安全

SSDFW 韌體模組提供 SF-2500 Flash Storage Processor 系列的韌體。

Sun Flash Accelerator F40 PCIe Card 中 SSDFW 模組的安全考量如下：

- SSDFW 韌體模組一端連接至 NAND Flash 介面，另一端連接至 SATA AHCI 介面。

- 主機端通訊透過 Serial ATA 規格與 ATA Command Set (ACS-2) 規格定義的 SATA 介面連接。
- 預設具備 SSDFW 韌體模組管理權限。
- 記錄檔會加密。記錄是經由序列埠來進行。
- SSDFW 模組是位於 SF-2500 Flash Storage Processor ASIC 中內嵌的韌體。
- SSDFW 韌體模組儲存系統資料 (例如，磁碟機狀態) 與使用者資料，並將之置於非揮發性 NAND 媒體。所有系統資料均以磁碟機唯一金鑰加密。
- 使用系統與使用者密碼來取得權限。
- SSDFW 韌體內嵌在 LSI-ASD 子系統中。
- 使用 AES-128 或 AES-256 來加密資料 (純文字)。SHA 引擎負責認證韌體。金鑰與計數器值在存入快閃記憶體之前會先加密。

DDCLI 安全

DDCLI 為使用者應用程式。DDCLI 是一個獨立 CLI，可監視系統連接的任何 WarpDrive。使用 ddcli 公用程式可擷取 WarpDrive 各種元件的重要資訊。

Sun Flash Accelerator F40 PCIe Card 中 DDCLI 應用程式的安全考量如下：

- DDCLI 出廠時並無執行權限。root 使用者將必須新增此權限。
- 必須變更檔案 ddcli 的權限，才能加以執行。為了儘量減少安全問題，請將權限設為 0744。檔案應該由 root 擁有。如此可讓所有人檢視檔案，但只有 root 使用者能夠執行檔案。
- 支援 MPT (訊息處理技術) API 的程式庫會靜態連結 DDCLI。該程式庫會傳送 IOCTL 至驅動程式，以取得必要的資訊。
- DDCLI 應用程式為具有執行權限的二進位檔案。