Sun Flash Accelerator F40 PCIe Card

보안 설명서

Part No: E39697-02
2013년 10월

Copyright © 2013 Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이센스 계약서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이센스 계약서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이센스, 전송, 배포, 진열, 실행, 발행, 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이센스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

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.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이센스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이센스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고, 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제 3자로부터 제공되는 컨텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. Oracle Corporation과 그 자회사는 제 3자의 컨텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제 3자의 컨텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다.

차례

1. Sun Flash Accelerator F40 PCIe Card 보안 5
- Sun Flash Accelerator F40 PCIe Card 설명 5
  - 하드웨어 구성 요소 6
  - 소프트웨어 및 펌웨어 구성 요소 6
- 보안 원칙 6
- 보안 환경 계획 7
  - 하드웨어 보안 7
  - 소프트웨어 보안 8
  - 펌웨어 보안 8
  - Oracle ILOM 펌웨어 8
  - 시스템 로그 8
- 보안 환경 유지 관리 9
  - 자산 추적 9
  - 펌웨어 업데이트 9
  - 소프트웨어 업데이트 9
  - 로그 보안 9
  - 모듈 보안 10
  - MSM 응용 프로그램 보안 10
  - Diagnostic Services 보안 11
  - Linux Diagnostic Driver 보안 11
  - SNMP 보안 12
  - WarpDrive Controller Firmware 보안 12
  - SSDFW 보안 12
  - DDCLI 보안 13

• • • 1 장

Sun Flash Accelerator F40 PCIe Card 보안

이 문서는 Sun Flash Accelerator F40 PCIe Card와 같은 Oracle x86 하드웨어 제품을 보호하는 데 도움이 되는 일반 보안 지침을 제공합니다.

이 문서는 다음 섹션으로 구성되어 있습니다.

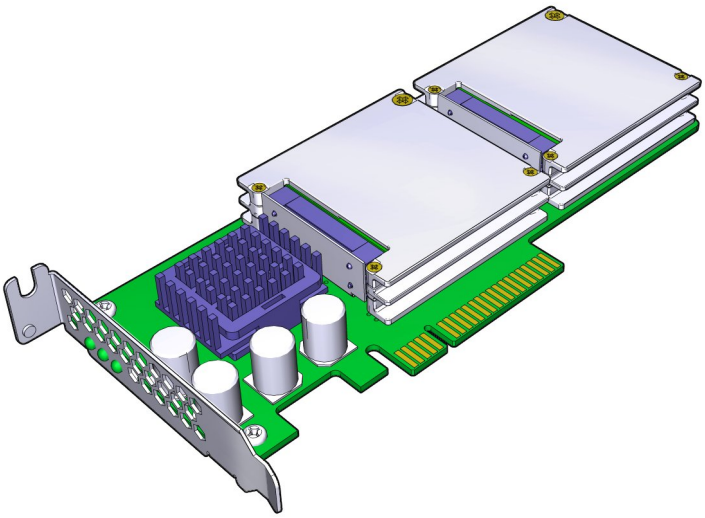
- “Sun Flash Accelerator F40 PCIe Card 설명” [5]
- “보안 원칙” [6]
- “보안 환경 계획” [7]
- “보안 환경 유지 관리” [9]

Sun Flash Accelerator F40 PCIe Card 설명

이 문서는 다음 섹션으로 구성되어 있습니다.

- “하드웨어 구성 요소” [6]
- “소프트웨어 및 펌웨어 구성 요소” [6]

Sun Flash Accelerator F40 PCIe Card는 턴키 PCI-E 2.0, HBA, 로우 프로파일 폼 팩터를 사용하는 플래시 메모리 스토리지 카드입니다. 다음 이미지는 Sun Flash Accelerator F40 PCIe Card를 보여줍니다.



자세한 제품 정보는 Sun Flash Accelerator F40 PCIe Card User Guide를 참조하십시오.

하드웨어 구성 요소

Sun Flash Accelerator F40 PCIe Card에는 다음과 같은 하드웨어 구성 요소가 포함되어 있습니다.

- 4개의 SSD 플래시 모듈: 총 400GB 32nm eMLC NAND 플래시 메모리가 카드에 직접 마운트되어 있습니다.
- PCI-E - SAS 간 프로토콜 컨트롤러: 프로토콜 컨트롤러에 대한 Sun Flash Accelerator F40 PCIe Card SATA 인터페이스에는 LSI 2008 SAS/SATA 2 x4 6Gbps 프로토콜 컨트롤러에 연결된 PCI-E 2.0 x8 호스트 인터페이스가 있습니다.
- 에너지 스토리지 구성 요소: 시스템 또는 PCIe 슬롯 전원 공급이 중단되면 완료되지 않은 쓰기 작업을 플래시 메모리로 비웁니다.

자세한 내용은 Sun Flash Accelerator F40 PCIe Card User Guide를 참조하십시오.

소프트웨어 및 펌웨어 구성 요소

Sun Flash Accelerator F40 PCIe Card에는 다음 모듈이 포함되어 있습니다.

구성 요소	참조 항목
MSM(MegaRAID Storage Manager)	7페이지의 “MSM 응용 프로그램 보안”
Diagnostic Services	8페이지의 “Diagnostic Services 보안”
Linux Diagnostic Driver	9페이지의 “Linux Diagnostic Driver 보안”
SNMP	9페이지의 “SNMP 보안”
WarpDrive Controller FW	10페이지의 “WarpDrive Controller Firmware 보안”
SSDFW	10페이지의 “SSDFW 보안”
DDCLI	11페이지의 “DDCLI 보안”

자세한 내용은 Sun Flash Accelerator F40 PCIe Card User Guide를 참조하십시오.

보안 원칙

액세스, 인증, 권한 부여 및 계정 관리의 네 가지 기본 보안 원칙이 있습니다.

- **액세스**

  물리적 제어 및 소프트웨어 제어를 통해 침입으로부터 하드웨어 또는 데이터를 보호합니다.
  - 하드웨어의 경우 액세스 제한은 일반적으로 물리적 액세스 제한을 의미합니다.
  - 소프트웨어의 경우 액세스는 물리적 수단 및 가상 수단을 통해 제한됩니다.
  - 펌웨어는 Oracle 업데이트 프로세스를 통해서만 변경될 수 있습니다.
- **인증**

  사용자가 실제로 등록된 사용자인지 확인할 수 있도록 사용 중인 플랫폼 운영 체제에서 암호 시스템 등의 인증 기능을 설정합니다.

  담당자가 컴퓨터실에 출입할 때는 사원 명찰을 사용하도록 합니다.
- **권한 부여**

  담당자가 사용 교육 및 자격을 받은 하드웨어와 소프트웨어만 사용할 수 있도록 합니다. 읽기/쓰기/실행 권한 시스템을 설정하여 명령, 디스크 공간, 장치 및 응용 프로그램에 대한 사용자 액세스 권한을 제어합니다.
- **계정 관리**

  Oracle 소프트웨어 및 하드웨어 기능을 사용하여 로그인 활동을 모니터하고 하드웨어 인벤토리를 유지 관리합니다.
  - 시스템 로그를 사용하여 사용자 로그인을 모니터할 수 있습니다. 특히 시스템 관리자 및 서비스 계정은 강력한 명령에 액세스할 수 있으므로 반드시 모니터하십시오.
  - 구성 요소 일련 번호를 사용하여 시스템 자산을 추적할 수 있습니다. Oracle 부품 번호는 모든 카드, 모듈 및 마더보드에 전자적으로 기록되어 있습니다.

보안 환경 계획

서버 및 Sun Flash Accelerator F40 PCIe Card를 설치하고 구성하기 전과 도중에 다음 사항을 참고하십시오.

이 문서는 다음 섹션으로 구성되어 있습니다.

- “하드웨어 보안 ” [7]
- “소프트웨어 보안 ” [8]
- “펌웨어 보안” [8]
- “Oracle ILOM 펌웨어” [8]
- “시스템 로그” [8]

하드웨어 보안

물리적 하드웨어는 하드웨어에 대한 액세스 제한 및 일련 번호 기록을 통해 매우 간단하게 보안을 설정할 수 있습니다.

- **액세스 제한**
  - 잠금 문이 있는 랙에 장비가 설치된 경우 랙의 구성 요소를 수리해야 하는 경우를 제외하고는 문을 잠가 둡니다.
  - 예비 현장 교체 가능 장치(Field-Replaceable Unit, FRU) 또는 자가 교체 가능 장치(Customer-Replaceable Unit, CRU)는 잠긴 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 접근할 수 있도록 제한합니다.

- **일련 번호 기록**
  - 모든 Sun Flash Accelerator F40 PCIe Card에 보안 표시를 합니다. 특수 자외선 펜 또는 돌출된 레이블을 사용합니다.
  - 모든 Sun Flash Accelerator F40 PCIe Card의 일련 번호 기록을 보관합니다.
  - 시스템 긴급 상황 시 시스템 관리자가 쉽게 액세스할 수 있는 보안 위치에 하드웨어 활성화 키 및 라이센스를 보유합니다. 인쇄된 문서가 유일한 소유권 증명이 될 수도 있습니다.

소프트웨어 보안

소프트웨어 구성 요소에 대한 보안 고려 사항은 다음과 같습니다.

- 소프트웨어에 사용 가능한 보안 기능을 사용으로 설정하려면 소프트웨어와 함께 제공된 설명서를 참조하십시오.
- Sun Flash Accelerator F40 PCIe Card 드라이버를 설치하거나 업데이트할 때는 수퍼 유저 계정을 사용합니다.
- 대부분의 하드웨어 보안은 소프트웨어 수단을 통해 구현됩니다.
- Sun Flash Accelerator F40 PCIe Card를 지원하는 소프트웨어 구성 요소는 시스템 보안 기능을 사용하여 보안 액세스를 제공합니다.

펌웨어 보안

Sun Flash Accelerator F40 PCIe Card는 설치된 모든 펌웨어와 함께 제공됩니다. 업데이트하는 경우가 아니라면 펌웨어를 설치할 필요는 없습니다.

- 펌웨어 업데이트가 필요한 경우 오라클 고객지원센터에 문의하여 지원을 요청하거나 제품에 대한 최신 업데이트 및 절차를 확인하십시오.

  https://support.oracle.com
- Sun Flash Accelerator F40 PCIe Card 펌웨어 관리 유틸리티를 설치하거나 업데이트할 때는 수퍼 유저 계정을 사용하십시오. 일반 사용자 계정을 사용하면 펌웨어를 볼 수는 있지만 편집할 수 없습니다. Oracle Solaris OS 펌웨어 업데이트 프로세스에서는 권한이 없는 사용자가 펌웨어를 수정할 수 없습니다.
- Sun Flash Accelerator F40 PCIe Card와 함께 제공된 제품 안내서에서 최신 뉴스, 펌웨어 업데이트 요구 사항에 대한 정보 또는 기타 보안 정보를 확인하십시오.
- SPARC OBP(OpenBootPROM) 보안 변수 설정에 대한 정보는 OpenBoot 4.x Command Reference Manual을 참조하십시오.

Oracle ILOM 펌웨어

일부 x86 서버에 사전 설치된 Oracle ILOM(Integrated Lights Out Manager) 펌웨어를 사용하여 적극적으로 시스템 구성 요소를 보안, 관리 및 모니터할 수 있습니다. 암호 설정, 사용자 관리 및 보안 셸(Secure Shell, SSH), SSL(Secure Socket Layer), RADIUS 인증을 비롯한 보안 관련 기능을 적용할 때 이 펌웨어 사용에 대해 좀 더 자세하게 이해하려면 다음 Oracle ILOM 설명서를 참조하십시오.

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

시스템 로그

- 로깅을 사용으로 설정하고 로그를 전용 보안 로그 호스트로 보냅니다.
- NTP 및 타임스탬프를 사용하여 정확한 시간 기록 정보가 포함되도록 로깅을 구성합니다.

보안 환경 유지 관리

Sun Flash Accelerator F40 PCIe Card의 초기 설치 및 설정 후 계속하여 Oracle 하드웨어 및 소프트웨어 보안 기능을 사용하여 하드웨어를 제어하고 시스템 자산을 추적할 수 있습니다.

이 문서는 다음 섹션으로 구성되어 있습니다.

- "자산 추적" [9]
- "펌웨어 업데이트" [9]
- "소프트웨어 업데이트 " [9]
- "로그 보안" [9]
- "모듈 보안" [10]

자산 추적

일련 번호를 사용하여 인벤토리를 추적할 수 있습니다. Oracle은 옵션 카드 및 시스템 마더보드의 펌웨어에 일련 번호를 포함합니다. LAN 연결을 통해 이러한 일련 번호를 확인할 수 있습니다.

또한 무선 RFID(Radio Frequency Identification) 판독기를 사용하여 자산 추적을 추가로 간소화할 수 있습니다. Oracle 백서 How to Track Your Oracle Sun System Assets by Using RFID를 참조하십시오.

펌웨어 업데이트

장비에서 펌웨어 버전을 최신 상태로 유지합니다.

- 정기적으로 업데이트를 확인하십시오.
- 운영 체제들이 대개 그렇지만 특히 Oracle Solaris에서는 카드를 관리하거나 드라이버 또는 펌웨어를 업그레이드하려면 루트 자격 증명으로 로그인해야 합니다.
- 항상 펌웨어의 최신 릴리스 버전을 설치하십시오.

소프트웨어 업데이트

장비에서 소프트웨어 버전을 최신 상태로 유지합니다.

- Oracle Solaris 드라이버에 대한 소프트웨어 업데이트는 Oracle Solaris 패치 및 업데이트를 통해 제공됩니다.
- 다른 운영 체제 드라이버의 소프트웨어 업데이트는 http://www.lsi.com에서 찾아볼 수 있습니다.
- Sun Flash Accelerator F40 PCIe Card와 함께 제공된 제품 안내서에서 최신 뉴스, 소프트웨어 업데이트 요구 사항에 대한 정보 또는 기타 보안 정보를 확인하십시오.
- 항상 소프트웨어의 최신 릴리스 버전을 설치하십시오.
- 소프트웨어에 필요한 모든 보안 패치를 설치하십시오.
- 장치에는 펌웨어가 포함되어 있으며 펌웨어 업데이트가 필요할 수도 있습니다.

로그 보안

정기적으로 로그 파일을 검사하고 유지 관리합니다.

- 발생 가능한 문제에 대비하여 로그를 검토하고 보안 정책에 따라 아카이브하십시오.
- 로그 파일이 적당한 크기를 초과할 경우 주기적으로 로그 파일을 처분하십시오. 나중에 참조하거나 통계 분석에 사용할 수 있도록 처분할 파일의 복사본을 유지 관리하십시오.

모듈 보안

소프트웨어 및 펌웨어 모듈은 다음을 참조하십시오.

- “MSM 응용 프로그램 보안” [10]
- “Diagnostic Services 보안” [11]
- “Linux Diagnostic Driver 보안” [11]
- “SNMP 보안” [12]
- “SSDFW 보안” [12]
- “DDCLI 보안” [13]



참고

여기서 WarpDrive라는 용어는 Sun Flash Accelerator F40 PCIe Card를 가리킵니다.

MSM 응용 프로그램 보안

MSM(MegaRAID Storage Manager)은 드라이버를 통해 WarpDrive 펌웨어를 구성하고 상호 작용하는 그래픽 사용자 인터페이스를 제공하는 소프트웨어 응용 프로그램입니다. MSM은 또한 LSI® MegaRAID, SAS 및 WarpDrive 컨트롤러에서 스토리지 구성을 모니터 및 유지 관리합니다.

Sun Flash Accelerator F40 PCIe Card의 MSM 모듈에 대한 보안 고려 사항은 다음과 같습니다.

- MegaRAID Storage Manager 호환성: Linux 64비트, Solaris X86
- LSI에서 제공하는 사용자 설명서, MSM에 기본 제공되는 온라인 도움말 및 설치 프로그램과 함께 제공되는 readme 파일을 참조합니다. http://www.lsi.com을 방문해 보십시오.
- 사용자는 액세스하기 전에 인증을 받아야 합니다.
  - 사용자가 루트로 인증되면 모든 하드웨어 액세스가 허용됩니다.
  - 사용자로 인증되면 읽기 전용 권한이 허용됩니다.
- 대개 로그 파일에는 쓰기 권한이, 이진 파일에는 실행 권한이, 기타 파일에는 읽기 전용 권한이 있습니다.
- 한 번에 한 명의 사용자만 관리자 권한을 가질 수 있습니다. 다른 사용자는 읽기 전용 권한을 가집니다. 클라이언트-서버 인증 시 Java 기본 제공 난수 생성기를 사용하여 세션 ID가 생성됩니다.
- 클라이언트와 서버는 Java로 구현됩니다. 클라이언트와 서버는 TCP/IP를 사용하여 서로 통신합니다. 서버는 JNI를 사용하여 라이브러리와 통신합니다.
- MSM은 인터넷과 상호 작용하지만 IPv6은 지원하지 않습니다.
- MSM은 클라이언트와 서버 간 통신에 SSL을 사용합니다.
- 시스템의 방화벽 설정은 수행된 설치 유형에 따라 다릅니다.
  - 로컬을 제외한 모든 설치에서 MSM 클라이언트 및 서버에 대한 액세스를 제어하기 위해 방화벽을 구성해야 합니다.
  - 로컬 설치는 localhost IP를 사용합니다.
- 설정을 구성/수정하려면 루트 사용자 액세스가 필요합니다. 잠재적인 공격자의 액세스를 제한하려면 다음 지침을 따릅니다.
  - 보안 암호를 선택합니다.
  - MSM 구성 요소를 실행하는 모든 시스템(클라이언트, 서버 모두)에 서로 다른 암호를 사용합니다.
- 원하는 경우 LDAP를 사용하여 서버에 대한 액세스를 인증할 수 있습니다.

- MSM(MegaRAID Storage Manager)은 다음과 같은 방법으로 설치할 수 있습니다.
  - 전체: 모든 구성 요소가 설치됩니다.
  - 클라이언트: 원격으로 서버를 보고 구성하는 데 필요한 구성 요소만 설치됩니다. 포트 3071 및 5571을 열어야 합니다.
  - 서버: 원격 서버 관리에 필요한 구성 요소만 설치됩니다.

    유니캐스트 주소 외에도 MSM 서버는 멀티캐스트 IP 주소 229.111.112.12 및 TCP/UDP 포트 3071, 5571을 사용합니다.

    SNMP의 경우 포트 161 및 162를 열어야 합니다. LDAP가 구성된 경우 포트 389를 열어야 합니다.
  - 독립형: 로컬 서버 관리에 필요한 구성 요소만 설치됩니다.
  - 로컬: 로컬 서버 구성에 필요한 구성 요소만 설치됩니다.

Diagnostic Services 보안

Diagnostic Services는 드라이버가 발생시킨 WarpDrive와 연관된 트리거 이벤트를 수신하는 서비스 데몬 응용 프로그램입니다. Diagnostic Services는 보고된 이벤트가 발생하거나 사용자가 요청할 때 WarpDrive에서 진단 정보를 수집합니다.

Sun Flash Accelerator F40 PCIe Card의 Diagnostic Services 모듈에 대한 보안 고려 사항은 다음과 같습니다.

- Diagnostic Services 데몬은 storelib 라이브러리 API를 사용하여 관련 트리거 이벤트를 구성하고 이벤트 통지를 가져옵니다.
- Diagnostic Services 이벤트 및 로그 정보는 storelib 라이브러리 API를 통해서만 획득되며 로그 파일에 저장됩니다.
- Diagnostic Services는 UDP 포트 162를 사용합니다.
- 샘플 사용자 이벤트 스크립트 파일이 기본적으로 설치되지만 디버깅 목적으로 구성되지 않는 한 사용되지 않습니다.
- Diagnostic Services 구성 및 로그 파일은 모든 사용자가 읽을 수 있으며 루트 사용자는 쓸 수 있습니다. 이진 파일은 모든 사용자가 읽을 수 있으며 루트 사용자는 쓰고 실행할 수 있습니다.
- 구성된 경우 Diagnostic Services는 이벤트가 발생할 때 SNMP 트랩 메시지를 보낼 수 있습니다. 모니터링을 위해 내부적으로 파이프가 사용됩니다.

Linux Diagnostic Driver 보안

Linux Diagnostic Driver는 시작 시 자동으로 Host Trace Buffer(2MB)를 게시하고, Diagnostic Service 트리거를 구현하고, 관리 인터페이스 응용 프로그램을 사용하여 여러 기능을 지원할 수 있는 MPT2SAS SAS2 6GB 드라이버입니다. 트리거 속성을 바탕으로 이 드라이버는 오류를 모니터하고, 향후 참조를 위해 새 Diagnostic Service 이벤트를 추가합니다.

Sun Flash Accelerator F40 PCIe Card의 Linux Diagnostic Driver에 대한 보안 고려 사항은 다음과 같습니다.

- Linux Diagnostic Driver는 커널 공간에서 실행됩니다. OS가 가상화된 경우 이 드라이버는 상위에서 실행됩니다.
- Linux Diagnostic Driver는 일련의 트리거 이벤트가 발생하면 펌웨어에서 추적 버퍼를 캡처합니다. 이러한 트리거 이벤트는 시스템 관리자에 의해 지정되며 커널의 Sysfs 인터페이스를 통해 드라이버에 전달됩니다.
- 루트 권한이 있는 사용자만 Linux Diagnostic Driver Sysfs 속성 파일에 쓸 수 있습니다.

- Linux Diagnostic Driver SAS2 생성 제품은 EEDP(End-to-End Data Protection)를 지원합니다.
- Linux Diagnostic Driver는 하드웨어, 펌웨어 및 운영 체제 중간 계층 사이에 있습니다. Linux Diagnostic Driver는 아래쪽에서는 확립된 업계 SAS2 및 SATA 프로토콜과 LSI 메시지 전달 기술을 사용하고, 위쪽에서는 OS 호출을 사용하여 스토리지 데이터 플로우를 처리합니다.
- Linux Diagnostic Driver 소스는 오픈 소스이며 Linux 커널 커뮤니티에 의해 점검됩니다.
- Linux Diagnostic Driver는 관리 중인 모든 하드웨어 및 이 하드웨어가 작동하는 데 필요한 모든 커널 구조에 대해 전체 액세스 권한을 가집니다. Linux Diagnostic Driver는 SCSI IO 관리에 사용되는 모든 커널 인터페이스에 대해 전체 액세스 권한을 가집니다.

SNMP 보안

SNMP 에이전트를 통해 SNMP(Simple Network Management Protocol)를 사용하여 LSI SAS 컨트롤러를 관리하고 모니터할 수 있습니다. SNMP에서 지원하는 컨트롤러 제품군은 LSI MR, IR, IR2 및 WarpDrive입니다. MIB 브라우저를 사용하거나 자체 브라우저를 만들어 LSI SNMP 에이전트가 표시하는 토폴로지를 모니터하고 구성할 수 있습니다.

Sun Flash Accelerator F40 PCIe Card의 SNMP 모듈에 대한 보안 고려 사항은 다음과 같습니다.

- SNMP 하위 에이전트는 Simple Network Management Protocol을 사용하여 모니터링 시스템의 정보를 SNMP 클라이언트에 제공합니다.
- SNMPv1을 지원하는 모든 MIB 브라우저는 SNMP 클라이언트가 될 수 있습니다.
- MR/IR SNMP 하위 에이전트는 storelib API를 사용하여 storelib 라이브러리에서 정보를 검색합니다. Storelib는 해당 정보를 가져오기 위해 드라이버에 대한 IOCTL(입력-출력 컨트롤)을 만듭니다.
- SNMP 로그 파일에는 쓰기 권한이, 이진 파일에는 실행 권한이, 기타 파일에는 읽기 전용 권한이 있습니다.
- 모든 SNMP 액세스에는 Net-SNMP 지원 인증 메커니즘을 사용하는 인증이 필요합니다.

WarpDrive Controller Firmware 보안

WarpDrive Controller Firmware는 WarpDrive 컨트롤러 보드에서 실행됩니다. 이 펌웨어는 WarpDrive 컨트롤러 보드에 연결된 SATA 반도체 드라이브(SSD)에 대해 6Gbps 또는 레거시 3Gbps 전송 속도를 제공합니다. WarpDrive 컨트롤러에 대한 호스트 연결은 PCIe 2.0 연결을 통해 지원됩니다.

Sun Flash Accelerator F40 PCIe Card의 WarpDrive Controller Firmware에 대한 보안 고려 사항은 다음과 같습니다.

- WarpDrive Controller Firmware는 컨트롤러 보드에 있는 프로세서에서 실행됩니다.
- WarpDrive OS 드라이버는 WarpDrive Controller Firmware 위에 있으며 MPI(메시지 전달 인터페이스)를 사용하여 PCIe를 통해 통신합니다.
- WarpDrive Controller Firmware는 SAS/SATA 인터페이스를 사용하여 펌웨어는 아래에 있는 SSD 드라이브 모듈과 상호 작용합니다.
- 올바른 서명 및 체크섬이 있는 WarpDrive Controller Firmware 이미지만 보드로 업로드가 허용됩니다.

SSDFW 보안

SSDFW 펌웨어 모듈은 SF-2500 Flash Storage Processor 제품군에 대한 펌웨어를 제공합니다.

Sun Flash Accelerator F40 PCIe Card의 SSDFW 모듈에 대한 보안 고려 사항은 다음과 같습니다.

- SSDFW 펌웨어 모듈은 한 쪽으로는 NAND 플래시 인터페이스에 연결되고 다른 쪽으로는 SATA AHCI 인터페이스에 연결됩니다.
- 호스트 측 통신은 Serial ATA Specification 및 ATA Command Set(ACS-2) Specification에 정의된 SATA 인터페이스를 통해 연결됩니다.
- SSDFW 펌웨어 모듈 관리 권한은 기본적으로 제공됩니다.
- 로그 파일은 암호화됩니다. 로깅은 직렬 포트를 통해 지원됩니다.
- SSDFW 모듈은 SF-2500 Flash Storage Processor ASIC에 포함된 펌웨어입니다.
- SSDFW 펌웨어 모듈은 시스템 데이터(예: 드라이브 상태) 및 사용자 데이터를 저장하여 비휘발성 NAND 매체에 보관합니다. 모든 시스템 데이터는 드라이브 고유 키로 암호화됩니다.
- 권한을 획득하기 위해 시스템 및 사용자 암호가 사용됩니다.
- SSDFW 펌웨어는 LSI-ASD 하위 시스템 내부에 포함되어 있습니다.
- AES-128 또는 AES-256을 사용하여 데이터가 암호화됩니다(일반텍스트). SHA 엔진이 펌웨어를 인증합니다. 키 및 카운터 값은 플래시 메모리에 저장되기 전에 암호화됩니다.

DDCLI 보안

DDCLI는 사용자 응용 프로그램입니다. DDCLI는 시스템에 연결된 모든 WarpDrive를 모니터할 수 있는 독립형 CLI입니다. WarpDrive의 다양한 구성 요소에 대한 중요한 정보는 **ddcli** 유틸리티를 사용하여 검색할 수 있습니다.

Sun Flash Accelerator F40 PCIe Card의 DDCLI 응용 프로그램에 대한 보안 고려 사항은 다음과 같습니다.

- DDCLI는 초기에 실행 권한 없이 제공됩니다. 루트 사용자가 실행 권한을 추가해야 합니다.
- ddcli 파일을 실행하려면 해당 권한을 변경해야 합니다. 보안 문제를 최소화하려면 권한을 0744로 설정하십시오. 이 파일은 루트가 소유해야 합니다. 이렇게 하면 모든 사용자가 파일을 볼 수 있지만 루트 사용자만 파일을 실행할 수 있습니다.
- MPT(메시지 처리 기술) API를 지원하는 라이브러리는 DDCLI에 정적으로 링크됩니다. 이 라이브러리는 필요한 정보를 가져오기 위해 IOCTL을 드라이버에 보냅니다.
- DDCLI 응용 프로그램은 실행 권한이 있는 이진 파일입니다.