Sun Flash Accelerator F40 PCIe Card

Security Guide

Part No.: E29743-02
October 2013

Contents

Sun Flash Accelerator F40 PCIe Card Security

This document provides general security guidelines to help you protect Oracle x86 hardware products such as the Sun Flash Accelerator F40 PCIe Card.

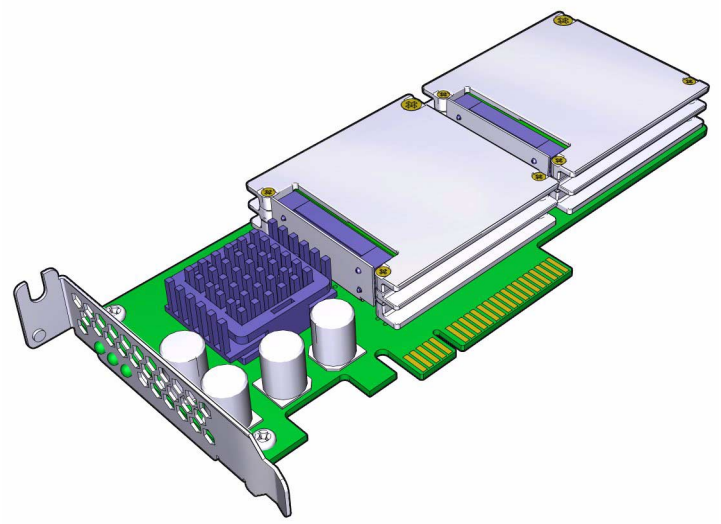
The following sections are included:

Sun Flash Accelerator F40 PCIe Card Description

The following sections are included:

The Sun Flash Accelerator F40 PCIe Card is a turnkey PCI-E 2.0, HBA, low-profile form factor, flash memory storage card.

The following image shows the Sun Flash Accelerator F40 PCIe Card:



Refer to the *Sun Flash Accelerator F40 PCIe Card User Guide* for detailed product information.

Hardware Components

The Sun Flash Accelerator F40 PCIe Card contains the following hardware components:

- Four SSD Flash modules: Total of 400 GB 32 nm eMLC NAND flash memory is directly mounted on the card.
- PCI-E to SAS protocol controller: Sun Flash Accelerator F40 PCIe Card SATA interface to the protocol controller has a PCI-E 2.0 x8 host interface connecting to an LSI 2008 SAS/SATA 2 x4 6 Gbps protocol controller.
- Energy storage components: Flush uncompleted writes to flash memory if system, or PCIe slot, power fails.

Refer to the *Sun Flash Accelerator F40 PCIe Card User Guide* for detailed information.

Software and Firmware Components

The following modules are included with the Sun Flash Accelerator F40 PCIe Card:

Component	See
MegaRAID Storage Manager (MSM)	"MSM Application Security" on page 7
Diagnostic Services	"Diagnostic Services Security" on page 8
Linux Diagnostic Driver	"Linux Diagnostic Driver Security" on page 9
SNMP	"SNMP Security" on page 9
WarpDrive Controller FW	"Warp Drive Controller Firmware Security" on page 10
SSDFW	"SSDFW Security" on page 10
DDCLI	"DDCLI Security" on page 11

Refer to the *Sun Flash Accelerator F40 PCIe Card User Guide* for detailed information.

Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

- **Access**

  Physical and software controls protect your hardware or data from intrusion.

  - For hardware, access limits usually mean *physical* access limits.
  - For software, access is limited through both physical and virtual means.
  - Firmware cannot be changed except through the Oracle update process.

- **Authentication**

  Set up the authentication features such as a password system in your platform operating systems to ensure that users are who they say they are.

  Ensure that your personnel use employee badges properly to enter the computer room.

- **Authorization**

  Allow personnel to work only with hardware and software that they are trained and qualified to use. Set up a system of Read/Write/Execute permissions to control user access to commands, disk space, devices, and applications.

- **Accounting**

Use Oracle software and hardware features to monitor login activity and maintain hardware inventories.

- Use system logs to monitor user logins. Monitor system administrator and service accounts in particular because these accounts can access powerful commands.
- Use component serial numbers to track system assets. Oracle part numbers are electronically recorded on all cards, modules, and motherboards.

Planning a Secure Environment

Use the following notes before and during the installation and configuration of a server and Sun Flash Accelerator F40 PCIe Card.

The following sections are included:

Hardware Security

Physical hardware can be secured fairly simply: limit access to the hardware and record serial numbers.

- **Restrict access**
  - If equipment is installed in a rack with a locking door, keep the door locked except when you have to service components in the rack.
  - Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- **Record serial numbers**
  - Security-mark all Sun Flash Accelerator F40 PCIe Cards. Use special ultraviolet pens or embossed labels.
  - Keep a record of the serial numbers of all Sun Flash Accelerator F40 PCIe Cards.

- Keep hardware activation keys and licenses in a secure location that is easily accessible to the system manager in system emergencies. The printed documents might be your only proof of ownership.

Software Security

The security considerations for software components are:

- Refer to the documentation that came with your software to enable any security features available for the software.
- Use the superuser account to set up and update the Sun Flash Accelerator F40 PCIe Card drivers.
- Most hardware security is implemented through software measures.
- The software components that support the Sun Flash Accelerator F40 PCIe Card rely on system security features to provide secure access.

Firmware Security

The Sun Flash Accelerator F40 PCIe Card ships with all of the firmware installed. Firmware installation is not required in the field, except for updates.

- If firmware updates are ever needed, contact Oracle support to arrange for support or check Oracle support for the latest updates and procedures for the product.

  `https://support.oracle.com`

- Use the superuser account to set up and update the Sun Flash Accelerator F40 PCIe Card firmware management utility. Ordinary user accounts allow users to view but not edit firmware. The Oracle Solaris OS firmware update process prevents unauthorized firmware modifications.
- Refer to the product notes provided with your Sun Flash Accelerator F40 PCIe Card for late-breaking news, information about firmware update requirements, or other security information.
- For information about setting SPARC OpenBootPROM (OBP) security variables, refer to the *OpenBoot 4.x Command Reference Manual*.

Oracle ILOM Firmware

You can actively secure, manage, and monitor system components through Oracle Integrated Lights Out Manager (Oracle ILOM) firmware which is preinstalled on some x86 servers.

To understand more about using this firmware when setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH), Secure Socket Layer (SSL), and RADIUS authentication, refer to Oracle ILOM documentation:

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

System Logs

- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.

Maintaining a Secure Environment

After the initial installation and setup of the Sun Flash Accelerator F40 PCIe Card, use Oracle hardware and software security features to continue controlling hardware and tracking system assets.

The following sections are included:

Asset Tracking

Use serial numbers to track inventory. Oracle embeds serial numbers in firmware on option cards and system motherboards. You can read these serial numbers through local area network connections.

You can also use wireless radio frequency identification (RFID) readers to further simplify asset tracking. Refer to an Oracle white paper, *How to Track Your Oracle Sun System Assets by Using RFID*.

Firmware Updates

Keep firmware versions current on your equipment.

- Check regularly for updates.
- All operating systems in general, and Oracle Solaris in particular, require you to log in with root credentials to administer the cards and to upgrade the drivers or firmware.
- Always install the latest released version of the firmware.

Software Updates

Keep your software versions current on your equipment.

- Software updates for Oracle Solaris drivers are available through Oracle Solaris patches and updates.
- Software updates for drivers for other operating systems may be available from http://www.lsi.com.
- Refer to the product notes provided with your Sun Flash Accelerator F40 PCIe Card for late-breaking news, information about software update requirements, or other security information.
- Always install the latest released version of the software.
- Install any necessary security patches for your software.
- Devices also contain firmware and might require firmware updates.

Log Security

Inspect and maintain your log files on a regular schedule.

- Review logs for possible incidents and archive them in accordance with a security policy.
- Periodically retire log files when they exceed a reasonable size. Maintain copies of the retired files for possible future reference or statistical analysis.

Module Security

The software and firmware modules are:

- "MSM Application Security" on page 8
- "Diagnostic Services Security" on page 9

Note – The term WarpDrive in the text refers to the Sun Flash Accelerator F40 PCIe Card.

MSM Application Security

MegaRAID Storage Manager (MSM) is a software application that provides a graphical user interface to configure and interact with the WarpDrive firmware through the driver. MSM also monitors, and maintains storage configurations on the LSI® MegaRAID, SAS, and WarpDrive controllers.

The security considerations for MSM modules in a Sun Flash Accelerator F40 PCIe Card are:

- MegaRAID Storage Manager compatibilty: Linux 64 bit, Solaris X86.
- Refer to the user guide provided by LSI, online help built-in with MSM and the readme file provided with installer. Go to `http://www.lsi.com`.
- Users are required to authenticate before any access is allowed.
  - If a user is authenticated as root, all hardware access is allowed.
  - If authenticated as user, view only privilege is allowed.
- Normally, log files have write permission, binary files have execution permission, and other files are read-only.
- Only one user has administrative privilege at a time. Other users have view only privilege. A Java inbuilt random number generator is used to generate a session ID at the time of client-server authentication.
- The client and the server are implemented in Java. The client and server use TCP/IP to communicate with each other. The server communicates with the library using JNI.
- MSM interacts with the Internet but does not support IPv6.
- MSM uses SSL to communicate between client and server.
- The firewall settings of your system depend upon the type of installation performed.
  - Under all installations except local, the firewall will need to be configured to control access to the MSM Client and Server.
  - The local installation will use the localhost IP.

- Root user access is needed to configure/modify settings. To limit access to potential attackers, follow these guidelines.
  - Choose a secure password.
  - Use different passwords for all systems that are running MSM components, both client and server.
- Optionally, LDAP can be used to authenticate access to the servers.
- The MegaRAID Storage Manager (MSM) can be installed in the following ways:
  - Complete: All components are installed.
  - Client: Only components required to remotely view and configure servers are installed. Ports 3071 and 5571 need to be opened.
  - Server: Only components required for remote server management are installed.

    Besides a unicast address, the MSM server also uses the multicast IP address 229.111.112.12 as well as TCP/UDP ports 3071 and 5571.

    For SNMP, ports 161 and 162 need to be opened.
    If LDAP is configured, port 389 needs to be opened.
  - StandAlone: Only components required for local server management are installed.
  - Local: Only components required for local server configuration are installed.

Diagnostic Services Security

Diagnostic Services is a service daemon application that listens for WarpDrive associated trigger events issued by the driver. Diagnostic Services collects diagnostic information from the WarpDrive when a reported event occurs, or when requested by a user.

The security considerations for Diagnostic Services modules in a Sun Flash Accelerator F40 PCIe Card are:

- The Diagnostic Services daemon uses the storelib library API to configure trigger events of interest and to get event notification.
- Diagnostic Services event and log information is obtained exclusively via the storelib library API and saved in log files.
- Diagnostic Services uses UDP port 162.
- A sample user event script file is installed by default but not used unless it is configured for debugging purposes.
- Diagnostic Services configuration and log files are read-only for everyone and have write permission for root user. Binary files are read-only for everyone, but have write and execution permission for a root user.

- Diagnostic Services, if configured, may send SNMP trap messages when events occur. A pipe is used internally for monitoring.

Linux Diagnostic Driver Security

The Linux Diagnostic Driver is the MPT2SAS SAS2 6 Gb driver that can automatically post a Host Trace Buffer (2MB) at startup, implement diagnostic service triggers, and support multiple functions using the management interface application. Based on the trigger attributes, the driver monitors errors, and adds a new diagnostic service event for future reference.

The security considerations for the Linux Diagnostic Driver in a Sun Flash Accelerator F40 PCIe Card are:

- The Linux Diagnostic Driver runs in kernel space. If the OS is virtualized, the driver runs in the parent.
- The Linux Diagnostic Driver captures the trace buffer from the firmware when a set of triggering events occurs. These trigger events are specified by the system administator and are fed to the driver through the Sysfs interface in the kernel.
- Only a user root with permission can write to the Linux Diagnostic Driver Sysfs attribute files.
- Linux Diagnostic Driver SAS2 generation products support EEDP (End-to-end data protection).
- The Linux Diagnostic Driver is between the hardware, firmware, and the operating system mid-layer. The Linux Diagnostic Driver uses established industry SAS2 and SATA protocols and LSI message-passing technology on the bottom end, and OS calls on the top end to handle storage data flow.
- The Linux Diagnostic Driver source is Open Source, and vetted by the Linux kernel community.
- The Linux Diagnostic Driver has full access to all the hardware it is managing, as well as access to all the kernel structures needed for it to function. The Linux Diagnostic Driver has full access to all the kernel interfaces used to manage SCSI IO's.

SNMP Security

The SNMP agent enables you to manage and monitor LSI SAS controllers using Simple Network Management Protocol (SNMP). The controller family supported by SNMP is LSI MR, IR, IR2, and WarpDrive. You can use a MIB browser, or create your own to monitor and configure the topology exposed by the LSI SNMP agent.

The security considerations for SNMP modules in a Sun Flash Accelerator F40 PCIe Card are:

- The SNMP subagent uses Simple Network Management Protocol to provide information of the monitoring system to an SNMP client.
- The SNMP client could be any MIB Browser that supports SNMPv1.
- The MR/IR SNMP sub-agent retrieves information from storelib libraries using the storelib API. Storelib makes IOCTLs (input-output control) to the driver to get that information.
- SNMP log files have write permission, binary files have execution permission, other files are read-only.
- Authentication using a Net-SNMP supported authentication mechanism is required for any SNMP access.

WarpDrive Controller Firmware Security

The WarpDrive Controller firmware runs on the WarpDrive controller board. It offers a 6 Gbps or legacy 3 Gbps transfer rate to SATA solid state drives (DFFs) connected to the WarpDrive controller board. Host connectivity to the WarpDrive controller is supported through a PCIe 2.0 connection.

The security considerations for WarpDrive Controller firmware in a Sun Flash Accelerator F40 PCIe Card are:

- WarpDrive Controller firmware executes on the processor located on the controller board.
- The WarpDrive OS drivers are above the Warp Drive Controller firmware and communicate through PCIe, using the MPI (message passing interface).
- The Warp Drive Controller firmware interacts with the SSD drive modules below it, using the SAS/SATA interface.
- Only Warp Drive Controller firmware images with the correct signature and checksum are allowed to be uploaded to the board.

SSDFW Security

The SSDFW firmware module provides firmware for the SF-2500 Flash Storage Processor family.

The security considerations for SSDFW modules in a Sun Flash Accelerator F40 PCIe Card are:

- The SSDFW firmware module connects to the NAND Flash interface on one side and the SATA AHCI interface on the other side.

- The host side communication connects through the SATA interface, defined in the Serial ATA specification and the ATA Command Set (ACS-2) Specification.
- The SSDFW firmware module admin permission is by default.
- Log files are encrypted. Logging is supported via a serial port.
- The SSDFW module is embedded firmware residing in the SF-2500 Flash Storage Processor ASIC.
- The SSDFW firmware module stores system data (such as a drive state) and user data and places it in non-volatile NAND media. All system data is encrypted with a drive unique key.
- System and user passwords are used to obtain privileges.
- The SSDFW firmware is embedded within the LSI-ASD sub-system.
- AES-128 or AES-256 is used to encrypt data (plaintext). A SHA engine authenticates the firmware. Keys and counter values are encrypted before being stored into flash memory.

DDCLI Security

DDCLI is a user application. DDCLI is a standalone CLI that allows you to monitor any WarpDrive connected to the system. Important information on various components of WarpDrive can be retrieved using the `ddcli` utility.

The security considerations for the DDCLI application in a Sun Flash Accelerator F40 PCIe Card are:

- DDCLI is initially shipped without executable permission. The root user will need to add this permission.
- The file, ddcli, will need its permissions changed so that it can be executed. To minimize security issues, set the permissions to 0744. It should be owned by root. This will allow everyone to see it, but only root users can execute it.
- A library that supports MPT (message processing technology) APIs is statically linked with DDCLI. That library sends an IOCTL to the driver to get the required information.
- The DDCLI application is a binary file with executable permission.