

Sun Flash Accelerator F40 PCIe Card

Sicherheitshandbuch

Copyright © 2013 Oracle und/oder verbundene Unternehmen. All rights reserved. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

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.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. AMD, Opteron, das AMD-Logo und das AMD Opteron-Logo sind Marken oder eingetragene Marken der Advanced Micro Devices. UNIX ist eine eingetragene Marke der The Open Group.

Diese Software oder Hardware und die zugehörige Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Inhaltsverzeichnis

1. Sicherheit der Sun Flash Accelerator F40 PCIe Card	5
Beschreibung der Sun Flash Accelerator F40 PCIe Card	5
Hardwarekomponenten	6
Software- und Firmwarekomponenten	6
Sicherheitsgrundsätze	7
Einrichten einer sicheren Umgebung	7
Hardwaresicherheit	7
Softwaresicherheit	8
Firmwaresicherheit	8
Oracle ILOM-Firmware	8
Systemprotokolle	9
Verwalten einer sicheren Umgebung	9
Ressourcenüberwachung	9
Firmwareupdates	9
Softwareupdates	9
Protokollsicherheit	10
Modulsicherheit	10
Sicherheit der MSM-Anwendung	10
Sicherheit von Diagnostic Services	11
Sicherheit des Linux Diagnostic Driver	12
SNMP-Sicherheit	12
Sicherheit der Firmware des WarpDrive-Controllers	13
SSDFW-Sicherheit	13
DDCLI-Sicherheit	14

1

• • • K a p i t e l 1

Sicherheit der Sun Flash Accelerator F40 PCIe Card

Dieses Dokument enthält allgemeine Sicherheitsrichtlinien für den Schutz von Oracle x86-Hardwareprodukten wie der Sun Flash Accelerator F40 PCIe Card.

Folgende Abschnitte sind enthalten:

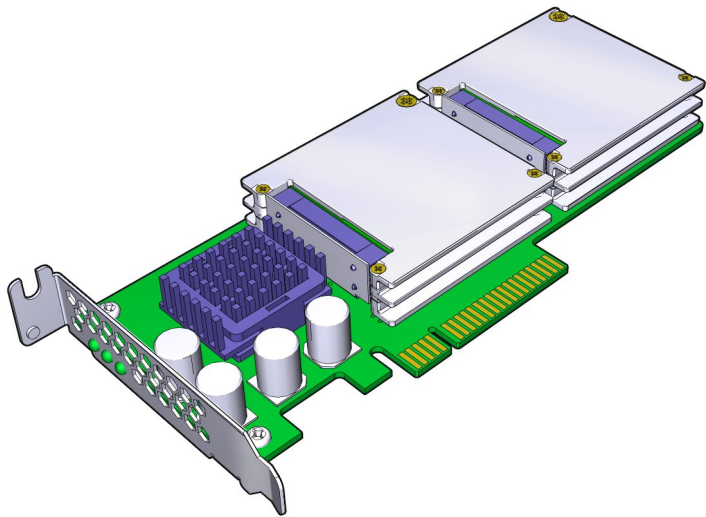
- „Beschreibung der Sun Flash Accelerator F40 PCIe Card“ [5]
- „Sicherheitsgrundsätze“ [7]
- „Einrichten einer sicheren Umgebung“ [7]
- „Verwalten einer sicheren Umgebung“ [9]

Beschreibung der Sun Flash Accelerator F40 PCIe Card

Folgende Abschnitte sind enthalten:

- „Hardwarekomponenten“ [6]
- „Software- und Firmwarekomponenten“ [6]

Die Sun Flash Accelerator F40 PCIe Card ist eine komplette PCI-E 2.0-kompatible HBA-Flash-Memory-Speicherkarte mit schlankem Formfaktor. Die folgende Abbildung zeigt die Sun Flash Accelerator F40 PCIe Card:



Ausführliche Produktinformationen finden Sie im *Benutzerhandbuch zur Sun Flash Accelerator F40 PCIe Card*.

Hardwarekomponenten

Die Sun Flash Accelerator F40 PCIe Card enthält die folgenden Hardwarekomponenten:

- Vier SSD-Flash-Module: Insgesamt sind 400 GB 32-nm-eMLC-NAND-Flashspeicher direkt auf der Karte untergebracht.
- PCI-E-zu-SAS-Protokollcontroller: Die SATA-Schnittstelle der Sun Flash Accelerator F40 PCIe Card zum Protokollcontroller verfügt über eine PCI-E 2.0 x8-Hostschnittstelle für den Anschluss an den LSI 2008 SAS/SATA 2 x4 6-Gbit/s-Protokollcontroller.
- Energiespeicherkomponenten: Bei einem Ausfall der Stromversorgung des Systems oder des PCIe-Slots werden unvollständige Schreibvorgänge im Flashspeicher gelöscht.

Ausführliche Informationen finden Sie im *Benutzerhandbuch zur Sun Flash Accelerator F40 PCIe Card*.

Software- und Firmwarekomponenten

Die folgenden Module sind in der Sun Flash Accelerator F40 PCIe Card enthalten:

Komponente	Siehe
MegaRAID Storage Manager (MSM)	"Sicherheit der MSM-Anwendung" auf Seite 7
Diagnostic Services	"Sicherheit von Diagnostic Services" auf Seite 8
Linux Diagnostic Driver	"Sicherheit des Linux Diagnostic Driver" auf Seite 9
SNMP	"SNMP-Sicherheit" auf Seite 9
Firmware des WarpDrive-Controllers	"Sicherheit der Firmware des WarpDrive-Controllers" auf Seite 10
SSDFW	"SSDFW-Sicherheit" auf Seite 10
DDCLI	"DDCLI-Sicherheit" auf Seite 11

Ausführliche Informationen finden Sie im *Benutzerhandbuch zur Sun Flash Accelerator F40 PCIe Card*.

Sicherheitsgrundsätze

Es gibt vier Sicherheitsgrundsätze: Zugang, Authentifizierung, Autorisierung und Überwachung.

- **Zugang**

Physische und virtuelle Steuerungsmechanismen schützen Ihre Hardware oder Daten vor unerlaubten Zugriffen.

- Bei Hardware beziehen sich Zugangsbeschränkungen in der Regel auf *physische* Zugangsbeschränkungen.
- Bei Software wird sowohl der physische als auch der virtuelle Zugang beschränkt.
- Firmware kann nur über den Oracle-Updateprozess geändert werden.

- **Authentifizierung**

Richten Sie die Funktionen zur Authentifizierung wie ein Passwortsystem in den Betriebssystemen Ihrer Plattform ein, damit die Identität von Benutzern geprüft werden kann.

Stellen Sie sicher, dass Ihr Personal beim Betreten des Computerraums Mitarbeiterausweise trägt.

- **Autorisierung**

Erlauben Sie Mitarbeitern, nur mit der Hardware und Software zu arbeiten, für deren Verwendung sie geschult und qualifiziert sind. Legen Sie Berechtigungen für das Lesen, Schreiben und Ausführen fest, um den Zugriff von Benutzern auf Befehle, Festplattenspeicher, Geräte und Anwendungen zu steuern.

- **Überwachung**

Verwenden Sie Hardware- und Softwarefunktionen von Oracle zur Überwachung von Anmeldevorgängen und zur Wartung der Hardware.

- Überwachen Sie die Anmeldung von Benutzern anhand von Systemprotokollen. Überwachen Sie insbesondere Systemadministrator- und Servicekonten, da vor allem diese Konten Zugriff auf Befehle mit großer Wirkung gewähren.
- Überwachen Sie die Systemkomponenten anhand ihrer Seriennummern. Oracle-Teilenummern sind auf allen Karten, Modulen und Hauptplatinen elektronisch gespeichert.

Einrichten einer sicheren Umgebung

Beachten Sie vor und während der Installation und Konfiguration eines Servers und einer Sun Flash Accelerator F40 PCIe die folgenden Hinweise.

Folgende Abschnitte sind enthalten:

- „[Hardwaresicherheit](#)“ [7]
- „[Softwaresicherheit](#)“ [8]
- „[Firmwaresicherheit](#)“ [8]
- „[Oracle ILOM-Firmware](#)“ [8]
- „[Systemprotokolle](#)“ [9]

Hardwaresicherheit

Physische Hardware kann durch Zugangseinschränkungen und Aufbewahrung von Seriennummern relativ einfach gesichert werden.

- **Schränken Sie den Zugang ein**
 - Wenn sich Geräte in einem Rack mit Türverriegelung befinden, halten Sie die Tür geschlossen, wenn Sie keine Wartungsarbeiten an Komponenten im Rack vornehmen müssen.
 - Lagern Sie nicht verwendete FRUs (Field Replaceable Units) oder CRUs (Customer Replaceable Units) in einem abschließbaren Schrank. Nur autorisiertes Personal sollte Zugang zu diesem Schrank haben.
- **Bewahren Sie Seriennummern auf**
 - Versehen Sie alle Sun Flash Accelerator F40 PCIe Cards mit einer Sicherheitskennzeichnung. Verwenden Sie spezielle UV-Stifte oder geprägte Beschriftungen.
 - Bewahren Sie die Seriennummern aller Sun Flash Accelerator F40 PCIe Cards auf.
 - Bewahren Sie Hardwareaktivierungsschlüssel und Lizenzen an einem sicheren Ort auf, der im Systemnotfall für den Systemverwalter einfach zugänglich ist. Die ausgedruckten Dokumente sind möglicherweise Ihr einziger Eigentumsnachweis.

Softwaresicherheit

Bei Softwarekomponenten sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- Informationen zum Aktivieren der Sicherheitsfunktionen Ihrer Software finden Sie in der produktbegleitenden Dokumentation.
- Verwenden Sie zum Einrichten und Updaten der Treiber für die Sun Flash Accelerator F40 PCIe Card das Superuser-Konto.
- Hardwaresicherheit wird größtenteils durch Softwaremaßnahmen umgesetzt.
- Ob die Softwarekomponenten, die die Sun Flash Accelerator F40 PCIe Card unterstützen, den sicheren Zugriff gewährleisten können, ist von den Sicherheitsfunktionen des jeweiligen Systems abhängig.

Firmwaresicherheit

Sämtliche Firmware ist auf der Sun Flash Accelerator F40 PCIe Card bei Lieferung bereits installiert. Mit Ausnahme von Updates ist keine nachträgliche Firmwareinstallation erforderlich.

- Wenn Sie Firmwareupdates benötigen, wenden Sie sich an den Oracle-Support, um Unterstützung oder aktuelle Updates und Prozeduren für das Produkt zu erhalten.

<https://support.oracle.com>

- Verwenden Sie zum Einrichten und Updaten des Verwaltungsdienstprogramms für die Firmware der Sun Flash Accelerator F40 PCIe Card das Superuser-Konto. Mit gewöhnlichen Benutzerkonten kann Firmware lediglich angezeigt, nicht jedoch bearbeitet werden. Der Firmwareupdateprozess des Oracle Solaris-Betriebssystems verhindert nicht autorisierte Firmwaremodifizierungen.
- Aktuelles, Informationen zu erforderlichen Firmwareupdates oder andere Sicherheitsinformationen zur Sun Flash Accelerator F40 PCIe Card finden Sie in den Produkthinweisen.
- Informationen zum Festlegen der SPARC OpenBootPROM-(OBP-)Sicherheitsvariablen finden Sie im *OpenBoot 4.x-Befehlsreferenzhandbuch*.

Oracle ILOM-Firmware

Sie können Systemkomponenten über die Firmware von Oracle ILOM (Oracle Integrated Lights Out Manager) selbst sichern, verwalten und überwachen. Diese Firmware ist auf einigen x86-Servern vorinstalliert. Weitere Informationen zur Verwendung dieser Firmware zum Einrichten von Passwörtern, Verwalten von Benutzern und Anwenden von Sicherheitsfunktionen, einschließlich SSH-,

SSL- und RADIUS-Authentifizierung (Secure Shell, Secure Socket, Remote Authentication Dial in User Service), finden Sie in der Dokumentation zu Oracle ILOM:

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

Systemprotokolle

- Aktivieren Sie den Protokollierungsvorgang, und senden Sie Protokolle an einen dezierten, sicheren Protokollhost.
- Konfigurieren Sie die Protokollierung mithilfe von NTP (Network Time Protocol) und Zeitstempeln, damit die Zeitangaben korrekt sind.

Verwalten einer sicheren Umgebung

Steuern Sie nach Erstinstallation und Einrichtung der Sun Flash Accelerator F40 PCIe Card die Hardware- und Überwachungssystemressourcen mithilfe von Oracle-Hardware- und Softwaresicherheitsfunktionen.

Folgende Abschnitte sind enthalten:

- „Ressourcenüberwachung“ [9]
- „Firmwareupdates“ [9]
- „Softwareupdates“ [9]
- „Protokollsicherheit“ [10]
- „Modulsicherheit“ [10]

Ressourcenüberwachung

Überwachen Sie Hardwarebestände mithilfe von Seriennummern. Bei Oracle-Produkten sind Firmwareseriennummern in Optionskarten und Systemhauptplatinen eingebettet. Diese Seriennummern sind über eine LAN-Verbindung einsehbar.

Die Ressourcenüberwachung gestaltet sich noch einfacher, wenn Sie drahtlose RFID-Lesegeräte (Radio Frequency Identification) verwenden. Weitere Informationen dazu finden Sie im Oracle-Whitepaper *How to Track Your Oracle Sun System Assets by Using RFID*.

Firmwareupdates

Halten Sie die Firmwareversionen Ihrer Geräte auf dem aktuellen Stand.

- Prüfen Sie in regelmäßigen Abständen, ob Updates verfügbar sind.
- Sie müssen sich bei allen Betriebssystemen im Allgemeinen und insbesondere bei Oracle Solaris mit Root-Zugangsdaten anmelden, um die Karten zu verwalten und die Treiber oder Firmware upzudaten.
- Installieren Sie immer die neueste Firmwareversion.

Softwareupdates

Halten Sie die Softwareversionen Ihrer Geräte auf dem aktuellen Stand.

- Softwareupdates für Oracle Solaris-Treiber sind über Oracle Solaris-Patches und -Updates verfügbar.

- Softwareupdates für Treiber anderer Betriebssysteme sind gegebenenfalls unter <http://www.lsi.com> verfügbar.
- Aktuelles, Informationen zu erforderlichen Softwareupdates oder andere Sicherheitsinformationen zur Sun Flash Accelerator F40 PCIe Card finden Sie in den Produkthinweisen.
- Installieren Sie immer die neueste Softwareversion.
- Installieren Sie alle erforderlichen Sicherheitspatches für Ihre Software.
- Geräte enthalten ebenfalls Firmware, für die Updates erforderlich sein können.

Protokollsicherheit

Überprüfen und verwalten Sie Ihre Protokolldateien in regelmäßigen Abständen.

- Prüfen Sie die Protokolle auf Vorfälle, und archivieren Sie sie gemäß den Sicherheitsrichtlinien.
- Entfernen Sie Protokolldateien regelmäßig, sobald sie eine bestimmte Größe erreichen. Bewahren Sie eine Kopie der entfernten Dateien für künftige Verwendungszwecke oder statistische Analysen auf.

Modulsicherheit

Die Software- und Firmwaremodule lauten:

- „Sicherheit der MSM-Anwendung“ [10]
- „Sicherheit von Diagnostic Services“ [11]
- „Sicherheit des Linux Diagnostic Driver“ [12]
- „SNMP-Sicherheit“ [12]
- „SSDFW-Sicherheit“ [13]
- „DDCLI-Sicherheit“ [14]



Anmerkung

Der Begriff "WarpDrive" im Text bezieht sich auf Sun Flash Accelerator F40 PCIe Card.

Sicherheit der MSM-Anwendung

MegaRAID Storage Manager (MSM) ist eine Softwareanwendung mit einer grafischen Benutzeroberfläche zur Konfiguration der WarpDrive-Firmware über den Treiber. Außerdem können mit MSM Speicherkonfigurationen auf den LSI® MegaRAID-, SAS- und WarpDrive-Controllern überwacht und verwaltet werden.

Bei MSM-Modulen in einer Sun Flash Accelerator F40 PCIe Card sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- Kompatibilität mit MegaRAID Storage Manager: Linux 64 Bit, Solaris X86.
- Informationen dazu finden Sie im Benutzerhandbuch von LSI, in der in MSM integrierten Onlinehilfe und in der Readme-Datei des Installationsprogramms. Rufen Sie <http://www.lsi.com> auf.
- Benutzer müssen vor dem Zugriff authentifiziert werden.
 - Wenn ein Benutzer als Root authentifiziert wird, kann dieser auf die gesamte Hardware zugreifen.
 - Wurde er als Benutzer authentifiziert, verfügt er lediglich über Berechtigungen zum Anzeigen.
- In der Regel besteht für Protokolldateien Schreib- und für Binärdateien Ausführberechtigung, alle anderen Dateien sind schreibgeschützt.

- Jeweils nur ein Benutzer kann über Administratorrechte verfügen. Andere Benutzer verfügen lediglich über Anzeigeberechtigungen. Ein in Java integrierter Zufallszahlengenerator erstellt zum Zeitpunkt der Client-Server-Authentifizierung eine Sitzungs-ID.
- Client und Server werden in Java implementiert. Die Kommunikation zwischen Client und Server findet mithilfe von TCP/IP statt. Der Server kommuniziert mithilfe von JNI mit der Bibliothek.
- MSM interagiert mit dem Internet, unterstützt jedoch nicht IPv6.
- MSM verwendet SSL zur Kommunikation zwischen Client und Server.
- Die Firewall-Einstellungen Ihres Systems sind von der durchgeführten Installationsart abhängig.
 - Bei allen Installationen außer der lokalen muss die Firewall zur Kontrolle des Zugriffs auf den MSM-Client und -Server konfiguriert werden.
 - Bei der lokalen Installation wird die Localhost-IP verwendet.
- Zur Konfiguration/Änderung von Einstellungen ist der Root-Benutzerzugriff erforderlich. Beachten Sie die folgenden Richtlinien, um den Zugriff potenzieller Angreifer einzuschränken.
 - Wählen Sie ein sicheres Passwort.
 - Verwenden Sie für jedes System (Client und Server), auf dem MSM-Komponenten ausgeführt werden, ein anderes Passwort.
- Optional kann LDAP zur Authentifizierung des Zugriffs auf die Server verwendet werden.
- Der MegaRAID Storage Manager (MSM) kann wie folgt installiert werden:
 - Vollständig: Alle Komponenten werden installiert.
 - Client: Nur Komponenten, die zur Remote-Ansicht und -Konfiguration der Server erforderlich sind, werden installiert. Die Ports 3071 und 5571 müssen geöffnet werden.
 - Server: Nur Komponenten, die zur Remote-Verwaltung von Servern erforderlich sind, werden installiert.

Neben einer Unicast-Adresse verwendet der MSM-Server die Multicast-IP-Adresse 229.111.112.12 und die TCP/UDP-Ports 3071 und 5571.

Für SNMP müssen die Ports 161 und 162 geöffnet werden. Wenn LDAP konfiguriert ist, muss Port 389 geöffnet werden.

- Eigenständig: Nur Komponenten, die zur lokalen Verwaltung von Servern erforderlich sind, werden installiert.
- Lokal: Nur Komponenten, die zur lokalen Konfiguration von Servern erforderlich sind, werden installiert.

Sicherheit von Diagnostic Services

Diagnostic Services ist eine Servicedämonanwendung, die mit WarpDrive zusammenhängende Auslöserereignisse abhört, die vom Treiber ausgegeben werden. Diagnostic Services erfasst Diagnoseinformationen vom WarpDrive, wenn ein Benutzer dies anfordert oder ein gemeldetes Ereignis auftritt.

Bei Diagnostic Services-Modulen in einer Sun Flash Accelerator F40 PCIe Card sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- Der Diagnostic Services-Dämon verwendet zur Konfiguration von relevanten Auslöserereignissen und zum Abrufen von Ereignisbenachrichtigungen die API der Storelib-Bibliothek.
- Diagnostic Services-Ereignisse und Protokollinformationen werden ausschließlich über die API der Storelib-Bibliothek abgerufen und in Protokolldateien gespeichert.
- Diagnostic Services verwendet den UDP-Port 162.

- Eine Musterskriptdatei für Benutzerereignisse wird standardmäßig installiert, jedoch nur verwendet, wenn sie zu Debugging-Zwecken konfiguriert wird.
- Die Diagnostic Services-Konfiguration und Protokolldateien sind für alle Benutzer außer dem Root-Benutzer schreibgeschützt. Binärdateien sind für alle Benutzer außer dem Root-Benutzer schreibgeschützt. Der Root-Benutzer verfügt über Schreib- und Ausführberechtigungen.
- Diagnostic Services kann bei entsprechender Konfiguration SNMP-Trap-Nachrichten senden, wenn Ereignisse auftreten. Zur Überwachung wird intern eine Pipe verwendet.

Sicherheit des Linux Diagnostic Driver

Der Linux Diagnostic Driver ist der MPT2SAS SAS2-6-GB-Treiber, der beim Starten automatisch einen Host-Trace-Puffer (2 MB) posten, Diagnoseserviceauslöser implementieren und über die Verwaltungsschnittstellenanwendung mehrere Funktionen unterstützen kann. Basierend auf den Ereignisattributen überwacht der Treiber Fehler und fügt zu zukünftigen Referenzzwecken ein neues Diagnoseserviceereignis hinzu.

Beim Linux Diagnostic Driver in einer Sun Flash Accelerator F40 PCIe Card sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- Der Linux Diagnostic Driver wird im Kernel-Bereich ausgeführt. Bei einem virtualisierten Betriebssystem wird der Treiber im übergeordneten Verzeichnis ausgeführt.
- Der Linux Diagnostic Driver erfasst den Trace-Puffer aus der Firmware, wenn eine Reihe auslösender Ereignisse auftreten. Diese Auslöserereignisse werden vom Systemadministrator festgelegt und dem Treiber über die Sysfs-Schnittstelle im Kernel zugeführt.
- Nur ein Root-Benutzer mit entsprechenden Berechtigungen kann in die Sysfs-Attributdateien des Linux Diagnostic Driver schreiben.
- Produkte der Linux Diagnostic Driver SAS2-Generation unterstützen EEDP (End-to-End Data Protection).
- Der Linux Diagnostic Driver befindet sich zwischen Hardware, Firmware und der Mittelschicht des Betriebssystems. Der Linux Diagnostic Driver verwendet zur Verwaltung des Speicherdatenflusses branchenweit bewährte SAS2- und SATA-Protokolle und LSI-Nachrichtenaustauschtechnologie am unteren Ende sowie Betriebssystemaufrufe am oberen Ende.
- Der Linux Diagnostic Driver stammt aus einer Open Source-Quelle, die von der Linux-Kernel-Community geprüft wird.
- Der Linux Diagnostic Driver verfügt über vollständigen Zugriff auf sämtliche von ihm verwaltete Hardware sowie auf alle Kernel-Strukturen, die für seine ordnungsgemäße Funktion erforderlich sind. Der Linux Diagnostic Driver hat vollständigen Zugriff auf alle Kernel-Schnittstellen, die zur Verwaltung von SCSI-IOs verwendet werden.

SNMP-Sicherheit

Mit dem SNMP-Agent können Sie LSI-SAS-Controller mithilfe des Simple Network Management Protocol (SNMP) verwalten und überwachen. Zur von SNMP unterstützten Controllerfamilie gehören LSI MR, IR, IR2 und WarpDrive. Sie können einen MIB-Browser verwenden oder einen eigenen Browser erstellen, um die Topologie des LSI-SNMP-Agents zu überwachen und zu konfigurieren.

Bei SNMP-Modulen in einer Sun Flash Accelerator F40 PCIe Card sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- Der SNMP-Subagent stellt dem SNMP-Client mithilfe des Simple Network Management Protocol Informationen zum Überwachungssystem bereit.

- Der SNMP-Client kann ein beliebiger MIB-Browser sein, der SNMPv1 unterstützt.
- Der MR/IR SNMP-Subagent ruft mithilfe der Storelib-API Informationen aus Storelib-Bibliotheken ab. Storelib sendet IOCTLs (Input-Output Controller) an den Treiber, um diese Informationen abzurufen.
- Für SNMP-Protokolldateien besteht Schreib- und für Binärdateien Ausführberechtigung, alle anderen Dateien sind schreibgeschützt.
- Für jeden SNMP-Zugang ist die Authentifizierung über einen von Net-SNMP unterstützten Authentifizierungsmechanismus erforderlich.

Sicherheit der Firmware des WarpDrive-Controllers

Die Firmware des WarpDrive-Controllers wird auf der WarpDrive-Controllerplatine ausgeführt. Sie bietet eine Übertragungsrate von 6 Gbit/s oder 3 Gbit/s (veraltet) zu SATA-Solid-State-Drives (DFFs), die mit der WarpDrive-Controllerplatine verbunden sind. Host-Verbindungen zum WarpDrive Controller werden über eine PCIe-2.0-Verbindung unterstützt.

Bei der Firmware des WarpDrive-Controllers in einer Sun Flash Accelerator F40 PCIe Card sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- Die Firmware des WarpDrive-Controllers wird auf dem Prozessor auf der Controllerplatine ausgeführt.
- Die Betriebssystemtreiber für WarpDrive sind der Firmware des WarpDrive-Controllers übergeordnet und kommunizieren über PCIe mithilfe der MPI (Nachrichtenaustauschnittstelle).
- Die Firmware des WarpDrive-Controllers interagiert über die SAS/SATA-Schnittstelle mit den untergeordneten SSD-Laufwerksmodulen.
- Nur Images der Firmware des WarpDrive-Controllers mit der richtigen Signatur und Prüfsumme dürfen auf die Platine geladen werden.

SSDFW-Sicherheit

Das SSDFW-Firmwaremodul bietet Firmware für die SF-2500 Flash Storage Processor-Familie.

Bei SSDFW-Modulen in einer Sun Flash Accelerator F40 PCIe Card sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- Das SSDFW-Firmwaremodul stellt auf der einen Seite eine Verbindung zur NAND-Flash-Schnittstelle und auf der anderen Seite zur SATA-AHCI-Schnittstelle her.
- Die hostseitige Kommunikation findet über die SATA-Schnittstelle statt, die in der Serial ATA-Spezifikation und der ATA Command Set-(ACS-2-)Spezifikation definiert ist.
- Für das SSDFW-Firmwaremodul sind standardmäßig Administratorrechte erforderlich.
- Protokolldateien sind verschlüsselt. Die Protokollierung wird über den seriellen Port unterstützt.
- Das SSDFW-Modul ist in die Firmware im SF-2500 Flash Storage Processor ASIC eingebettet.
- Das SSDFW-Firmwaremodul speichert Systemdaten (wie z.B. einen Laufwerksstatus) und Benutzerdaten und platziert sie auf einem nicht flüchtigen NAND-Medium. Alle Systemdaten sind mit einem treiberspezifischen Schlüssel verschlüsselt.
- System- und Benutzerpasswörter werden zum Abruf von Berechtigungen verwendet.
- Die SSDFW-Firmware ist in das LSI-ASD-Subsystem eingebettet.
- AES-128 oder AES-256 wird zur Datenverschlüsselung (Nur Text) verwendet. Eine SHA-Engine authentifiziert die Firmware. Schlüssel und Zählerwerte werden vor dem Speichern im Flash-Speicher verschlüsselt.

DDCLI-Sicherheit

DDCLI ist eine Benutzeranwendung. DDCLI ist eine eigenständige CLI, über die Sie jedes an das System angeschlossene WarpDrive überwachen können. Mithilfe des Dienstprogramms **ddcli** können wichtige Informationen zu verschiedenen Komponenten von WarpDrive abgerufen werden.

Bei der DDCLI-Anwendung in einer Sun Flash Accelerator F40 PCIe Card sind folgende Punkte im Hinblick auf Sicherheit zu beachten:

- DDCLI wird standardmäßig ohne Ausführberechtigung geliefert. Diese Berechtigung muss vom Root-Benutzer hinzugefügt werden.
- Für die Datei "ddcli" muss diese Berechtigung geändert werden, damit sie ausgeführt werden kann. Um Sicherheitsrisiken zu minimieren, setzen Sie die Berechtigungen auf 0744. Ein Root-Benutzer sollte Eigentümer der Datei sein. So kann die Datei von jedem Benutzer angezeigt, jedoch nur von Root-Benutzern ausgeführt werden.
- Eine Bibliothek, die APIs für MPT (Nachrichtenverarbeitungstechnologie) unterstützt, ist statisch mit DDCLI verknüpft. Diese Bibliothek sendet einen IOCTL an den Treiber, um die erforderlichen Informationen abzurufen.
- Die DDCLI-Anwendung ist eine Binärdatei mit Ausführberechtigung.