Sun Flash Accelerator F40 PCIe Card

Guida per la sicurezza

N. di parte: E39700-02
Ottobre 2013

Copyright © 2013 Oracle e/o relative consociate. Tutti i diritti riservati.

Il software e la relativa documentazione vengono distribuiti sulla base di specifiche condizioni di licenza che prevedono restrizioni relative all'uso e alla divulgazione e sono inoltre protetti dalle leggi vigenti sulla proprietà intellettuale. Ad eccezione di quanto espressamente consentito dal contratto di licenza o dalle disposizioni di legge, nessuna parte può essere utilizzata, copiata, riprodotta, tradotta, diffusa, modificata, concessa in licenza, trasmessa, distribuita, presentata, eseguita, pubblicata o visualizzata in alcuna forma o con alcun mezzo. La decodificazione, il disassemblaggio o la decompilazione del software sono vietati, salvo che per garantire l'interoperabilità nei casi espressamente previsti dalla legge.

Le informazioni contenute nella presente documentazione potranno essere soggette a modifiche senza preavviso. Non si garantisce che la presente documentazione sia priva di errori. Qualora l'utente riscontrasse dei problemi, è pregato di segnalarli per iscritto a Oracle.

Qualora il software o la relativa documentazione vengano forniti al Governo degli Stati Uniti o a chiunque li abbia in licenza per conto del Governo degli Stati Uniti, sarà applicabile la clausola riportata di seguito:

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.

Il presente software o hardware è stato sviluppato per un uso generico in varie applicazioni di gestione delle informazioni. Non è stato sviluppato né concepito per l'uso in campi intrinsecamente pericolosi, incluse le applicazioni che implicano un rischio di lesioni personali. Qualora il software o l'hardware venga utilizzato per impieghi pericolosi, è responsabilità dell'utente adottare tutte le necessarie misure di emergenza, backup e di altro tipo per garantirne la massima sicurezza di utilizzo. Oracle Corporation e le sue consociate declinano ogni responsabilità per eventuali danni causati dall'uso del software o dell'hardware per impieghi pericolosi.

Oracle e Java sono marchi registrati di Oracle e/o delle relative consociate. Altri nomi possono essere marchi dei rispettivi proprietari.

Intel e Intel Xeon sono marchi o marchi registrati di Intel Corporation. Tutti i marchi SPARC sono utilizzati in base alla relativa licenza e sono marchi o marchi registrati di SPARC International, Inc. AMD, Opteron, il logo AMD e il logo AMD Opteron sono marchi o marchi registrati di Advanced Micro Devices. UNIX è un marchio registrato di The Open Group.

Il software o l'hardware e la documentazione possono includere informazioni su contenuti, prodotti e servizi di terze parti o collegamenti agli stessi. Oracle Corporation e le sue consociate declinano ogni responsabilità ed escludono espressamente qualsiasi tipo di garanzia relativa a contenuti, prodotti e servizi di terze parti. Oracle Corporation e le sue consociate non potranno quindi essere ritenute responsabili per qualsiasi perdita, costo o danno causato dall'accesso a contenuti, prodotti o servizi di terze parti o dall'utilizzo degli stessi.

Indice

1. Sicurezza della scheda Sun Flash Accelerator F40 PCIe Card 5
Descrizione della scheda Sun Flash Accelerator F40 PCIe Card 5
Componenti hardware 6
Componenti firmware e software 6
Principi di sicurezza 7
Pianificare un ambiente sicuro 7
Sicurezza hardware 7
Sicurezza del software 8
Sicurezza firmware 8
Firmware Oracle ILOM 8
Log di sistema 9
Gestione di un ambiente sicuro 9
Registrazione degli asset 9
Aggiornamenti firmware 9
Aggiornamenti software 9
Sicurezza dei log 10
Sicurezza dei moduli 10
Sicurezza dell'applicazione MSM 10
Sicurezza di Diagnostic Services 11
Sicurezza del driver di diagnostica Linux 12
Sicurezza SNMP 12
Sicurezza del firmware del controller WarpDrive 13
Sicurezza SSDFW 13
Sicurezza DDCLI 14

• • • Capitolo 1

Sicurezza della scheda Sun Flash Accelerator F40 PCIe Card

Questo documento fornisce linee guida generali sulla sicurezza per la protezione dei prodotti hardware Oracle x86 quali la scheda Sun Flash Accelerator F40 PCIe Card.

Sono incluse le seguenti sezioni:

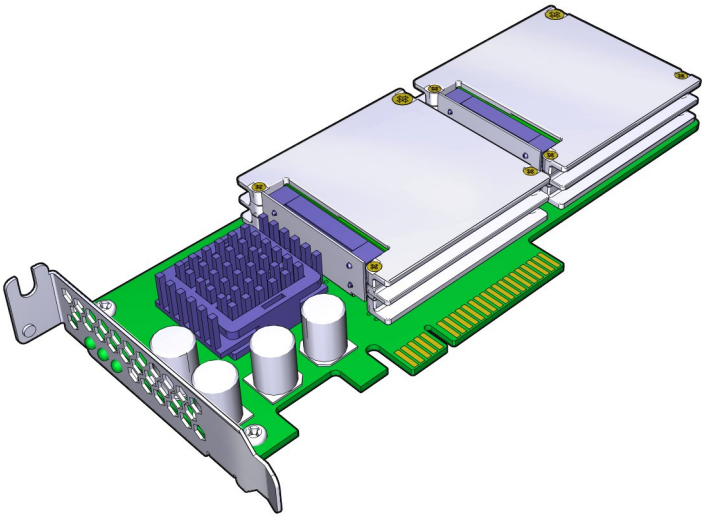
- sezione chiamata «Descrizione della scheda Sun Flash Accelerator F40 PCIe Card» [5]
- sezione chiamata «Principi di sicurezza» [7]
- sezione chiamata «Pianificare un ambiente sicuro» [7]
- sezione chiamata «Gestione di un ambiente sicuro» [9]

Descrizione della scheda Sun Flash Accelerator F40 PCIe Card

Sono incluse le seguenti sezioni:

- sezione chiamata «Componenti hardware» [6]
- sezione chiamata «Componenti firmware e software» [6]

La scheda Sun Flash Accelerator F40 PCIe Card è una scheda di memoria flash form factor di basso profilo PCI-E 2.0, HBA turn-key. L'immagine riportata di seguito mostra la scheda Sun Flash Accelerator F40 PCIe Card:



Per informazioni dettagliate sul prodotto, fare riferimento a *Sun Flash Accelerator F40 PCIe Card User Guide*.

Componenti hardware

La scheda Sun Flash Accelerator F40 PCIe Card contiene i seguenti componenti hardware:

- Quattro moduli flash SSD: un totale di 400 GB di memoria flash NAND a 32 nm eMLC è montato direttamente sulla scheda.
- Controller di protocollo PCI-E to SAS: l'interfaccia SATA della scheda Sun Flash Accelerator F40 PCIe Card al controller di protocollo dispone di un'interfaccia host PCI-E 2.0 x8 che si connette a un controller di protocollo LSI 2008 SAS/SATA 2 x4 6 Gbps.
- Componenti per l'immagazzinamento di energia: eseguono il flush delle scritture incomplete nella memoria flash in caso di caduta dell'alimentazione del sistema o dello slot PCIe.

Per informazioni dettagliate, fare riferimento al manuale *Sun Flash Accelerator F40 PCIe Card User Guide*.

Componenti firmware e software

I seguenti moduli sono inclusi con la scheda Sun Flash Accelerator F40 PCIe Card:

Componente	Vedere
MegaRAID Storage Manager (MSM)	“Sicurezza dell'applicazione MSM” a pagina 7
Diagnostic Services	“Sicurezza di Diagnostic Services” a pagina 8
Driver di diagnostica Linux	“Sicurezza del driver di diagnostica Linux” a pagina 9
SNMP	“Sicurezza SNMP” a pagina 9
FW del controller WarpDrive	“Sicurezza del firmware del controller WarpDrive” a pagina 10
SSDFW	“Sicurezza SSDFW” a pagina 10
DDCLI	“Sicurezza DDCLI” a pagina 11

Per informazioni dettagliate, fare riferimento al manuale *Sun Flash Accelerator F40 PCIe Card User Guide*.

Principi di sicurezza

Esistono quattro principi di sicurezza di base: accesso, autenticazione, autorizzazione e account.

- **Accesso**

  Controlli fisici e software proteggono l'hardware o i dati dall'intrusione.
  - Per l'hardware, i limiti di accesso sono generalmente limiti all'accesso *fisico*.
  - Per il software, l'accesso viene limitato sia mediante mezzi fisici che virtuali.
  - Il firmware non può essere modificato se non tramite il processo di aggiornamento Oracle.
- **Autenticazione**

  Configurare le funzioni di autenticazione quali un sistema di password nel sistema operativo della piattaforma per garantire che gli utenti siano realmente chi affermano di essere.

  Assicurarsi che il personale utilizzi i badge dei dipendenti in modo adeguato per accedere alla stanza dei computer.
- **Autorizzazione**

  Consentire ai dipendenti di lavorare solo con hardware e software per i quali sono qualificati e hanno sufficiente competenza. Configurare un sistema di autorizzazioni di Lettura/Scrittura/Esecuzione per controllare l'accesso degli utenti a comandi, spazio su disco, dispositivi e applicazioni.
- **Account**

  Utilizzare le funzioni software e hardware Oracle per monitorare l'attività di login e gestire gli inventari hardware.
  - Utilizzare i log di sistema per monitorare i login utente. Monitorare in particolare gli account di servizio e amministratore di sistema poiché questi account possono accedere a comandi determinanti.
  - Utilizzare i numeri di serie dei componenti per tenere traccia degli asset del sistema. I numeri parte Oracle sono elettronicamente registrati su tutte le schede, i moduli e le schede madri.

Pianificare un ambiente sicuro

Utilizzare le note riportate di seguito prima e durante l'installazione e la configurazione di un server e della scheda Sun Flash Accelerator F40 PCIe Card.

Sono incluse le seguenti sezioni:

- sezione chiamata «Sicurezza hardware » [7]
- sezione chiamata «Sicurezza del software » [8]
- sezione chiamata «Sicurezza firmware» [8]
- sezione chiamata «Firmware Oracle ILOM» [8]
- sezione chiamata «Log di sistema» [9]

Sicurezza hardware

L'hardware fisico può essere protetto piuttosto semplicemente, limitando l'accesso all'hardware e registrando i numeri di serie.

- **Limitare l'accesso**

  - Se le apparecchiature sono installate in un rack dotato di sportello, tenere lo sportello sempre chiuso, eccetto che per eventuali interventi sui componenti contenuti nel rack.
  - Conservare le unità di ricambio sostituibili in loco (FRU) o le unità sostituibili dal cliente (CRU) in un cabinet chiuso. Limitare l'accesso al cabinet chiuso a personale autorizzato.
- **Registrare i numeri di serie**
  - Apporre contrassegni di sicurezza a tutte le schede Sun Flash Accelerator F40 PCIe Cards. Utilizzare le speciali penne ultraviolette o etichette a rilievo.
  - Tenere un registro dei numeri di serie di tutte le schede Sun Flash Accelerator F40 PCIe Cards.
  - Conservare le licenze e le chiavi di attivazione dell'hardware in un luogo sicuro e facilmente accessibile ai system manager in caso di emergenze relative al sistema. I documenti stampati potrebbero essere l'unica prova di proprietà.

Sicurezza del software

Le considerazioni sulla sicurezza per i componenti software sono:

- Fare riferimento alla documentazione fornita con il software per abilitare eventuali funzioni di sicurezza disponibili per il software.
- Utilizzare l'account utente privilegiato per configurare e aggiornare i driver della scheda Sun Flash Accelerator F40 PCIe Card.
- In gran parte la sicurezza dell'hardware viene implementata mediante misure software.
- I componenti software che supportano la scheda Sun Flash Accelerator F40 PCIe Card utilizzano funzioni di sicurezza di sistema per fornire accesso sicuro.

Sicurezza firmware

La scheda Sun Flash Accelerator F40 PCIe Card viene fornita con tutto il firmware installato. L'installazione del firmware non è richiesta in loco, eccetto gli aggiornamenti.

- In caso siano necessari aggiornamenti firmware, contattare il Supporto Oracle per concordare interventi di supporto o controllare presso il Supporto Oracle gli aggiornamenti e le procedure più recenti per il prodotto.

  https://support.oracle.com
- Utilizzare l'account utente privilegiato per configurare e aggiornare la utility di gestione del firmware della scheda Sun Flash Accelerator F40 PCIe Card. I normali account utente consentono agli utenti di visualizzare il firmware ma non di modificarlo. Il processo di aggiornamento del firmware del sistema operativo Oracle Solaris impedisce modifiche non autorizzate al firmware.
- Fare riferimento alle note del prodotto fornite con la scheda Sun Flash Accelerator F40 PCIe Card per notizie aggiornate, informazioni sui requisiti per l'aggiornamento del firmware o altre informazioni sulla sicurezza.
- Per informazioni sull'impostazione delle variabili di sicurezza SPARC OpenBootPROM (OBP), fare riferimento al manuale *OpenBoot 4.x Command Reference Manual*.

Firmware Oracle ILOM

È possibile proteggere attivamente, gestire e monitorare i componenti del sistema mediante il firmware Oracle Integrated Lights Out Manager (Oracle ILOM) preinstallato in alcuni server x86. Per comprendere maggiormente l'uso di questo firmware nella configurazione di password, nella gestione

degli utenti e nell'applicazione di funzioni relative alla sicurezza, tra cui l'autenticazione Secure Shell (SSH), Secure Socket Layer (SSL) e RADIUS, fare riferimento alla documentazione di Oracle ILOM:

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

Log di sistema

- Abilitare i log e inviarli a un host sicuro dedicato.
- Configurare i log in modo da includere informazioni precise sull'ora, utilizzando NTP e gli indicatori orari.

Gestione di un ambiente sicuro

Dopo l'installazione e la configurazione iniziale della scheda Sun Flash Accelerator F40 PCIe Card, utilizzare le funzioni di sicurezza software e hardware Oracle per continuare a controllare l'hardware e tenere traccia degli asset del sistema.

Sono incluse le seguenti sezioni:

- sezione chiamata «Registrazione degli asset» [9]
- sezione chiamata «Aggiornamenti firmware» [9]
- sezione chiamata «Aggiornamenti software » [9]
- sezione chiamata «Sicurezza dei log» [10]
- sezione chiamata «Sicurezza dei moduli» [10]

Registrazione degli asset

Utilizzare i numeri di serie per tenere traccia dell'inventario. Oracle incorpora i numeri di serie nel firmware nelle schede opzionali e nelle schede madri di sistema. È possibile visualizzare i numeri di serie mediante connessioni LAN.

È inoltre possibile utilizzare reader wireless RFID (Radio Frequency IDentification) per semplificare ulteriormente la registrazione degli asset. Fare riferimento all'apposito documento tecnico Oracle, intitolato , *How to Track Your Oracle Sun System Assets by Using RFID*.

Aggiornamenti firmware

Mantenere aggiornate le versioni del firmware nelle apparecchiature.

- Controllare regolarmente la presenza di aggiornamenti.
- Tutti i sistemi operativi in generale, e Oracle Solaris in particolare, richiedono di effettuare il login con credenziali root per amministrare le schede e aggiornare i driver o il firmware.
- Installare sempre l'ultima versione rilasciata del firmware.

Aggiornamenti software

Mantenere aggiornate le versioni del software nelle apparecchiature.

- Gli aggiornamenti software per i driver di Oracle Solaris sono disponibili mediante le patch e gli aggiornamenti di Oracle Solaris.

- Gli aggiornamenti software per i driver per gli altri sistemi operativi sono disponibili da http://www.lsi.com.
- Fare riferimento alle note del prodotto fornite con la scheda Sun Flash Accelerator F40 PCIe Card per notizie aggiornate, informazioni sui requisiti per l'aggiornamento del software o altre informazioni sulla sicurezza.
- Installare sempre l'ultima versione rilasciata del software.
- Installare eventuali patch di sicurezza necessarie per il software.
- I dispositivi contengono anche firmware e potrebbero richiedere aggiornamenti del firmware.

Sicurezza dei log

Controllare e gestire i file di log regolarmente.

- Esaminare i log per verificare la presenza di possibili incidenti e archiviarli in conformità con un criterio di sicurezza.
- Ritirare periodicamente i file di log quando superano dimensioni ragionevoli. Conservare copie dei file ritirati per possibile riferimento futuro o analisi statistiche.

Sicurezza dei moduli

I moduli software e firmware sono:

- sezione chiamata «Sicurezza dell'applicazione MSM» [10]
- sezione chiamata «Sicurezza di Diagnostic Services» [11]
- sezione chiamata «Sicurezza del driver di diagnostica Linux» [12]
- sezione chiamata «Sicurezza SNMP» [12]
- sezione chiamata «Sicurezza SSDFW» [13]
- sezione chiamata «Sicurezza DDCLI» [14]



Nota

Il termine WarpDrive nel testo si riferisce a Sun Flash Accelerator F40 PCIe Card.

Sicurezza dell'applicazione MSM

MegaRAID Storage Manager (MSM) è un'applicazione software che fornisce un'interfaccia utente grafica per configurare e interagire con il firmware WarpDrive mediante il driver. MSM consente inoltre di monitorare e gestire le configurazioni della memorizzazione sui controller LSI® MegaRAID, SAS e WarpDrive.

Le considerazioni di sicurezza per i moduli MSM in una scheda Sun Flash Accelerator F40 PCIe Card sono:

- Compatibilità Storage Manager MegaRAID: Linux 64 bit, Solaris X86.
- Fare riferimento al manuale dell'utente fornito da LSI, alla Guida in linea incorporata in MSM e al file Readme fornito con il programma di installazione. Andare a http://www.lsi.com.
- Agli utenti viene richiesto di autenticarsi per poter accedere.
  - Agli utenti che eseguono l'autenticazione come root è consentito l'accesso completo all'hardware.

    - Agli utenti che eseguono l'autenticazione come semplici utenti è concesso solo il privilegio di visualizzazione.
- Di solito, i file di log dispongono dell'autorizzazione di scrittura, i file binari di quella di esecuzione e gli altri file sono in sola lettura.
- Un solo utente alla volta dispone del privilegio amministrativo. Gli altri utenti dispongono unicamente del privilegio di visualizzazione. Un generatore di numeri casuali Java incorporato viene utilizzato per generare un ID sessione al momento dell'autenticazione client-server.
- Il client e il server sono implementati in Java. Il client e il server utilizzano il protocollo TCP/IP per comunicare tra loro. Il server comunica con la libreria mediante JNI.
- MSM interagisce con Internet ma non supporta IPv6.
- MSM utilizza SSL per le comunicazioni tra client e server.
- Le impostazioni del firewall per il sistema dipendono dal tipo di installazione effettuato.
    - Con tutte le installazioni, eccetto quella locale, il firewall dovrà essere configurato in modo da controllare l'accesso a client e server MSM.
    - L'installazione locale utilizzerà l'IP localhost.
- Per configurare o modificare le impostazioni è necessario l'accesso utente root. Per limitare l'accesso a potenziali attacchi, seguire le linee guida riportate di seguito.
    - Scegliere una password sicura.
    - Utilizzare password diverse per tutti i sistemi che eseguono componenti MSM, sia client che server.
- Facoltativamente, LDAP può essere utilizzato per autenticare l'accesso ai server.
- MegaRAID Storage Manager (MSM) può essere installato secondo le modalità riportate di seguito.
    - Completa: vengono installati tutti i componenti.
    - Client: vengono istallati solo i componenti richiesti per la visualizzazione e la configurazione remota dei server. Le porte 3071 e 5571 devono essere aperte.
    - Server: vengono installati solo i componenti richiesti per la gestione del server remoto.

      Oltre a un indirizzo unicast, il server MSM utilizza anche l'indirizzo IP multicast 229.111.112.12, nonché le porte TCP/UDP 3071 e 5571.

      Per SNMP, le porte 161 e 162 devono essere aperte. Se LDAP è configurato, la porta 389 deve essere aperta.
    - StandAlone: vengono installati solo i componenti richiesti per la gestione del server locale.
    - Locale: vengono installati solo i componenti richiesti per la configurazione del server locale.

Sicurezza di Diagnostic Services

Diagnostic Services è un'applicazione daemon di servizi che ascolta gli eventi di trigger associati a WarpDrive eseguiti dal driver. Diagnostic Services raccoglie le informazioni di diagnostica da WarpDrive quando si verifica un evento segnalato o quando richiesto da un utente.

Le considerazioni di sicurezza per i moduli di Diagnostic Services in una scheda Sun Flash Accelerator F40 PCIe Card sono:

- Il daemon Diagnostic Services utilizza l'API della libreria storelib per configurare gli eventi di trigger rilevanti e per ottenere notifiche degli eventi.
- Le informazioni di evento e di log di Diagnostic Services vengono ottenute esclusivamente tramite l'API della libreria storelib e salvate in file di log.
- Diagnostic Services utilizza la porta UDP 162.

- Un file di script evento utente di esempio è installato per impostazione predefinita ma non viene utilizzato a meno che non venga configurato a scopo di debug.
- I file di configurazione e di log di Diagnostic Services sono in sola lettura per tutti e presentano l'autorizzazione in scrittura per l'utente root. I file binari sono in sola lettura per tutti, mentre per l'utente root presentano l'autorizzazione di scrittura e di esecuzione.
- Diagnostic Services, se configurato, può inviare messaggi di interrupt SNMP quando si verifica un evento. Internamente viene utilizzato un pipe per il monitoraggio.

Sicurezza del driver di diagnostica Linux

Il driver di diagnostica Linux è il driver MPT2SAS SAS2 da 6 Gb che può automaticamente inviare un buffer Host Trace (2MB) all'avvio, implementare trigger del servizio di diagnostica e supportare diverse funzioni utilizzando l'applicazione dell'interfaccia di gestione. In base agli attributi di trigger, il driver esegue il monitoraggio degli errori e aggiunge un nuovo evento del servizio di diagnostica per riferimento futuro.

Le considerazioni di sicurezza per il driver di diagnostica Linux in una scheda Sun Flash Accelerator F40 PCIe Card sono:

- Il driver di diagnostica Linux viene eseguito nello spazio kernel. Se il sistema operativo è virtualizzato, il driver viene eseguito nell'elemento padre.
- Il driver di diagnostica Linux acquisisce il trace buffer dal firmware quando si verifica un set di eventi di trigger. Questi eventi di trigger sono specificati dall'amministratore del sistema e vengono trasmessi al driver mediante l'interfaccia Sysfs nel kernel.
- Solo un utente root con autorizzazione può scrivere nel file degli attributi Sysfs del driver di diagnostica Linux.
- I prodotti driver di diagnostica Linux generazione SAS2 supportano la protezione EEDP (End-to-End Data Protection).
- Il driver di diagnostica Linux si trova tra hardware, firmware e il layer intermedio del sistema operativo. Il driver di diagnostica Linux utilizza gli affermati protocolli di settore SAS2 e SATA e la tecnologia di passaggio dei messaggi LSI nell'estremità finale, le chiamate del sistema operativo nell'estremità iniziale per gestire il flusso di dati di memorizzazione.
- L'origine del driver di diagnostica Linux è Open Source e verificata dalla community del kernel Linux.
- Il driver di diagnostica Linux ha accesso completo a tutto l'hardware che gestisce, nonché accesso a tutte le strutture del kernel necessarie per il suo funzionamento. Il driver di diagnostica Linux ha accesso completo a tutte le interfacce del kernel utilizzate per gestire gli I/O SCSI.

Sicurezza SNMP

L'agente SNMP consente di gestire e monitorare i controller LSI SAS utilizzando il protocollo SNMP (Simple Network Management Protocol). La famiglia di controller supportata da SNMP è LSI MR, IR, IR2 e WarpDrive. È possibile utilizzare un browser MIB o crearne uno proprio per monitorare e configurare la topologia esposta dall'agente LSI SNMP.

Le considerazioni di sicurezza per i moduli SNMP in una scheda Sun Flash Accelerator F40 PCIe Card sono:

- L'agente secondario SNMP utilizza il protocollo SNMP (Simple Network Management Protocol) per fornire informazioni sul sistema di monitoraggio a un client SNMP.
- Il client SNMP può essere un qualsiasi browser MIB che supporti SNMPv1.

- L'agente secondario MR/IR SNMP raccoglie informazioni dalle librerie storelib utilizzando l'API storelib. Storelib esegue controlli di I/O (IOCTL) al driver per recuperare l'informazione.
- I file di log SNMP dispongono dell'autorizzazione di scrittura, i file binari dell'autorizzazione di esecuzione, gli altri file sono in sola lettura.
- Per qualsiasi accesso SNMP è richiesta un'autenticazione che utilizzi un meccanismo di autenticazione supportato da Net-SNMP.

Sicurezza del firmware del controller WarpDrive

Il firmware del controller WarpDrive viene eseguito sulla scheda del controller WarpDrive. Offre una velocità di trasferimento di 6 Gbps o 3 Gbps legacy ai Solid State Drives (DFF) SATA connessi alla scheda del controller WarpDrive. La connettività dell'host al controller WarpDrive è supportata mediante una connessione PCIe 2.0.

Le considerazioni di sicurezza per il firmware del controller WarpDrive in una scheda Sun Flash Accelerator F40 PCIe Card sono:

- Il firmware del controller WarpDrive viene eseguito sul processore situato sulla scheda del controller.
- I driver del sistema operativo WarpDrive sono sopra il firmware del controller WarpDrive e comunicano mediante PCIe, utilizzando l'interfaccia MPI (Message Passing Interface).
- Il firmware del controller WarpDrive interagisce con i moduli dell'unità SSD sottostanti, utilizzando l'interfaccia SAS/SATA.
- Solo le immagini del firmware del controller WarpDrive con firma e checksum corretti possono essere caricate sulla scheda.

Sicurezza SSDFW

Il modulo del firmware SSDFW fornisce il firmware per la famiglia di processori con memoria flash SF-2500.

Le considerazioni di sicurezza per i moduli SSDFW in una scheda Sun Flash Accelerator F40 PCIe Card sono:

- Il modulo del firmware SSDFW si connette all'interfaccia NAND Flash su un lato e all'interfaccia SATA AHCI sull'altro lato.
- La comunicazione lato host si connette mediante interfaccia SATA, definita nelle specifiche Serial ATA e del set di comandi ATA (ACS-2).
- L'autorizzazione amministrativa del modulo del firmware SSDFW è predefinita.
- I file di log sono cifrati. I log sono supportati mediante una porta seriale.
- Il modulo SSDFW è un firmware incorporato che si trova nel circuito integrato specifico dell'applicazione (ASIC) del processore con memoria flash SF-2500.
- Il modulo del firmware SSDFW memorizza i dati di sistema (come uno stato dell'unità) e i dati utente in un supporto NAND non volatile. Tutti i dati di sistema vengono cifrati con una chiave univoca dell'unità.
- Le password utente e di sistema vengono utilizzate per ottenere i privilegi.
- Il firmware SSDFW è incorporato nel sottosistema LSI-ASD.
- Per cifrare i dati (testo non codificato) viene utilizzata la cifratura AES-128 o AES-256. Un motore SHA autentica il firmware. Le chiavi e i valori del contatore vengono cifrati prima di essere memorizzati nella memoria flash.

Sicurezza DDCLI

DDCLI è un'applicazione utente. DDCLI è una CLI standalone che consente di monitorare tutti gli elementi WarpDrive connessi al sistema. Informazioni importanti su vari componenti di WarpDrive possono essere richiamate utilizzando la utility **ddcli**.

Le considerazioni di sicurezza per l'applicazione DDCLI in una scheda Sun Flash Accelerator F40 PCIe Card sono:

- L'applicazione DDCLI viene fornita inizialmente senza autorizzazione di esecuzione. L'utente root dovrà aggiungere questa autorizzazione.
- Perché il file ddcli possa essere eseguito, sarà necessario modificarne l'autorizzazione. Per ridurre al minimo i problemi di sicurezza, impostare le autorizzazioni su 0744. Il file deve essere di proprietà dell'utente root. Ciò consente a tutti gli utenti di vedere il file ma solo all'utente root di eseguirlo.
- Una libreria che supporta le API MPT (Message Processing Technology) è collegata in modo statico a DDCLI. La libreria invia un controllo I/O (IOCTL) al driver per ottenere l'informazione richiesta.
- L'applicazione DDCLI è un file binario con autorizzazione di esecuzione.