Sun Flash Accelerator F40 PCIe Card

Guía de seguridad

Referencia: E39694-02
Octubre de 2013

Copyright © 2013 Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comunique por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera licencias en nombre del Gobierno de EE.UU. se aplicará la siguiente disposición:

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.

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden ofrecer acceso a contenidos, productos o servicios de terceros o información sobre los mismos. Ni Oracle Corporation ni sus subsidiarias serán responsables de ofrecer cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros y renuncian explícitamente a ello. Oracle Corporation y sus subsidiarias no se harán responsables de las pérdidas, los costos o los daños en los que se incurra como consecuencia del acceso o el uso de contenidos, productos o servicios de terceros.

Tabla de contenidos

1. Seguridad de Sun Flash Accelerator F40 PCIe Card 5
Descripción de Sun Flash Accelerator F40 PCIe Card 5
Componentes de hardware 6
Componentes de software y firmware 6
Principios de seguridad 7
Planificación de un entorno seguro 7
Seguridad de hardware 7
Seguridad de software 8
Seguridad de firmware 8
Firmware de Oracle ILOM 8
Registros del sistema 9
Mantenimiento de un entorno seguro 9
Seguimiento de activos 9
Actualizaciones de firmware 9
Actualizaciones de software 9
Seguridad de los registros 10
Seguridad del módulo 10
Seguridad de la aplicación MSM 10
Seguridad de Diagnostic Services 11
Seguridad del controlador de diagnóstico de Linux 12
Seguridad de SNMP 12
Seguridad del firmware del controlador WarpDrive 13
Seguridad de SSDFW 13
Seguridad de DDCLI 14

• • • Capítulo 1

Seguridad de Sun Flash Accelerator F40 PCIe Card

En este documento, se proporcionan directrices de seguridad generales para ayudarlo a proteger los productos de hardware x86 de Oracle, como Sun Flash Accelerator F40 PCIe Card.

Se incluyen las siguientes secciones:

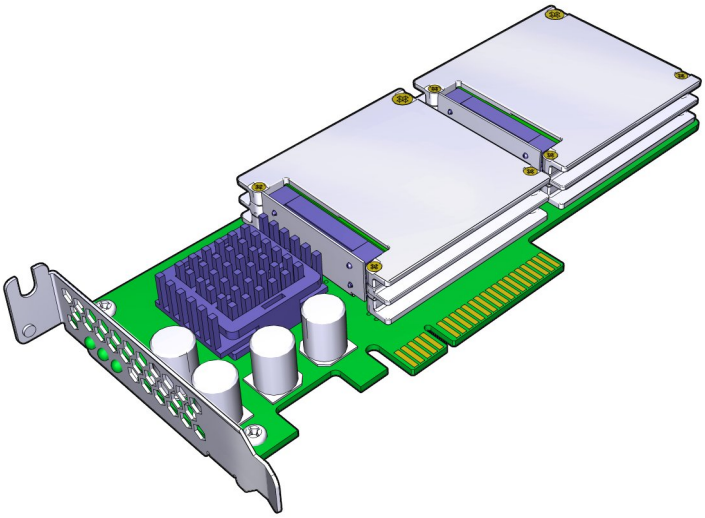
- “Descripción de Sun Flash Accelerator F40 PCIe Card” [5]
- “Principios de seguridad” [7]
- “Planificación de un entorno seguro” [7]
- “Mantenimiento de un entorno seguro” [9]

Descripción de Sun Flash Accelerator F40 PCIe Card

Se incluyen las siguientes secciones:

- “Componentes de hardware” [6]
- “Componentes de software y firmware” [6]

Sun Flash Accelerator F40 PCIe Card es una tarjeta de almacenamiento PCI-E 2.0 de memoria flash, con factor de forma de bajo perfil, de adaptador bus de host (HBA), lista para usar. La siguiente imagen muestra la tarjeta Sun Flash Accelerator F40 PCIe Card:



Consulte la *Guía del usuario de Sun Flash Accelerator F40 PCIe Card* para obtener información detallada del producto.

Componentes de hardware

Sun Flash Accelerator F40 PCIe Card tiene los siguientes componentes de hardware:

- Cuatro módulos flash de unidad de estado sólido (SSD): un total de 400 GB de memoria flash NAND eMLC de 32 nm se monta directamente en la tarjeta.
- Controlador de protocolo PCI-E a SAS: la interfaz SATA de Sun Flash Accelerator F40 PCIe Card al controlador de protocolo tiene una interfaz de host PCI-E 2.0 x8 que se conecta a un controlador de protocolo LSI 2008 SAS/SATA 2 x4 6 de Gbps.
- Componentes de almacenamiento de energía: las tareas de escritura no completadas se vuelcan en la memoria flash si falla la energía del sistema o la ranura PCIe.

Consulte la *Guía del usuario de Sun Flash Accelerator F40 PCIe Card* para obtener información detallada.

Componentes de software y firmware

Los siguientes módulos se incluyen con Sun Flash Accelerator F40 PCIe Card:

Componente	Consulte
MegaRAID Storage Manager (MSM)	“Seguridad de la aplicación MSM” en la página 7
Diagnostic Services	“Seguridad de Diagnostic Services” en la página 8
Controlador de diagnóstico de Linux	“Seguridad del controlador de diagnóstico de Linux” en la página 9
SNMP	“Seguridad de SNMP” en la página 9
Firmware del controlador WarpDrive	“Seguridad del firmware del controlador WarpDrive” en la página 10
SSDFW	“Seguridad de SSDFW” en la página 10
DDCLI	“Seguridad de DDCLI” en la página 11

Consulte la *Guía del usuario de Sun Flash Accelerator F40 PCIe Card* para obtener información detallada.

Principios de seguridad

Hay cuatro principios básicos de seguridad: acceso, autenticación, autorización y contabilidad.

- **Acceso**

  Los controles físicos y de software protegen el hardware y sus datos frente a posibles intrusiones.
  - En el caso del hardware, los límites de acceso por lo general son límites de acceso *físicos*.
  - En el caso del software, el acceso está limitado por medios físicos y virtuales.
  - El firmware no se puede cambiar, salvo a través del proceso de actualización de Oracle.
- **Autenticación**

  Configure las funciones de autenticación, por ejemplo, un sistema de contraseñas, en los sistemas operativos de la plataforma para asegurarse de que los usuarios sean quienes dicen ser.

  Asegúrese de que el personal utilice correctamente las identificaciones de empleado para ingresar a la sala de cómputo.
- **Autorización**

  Permita al personal trabajar únicamente con hardware y software para cuyo uso estén capacitados y cualificados. Establezca un sistema de permisos de lectura, escritura y ejecución para controlar el acceso del usuario a los comandos, el espacio en el disco, los dispositivos y las aplicaciones.
- **Contabilidad**

  Utilice las funciones de software y de hardware de Oracle para supervisar la actividad de conexión y mantener los inventarios de hardware.
  - Utilice los registros del sistema para supervisar las conexiones de los usuarios. Supervise las cuentas de servicio y de administrador del sistema en particular, ya que estas cuentas pueden acceder a comandos importantes.
  - Utilice los números de serie de los componentes para hacer un seguimiento de los activos del sistema. Los números de pieza de Oracle se registran electrónicamente en todas las tarjetas, módulos y placas base.

Planificación de un entorno seguro

Utilice las siguientes notas antes de la instalación y la configuración de un servidor y de Sun Flash Accelerator F40 PCIe Car, o después de ellas.

Se incluyen las siguientes secciones:

- “Seguridad de hardware ” [7]
- “Seguridad de software ” [8]
- “Seguridad de firmware” [8]
- “Firmware de Oracle ILOM” [8]
- “Registros del sistema” [9]

Seguridad de hardware

El hardware físico se puede proteger con relativa facilidad limitando el acceso al hardware y registrando los números de serie.

- **Restringir el acceso**

  - Si el equipo está instalado en un bastidor que tiene una puerta con llave, mantenga la puerta cerrada con llave, excepto cuando tenga que reparar los componentes del bastidor.
  - Almacene las unidades sustituibles en campo (FRU) o las unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado a personal autorizado.
- **Registrar los números de serie**
  - Realice una marca de seguridad en todas las tarjetas Sun Flash Accelerator F40 PCIe Card. Utilice plumas ultravioletas o etiquetas en relieve especiales.
  - Mantenga un registro de los números de serie de todas las tarjetas Sun Flash Accelerator F40 PCIe Card.
  - Mantenga las licencias y las claves de activación de hardware en una ubicación segura y de fácil acceso para el administrador del sistema en caso de emergencia del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.

Seguridad de software

Las siguientes son las consideraciones de seguridad para los componentes de software:

- Consulte la documentación que se facilita con el software para activar las funciones de seguridad disponibles para el software.
- Use una cuenta de superusuario para configurar y actualizar los controladores de Sun Flash Accelerator F40 PCIe Card.
- La mayoría de las medidas de protección del hardware se implementan mediante medidas de software
- Los componentes de software que admiten Sun Flash Accelerator F40 PCIe Card se basan en funciones de seguridad de sistema para proporcionar acceso seguro.

Seguridad de firmware

Sun Flash Accelerator F40 PCIe Card se suministra con todo el firmware instalado. No es necesario realizar la instalación del firmware en el campo, salvo las actualizaciones.

- Si alguna vez necesita actualizar el firmware, póngase en contacto con la asistencia técnica de Oracle a fin de coordinar la asistencia o visite My Oracle Support para conocer las últimas actualizaciones y procedimientos para el producto:

  https://support.oracle.com
- Use la cuenta de superusuario para configurar y actualizar la utilidad de gestión de firmware de Sun Flash Accelerator F40 PCIe Card. Las cuentas de usuarios comunes sólo le permiten al usuario ver el firmware, no editarlo. El proceso de actualización del firmware del sistema operativo Oracle Solaris evita que se realicen modificaciones de firmware sin autorización.
- Consulte las notas del producto que se proporcionan con Sun Flash Accelerator F40 PCIe Card para conocer información de última hora, información sobre requisitos de actualización de firmware u otra información de seguridad.
- Para obtener más información sobre la configuración de las variables de seguridad de OpenBootPROM (OBP), consulte el *Manual de referencia del comando OpenBoot 4.x*.

Firmware de Oracle ILOM

Puede proteger, gestionar y supervisar de manera activa los componentes del sistema mediante el firmware Oracle Integrated Lights Out Manager (Oracle ILOM), que está preinstalado en algunos

servidores x86. Para obtener más información sobre el uso de este firmware al configurar contraseñas, administrar usuarios y aplicar funciones relacionadas con la seguridad, así como los Secure Shell (SSH), los Secure Socket Layer (SSL) y la autenticación RADIUS, consulte la documentación de Oracle ILOM:

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

Registros del sistema

- Active el registro y envíe los registros a un host de registro dedicado seguro.
- Configure el registro para incluir información de tiempo precisa mediante NTP y registros de hora.

Mantenimiento de un entorno seguro

Después de la instalación y la configuración iniciales de Sun Flash Accelerator F40 PCIe Card, utilice las funciones de seguridad del hardware y el software de Oracle para seguir controlando el hardware y realizando el seguimiento de los activos del sistema.

Se incluyen las siguientes secciones:

- “Seguimiento de activos” [9]
- “Actualizaciones de firmware” [9]
- “Actualizaciones de software ” [9]
- “Seguridad de los registros” [10]
- “Seguridad del módulo” [10]

Seguimiento de activos

Utilice los números de serie para hacer un seguimiento del inventario. Oracle incrusta los números de serie del firmware en tarjetas opcionales y placas base del sistema. Puede leer estos números de serie mediante conexiones de red de área local.

También puede utilizar lectores inalámbricos de identificación por radiofrecuencia (RFID) para simplificar aún más el seguimiento de activos. Consulte las notas del producto de Oracle, *Cómo realizar un seguimiento de sus activos del sistema Oracle Sun mediante RFID*.

Actualizaciones de firmware

Mantenga actualizadas las versiones de firmware en sus equipos.

- Consulte periódicamente si hay actualizaciones.
- Todos los sistemas operativos en general, y Oracle Solaris en particular, requieren que se conecte con credenciales de usuario root para administrar las tarjetas y actualizar los controladores o el firmware.
- Instale siempre la versión más reciente del firmware.

Actualizaciones de software

Mantenga actualizadas sus versiones de software en sus equipos.

- Las actualizaciones de software de los controladores de Oracle Solaris están disponibles mediante parches y actualizaciones de Oracle Solaris.

- Las actualizaciones de software para los controladores de otros sistemas operativos pueden estar disponibles en http://www.lsi.com.
- Consulte las notas del producto que se proporcionan con Sun Flash Accelerator F40 PCIe Card para obtener información de última hora, información sobre requisitos de actualización de software u otra información de seguridad.
- Instale siempre la versión más reciente del software.
- Instale los parches de seguridad necesarios para el software.
- Los dispositivos también contienen firmware y pueden requerir actualizaciones de firmware.

Seguridad de los registros

Inspeccione y mantenga los archivos de registro de manera periódica.

- Revise los registros para detectar posibles incidentes y archívelos de acuerdo con una política de seguridad.
- Retire con regularidad los archivos de registro cuando excedan un tamaño razonable. Mantenga copias de los archivos retirados para posible referencia futura o análisis estadísticos.

Seguridad del módulo

Los módulos de software y firmware son los siguientes:

- “Seguridad de la aplicación MSM” [10]
- “Seguridad de Diagnostic Services” [11]
- “Seguridad del controlador de diagnóstico de Linux” [12]
- “Seguridad de SNMP” [12]
- “Seguridad de SSDFW” [13]
- “Seguridad de DDCLI” [14]



Nota

El término WarpDrive en este texto hace referencia a Sun Flash Accelerator F40 PCIe Card.

Seguridad de la aplicación MSM

MegaRAID Storage Manager (MSM) es una aplicación de software que proporciona una interfaz gráfica de usuario para configurar el firmware de WarpDrive mediante el controlador e interaccionar con él. MSM también supervisa y mantiene las configuraciones de almacenamiento en los controladores LSI® MegaRAID, SAS y WarpDrive.

Las siguientes son las consideraciones de seguridad para los módulos MSM en Sun Flash Accelerator F40 PCIe Card:

- Compatibilidad con MegaRAID Storage Manager: Linux de 64 bits, Solaris X86.
- Consulte la guía del usuario proporcionada por LSI, la ayuda en pantalla integrada con MSM y el archivo léame que se proporciona con el instalador. Visite http://www.lsi.com.
- Los usuarios deben autenticarse antes de que se les permita el acceso.
  - Si un usuario se autentica como usuario root, se le permite el acceso a todo el hardware.

  - Si se autentica como usuario, se le otorga privilegio de sólo lectura.
- Por lo general, los archivos de registro tienen permiso de escritura, los archivos binarios tienen permiso de ejecución y otros archivos son de sólo lectura.
- Sólo un usuario por vez puede tener privilegios administrativos. Los demás usuarios tienen privilegios de sólo lectura. Se utiliza un generador de números aleatorios Java incorporado para generar una ID de sesión cuando se realiza la autenticación de cliente-servidor.
- El cliente y el servidor se implementan en Java. El cliente y el servidor usan TCP/IP para comunicarse entre sí. El servidor se comunica con la biblioteca mediante JNI.
- MSM interacciona con Internet, pero no admite IPv6.
- MSM utiliza SSL para la comunicación entre el cliente y el servidor.
- La configuración del cortafuegos de su sistema depende del tipo de instalación que se realiza.
  - En todas las instalaciones, salvo las locales, el cortafuegos necesitará configurarse para controlar el acceso al cliente y servidor MSM.
  - La instalación local usará la dirección IP de host local.
- Se necesita acceso de usuario root para configurar/modificar la configuración. Para limitar el acceso de los posibles atacantes, siga las siguientes directrices:
  - Elija una contraseña segura.
  - Use contraseñas diferentes para todos los sistemas que ejecutan componentes MSM, tanto en el cliente como en el servidor.
- Opcionalmente, se puede utilizar LDAP para autenticar el acceso a los servidores.
- MegaRAID Storage Manager (MSM) se puede instalar de las siguientes maneras:
  - Instalación completa: se instalan todos los componentes.
  - Cliente: sólo se instalan los componentes requeridos para ver y configurar servidores de manera remota. Deben abrirse los puertos 3071 y 5571.
  - Servidor: sólo se instalan los componentes requeridos para la gestión remota del servidor.

    Además de utilizar una dirección de unidifusión, el servidor MSM también utiliza la dirección IP de multidifusión 229.111.112.12 y los puertos TCP/UDP 3071 y 5571.

    Para SNMP, deben abriese los puertos 161 y 162. Si se configura LDAP, debe abrirse el puerto 389.
  - Independiente: sólo se instalan los componentes requeridos para la gestión del servidor local.
  - Local: sólo se instalan los componentes requeridos para la configuración del servidor local.

Seguridad de Diagnostic Services

Diagnostic Services es una aplicación de daemon de servicio que realiza el proceso de escucha para detectar eventos de activación asociados con WarpDrive emitidos por el controlador. Diagnostic Services recopila información de diagnóstico de WarpDrive cuando ocurre un evento informado o cuando lo solicita un usuario.

Las siguientes son las consideraciones de seguridad para los módulos de Diagnostic Services en Sun Flash Accelerator F40 PCIe Card:

- El daemon de Diagnostic Services utiliza la API de la biblioteca storelib para configurar eventos de activación de interés y para obtener notificaciones de eventos.
- La información de evento y de registro de Diagnostic Services se obtiene exclusivamente mediante la API de la biblioteca storelib y se guarda en archivos de registro.
- Diagnostic Services utiliza el puerto 162 de UDP.

- De manera predeterminada, se instala un archivo de secuencia de comandos de eventos de usuario de ejemplo, pero no se utiliza a menos que se lo configure para depuración.
- Los archivos de registro y configuración de Diagnostic Services son de sólo lectura para todos, y sólo el usuario root tiene permiso de escritura. Los archivos binarios son de sólo lectura para todos, y sólo el usuario root tiene permisos de ejecución y escritura.
- Diagnostic Services, si se configura, puede enviar mensajes de captura SNMP cuando ocurre un evento. Internamente, se utiliza una canalización para la supervisión.

Seguridad del controlador de diagnóstico de Linux

El controlador de diagnóstico de Linux es el controlador MPT2SAS SAS2 6 Gb que puede publicar automáticamente un búfer de seguimiento de host (2MB) en el inicio, implementar activadores de servicio de diagnóstico y admitir varias funciones mediante la aplicación de interfaz de gestión. Según los atributos de activación, el controlador supervisa los errores y agrega un evento de servicio de diagnóstico nuevo para referencia futura.

Las siguientes son las consideraciones de seguridad para el controlador de diagnóstico de Linux en Sun Flash Accelerator F40 PCIe Card:

- El controlador de diagnóstico de Linux se ejecuta en espacio del núcleo. Si el sistema operativo está virtualizado, el controlador se ejecuta en el sistema principal.
- El controlador de diagnóstico de Linux captura el búfer de seguimiento del firmware cuando ocurre un conjunto de eventos de activación. Estos eventos de activación son especificados por el administrador del sistema y se envían al controlador mediante la interfaz Sysfs en el núcleo.
- Sólo un usuario root con permiso puede escribir en los archivos de atributos Sysfs del controlador de diagnóstico de Linux.
- Los productos del controlador de diagnóstico de Linux de la generación SAS2 admiten EEDP (protección de datos de extremo a extremo).
- El controlador de diagnóstico de Linux se ubica entre el hardware, el firmware y la capa media del sistema operativo. El controlador de diagnóstico de Linux usa los protocolos de la industria SAS2 y SATA establecidos y tecnología de especificación de mensajes LSI en el extremo inferior, y llamadas al sistema operativo en extremo superior para manejar el flujo de datos de almacenamiento.
- El controlador de diagnóstico de Linux es de código abierto y es revisado por la comunidad del kernel de Linux.
- El controlador de diagnóstico de Linux tiene acceso completo a todo el hardware que gestiona y, además, cuenta con acceso a todas las estructuras del núcleo que necesita para funcionar. El controlador de diagnóstico de Linux tiene acceso completo a todas las interfaces del núcleo que se usan para gestionar las E/S de SCSI.

Seguridad de SNMP

El agente SNMP le permite gestionar y supervisar los controladores LSI SAS mediante el Protocolo Simple de Gestión de Red (SNMP). SNMP admite la familia de controladores LSI MR, IR, IR2 y WarpDrive. Puede usar un explorador MIB, o crear el suyo propio, para supervisar y configurar la topología expuesta por el agente LSI SNMP.

Las siguientes son las consideraciones de seguridad para los módulos SNMP en Sun Flash Accelerator F40 PCIe Card:

- Los subagentes SNMP usan el Protocolo Simple de Gestión de Red para proporcionar información del sistema de supervisión a un cliente SNMP.

- El cliente SNMP puede ser cualquier explorador MIB que admita SNMPv1.
- El subagente MR/IR SNMP recupera información de las bibliotecas storelib mediante la API storelib. Storelib realiza controles de entrada/salida (IOCTL) del controlador para obtener información.
- Los archivos de registro de SNMP tienen permiso de escritura, los archivos binarios tienen permiso de ejecución, los demás archivos son de sólo lectura.
- Se requiere un mecanismo de autenticación que admita Net-SNMP para el acceso de SNMP.

Seguridad del firmware del controlador WarpDrive

El firmware del controlador WarpDrive se ejecuta en la placa del controlador WarpDrive. Ofrece unidades de estado sólido (SDD) SATA con velocidad de transferencia de 6 Gbps (o 3 Gbps heredados) conectadas a la placa del controlador WarpDrive. La conectividad de host del controlador WarpDrive se admite mediante una conexión PCIe 2.0.

Las siguientes son las consideraciones de seguridad para el firmware del controlador WarpDrive en Sun Flash Accelerator F40 PCIe Card:

- El firmware del controlador WarpDrive se ejecuta en el procesador ubicado en la placa del controlador.
- Las unidades del sistema operativo de WarpDrive se ubican sobre el firmware del controlador Warp Drive y se comunican mediante PCIe, usando MPI (interfaz de especificación de mensajes).
- El firmware del controlador WarpDrive interacciona con los módulos de unidades SSD debajo de él, usando la interfaz SAS/SATA.
- Sólo se permite cargar a la placa las imágenes de firmware del controlador WarpDrive con la firma y el total de control correctos.

Seguridad de SSDFW

El módulo de firmware de SSDFW proporciona firmware para la familia del procesador de almacenamiento flash SF-2500.

Las siguientes son las consideraciones de seguridad para los módulos SSDFW en Sun Flash Accelerator F40 PCIe Card:

- El módulo de firmware de SSDFW conecta la interfaz de memoria flash NAND en un lado y la interfaz SATA AHCI en el otro.
- La comunicación del lado del host se conecta mediante la interfaz SATA, definida en la especificación Serial ATA y la especificación ATA Command Set (ACS-2).
- El permiso de administrador del módulo de firmware SSDFW es predeterminado.
- Los archivos de registro están cifrados. La generación de archivos de registro se admite mediante puerto serial.
- El módulo SSDFW tiene firmware incrustado que reside en el ASIC del procesador de almacenamiento flash SF-2500.
- El módulo de firmware SSDFW almacena datos del sistema (como el estado de la unidad) y datos del usuario, y los ubica en medios NAND no volátiles. Todos los datos del sistema se cifran con una clave única de unidad.
- Se utilizan contraseñas de sistema y usuario para obtener privilegios.
- El firmware de SSDFW está incrustado con el subsistema LSI-ASD.
- Se usa AES-128 o AES-256 para cifrar datos (texto sin formato). Un motor SHA autentica el firmware. Las claves y los valores del contador se cifran antes de almacenarse en la memoria flash.

Seguridad de DDCLI

DDCLI es una aplicación de usuario. DDCLI es una interfaz de línea de comandos independiente que le permite supervisar cualquier WarpDrive conectado al sistema. Es posible recuperar información importante sobre varios componentes de WarpDrive usando la utilidad **ddcli**.

Las siguientes son las consideraciones de seguridad para la aplicación DDCLI en Sun Flash Accelerator F40 PCIe Card:

- DDCLI se proporciona inicialmente sin permisos de ejecución. El usuario root necesitará agregar este permiso.
- El archivo ddcli necesitará que se cambien sus permisos para que se pueda ejecutar. Para minimizar los problemas de seguridad, establezca los permisos en 0744. Debe ser propiedad del usuario root. Esto permitirá que todos puedan verlo, pero sólo el usuario root podrá ejecutarlo.
- Hay una biblioteca que admite API de MPT (tecnología de procesamiento de mensajes) que está estáticamente vinculada con DDCLI. Esa biblioteca envía una llamada de control de entrada/salida al controlador para obtener la información requerida.
- La aplicación DDCLI es un archivo binario con permiso de ejecución.