Sun Flash Accelerator F40 PCIe Card

Security Guide

Parte No: E39702-02
Outubro de 2013

Índice

• • • Capítulo 1

Segurança do Sun Flash Accelerator F40 PCIe Card

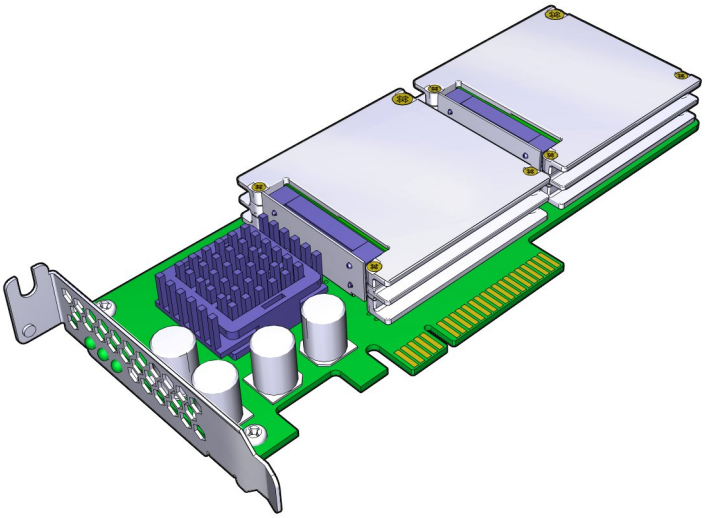
Este documento fornece diretrizes gerais de segurança para ajudá-lo a proteger os produtos de hardware Oracle x86, como o PCIe Sun Flash Accelerator F40 PCIe Card.

As seguintes seções estão incluídas:

Descrição do Sun Flash Accelerator F40 PCIe Card

As seguintes seções estão incluídas:

O Sun Flash Accelerator F40 PCIe Card é um cartão compacto de armazenamento em memória flash HBA PCI-E 2.0 pronto para ser usado. O cartão é ilustrado na imagem a seguir:



Consulte o *Sun Flash Accelerator F40 PCIe Card User Guide* para obter informações detalhadas sobre o produto.

Componentes de Hardware

O Sun Flash Accelerator F40 PCIe Card contém os seguintes componentes de hardware:

- Quatro módulos Flash SSD: Um total de memória flash NAND eMLC de 32 nm e 400 GB é montado diretamente no cartão.
- Controlador de protocolo PCI-E para SAS: A interface SATA do Sun Flash Accelerator F40 PCIe Card com o controlador de protocolo tem uma interface de host x8 PCI-E 2.0 que estabelece conexão com um controlador de protocolo de 6 Gbps x4 LSI 2008 SAS/SATA 2.
- Componentes de armazenamento de energia: Descarregam gravações não concluídas para a memória flash em caso de falha de energia do sistema ou do slot PCIe.

Consulte o *Sun Flash Accelerator F40 PCIe Card User Guide* para obter informações detalhadas.

Componentes de Software e Firmware

Os seguintes módulos são fornecidos com o Sun Flash Accelerator F40 PCIe Card:

Componente	Consulte
MSM (MegaRAID Storage Manager)	“Segurança do Aplicativo MSM” na página 7
Diagnostic Services	“Segurança do Diagnostic Services” na página 8
Linux Diagnostic Driver	“Segurança do Linux Diagnostic Driver” na página 9
SNMP	“Segurança do SNMP” na página 9
FW do Controlador WarpDrive	“Segurança do Firmware do Controlador Warp Drive” na página 10
SSDFW	“Segurança do SSDFW” na página 10
DDCLI	“Segurança do DDCLI” na página 11

Consulte o *Sun Flash Accelerator F40 PCIe Card User Guide* para obter informações detalhadas.

Princípios de Segurança

Há quatro princípios básicos de segurança: acesso, autenticação, autorização e contabilidade.

- **Acesso**

  Os controles físicos e de software protegem o hardware ou os dados de intrusão.
  - No caso do hardware, limites de acesso geralmente significam limites de acesso *físico*.
  - No caso do software, o acesso é limitado através de meios físicos e virtuais.
  - O firmware só pode ser alterado por meio do processo de atualização da Oracle.
- **Autenticação**

  Configure recursos de autenticação, como um sistema de senhas nos sistemas operacionais da plataforma, para garantir que os usuários são realmente quem eles dizem ser.

  Certifique-se de que sua equipe use crachás para entrar na sala do computador.
- **Autorização**

  Permita que sua equipe trabalhe somente com hardware e software nos quais foi treinada e esteja qualificada para usar. Configure um sistema de permissões de Leitura/Gravação/Execução para controlar o acesso de usuários a comandos, espaço em disco, dispositivos e aplicativos.
- **Contabilidade**

  Use os recursos de software e hardware da Oracle para monitorar a atividade de log-in e manter os inventários de hardware.
  - Use logs do sistema para monitorar log-ins de usuário. Monitore contas de serviço e administrador do sistema em particular porque essas contas podem acessar comandos avançados.
  - Use números de série de componente para rastrear ativos do sistema. Os números de peças Oracle são gravados eletronicamente em todos os cartões, módulos e placas-mãe.

Planejando um Ambiente Seguro

Use as seguintes notas antes e durante a instalação e a configuração de um servidor e do Sun Flash Accelerator F40 PCIe Card.

As seguintes seções estão incluídas:

Segurança do Hardware

É possível proteger o hardware físico de maneira bastante simples: limite o acesso ao hardware e registre os números de série.

- **Restringir o acesso**
  - Se o equipamento for instalado em um rack com uma porta com fechadura, mantenha a porta trancada, exceto durante os períodos de manutenção nos componentes do rack.

  - Guarde unidades substituíveis no campo (FRUs) e unidade substituíveis pelo cliente (CRUs) sobressalentes em um armário trancado. Restrinja o acesso ao armário trancado a pessoas autorizadas.
- **Registre os números de série**
  - Proteja com uma marca todos os Sun Flash Accelerator F40 PCIe Cards. Use canetas especiais ultravioletas ou etiquetas em alto-relevo.
  - Mantenha um registro dos números de série de todos os Sun Flash Accelerator F40 PCIe Cards.
  - Mantenha as chaves de ativação e as licenças do hardware em um local seguro e de fácil acesso ao gerente do sistema em caso de emergências. Os documentos impressos talvez sejam o seu único comprovante de propriedade.

Segurança do Software

Estas são as considerações de segurança para os componentes de software:

- Consulte a documentação que acompanha o software para ativar todos os recursos de segurança disponíveis para o software.
- Use a conta de superusuário para configurar e atualizar os drivers do Sun Flash Accelerator F40 PCIe Card.
- A maior parte da segurança do hardware é implementada por meio de medidas de software.
- Os componentes de software que oferecem suporte ao Sun Flash Accelerator F40 PCIe Card contam com recursos de segurança do sistema para garantir o acesso seguro.

Segurança do Firmware

O Sun Flash Accelerator F40 PCIe Card é fornecido com todo o firmware instalado. A instalação do firmware não é necessária no campo, exceto no caso de atualizações.

- Caso sejam necessárias atualizações do firmware, entre em contato com o suporte Oracle a fim de obter ajuda ou solicite a ele as atualizações e os procedimentos mais recentes do produto.

  https://support.oracle.com
- Use a conta de superusuário para configurar e atualizar o utilitário de gerenciamento do firmware do Sun Flash Accelerator F40 PCIe Card. Contas de usuário comuns permitem que os usuários visualizem, mas não editem o firmware. O processo de atualização do firmware do sistema operacional Oracle Solaris impede modificações não autorizadas no firmware.
- Consulte as notas do produto fornecidas com o Sun Flash Accelerator F40 PCIe Card para obter as informações mais recentes sobre os requisitos de atualização do firmware ou outras informações sobre segurança.
- Para obter informações sobre como definir as variáveis de segurança SPARC OpenBootPROM (OBP), consulte o *OpenBoot 4.x Command Reference Manual*.

Firmware do Oracle ILOM

É possível proteger, gerenciar e monitorar ativamente os componentes do sistema usando o firmware do Oracle ILOM (Integrated Lights Out Manager), o qual é pré-instalado em alguns servidores x86. Para saber mais sobre como usar esse firmware durante a configuração de senhas, o gerenciamento de usuários e a aplicação de recursos relacionados a segurança, incluindo autenticação Secure Shell (SSH), Secure Socket Layer (SSL) e RADIUS, consulte a documentação do Oracle ILOM:

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

Logs do Sistema

- Ative o registro em log e envie os logs para um host de log protegido dedicado.
- Configure o registro em log para incluir informações de tempo precisas, usando NTP e registros de hora e data.

Mantendo um Ambiente Seguro

Após a instalação e a configuração iniciais do Sun Flash Accelerator F40 PCIe Card, use os recursos de segurança de hardware e software da Oracle para continuar a controlar o hardware e rastrear os ativos do sistema.

As seguintes seções estão incluídas:

Rastreamento de Ativos

Use números de série para rastrear o estoque. A Oracle insere números de série em cartões de opção e em placas-mãe do sistema de firmware. É possível ler esses números de série por meio de conexões de rede local.

Também é possível usar leitores sem fio RFID (Radio Frequency Identification) para simplificar ainda mais o rastreamento de ativos. Consulte o white paper da Oracle *How to Track Your Oracle Sun System Assets by Using RFID*.

Atualizações de Firmware

Mantenha as versões de firmware atualizadas em seu equipamento.

- Verifique regularmente se há atualizações.
- Todos os sistemas operacionais, em geral, e o Oracle Solaris, em particular, exigem que você faça log-in com as credenciais de root para administrar os cartões e fazer upgrade dos drivers ou do firmware.
- Instale sempre a última versão lançada do firmware.

Atualizações de Software

Mantenha as versões de software atualizadas em seu equipamento.

- As atualizações de software para os drivers do Oracle Solaris são disponibilizadas por meio de patches e atualizações desse sistema operacional.
- As atualizações de software para os drivers de outros sistemas operacionais podem ser obtidas em http://www.lsi.com.
- Consulte as notas do produto fornecidas com o Sun Flash Accelerator F40 PCIe Card para obter as informações mais recentes sobre os requisitos de atualização de software ou outras informações sobre segurança.

- Instale sempre a última versão lançada do software.
- Instale todos os patches de segurança necessários para o software.
- Os dispositivos também contêm firmware, o qual pode exigir atualizações.

Segurança do Log

Inspecione e faça a manutenção de seus arquivos de log regularmente.

- Verifique possíveis incidentes nos logs e arquive-os de acordo com uma política de segurança.
- Remova periodicamente arquivos de log quando excederem um tamanho considerável. Mantenha cópias dos arquivos removidos para possíveis referências futuras ou análise estatística.

Segurança dos Módulos

Os módulos de software e firmware são:

- "Segurança do Aplicativo MSM" [10]
- "Segurança do Diagnostic Services" [11]
- "Segurança do Linux Diagnostic Driver" [12]
- "Segurança do SNMP" [12]
- "Segurança do SSDFW" [13]
- "Segurança do DDCLI" [13]

Observação

No texto, o termo WarpDrive se refere ao Sun Flash Accelerator F40 PCIe Card.

Segurança do Aplicativo MSM

O MSM (MegaRAID Storage Manager) é um aplicativo que fornece uma interface gráfica do usuário que permite configurar e interagir com o firmware do WarpDrive por meio do driver. O MSM também monitora e mantém as configurações de armazenamento nos controladores LSI® MegaRAID, SAS e WarpDrive.

Estas são as considerações de segurança para os módulos MSM em um Sun Flash Accelerator F40 PCIe Card:

- Compatibilidade com o MegaRAID Storage Manager: Linux 64 bits, Solaris X86.
- Consulte o guia do usuário fornecido pela LSI, a ajuda on-line incorporada no MSM e o arquivo readme fornecido com o instalador. Vá para http://www.lsi.com.
- Os usuários devem fazer a autenticação para obter permissão de acesso.
  - Se o usuário for autenticado como root, todo acesso ao hardware será permitido.
  - Se ele for autenticado como user, será concedido o privilégio somente de visualização.
- Normalmente, os arquivos de log têm permissão de gravação, os arquivos binários têm permissão de execução e os demais arquivos são somente leitura.
- Somente um usuário de cada vez tem privilégio administrativo. Os demais usuários têm privilégio somente de visualização. Um gerador de números aleatórios incorporado Java é usado para gerar um ID de sessão durante a autenticação do cliente-servidor.

- O cliente e o servidor são implementados em Java. O cliente e o servidor usam TCP/IP para se comunicarem entre si. O servidor se comunica com a biblioteca usando JNI.
- O MSM interage com a Internet, mas não oferece suporte a IPv6.
- O MSM usa o SSL para a comunicação entre o cliente e o servidor.
- As definições de firewall do sistema dependem do tipo de instalação executado.
  - Em todas as instalações, exceto a local, o firewall precisará ser configurado para controlar o acesso ao Cliente e ao Servidor MSM.
  - A instalação local usará o IP localhost.
- O acesso como usuário root é necessário para configurar/modificar as definições. Para limitar o acesso de possíveis invasores, use as diretrizes a seguir.
  - Escolha uma senha segura.
  - Use senhas diferentes para todos os sistemas que estejam executando componentes do MSM, tanto cliente como servidor.
- Opcionalmente, o LDAP poderá ser usado para autenticar o acesso aos servidores.
- O MSM (MegaRAID Storage Manager) pode ser instalado das seguintes maneiras:
  - Completa: Todos os componentes são instalados.
  - Cliente: Somente os componentes necessários para visualizar e configurar remotamente os servidores são instalados. As portas 3071 e 5571 precisam estar abertas.
  - Servidor: Somente os componentes necessários para o gerenciamento remoto do servidor são instalados.

    Além de um endereço unicast, o servidor MSM usa o endereço IP multicast 229.111.112.12, bem como as portas TCP/UDP 3071 e 5571.

    Para o SNMP, as portas 161 e 162 precisam estar abertas. Se o LDAP estiver configurado, a porta 389 precisará estar aberta.
  - Independente: Somente os componentes necessários para o gerenciamento local do servidor são instalados.
  - Local: Somente os componentes necessários para a configuração local do servidor são instalados.

Segurança do Diagnostic Services

O Diagnostic Services é um aplicativo daemon de serviços que atua como listener de eventos acionadores associados ao WarpDrive emitidos pelo driver. O Diagnostic Services coleta informações de diagnóstico do WarpDrive quando ocorre um evento relatado ou quando solicitado pelo usuário.

Estas são as considerações de segurança para os módulos do Diagnostic Services em um Sun Flash Accelerator F40 PCIe Card:

- O daemon Diagnostic Services usa a API da biblioteca storelib para configurar eventos acionadores relevantes e obter uma notificação de evento.
- As informações de eventos e log do Diagnostic Services são obtidas exclusivamente por meio da API da biblioteca storelib e salvas em arquivos de log.
- O Diagnostic Services usa a porta UDP 162.
- Um exemplo de arquivo de script de eventos do usuário é instalado, por padrão, mas não é usado, a menos que seja configurado para fins de depuração.
- Os arquivos de configuração e de log do Diagnostic Services são somente leitura para todos os usuários e têm permissão de gravação para o usuário root. Os arquivos binários são somente leitura para todos os usuários, mas têm permissão de gravação e execução para o usuário root.

- Se configurado, o Diagnostic Services poderá enviar mensagens de trap do SNMP quando ocorrerem eventos. Um pipe é usado internamente para fins de monitoramento.

Segurança do Linux Diagnostic Driver

O Linux Diagnostic Driver é o driver de 6 Gb MPT2SAS SAS2 capaz de gerar automaticamente um buffer de rastreamento do host (2MB) durante a inicialização, implementar acionadores de serviços de diagnóstico e oferecer suporte a várias funções usando o aplicativo de interface de gerenciamento. Com base nos atributos do acionador, o driver monitora os erros e adiciona um novo evento de serviço de diagnóstico para referência futura.

Estas são as considerações de segurança para o Linux Diagnostic Driver em um Sun Flash Accelerator F40 PCIe Card:

- O Linux Diagnostic Driver é executado no espaço do kernel. Se o SO estiver virtualizado, o driver será executado no pai.
- O Linux Diagnostic Driver captura o buffer de rastreamento a partir do firmware quando ocorre um conjunto de eventos acionadores. Esses eventos acionadores são especificados pelo administrador do sistema e alimentados no driver por meio da interface Sysfs no kernel.
- Somente um usuário root com permissão poderá gravar nos arquivos de atributos Sysfs do Linux Diagnostic Driver.
- Os produtos da geração Linux Diagnostic Driver SAS2 oferecem suporte à Proteção de dados ponta a ponta (EEDP).
- O Linux Diagnostic Driver encontra-se entre o hardware, o firmware e a camada intermediária do sistema operacional. O Linux Diagnostic Driver usa os protocolos SAS2 e SATA, consolidados no setor, e baseia-se na tecnologia de transmissão de mensagens LSI e em chamadas do SO para tratar o fluxo de dados de armazenamento.
- O Linux Diagnostic Driver tem código-fonte aberto, e esse código é monitorado pela comunidade do kernel Linux.
- O Linux Diagnostic Driver tem acesso completo a todo o hardware gerenciado por ele, bem como a todas as estruturas do kernel necessárias para o seu funcionamento. O Linux Diagnostic Driver tem acesso completo a todas as interfaces do kernel usadas para gerenciar entradas/saídas SCSI.

Segurança do SNMP

O agente SNMP permite o gerenciamento e o monitoramento dos controladores LSI SAS por meio do protocolo SNMP (Simple Network Management Protocol). A família de controladores suportada pelo SNMP compreende LSI MR, IR, IR2 e WarpDrive. Você pode usar um browser MIB ou criar o seu próprio browser para monitorar e configurar a topologia exposta pelo agente LSI SNMP.

Estas são as considerações de segurança para os módulos SNMP em um Sun Flash Accelerator F40 PCIe Card:

- O subagente SNMP usa o Simple Network Management Protocol para fornecer informações do sistema de monitoramento a um cliente SNMP.
- O cliente SNMP poderá ser qualquer Browser MIB que ofereça suporte a SNMPv1.
- O subagente SNMP MR/IR recupera informações das bibliotecas storelib usando a API storelib. A storelib envia IOCTLs (input-output control) para o driver a fim de obter essas informações.
- Os arquivos de log SNMP têm permissão de gravação, os arquivos binários têm permissão de execução e os demais arquivos são somente leitura.
- A autenticação por meio de um mecanismo suportado pelo Net-SNMP é necessária para qualquer acesso SNMP.

Segurança do Firmware do Controlador WarpDrive

O firmware do Controlador WarpDrive é executado na sua placa controladora. Ele oferece uma taxa de transferência de 6 Gbps ou de 3 Gbps legada às unidades de estado sólido SATA (DFFs) conectadas à placa controladora do WarpDrive. A conectividade do host com o controlador WarpDrive é suportada por meio de uma conexão PCIe 2.0.

Estas são as considerações de segurança para o firmware do Controlador WarpDrive em um Sun Flash Accelerator F40 PCIe Card:

- O firmware do Controlador WarpDrive é executado no processador localizado na placa controladora.
- Os drivers do SO do WarpDrive estão acima do firmware do controlador e se comunicam por meio de PCIe usando a MPI (message passing interface).
- O firmware do Controlador Warp Drive interage com os módulos da unidade SSD abaixo dele usando a interface SAS/SATA.
- Somente as imagens do firmware do Controlador Warp Drive com a assinatura e a soma de verificação corretas podem ser carregadas na placa.

Segurança do SSDFW

O módulo de firmware SSDFW fornece o firmware para a família SF-2500 Flash Storage Processor.

Estas são as considerações de segurança para os módulos SSDFW em um Sun Flash Accelerator F40 PCIe Card:

- O módulo de firmware SSDFW se conecta a uma interface Flash NAND em uma extremidade e à interface SATA AHCI na outra.
- A comunicação no host é estabelecida por meio da interface SATA, definida nas especificações Serial ATA e ATA Command Set (ACS-2).
- O módulo de firmware SSDFW tem a permissão de administrador por padrão.
- Os arquivos de log são criptografados. O registro em log é suportado por meio de uma porta serial.
- O módulo SSDFW é um firmware incorporado que reside no ASIC do SF-2500 Flash Storage Processor.
- O módulo de firmware SSDFW armazena os dados do sistema (como o estado de uma unidade) e os dados do usuário e coloca-os na mídia NAND não volátil. Todos os dados do sistema são criptografados com uma chave exclusiva da unidade.
- As senhas do sistema e do usuário são usadas para obter privilégios.
- O firmware SSDFW é incorporado no subsistema LSI-ASD.
- O AES-128 ou o AES-256 é usado para criptografar dados (texto simples). Um mecanismo SHA autentica o firmware. As chaves e os valores de contadores são criptografados antes de serem armazenados na memória flash.

Segurança do DDCLI

O DDCLI é um aplicativo voltado ao usuário. O DDCLI é uma CLI independente que permite monitorar qualquer WarpDrive conectado ao sistema. Informações importantes sobre diversos componentes do WarpDrive podem ser recuperadas com o utilitário **ddcli**.

Estas são as considerações de segurança para o aplicativo DDCLI em um Sun Flash Accelerator F40 PCIe Card:

- O DDCLI é fornecido inicialmente sem permissão executável. O usuário root precisará adicionar essa permissão.
- Será necessário alterar as permissões do arquivo ddcli para que ele possa ser executado. Para minimizar os problemas de segurança, defina as permissões como 0744. O arquivo deve pertencer ao usuário root. Isso permitirá que todos vejam o arquivo, mas somente os usuários root poderão executá-lo.
- Uma biblioteca que oferece suporte a APIs MPT (message processing technology) é vinculada estaticamente ao DDCLI. Essa biblioteca envia um IOCTL ao driver para obter as informações necessárias.
- O aplicativo DDCLI é um arquivo binário com permissão executável.