Carte PCIe Sun Flash Accelerator F40

Guide de sécurité

Référence: E39695-02
Octobre 2013

Table des matières

• • • Chapitre 1

Sécurité de la carte PCIe Sun Flash Accelerator F40

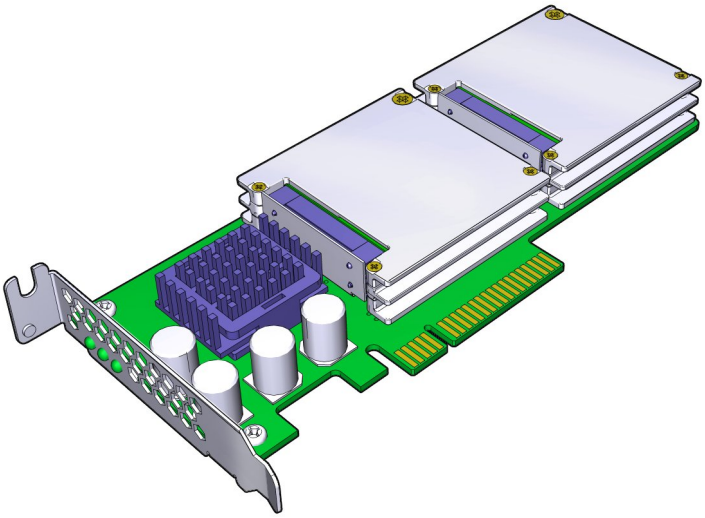
Ce document livre des recommandations de sécurité générales visant à vous aider à protéger vos produits matériels Oracle x86 tels que la carte PCIe Sun Flash Accelerator F40.

Les sections suivantes sont incluses :

Description de la carte PCIe Sun Flash Accelerator F40

Les sections suivantes sont incluses :

La carte PCIe Sun Flash Accelerator F40 est une carte de stockage de mémoire flash clé en main, de facteur de forme profil bas, HBA PCI-E 2.0. L'image suivante présente cette carte :



Pour des informations détaillées sur le produit, reportez-vous au *Guide de l'utilisateur de la carte PCIe Sun Flash Accelerator F40*.

Composants matériels

La carte PCIe Sun Flash Accelerator F40 contient les composants matériels suivants :

- Quatre modules flash SSD : 400 Go de mémoire flash NAND eMLC 32 nm au total, directement montée sur la carte.
- PCI-E du contrôleur de protocole SAS : l'interface SATA de la carte PCIe Sun Flash Accelerator F40 vers le contrôleur de protocole comporte une interface hôte PCI-E 2.0 8x connectée à un contrôleur de protocole SAS/SATA 2 x4 6 Gb/s LSI 2008.
- Composants de stockage d'énergie : videz les écritures non achevées dans la mémoire flash en cas d'échec de l'alimentation du système ou de l'emplacement PCIe.

Pour plus d'informations, reportez-vous au *Guide de l'utilisateur de la carte PCIe Sun Flash Accelerator F40*.

Composants logiciels et microprogrammes

La carte PCIe Sun Flash Accelerator F40 contient les modules suivants :

Composant	Voir
MegaRAID Storage Manager (MSM)	"Sécurité de l'application MSM" à la page 7
Diagnostic Services	"Sécurité de Diagnostic Services" à la page 8
Linux Diagnostic Driver	"Sécurité de Linux Diagnostic Driver" à la page 9
SNMP	"Sécurité SNMP" à la page 9
WarpDrive Controller FW	"Sécurité de Warp Drive Controller Firmware" à la page 10
SSDFW	"Sécurité de SSDFW" à la page 10
DDCLI	"Sécurité de DDCLI" à la page 11

Pour plus d'informations, reportez-vous au *Guide de l'utilisateur de la carte PCIe Sun Flash Accelerator F40*.

Principes de sécurité

Il existe quatre principes de sécurité élémentaires : l'accès, l'authentification, l'autorisation et la comptabilisation.

- **Accès**

  Les contrôles physiques et logiciels protègent votre matériel ou vos données contre les intrusions.
  - Pour le matériel, les limites d'accès correspondent généralement à des limites d'accès *physiques*.
  - Pour les logiciels, l'accès est limité à l'aide de moyens physiques et virtuels.
  - Seul le processus de mise à jour Oracle permet de modifier les microprogrammes.
- **Authentification**

  Configurez des fonctions d'authentification, comme un système de mots de passe dans les systèmes d'exploitation de votre plate-forme, afin d'éviter toute usurpation d'identité.

  Veillez à ce que les employés utilisent correctement leur badge pour pénétrer dans la salle informatique.
- **Autorisation**

  Autorisez uniquement les employés à utiliser le matériel et les logiciels pour lesquels ils ont été formés et certifiés. Mettez en place un système d'autorisations en lecture, écriture et exécution pour contrôler l'accès des utilisateurs aux commandes, à l'espace disque, aux périphériques et aux applications.
- **Comptabilisation**

  Tirez parti des fonctions logicielles et matérielles Oracle pour surveiller les connexions et tenir à jour les inventaires de matériel.
  - Surveillez les connexions des utilisateurs par le biais de journaux système. Surveillez étroitement les comptes d'administrateur système et de maintenance, lesquels ont accès à des commandes puissantes.
  - Assurez le suivi des ressources système à l'aide des numéros de série. Les numéros de référence Oracle sont enregistrés au format électronique sur tous les modules, cartes et cartes mère.

Planification d'un environnement sécurisé

Prenez en compte les remarques suivantes avant et pendant l'installation et la configuration d'un serveur et de la carte PCIe Sun Flash Accelerator F40.

Les sections suivantes sont incluses :

- “Sécurité du matériel ” à la page 7
- “Sécurité des logiciels ” à la page 8
- “Sécurité des microprogrammes” à la page 8
- “Microprogramme Oracle ILOM” à la page 8
- “Journaux système” à la page 9

Sécurité du matériel

Le matériel physique peut être sécurisé de manière relativement simple : limitez l'accès au matériel et enregistrez les numéros de série.

- **Limiter l'accès**
  - Si le matériel est installé dans un rack dont la porte est équipée d'un verrou, maintenez-la verrouillée et ne l'ouvrez que pour effectuer la maintenance des composants du rack.
  - Installez les unités remplaçables sur site (FRU) ou les unités remplaçables par l'utilisateur (CRU) de remplacement dans une armoire verrouillée. Limitez l'accès à l'armoire verrouillée au personnel autorisé.
- **Enregistrer les numéros de série**
  - Apposez une marque de sécurité sur toutes les cartes PCIe Sun Flash Accelerator F40. Utilisez des stylos à ultraviolet ou des étiquettes en relief.
  - Enregistrez les numéros de série de toutes les cartes PCIe Sun Flash Accelerator F40.
  - Conservez les clés d'activation et les licences matérielles dans un emplacement sécurisé auquel l'administrateur système peut facilement accéder en cas d'urgence. Les documents imprimés peuvent être votre seule preuve de propriété.

Sécurité des logiciels

Prenez les mesures de sécurité suivantes pour les composants logiciels :

- Reportez-vous à la documentation fournie avec votre logiciel pour activer les fonctionnalités de sécurité disponibles pour celui-ci.
- Configurez et mettez à jour les pilotes de la carte PCIe Sun Flash Accelerator F40 à l'aide du compte superutilisateur.
- La sécurité du matériel passe en grande partie par des logiciels.
- Les composants logiciels prenant en charge la carte PCIe Sun Flash Accelerator F40 s'appuient sur des fonctions de sécurité système pour sécuriser l'accès.

Sécurité des microprogrammes

A la livraison, tous les microprogrammes sont préinstallés sur la carte PCIe Sun Flash Accelerator F40. Aucune installation de microprogramme n'est requise sur le terrain, à l'exception des mises à jour.

- Si des mises à jour des microprogrammes sont requises, contactez le support Oracle pour obtenir de l'aide ou recherchez les dernières mises à jour et procédures du produit sur le site de support Oracle.

  https://support.oracle.com
- Configurez et mettez à jour l'utilitaire de gestion des microprogrammes de la carte PCIe Sun Flash Accelerator F40 à l'aide du compte superutilisateur. Les comptes des utilisateurs ordinaires permettent à ces derniers d'afficher les microprogrammes, mais pas de les modifier. Le processus de mise à jour des microprogrammes du système d'exploitation Oracle Solaris empêche les modifications non autorisées des microprogrammes.
- Reportez-vous aux notes de produit fournies avec votre carte PCIe Sun Flash Accelerator F40 pour des informations de dernière minute, pour connaître les besoins de mise à jour des microprogrammes et pour toute autre information relative à la sécurité.
- Pour plus d'informations sur la configuration des variables de sécurité SPARC OpenBootPROM (OBP), reportez-vous au *OpenBoot 4.x Command Reference Manual*.

Microprogramme Oracle ILOM

Vous pouvez sécuriser, gérer et surveiller de manière active les composants du système à l'aide du microprogramme de gestion Oracle Integrated Lights Out Manager (ILOM) préinstallé sur certains serveurs x86. Pour en savoir plus sur l'utilisation de ce microprogramme lors de la configuration des

mots de passe, de la gestion des utilisateurs et de l'application des fonctions de sécurité, y compris l'authentification SSH (Secure Shell), SSL (Secure Socket Layer) et RADIUS, reportez-vous à la documentation d'Oracle ILOM :

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

Journaux système

- Activez la journalisation et envoyez les journaux à un hôte de journal sécurisé dédié.
- Configurez la journalisation pour inclure des informations horaires exactes, à l'aide du protocole NTP et d'horodatages.

Gestion d'un environnement sécurisé

Après l'installation et la configuration initiales de la carte PCIe Sun Flash Accelerator F40, servez-vous des fonctions de sécurité matérielles et logicielles Oracle pour continuer à contrôler le matériel et assurer le suivi des ressources système.

Les sections suivantes sont incluses :

Suivi des ressources

Assurez le suivi de l'inventaire à l'aide des numéros de série. Les numéros de série Oracle sont incorporés dans le microprogramme des cartes d'option et des cartes mères système. Ces numéros de série peuvent être lus par le biais de connexions au réseau local.

Vous pouvez également utiliser des lecteurs d'identification par radiofréquence (RFID) pour simplifier davantage le suivi des ressources. Reportez-vous au livre blanc d'Oracle intitulé *How to Track Your Oracle Sun System Assets by Using RFID*.

Mises à jour des microprogrammes

Maintenez à jour les versions des microprogrammes de votre équipement.

- Vérifiez régulièrement la présence de mises à jour.
- Sur la plupart des systèmes d'exploitation, et en particulier sur le système d'exploitation Oracle Solaris,la gestion des cartes et la mise à niveau des pilotes ou des microprogrammes ne peut être effectuée que par un utilisateur connecté à l'aide d'informations d'identification root.
- Installez toujours la dernière version officielle des microprogrammes.

Mises à jour des logiciels

Maintenez à jour les versions des logiciels de votre équipement.

- Les mises à jour des logiciels des pilotes Oracle Solaris sont disponibles par le biais de patches et de mises à jour Oracle Solaris.

- Les mises à jour des logiciels des pilotes pour d'autres systèmes d'exploitation peuvent être disponibles à l'adresse http://www.lsi.com.
- Reportez-vous aux notes de produit fournies avec votre carte PCIe Sun Flash Accelerator F40 pour des informations de dernière minute, pour connaître les besoins de mise à jour des logiciels et pour toute autre information relative à la sécurité.
- Installez toujours la dernière version officielle d'un logiciel.
- Le cas échéant, installez les patches de sécurité nécessaires pour votre logiciel.
- Les périphériques contiennent également des microprogrammes et peuvent nécessiter des mises à jour de microprogrammes.

Sécurité des journaux

Contrôlez et assurez à intervalles réguliers la maintenance des fichiers journaux.

- Consultez les journaux afin de rechercher d'éventuels incidents et archivez-les conformément à la stratégie de sécurité.
- Archivez régulièrement les fichiers journaux lorsque leur taille devient excessive. Conservez des copies des fichiers archivés pour pouvoir vous y reporter à l'avenir ou en vue d'une analyse statistique.

Sécurité des modules

Les modules logiciels et de microprogrammes sont les suivants :

- “Sécurité de l'application MSM” à la page 10
- “Sécurité de Diagnostic Services” à la page 11
- “Sécurité de Linux Diagnostic Driver” à la page 12
- “Sécurité SNMP” à la page 12
- “Sécurité de SSDFW” à la page 13
- “Sécurité de DDCLI” à la page 14

Remarque

Le terme WarpDrive dans le texte fait référence à la carte carte PCIe Sun Flash Accelerator F40.

Sécurité de l'application MSM

MegaRAID Storage Manager (MSM) est une application logicielle offrant une interface graphique permettant de configurer et d'interagir avec le microprogramme WarpDrive par le biais du pilote. En outre, MSM surveille et gère les configurations de stockage sur les contrôleurs LSI® MegaRAID, SAS et WarpDrive.

Les considérations relatives à la sécurité concernant les modules MSM dans la carte PCIe Sun Flash Accelerator F40 sont les suivantes :

- Compatibilité MegaRAID Storage Manager : Linux 64 bits, Solaris X86.
- Reportez-vous au guide de l'utilisateur fournit par LSI, à l'aide en ligne intégrée à MSM et au fichier README fourni avec le programme d'installation. Accédez au site http://www.lsi.com.

- Les utilisateurs doivent s'authentifier pour pouvoir accéder aux modules.
  - Si un utilisateur s'authentifie en tant que root, il est autorisé à accéder à l'ensemble du matériel.
  - Si un utilisateur s'authentifie en tant qu'utilisateur, il ne dispose que d'une autorisation d'affichage.
- Normalement, les fichiers journaux disposent d'une autorisation d'écriture, les fichiers binaires d'une autorisation d'exécution et les autres fichiers sont en lecture seule.
- Un seul utilisateur à la fois peut disposer du privilège d'administration. Les autres utilisateurs disposent du privilège d'affichage seul. Un ID de session est généré au moment de l'authentification client-serveur grâce à un générateur de numéros aléatoires Java intégré.
- Le client et le serveur sont implémentés dans Java. Le client et le serveur utilisent TCP/IP pour communiquer entre eux. Le serveur communique avec la bibliothèque à l'aide de JNI.
- MSM interagit avec Internet mais ne prend pas en charge IPv6.
- MSM utilise SSL pour la communication entre le client et le serveur.
- Les paramètres de pare-feu de votre système dépendent du type d'installation effectué.
  - Dans tous les types d'installation à l'exception des installations locales, vous devez configurer le pare-feu de manière à ce qu'il contrôle l'accès au client et au serveur MSM.
  - Une installation locale utilise l'IP localhost.
- Un accès en tant qu'utilisateur root est nécessaire pour la configuration/modification des paramètres. Pour limiter l'accès des personnes potentiellement malveillantes, suivez ces recommandations.
  - Choisissez un mot de passe sûr.
  - Utilisez des mots de passe différents pour tous les systèmes qui exécutent des composants MSM, qu'ils soient client ou serveur.
- De manière optionnelle, une authentification LDAP peut être mise en place pour l'accès aux serveurs.
- Pour l'installation de MegaRAID Storage Manager (MSM), vous disposez des types d'installation suivants :
  - Complete : tous les composants sont installés.
  - Client : seuls les composants requis pour afficher et configurer à distance des serveurs sont installés. Les ports 3071 et 5571 doivent être ouverts.
  - Server : seuls les composants requis pour la gestion des serveurs à distance sont installés.

    En plus d'une adresse monodiffusion, le serveur MSM utilise également l'adresse IP de multidiffusion 229.111.112.12 et les ports TCP/UDP 3071 et 5571.

    Pour SNMP, les ports 161 et 162 doivent être ouverts. Si LDAP est configuré, le port 389 doit être ouvert.
  - StandAlone : seuls les composants requis pour la gestion du serveur local sont installés.
  - Local : seuls les composants requis pour la configuration du serveur local sont installés.

Sécurité de Diagnostic Services

Diagnostic Services est une application de démon de service qui écoute les événements déclencheurs associés à WarpDrive générés par le pilote. Diagnostic Services collecte des informations de diagnostic à partir de WarpDrive lorsqu'un événement signalé se produit ou à la demande d'un utilisateur.

Les considérations relatives à la sécurité concernant les modules Diagnostic Services d'une carte PCIe Sun Flash Accelerator F40 sont les suivantes :

- Le démon Diagnostic Services utilise l'API de la bibliothèque storelib pour configurer les événements déclencheurs présentant un intérêt et pour obtenir une notification d'événement.

- Les informations relatives aux événements et aux journaux Diagnostic Services peuvent uniquement être obtenues par le biais de l'API de la bibliothèque storelib et sont enregistrées dans des fichiers journaux.
- Diagnostic Services utilise le port UDP 162.
- Un exemple de fichier de script d'événement utilisateur est installé par défaut, mais n'est pas utilisé, sauf s'il est configuré à des fins de débogage.
- Les fichiers de configuration et les fichiers journaux de Diagnostic Services sont en lecture seule pour tout le monde et disposent d'une autorisation d'écriture pour l'utilisateur root. Les fichiers binaires sont en lecture seule pour tout le monde mais disposent d'une autorisation d'écriture et d'exécution pour l'utilisateur root.
- S'il est configuré, le service Diagnostic Services peut envoyer des messages de déroutement SNMP lorsque des événements se produisent. Un tube est utilisé en interne pour la surveillance.

Sécurité de Linux Diagnostic Driver

Linux Diagnostic Driver est le pilote MPT2SAS SAS2 6 Go qui peut automatiquement poster un tampon de suivi de l'hôte (2 Mo) au démarrage, implémenter des déclenchements de service de diagnostic et prendre en charge plusieurs fonctions à l'aide de l'application d'interface de gestion. Sur la base des attributs de déclenchement, le pilote surveille les erreurs et ajoute un nouvel événement de service de diagnostic pour référence future.

Les considérations relatives à la sécurité concernant Linux Diagnostic Driver dans une carte PCIe Sun Flash Accelerator F40 sont les suivantes :

- Le pilote Linux Diagnostic Driver s'exécute dans l'espace noyau. Si le système d'exploitation est virtualisé, le pilote s'exécute dans le parent.
- Le pilote Linux Diagnostic Driver capture le tampon de suivi à partir du microprogramme lorsqu'un ensemble d'événements déclencheurs se produit. Les événements déclencheurs concernés sont spécifiés par l'administrateur système et sont amenés au pilote par le biais de l'interface Sysfs dans le noyau.
- Seul un utilisateur root autorisé peut écrire dans les fichiers d'attribut Sysfs du pilote Linux Diagnostic Driver.
- Les produits de génération SAS2 de Linux Diagnostic Driver prennent en charge l'EEDP (End-to-end data protection).
- Le pilote Linux Diagnostic Driver se situe entre le matériel, les logiciels et la couche intermédiaire du système d'exploitation. Linux Diagnostic Driver utilise à l'extrémité inférieure des protocoles SAS2 et SATA et une technologie de transmission de messages LSI établis dans le secteur, et le SE sollicite l'extrémité supérieure pour gérer le flux de données de stockage.
- La source de Linux Diagnostic Driver est Open Source et approuvée par la communauté Linux.
- Le pilote Linux Diagnostic Driver dispose d'un accès complet à tous les matériels qu'il gère, ainsi que d'un accès à toutes les structures de noyau nécessaires à son fonctionnement. Linux Diagnostic Driver dispose d'un accès complet à toutes les interfaces de noyau utilisées pour la gestion des E/S SCSI.

Sécurité SNMP

L'agent SNMP permet de gérer et de surveiller les contrôleurs SAS LSI à l'aide du protocole SNMP (Simple Network Management Protocol). La famille de contrôleurs prise en charge par SNMP est LSI MR, IR, IR2 et WarpDrive. Vous pouvez utiliser un navigateur MIB ou créer un navigateur personnalisé pour surveiller et configurer la topologie exposée par l'agent LSI SNMP.

Les considérations relatives à la sécurité concernant les modules SNMP dans une carte PCIe Sun Flash Accelerator F40 sont les suivantes :

- Le sous-agent SNMP fournit des informations sur le système de surveillance à un client SNMP à l'aide du protocole SNMP.
- Tout navigateur MIB prenant en charge SNMPv1 peut être un client SNMP.
- Le sous-agent SNMP MR/IR extrait des informations des bibliothèques storelib à l'aide de l'API storelib. Storelib émet des appels IOCTL (contrôle des entrées/sorties) vers le pilote pour obtenir ces informations.
- Les fichiers journaux SNMP disposent d'une autorisation d'écriture, les fichiers binaires d'une autorisation d'exécution et les autres fichiers sont en lecture seule.
- Une authentification à l'aide d'un mécanisme d'authentification pris en charge par Net-SNMP est nécessaire pour accéder à SNMP.

Sécurité de WarpDrive Controller Firmware

Le microprogramme WarpDrive Controller s'exécute sur la carte de contrôleur WarpDrive. Il offre un taux de transfert de 6 Gb/s ou de 3 Mb/s hérité aux disques durs électroniques (SSD) SATA connectés à la carte du contrôleur WarpDrive. La connexion de l'hôte au contrôleur WarpDrive est assurée par une connexion PCIe 2.0.

Les considérations relatives à la sécurité concernant le microprogramme WarpDrive Controller dans une carte PCIe Sun Flash Accelerator F40 sont les suivantes :

- Le microprogramme WarpDrive Controller s'exécute sur le processeur situé sur la carte de contrôleur.
- Les pilotes de système d'exploitation WarpDrive sont au-dessus du microprogramme Warp Drive Controller et communiquent via PCIe, à l'aide de l'interface MPI (message passing interface).
- Le microprogramme Warp Drive Controller interagit avec les modules de disques SSD qui lui sont subordonnés par le biais de l'interface SAS/SATA.
- Seules les images du microprogramme Warp Drive Controller présentant la signature et la somme de contrôle correctes peuvent être téléchargées vers la carte.

Sécurité de SSDFW

Le module de microprogramme SSDFW fournit des microprogramme pour la famille de processeurs Flash Storage Processor SF-2500.

Les considérations relatives à la sécurité concernant les modules SSDFW dans une carte PCIe Sun Flash Accelerator F40 sont les suivantes :

- Le module de microprogramme SSDFW se connecte à l'interface flash NAND d'un côté et à l'interface SATA AHCI de l'autre côté.
- La communication côté hôte se connecte via l'interface SATA, définie dans les spécifications Serial ATA et ATA Command Set (ACS-2).
- L'autorisation admin du module de microprogramme SSDFW est activée par défaut.
- Les fichiers journaux sont chiffrés. La journalisation est prise en charge via le port série.
- Le module SSDFW est un microprogramme intégré qui se trouve dans l'ASIC de Flash Storage Processor SF-2500.
- Le module de microprogramme SSDFW stocke des données système (comme l'état d'une unité) et des données utilisateur et les place sur un média NAND non volatile. Toutes les données système sont chiffrées à l'aide d'une clé propre à chaque unité.

- Des mots de passe système et utilisateur sont utilisés pour l'octroi de privilèges.
- Le microprogramme SSDFW est intégré au sous-système LSI-ASD.
- Le chiffrement des données s'effectue à l'aide d'AES-128 ou d'AES-256 (texte brut). Un moteur SHA authentifie le microprogramme. Les clés et les valeurs des compteurs sont chiffrées avant leur stockage dans la mémoire flash.

Sécurité de DDCLI

DDCLI est une application utilisateur. DDCLI est une interface de ligne de commande autonome qui vous permet de surveiller tout WarpDrive connecté au système. L'utilitaire **ddcli** permet d'extraire des informations importantes relatives à différents composants de WarpDrive.

Les considérations relatives à la sécurité concernant l'application DDCLI dans une carte PCIe Sun Flash Accelerator F40 sont les suivantes :

- DDCLI est initialement fourni sans autorisation exécutable. L'utilisateur root doit ajouter cette autorisation.
- Vous devez modifier les autorisations du fichier ddcli pour permettre son exécution. Pour réduire les problèmes de sécurité, définissez les autorisations sur 0744. Root doit être propriétaire de ce fichier. De cette manière, le fichier peut être affiché par tous les utilisateurs, mais il peut uniquement être exécuté par des utilisateurs root.
- Une bibliothèque prenant en charge les API MPT (message processing technology) est liée de manière statique à DDCLI. Cette bibliothèque envoie un appel IOCTL (contrôle des entrées/sorties) pour obtenir les informations requises.
- L'application DDCLI est un fichier binaire doté d'une autorisation exécutable.