Guide de sécurité du HBA Oracle® Storage 12 Gb/s SAS PCIe RAID HBA, interne

Pour les modèles de HBA 7110116 et 7110117

Référence: E59791-01
Décembre 2014

Table des matières

Guide de sécurité du HBA Oracle Storage 12 Gb/s SAS PCIe RAID HBA, interne

Ce document contient des instructions et des principes généraux de sécurité à prendre en considération lors de l'utilisation du HBA Oracle Storage 12 Gb/s SAS PCIe RAID HBA, interne.

Cette documentation n'aborde *pas* les thèmes relatifs à la sécurité suivants :

- Aspects de la sécurité spécifique du microprogramme d'une plate-forme liés au BIOS, à Open Boot Prom (OBP) et à l'hyperviseur
- Problèmes liés à la sécurité du système d'exploitation
- Sécurité physique du système matériel
- Sécurité réseau de l'infrastructure de mise en réseau externe
- Informations relatives au module de plate-forme sécurisée

Pour plus d'informations sur ces aspects de la sécurité, reportez-vous à la documentation relative à la sécurité du produit concerné.

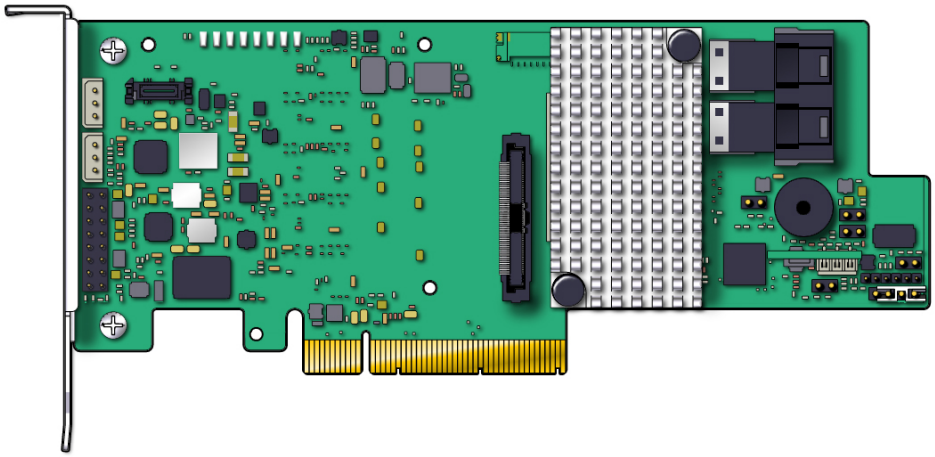
Ce document traite des sujets suivants :

Présentation du HBA

Le HBA Oracle Storage 12 Gb/s SAS PCIe RAID HBA, interne (numéros de référence marketing 7110116 et 7110117) est un contrôleur RAID PCIe 3.0 profil bas qui prend en charge huit ports SAS/SATA 12 Gbit/s internes via deux connecteurs mini-SAS HD SFF-8643 x4 internes.

Remarque - SATA II est le seul type de SATA pris en charge par ce HBA.

L'image suivante montre le HBA Oracle Storage 12 Gb/s SAS PCIe RAID HBA, interne:



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.
  - Les microprogrammes peuvent uniquement être modifiés par le processus de mise à jour Oracle.
- **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 mères.

Planification d'un environnement sécurisé

Consultez les informations de cette section avant et pendant l'installation et la configuration d'un serveur et du HBA Oracle Storage 12 Gb/s SAS PCIe RAID HBA, interne.

Cette section s'articule autour des rubriques suivantes :

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**

  Enregistrez les numéros de série de l'ensemble de vos cartes HBA.

Sécurité des logiciels

Prenez les mesures de sécurité suivantes pour les composants logiciels :

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

Sécurité des microprogrammes

A la livraison, tous les microprogrammes sont préinstallés sur le HBA. Aucune installation de microprogramme n'est requise sur le terrain, à l'exception des mises à jour.

- Si des mises à jour du microprogramme sont nécessaires, téléchargez-les dans la rubrique de support Oracle du site Web de LSI à l'adresse suivante : http://www.lsi.com/sep/Pages/oracle/index.aspx

  Vous pouvez également contacter le support Oracle pour obtenir de l'aide ou rechercher 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 du HBA 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 au guide d'installation du HBA, disponible sur le site Web d'Oracle, 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 manuel *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.

Maintien d'un environnement sécurisé

Après l'installation et la configuration initiales du HBA, 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 :

Asset Tracking

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 peuvent être effectuées 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 pilotes pour d'autres systèmes d'exploitation peuvent être disponibles à l'adresse suivante : http://www.lsi.com/sep/Pages/oracle/index.aspx
- Reportez-vous à la documentation du HBA, disponible sur le site Web d'Oracle, 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 patchs 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.
- Retirez régulièrement les fichiers journaux lorsque leur taille devient excessive. Conservez des copies des fichiers retirés pour pouvoir vous y reporter à l'avenir ou en vue d'une analyse statistique.

Sécurité des modules

Le HBA est géré par le biais de l'interface de ligne de commande (CLI) LSI StorCLI ou l'interface graphique (GUI) MegaRAID SAS. Ces logiciels vous permettent de faire les choses suivantes :

- Surveiller le fonctionnement du HBA.

- Mise à jour du microprogramme du HBA.

La CLI StorCLI et la GUI MegaRAID SAS sont uniquement accessibles aux utilisateurs qui disposent d'informations d'identification `root`. Par conséquent, les utilisateurs sans privilèges ne peuvent pas apporter de modifications à l'environnement SAN par le biais de ces utilitaires.

Pour plus d'informations sur la CLI StorCLI et la GUI MegaRAID SAS, reportez-vous à la documentation de LSI sur le site Web suivant : http://www.lsi.com/sep/Pages/oracle/index.aspx