Oracle® Storage 12 Gb/s SAS PCIe RAID 内蔵 HBA セキュリティーガイド

(HBA モデル 7110116 および 7110117 対応)

Part No: E59788
2014 年 12 月

目次

Oracle Storage 12 Gb/s SAS PCIe RAID 内蔵 HBA セキュリティー

このドキュメントでは、Oracle Storage 12 Gb/s SAS PCIe RAID 内蔵 HBA を使用するときに考慮するセキュリティーの原則とガイドラインについて説明します。

このドキュメントには、次のセキュリティー情報は記載されて*いません*。

- BIOS、Open Boot Prom (OBP)、および Hypervisor など、個々のプラットフォームファームウェアのセキュリティー
- オペレーティングシステムのセキュリティーに関する注意事項
- ハードウェアシステムの物理的なセキュリティー
- 外部ネットワーク基盤のネットワークセキュリティー
- Trusted Platform Module の情報

これらのセキュリティー領域に関する情報については、個々の製品に付属のセキュリティードキュメントを参照してください。

このドキュメントには、次のトピックが含まれています。

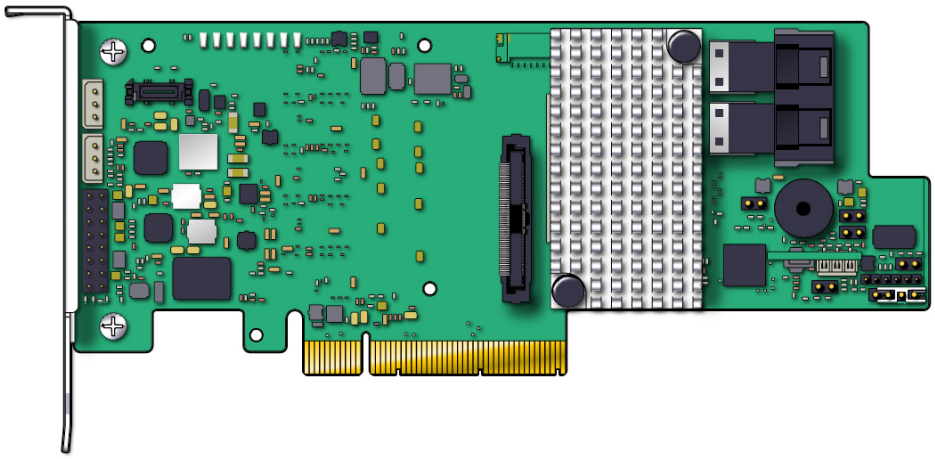
HBA の概要

Oracle Storage 12 Gb/s SAS PCIe RAID 内蔵 HBA (マーケティングパーツ番号 7110116 および 7110117) は、2 つの SFF-8643 x4 内部 Mini SAS HD コネクタを通じ

て 8 つの内部 12G ビット SAS/SATA ポートをサポートする PCIe 3.0 で薄型の RAID コントローラです。

注記 - この HBA でサポートされる SATA の種類は SATA II だけです。

次の図は、Oracle Storage 12 Gb/s SAS PCIe RAID 内蔵 HBA を示しています。



セキュリティーの原則

基本的なセキュリティーの原則として、アクセス、認証、承認、およびアカウンティングの 4 つがあります。

- **アクセス**

  物理的な制御とソフトウェアの制御によって、ハードウェアやデータを侵入から保護します。

  - ハードウェアの場合、アクセス制限とは、通常は*物理的な*アクセス制限を意味します。
  - ソフトウェアの場合、物理的な手段と仮想的な手段の両方でアクセスが制限されます。
  - ファームウェアは、Oracle の更新プロセス以外では変更できません。

- **認証**

  ユーザーが本人であることを保証するには、プラットフォームのオペレーティングシステムにパスワードシステムなどの認証機能を設定します。

担当者がコンピュータ室に入室する際に、従業員バッジを適切に付けていることを確認してください。

- **承認**

  トレーニングを受けて使用を認定されたハードウェアとソフトウェアの操作のみを担当者に許可します。読み取り/書き込み/実行のアクセス権を設定して、コマンド、ディスク領域、デバイス、およびアプリケーションへのユーザーアクセスを制御します。

- **アカウンティング**

  Oracle のソフトウェアおよびハードウェア機能を使用して、ログイン操作を監視したりハードウェアインベントリを管理したりします。

  - ユーザーログインをモニターするには、システムログを使用します。特にシステム管理者アカウントとサービスアカウントは強力なコマンドにアクセスできるため、これらのアカウントをモニターしてください。
  - システムアセットを追跡するには、コンポーネントのシリアル番号を使用します。すべてのカード、モジュール、およびマザーボードには、Oracle パーツ番号が電子的に記録されています。

セキュアな環境の計画

サーバーおよび Oracle Storage 12 Gb/s SAS PCIe RAID 内蔵 HBA をインストールおよび構成する前およびその最中には、このセクションの情報を確認してください。

このセクションには、次のトピックが含まれています。

- 7 ページの「ハードウェアのセキュリティー 」
- 8 ページの「ソフトウェアのセキュリティー 」
- 8 ページの「ファームウェアのセキュリティー」
- 9 ページの「Oracle ILOM ファームウェア」
- 9 ページの「システムログ」

ハードウェアのセキュリティー

物理的なハードウェアのセキュリティー保護は非常にシンプルで、ハードウェアへのアクセスを制限すること、およびシリアル番号を記録することです。

- **アクセスを制限する**

- 鍵付きのドアがあるラックに装置を設置する場合は、ラック内のコンポーネントを保守する必要があるとき以外はドアの鍵は掛けたままにしてください。
- 予備の現場交換可能ユニット (FRU) または顧客交換可能ユニット (CRU) は鍵の掛かったキャビネットに保管してください。鍵の掛かったキャビネットへのアクセスは、承認された人だけに制限してください。

- **シリアル番号を記録する**

  すべての HBA カードのシリアル番号を記録しておいてください。

ソフトウェアのセキュリティー

ソフトウェアコンポーネントのセキュリティー考慮事項は次のとおりです。

- ソフトウェアに付属のドキュメントを参照して、ソフトウェアで使用可能なセキュリティー機能を有効にします。
- HBA ドライバを設定および更新するには、スーパーユーザーアカウントを使用します。
- ハードウェアのほとんどのセキュリティーは、ソフトウェアを通じて実装されます。
- HBA をサポートするソフトウェアコンポーネントは、セキュアなアクセスを実現するために、システムのセキュリティー機能に依存しています。

ファームウェアのセキュリティー

HBA は出荷時にすべてのファームウェアがインストールされています。更新を除き、現場でファームウェアのインストールは必要ありません。

- ファームウェアの更新が必要になった場合は、LSI Web サイトの Oracle サポート領域 (http://www.lsi.com/sep/Pages/oracle/index.aspx) からファームウェアの更新を入手してください。

  また、Oracle サポートに問い合わせてサポートを手配したり、Oracle サポートに製品の最新の更新と手順について確認したりすることもできます。

  https://support.oracle.com

- HBA ファームウェア管理ユーティリティーを設定および更新するには、スーパーユーザーアカウントを使用します。通常のユーザーアカウントでは、ファームウェアを表示することはできますが、編集できません。Oracle Solaris OS ファームウェア更新プロセスでは、未承認のファームウェア変更を防止しています。

- 最新ニュース、ファームウェア更新要件に関する情報、またはその他のセキュリティー情報については、Oracle の Web サイトにある HBA のインストールガイドを参照してください。
- SPARC OpenBootPROM (OBP) セキュリティー変数の設定については、*OpenBoot 4.x のコマンドリファレンスマニュアル*を参照してください。

Oracle ILOM ファームウェア

x86 サーバーにプリインストールされている Oracle Integrated Lights Out Manager (Oracle ILOM) ファームウェアを使用すると、システムコンポーネントをアクティブにセキュリティー保護、管理、およびモニターできます。このファームウェアを使用したパスワードの設定、ユーザーの管理、およびセキュリティー関連機能 (Secure Shell (SSH)、Secure Socket Layer (SSL)、RADIUS 認証など) の適用に関する詳細は、Oracle ILOM のドキュメントを参照してください。

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

システムログ

- ロギングを有効にし、専用のセキュアなログホストにログを送信してください。
- NTP およびタイムスタンプを使用して正確な時間情報を含めるようにロギングを構成してください。

セキュアな環境の保守

HBA の初期インストールおよび設定のあと、Oracle ハードウェアおよびソフトウェアのセキュリティー機能を使用して、ハードウェアの制御およびシステムアセットの追跡を続行してください。

次のセクションが含まれています。

アセットの追跡

インベントリを追跡するには、シリアル番号を使用します。シリアル番号は、オプションのカードやシステムのマザーボード上のファームウェアに組み込まれています。これらのシリアル番号は、ローカルエリアネットワーク接続で読み取ることができます。

また、ワイヤレスの無線周波数識別 (RFID) リーダーを使用すると、より簡単にアセットを追跡できます。*RFID を使用して Oracle Sun システムアセットを追跡する方法*に関する Oracle のホワイトペーパーを参照してください。

ファームウェアの更新

装置のファームウェアのバージョンを最新に維持してください。

- 更新を定期的にチェックしてください。
- カードを管理したり、ドライバやファームウェアをアップグレードしたりするには、一般にすべてのオペレーティングシステム、特に Oracle Solaris では、root 資格情報でログインする必要があります。
- 常に、最新のリリースバージョンのファームウェアをインストールしてください。

ソフトウェアの更新

装置のソフトウェアは最新バージョンを維持してください。

- Oracle Solaris ドライバのソフトウェアの更新は、Oracle Solaris のパッチおよび更新を通じて入手できます。
- その他のオペレーティングシステムのドライバのソフトウェア更新は、http://www.lsi.com/sep/Pages/oracle/index.aspx から入手できる場合があります。
- 最新ニュース、ソフトウェア更新要件に関する情報、またはその他のセキュリティー情報については、Oracle の Web サイトにある HBA のドキュメントを参照してください。
- 常に、最新のリリースバージョンのソフトウェアをインストールしてください。
- ソフトウェアに必要なセキュリティーパッチをインストールしてください。
- デバイスにはファームウェアも搭載されており、ファームウェアの更新が必要な場合があります。

ログのセキュリティー

ログファイルは定期的に検査および保守してください。

- 可能性がある問題をログで確認し、セキュリティーポリシーに従ってアーカイブしてください。
- ログファイルが適切なサイズを超えたら、定期的に回収してください。あとで参照したり、統計的に分析したりできるように、回収したファイルのコピーを保守してください。

モジュールのセキュリティー

HBA は、LSI StorCLI コマンド行インタフェース (CLI) または MegaRAID SAS グラフィカルユーザーインタフェース (GUI) ソフトウェアによって管理されます。このソフトウェアを使用すると、次の作業ができます。

- HBA の操作をモニターします。
- HBA ファームウェアを更新します。

StorCLI および MegaRAID SAS GUI ソフトウェアは、`root` 資格証明を持つユーザーのみにアクセスを提供します。したがって、特権のないユーザーは、これらのユーティリティーを使用して SAN 環境を変更することができません。

StorCLI CLI および MegaRAID SAS GUI については、Web サイト (http://www.lsi.com/sep/Pages/oracle/index.aspx) で LSI のドキュメントを参照してください