Oracle® EDR InfiniBand Switch および仮想 I/O システムハードウェアセキュリティーガイド

Part No: E75983-01
2016 年 9 月

Part No: E75983-01

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。

目次

このドキュメントの使用法

- **概要** – Oracle からスイッチのセキュリティーポリシーを実装する方法について説明します
- **対象読者** – 技術者、システム管理者、および認定サービスプロバイダ
- **必要な知識** – ネットワークハードウェアの管理に関する豊富な経験

製品ドキュメントライブラリ

この製品および関連製品のドキュメントとリソースは http://www.oracle.com/goto/is2-46/docs で入手可能です。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお寄せください。

Oracle InfiniBand Switch IS2-46 セキュリティーガイド

このドキュメントでは、Oracle IS2-46 Switch のシャーシを保護するために役立つ一般的なセキュリティーガイドラインについて説明します。

次のトピックについて説明します。

セキュリティーの原則について

基本的なセキュリティーの原則として、アクセス (Access)、認証 (Authentication)、承認 (Authorization)、およびアカウンティング (Accounting) の 4 つの A (AAAA) 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 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、スイッチにパスワードシステムなどの認証機能を設定します。

  担当者がデータセンターに入室する際に、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みの操作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、ログインアクティビティーをモニター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、システムログおよび Oracle ILOM のログを使用します。特に `root` アカウントと root 権限を持つ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。Oracle のシリアル番号は、シャーシには物理的にマークされており、すべての SP、SCP、およびメインボードには電子的に記録されています。

セキュアな環境の計画

スイッチを設置および構成する前、およびその作業中に、次のトピックを確認してください。

- 10 ページの「ハードウェアのセキュリティー」
- 11 ページの「ソフトウェアのセキュリティー」
- 11 ページの「Oracle ILOM ファームウェア」
- 12 ページの「VLAN のセキュリティー」
- 12 ページの「ユーザーアカウント」
- 13 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**
  - ロックされている制限されたアクセス領域にスイッチを取り付けます。
  - 鍵付きのドアがあるラックに装置を設置する場合、ドアの鍵は常に掛けたままにしてください。
  - スイッチファブリックおよびネットワーク接続へのアクセスを制限します。これにより、スイッチに加えてピアノードも保護されます。
  - スイッチ自体のシリアルコンソールへのアクセスを制限し、セキュアに保たれるようにします。ターミナルサーバーまたはポート集配信装置を使用しないでください。シリアルコンソールでは、ユーザー管理、およびエラーとデバッグのメッセージングにより高い権限が与えられます。これらのメッセージでは、

悪意のある侵入およびセキュリティーの侵害を可能にする手がかりが不用意に提供されます。シリアルコンソールは暗号化されておらず、その点で SSH 接続よりセキュアではありません。

- 特に電源装置、ファンモジュール、およびトランシーバは簡単に取り外せるため、アクセスを制限してください。
- 予備の交換コンポーネント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は、承認された人のみがアクセスできるようにしてください。

- **シリアル番号を記録する**
  - すべての主要なアイテム (交換コンポーネントを含む) にセキュリティーのマークを付けます。専用の紫外線ペンまたはエンボスラベルを使用してください。
  - すべてのハードウェアのシリアル番号を記録しておいてください。
  - 納品書、購入記録、およびライセンスのコピーは、システム緊急時にシステムマネージャーが簡単に取り出せるセキュアな場所に保管しておいてください。これらの印刷ドキュメントは、所有権を示す唯一の証明になります。

ソフトウェアのセキュリティー

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。

- ファームウェア内にセキュリティー機能を実装するためのその他のガイドラインについては、スイッチのドキュメントを参照してください。
- ソフトウェアスイートで使用可能なセキュリティー機能を有効にするには、OFOS および OFM のドキュメントを参照してください。
- スイッチの管理は、SER MGT ポートを使用して帯域外で行います。このポートはデータトラフィックおよび一般のネットワークから分離されています。
- 帯域外管理を実現できない場合は、帯域内管理用に一意の VLAN 番号を用意してください。
- 新しいスイッチを取り付けるときは、すべてのデフォルトのパスワードをできるかぎり早く変更します。スイッチにはデフォルトのユーザーアカウントが 1 つ (`root`) あります。`root` ユーザーにはスーパーユーザー権限があります。デフォルトのパスワードは `changeme` です。スイッチをネットワークに接続する前に、Oracle ILOM の `set /SP/users/root password=`*password* コマンドを使用してパスワードを変更することをお勧めします。
- 特に追加のユーザーアカウントとともに構成されている場合は、スイッチのすべてのパスワードの変更をスケジュールして定期的に変更します。

Oracle ILOM ファームウェア

スイッチにプリインストールされている 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

リングできます。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)、および RADIUS、Active Directory、LDAP の認証プロトコルを含む) の適用の詳細については、Oracle ILOM のドキュメントを参照してください。Oracle ILOM に固有のセキュリティーガイドラインについては、Oracle ILOM 3.2 ドキュメントライブラリの一部である、『*Oracle ILOM* セキュリティーガイドファームウェア *Release 3.0*、*3.1*、および *3.2*』を参照してください。Oracle ILOM 3.2 のドキュメントは次の場所で検索できます。

http://docs.oracle.com/cd/E37444_01

VLAN のセキュリティー

仮想ローカルエリアネットワーク (VLAN) を構成する場合 (たとえば、帯域内ネットワーク管理のため) は、VLAN ではネットワーク上の帯域幅が共有され、追加のセキュリティー対策が必要であることを忘れないでください。

- 機密性のある一連のシステムをその他のネットワークと切り離すように、VLAN を定義してください。これにより、それらのクライアントやサーバーに格納された情報にアクセスされる可能性が少なくなります。
- トランクポートには、一意のネイティブ VLAN 番号を割り当ててください。
- VLAN でのトランク経由のトランスポートは、どうしても必要な場合だけにしてください。
- VLAN Trunking Protocol (VTP) は、可能な場合は無効にしてください。無効にできない場合は、VTP に対して管理ドメイン、パスワード、およびプルーニングを設定します。その後、VTP を透過モードに設定してください。

ユーザーアカウント

- Active Directory、LDAP、RADIUS などのセキュアな認証プロトコルを実装します。認証および承認の集中管理を使用します。
- `root` スーパーユーザーアカウントの使用を制限してください。代わりに、管理用途のみのためのより権限の低い Oracle ILOM アカウントを作成します。一般的なガイドラインとしては、特定のタスクを実行するために十分な最小権限を持つユーザーアカウントを作成して使用します。
- 必要に応じて、アクセス制御リストを使用してください。
- 長時間のセッションにタイムアウトを設定してください。
- 特権レベルを設定してください。
- 承認されていないアクセスは禁止されていることをユーザーに知らせるために、システムバナーを作成してください。

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

初期インストールおよび設定が終了したら、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。

- 13 ページの「ハードウェアの電源制御」
- 13 ページの「アセットの追跡」
- 14 ページの「ソフトウェアおよびファームウェアの更新」
- 14 ページの「ネットワークアクセス」
- 15 ページの「データ保護」
- 15 ページの「ログのセキュリティー」

ハードウェアの電源制御

一部の Oracle システムへの電源は、ソフトウェアを使用してオンとオフを切り替えることができます。リモートから配電盤 (PDU) を有効および無効にできるシステムキャビネットもあります。これらのコマンドの承認は、一般にシステムの構成時に設定され、通常はシステム管理者とサービス担当者に制限されます。詳細は、システムまたはキャビネットのドキュメントを参照してください。

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。Oracle のシリアル番号は、SP および SCP のファームウェア、およびメインボードに組み込まれています。これらのシリアル番号を読み取る手順については、スイッチのドキュメントを参照してください。

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* を使用した *Oracle Sun* システムアセットの追跡方法に関する Oracle のホワイトペーパーを参照してください。

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`

ソフトウェアおよびファームウェアの更新

スイッチ上のソフトウェアとファームウェアを最新のバージョンに保ちます。

- 更新を定期的にチェックしてください。
- 常に、最新リリースバージョンのソフトウェアや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。

更新およびパッチが入手可能かどうかについては、次のサイトで確認します。

http://support.oracle.com

ネットワークアクセス

システムへのローカルアクセスとリモートアクセスをセキュリティー保護するために、次のガイドラインに従ってください。

- MAC アドレスに基づいてアクセスを制限するには、ポートのセキュリティーを実装してください。自動トランキングはすべてのポートで無効にしてください。
- リモート構成を特定の IP アドレスに制限するときは、Telnet ではなく SSH を使用してください。Telnet では、ユーザー名とパスワードが平文で渡されるため、ログイン資格情報が LAN セグメントのすべてのユーザーに公開される可能性があります。SSH の強力なパスワードを設定してください。
- セキュアな転送を提供するために、SNMP のバージョン 3 (v3) を構成および使用してください。SNMP のバージョン v1 および v2c はセキュアではなく、認証データを暗号化されていないテキストで転送します。
- SNMP が必要な場合は、デフォルトの SNMP コミュニティー文字列 (PUBLIC) を強力なコミュニティー文字列に変更してください。攻撃者によってコミュニティーが照会されると、完全なネットワークマップが作成され、管理情報ベース (MIB) の値が変更される可能性もあります。
- 絶対に必要な場合を除いて、SNMP の `set` 要求を有効にしないでください。有効な場合は、読み取り専用アクセス権および読み取り/書き込みアクセス権を持つ別個の SNMP v3 ユーザーを作成します。
- Web インタフェースから SP または SCP にアクセスした場合は、必ずログアウトします。
- 使用していないサービスまたは不要なサービス (TCP スモールサーバーなど) を無効にします。必要なサービスのみを有効にして、それらのサービスをセキュアに構成してください。
- 使用していない場合は、IPMI サービスを無効にします。IPMI プロトコルは、SP にアクセスするためのセキュアでない手段です。
- HTTP サービスを無効にして、代わりに HTTPS を使用します。状況によっては、Java の互換性のために HTTP を一時的に有効にしなければならない場合があります。その場合は慎重に行なってください。

- 使用されていないスイッチのポートを無効にします。

データ保護

データのセキュリティーを最大限に高めるために、これらのガイドラインに従ってください。

- スイッチの構成ファイルをリモートのセキュアな場所にバックアップし、承認された管理者のみがアクセスできるように制限します。構成ファイルには各設定の説明がコメントとして含まれています。
- データ暗号化ソフトウェアを使用して、ハードドライブ上の機密情報をセキュアな状態にしてください。
- SP、SCP、および SSD は、システムのハードドライブと同等のデータが含まれているスイッチコンポーネントです。スイッチを交換する場合は、これらのコンポーネントを物理的に壊すか、それぞれのファイルシステム内のすべてのデータを完全に消去します。ファイルシステム上のすべてのデータを完全に消去するには、ディスクワイプソフトウェアを使用してください。

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システムログおよび Oracle ILOM のログで確認し、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、定期的にアーカイブおよびクリアしてください。あとで参照したり、統計的に分析したりできるように、アーカイブをセキュアな場所に保持してください。