Oracle Hardware Management Pack セキュリティーガイド

Part No: E39910–01
2013 年 3 月

ORACLE

130322@25097

目次

概要

このセクションでは、セキュリティーガイド情報を含む Oracle Hardware Management Pack (HMP) 製品の概要と、アプリケーションセキュリティーの一般的な原則について説明します。

次のトピックで構成されています。

製品の概要

Oracle Hardware Management Pack はお使いのサーバー、および多くの x86 ベースのサーバーと一部の SPARC ベースのサーバーで利用できます。Oracle Hardware Management Pack には、サーバーを管理するための 2 つのコンポーネント (SNMP 監視エージェントと、クロスオペレーティングシステムのコマンド行インタフェースツール (CLI ツール) のファミリ) が用意されています。

Hardware Management Agent SNMP Plugins を使用すると、SNMP を使用してデータセンター内の Oracle サーバーおよびサーバーモジュールを監視でき、2 つの管理ポイント (ホストと Oracle ILOM) にアクセスする必要がなくなるという利点が得られます。この機能により、単一の IP アドレス (ホストの IP) を使用して、複数のサーバーおよびサーバーモジュールを監視できます。

Hardware Management Agent SNMP Plugins は、Oracle サーバーのホストオペレーティングシステム上で動作します。SNMP Plugin では、サービスプロセッサとの通信に Oracle Hardware Storage Access Libraries が使用されます。サーバーの現在の状態に関する情報が Hardware Management Agent によって自動的に取得されます。

Oracle Server CLI ツールを使用して、Oracle サーバーを構成できます。CLI ツールは、Oracle Solaris、Oracle Linux、Oracle VM、Linux のその他のバリアント、および Windows オペレーティングシステムで動作します。次の表では、CLI ツールを使用して実行できるタスクについて説明します。

ホスト OS からのシステム管理タスク	CLI ツール
BIOS 設定、デバイスのブート順序、一部のサービスプロセッサ設定を構成します。	`ubiosconfig` `biosconfig`
Oracle ILOM と BIOS を更新します。	`fwupdate`
サポートされる SAS ストレージデバイス、組み込み SAS ストレージコントローラ、SAS ストレージエクスパンダ、およびストレージドライブのファームウェアバージョンを照会、更新、検証します。	
Oracle ILOM の構成設定を復元、設定、表示するほかに、ネットワーク管理、クロック設定、ユーザー管理に関連のある Oracle ILOM プロパティーを表示および設定します。	`ilomconfig`
ストレージアレイなど、RAID コントローラに接続されたストレージドライブ上の RAID ボリュームを表示または作成します。	`raidconfig`
システムの健全性を監視します。	`hwmgmt`

このセキュリティーガイドについて

このドキュメントでは、Oracle Hardware Management Pack の一般的なセキュリティーガイドラインついて説明します。このガイドは、ネットワークスイッチやネットワークインタフェースカードなどの他の Oracle ハードウェア製品を使用する場合のセキュリティーの確保に役立つように考えられています。

次のトピックで構成されています。

基本的なセキュリティー原則

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

  ハードウェアやデータを侵入から保護するには、物理的な制御またはソフトウェアの制御を行います。

  - 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、通常は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検証するには、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すべて設定します。

  認証では、バッジやパスワードなどを通じてさまざまなレベルのセキュリティーを提供します。たとえば、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

  承認では、各担当者が使用できるハードウェアやソフトウェアを、トレーニングを受けて使用を許可されたものだけに制限します。

  たとえば、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

  顧客の IT 担当者は、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の監視やハードウェアインベントリの管理を行います。
    - ユーザーログインを監視するには、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システムログから監視してください。
    - ログファイルが適当なサイズを超えたときは、顧客の会社方針に従って定期的に回収してください。一般に、ログは長期間保持されるため、保持する方法が重要となります。
    - インベントリの目的でシステム資産を追跡するには、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。

Oracle Hardware Management Pack のセキュリティーに関するサマリー

すべてのシステム管理ツールを構成するときに留意する必要のある重要なセキュリティー項目は次のとおりです。

- システム管理製品を使用して、ブート可能なルート環境を構築できます。

  ブート可能なルート環境では、Oracle ILOM、Oracle System Assistant、およびハードディスクへのアクセス権が与えられます。
- システム管理製品には、実行するには管理者およびルート特権が必要な強力なツールが含まれています。

このレベルのアクセス権では、ハードウェア構成の変更やデータの消去を実行することも可能です。

- Oracle Hardware Management Pack ドキュメントライブラリ (http://www.oracle.com/pls/topic/lookup?ctx=ohmp)

Oracle Hardware Management Pack のインストール前

初期インストールおよび設定の間、Oracle ソフトウェアのセキュリティー機能を使用して、ハードウェアを制御し、システム資産を追跡します。

次のトピックで構成されています。

Oracle Hardware Management Pack のコンポーネント

Oracle Hardware Management Pack には、RAID、BIOS、Oracle ILOM を構成し、ファームウェアを更新するための、一連のハードウェア管理コマンド行ツールが含まれています。監視用の SNMP Plugin も含まれています。Oracle Hardware Management Pack には、内部チャネルを介して Oracle ILOM と通信し、サーバーに関するインベントリおよび健全性情報を共有するデーモンまたはサービスも含まれます。

これらのツールとプラグインはホストオペレーティングシステムにインストールされているので、ホストから直接、システム管理タスクを実行できます。Oracle Hardware Management Pack には、Oracle サーバーの管理に役立つ機能が用意されていますが、これは完全にオプションです。

Oracle Hardware Management Pack の機能の詳細について Oracle Hardware Management Pack のユーザーズガイドを参照し、これを使用およびインストールするかどうかの判断に役立ててください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)
- Oracle ILOM の全般的な情報については、`http://www.oracle.com/pls/topic/lookup?ctx=ilom31` を参照してください。

エージェントに基づいた SNMP Plugin のセキュリティー設定

Oracle Hardware Management Pack には、ホストオペレーティングシステムのネイティブの SNMP エージェントを拡張して追加の Oracle MIB 機能を提供する SNMP Plugin モジュールが含まれています。Oracle Hardware Management Pack 自体には SNMP エージェントが含まれていないので特に注意してください。Linux の場合、モジュールは、あらかじめインストールしておく必要のある net-snmp エージェントに追加されます。Solaris の場合、モジュールは Solaris Management Agent に追加されます。Windows の場合、このプラグインはネイティブの SNMP サービスを拡張します。

同様に、Oracle Hardware Management Pack SNMP Plugin の SNMP に関連したセキュリティー設定は、プラグインによってではなく、ネイティブの SNMP エージェントまたはサービスの設定によって決まります。SNMP をセキュアに構成する方法については、net-snmp または Windows SNMP サービスのドキュメントを参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

SNMP エージェントの SNMP プロトコルバージョンの選択

SNMP は、システムを監視または管理するための標準のプロトコルです。SNMPv1/v2c は暗号化機能を備えておらず、認証の一形態としてコミュニティー文字列を使用します。コミュニティー文字列は平文のままネットワーク経由で送信され、個々のユーザーに専有的に使用されるのではなく、通常はグループ全体で共有されます。これに対し、SNMPv3 では暗号化機能を使用してセキュアなチャネルを確保し、個別のユーザー名とパスワードを使用します。SNMPv3 のユーザーパスワードは、管理ステーション上にセキュアに格納できるようにまとめられます。

ネイティブの SNMP エージェントでサポートされている場合は、SNMPv3 を使用することをお勧めします。SNMPv3 を構成する方法については、net-snmp または Windows SNMP サービスのドキュメントを参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Oracle Hardware Management Pack のインストール

次のトピックで構成されています。

Oracle Hardware Management Pack のインストーラの実行

Oracle Hardware Management Pack は、RPM など、オペレーティングシステムのネイティブのインストールツールを使用してインストールできる、一連のネイティブのインストールパッケージから構成されます。さらに、ウィザードベースのインストーラを使用して、簡単にインストールすることができます。インストーラは、ネイティブのパッケージの追加以外にも、Oracle Hardware Management Pack を使用できるように構成するときにも役立ちます。

Oracle Hardware Management Pack のインストーラは、ネイティブのパッケージをインストールする必要があるので、ルートまたは管理者として実行する必要があります。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

LAN インターコネクトの有効化の選択

KCS インタフェースに替わる高速なインタフェースとして、ホストオペレーティングシステム上で動作するクライアントは、内蔵の高速インターコネクトを介して Oracle ILOM と通信できます。このインターコネクトは、内蔵の Ethernet-over-USB 接続によって実装されており、IP スタックを実行します。Oracle ILOM およびホストには、このチャネルで通信するためのルーティング不可能な内部の IP アドレスが与えられています。

LAN インターコネクトを介して Oracle ILOM に接続するには認証が必要になりますが、これはちょうど、接続がネットワーク経由で Oracle ILOM 管理ポートに対して送られてくる場合と同じです。管理ネットワーク上で公開されているサービスまたは

プロトコルはすべて、LAN インターコネクトを介してホストから利用できます。たとえば、ホスト上の Web ブラウザを使用して Oracle ILOM の Web インタフェースにアクセスしたり、Secure Shell クライアントを使用して Oracle ILOM CLI に接続することができます。どのようなケースであれ、LAN インターコネクトを使用するには、有効なユーザー名とパスワードを入力する必要があります。

Oracle Hardware Management Pack のインストーラは、LAN インターコネクトを有効にするオプションを表示します。ネットワーク手順で RFC 3927 と、リンクローカル IPv4 アドレスの割り当て機能をサポートしている場合に限り、LAN インターコネクトを有効にすることをお勧めします。また、オペレーティングシステムがブリッジまたはルーターとして機能していないことを慎重に確認する必要があります。これにより、ホストと Oracle ILOM との間の管理トラフィックがプライベートのままであることが確実になります。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

ファイルでの資格情報の保存の選択

Oracle Hardware Management Pack に含まれている ilomconfig ツールと fwupdate ツールは、高速 LAN インターコネクトを使用して Oracle ILOM に接続できます。低速な KCS インタフェースに替えて LAN インターコネクトを使用すれば、Oracle ILOM ファームウェアの更新などの主要操作のパフォーマンスを大幅に向上させることができます。

LAN インターコネクトでは認証が必要なので、これらのツールを呼び出すたびに、Oracle ILOM で認証を受ける必要があります。便利な方法として、資格情報をファイルにキャッシュして、ツールが自動的に使用できるようにすることができます。これにより、Oracle Hardware Management Pack ツールを使用するスクリプトに平文のパスワードを埋め込む必要がなくなります。

ilomconfig ツールを使用して、ルートで読み取り専用の暗号化ファイルにユーザー名とパスワードを格納できます。ilomconfig または fwupdate を使用して Oracle ILOM にアクセスするときにこのファイルが検出されると、キャッシュされた資格情報が使用されます。または、ツールを呼び出すごとに、コマンド行でユーザー名とパスワードを指定することもできます。

使用される暗号化アルゴリズムはシステムごとに異なります。ただし鍵が検出された場合は、ファイルを復号して、ユーザー名とパスワードを明らかにすることができます。危殆化したパスワードを他の Oracle ILOM システムで使用できないようにするなどの理由で、それぞれの Oracle ILOM で一意のパスワードを作成することをお勧めします。

ファイルに資格情報を保存する方法については、Oracle Hardware Management Pack のユーザーズガイドを参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (http://www.oracle.com/pls/topic/lookup?ctx=ohmp)

Oracle Hardware Management Pack のインストール後

次のトピックで構成されています。

Oracle Hardware Management Pack のアンインストール

Oracle Hardware Management Pack パッケージは、RPM などのネイティブパッケージツールを使用するか、Oracle Hardware Management Pack に付属のウィザードベースのアンインストーラを使用してアンインストールできます。ネイティブパッケージの方法でパッケージを削除する場合、LAN インターコネクトで使用するためにキャッシュしたユーザー名とパスワードが格納されている暗号化ファイルは削除されません。これは手動で削除する必要があります。

ウィザードベースのアンインストーラは資格情報ファイルを削除します。したがって、Oracle Hardware Management Pack のアンインストールには、ウィザードベースのインストーラを使用することをお勧めします。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)