Oracle® Hardware Management Pack for Oracle Solaris 11.3 セキュリティーガイド

Part No: E76536-02
2017 年 3 月

Part No: E76536-02

Copyright © 2015, 2017, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクルまでご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアまたはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアまたはハードウェアは、危険が伴うアプリケーション(人的傷害を発生させる可能性があるアプリケーションを含む)への用途を目的として開発されていません。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、Oracle Corporationおよびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはオラクル およびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。適用されるお客様とOracle Corporationとの間の契約に別段の定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。適用されるお客様とOracle Corporationとの間の契約に定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

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

製品およびアプリケーションのセキュリティーの概要 7
Oracle Hardware Management Pack for Oracle Solaris について 7
基本的なセキュリティー原則 8
Oracle Hardware Management Pack のセキュリティーに関するサマリー 9

Oracle Hardware Management Pack のセキュリティー保護 11
ホストと ILOM の相互接続のインタフェース 11
IPMI を Transport Layer Security (TLS) と組み合わせて使用するためのサポート 12
古い資格情報ファイルの削除 12
SNMP セキュリティー設定の選択 13

Oracle Hardware Management Pack コンポーネントのインストールまたはアンインストール 15
コンポーネントのインストール 15
コンポーネントのアンインストール 15

製品およびアプリケーションのセキュリティーの概要

このセクションでは、Oracle Hardware Management Pack (HMP) for Oracle Solaris 製品と基本的なアプリケーションのセキュリティーの概要について説明します。

次のトピックで構成されています。

- 7 ページの「Oracle Hardware Management Pack for Oracle Solaris について」
- 8 ページの「基本的なセキュリティー原則」
- 9 ページの「Oracle Hardware Management Pack のセキュリティーに関するサマリー」

Oracle Hardware Management Pack for Oracle Solaris について

Oracle Hardware Management Pack for Oracle Solaris は、多くの Oracle 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 モニタリングエージェントと、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モニターでき、2 つの管理ポイント (ホストと Oracle ILOM) に接続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モニターできます。

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 Plugins 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。Hardware Management Agent の詳細は、*Oracle® Server Management Agents for Oracle Solaris 11.3 ユーザーズガイド*を参照してください。

Oracle Server CLI ツールを使用すると、Oracle サーバーを構成できます。ツールのリストについては、*Oracle® CLI Tools for Oracle Solaris 11.3 ユーザーズガイド*を参照してください。

機能と使用法の詳細は、Oracle Hardware Management Pack for Oracle Solaris のドキュメントを参照してください。

- Oracle Hardware Management Pack for Oracle Solaris のドキュメントライブラリ: `http://www.oracle.com/goto/ohmp/solarisdocs`
- 一般的な Oracle ILOM の情報: `http://www.oracle.com/goto/ilom/docs`

基本的なセキュリティー原則

基本的なセキュリティー原則として、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は通常、アクセス制限は物理的および仮想的な手段の両方を意味します。
  - 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の手段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は、従業員バッジを正しく使用してもらうようにします。
- 承認

  承認では、会社の担当者は、トレーニングを受けて使用を許可されたハードウェアやソフトウェアの操作だけが許可されます。

  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をモニターしたりハードウェアインベントリを保守したりします。

- 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。ログは一般的に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すると、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 *root* アクセス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、ハードウェア構成を変更したり、データを消去したりできます。

Oracle Hardware Management Pack のセキュリティー保護

Oracle Solaris では、もっとも頻繁に使用される Oracle Hardware Management Pack コンポーネントは事前インストールされています。セキュリティーを確保するには、追加の構成が必要になることがあります。

- 11 ページの「ホストと ILOM の相互接続のインタフェース」
- 12 ページの「IPMI を Transport Layer Security (TLS) と組み合わせて使用するためのサポート」
- 12 ページの「古い資格情報ファイルの削除」
- 13 ページの「SNMP セキュリティー設定の選択」

ホストと ILOM の相互接続のインタフェース

ホストと ILOM の相互接続のインタフェースを使用すると、ホストオペレーティングシステム上のクライアントは、内蔵の高速相互接続を介して Oracle ILOM と通信できます。この相互接続は、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。この接続は Oracle Solaris オペレーティングシステムではデフォルトで有効になっています。

ホストと ILOM の相互接続を介して 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 管理ポートに入っ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、ホストと ILOM の相互接続を介して利用できます。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 に接続したりすることができます。どのようなケースであれ、LAN 相互接続を使用するには、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。

RFC 3927 と、リンクローカル IPv4 アドレスを使用する機能をネットワークでサポート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してください。これにより、ホストと ILOM の相互接続を介したホストと 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。

侵害されたパスワードをほかの Oracle ILOM を使用したシステムに対して使用できないように、各 Oracle ILOM サービスプロセッサでユーザーごとに一意のパスワードを作成することをお勧めします。

詳細は、*Oracle® Hardware Management Pack for Oracle Solaris 11.3 インストールガイド*を参照してください。

IPMI を Transport Layer Security (TLS) と組み合わせて使用するためのサポート

Oracle Solaris 11.3 SRU 18 より前の Oracle Hardware Management Pack for Oracle Solaris バージョンでは、ネットワークの IPMI 暗号化は LANPLUS プロトコルを使用して処理されていました。IPMI を TLS プロトコル (ターゲットの Oracle ILOM でサポートされている場合) と組み合わせて使用するためのサポートが追加されました。IPMI over TLS を使用するには、ターゲットの Oracle ILOM がバージョン 3.2.8.1 以降である必要があります。サポート状況を確認するには、Web インタフェースからターゲットの Oracle ILOM にログインし、「Administration」>「Management Access」>「IPMI」で「TLS Sessions」設定をチェックしてください。

ターゲットの Oracle ILOM で IPMI over TLS がサポートされていない場合、プロトコルは LANPLUS プロトコル (有効になっている場合) に戻ります。

注記 - Oracle Hardware Management Pack for Oracle Solaris 11.3 SRU 18 では IPMI over TLS 用の暗号化通信がサポートされていますが、証明書の検証は現在サポートされていません。証明書の完全な検証は、Oracle Hardware Management Pack for Oracle Solaris 11.3 の将来のリリースでサポートされる予定です。

古い資格情報ファイルの削除

Oracle Solaris 11.3 より前の Oracle Hardware Management Pack for Oracle Solaris バージョンでは、`ilomconfig` ツールを使用して、root 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した。`ilomconfig`、`fwupdate`、または `ubiosconfig` ツールを使用して Oracle ILOM にアクセスする際に、このファイルが検出された場合、キャッシュされた資格情報が使用されていました。Oracle Hardware Management Pack for Oracle Solaris 11.3 では、この資格情報ファイル機能がサポートされていません。

Oracle Solaris の以前のバージョンから Oracle Solaris 11.3 にアップグレードしており、以前に資格情報ファイルを保存した場合は、`ilomconfig delete credential` コマンドを実行して、このファイルを削除してください。

サービスプロセッサにアクセスするコマンドを呼び出す手順については、*Oracle® CLI Tools for Oracle Solaris 11.3 ユーザーズガイド*を参照してください。

SNMP セキュリティー設定の選択

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 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ことに留意することが特に重要です。Oracle Solaris オペレーティングシステムでは、モジュールは Solaris Management Agent に追加されます。

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 設定には次を含める必要があります。

- SNMPv1/v2c。このバージョン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、個々のユーザー専用ではなく、通常は個人のグループ全体で共有されます。
- SNMPv3。このバージョン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 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 のために net-snmp を構成する方法については、Oracle Solaris のドキュメントを参照してください。

また、すべての SNMP トラフィックを個別のセキュアな管理ネットワークに隔離することもお勧めします。

注記 - SNMP 機能はデフォルトで無効になっているため、*Oracle® Server Management Agents for Oracle Solaris 11.3 ユーザーズガイド*の説明に従ってユーザーが有効にして構成する必要があります。

Oracle Hardware Management Pack コンポーネントのインストールまたはアンインストール

次のトピックで構成されています。

- 15 ページの「コンポーネントのインストール」
- 15 ページの「コンポーネントのアンインストール」

コンポーネントのインストール

Oracle Hardware Management Pack for Oracle Solaris は、事前インストールされたツールのセットで構成されます。事前インストールされていないその他の Oracle Hardware Management Pack コンポーネントパッケージは、Oracle Solaris Image Packaging System (IPS) を使用してインストールできます。

root 権限を持つ管理者だけが Oracle Hardware Management Pack パッケージをインストールできます。

- Oracle Hardware Management Pack for Oracle Solaris のドキュメントライブラリ: `http://www.oracle.com/goto/ohmp/solarisdocs`

コンポーネントのアンインストール

Oracle Hardware Management Pack for Oracle Solaris パッケージは、Oracle Solaris の `pkg uninstall` コマンドを使用してアンインストールできます。

注記 - パッケージをアンインストールするときに、ホストと ILOM の相互接続を使用した Oracle ILOM へのアクセスが容易になるように、Oracle Hardware Management Pack の `ilomconfig` コマンドを使用して事前にホスト資格情報をキャッシュファイルに保存した場合、そのファイルは削除されません。このようなケースでこのファイルを削除するには、Oracle Hardware Management Pack パッケージをアンインストールする前に、`ilomconfig delete credential` コマンドを実行してください。

- Oracle Hardware Management Pack for Oracle Solaris のドキュメントライブラリ: http://www.oracle.com/goto/ohmp/solarisdocs