Netra Modular System セキュリティーガイド

Part No: E68380-01
2015 年 8 月

Part No: E68380-01

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

セキュリティーの概要

Oracle の Netra Modular System は、データセンターでのコストを削減して配備時間を短縮するために完全に仮想化できる、事前に統合およびケーブル接続されたプラットフォームです。モジュラーシステムは指定したハードウェアを装備しており、工場で組み立てられて出荷されます。

次のトピックでは、モジュラーシステムのセキュリティーの概念と機能について説明します。

基本的なセキュリティー原則

モジュラーシステムのすべてのソフトウェアとハードウェアについて、次の基本的なセキュリティー原則に従ってください。

- 認証 – 認証とはユーザーを識別する方法で、通常ユーザー名とパスワードなどの機密情報または共有鍵を介して行います。認証はハードウェアまたはソフトウェアのユーザーが本人であることを保証します。デフォルトでは、ローカルユーザー名とパスワードが認証に使用されます。共有鍵ベースの認証も使用できます。
- アカウンティングと監査 – アカウンティングと監査は、システムで行われたユーザーアクティビティーの記録を保持します。管理者はモジュラーシステムのソフトウェアとハードウェアの機能を使用して、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できます。
  - ユーザーのログインはシステムログでモニターされます。システム管理者とサービスアカウントは、不正に使用されると危害やデータ損失につながる可能性があるコマンドにアクセスできます。
  - ハードウェアアセットは、シリアル番号で追跡されます。Oracle の部品番号は、すべてのカード、モジュール、およびマザーボードに電子的に記録されており、インベントリのために使用できます。

セキュリティーに関する詳細な考慮事項

基本的なセキュリティー原則に加えて、モジュラーシステムは耐障害性と多層防御に対処しています。モジュラーシステムは、重要なセキュリティー要件と考慮事項を満たすために、適切に統合されたセキュリティー機能のセットを備えています。次のセクションでは、これらの原則について説明します。

- ミッションクリティカルなワークロードの耐障害性 – ミッションクリティカルなワークロードのためのハードウェアとソフトウェアのプラットフォームを選択する組織は、内部ユーザーまたは外部の関係者によって実行された偶発的なアクションまたは悪意のあるアクションが原因の損傷をモジュラーシステムによって確実に防いだり最小限に抑えたりできます。Oracle Maximum Availability Architecture のベストプラクティスの一部である次の対策によって、耐障害性が向上します。
  - 使用するコンポーネントが、一緒に適切に動作してセキュアな配備アーキテクチャーを支援するように設計およびテストされていることを確認します。モジュラーシステムでは、セキュアな分離、アクセス制御、サービス品質、およびセキュアな管理がサポートされます。
  - 構成製品のデフォルトの攻撃面を減らすことで、マシンの全体的な露出を最小限に抑えることができます。
  - さまざまなオープンプロトコルおよび検査済みのプロトコルと、強力な認証、アクセス制御、機密性、整合性、および可用性という従来のセキュリティー目標をサポートできる API を使用して、操作インタフェースや管理インタフェースを含むマシンを保護します。
  - ソフトウェアとハードウェアに、障害が発生した場合でもサービスの可用性を維持する機能が含まれていることを確認します。これらの機能は、攻撃者がシステム内の 1 つ以上の個々のコンポーネントを無効にしようとした場合に役立ちます。
- オペレーティング環境をセキュリティー保護する多層防御 – モジュラーシステムでは、ワークロードとデータのセキュアなオペレーティング環境を作成するために役立つ、複数の独立した、相互に補強し合うセキュリティー制御が採用されています。モジュラーシステムでは、次のように多層防御の原則がサポートされます。
  - 転送中、使用中、および休止状態の情報をセキュリティー保護するためのさまざまな強力な保護が用意されています。セキュリティー制御は、サーバー層およびネットワーク層で使用できます。各層の固有のセキュリティー制御をほかのセキュリティー制御と統合して、階層化された強力なセキュリティーアーキテクチャーを作成できます。
  - 明確に定義されたオープンスタンダード、プロトコル、およびインタフェースの使用をサポートします。モジュラーシステムは、既存のセキュリティーポリシー、アーキテクチャー、対策、および標準に統合できます。

セキュリティー機能

モジュラーシステムのハードウェアとソフトウェアは強固な構造になっています。Oracle では、NTP や SSH などのサービスに推奨されるセキュアな構成も用意しています。さらに、モジュ

ラーシステムのアーキテクチャーは、コアコンポーネントに対するセキュリティー機能を提供します。これらのセキュリティー機能はほとんどの場合、階層化されたセキュリティー計画を配備している組織によって適用されます。機能は次のカテゴリに分けられます。

- 9 ページの「ネットワークトラフィックの分離」
- 9 ページの「セキュアな管理のための Oracle ILOM」

ネットワークトラフィックの分離

IT インフラストラクチャーを統合して、共有サービスアーキテクチャーを実装し、セキュアなマルチテナントサービスを提供する場合は、ネットワークトラフィックを分離することを検討してください。モジュラーシステムでは、ニーズに基づいて、分離のポリシーと計画を柔軟に実装できます。

物理ネットワークレベルで、クライアントアクセスはデバイス管理とデバイス間通信から分離されます。クライアントと管理のネットワークトラフィックは、別個のネットワーク上に分離されます。クライアントアクセスは、システムで実行されているサービスに対する信頼できる高速アクセスを実現する冗長な 10G ビット/秒 Ethernet ネットワークを介して行われます。管理アクセスは、物理的に分離された 1G ビット/秒 Ethernet ネットワークを介して行われます。これによって、操作ネットワークと管理ネットワークが分離されます。

組織は、仮想 LAN (VLAN) を構成することで、クライアントアクセスの Ethernet ネットワークを介してネットワークトラフィックをさらに分離することを選択できます。VLAN は、要件に基づいてネットワークトラフィックを分離します。Oracle では、通信の機密性と整合性を保証するために、VLAN 経由で暗号化されたプロトコルを使用することを推奨しています。

セキュアな管理のための Oracle ILOM

個々のアプリケーションとサービスを適切にセキュリティー保護するには、セキュリティー制御と機能のコレクションが必要です。配備されたサービスとシステムのセキュリティーを維持するためには、包括的な管理機能を使用できることも等しく重要です。モジュラーシステムでは、Oracle ILOM のセキュリティー管理機能を使用します。

Oracle ILOM は、モジュラーシステムのコンピュートノードに組み込まれた SP です。Oracle ILOM は、次のような帯域外管理アクティビティーを実行するために使用されます。

- データベースサーバーとストレージサーバーのセキュアな電源管理を実行するためにセキュアアクセスを提供します。アクセスには、SSL によって保護される Web ベースのアクセス、セキュアシェルを使用するコマンド行アクセス、および IPMI v2.0 プロトコルと SNMPv3 プロトコルが含まれます。
- 役割ベースのアクセス制御モデルを使用して、職務要件を分離します。個々のユーザーに、実行できる機能を制限する特定の役割が割り当てられます。

- すべてのログインと構成変更の監査記録が提供されます。それぞれの監査ログエントリには、アクションを実行したユーザーと、タイムスタンプの一覧が表示されます。監査レコードにより、組織は、未承認のアクティビティーまたは変更を検出して、これらのアクションが特定のユーザーに起因すると推定できます。

Oracle ILOM セキュリティーの詳細は、http://www.oracle.com/goto/ILOM/docs にある『*Oracle ILOM セキュリティーガイド*』を参照してください。

セキュアな環境の計画

Netra Modular System が到着する前にセキュリティーガイドラインの準備を整えます。システムの設置後は、組織の現行のセキュリティー要件に即するようセキュリティーガイドラインを定期的にレビューして調整してください。

次のトピックでは、Netra Modular System を設置するためのセキュリティーガイドラインについて説明します。

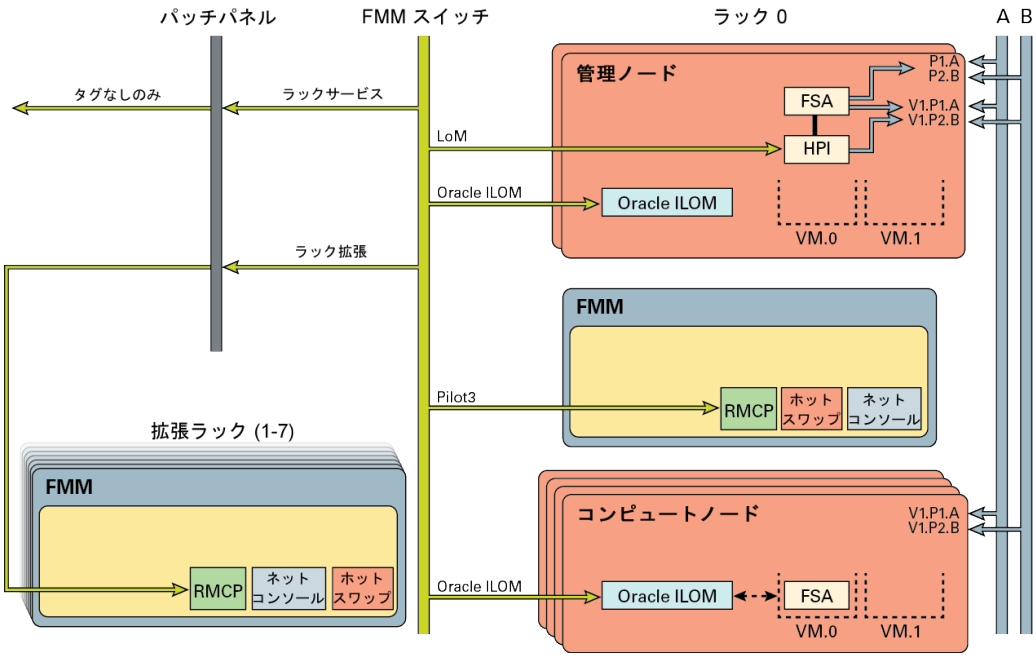
- 11 ページの「デフォルトのネットワーク」
- 12 ページの「ユーザーアカウント」
- 12 ページの「デフォルトのセキュリティー設定」

ご使用のシステムおよび特定環境に関するその他のセキュリティー要件については、組織の IT セキュリティー責任者に確認してください。

デフォルトのネットワーク

次に、Netra Modular System のデフォルトのネットワークの図と説明を示します。

- システム/テレメトリネットワーク (薄い緑色のネットワーク) には、FMM スイッチを介した VLAN 4090 上の管理ノードの LoM ポートが含まれています。
- FMM を使用した内部 VLAN 4094 上のテレメトリ ILOM ネットワークには、FMM スイッチを介したコンピュートノードの Oracle ILOM、およびネットワークノードの Oracle ILOM が含まれています。
- パッチパネルは、テレメトリネットワークをラック 1 - 7 に拡張します。マルチラック構成では、同じサブネットと、異なるラック ID を持つ VLAN がサポートされます
- VLAN(1) は、正しい認証によってテレメトリネットワークにその他のサービスを提供します。
- データネットワーク (A および B) は、FSA ノードへの帯域内アクセスを提供します。
- HA アプリケーションは、モジュラーシステムの公開されたインタフェース (JMX、C- API など) を介してラックを管理できます。



ユーザーアカウント

この表は、モジュラーシステムコンポーネントのデフォルトのユーザーとパスワードの一覧を示しています。Netra Modular System の設置後に、すべてのデフォルトパスワードを変更してください。

コンポーネント	ユーザー名とパスワード
Ethernet スイッチ	`root/changeme` **注記 -** `admin` ユーザーの `enable mode password` 値と `secret` 値をセキュリティー保護します。
管理ノードとコンピュートノード	`root/changeme`

デフォルトのセキュリティー設定

モジュラーシステムには、多くのデフォルトのセキュリティー設定がインストールされています。可能で実用的な場合は常に、セキュアなデフォルト設定を構成してください。`http://www.oracle.com/goto/ILOM/docs` で、使用しているバージョンの Oracle ILOM のデフォルト設定を参照してください。

ハードウェアのセキュリティー保護

物理的な分離とアクセス制御は、セキュリティーアーキテクチャーを構築するための基盤です。物理システムを確実にセキュアな環境に設置することで、不正アクセスからシステムを保護します。同様に、すべてのシリアル番号を記録しておくと、ハードウェアコンポーネントの未承認の使用の防止に役立ちます。

これらのセクションでは、モジュラーシステムのハードウェアの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。

アクセス制限

- システムと関連装置は、アクセスが制限された鍵の掛かった部屋に設置してください。
- 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の保守を行うとき以外はラックのドアに常に鍵を掛けておいてください。ドアに鍵を掛けることで、ホットプラグまたはホットスワップデバイスへのアクセスも制限されます。
- 予備の交換部品はすべて、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、承認された人だけがアクセスするように制限してください。
- ラックと予備のキャビネットの鍵のステータスと整合性を定期的に検証して、改ざんやドアの鍵が掛かっていない状態にならないよう防止または検出します。
- キャビネットの鍵はアクセスが制限されたセキュアな場所に保管します。
- USB コンソールへのアクセスを制限します。システムコントローラ、PDU、ネットワークスイッチなどのデバイスは、USB 接続が可能です。物理アクセスは、ネットワークベースの攻撃の影響を受けないため、よりセキュアにコンポーネントにアクセスできます。
- コンソールを外付けの KVM に接続して、リモートコンソールアクセスを有効にします。KVM デバイスでは多くの場合、ツーファクタ認証、集中管理されたアクセス制御、および監査がサポートされます。KVM のセキュリティーガイドラインとベストプラクティスの詳細は、KVM デバイスに付属のドキュメントを参照してください。

シリアル番号

コンポーネントを受領しインベントリに加えるときにすべてのシリアル番号を慎重に記録することで、ハードウェアコンポーネントの未承認の使用を防止します。すべてのコンポーネントを取り付けたり使用したりする前に、そのシリアル番号をコンポーネントの受領時に記録した番号と比較して信頼性を確認してください。ハードウェアをセキュリティー保護するには次の対策に従ってください。

- 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。
- すべての主要なコンピュータハードウェア項目 (交換部品など) 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。
- ハードウェアのアクティベーションキーとライセンスは、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が、唯一の所有権証明になる場合があります。

ワイヤレスの無線周波数識別 (Radio Frequency Identification、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。http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf にある、Oracle のホワイトペーパー、*RFID を使用した Oracle Sun システムアセットの追跡方法*を参照してください。

ハードドライブ

ハードドライブは多くの場合、機密情報を格納するために使用されます。この情報が不正に開示されないよう保護するため、ハードドライブを再利用、廃止、または廃棄する前にサニタイズしてください。

- データ保護ポリシーを参照して、ハードドライブをサニタイズするために最適な方法を決定してください。
- 必要に応じて、Oracle の Customer Data and Device Retention Service をご活用下さい。

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

ソフトウェアのセキュリティー保護

ほとんどのハードウェアセキュリティーは、ソフトウェア手段を通じて実装されます。これらのセクションでは、Netra Modular System のソフトウェアの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。

▼ 未承認のアクセスを防止する (Oracle Linux)

- **Oracle Linux OS コマンドを使用して、ソフトウェアへのアクセスの制限、OS の強化、セキュリティー機能の使用、およびアプリケーションの保護を実行します。**

  `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html` にある『*Oracle Linux セキュリティ・ガイド リリース6*』を参照してください。

▼ 未承認のアクセスを防止する (Oracle ILOM)

- **Oracle ILOM コマンドを使用して、Oracle ILOM ファームウェアへのアクセスの制限、出荷時に設定されたパスワードの変更、root スーパーユーザーアカウントの使用の制限、および SP へのプライベートネットワークのセキュリティー保護を実行します。**

  `http://www.oracle.com/goto/ILOM/docs` で、使用しているバージョンの『*Oracle ILOM セキュリティーガイド*』を参照してください。

▼ 未承認のアクセスを防止する (Oracle VM Server With Oracle Linux)

- **Oracle Linux コマンドを使用して、Oracle VM Server ソフトウェアへのアクセスの制限、セキュリティー機能の使用、およびアプリケーションの保護を実行します。**

http://docs.oracle.com/cd/E50245_01/E50254/html/index.html にある *Oracle VM Release 3.3 のセキュリティーガイド*を参照してください。

Oracle Hardware Management Pack のセキュリティー

Oracle Hardware Management Pack には、システムを管理するための 2 つのコンポーネント (SNMP モニタリングエージェントと、オペレーティングシステム間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) が備わっています。

- Hardware Management Agent SNMP Plugins – SNMP は、システムをモニターまたは管理する標準のプロトコルです。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 システムをモニターでき、2 つの管理ポイント (ホストと Oracle ILOM) に接続する必要がないという利点が得られます。この機能により、複数のシステムのモニターに単一の IP アドレス (ホストの IP アドレス) を使用できます。

  SNMP Plugins は、Oracle システムのホスト OS で実行します。SNMP Plugin はホスト OS のネイティブの SNMP エージェントを拡張して追加の Oracle MIB 機能を提供します。Oracle Hardware Management Pack 自体には SNMP エージェントは含まれていません。Oracle Linux の場合、モジュールは `net-snmp` エージェントに追加されます。Microsoft 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。Oracle Hardware Management Pack 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。

  SNMPv1 と SNMPv2c 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。よりセキュアな SNMPv3 は暗号化および個々のユーザー名とパスワードを使用してセキュアなチャネルを提供するため、このバージョンを使用することを推奨します。
- Oracle Hardware Management Pack のドキュメント – Oracle Hardware Management Pack に固有のセキュリティーガイドラインについては、http://www.oracle.com/goto/OHMP/docs にある『*Oracle Hardware Management Pack (HMP) セキュリティーガイド*』を参照してください。

関連セキュリティーガイドの場所

セキュリティーガイド

これらのガイドでは、関連製品をセキュアな状態にするためのポリシーと手順について説明しています。

- 『Oracle Server X5-2 Security Guide 』
- 『Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide 』
- http://docs.oracle.com/cd/E37670_01/E36387/html/index.html にある『*Oracle Linux セキュリティ・ガイド リリース6*』
- http://www.oracle.com/goto/ILOM/docs にある『*Oracle ILOM セキュリティーガイド*』
- http://docs.oracle.com/cd/E50245_01/E50254/html/index.html にある *Oracle VM Release 3.3 のセキュリティーガイド*
- http://www.oracle.com/goto/OHMP/docs にある『*Oracle Hardware Management Pack (HMP) セキュリティーガイド*』