Netra Server X3-2 (旧 Sun Netra X4270 M3 サーバー)

セキュリティーガイド

Part No: E35609–01
2012 年 7 月

130425@25097

目次

Netra Server X3-2 セキュリティーガイド

このドキュメントでは、Oracle Netra Server X3-2 (旧 Sun Netra X4270 M3 サーバー)、ネットワークインタフェース、および接続されているネットワークスイッチを保護する際に役立つ一般的なセキュリティーガイドラインを示します。

この章は、次のセクションで構成されています:

システムの概要

Netra Server X3-2 は、2 基のプロセッサを備え、16 基の DDR3 DIMM (1 プロセッサあたり 8 基)、6 基の PCIe Gen3 スロット、8 台または 6 台の SAS/SATA ストレージドライブがサポートされている、エンタープライズクラスの NEBS 認定 2U サーバーです。6 ドライブモデルには DVD も装備されています。

このサーバーのシステムボード上には、Oracle Integrated Lights Out Manager (Oracle ILOM) サービスプロセッサ (SP) が搭載されています。サーバー構成の一部として、設置済みの USB ドライブに Oracle System Assistant と呼ばれるサーバー設定ツールも組み込まれています。

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

  アクセスとは、ハードウェアへの物理的なアクセス、またはソフトウェアへの物理的、または仮想的なアクセスのことを指します。

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

- 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てください。
- サーバーと関連装置は、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。
- アクセスをコネクタまたはポートに制限すると、SSH 接続よりも強力なアクセスを提供できます。システムコントローラ、配電盤、ネットワークスイッチなどのデバイスには、コネクタおよびポートが搭載されています。
- 特にホットプラグまたはホットスワップのデバイスは簡単に取り外すことができるため、これらのデバイスにアクセスを制限してください。
- 予備の現場交換可能ユニットおよび顧客交換可能ユニットは、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、承認された人だけがアクセスするように制限してください。

- 認証

  認証とは、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することを指します。

  - 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。
  - ユーザーアカウントの場合は、必要に応じてアクセス制御リストを使用してください。延長セッションにはタイムアウトを設定し、ユーザーに権限レベルを設定します。

- 承認

  承認とは、ハードウェアやソフトウェアを操作する担当者に課せられた制限のことを指します。

  - 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、および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

  アカウンティングとは、ログインアクティビティーの監視およびハードウェア目録の保守で使用されるソフトウェアおよびハードウェアの機能のことを指します。

  - 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監視してください。

- 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。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。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。
- コンポーネントを検出および追跡するには、コンピュータハードウェアのすべての主要品目 (FRU など) にセキュリティーマークを付けます。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。

サーバー構成および管理ツールの使用

ソフトウェアおよびファームウェアのツールを使用してサーバーを構成および管理するときは、次のセキュリティーガイドラインに従ってください。

Oracle System Assistant のセキュリティー

Oracle System Assistant は、サーバーハードウェアをローカルまたはリモートで構成および更新したり、サポートされているオペレーティングシステムをインストールしたりする際に役立つインストール済みのツールです。Oracle System Assistant を使用する方法については、次の場所にあるサーバーの『管理ガイド』を参照してください。

http://docs.oracle.com/cd/E27124_01

次の情報は、Oracle System Assistant に関するセキュリティー問題を理解する際に役立ちます。

- **Oracle System Assistant** にはブート可能なルート環境が含まれます。

Oracle System Assistant は、設置済みの内蔵 USB フラッシュドライブで実行されるアプリケーションです。ブート可能な Linux ルート環境上に構築されます。Oracle System Assistant には、基盤となるルートシェルにアクセスする機能も用意されています。システムに物理的にアクセスするユーザーや、Oracle ILOM 経由でシステムにリモート KVMS (キーボード、ビデオ、マウス、およびストレージ) アクセスするユーザーは、Oracle System Assistant およびルートシェルにアクセスできます。

ルート環境を使用すると、システム構成およびポリシーを変更したり、その他のディスク上のデータにアクセスしたりできます。サーバーへの物理的なアクセスを保護し、Oracle ILOM ユーザーに対する管理者権限およびコンソール権限を慎重に割り当てることをお勧めします。

- **Oracle System Assistant** では、オペレーティングシステムにアクセス可能な **USB** ストレージデバイスがマウントされます。

Oracle System Assistant はブート可能な環境であることに加えて、インストール後にホストオペレーティングシステムにアクセス可能な USB ストレージデバイス (フ

ラッシュドライブ) としてマウントされます。これは、保守および再構成のためにツールやドライバにアクセスする際に役立ちます。Oracle System Assistant の USB ストレージデバイスは、読み取りと書き込みの両方が可能であり、ウイルスによって攻撃される可能性があります。

定期的なウイルススキャンや整合性チェックなど、ディスクを保護するときと同じ方法を Oracle System Assistant のストレージデバイスにも適用することをお勧めします。

- **Oracle System Assistant** は無効にできます。

Oracle System Assistant は、サーバーの設定、ファームウェアの更新と構成、およびホストオペレーティングシステムのインストールの際に役立つ便利なツールです。ただし、前述のセキュリティーによる影響が受け入れられない場合や、ツールが必要ない場合は、Oracle System Assistant を無効にすることができます。Oracle System Assistant を無効にすると、USB ストレージデバイスがホストオペレーティングシステムにアクセスできなくなります。さらに、Oracle System Assistant のブートもできなくなります。

Oracle System Assistant はツール自体または BIOS から無効にすることができます。Oracle System Assistant を無効にしたら、BIOS 設定ユーティリティーからしか再度有効にすることはできません。承認されたユーザーのみが Oracle System Assistant を再度有効にできるように、BIOS 設定をパスワードで保護することをお勧めします。Oracle System Assistant を無効にして再度有効にする方法については、サーバーの『管理ガイド』を参照してください。

Oracle ILOM のセキュリティー

サーバー、その他の Oracle x86 ベースのサーバー、および一部の Oracle SPARC ベースのサーバーにインストール済みの Oracle Integrated Lights Out Manager (Oracle ILOM) 管理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積極的にセキュリティー保護、管理、および監視できます。

一般的なネットワークから切り離すには、サービスプロセッサ専用のネットワークを使用します。`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。その代わりに、可能なかぎり `ilom-operator` や `ilom-admin` などの Oracle ILOM アカウントを割り当ててください。新規システムのインストール時に、デフォルトのパスワードをすべて変更してください。ほとんどの種類の装置では、`changeme` のようなデフォルトのパスワードが使用されています。このパスワードは広く知られているため、承認されていないユーザーによって装置にアクセスされる可能性があります。

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)、RADIUS 認証など) 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 3.1 のドキュメントライブラリに含まれ

る『Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide』を参照してください。Oracle ILOM 3.1 のドキュメントは次の場所で検索できます:

http://docs.oracle.com/cd/E24707_01

Oracle Hardware Management Pack のセキュリティー

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、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 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、複数のサーバーおよびサーバーモジュールの監視に単一の 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 サーバーのホストオペレーティングシステム上で実行します。

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、その他の Linux バリアント、および Microsoft Windows オペレーティングシステムで動作します。

これらの機能の詳細については、Oracle Hardware Management Pack のドキュメントを参照してください。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、Oracle Hardware Management Pack のドキュメントライブラリに含まれる『Oracle Hardware Management Pack (HMP) Security Guide』を参照してください。Oracle Hardware Management Pack のドキュメントは次の場所で検索できます:

http://docs.oracle.com/cd/E20451_01

セキュアな環境の計画

サーバーおよび関連する装置をインストールして構成するときは、次の情報を使用してください。

Oracle オペレーティングシステムのガイドライン

次の詳細については、Oracle オペレーティングシステム (OS) のドキュメントを参照してください:

- システムの構成時にセキュリティー機能を使用する方法
- システムにアプリケーションやユーザーを追加する場合のセキュアな運用方法
- ネットワークベースのアプリケーションを保護する方法

サポートされている Oracle オペレーティングシステムに関するセキュリティーガイドドキュメントは、オペレーティングシステムのドキュメントライブラリに含まれています。Oracle オペレーティングシステムに関するセキュリティーガイドドキュメントを検索するには、Oracle オペレーティングシステムのドキュメントライブラリに移動します:

- **Oracle Solaris** - `http://docs.oracle.com/cd/E23824_01`
- **Oracle Linux** - `http://linux.oracle.com/documentation/`
- **Oracle VM** - `http://www.oracle.com/technetwork/documentation/vm-096300.html`

ネットワークポートとネットワークスイッチ

提供されるポートセキュリティー機能のレベルはスイッチによって異なります。次の実行方法については、スイッチのドキュメントを参照してください。

- スイッチへのローカルアクセスとリモートアクセスには、認証、承認、アカウンティング機能を使用してください。
- デフォルトで複数のユーザーアカウントとパスワードを持っている可能性のあるネットワークスイッチで、すべてのパスワードを変更してください。
- スイッチの管理は、帯域外で (データトラフィックと切り離して) 行なってください。帯域外管理を実現できない場合は、帯域内管理用に専用の仮想ローカルエリアネットワーク (VLAN) 番号を用意してください。
- 侵入検知システム (IDS) のアクセスには、ネットワークスイッチのポートのミラー化機能を使用してください。
- スイッチの構成ファイルはオフラインで管理し、承認された管理者しかアクセスできないようにしてください。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。
- 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。
- スイッチに次のようなポートセキュリティー機能がある場合は、これらの機能を使用してください。
  - **MAC Locking** では、接続された 1 つ以上のデバイスのメディアアクセス制御 (MAC) アドレスがスイッチの物理ポートに関連付けられます。スイッチのポートを特定の MAC アドレスに固定すると、スーパーユーザーによるバックドアの作成を防ぎ、不正アクセスポイントを利用したネットワークへのアクセスを防止することができます。
  - **MAC Lockout** では、指定した MAC アドレスからのスイッチへの接続を無効にします。
  - **MAC Learning** では、ネットワークスイッチが現在の接続に基づいてセキュリティーを設定できるように、各スイッチポートの直接接続に関する情報を使用します。

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) を設定する場合は、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、VTP を透過モードに設定してください。

Infiniband のセキュリティー

Infiniband ホストをセキュアな状態にしてください。Infiniband ファブリックのセキュリティーは、もっともセキュリティーが低い Infiniband ホストに依存します。

- パーティションを分割しても Infiniband ファブリックを保護する効果はないことに注意してください。パーティション分割は、ホストの仮想マシン間で Infiniband のトラフィックを分散させる機能です。
- VLAN を構成する際、可能な場合は静的 VLAN を使用してください。
- スイッチの未使用のポートは無効にし、未使用の VLAN 番号を割り当ててください。

セキュアな環境の保守

初期インストールおよび構成が終了したら、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。

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。詳細については、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

目録を追跡するには、シリアル番号を使用します。Oracle のシリアル番号は、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。Oracle のホワイトペーパー『How to Track Your Oracle Sun System Assets by Using RFID』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

サーバー装置上のソフトウェアとファームウェアは、最新のバージョンに保ってください。

- 更新を定期的にチェックしてください。
- 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。
- ネットワークスイッチなどのデバイスにはファームウェアも搭載され、パッチやファームウェア更新が必要な場合もあることを忘れないでください。

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。

- 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。
- 簡易ネットワーク管理プロトコル (SNMP) バージョン 3 を使用して、転送をセキュリティー保護してください。古いバージョンの SNMP 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を強力なコミュニティー文字列に変更してください。一部の製品では、デフォルトの SNMP コミュニティー文字列として PUBLIC が設定されています。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。

- システムコントローラでブラウザインタフェースを使用する場合は、使用後に必ずログアウトしてください。
- 伝送制御プロトコル (TCP) またはハイパーテキスト転送プロトコル (HTTP) などの不要なネットワークサービスを無効にしてください。必要なネットワークサービスについては、有効にしてセキュアに構成してください。

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、次のガイドラインに従ってください。

- 重要なデータは、外付けハードドライブ、ペンドライブ、メモリースティックなどのデバイスを使用してバックアップしてください。バックアップしたデータは、遠隔地のセキュアな場所に保管してください。
- 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。
- 古いハードドライブを廃棄するときは、ドライブを物理的に破壊するか、ドライブ上のすべてのデータを完全に消去してください。ファイルが削除されたあとや、ドライブが再フォーマットされたあとでも、情報はドライブから回復できます。ファイルを削除しても、またはドライブを再フォーマットしても、ドライブ上のアドレステーブルしか削除されません。ドライブ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。

ログの保守

ログファイルは定期的に検査および保守してください。次の方法を使用して、ログファイルをセキュリティー保護してください。

- ログ記録を有効にし、専用のセキュアなログホストにシステムログを送信してください。
- ネットワークタイムプロトコル (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グ記録を構成してください。
- 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、定期的にアーカイブし、リセットしてください。アーカイブしたファイルは参照したり、統計的な分析のために使用できます。