Netra Blade X3-2B (旧 Sun Netra X6270 M3 サーバーモジュール)

セキュリティーガイド

Part No: E37771–01
2012 年 9 月

121030@25097

目次

概要

この概要では、次のトピックについて説明します。

製品の概要

Sun Blade X6270 M3 サーバーモジュールは、2P (2 基のプロセッサ) 構成をサポートするエンタープライズクラスのサーバーブレードです。サーバーモジュールには、標準の Sun Blade 6000 シャーシブレードフォームファクタ、レイアウト、通気、および RAID 拡張モジュール (REM) とファブリック拡張モジュール (FEM) との互換性があります。Sun Blade X6270 M3 サーバーモジュールは、E5-2600 ファミリの 2 基の Intel(R) Xeon(R) プロセッサと、Intel C600 シリーズチップセットに基づいています。Sun Blade X6270 M3 サーバーモジュールには、Oracle ILOM サービスプロセッサ (SP) が搭載されています。

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、ログイン操作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。
- 目録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。

セキュアな環境の計画

このセクションでは、サーバーおよび関連装置の設置と構成の実行前および実行時に使用するガイドラインを示します。

次のトピックで構成されています。

ハードウェアの物理的なセキュリティー

物理的なハードウェアのセキュリティー保護方法は非常にシンプルで、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の 2 つです。

次のトピックで構成されています。

アクセスを制限する

- 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。装置を保守したあとはドアに鍵を掛けてください。
- SSH 接続よりも強力なアクセスを提供できるように、USB コンソールへのアクセスを制限してください。システムコントローラ、配電盤 (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。
- 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、これらのデバイスへの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 (FRU) または顧客交換可能ユニット (CRU) を保管してください。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。

シリアル番号を記録する

- すべての主要なコンピュータハードウェア (FRU 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。
- 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。
- 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、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。

- 新しいシステムをインストールする際は、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。
- 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。
- 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。可能な限り、Oracle Integrated Lights Out Manager (Oracle ILOM) の ilom-operator や ilom-admin などのアカウントを代わりに使用するようにします。
- サービスプロセッサには、一般的なネットワークと区別した専用のネットワークを使用してください。
- USB コンソールへのアクセスを保護してください。システムコントローラ、配電盤 (PDU)、ネットワークスイッチなどのデバイスの USB 接続では、SSH 接続よりも強力なアクセスが提供されます。
- 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。
- 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。

Oracle ILOM ファームウェア

Oracle Integrated Lights Out Manager (Oracle ILOM) を使用して、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、および監視できます。Oracle ILOM 管理ファームウェアは、Sun Netra X6270 M3 サーバーモジュール 上の SP に事前にインストールされています。

このファームウェアを使用したパスワードの設定、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) の適用に関する詳細については、Oracle Integrated Lights Out Manager (Oracle ILOM) のドキュメントを参照してください。

http://www.oracle.com/pls/topic/lookup?ctx=ilom31

オペレーティングシステムのセキュリティーガイドライン

オペレーティングシステム	リンク
Oracle Solaris OS	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Oracle Linux OS	http://linux.oracle.com/documentation/
Windows OS	Oracle 以外のオペレーティングシステムについては、ベンダーのドキュメントを参照してください。
Oracle VM OS	http://www.oracle.com/technetwork/documentation/vm-096300.html
VMware OS	Oracle 以外のオペレーティングシステムについては、ベンダーのドキュメントを参照してください。

Oracle System Assistant のセキュリティー情報

次のインストール後のトピックで構成されています。

- 9 ページの「OSA にブート可能なルート環境が含まれることを理解する」
- 10 ページの「OSA によって OS 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ることを理解する」
- 10 ページの「OSA を無効にする」

OSA にブート可能なルート環境が含まれることを理解する

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。OSA 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、ILOM 経由でシステムにリモート KVMS アクセスするユーザーは、OSA 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、ILOM 構成およびシステム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、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。また、オペレーティングシステムのファイルシステムを暗号化すると、OSA のルートシェルユーザーがディスクの内容を読み取ることができなくなります。

OSA によって OS 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ることを理解する

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。OSA フラッシュ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 OSA 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。

OSA を無効にする

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に役立つツールです。ただし、前述のセキュリティーの影響が望ましくない場合や、単にツールが必要でない場合は、OSA 自体を無効にすることもできます。OSA 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、OSA 自体または BIOS から無効にすることができます。一度無効にしたら、BIOS 設定からしか再度有効にすることができません。承認されたユーザーのみが OSA 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 のドキュメントで OSA を無効にする手順を確認するか、『Netra Blade X3-2B 管理者ガイド』を参照してください。

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資産の追跡を続行してください。

次のトピックで構成されています。

Oracle ILOM のセキュリティー

Oracle Integrated Lights OutManager (Oracle ILOM) の詳細については、『Oracle ILOM セキュリティーガイド』を参照してください。

一般的な Oracle ILOM の情報については、次を参照してください。

`http://www.oracle.com/pls/topic/lookup?ctx=ilom31`

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の保守

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。
- 装置にインストールするソフトウェアやファームウェアのバージョンは、常に最新のものを使用してください。
- 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や ExpressModule に搭載されたファームウェアには、パッチやファームウェア更新が必要なものもあります。

ローカルアクセスとリモートアクセス

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

- LDAP を使用してシステムにアクセスする際は、LDAP のセキュリティー対策に従ってください。『Oracle ILOM セキュリティーガイド』を参照してください。
- 無許可のアクセスを禁止することを明記したバナーを作成してください。
- 必要に応じて、アクセス制御リストを使用してください。
- 拡張セッションのタイムアウトを設定し、特権レベルを設定してください。
- 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 (AAA) 機能を使用してください。
- 可能な場合は、RADIUS および TACACS+ セキュリティープロトコルを使用してください。

    - RADIUS (Remote Authentication Dial In User Service) は、無許可のアクセスからネットワークをセキュリティー保護するクライアント/サーバープロトコルです。
    - TACACS+ (Terminal Access Controller Access-Control System) は、リモートアクセスサーバーと認証サーバーの通信を確立して、ユーザーがネットワークにアクセスできるかどうかを判定するプロトコルです。
- 侵入検知システム (IDS) のアクセスには、スイッチのポートのミラー化機能を使用してください。
- 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。
- 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。転送がセキュリティー保護されるのは SNMP バージョン 3 だけです。
- 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。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。
- 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。
- 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情報を保存してください。
- 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。

データのセキュリティー

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。

- データの破棄: 古いハードドライブを処分する際は、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。すべてのファイルを削除したり、ドライブを再フォーマットしたりしても、ドライブ上のアドレステーブルしか削除されず、ファイルの削除やドライブの再フォーマット後にドライブから情報を復元できてしまいます。(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。)