SuperCluster システム

セキュリティーガイド

Part No: E48454-01
2013 年 7 月

目次

・・・第 1 章

SuperCluster システム セキュリティーガイド

このドキュメントでは、Oracle のサーバー、ネットワークスイッチ、ネットワークインタフェースカードなどのハードウェア製品の保護に役立つ、全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。

セキュリティーの原則について

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、物理的な制御とソフトウェアの制御が必要です。
  - 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、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

  プラットフォームオペレーティングシステムには、ユーザーを確認するための認証機能が必ず用意されています。

  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。
- 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。これを実現するために、システム管理者は、読み取り/書き込み/

実行の許可で構成されるシステムを構築して、コマンド、ディスクスペース、デバイス、およびアプリケーションに対するユーザーアクセスを制御します。

- アカウンティング

  Oracle のソフトウェアおよびハードウェアには、顧客の IT 部門がログイン活動の監視やハードウェアインベントリの保守を行える機能が用意されています。

  - ユーザーのログインはシステムログで監視できます。特に、システム管理者アカウントとサービスアカウントについては、強力なコマンドにアクセスできるため、システムログで注意して監視する必要があります。ログは一般に長期にわたって保持されるため、顧客の企業ポリシーに従って、ログファイルが特定のサイズを超えたら定期的にリタイアすることが重要です。
  - 顧客の IT 資産は、通常はシリアル番号で追跡されます。Oracle のパーツ番号は、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、インベントリの管理に使用できます。

セキュアな環境の計画

サーバーおよび関連装置を設置して構成するときは、実行前および実行時に次の点に注意してください。

ハードウェアのセキュリティー

物理的なハードウェアのセキュリティーは非常に単純に保護できます。ハードウェアへのアクセスを制限し、シリアル番号を記録するだけです。

- 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。
  - ホットプラグまたはホットスワップに対応したデバイスは取り外しが簡単であるため、アクセスの制限に特に注意してください。
  - 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) 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のアクセスは、承認された人だけ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項目 (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、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。

ソフトウェアのセキュリティー

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。

- 新しいシステムを設置したら、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。また、ネットワークスイッチなどのデバイスには、デフォルトで複数のユーザーアカウントが設定されている場合もあります。必ずすべてのアカウントのパスワードを変更するようにしてください。

- `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。可能なかぎり、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てください。
- サービスプロセッサには、一般的なネットワークから分離された専用のネットワークを使用してください。
- Oracle Solaris のインストールプロセスでは、ユーザーアカウントとパスワード、およびシステムの **root** パスワードを入力するように求められます。このプロセスの一環として、**root** ユーザーの役割が割り当てられます。このアカウントの設定を変更する場合は、**root** ユーザーアカウントを削除し、より特権が少ないユーザーに root の役割を割り当てます。
- 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では USB 接続が可能であり、SSH 接続よりも強力なアクセスを提供する可能性があります。
- 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ます。
- WAN ブートや iSCSI ブートを使用すると、サーバーをセキュアに起動できます。詳細は、ご使用の Oracle Solaris リリースの『*Oracle Solaris インストールガイド (ネットワークインストール)*』を参照してください。

Oracle Solaris セキュリティーガイドラインのドキュメントでは、次の情報が提供されます。

- Oracle Solaris を強化する方法
- システムの構成時に Oracle Solaris の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

Oracle Solaris のセキュリティーガイドラインのドキュメントは、次のページから参照できます。

- http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

ファームウェアのセキュリティー

OpenBoot PROM (OBP) などの Oracle のファームウェアは、通常のユーザーアカウントでは編集できません。Oracle Solaris オペレーティングシステムでは、制御されたファームウェア更新プロセスを使用して、無許可のファームウェアの変更を防止しています。更新プロセスを使用できるのはスーパーユーザーだけです。

OBP のセキュリティー変数の設定については、『*OpenBoot 4.x Command Reference Manual*』を参照してください。

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM ファームウェア

Oracle ILOM (Oracle Integrated Lights Out Manager) は、一部の SPARC サーバーにプリインストールされているシステム管理ファームウェアです。Oracle ILOM を使用すると、システムにインストールされたコンポーネントをアクティブに管理および監視できます。Oracle ILOM の使用方法によっては、システムのセキュリティーが影響を受けます。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は、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=E19860-01

セキュアな環境の保守

Oracle のハードウェアとソフトウェアには、ハードウェアの制御やアセットの追跡のためのセキュリティー機能が多数用意されています。

ハードウェアの制御

Oracle の一部のシステムでは、オンとオフをソフトウェアのコマンドで設定できます。また、ソフトウェアのコマンドを使用してリモートから配電盤 (Power Distribution Unit、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

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に搭載された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をローカルエリアネットワーク接続で読み取ることで、インベントリの追跡に使用できます。

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。*RFID を使用した Oracle Sun システムアセットの追跡方法*に関する Oracle のホワイトペーパーを参照してください。

- http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

ソフトウェアとファームウェア

- 装置には、常に最新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。ネットワークスイッチなどのデバイス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。
- 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。

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。

- 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との通信を許可して、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。
- インストーラによる SuperCluster システム の設定が完了すると、システムのセキュリティー対策として、SSH キーがすべて無効になり、パスワードもすべて期限切れになります。SSH キーを無効にしない場合やパスワードを期限切れにしない場合は、SuperCluster システム のインストールの終了時にインストーラで指定してください。
- 古いバージョンの SNMP では、認証データがセキュリティーで保護されないため、暗号化されずに転送されます。SNMP のバージョン 3 だけがセキュアな転送を提供できます。
- 一部の製品は、デフォルトの SNMP コミュニティー文字列として PUBLIC が設定された状態で出荷されています。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。
- 可能性があるインシデントをログで確認し、セキュリティーポリシーに従ってそれらをアーカイブしてください。
- 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。
- 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。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、ファイルを削除したり、ドライブを再フォーマットしたあとにドライブから情報を復元できます。(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。)

ネットワークのセキュリティー

ネットワーク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。

- ほとんどのスイッチでは、仮想ローカルエリアネットワーク (Virtual Local Area Network、VLAN) を定義できます。スイッチを使用して VLAN を定義する場合は、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。
- 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 VLAN 番号を用意してください。
- 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。
- 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。
- 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。
- 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ます。次に、VTP を透過モードに設定します。
- TCP スモールサーバーや HTTP など、不要なネットワークサービスは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。
- 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。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 固定 (Locking): 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できます。
  - MAC ロックアウト (Lockout): 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 学習 (Learning): スイッチのポートごとに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、各ポートの直接接続に関する情報を収集します。

関連セキュリティーガイド

SuperCluster システム で使用されるソフトウェアおよびハードウェアの各コンポーネントにも、そのコンポーネント固有のセキュリティーガイドが提供されているものがあります。SuperCluster システム で使用されるコンポーネントと、そのコンポーネント固有のセキュリティーガイドの場所 (セキュリティーガイドが提供されている場合) を次に示します。

- SPARC T4-4 サーバー:

  http://www.oracle.com/pls/topic/lookup?ctx=E23411_01
- SPARC T5-8 サーバー:

  http://www.oracle.com/pls/topic/lookup?ctx=E35078_01
- Sun ZFS Storage 7320 アプライアンス:

  http://www.oracle.com/pls/topic/lookup?ctx=ZFS_Storage_7x20_2011.1
- Sun Datacenter InfiniBand Switch 36 スイッチ:

  http://www.oracle.com/pls/topic/lookup?ctx=E19197-01
- Exadata Storage Server: Exadata Storage Server の **/opt/oracle/cell/doc** ディレクトリにインストールされるドキュメント
- Oracle Solaris オペレーティングシステム:

  http://www.oracle.com/technetwork/documentation/index.html#sys_sw