Oracle SuperCluster M7 シリーズセキュリティーガイド

Part No: E69648-01
2016 年 2 月

Part No: E69648-01

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

このドキュメントの使用法

- **概要** – Oracle SuperCluster M7 シリーズシステムのセキュアな環境の計画、構成、および保守に関する情報を提供します。
- **対象読者** – 技術者、システム管理者、および認定サービスプロバイダ
- **前提知識** – UNIX およびデータベース管理に関する豊富な経験。

製品ドキュメントライブラリ

この製品および関連製品のドキュメントとリソースは http://www.oracle.com/goto/sc-m7/docs で入手可能です。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお寄せください。

セキュリティーの原則について

このガイドでは、Oracle SuperCluster M7 シリーズシステムのセキュアな環境の計画、構成、および保守に関する情報を提供します。

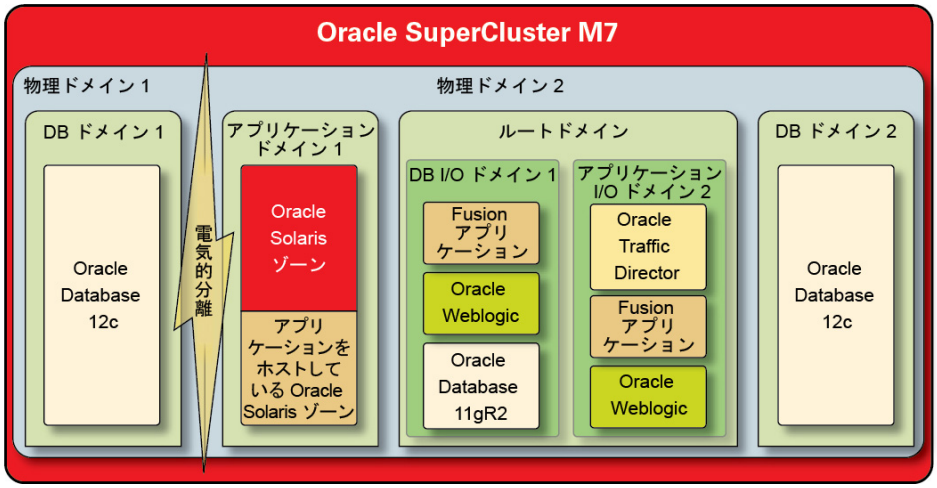
このセクションでは、これらのトピックについて説明します。

セキュアな分離

SuperCluster M7 は、セキュリティーおよび保証の要件に基づいてクラウドプロバイダが選択できるさまざまな分離方針をサポートしています。この柔軟性により、クラウドプロバイダはその業務に合わせてカスタマイズされたセキュアなマルチテナントアーキテクチャーを作成できます。

SuperCluster M7 は、数多くのワークロード分離方針をサポートし、それぞれ独自に一意となる一連の機能をサポートしています。各実装方針は独立して使用できますが、ハイブリッドなアプローチで一緒に使用することもできるため、クラウドプロバイダはセキュリティー、パフォーマンス、可用性の要件、およびその他の要件のバランスを一層効果的にできるようにアーキテクチャーを配備できます。

図 1 動的なテナント構成によるセキュアな分離



クラウドプロバイダは、テナントホストが物理的にほかの作業負荷から分離される必要があるアプリケーションとデータベースを実行している状況で、物理ドメイン (PDomain とも呼ばれる) を使用できます。組織にとっての重大度、含まれる情報の機密性、コンプライアンス義務のために、または単にデータベースやアプリケーションの作業負荷によって物理システム全体のリソースをフルに利用するために、配備には専用の物理リソースが必要になることがあります。

ハイパーバイザが調停する分離を必要とする組織では、アプリケーションやデータベースのインスタンスを分離する仮想環境を作成するために、Oracle VM Server for SPARC ドメイン (専用ドメインと呼ばれます) が使用されます。SuperCluster インストールの一部として作成される専用ドメインは、それぞれ独自で一意のインスタンスの Oracle Solaris OS を実行します。物理リソースへのアクセスは、SPARC プロセッサに組み込まれたハードウェア支援ハイパーバイザによって調停されます。

さらに、SuperCluster では、ルートドメインと呼ばれる追加のドメインを作成して、シングルルート I/O 仮想化 (SR-IOV) テクノロジを利用できます。ルートドメインは、1 つまたは 2 つの IB HCA および 10 GbE NIC を持ちます。ルートドメインの上に、I/O ドメインと呼ばれる追加のドメインを動的に作成できます。SuperCluster M7 には、それらを作成および管理するブラウザベースのツールが含まれています。

ただし、これらの各ドメイン内では、クラウドコンシューマテナントは Oracle Solaris ゾーンテクノロジを活用して、追加の分離された環境を作成できます。ゾーンを使用して、アプリケーションやデータベースのインスタンスの個々のインスタンス、また

はアプリケーションやデータベースのグループを、単一の OS カーネルの上で一括して実行される 1 つ以上の仮想化コンテナに配備できます。仮想化に対するこの軽量アプローチは、配備されるサービスに関する強力なセキュリティー境界を作成するために使用されます。

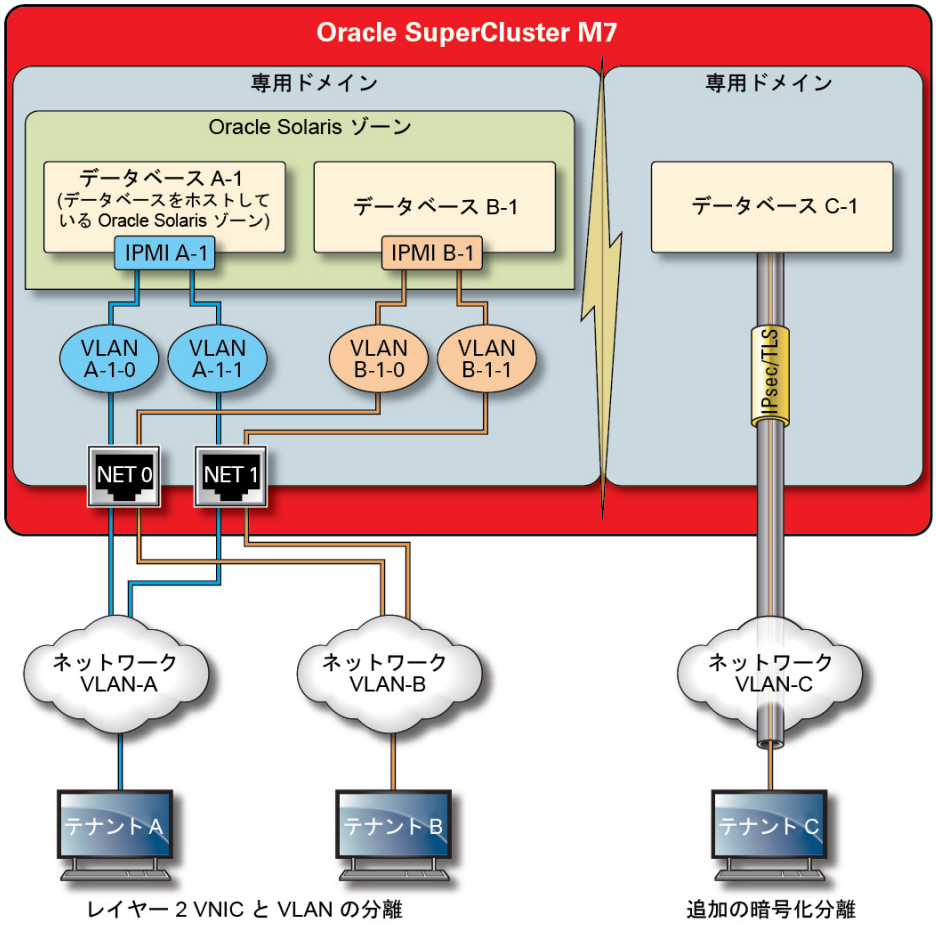
SuperCluster 上の複数のアプリケーションやデータベースをホストしているテナントは、クラウドインフラストラクチャーのニーズに合わせて柔軟性と回復性を備えたアーキテクチャーを作成するために、Oracle Solaris ゾーン、I/O ドメイン、および専用ドメインに基づいて分離方針の組み合わせを使用するハイブリッドアプローチを採用することもできます。仮想化オプションのホストでは、SuperCluster はクラウドにホストされるテナントをハードウェア層でセキュアに分離でき、実行時環境での強化されたセキュリティーとさらなる分離のために Oracle Solaris ゾーンを提供します。

個々のアプリケーション、データベース、ユーザー、プロセスがホスト OS 上で適切に分離されたことを確認することは、よい最初の手順です。ただし、SuperCluster で使用される 3 つのプライマリネットワークと、ネットワーク分離機能およびネットワーク上を流れる通信を保護する方法を考慮することも同様に重要です。

- 10 GbE クライアントアクセスネットワーク
- プライベート IB サービスネットワーク
- 管理ネットワーク

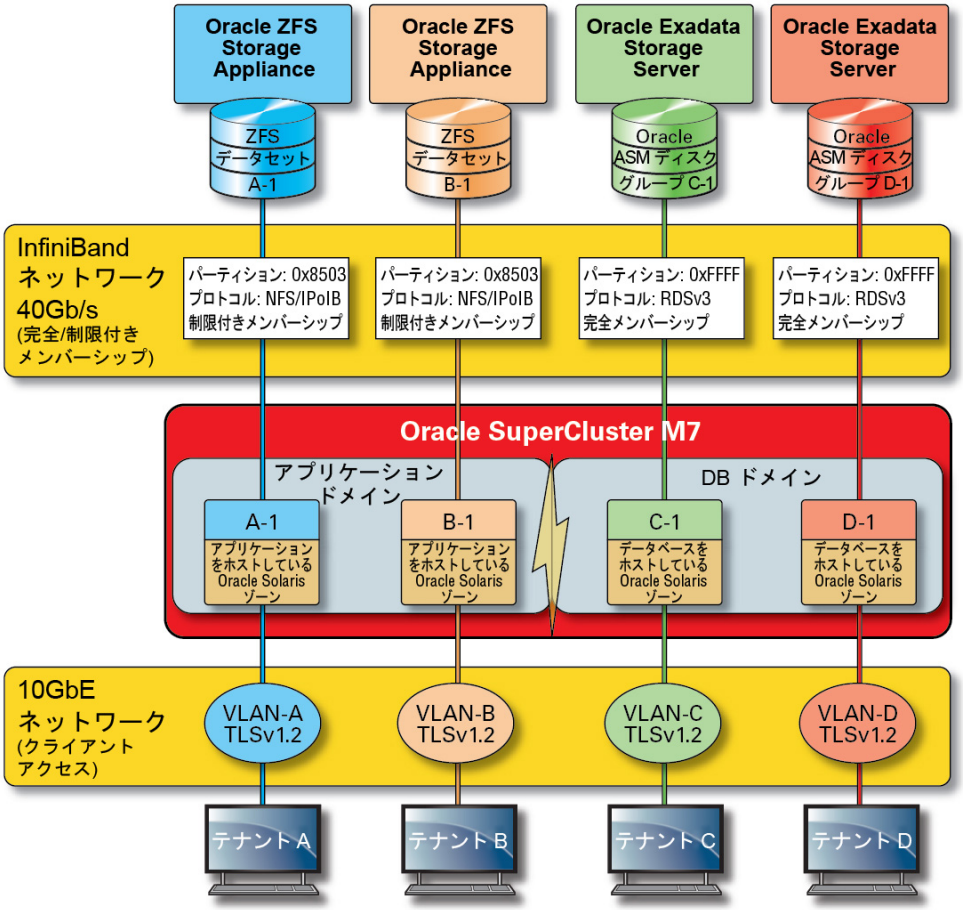
SuperCluster クライアントアクセスネットワーク上を流れるネットワークトラフィックは、さまざまな手法を使用して分離できます。この図では、4 つのデータベースインスタンスが 3 つの異なる仮想 LAN (VLAN) 上で動作するように構成されている可能性のある構成の 1 つを示しています。VLAN を使用するように SuperCluster のネットワークインタフェースを構成することによって、Oracle VM Server for SPARC 専用ドメイン間および Oracle Solaris ゾーン間で、ネットワークトラフィックを分離できます。

図 2 クライアントアクセスネットワーク上でのセキュアなネットワーク分離



SuperCluster には、Exadata ストレージサーバーと ZFS Storage Appliance 上に格納されている情報にアクセスするため、およびクラスタ化および高可用性に必要な内部通信を実行するために、データベースインスタンスによって使用されるプライベート IB ネットワークが含まれています。この図は、SuperCluster M7 上のセキュアなネットワーク分離を示しています。

図 3 40 Gbs IB ネットワーク上でのセキュアなネットワーク分離



デフォルトでは、SuperCluster IB ネットワークは、インストールおよび構成中に 6 つのパーティションに分割されます。デフォルトのパーティションを変更することはできませんが、Oracle では IB ネットワークのさらなるセグメントが必要な状況での追加の専用パーティションの作成と使用をサポートしています。さらに、IB ネットワークでは、制限と完全の両方のパーティションメンバーシップの概念をサポートしています。制限メンバーは完全メンバーのみと通信できるのに対し、完全メンバーはパーティション上のすべてのノードと通信できます。アプリケーション I/O ドメインおよび Oracle Solaris 11 ゾーンは、それぞれの IB パーティションの制限メンバーとして構成できます。これにより、その同じパーティションに存在する可能性があるその他の

制限メンバーシップノードではなく完全メンバーとして構成されている ZFS Storage Appliance のみと通信できることが保証されます。

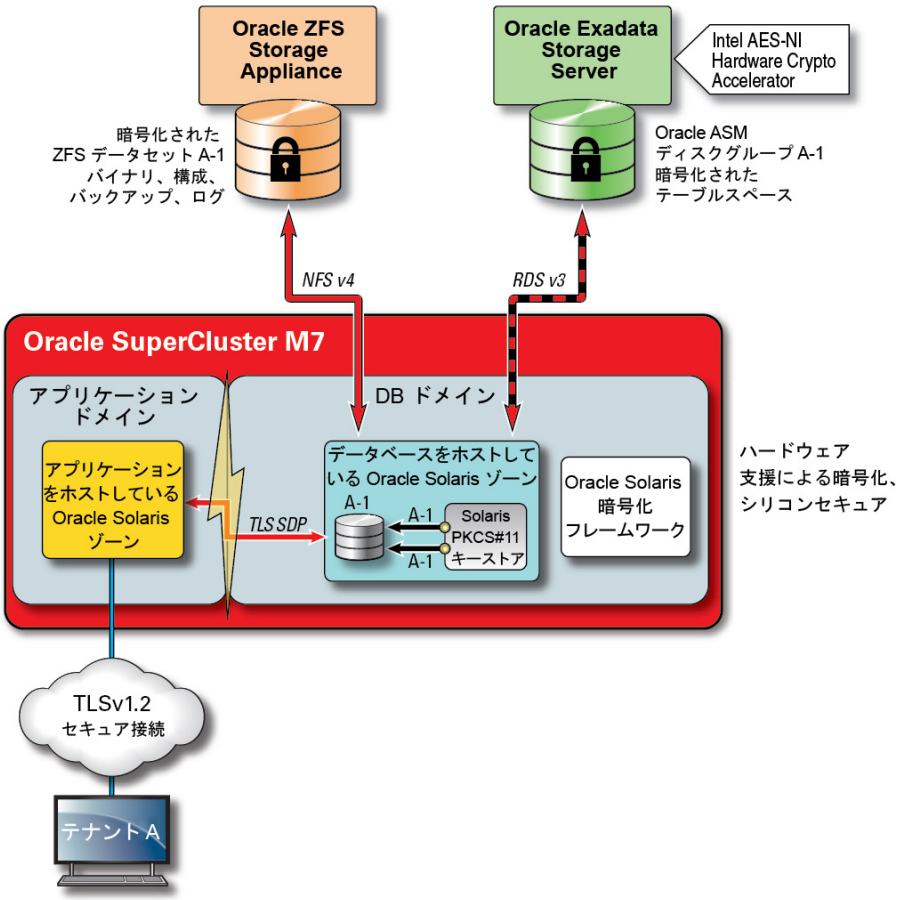
SuperCluster には、すべてのコアコンポーネントを管理およびモニターできるように使用される専用の管理ネットワークも含まれます。この方針により、機密性の高い管理およびモニタリング機能を、クライアントリクエストを処理するために使用されるネットワークパスから分離できます。管理機能をこの管理ネットワークに分離することで、SuperCluster は、クライアントアクセスおよび IB ネットワークを介して公開されるネットワーク攻撃対象領域をさらに削減できます。クラウドプロバイダはこの推奨プラクティスに従い、管理、モニタリング、および関連する機能を分離してそれらが管理ネットワークからのみアクセスできるようにすることを強くお勧めします。

データ保護

クラウドプロバイダにとって、データ保護はセキュリティー戦略の核心です。プライバシとコンプライアンス義務の重要性を考えると、マルチテナントアーキテクチャーを検討する組織は、データベースを出入りする情報を保護するために暗号化の使用を強く検討するべきです。データ保護には暗号化サービスの使用がシステム上適用されるため、情報がネットワークを流れるときとディスク上に存在するときに情報の機密性と整合性が保証されます。

セキュリティーが重要な IT 環境のデータ保護ニーズを満たすため、SuperCluster の SPARC M7 プロセッサはハードウェア支援の高パフォーマンス暗号化を容易にします。SPARC M7 プロセッサは、メモリースクラップ、サイレントメモリー破壊、バッファーオーバーラン、および関連攻撃などの悪質なアプリケーションレベルの攻撃を確実に防止するための Silicon Secured Memory テクノロジも採用しています。

図 4 ハードウェア支援暗号化アクセラレーションとメモリー侵入保護によって提供されるデータ保護



セキュアなマルチテナントアーキテクチャーでは、データ保護がアーキテクチャーのほぼあらゆる側面に影響を与えるため、SuperCluster とそのサポートするソフトウェアにより、組織ではパフォーマンスを犠牲にする必要なしにセキュリティーとコンプライアンスの目標を満たすことができます。SuperCluster は、暗号化操作を加速したりメモリー侵入保護を保証したりしながらパフォーマンスに影響を与えないようにするために SPARC M7 プロセッサに搭載された、コア上の暗号化命令と Silicon Secured Memory 機能を利用します。これらの機能により、暗号化のパフォーマンスが向上され、メモリー侵入検査が提供されます。また、多くの計算リソースをテナントの作業負荷の処理に特化させることができるため、全体のパフォーマンスを向上させます。

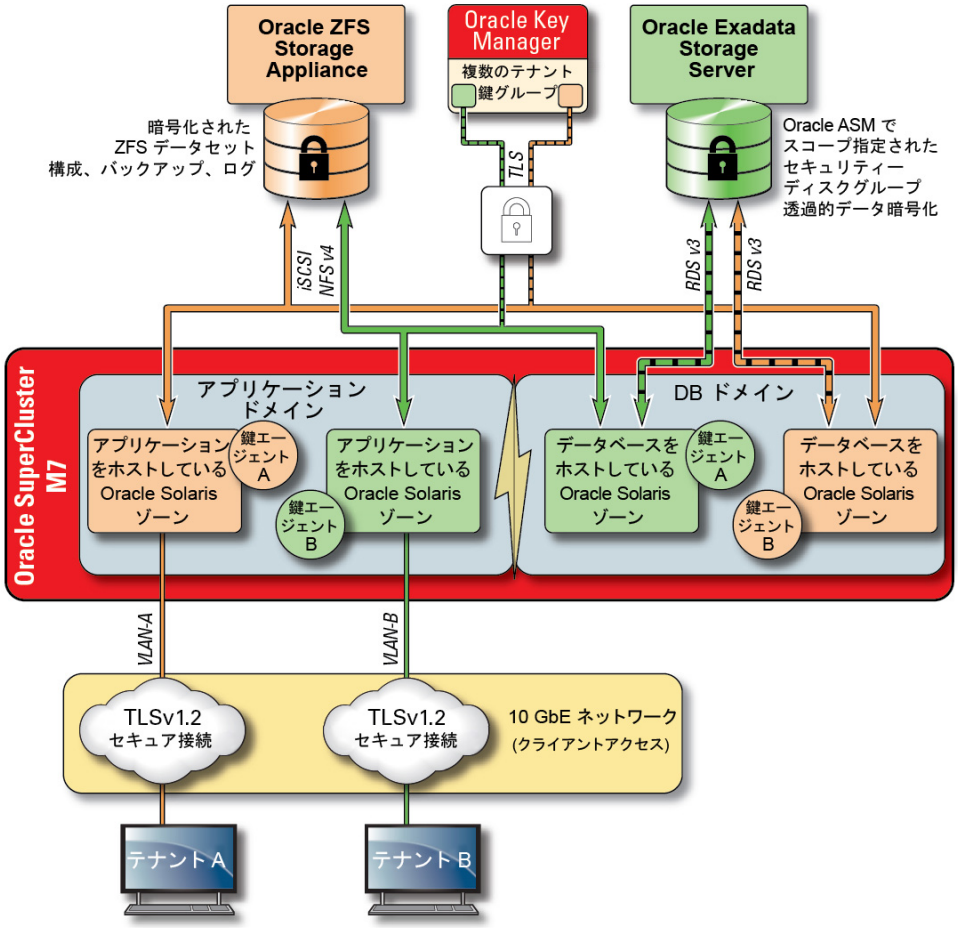
SPARC プロセッサでは、16 を超える業界標準暗号化アルゴリズムのハードウェア支援暗号化アクセラレーションをサポートできます。これらのアルゴリズムを組み合わせることで、公開鍵暗号化、対称鍵暗号化、乱数生成、デジタル署名とメッセージダイジェストの計算と検証を含むほとんどの最新の暗号化ニーズをサポートします。さらに OS レベルでは、Secure Shell、IPSec/IKE、暗号化された ZFS データセットを含むほとんどのコアサービスに対して、デフォルトで暗号化ハードウェアアクセラレーションが有効になっています。

Oracle Database および Oracle Fusion Middleware は、SuperCluster によって使用される Oracle Solaris OS および SPARC プロセッサを自動的に識別します。これにより、データベースとミドルウェアは、TLS、WS-Security、およびテーブルスペースの暗号化操作に対して、プラットフォームのハードウェア暗号化アクセラレーション機能を自動的に使用します。また、メモリー保護のために Silicon Secured Memory 機能を使用でき、エンドユーザーの構成を必要としなくてもアプリケーションデータの整合性を保証します。IB ネットワーク上を流れるテナント固有のゾーン間 IP ベース通信の機密性をおよび整合性を保護するために、IPSec (IP セキュリティー) および IKE (インターネット鍵交換) を使用します。

暗号化のどのような議論も、暗号化鍵の管理方法を議論しなくては不完全です。特にサービスの大規模なコレクションに対する暗号化鍵の生成および管理は、従来、組織にとって大きな課題であり、クラウドベースのマルチテナント環境の場合、この課題は一層大きなものになります。SuperCluster では、ZFS データセット暗号化および Oracle Database Transparent Data Encryption は Oracle Solaris PKCS #11 キーストアを活用して、マスター鍵をセキュアに保護できます。Oracle Solaris PKCS #11 キーストアを使用すると、任意のマスター鍵操作に対して、SPARC ハードウェア支援暗号化アクセラレーションが自動的に使用されます。これにより、SuperCluster は、ZFS データセットの暗号化、Oracle Database テーブルスペースの暗号化、暗号化データベースのバックアップ (Oracle Recovery Manager [Oracle RMAN] を使用)、暗号化データベースのエクスポート (Oracle Database のデータポンプ機能を使用)、および Redo ログ (Oracle Active Data Guard を使用) に関連する暗号化および復号化操作のパフォーマンスを大幅に向上できます。

共有ウォレットアプローチを使用するテナントは、ZFS Storage Appliance を利用してクラスタ内のすべてのノードで共有できるディレクトリを作成します。共有された集中管理型キーストアを使用すると、鍵はクラスタ内の各ノード間で同期されるため、テナントは Oracle Real Application Clusters (Oracle RAC) などのクラスタ化データベースアーキテクチャーで鍵を適切に管理、保守、交換できます。

図 5 Oracle Key Manager を使用するマルチテナント鍵管理シナリオでのデータ保護



クラウドベースのマルチテナント環境における複数のホストやアプリケーションに関連した鍵管理の複雑さや問題に対処するため、管理ネットワークに統合されたアプライアンスとしてオプションの Oracle Key Manager を使用します。Oracle Key Manager は、Oracle Database、Oracle Fusion アプリケーション、Oracle Solaris、および ZFS Storage Appliance によって使用される暗号化鍵へのアクセスを集中的に承認、セキュリティー保護、および管理します。Oracle Key Manager は、Oracle の StorageTek 暗号化テープドライブもサポートします。ZFS データセット (ファイルシステム) レベルで暗号化ポリシーおよび鍵管理を設定することで、鍵の破棄を通じたテナントファイルシステムの削除保証を提供します。

Oracle Key Manager は、ライフサイクル鍵管理操作を信頼できる鍵ストレージをサポートする完全な鍵管理アプライアンスです。Oracle の追加の Sun Crypto Accelerator 6000 PCIe Card を使用して構成されている場合、Oracle Key Manager は AES 256 ビット暗号化鍵の FIPS 140-2 レベル 3 認証鍵ストレージ、および FIPS 186-2 準拠乱数生成を提供します。SuperCluster 内では、アプリケーション、データベース、および暗号化 ZFS データセットに関連する鍵の管理で Oracle Key Manager を使用するように、大域ゾーンおよび非大域ゾーンを含むすべてのデータベースおよびアプリケーションドメインを構成できます。実際には、Oracle Key Manager は個々または複数のデータベースインスタンス、Oracle RAC、Oracle Active Data Guard、Oracle RMAN、および Oracle Database のデータポンプ機能に関連する鍵管理操作をサポートできます。

最後に、Oracle Key Manager によって適用される役割を分離することで、各テナントはその暗号化鍵の詳細な制御を維持でき、鍵管理操作に一貫した可視性が得られます。情報の保護に鍵が重要であることを考えると、鍵がその有効期間を通じて適切に保護されるように、テナントは役割ベースのアクセス制御と監査の必要なレベルを実装することが重要です。

関連情報

- 128 ページの「Oracle Key Manager」

アクセス制御

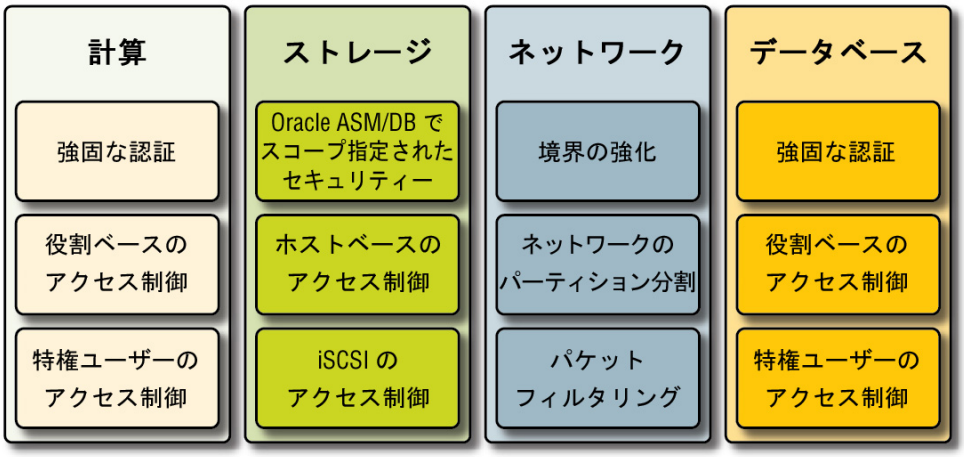
クラウドホスティング環境方針を採用する組織の場合、アクセス制御は解決するもっとも重要な課題の 1 つです。テナントは、共有インフラストラクチャーに保存されている情報が保護されていて、承認されたホスト、サービス、ユーザー、グループ、および役割のみが使用可能であるという確信を持つ必要があります。承認されたホスト、ユーザー、およびサービスは、特定の操作に必要な権利と特権のみを持っているといった最小特権の原則に従ってさらに制約される必要があります。

SuperCluster では、スタックのすべての階層を対象にし、エンドユーザー、データベース管理者、システム管理者などのさまざまな役割をサポートする、柔軟で階層化されたアクセス制御アーキテクチャーを促進します。これにより、組織はホスト、アプリケーション、およびデータベースを個別に保護するポリシーを定義したり、それらのサービスを実行する基となる計算、ストレージ、およびネットワークインフラストラクチャーを保護したりできます。

仮想化および OS レイヤーでのアクセス制御は、ネットワーク上で公開されているサービスの数を減らすことから始まります。これは、SPARC コンソール、ドメイン、およびゾーンに関して Oracle VM Server へのアクセスを制御するのに役立ちます。システムにアクセスできるエントリポイントの数を減らすことによって、アクセス制御ポリシーの数も削減でき、システムの有効期間にわたって簡単に維持できます。

Oracle Solaris OS 内でのアクセス制御は、Oracle Solaris の役割ベースのアクセス制御 (RBAC) 機能と POSIX アクセス権の組み合わせを使用して実装されます。ホスト、アプリケーション、データベース、および SuperCluster 上で実行されている関連サービスをネットワークベースの攻撃から保護する機能も同様に重要です。これを行うには、テナントは、承認されたネットワークサービスのみが実行されていて、着信ネットワーク接続を待機していることを最初に検証するべきです。ネットワーク攻撃対象領域が最小化されたら、テナントは、承認されたネットワークおよびインタフェース上でのみ入接続を待機するように残りのサービスを構成します。この単純なプラクティスにより、Secure Shell などの管理プロトコルに対して管理ネットワーク以外の任意の場所からアクセスできないようになります。

図 6 エンドツーエンドのアクセス制御のサマリー



さらに、テナントは、Oracle Solaris の IP フィルタサービスなどのホストベースのファイアウォールを実装することもできます。ホストベースのファイアウォールは、ネットワークサービスへのアクセスを制御する豊富な機能を備えた方法をホストに提供するため、便利です。たとえば、IP フィルタはステートフルパケットフィルタリング機能をサポートし、IP アドレス、ポート、プロトコル、ネットワークインタフェース、およびトラフィックリダイレクションでパケットをフィルタリングできます。これらの機能は、SuperCluster などの、多くのネットワークインタフェースが動作していてさまざまなインバウンドおよびアウトバウンドのネットワーク通信をサポートするプラットフォームで重要です。

SuperCluster では IP フィルタは、Oracle VM Server for SPARC ドメイン内で構成したり、Oracle Solaris 内から操作したりできます。これにより、ネットワークアクセス制御ポリシーは、データベースサービスが提供される同じ OS コンテナ内で適用されま

す。マルチテナントシナリオでは、アウトバウンドネットワークアクティビティーの量が最小限になる可能性があり、簡単に分類できるため、特定のネットワークインタフェースと宛先への通信を制限するポリシーを作成できます。その他のすべてのトラフィックは拒否され、インバウンドとアウトバウンドの両方の承認されていない通信をブロックするという「デフォルトの拒否」ポリシーの一部として記録されます。

Oracle End User Security では、テナントは、シングルサインオン (SSO) および集中管理されたユーザーおよび役割管理をサポートするために、アプリケーションとデータベースと既存のアイデンティティー管理サービスと統合できます。具体的には、Oracle End User Security は、(1) データベースユーザーと管理者のプロビジョニングおよびプロビジョニング解除、(2) パスワード管理およびセルフサービスパスワードリセット、および (3) グローバルデータベース役割を使用した承認の管理を集中管理することで役立ちます。Kerberos や PKI といった多要素認証方法を要求する組織は、Oracle Advanced Security を活用できます。

Oracle Exadata Storage Server テクノロジは、それぞれ個別の特権を持つ定義済みのユーザーアカウントセットをサポートします。Oracle Exadata Storage Server 管理を実行する管理者は、これらの事前に定義された役割の 1 つを使用してシステムにアクセスする必要があります。一方、ZFS Storage Appliance は、ローカルとリモートの管理アカウントの作成をサポートします。どちらのアカウントも役割および特権の個々の割り当てをサポートできます。

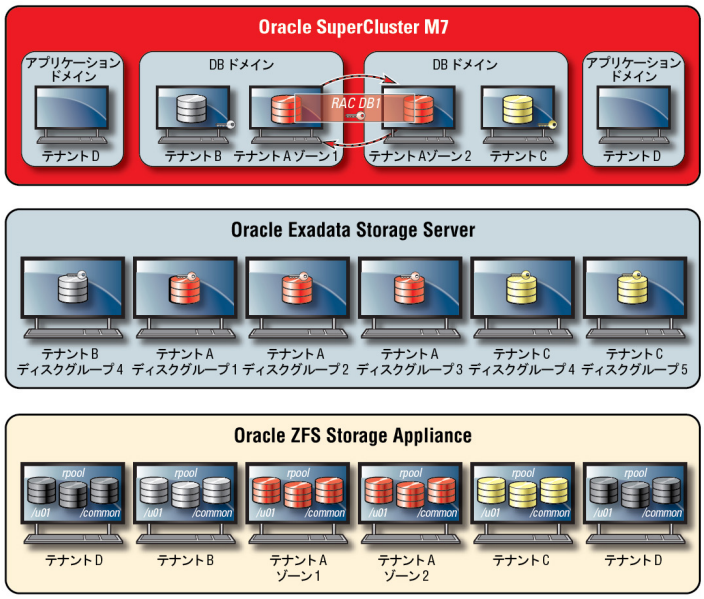
デフォルトでは、SuperCluster で使用される Oracle Exadata Storage Server は、Oracle Automatic Storage Management 機能を使用してデータベースドメインによってアクセスされます。この機能により、クラウドプロバイダは、容量、パフォーマンス、および可用性の要件を満たせるテナントごとに異なるディスクグループを作成できます。アクセス制御に関して Oracle Automatic Storage Management は、オープンなセキュリティー、Oracle Automatic Storage Management でスコープ指定されたセキュリティー、データベースでスコープ指定されたセキュリティーの 3 つのアクセス制御モードをサポートします。

マルチテナントシナリオでは、もっともきめ細かいレベルのアクセス制御を提供するため、データベースにスコープ指定されたセキュリティーが推奨されます。このモードでは、単一のデータベースのみがアクセスできるようにディスクグループを構成できます。具体的には、データベース管理者とユーザーの両方に対して、アクセス特権を持っている情報が格納されているグリッドディスクのみにアクセスを制限できることを意味します。個々のデータベースが異なる組織またはテナントをサポートしている可能性があるデータベース統合シナリオでは、各テナントが専用のストレージのみにアクセスして操作できることが重要です。特に、前述の作業負荷とデータベースの分離方針と組み合わせると、テナントは個々のデータベースへのアクセスを実質的にコンパートメント化できます。

データベースにスコープ指定されたセキュリティーは、Oracle ASM グリッドディスクへのアクセスを制限するための有効なツールです。この図は、Oracle ASM にスコープ指定されたセキュリティーと ZFS セキュリティーを示します。SuperCluster プラットフォーム上に多数の Oracle Database インスタンスが配備されている状況では、テ

ナントごとの Oracle ASM にスコープ指定されたセキュリティー方針は、作成、割り当て、および管理される鍵の数が大幅に削減されるため、より意味があります。さらに、データベースにスコープ指定されたセキュリティーではデータベースごとに個別のディスクグループを作成する必要があるため、このアプローチによって、Exadata Storage Server 上に作成する必要がある個別のグリッドディスクの数が大幅に削減されます。

図 7 テナントごとの Oracle ASM にスコープ指定されたセキュリティー



SuperCluster では Oracle Solaris データリンク保護を利用して、悪意のあるテナント仮想マシンによってネットワークに発生する可能性のある損害を回避しようとします。この統合された Oracle Solaris 機能では、IP および MAC アドレススプーフィングや L2 フレームスプーフィング (たとえば Bridge Protocol Data Unit 攻撃) といった基本的な脅威に対する保護を提供します。Oracle Solaris データリンク保護は、マルチテナント環境内に配備されているすべての Oracle Solaris 非大域ゾーンに個別に適用する必要があります。

個々のテナントは Exadata Storage Server に対して管理またはホストレベルのアクセスを必要としてはならないため、そのようなアクセスは制限することを強くお勧めします。Exadata Storage Server は、SuperCluster データベースドメイン (クラウドプロバイダによって運用) からのアクセスは引き続き許可しながら、テナントの非大域ゾーンおよびデータベース I/O ドメインに関する直接アクセスは防止するように構成される

べきです。これにより、Exadata Storage Server は管理ネットワーク上の信頼できる場所からのみ管理できるようになります。

テナントのセキュリティー構成が定義および実装されたら、サービスプロバイダは、テナント固有の大域ゾーンおよび非大域ゾーンを読み取り専用環境として不変であるように構成するための追加の手順を検討できます。不変ゾーンは、テナントが独自のサービスを運用する可能性のある、回復性があり統合性の高い運用環境を作成します。Oracle Solaris 本来のセキュリティー機能を基にしているため、不変ゾーンでは、クラウドサービスプロバイダによる介入がないと、一部 (またはすべて) の OS ディレクトリおよびファイルを変更できません。このような読み取り専用の状態を適用すると、未承認の変更を回避したり、さらに強力な変更管理の手順を推進したり、カーネルベースとユーザーベースの両方のマルウェアの侵入を抑止したりできます。

モニタリングおよびコンプライアンス監査

クラウド環境における事前のモニタリングおよびロギングは非常に重要であり、多くの場合はセキュリティーの抜け穴や脆弱性に起因する攻撃を軽減できます。コンプライアンスレポートであるのか、インシデントレスポンスであるのかには関係なく、モニタリングおよび監査はクラウドプロバイダにとって重要な機能であり、テナント組織は適切に定義されたロギングおよび監査ポリシーを適用して、ホスティング環境の可視性を高めることが必要です。多くの場合、モニタリングおよび監査が採用される範囲は、保護される環境のリスクや重大度に基づきます。

SuperCluster クラウドアーキテクチャーでは、監査イベント情報を収集、保存、および処理するために Oracle Solaris の監査サブシステムの使用に依存します。各テナント固有の非大域ゾーンは、各 SuperCluster 専用ドメイン (大域ゾーン) にローカルで保存される監査レコードを生成します。このアプローチでは、クラウドサービスプロバイダにその責任があるため、個々のテナントは監査ポリシー、構成、または記録データを変更できません。Oracle Solaris 監査機能は、テナントゾーンとドメインの両方で、すべての管理アクション、コマンド呼び出し、さらには個々のカーネルレベルのシステム呼び出しをモニターします。この機能は高度な構成が可能であるため、大域、ゾーンごと、さらにユーザーごとの監査ポリシーが提供されます。テナントゾーンを使用するように構成されている場合、各ゾーンの監査レコードを大域ゾーンに保存して、改ざんから保護できます。専用ドメインおよび I/O ドメインでは、ネイティブの Oracle Solaris 監査機能を利用して、仮想化イベントおよびドメイン管理に関連付けられたアクションおよびイベントを記録します。

Exadata Storage Server および ZFS Storage Appliance は、ログイン、ハードウェア、および構成の監査をサポートします。これにより、組織ではデバイスにだれがアクセスしたのか、およびどのアクションが実行されたのかを判断できます。エンドユーザーには直接公開されませんが、Oracle Solaris の監査では、ZFS Storage Appliance によって提供される情報の基となる内容を提供します。

同様に、Exadata Storage Server の監査は、Exadata Storage Server ソフトウェアによって提供されるハードウェアおよび構成アラート情報とともに使用できるシステムイベントの豊富なコレクションです。Oracle Solaris の IP フィルタ機能を使用すると、クラウドプロバイダはインバウンドおよびアウトバウンドの両方のネットワーク通信を選択的に記録できます。この機能は、ドメインと非大域ゾーンの両方のレベルで適用できます。これにより、組織はネットワークポリシーをセグメント化して、アクティビティーレコードを確認できます。オプションで、さまざまな Oracle および Oracle 以外のデータベースからの監査情報および Oracle Solaris からの監査情報をセキュアに集約して解析するように Oracle Audit Vault and Database Firewall アプライアンスを配備できます。

Oracle Enterprise Manager との統合を通じ、SuperCluster では、さまざまなクラウドセルフサービス操作をサポートできます。クラウドプロバイダは、リソースのプールを定義し、プールと割り当て制限を個々のテナントに割り当てて、サービスカタログを識別および公開し、最終的にはアプリケーションおよびデータベースリソースのモニタリングおよびロギングをサポートできます。

関連情報

- 121 ページの「コンプライアンスの監査」
- 131 ページの「セキュリティーのモニタリング」

SuperCluster セキュリティーのベストプラクティスの追加リソース

SuperCluster のセキュリティー、アーキテクチャー、およびベストプラクティスに関する追加の情報については、これらのリソースを参照してください。

- Oracle SuperCluster M7 - プラットフォームのセキュリティーの原則および機能

  `http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf`
- Oracle SuperCluster M7 - セキュアなプライベートクラウドアーキテクチャー

  `http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf`
- Oracle SuperCluster での包括的なデータ保護

  `https://community.oracle.com/docs/DOC-918251`
- Oracle SuperCluster でのセキュアなデータベース統合

http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf

- Oracle SuperCluster と PCI コンプライアンス

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster - セキュリティーの技術的実装ガイド (STIG) の検証とベストプラクティス

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Oracle Solaris 11 セキュリティーサービス開発ガイド

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Oracle Solaris 11 と PCI コンプライアンス

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Oracle Solaris 11 監査クイックスタート

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- Oracle Solaris 11 セキュリティーガイドライン

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Oracle Database セキュリティーガイド 12c リリース 1 (12.1)

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

デフォルトのセキュリティー構成の確認

次のトピックでは、SuperCluster M7 のデフォルトのセキュリティー構成について説明します。

デフォルトのセキュリティー設定

SuperCluster M7 ソフトウェアは、多くのデフォルトのセキュリティー設定を使用してインストールされています。可能であれば、セキュアなデフォルト設定を使用してください。

- パスワードポリシーによって、最低限のパスワードの複雑さが適用されます。
- ログインの試みに一定の回数失敗すると、ロックアウトが発生します。
- OS 内のデフォルトのシステムアカウントがすべてロックされ、ログインが禁止されます。
- 限定的に `su` コマンドを使用する機能が構成されています。
- OS カーネルから不要なプロトコルおよびモジュールが無効になっています。
- ブートローダーがパスワードで保護されています。
- `inetd` (インターネットサービスデーモン) を含む、すべての不要なシステムサービスが無効になっています。
- ストレージセル上にソフトウェアファイアウォールが構成されています。
- 主要なセキュリティー関連の構成ファイルおよび実行可能ファイル上に、制限されたファイルアクセス権が設定されています。
- SSH 待機ポートが管理およびプライベートネットワークに制限されています。
- SSH が v2 プロトコルに制限されています。
- セキュアでない SSH 認証メカニズムが無効になっています。

- 特定の暗号化方式が構成されています。
- システム内のスイッチがネットワーク上のデータトラフィックから分離されています。

デフォルトのユーザーアカウントとパスワード

この表には、SuperCluster M7 のデフォルトのユーザーアカウントとパスワードが一覧表示されています。デフォルトのパスワードを変更するための追加の手順については、各コンポーネントに関する後続の章で説明します。

コンポーネント	ユーザー名	パスワード	ユーザーアカウントとパスワードの情報
Oracle ILOM: ■ SPARC M7 シリーズサーバー ■ Exadata Storage Server ■ ZFS Storage Appliance	■ `root`	`welcome1`	Oracle ILOM のドキュメントコレクション (`http://docs.oracle.com/cd/E24707_01/html/E24528`) で構成と保守に関するセクションを参照してください
SPARC M7 シリーズサーバー	■ `root` ■ `oracle` ■ `grid`	`welcome1` `welcome1` `welcome1`	53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。 次の資料も参照してください。 ■ **Oracle Solaris 11** – Oracle Solaris 11 のセキュリティードキュメント (`http://www.oracle.com/goto/Solaris11/docs`) を参照してください。 ■ **Oracle Solaris 10** – 『*Oracle Solaris* 管理*:* 基本管理』(`http://docs.oracle.com/cd/E26505_01`) を参照してください。

Exadata Storage Server	■ `root`
	■ `celladmin`
	■ `cellmonitor`
		`welcome1`
		`welcome`
		`welcome`
			94 ページの「ストレージサーバーのパスワードの変更」を参照してください。

Oracle ZFS Storage ZS3-ES	■ `root`	`welcome1`	83 ページの「ZFS Storage Appliance の `root` パスワードの変更」を参照してください。 『*Oracle ZFS Storage Appliance* 管理ガイド』(`http://www.oracle.com/goto/ZS3-ES/docs`) でユーザーに関するセクションを参照してください。
InfiniBand スイッチ	■ `root` ■ `nm2user`	`welcome1` changeme	111 ページの「`root` および `nm2user` パスワードの変更」を参照してください。 *Sun Datacenter InfiniBand Switch 36* の *HTML* ドキュメントコレクション *(*ファームウェアバージョン *2.1)* (`http://docs.oracle.com/cd/E36265_01`) のシャーシの制御に関するセクションも参照してください。

コンポーネント	ユーザー名	パスワード	ユーザーアカウントとパスワードの情報
InfiniBand Oracle ILOM	■ ilom-admin ■ ilom-operator	ilom-admin ilom-operator	112 ページの「IB スイッチのパスワードの変更 (Oracle ILOM)」を参照してください。 InfiniBand のドキュメント (http://docs.oracle.com/cd/E36265_01) も参照してください。
Ethernet 管理スイッチ	■ admin	welcome1	118 ページの「Ethernet スイッチのパスワードの変更」を参照してください。
Oracle I/O ドメイン作成ツール	■ admin	welcome1	『*Oracle I/O* ドメイン管理ガイド』(http://www.oracle.com/goto/sc-m7/docs) を参照してください。
Oracle Engineered Systems Hardware Manager	■ admin ■ service	welcome1 welcome1	『*Oracle SuperCluster M7* シリーズオーナーズガイド: 管理』(http://www.oracle.com/goto/sc-m7/docs) を参照してください。

注記 - このコンポーネントで root または admin のパスワードが変更された場合は、Oracle Engineered Systems Hardware Manager でも変更する必要があります。手順については、『*Oracle SuperCluster M7* シリーズオーナーズガイド: 管理』を参照してください。31 ページの「Oracle Engineered Systems Hardware Manager で既知のパスワード」も参照してください。

Oracle Engineered Systems Hardware Manager で既知のパスワード

Oracle Engineered Systems Hardware Manager には、この表で示したコンポーネントのアカウントとパスワードを構成する必要があります。

注記 - Oracle Engineered Systems Hardware Manager で論理ドメインまたはゾーンのパスワードを記憶する必要はありません。

コンポーネント	アカウント
すべての Oracle ILOM	root
Exadata Storage Server OS	root
ZFS ストレージコントローラの OS	root
IB スイッチ	root
Ethernet 管理スイッチ	admin
PDU	admin

Oracle Engineered Systems Hardware Manager の詳細は、129 ページの「Oracle Engineered Systems Hardware Manager」および『*Oracle SuperCluster M7* シリーズ管理ガイド』(`http://www.oracle.com/goto/sc-m7/docs`) 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

これらのセクションでは、ハードウェアをセキュリティー保護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。

アクセス制限

- 施錠されアクセスが制限された部屋に Oracle SuperCluster M7 シリーズシステムおよび関連する装置を取り付けます。
- ラック内のコンポーネントの保守が必要になるまで、ラックのドアを施錠します。そうすることで、ホットプラグ対応またはホットスワップ対応デバイス、USB ポート、ネットワークポート、システムコンソールへのアクセスが制限されます。
- 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、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。物理アクセスを制限すると、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。

シリアル番号

- SuperCluster M7 シリーズシステムのコンポーネントのシリアル番号を記録します。
- 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の記録は、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は、所有権を示す唯一の証明になる可能性があります。
- システムで提供されるすべての情報シートをセキュアに格納します。

ドライブ

ハードドライブおよびソリッドステート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。

- Oracle Solaris の `format(1M)` コマンドなどのディスク抹消ツールを使用して、すべてのデータをドライブから完全に消去します。
- 組織は、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判別してください。
- 必要に応じて、Oracle の Customer Data and Device Retention Service をご活用ください。参照ドキュメント: `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

注意 - ディスク抹消ソフトウェアは、最新のドライブでは、そのデータアクセスの管理方法のために一部のデータを削除できないことがあります。

OBP

デフォルトでは、SPARC M7 シリーズ OBP はパスワードで保護されません。これらのアクションを実行して OBP へのアクセスを制限することによって、システムのセキュリティーを強化できます。

- パスワード保護を実装します。

- 失敗した OBP ログインを確認します。
- OBP 電源投入バナーを提供します。

追加のハードウェアリソース

『*SPARC M7* シリーズサーバーセキュリティーガイド』で説明するセキュリティー原則のすべてが SuperCluster の SPARC M7 サーバーに該当します。このセキュリティーガイドは、http://www.oracle.com/goto/M7/docs で入手できます

Oracle ILOM のセキュリティー保護

Oracle ILOM は、計算サーバー、ストレージサーバー、ZFS Storage Appliance、IB スイッチを含む Oracle SuperCluster コンポーネントの管理およびモニターに使用される、高度なサービスプロセッサハードウェアとソフトウェアを提供します。

Oracle ILOM では、OS の状態とは独立して、ベースとなるサーバーとデバイスをアクティブに管理およびモニターでき、信頼できる Lights Out 管理機能を提供します。

SuperCluster M7 上の Oracle ILOM に完全にセキュリティー保護するには、すべての Oracle ILOM 対応コンポーネントに対して個別に構成設定を適用する必要があります。これらのコンポーネントに Oracle ILOM があります。

- 計算サーバー
- ストレージサーバー
- ZFS Storage Appliance
- IB スイッチ

Oracle ILOM をセキュリティー保護するためにこれらのタスクを実行します。

- 37 ページの「Oracle ILOM CLI へのログイン」
- 38 ページの「Oracle ILOM のバージョンの判別」
- 38 ページの「(必要な場合) FIPS-140 準拠の動作の有効化 (Oracle ILOM)」
- 40 ページの「デフォルトのアカウントとパスワード (Oracle ILOM)」
- 40 ページの「デフォルトの公開ネットワークサービス (Oracle ILOM)」
- 41 ページの「Oracle ILOM のセキュリティー構成の強化」
- 52 ページの「追加の Oracle ILOM のリソース」

▼ Oracle ILOM CLI へのログイン

1. **管理ネットワークで Oracle ILOM にログインします。**

   この例では、*ILOM_SP_ipaddress* を、アクセスするコンポーネントの Oracle ILOM の IP アドレスに置き換えます。

   - 計算サーバー

- ストレージサーバー
- ZFS Storage Appliance
- IB スイッチ

構成用の IP アドレスは、Oracle の担当者によって提供される配備サマリーで示されます。

```
% ssh root@ILOM_SP__ipaddress
```

2. **Oracle ILOM の root パスワードを入力します。**
40 ページの「デフォルトのアカウントとパスワード (Oracle ILOM)」を参照してください。

▼ Oracle ILOM のバージョンの判別

最新の機能やセキュリティー拡張機能を活用するには、Oracle ILOM ソフトウェアを最新のサポートされているバージョンに更新します。

1. **管理ネットワークで Oracle ILOM にログインします。**
37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **Oracle ILOM のバージョンを表示します。**
この例では、Oracle ILOM ソフトウェアはバージョン 3.2.4.1.b です。

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

注記 - いずれかの SuperCluster コンポーネントの Oracle ILOM のバージョンを更新するには、`https://support.oracle.com` の My Oracle Support から入手可能な最新の SuperCluster Quarterly Full Stack Download Patch をインストールします。

注記 - SuperCluster などの Oracle Engineered Systems は、使用できる Oracle ILOM のバージョン、およびそれらのバージョンの更新方法に制限されます。詳細は、Oracle の担当者に連絡してください。

▼ (必要な場合) FIPS-140 準拠の動作の有効化 (Oracle ILOM)

米国連邦政府関係の顧客は FIPS 140 検証済み暗号化の使用が必要です。

デフォルトでは、Oracle ILOM は FIPS 140 検証済み暗号化を使用して動作しません。ただし、FIPS 140 検証済み暗号化の使用は、必要に応じて有効にできます。

FIPS 140 準拠の動作用に構成されているときは、一部の Oracle ILOM の特長と機能を使用できません。このような機能の一覧は、『*Oracle ILOM* セキュリティーガイド』の「FIPS モードが有効の時にサポートされない機能」セクションを参照してください (52 ページの「追加の Oracle ILOM のリソース」を参照してください)。

また、124 ページの「FIPS-140-2 レベル 1 コンプライアンス」も参照してください。

注意 - このタスクでは、Oracle ILOM をリセットする必要があります。リセットにより、ユーザーが構成したすべての設定が失われます。このため、追加のサイト固有の変更を Oracle ILOM に加える前に、FIPS 140 準拠の動作を有効にする必要があります。サイト固有の構成変更が加えられているシステムの場合、Oracle ILOM がリセットされたあとで復元できるように、Oracle ILOM 構成をバックアップします。そうしないと、そのような構成変更は失われます。

1. **管理ネットワークで Oracle ILOM にログインします。**

   37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **Oracle ILOM が FIPS 140 準拠の動作用に構成されているかどうかを確認します。**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

   Oracle ILOM の FIPS 140 準拠モードは、`state` および `status` プロパティーによって表されます。`state` プロパティーは Oracle ILOM に構成されているモードを表し、`status` プロパティーは Oracle ILOM の動作モードを表しています。FIPS の `state` プロパティーが変更された場合、その変更は、次回の Oracle ILOM のリブートまで動作モード FIPS の `status` プロパティーに影響を与えません。

3. **FIPS 140 準拠の動作を有効にします。**

```
-> set /SP/services/fips state=enabled
```

4. **Oracle ILOM サービスプロセッサを再起動します。**

   この変更を有効にするには、Oracle ILOM SP を再起動する必要があります。

```
-> reset /SP
```

デフォルトのアカウントとパスワード (Oracle ILOM)

アカウント	タイプ	デフォルトのパスワード	説明
`root`	管理者	`welcome1`	これは、このコンポーネント用に提供および有効化されるデフォルトのアカウントです。このアカウントは、初期構成の実行、および追加の共有されない管理者アカウントの作成を許可するために使用されます。 セキュリティーの面から、デフォルトのパスワードを変更します。

デフォルトの公開ネットワークサービス (Oracle ILOM)

この表は、Oracle ILOM によって再公開されているデフォルトのネットワークサービスが一覧表示されています。

これらのサービスに関する追加情報については、『*Oracle ILOM* セキュリティーガイド』を参照してください (52 ページの「追加の Oracle ILOM のリソース」を参照してください)。

サービス名	プロトコル	ポート	説明
SSH	TCP	22	統合された Secure Shell サービスで CLI を使用して、Oracle ILOM への管理アクセスを有効にするために使用されます。
HTTP (BUI)	TCP	80	統合された HTTP サービスでブラウザインタフェースを使用して、Oracle ILOM への管理アクセスを有効にするために使用されます。TCP/80 は通常、クリアテキストのアクセスに使用されますが、デフォルトでは TCP/443 で実行されるこのサービスのセキュアなバージョンに対して、Oracle ILOM が着信リクエストを自動的にリダイレクトします。
NTP	UDP	123	統合された Network Time Protocol (NTP) (クライアントのみ) サービスで、ローカルシステムクロックを 1 つ以上の外部時間ソースと同期させるために使用されます。
SNMP	UDP	161	統合された SNMP サービスで、Oracle ILOM の健全性をモニターし、受信したトラップ通知をモニターする管理インタフェースを提供するために使用されます。
HTTPS (BUI)	TCP	443	統合された HTTPS サービスでブラウザインタフェースを使用して、Oracle ILOM への暗号化された (SSL/TLS) チャネルを介した管理アクセスを有効にするために使用されます。
IPMI	TCP	623	統合された Intelligent Platform Management Interface (IPMI) サービスで、さまざまなモニタリングおよび管理機能のコンピュータインタフェースを提供するために使用されます。ハードウェアのインベントリデータ、FRU の説明、ハードウェアのセンサー情報、およびハードウェアコンポーネントのステータス情報を収集するために Oracle Enterprise Manager Ops Center で使用されるため、このサービスは無効にするべきではありません。
リモート KVMS	TCP	5120 5121	リモート KVMS ポートは、Oracle Integrated Lights Out Manager で使用できるリモートのキーボード、ビデオ、マウス、およびストレージ機能を提供するプロトコルのセットを一括して提供します。

サービス名	プロトコル	ポート	説明
		5123	
		5555	
		5556	
		7578	
		7579	
サービスタグ	TCP	6481	Oracle サービスタグサービスによって使用されます。これは、サーバーを識別し、サービス要求を容易にするための Oracle の発見プロトコルです。このサービスは、Oracle ILOM ソフトウェアを検索したりその他の Oracle の自動サービスソリューションと統合したりするために、Oracle Enterprise Manager Ops Center などの製品によって使用されます。
WS-Man over HTTPS	TCP	8888	統合された WS-Man サービスで、HTTPS プロトコルを介して Oracle ILOM を管理するために使用される標準ベースの Web サービスインタフェースを提供するために使用されます。このサービスを無効にすると、このプロトコルを使用して Oracle ILOM を管理できなくなります。このサービスは、Oracle ILOM バージョン 3.2 の時点で含まれなくなりました。
WS-Man over HTTP	TCP	8889	このポートは、統合された WS-Man サービスで、HTTP プロトコルを介して Oracle ILOM を管理するために使用される標準ベースの Web サービスインタフェースを提供するために使用されます。このサービスを無効にすると、このプロトコルを使用して Oracle ILOM を管理できなくなります。このサービスは、Oracle ILOM バージョン 3.2 の時点で含まれなくなりました。
シングルサインオン	TCP	11626	このポートは、ユーザーによるユーザー名とパスワードの入力回数を減らす統合されたシングルサインオン機能によって使用されます。このサービスを無効にすると、パスワードを再入力せずに KVMS を起動できなくなります。

Oracle ILOM のセキュリティー構成の強化

これらのトピックでは、各種の構成設定を通じて Oracle ILOM をセキュリティー保護する方法について説明します。

- 50 ページの「ログイン警告バナーの構成 (Oracle ILOM)」

▼ 不要なサービスの無効化 (Oracle ILOM)

プラットフォームの運用および管理要件をサポートするために必要がないサービスを無効にします。

デフォルトで Oracle ILOM はネットワークのデフォルトでのセキュリティー強化 (Secure By Default) 構成を採用します。この構成では、重要でないサービスはすでに無効になっています。ただし、セキュリティーポリシーおよび要件に基づいて、追加のサービスを無効にしなければならない場合があります。

1. **管理ネットワークで Oracle ILOM にログインします。**
   37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **Oracle ILOM によってサポートされているサービスのリストを確認します。**

   ```
   -> show /SP/services
   ```

3. **特定のサービスが有効になっているかどうかを確認します。**
   servicename を ステップ 2 で識別されているサービス名に置き換えます。

   ```
   -> show /SP/services/servicename servicestate
   ```

   大半のサービスでは `servicestate` パラメータを認識および使用してサービスが有効と無効のどちらであるのかを記録しますが、`state` というパラメータを使用する `servicetag`、`ssh`、`sso`、`wsman` などのサービスがいくつかあります。使用される実際のパラメータにかかわらず、これらの例で示すように、`servicestate` または `state` パラメータが値 `enabled` の値を返す場合、サービスは有効です。

   ```
   -> show /SP/services/https servicestate
   /SP/services/https
   Properties:
   servicestate = enabled
   ```

   ```
   -> show /SP/services/ssh state
   /SP/services/ssh
   Properties:
   state = enabled
   ```

4. **必要がないサービスを無効にするには、サービス状態を `disabled` に設定します。**

   ```
   -> set /SP/services/http servicestate=disabled
   ```

5. **これらのいずれかのサービスを無効にする必要があるかどうかを確認します。**

使用されるツールおよび方法に応じて、これらの追加のサービスが必要ないか使用されていない場合は、無効にできます。

- **ブラウザ管理インタフェース (HTTP、HTTPS) の場合は、次のように入力します。**

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

- **キーボード、ビデオ、マウスサービス (KVMS) の場合は、次のように入力します。**

```
-> set /SP/services/kvms servicestate=disabled
```

- **Web サービス管理 (WS-Man over HTTP/HTTPS) の場合は (Oracle ILOM バージョン 3.1 およびそれ以前)、次のように入力します。**

```
-> set /SP/services/wsman state=disabled
```

- **シングルサインオンサービス (SSO) の場合は、次のように入力します。**

```
-> set /SP/services/sso state=disabled
```

▼ HTTPS への HTTP リダイレクションの構成 (Oracle ILOM)

ブラウザベースの通信のすべてが Oracle ILOM と管理者との間で確実に暗号化されるように、Oracle ILOM はデフォルトで着信 HTTP 要求を HTTPS サービスにリダイレクトするように構成されています。

1. **管理ネットワークで Oracle ILOM にログインします。**
   37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **セキュアなリダイレクションが有効になっていることを確認します。**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **デフォルトが変更されている場合は、セキュアなリダイレクションを有効にできます。**

```
-> set /SP/services/http secureredirect=enabled
```

4. **ステップ 2 を繰り返して設定を確認します。**

未承認のプロトコルの無効化

これらのトピックを使用して、未承認のプロトコルを無効にします。

- 44 ページの「HTTPS 用 SSLv2 プロトコルの無効化」
- 44 ページの「HTTPS 用 SSLv3 プロトコルの無効化」

▼ HTTPS 用 SSLv2 プロトコルの無効化

デフォルトで、SSLv2 プロトコルは HTTPS サービスに対して無効になっています。

セキュリティーのために、SSLv2 が無効になっていることが非常に重要です。

1. **管理ネットワークで Oracle ILOM にログインします。**
37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **SSLv2 プロトコルが HTTP サービスに対して無効になっているかどうかを確認します。**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **サービスが有効になっている場合は、SSLv2 プロトコルを無効にします。**

```
-> set /SP/services/https sslv2=disabled
```

4. **ステップ 2 を繰り返して設定を確認します。**

▼ HTTPS 用 SSLv3 プロトコルの無効化

デフォルトで、SSLv3 プロトコルは HTTPS サービスに対して有効になっています。

セキュリティーのために、SSLv3 プロトコルを無効にします。

1. **管理ネットワークで Oracle ILOM にログインします。**
   37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **SSLv3 プロトコルが HTTP サービスに対して無効になっているかどうかを確認します。**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **SSLv3 プロトコルを無効にします。**

```
-> set /SP/services/https sslv3=disabled
```

4. **ステップ 2 を繰り返して設定を確認します。**

▼ 未承認の HTTPS 用 TLS プロトコルの無効化

デフォルトでは、TLSv1.0、TLSv1.1、および TLSv1.2 プロトコルは HTTPS サービスに対して有効になっています。

セキュリティーポリシーに準拠していない 1 つ以上の TLS プロトコルバージョンを無効にできます。

セキュリティーのために、TLS プロトコルの以前のバージョンのサポートが必要でないかぎり、TLSv1.2 を使用します。

1. **管理ネットワークで Oracle ILOM にログインします。**
   37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **HTTPS サービスに対して有効になっている TLS プロトコルバージョンのリストを確認します。**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **TLSv1.0 を無効にします。**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **TLSv1.1 を無効にします。**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **ステップ 2 を繰り返して設定を確認します。**

▼ HTTPS 用の SSL 弱および中強度暗号化の無効化

デフォルトで、Oracle ILOM では HTTPS サービスに対する弱および中強度暗号化の使用は無効になっています。

1. **管理ネットワークで Oracle ILOM にログインします。**
37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **弱および中強度暗号化が無効になっているかどうかを確認します。**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **デフォルトが変更されている場合は、弱および中強度暗号化の使用を無効にできます。**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **ステップ 2 を繰り返して設定を確認します。**

▼ 未承認の SNMP プロトコルの無効化 (Oracle ILOM)

デフォルトでは、Oracle ILOM をモニターおよび管理するために使用される SNMP サービスについて、SNMPv3 プロトコルのみが有効です。必要でないかぎり古いバージョンの SNMP プロトコルが無効になっていることを確認します。

一部の Oracle およびサードパーティー製品には、新しい SNMP プロトコルバージョンのサポートに関して制限があります。特定の SNMP プロトコルバージョンのサポートを確認するには、コンポーネントに関連する製品ドキュメントを参照してください。コンポーネントで要求されるプロトコルバージョンをサポートするように Oracle ILOM が構成されていることを確認します。

注記 - SNMP プロトコルのバージョン 3 では、ユーザーベースのセキュリティーモデル (USM) のサポートが導入されました。この機能は、従来の SNMP コミュニティー文字列を、特定のアクセス権、認証、およびプライバシプロトコルで構成可能な実際のユーザーアカウントとパスワードで置き換えます。デフォルトでは、Oracle ILOM に USM アカウントは含まれていません。独自の配備、管理、およびモニタリングの要件に基づいて、SNMPv3 USM アカウントを構成します。

1. **管理ネットワークで Oracle ILOM にログインします。**
37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **それぞれの SNMP プロトコルのステータスを確認します。**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **必要に応じて、SNMPv1 と SNMPv2c を無効にします。**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **ステップ 2 を繰り返して設定を確認します。**

▼ SNMP v1 および v2c コミュニティー文字列の構成 (Oracle ILOM)

このタスクは、SNMP v1 または SNMPv2c が有効で使用するために構成されている場合のみ適用できます。

SNMP が正しく動作するには、アクセスを認証するために使用されるコミュニティー文字列がクライアントとサーバーで一致する必要があります。したがって、SNMP コミュニティー文字列を変更する場合は、両方の Oracle ILOM で SNMP プロトコルを使用して Oracle ILOM に接続しようとしているすべてのコンポーネントについて、新しい文字列が構成されるようにします。

SNMP はデバイスの健全性をモニターするために使用されることが多いため、デバイスによって使用されるデフォルトの SNMP コミュニティー文字列を顧客定義の値に置き換えることが重要です。

1. **管理ネットワークで Oracle ILOM にログインします。**

37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **新しい SNMP コミュニティー文字列を作成します。**

   この例では、コマンド行でこれらの項目を置き換えます。

   - *string* – SNMP コミュニティー文字列の構成に関する米国国防総省の要件に準拠する顧客定義の値で置き換えます。
   - *access* – これが読み取り専用と書き込み専用のどちらのアクセス文字列であるのかに応じて、`ro` または `rw` で置き換えます。

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   新しいコミュニティー文字列が作成されたら、デフォルトのコミュニティー文字列を削除する必要があります。

3. **デフォルトの SNMP コミュニティー文字列を削除します。**

   ```
   -> delete /SP/services/snmp/communities/public
   -> delete /SP/services/snmp/communities/private
   ```

4. **SNMP コミュニティー文字列を確認します。**

   ```
   -> show /SP/services/snmp/communities
   ```

▼ デフォルトの自己署名付き証明書の交換 (Oracle ILOM)

Oracle ILOM は、SSL および TLS プロトコルをデフォルトの状態で使用できるように、自己署名付き証明書を使用します。可能な場合は、自己署名付き証明書を、使用中の環境で使用することが承認され、認識された認証局によって署名された証明書で置き換えます。

Oracle ILOM は、デジタル証明書および非公開鍵へのアクセスに使用できるさまざまな方法 (HTTPS、HTTP、SCP、FTP、TFTP) をサポートし、情報を Web ブラウザインタフェースに直接渡します。詳細は、『*Oracle ILOM* 構成および保守ガイド』を参照してください (52 ページの「追加の Oracle ILOM のリソース」を参照してください)。

1. **Oracle ILOM でデフォルトの自己署名付き証明書を使用しているかどうかを確認します。**

   ```
   -> show /SP/services/https/ssl cert_status
   ```

```
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **組織の証明書をインストールします。**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

▼ 管理ブラウザインタフェースの非アクティブタイムアウトの構成

Oracle ILOM は、事前に定義された分数よりも長い時間非アクティブになっている管理セッションを切断してログアウトする機能がサポートされています。デフォルトでは、ブラウザインタフェースセッションは 15 分後にタイムアウトします。

HTTPS および HTTP サービスに関連付けられたセッションタイムアウトパラメータは、独立して設定および管理されます。各サービスに関連付けられた `sessiontimeout` パラメータを設定してください。

1. **管理ネットワークで Oracle ILOM にログインします。**
37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **HTTPS サービスに関連付けられた非アクティブタイムアウトパラメータを確認します。**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **非アクティブタイムアウトパラメータを設定します。**
n を分で指定された値で置き換えます。

```
-> set /SP/services/https sessiontimeout=n
```

4. **HTTP サービスに関連付けられた非アクティブタイムアウトパラメータを確認します。**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **非アクティブタイムアウトパラメータを設定します。**

n を分で指定された値で置き換えます。

```
-> set /SP/services/http sessiontimeout=n
```

6. **ステップ 2 およびステップ 4 を繰り返して設定を確認します。**

▼ 管理インタフェースのタイムアウトの構成 (Oracle ILOM CLI)

Oracle ILOM は、事前に定義された分数よりも長い時間非アクティブになっている管理 CLI セッションを切断してログアウトする機能がサポートされています。

デフォルトでは、SSH CLI に指定されたタイムアウト値はなく、その結果、このサービスにアクセスする管理ユーザーは無期限にログインしたままになります。

セキュリティーのために、ブラウザユーザーインタフェースに関連付けられた値に一致するようにこのパラメータを設定します。これは、15 分などの値になります。

1. **管理ネットワークで Oracle ILOM にログインします。**
37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **CLI に関連付けられた非アクティブタイムアウトパラメータを確認します。**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **非アクティブタイムアウトパラメータを設定します。**
n を分で指定された値で置き換えます。

```
-> set /SP/cli timeout=n
```

4. **ステップ 2 を繰り返して設定を確認します。**

▼ ログイン警告バナーの構成 (Oracle ILOM)

Oracle ILOM では、管理者がデバイスに接続する前とあとの両方で、顧客固有のメッセージを表示する機能をサポートしています。

Oracle ILOM の接続メッセージは認証前に表示されますが、ログインメッセージは認証後に表示されます。

オプションで、Oracle ILOM 機能へのアクセスが付与される前に、ログインメッセージの同意を必要とするように Oracle ILOM を構成できます。接続とログインの両方のメッセージ、およびオプションの同意要件は、ブラウザとコマンド行アクセスインタフェースの両方によって実装されます。

Oracle ILOM では、最大 1,000 文字の接続およびログインメッセージをサポートします。

1. **管理ネットワークで Oracle ILOM にログインします。**
   37 ページの「Oracle ILOM CLI へのログイン」を参照してください。

2. **接続およびログインメッセージが構成されているかどうかを確認します。**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **接続またはログインメッセージを設定します。**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **ログインメッセージの同意が有効になっているかどうかを確認します。**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(オプション) ログインメッセージの同意を強制します。**

注意 - ログインメッセージの同意を要求すると、SSH を使用する自動管理プロセスは、同意要求に応答できないまたは応答するように構成されていない可能性があるため、その適切な動作が抑止されることがあります。その結果、Oracle ILOM はメッセージの同意要件が満たされるまで CLI の使用を許可しないため、このような接続がハングまたはタイムアウトすることがあります。

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **ステップ 2 およびステップ 4 を繰り返して設定を確認します。**

追加の Oracle ILOM のリソース

Oracle ILOM の管理およびセキュリティーの手順の詳細は、SuperCluster M7 で実行しているバージョンに対応する Oracle ILOM のドキュメントライブラリを参照してください。

- *Oracle ILOM* セキュリティーガイドファームウェア *Release 3.0*、*3.1* および *3.2*:
  `http://docs.oracle.com/cd/E37444_01/html/E37451`
- Oracle Integrated Lights Out Manager バージョン 3.2.*x*:
  `http://docs.oracle.com/cd/E37444_01`
- Oracle Integrated Lights Out Manager バージョン 3.1.*x*:
  `http://docs.oracle.com/cd/E24707_01`
- Oracle Integrated Lights Out Manager バージョン 3.0.*x*:
  `http://docs.oracle.com/cd/E19860-01`

計算サーバーのセキュリティー保護

SuperCluster M7 には、1 台または 2 台の SPARC M7 サーバー (計算サーバー) がインストールされています。各計算サーバーは 2 つのハードウェアパーティション (2 つの PDomain) に分割されます。各 PDomian には、シャーシ内に搭載可能なプロセッサ、メモリー、および PCIe 拡張スロットの半分が備わっています。両方の PDomain は、同じシャーシ内の別々のサーバーとして動作します。各パーティションは、冗長化されたサービスプロセッサモジュール (SPM) のペアによって管理されます。

各 PDomain をセキュリティー保護する必要があります。

このセクションでは、計算サーバーのセキュリティー制御セットを示します。

▼ 計算サーバーへのログインとデフォルトパスワードの変更

Oracle ILOM から単一の PDomain にアクセスするには、その PDomain を制御しているアクティブな SPM にログインする必要があります。1 つのパーティションが引き続き正常に機能している間に、もう 1 つのパーティションを電源投入、リブート、または管理できます。

SuperCluster 計算サーバーには、さまざまな方法を使用してログインできます。このタスクで説明する方法では、計算サーバーの SPM 上の Oracle ILOM CLI にログインする必要があります。この方法を使用すると、次の状態のいずれかでサーバーにアクセスできます。

- スタンバイ電源モード

- システムの電源が投入されているが、ホストが実行されていない状態
- OP のブート中
- 完全に電源が投入され、OS が実行されている状態

1. **管理ネットワーク上で ssh コマンドを使用してログインします。**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **プロンプトが表示されたら、パスワードを入力します。**
   出荷時のデフォルトの `root` パスワードは `welcome1` です。
   パスワードの変更を求めるプロンプトが表示されたら、それに従ってください。
   この時点で、計算サーバー上の Oracle ILOM 上で実行されている任意のセキュリティータスクを実行できます。

3. **計算サーバーのホストコンソールにアクセスする場合は、ホストコンソールを起動します。**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

注記 - ホストが稼働していない場合、PDomain プロンプトは表示されません。

注記 - ふたたび Oracle ILOM プロンプトに切り替えるには、エスケープ文字 (デフォルトの文字は `#.`) を入力します。

4. **必要に応じて、スーパーユーザーの役割になります。**
   `su` コマンドを使用して、`root` の役割で構成されているユーザーに切り替えます。

デフォルトのアカウントとパスワード (計算サーバー)

アカウント	デフォルトのパスワード	説明
`root`	`welcome1`	Oracle ILOM では、最初に正常にログインした直後にデフォルトのパスワードを変更する必要があります。
`oracle`	`welcome1`	

アカウント	デフォルトのパスワード	説明
grid	welcome1	

▼ SuperCluster ソフトウェアバージョンの判別

1. **計算サーバーのいずれかにログインし、ホストコンソールにアクセスします。**
   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **このコマンドを入力します。**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

出力で ssc に付加された数値は、ソフトウェアのバージョンを表します。

SuperCluster ソフトウェアのバージョンを更新するには、My Oracle Support (https://support.oracle.com) から入手可能な最新の SuperCluster Quarterly Full Stack Download Patch をインストールします。

注記 - SuperCluster の場合、追加の制限によって、ソフトウェアのどのバージョンを使用できるのかが制限されたり、それらのバージョンの更新方法が制限されたりすることがあります。これらの状況では、Oracle の担当者に連絡してください。

▼ Secure Shell サービスの構成

このタスクを実行すると、Oracle SuperCluster に配備されている Secure Shell のセキュリティー構成を改善できます。

/etc/ssh/sshd_config ファイルは、Secure Shell サービスのパラメータを構成するシステム全体の構成ファイルです。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **/etc/ssh/sshd_config ファイルを編集します。**

3. **SuperCluster クライアントアクセスネットワークからの接続のみが受け入れられるように ListenAddress パラメータを構成します。**

ListenAddress の IP アドレスがクライアントネットワークに設定されていることを確認します。

これにより、管理または IB ネットワーク上のコンポーネント間で Secure Shell 接続を正常に開始できません。

4. **その他の sshd_config パラメータを確認し、サイトの要件に従って設定します。**

   Secure Shell サービスは、次の設定によってセキュリティー保護されます。

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
ClientAliveCountMax 0
```

5. **sshd_config ファイルを保存します。**

6. **サービスを再起動します。**

   変更を有効にするには、サービスを再起動する必要があります。

```
# svcadm restart ssh
```

▼ root が役割であることの確認

デフォルトでは、root がユーザーアカウントではなく、役割になるように Oracle Solaris が構成されています。さらに、SuperCluster 構成では匿名の root ユーザーによるログインが許可されません。代わりに、すべてのユーザーが通常のユーザーとしてログインしてから、root の役割になる必要があります。SuperCluster のすべての管理操作は、root を役割として使用して実行する必要があります。

1. **計算サーバーのいずれかにログインし、ホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **root 属性が type=role に設定されていることを確認します。**

```
# grep root /etc/user_attr
root::::type=role
```

3. **(オプション) 通常のユーザーに root の役割を割り当てます。**

```
# usermod -R root user_name
```

デフォルトの公開ネットワークサービス (計算サーバー)

この表には、計算サーバー上で公開されているデフォルトのネットワークサービスが一覧表示されています。

サービス名	プロトコル	ポート	説明
SSH	TCP	22	統合された Secure Shell サービスで CLI を使用して、計算サーバーへの管理アクセスを有効にするために使用されます。
HTTP (BUI)	TCP	80	統合された HTTP サービスでブラウザインタフェースを使用して、計算サーバーへの管理アクセスを有効にするために使用されます。
HTTPS (BUI)	TCP	443	統合された HTTPS サービスでブラウザインタフェースを使用して、暗号化された (SSL/TLS) チャネル上の計算サーバーへの管理アクセスを有効にするために使用されます。
SNMP	UDP	161	統合された SNMP サービスで、計算サーバーの健全性をモニターし、受信したトラップ通知をモニターする管理インタフェースを提供するために使用されます。

計算サーバーのセキュリティー構成の強化

次のトピックでは、計算サーバーをセキュアに構成する方法について説明します。

▼ intrd サービスの有効化

割り込みバランサ (intrd) サービスでは、最適なパフォーマンスが実現されるように、割り込みと CPU 間の割り当てがモニターされます。詳細は、intrd(1M) のマニュアルページを参照してください。

このサービスは、大域ゾーンでのみ実行されます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **サービスを起動します。**

```
# svcadm enable intrd
```

▼ 不要なサービスの無効化 (計算サーバー)

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **システムが NFS クライアントまたはサーバーではない場合は、NFS ステータスモニターを無効にします。**

   このサービスを `lockd(1M)` と同時に使用すると、NFS 上のロックサービスにクラッシュおよび回復機能が提供されます。

   ```
   # svcadm disable svc:/network/nfs/status
   ```

3. **まったく NFS を使用していない場合、または NFSv4 を使用している場合は、NFS のロックマネージャーサービスを無効にします。**

   NFS ロックマネージャーでは、NFSv2 および NFSv3 の NFS ファイル上でのレコードロック操作がサポートされています。

   ```
   # svcadm disable svc:/network/nfs/nlockmgr
   ```

4. **システムでファイルがマウントされていない場合は、NFS クライアントサービスを無効にするか、そのパッケージをアンインストールできます。**

   NFS クライアントサービスは、システム上のファイルが NFS サーバーからマウントされている場合にのみ必要です。詳細は、`mount_nfs(1M)` のマニュアルページを参照してください。

   ```
   # svcadm disable svc:/network/nfs/client
   ```

5. **NFS ファイルサーバー以外のシステム上で NFS サーバーサービスを無効にします。**

   NFS サーバーサービスでは、NFS バージョン 2、3、および 4 上のクライアントファイルシステム要求が処理されます。このシステムが NFS サーバーでない場合は、サービスを無効にします。

   ```
   # svcadm disable svc:/network/nfs/server
   ```

6. **DNS SRV レコードまたは LDAP ベースのリフェラル用に FedFS を使用していない場合は、サービスを無効にします。**

   フェデレーテッドファイルシステム (FedFS) クライアントサービスでは、FedFS 情報を格納する LDAP サーバーに関するデフォルトおよび接続情報が管理されます。

   ```
   # svcadm disable svc:/network/nfs/fedfs-client
   ```

7. **`rquota` サービスを無効にします。**

   `remote` 割り当てサーバーは、NFS 上でマウントされているローカルファイルシステムのユーザーに対する割り当てを返します。結果を `quota(1M)` で使用すると、リモートファイルシステムに対するユーザー割り当てが表示されます。通常、`rquotad(1M)` デーモンは `inetd(1M)` から呼び出されます。このデーモンによって、悪意のある可能性があるユーザーにネットワークに関する情報が提供されます。

```
# svcadm disable svc:/network/nfs/rquota
```

8. **cbd サービスを無効にします。**
   cbd サービスでは、NFS Version 4 プロトコル用の通信エンドポイントが管理されます。nfs4cbd(1M) デーモンは、NFS Version 4 クライアント上で実行され、コールバック用のリスナーポートを作成します。

```
# svcadm disable svc:/network/nfs/cbd
```

9. **NFSv4 を使用していない場合は、mapid サービスを無効にします。**
   NFS ユーザーとグループ ID とのマッピングデーモンサービスでは、NFS バージョン 4 の識別属性 owner および owner_group と、NFS バージョン 4 クライアントとサーバーの両方で使用されるローカル UID および GID 番号間がマップされます。

```
# svcadm disable svc:/network/nfs/mapid
```

10. **ftp サービスを無効にします。**
    FTP サービスでは、暗号化されていないファイル転送サービスが提供され、プレーンテキスト認証が使用されます。セキュアなコピープログラム scp(1) では、暗号化された認証およびファイル転送が提供されるため、ftp の代わりに、このプログラムを使用してください。

```
# svcadm disable svc:/network/ftp:default
```

11. **リモートのボリュームマネージャーサービスを無効にします。**
    リムーバブルボリュームマネージャーは、リムーバブルメディアとホットプラグ可能なストレージを自動的にマウントおよびアンマウントできる HAL 対応のボリュームマネージャーです。ユーザーが悪質のあるプログラムをインポートしたり、システムから機密データを転送したりする可能性があります。詳細は、rmvolmgr(1M) のマニュアルページを参照してください。
    このサービスは、大域ゾーンでのみ実行されます。

```
# svcadm disable svc:/system/filesystem/rmvolmgr
```

12. **smserver サービスを無効にします。**
    smserver サービスは、リムーバブルメディアデバイスにアクセスするために使用されます。

```
# svcadm disable rpc/smserver:default
```

13. **/etc/pam.d ディレクトリで r-protocol サービスの認証スタック用のモジュールとして、pam_deny.so.1 を指定します。**
    デフォルトでは、r-protocols、rlogin(1)、および rsh(1) などの旧バージョンのサービスはインストールされません。ただし、これらのサービスは /etc/pam.d で定

義されています。旧バージョンのサービスが有効になっている場合に、/etc/pam.d からサービスの定義を削除すると、その他のサービス (SSH など) がサービスで使用されます。

```
# cd /etc/pam.d
# cp rlogin rlogin.orig
# pfedit rlogin
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

14. /etc/default/keyserv ファイルを編集して、ENABLE_NOBODY_KEYS の値を NO に変更します。

keyserv サービスでは、nobody ユーザー鍵を使用できません。デフォルトでは、ENABLE_NOBODY_KEYS の値は YES です。

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

15. ftp アクセスを制限するユーザーを ftpusers ファイルに追加します。

すべてのユーザーが FTP ファイル転送を使用できる必要はありません。これを使用するには、権限を持つユーザーの名前とパスワードを指定する必要があります。一般に、システムユーザーには FTP の使用を許可しないようにしてください。このチェックでは、FTP の使用が許可されないように、システムアカウントが /etc/ftpd/ftpusers ファイルに含まれていることが確認されます。

/etc/ftpd/ftpusers ファイルは、ユーザーによる FTP サービスの使用を禁止するために使用されます。少なくとも、すべてのシステムユーザー (root、bin、adm など) を含めてください。

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

16. FTP サーバーで作成されたファイルに、強固なデフォルトのファイル作成マスクを設定します。

FTP サーバーでは、必ずしもユーザーのシステムファイル作成マスクを使用する必要はありません。FTP umask を設定すると、FTP 経由で転送されたファイルで強固なファイル作成 umask が使用されます。

```
# pfedit /etc/proftpd.conf
Umask          027
```

17. **ネットワークトポロジクエリーへの応答を無効にします。**

    エコー要求への応答を無効にすることが重要です。ICMP 要求は、`ipadm` コマンドを使用して管理されます。

    このように設定することで、ネットワークトポロジに関する情報が流布されることが回避されます。

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip
```

18. **リダイレクト ICMP メッセージを無効にします。**

    ルーターは ICMP リダイレクトメッセージを使用して、ホストに宛先へのより直接的なルートを通知します。不正な ICMP リダイレクトメッセージによって、中間者攻撃を受ける可能性があります。

```
# ipadm set-prop -p _ignore_redirect=1 ipv4
```

19. **リモート端末への `talk(1)` および `write(1)` アクセスを回避するために、`mesg(1)` を無効にします。**

```
# mesg -n
```

20. **(オプション) ネットワーク上で待機している不要なサービスを確認し、無効にします。**

    デフォルトでは、ネットワークパケットを送受信できる唯一のネットワークサービスは `ssh(1)` です。

```
# svcadm disable FMRI_of_unneeded_service
```

▼ 厳格なマルチホーミングの有効化

ほかのドメインへのゲートウェイであるシステム (ファイアウォールや VPN ノードなど) では、厳格なマルチホーミングを有効にする必要があります。`hostmodel` プロパティーは、マルチホームシステム上での IP パケットの送受信動作を制御します。別のインタフェース上でパケットが受け入れられないように、厳格なマルチホーミングを `1` に設定します。デフォルトは `0` です。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

    53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **厳格なマルチホーミングを `1` に設定します。**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

▼ ASLR の有効化

注記 - データベースドメインまたはデータベースゾーン内の ASLR は有効にしないでください。

Oracle Solaris では、アドレス空間レイアウトのランダム化 (ASLR) を有効にするために、多くのユーザーバイナリにタグが付けられます。ASLR では、アドレス空間の主要な部分の開始アドレスがランダム化されます。このセキュリティー防御メカニズムにより、ソフトウェアの脆弱性を悪用しようとする ROP (Return Oriented Programming) 攻撃を失敗させることができます。ゾーンは、そのプロセス用にこのランダム化されたレイアウトを継承します。すべてのバイナリにとって ASLR を使用することが最適とは限らないため、ASLR はゾーンおよびバイナリレベルで構成できます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **ASLR を有効にします。**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS                CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

▼ TCP 接続の構成

ポートごとに 1 つの IP アドレス当たりの半開き TCP 接続の最大数を 4096 に設定すると、SYN フラッドサービス拒否攻撃から防ぐことができます。キューに入れられる受信接続の最大数を 1024 以上に設定すると、特定の分散サービス拒否 (DDoS) 攻撃から防ぐことができます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **半開きでキューに入れられる受信 TCP 接続の最大数を設定します。**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

▼ PCI に準拠するためのパスワード履歴ログとパスワードポリシーの設定

/etc/default/passwd ファイルに HISTORY パラメータを指定すると、ユーザーが HISTORY 値を含む同様のパスワードを使用できなくなります。

MINWEEKS が 3 に設定され、HISTORY が 10 に設定されている場合は、パスワードを 10 か月間再使用できません。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **/etc/default/passwd ファイルを編集して、パスワードパラメータを設定します。**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **これらのパラメータが含まれるように /etc/default/login ファイルを編集します。**

```
# pfedit /etc/default/login
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

▼ ユーザーのホームディレクトリが適切なアクセス権を持っていることの確認

ホームディレクトリは、所有者によって書き込み可能および検索可能である必要があります。通常、その他のユーザーはこれらのファイルを変更したり、ユーザーのホームディレクトリにファイルを追加したりする権利を持っていません。これに該当することを確認するには、ユーザーのディレクトリ上でアクセス権を設定します。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **ユーザーのディレクトリ上でアクセス権を設定します。**

```
# chmod 750 /export/home/user_home_directory
```

▼ IP フィルタファイアウォールの有効化

IP フィルタは、ステートフルパケットフィルタリングとネットワークアドレス変換 (NAT) を提供するホストベースのファイアウォールです。パケットのフィルタリングは、ネットワークベースの攻撃に対する基本的な保護を提供します。IP フィルタにはステートレスパケットフィルタリングも備わっているため、アドレスプールを作成および管理できます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **IP フィルタファイアウォールを有効にします。**

```
# svcadm svc:/network/ipfilter:default
```

▼ ネームサービスでローカルファイルのみが使用されていることの確認

OS では、hosts、`ipnodes`、users (`passwd(4)`、`shadow(4)`、`user_attr(4)`)、および `groups` に関する情報のデータベースが数多く使用されています。これらの項目に関するデータは、さまざまなソースから取得されます。たとえば、ホスト名とホストアドレスは、`/etc/hosts`、NIS、LDAP、DNS、またはマルチキャスト DNS で見つけることができます。これらの項目でローカルファイルエントリのみが使用されている場合は、制限されている環境内のシステムがさらにセキュアになります。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **ローカルファイルのみが使用されるようにネームサービスを構成します。**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

▼ Sendmail と NTP サービスの有効化

sendmail サービスが実行中である必要があります。それ以外の場合は、`root` に重要なシステムメールが配信されません。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **sendmail を有効にします。**

```
# svcadm enable smtp:sendmail
```

3. **必要に応じて、NTP サービスをインストールします。**

セキュリティーやコンプライアンスが必要なすべてのシステム上で、`ntp` サービスをインストールする必要があります。

```
# pkg install service/network/ntp
```

4. **NTP サービスをクライアントとして構成し、サービスを有効にします。**

ネットワークタイムプロトコルデーモンが有効になっていて、クライアントとして適切に構成されている必要があります。`/etc/inet/ntp.conf` ファイルには、少なくとも 1 つのサーバー定義が含まれている必要があります。クライアントがサーバーとしても機能しないようにするには、ファイルに `restrict default ignore` 行も含まれている必要があります。

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

▼ GSS の無効化 (Kerberos を使用していない場合)

汎用セキュリティーサービス (gss) では、Generic Security Service Application Program Interface (GSS-API) セキュリティートークンの生成および検証が管理されます。gssd (1M) デーモンは、カーネル rpc と GSS-API 間で動作します。

注記 - このサービスは Kerberos で使用されます。Kerberos が構成および使用されていない場合は、rpc/gss サービスを無効にします。

---

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **rpc/gss を有効にします。**

```
# svcadm enable rpc/gss
```

3. **/tmpfs のサイズ制限を設定します。**
デフォルトでは、tmpfs ファイルシステムのサイズは無制限です。パフォーマンスへの影響を避けるために、それぞれの tmpfs マウントのサイズを制限できます。詳細は、mount_tmpfs(1M) および vfstab(4) のマニュアルページを参照してください。

```
# pfedit /etc/vfstab
...
swap - /tmp tmpfs - yes size=sz
```

4. **計算サーバーをリブートします。**

```
# reboot
```

▼ だれでも書き込めるファイルへのスティッキービットの設定

ディレクトリ上にスティッキービットを設定すれば、だれでも書き込めるディレクトリ内のファイルを、ファイルの所有者や root の役割を除く任意のユーザーが削除または移動できなくなります。この設定は、多数のユーザーに共通のディレクトリ (/tmp ディレクトリなど) で役立ちます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **`/tmp` およびその他のだれでも書き込めるファイル上にスティッキービットを設定します。**

```
# chmod 1777 /tmp
```

▼ コアダンプの保護

コアダンプには機密データが含まれている可能性があります。ファイルへのアクセス権およびコアダンプイベントのロギングを保護に含めることができます。`coreadm(1m)` および `chmod(1M)` のマニュアルページを参照してください。

現在の構成を表示および設定するには、`coreadm` コマンドを使用します。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **現在の構成を表示します。**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **コアファイルを構成して、コアダンプディレクトリを保護します。**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
          -d process -d proc-setid
```

4. **アクセス権を確認します。**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **ディレクトリ上でアクセス権を適切に設定します。**

```
# chmod 700 /var/share/cores
```

▼ 非実行可能スタックの適用

非実行可能スタックを有効にすることは、特定の種類のバッファーオーバーフロー攻撃を阻止するための非常に有用な方法です。Oracle Solaris の `nxstack` を有効にすると、プロセススタックメモリーのセグメントに非実行可能のマークが付けられます。この拡張機能によって、悪意のあるコードの侵入やスタック上の実行に依存する攻撃から防御されます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **`nxstack` を有効にします。**

```
# sxadm set model=all nxstack
```

3. **構成を確認します。**

```
# sxadm get all nxstack
EXTENSION     PROPERTY     VALUE
nxstack         model        all
```

▼ 暗号化されたスワップ空間の有効化

ZFS ボリュームであるのか、raw デバイスであるのかに関係なく、スワップ空間は暗号化してください。暗号化すると、これらのページをシステムからディスクにスワップアウトする必要がある場合に、ユーザーパスワードなどの機密データが保護されます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **`/etc/vfstab` ファイルを編集して、`swap` を `encrypted` に設定します。**

```
# pfedit /etc/vfstab
```

```
...
/dev/zvol/dsk/rpool/swap - - swap - no encrypted
```

3. **PKCS #11 キーストアを作成して初期化します。**

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. **対称鍵を生成して、PKCS #11 キーストアに格納します。**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

▼ 監査の有効化

監査ログですべての管理アクション (引数を付けたコマンドを含む) が取得されることを確認します。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **監査機能を構成します。**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

▼ 大域ゾーンでのデータリンク (なりすまし) 保護の有効化

Oracle Solaris のデータリンクを保護すると、悪意のあるゲスト VM がネットワークにアクセスすることで発生する可能性のある損害が回避されます。

スヌープスプーフィング構成を有効にすると、仮想環境のネットワークトラフィックをホストシステムで送受信される幅広いトラフィックから分離できることで、ネットワークのパフォーマンスが改善されます。リンクを保護すると、悪意のあるゲスト VM がネットワークにアクセスすることで発生する可能性のある損害が回避されます。この機能によって、次の基本的な脅威から保護されます。

- IP および MAC のなりすまし

- Bridge Protocol Data Unit (BPDU) 攻撃などの L2 フレームのなりすまし

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **リンク保護を設定します。**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof net0
```

3. **構成を確認します。**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
                                   ip-nospoof    ip-nospoof         --         ip-nospoof,

                                   dhcp-nospoof  dhcp-nospoof       --         dhcp-nospoof
```

4. **リンク上で許可される IP を設定します。**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

▼ 非大域ゾーンでのデータリンク (なりすまし) 保護の有効化

SuperCluster 環境内に配備されているすべての Oracle Solaris 非大域ゾーンに、Oracle Solaris のデータリンク保護を個別に適用することもできます。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **`zonecfg(1M)` コマンドを使用して、特定のネットワークインタフェース上でデータリンクの保護を適用します。**
   許可される IP アドレスのリストが正確かつ完全であることを確認します。このリストには、Oracle Solaris IPMP や Oracle Real Application Clusters などで使用される任意の仮想 IP アドレスを含める必要があります。また、SuperCluster 非大域ゾーンの構成に行われた変更は、非大域ゾーンが再起動するまで有効にならないことにも注意してください。

```
# zonecfg -z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

▼ 暗号化された ZFS データセットの作成

保存データを保護する必要がある組織は、暗号化された ZFS データセットを使用することで、ゾーン配備されたアプリケーションおよび情報がさらに保護されるように選択できます。管理者の介入なしで各非大域ゾーンを起動できるようにするために、個々のデータベースまたはアプリケーションドメイン内でローカルに格納されている ZFS 暗号化鍵にアクセスするように、暗号化された ZFS データセットが構成されています。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**
   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **ZFS 暗号化鍵を作成します。**
   必要な鍵を作成するための簡単な方法は、次のようなコマンドを使用する方法です。

   ```
   # zfs createzfs_pool_name/zfskeystore
   $ chown root:root /zfs_pool_name/zfskeystore
   $ chmod 700 /zfs_pool_name/zfskeystore
   $ pktool genkey keystore=file keytype=aes keylen=256 \
   outkey=/zfs_pool_name/zfskeystore/zone_name.key
   ```

3. **暗号化された ZFS データセットを作成します。**

   ```
   # zfs create -o encryption=aes-256-ccm -o \
   keysource=raw,file:///zfs_pool_name/zone_name.key \
   zfs_pool_name/zone_name
   ```

4. **u01 および共通データセットを暗号化します。**
   このように同じアプローチを使用すると、サイト固有の要件およびポリシーに応じて、同じ (SuperCluster 固有の) 鍵とデータセットごとに一意の鍵のいずれかを使用して、u01 および共通データセットを暗号化できます。この例では、ステップ 3で作成されたものと同じ鍵を使用して、共通データセットが作成されています。追加の ZFS 構成パラメータ (compression など) は、これらの追加データセットの作成時にも定義できます。

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

▼ (オプション) キーストアへのアクセス用のパスフレーズの設定

以前のタスク72 ページの「暗号化された ZFS データセットの作成」では、ローカルで定義されている (raw) 鍵ファイルが使用されます。このファイルは、ファイルシステム上に直接格納されている必要があります。鍵を格納する別の方法では、*Sun Software PKCS #11* ソフトトークンと呼ばれる、パスフレーズで保護された PKCS #11 キーストアが使用されます。この方法を使用するには、次のタスクを実行します。

鍵が ZFS で使用可能になる前に、PKCS #11 キーストアのロックを手動で解除する必要があります。最後に、これは、暗号化された ZFS データセットをマウントする (ゾーンでも暗号化された ZFS データセットが使用されている場合は、非大域ゾーンを起動する) には、管理者が手動で介入する必要があることを意味します。その他の鍵の格納方針の詳細は、`zfs_encrypt(1M)` のマニュアルページを参照してください。

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **キーストアにアクセスするために必要となる PIN (パスフレーズ) を設定します。**

   新しい PKCS #11 キーストアに関連付けられたデフォルトの PIN は `changeme` です。この例では、このパスフレーズが 1 番目のプロンプトで使用されています。

```
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

3. **鍵を別の場所に格納するには、`${SOFTTOKEN}` 環境変数を定義します。**

   デフォルトでは、PKCS #11 Softtoken で使用される鍵マテリアルが `/var/user/${USERNAME}/pkcs11_softtoken` ディレクトリに格納されます。`${SOFTTOKEN}` 環境変数を定義すると、鍵マテリアルを別の場所に格納できます。この機能を使用すると、このパスフレーズで保護されている鍵マテリアルで SuperCluster 固有の格納を有効にすることができます。

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
Enter token passphrase:
```

```
Create new passphrase:
Re-enter new passphrase:
```

4. **鍵を作成します。**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **前の手順で作成された鍵を参照している暗号化された ZFS データセットを作成します。**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

▼ 不変大域ゾーンの作成

不変性を使用して改ざんを防止することで、大域ゾーンおよび非大域ゾーンに回復性と高い整合性を持つオペレーティング環境を作成できます。このような環境内では、SuperCluster 計算サーバー独自のサービスが動作します。不変ゾーンでは、Oracle Solaris の大域ゾーンおよび非大域ゾーンの固有のセキュリティー機能に基づいて、(一部またはすべての) OS ディレクトリおよびファイルを (管理者の介入なしで) 変更できません。このような読み取り専用の状態を適用すると、未承認の変更を回避したり、さらに強力な変更管理の手順を推進したり、カーネルベースとユーザーベースの両方のマルウェアの侵入を抑止したりできます。

注記 - 不変ゾーンは一度構成されると、トラステッドパスログインから、または `reboot -- -w` を使用して書き込み可能モードでシステムをリブートするとき以外は更新できません。

アプリケーションソフトウェアが不変環境で期待どおりに動作していることを常に確認する場合は、Oracle Solaris の不変大域ゾーン内で Oracle Database インスタンスと Oracle RAC クラスタが正常に実行されていることを確認してください。

1. **スーパーユーザーとして Oracle Solaris の大域ゾーン (専用ドメイン、ルートドメイン、または I/O ドメイン) にログインします。**

53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **`file-mac-profile` プロパティーを設定して、Oracle Solaris 大域ゾーンの構成を変更します。**

```
# zonecfg -z global set file-mac-profile=fixed-configuration
```

```
zonecfg:global> commit
```

3. **変更を有効にするために、Oracle Solaris 大域ゾーンをリブートします。ILOM コンソールからドメインにログインします。**

4. **不変大域ゾーンのトラステッドパスコンソールを起動します。**
   不変大域ゾーンが構成されたら、次のブレークシーケンスのいずれかを使用してコンソールログインを入力することが重要となります。

   - **グラフィカルコンソール** –F1-A
   - **シリアルコンソール** –<Break> または代替のブレークシーケンス (CR~ Ctrl-b)

```
trusted path console login:
```

5. **I/O ドメインの大域ゾーンにログインし、`root` の役割になってシステムへの特定の更新を実行します。次に、システムをリブートして読み取り専用モードに戻ります。**

```
# reboot
```

▼ 不変非大域ゾーンの構成

不変になるように Oracle Solaris 非大域ゾーンを構成するには、このタスクを実行します。

注記 - Oracle Solaris 11 OS では、このタスクで確認された構成 (fixed-configuration) よりも多くの追加の不変ゾーン構成がサポートされています。これらのオプションの詳細は、`zonecfg(1M)` のマニュアルページを参照してください。ただし、SuperCluster アーキテクチャーの一部として fixed-configuration オプションしかテストされていません。

注意 - このタスクで説明するように、Oracle Solaris 非大域ゾーンの不変性が有効になると、ゾーンのユーザーアカウントとパスワードの追加、変更、または削除を実行できなくなります。ただし、ゾーン固有の情報 (ユーザー、役割、グループ、権利プロファイルなど) が含まれる LDAP ディレクトリを配備することで、この問題は解決できます。

注意 - Oracle Solaris の不変ゾーン機能は、Oracle Solaris 非大域ゾーンにデフォルトで実装される ZFS データセットに制限されています。追加のファイルシステム、プール、またはデータセットは、不変ゾーンポリシーの対象ではありません。ただし、読み取り専用のループバックマウントを使用するなど、その他の方法を使用すれば、それらのファイル要素へのアクセスを制御できます。

---

1. **計算サーバーのいずれかにログインし、スーパーユーザーとしてホストコンソールにアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **Oracle Solaris 非大域ゾーンが停止していることを確認します。**

   このコマンドで値が返される場合は、Oracle Solaris 非大域ゾーンが実行中であるため、停止する必要があります。

   注記 - `zoneadm(1M)` コマンドを使用してゾーンを停止できる場合は、組織で確立された適切な停止手順に従って、サービスの中断やデータの損失が発生する可能性を回避してください。

   ```
   # zoneadm list | grep -w "zone_name"
   ```

3. **`file-mac-profile` ゾーン構成プロパティーを設定して、Oracle Solaris 非大域ゾーンの構成を調整します。**

   ```
   # zonecfg -z zone_name set file-mac-profile=fixed-configuration
   ```

4. **必要に応じて、不変非大域ゾーンの構成を無効にします。**

   ```
   # zonecfg -z zone_name set file-mac-profile=none
   ```

5. **変更を有効にするために、Oracle Solaris 非大域ゾーンを再起動します。**

   ```
   # zoneadm -z zone_name boot
   ```

▼ セキュアなベリファイドブートの有効化 (Oracle ILOM CLI)

Oracle ILOM CLI からセキュアなベリファイドブートを有効にするには、このタスクを使用します。また、Oracle ILOM Web インタフェースを使用することもできます。78 ページの「セキュアなベリファイドブート (Oracle ILOM Web インタフェース)」を参照してください。

ベリファイドブートとは、デジタル署名を使用して、実行前にオブジェクトモジュールを検証することです。Oracle Solaris では、不正なカーネルモジュールがロードされないように保護されます。ベリファイドブートでは、実行前にカーネルモジュールが検証されるため、Oracle Solaris の安全性と堅牢性が増加します。

有効にすると、モジュールをロードして実行する前に、Oracle Solaris のベリファイドブートによってカーネルモジュールで出荷時に行われた署名がチェックされます。このチェックでは、モジュールの偶発的な変更や悪意のある変更が検出されます。実行されたアクションは構成可能です。これを有効にすると、警告メッセージが出力され、モジュールのロードおよび実行が続行されるか、または失敗し、モジュールがロードおよび実行されません。

1. **計算サーバー上の Oracle ILOM にアクセスします。**

   53 ページの「計算サーバーへのログインとデフォルトパスワードの変更」を参照してください。

2. **ベリファイドブートを有効にします。**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **Oracle で提供された証明書にアクセスし、表示します。**

   事前にインストールされたベリファイドブートの証明書ファイル `/etc/certs/ORCLS11SE` は、Oracle ILOM の一部として提供されています。

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **証明書のロードを開始します。**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **`/etc/certs/ORCLS11SE` ファイルの内容をコピーし、Oracle ILOM コンソールにペーストします。**

   情報を保存して処理するには、Ctrl-Z を押します。

   変更を終了して破棄するには、Ctrl-C を押します。

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. **証明書を検証します。**

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. **OBP の `use-nvram` パラメータが `false` に設定されていることを確認します。**

   ベリファイドブートを使用する場合は、OBP の `use-nvram` パラメータを `false` に設定する必要があります。このように設定すると、ベリファイドブート機能が無効になるように OBP を変更できなくなります。デフォルト値は false です。Oracle Solaris にログインして、次のように入力します。

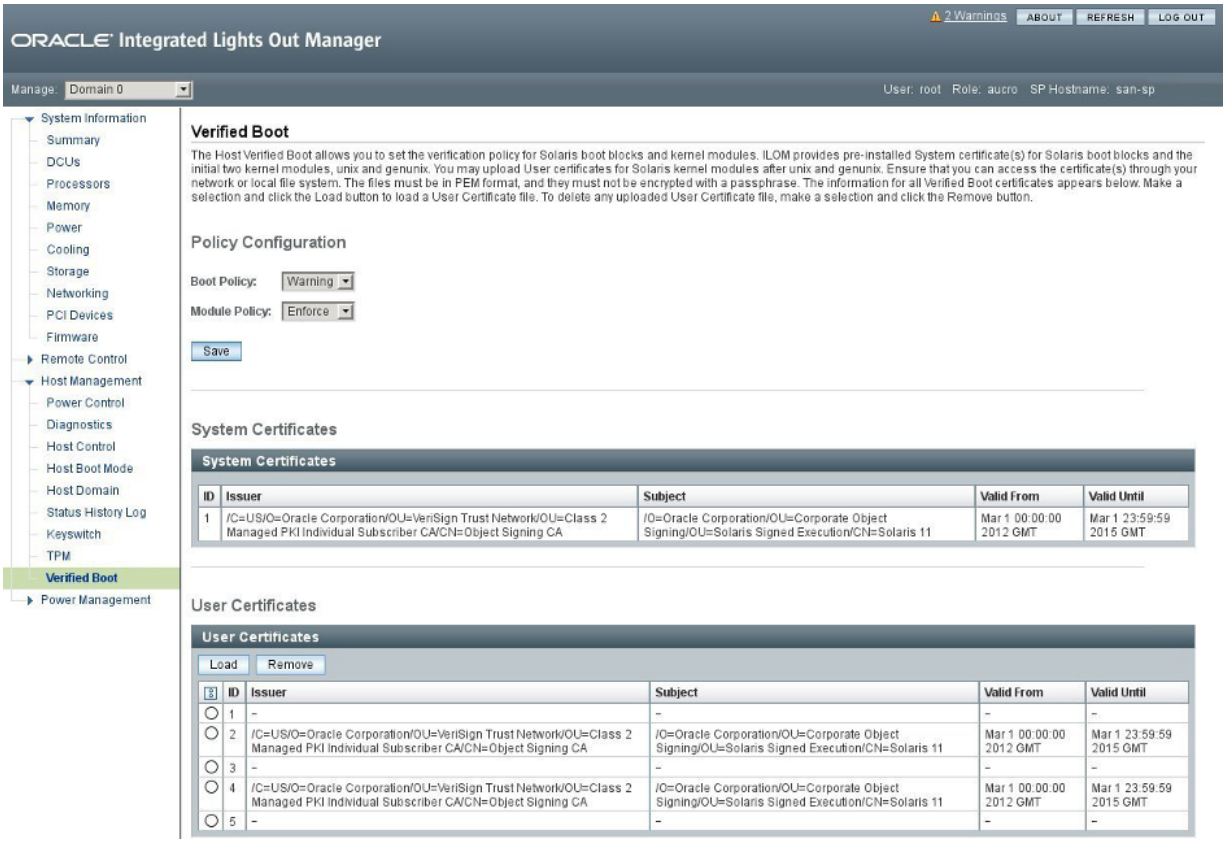
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

セキュアなベリファイドブート (Oracle ILOM Web インタフェース)

Oracle ILOM Web インタフェースでも、ベリファイドブートポリシー変数の設定および証明書ファイルの管理がサポートされているため、CLI と同じ機能が提供されます。ホスト管理ナビゲーションメニューの下にある「Verified Boot」リンクに移動します。

例:



追加の計算サーバーリソース

Oracle Solaris OS および Oracle Solaris Cluster のセキュリティーガイドについては、使用している OS バージョンに対応したドキュメントライブラリを参照してください。ライブラリは、http:/docs.oracle.com/en/operating-systems で入手できます。

Oracle VM Server for SPARC に関するセキュリティー情報については、http://docs.oracle.com/cd/E62357_01 にあるセキュリティーガイドを参照してください。

計算サーバーハードウェアに関するセキュリティー情報については、http://docs.oracle.com/cd/E55211_01 にあるセキュリティーガイドを参照してください。

ZFS Storage Appliance のセキュリティー保護

ZFS Storage Appliance は、ビジネスインテリジェンス、データウェアハウス、仮想化、開発およびテスト、およびデータ保護といった要求のきびしいさまざまなワークロードで、ストレージの統合をサポートするための SuperCluster コンポーネントの 1 つです。

ZFS Storage Appliance には 2 つの冗長 ZFS ストレージコントローラが含まれています。両方のコントローラをセキュリティー保護する必要があります。

これらのセクションでは、ZFS Storage Appliance のセキュリティーのガイドラインおよび機能について説明します。

▼ ZFS Storage Appliance へのログイン

このセクションのセキュリティータスクを実行するには、管理ネットワークを介して ZFS Storage Appliance にログインします。

このタスクでは、CLI を使用してログインする方法について説明します。Oracle ILOM Web インタフェースにログインする場合の同等な手順については、『*Oracle ZFS Storage Appliance* 管理ガイド』を参照してください。91 ページの「追加の ZFS Storage Appliance のリソース」を参照してください。

1. **管理ネットワーク上で、SSH を使用して ZFS Storage Appliance に接続します。**
   このアプライアンスを管理するほかのユーザーを構成していない場合は、`root` としてログインする必要があります。

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **必要に応じて、CLI ヘルプにアクセスします。**

   `help` コマンドはコンテキストヘルプを提供します。特定のトピックのヘルプは、そのトピックを `help` の引数として指定することによって使用できます。使用可能なトピックは、help コマンドをタブ完了するか、または `help topics` を入力することによって表示されます。

▼ ZFS Storage Appliance ソフトウェアのバージョンの判別

ZFS Storage Appliance 上のソフトウェアのバージョンを判別するには、この手順を使用します。

1. **ZFS Storage Appliance にログインします。**

   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **ソフトウェアのバージョンを表示します。**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

この例では、ZFS Storage Appliance ソフトウェアはバージョン `2013.06.05.2.10` です。

ZFS Storage Appliance ソフトウェアのバージョンを更新するには、`https://support.oracle.com` の My Oracle Support から入手可能な最新の SuperCluster Quarterly Full Stack Download Patch をインストールします。

注記 - SuperCluster の場合、追加の制限によって、ZFS Storage Appliance ソフトウェアのどのバージョンを使用できるのかが制限されたり、それらのバージョンの更新方法が制限されたりすることがあります。これらの状況では、Oracle の担当者に連絡してください。

▼ ZFS Storage Appliance の root パスワードの変更

ZFS Storage Appliance 自体は、デフォルトの root パスワードを使用して事前構成されていません。ZFS Storage Appliance の初期構成は、その組み込み Oracle ILOM からコンソールセッションを介して実行されます。アプライアンスの root パスワードはこの初期構成セッション中に設定されます。

最初にアプライアンスのコンソールにアクセスすると、シェルインタフェース構成画面が表示されます。画面の情報を確認し、必要な値を入力します。ZFS Storage Appliance の root パスワードはこのプロセス中に設定されます。

注記 - アプライアンス用 Oracle ILOM には、デフォルトの root アカウントとパスワード welcome1 が設定されています。37 ページの「Oracle ILOM のセキュリティー保護」を参照してください。

---

root アカウントを作成したら、このタスクの説明に従っていつでもパスワードを変更できます。

注記 - Oracle Engineered Systems Hardware Manager で管理される任意の SuperCluster コンポーネント (AFS ストレージコントローラ OS など) のパスワードが変更された場合は、Oracle Engineered Systems Hardware Manager でもパスワードを更新する必要があります。詳細は、『*Oracle SuperCluster M7* シリーズ管理ガイド』を参照してください。

---

1. **ZFS Storage Appliance にログインします。**

   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **root パスワードを変更します。**

   この例では、*password* を米国国防総省のパスワードの複雑性ポリシーに準拠するパスワードで置き換えます。

```
hostname:> configuration users select root set initial_password=password initial_password = *************
hostname:configuration users> done
```

ZFS Storage Appliance の初期インストールおよび構成の詳細は、*Oracle ZFS Storage Appliance* の設置ガイドを参照してください。91 ページの「追加の ZFS Storage Appliance のリソース」を参照してください。

デフォルトの公開ネットワークサービス (ZFS Storage Appliance)

この表は、ZFS Storage Appliance によって公開されているデフォルトのネットワークサービスが一覧表示されています。

サービス	プロトコル	ポート	説明
SSH	TCP	22	Secure Shell サービスで、CLI を使用して ZFS Storage Appliance への管理アクセスを有効にするために使用されます。
PORTMAP	TCP/UDP	111	リモート手続き呼び出し (RPC) ポートマッピングデーモン (`rpcbind` または `portmap` と呼ばれます) によって使用されます。このサービスは、NFS バージョン 3 をサポートする必要があります。
NTP	UDP	123	ローカルシステムクロックを 1 つ以上の外部時間ソースと同期させるために、統合された Network Time Protocol (NTP) サービス (クライアントのみ) によって使用されます。
HTTPS (BUI)	TCP	215	統合された HTTPS サービスでブラウザインタフェースを使用して、ZFS Storage Appliance への暗号化された (SSL/TLS) チャネルを介した管理アクセスを有効にするために使用されます。
リモートレプリケーション	TCP	216	統合されたリモートデータレプリケーションサービスによって使用されます。リモートデータレプリケーションは、暗号化された (SSL/TLS) チャネルを介して、プロジェクトやシェアを ZFS Storage Appliance 間で複製および同期します。
NFS	TCP/UDP	2049 4045 各種	ネットワークファイルシステム (NFS) サービスによって使用されます。NFS は、ネットワークファイル共有サービスを提供します。実際のポート番号は、NFS プロトコルのどのバージョンが使用されるのかによって異なります。NFS バージョン 3 は、マウント、ステータス、割り当て、および関連サービスを提供するために RPC ポートマッピングデーモン (前述) と動的に割り当てられたポートに依存します。ただし、NFS バージョン 4 は、TCP/2049 のみに依存します。NFS ロックサービスは、TCP/4045 を使用します。
iSCSI / iSNS	TCP	3260	IP ベースのストレージネットワーキングプロトコルを提供する iSCSI サービスで、データストレージ機能をリンクするために使用されます。ZFS Storage Appliance は、ネットワークに接続されたクライアントと iSCSI デバイス (LUN と呼ばれます) を共有するように構成できます。
サービスタグ	TCP	6481	Oracle サービスタグサービスによって使用されます。これは、サーバーを識別し、サービス要求を容易にするための Oracle の発見プロトコルです。このサービスは、ZFS Storage Appliance ソフトウェアを検索したりその他の Oracle の自動サービスソリューションと統合したりするために、Oracle Enterprise Manager Ops Center などの製品によって使用されます。
NDMP	TCP	10000	リモートで調整されたバックアップに ZFS Storage Appliance が参加できるようにするために、Network Data Management Protocol (NDMP) サービスによって使用されます。

ZFS Storage Appliance は、`HTTP`、`FTP`、`SFTP`、`TFTP`、`WebDAV` など、デフォルトでは無効になっている各種のその他サービスもサポートします。設置後にこれらのサービスが有効になった場合、追加のネットワークポートが公開される可能性があります。

ZFS Storage Appliance のセキュリティー構成の強化

これらのトピックでは、ZFS Storage Appliance のセキュリティー構成を強化する方法について説明します。

▼ Oracle ILOM のセキュリティー構成の強化の実装

ZFS Storage Appliance には、製品の一部として Oracle ILOM が組み込まれています。その他の Oracle ILOM 実装と同様に、デバイスのデフォルトセキュリティー構成を改善するために、セキュリティー関連の構成の変更を実装できます。

- **37 ページの「Oracle ILOM のセキュリティー保護」の手順を実行することによって、ZFS Storage Appliance の Oracle ILOM インタフェースをセキュリティー保護します。**

▼ 不要なサービスの無効化 (ZFS Storage Appliance)

プラットフォームの運用および管理要件をサポートするために必要がないサービスを無効にします。

デフォルトで ZFS Storage Appliance はネットワークのデフォルトでのセキュリティー強化 *(Secure By Default)* 構成を採用します。この構成では、重要でないサービスは無効になっています。ただし、セキュリティーポリシーおよび要件に基づいて、追加のサービスを有効または無効にしなければならない場合があります。

1. **ZFS Storage Appliance にログインします。**

81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **ZFS Storage Appliance によってサポートされているサービスのリストを表示します。**

```
hostname:> configuration services
```

3. **特定のサービスが有効になっているかどうかを確認します。**
servicename を ステップ 2 で識別されているサービス名に置き換えます。

```
hostname:> configuration services servicename get <status>
```

サービス状態パラメータが値 `enabled` の値を返す場合、サービスは有効です。例:

```
hostname:> configuration services iscsi get <status>
<status> = online
```

4. **必要がなくなったサービスを無効にします。**
サービスの状態を無効に設定します。例:

```
hostname:> configuration services iscsi disable
```

▼ 動的ルーティングの無効化

ZFS Storage Appliance は、デフォルトで動的ルーティングプロトコルを実行するように構成されています。

動的ルーティングサービスを無効にする前に、ZFS Storage Appliance が通信する必要があるネットワークに直接接続されていることを確認するか、静的ルーティングまたはデフォルトルートを使用するように構成されていることを確認します。動的ルーティングが無効になったあとに接続が失われることがないようにするため、この手順が必要です。

1. **ZFS Storage Appliance にログインします。**
81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **動的ルーティングを無効にします。**

```
hostname:> configuration services dynrouting disable
```

3. **動的ルーティングが有効になっているかどうかを確認するには、次のように入力します。**

```
hostname:> configuration services dynrouting get <status>
```

▼ Secure Shell を使用したリモート root アクセスの制限

デフォルトでは、ZFS Storage Appliance は Secure Shell (SSH) サービスを使用して root アカウントへのリモート管理アクセスを許可するように構成されています。

SSH を使用してリモート root アクセスを無効にするには、この手順を使用します。

この構成変更が行われると、root アカウントは SSH を使用してシステムにアクセスできなくなります。ただし、root アカウントは、HTTPS 管理インタフェースを使用してこのシステムにアクセスできます。

1. **ZFS Storage Appliance にログインします。**
   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **リモート root アクセスを無効にします。**

   ```
   hostname:> configuration services ssh set permit_root_login=false
   ```

3. **root アカウントが SSH を使用してシステムにアクセスできなくなったことを確認します。**

   ```
   hostname:> configuration services ssh get permit_root_login
   ```

4. **SSH 管理アクセスが必要な場合は、少なくとも 1 つの非 root アカウントを作成します。**
   手順については、ZFS Storage Appliance 上で実行されているリリースに対応した『*Oracle ZFS Storage Appliance* 管理ガイド』を参照してください。91 ページの「追加の ZFS Storage Appliance のリソース」を参照してください。

▼ 管理インタフェースの非アクティブタイムアウトの構成 (HTTPS)

ZFS Storage Appliance は、事前に定義された分数非アクティブになっている管理セッションを切断してログアウトする機能がサポートされています。デフォルトでは、ブラウザユーザーインタフェース (HTTPS) は 15 分後にセッションがタイムアウトします。

注記 - ZFS Storage Appliance の SSH コマンド行インタフェースで非アクティビティータイムアウトを適用する同等のパラメータはありません。

非アクティビティータイムアウトパラメータをカスタム値に設定するには、この手順を使用します。

1. **ZFS Storage Appliance にログインします。**
   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **ブラウザインタフェースに関連付けられた現在の非アクティブタイムアウトパラメータを表示します。**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **タイムアウトパラメータを構成します。**
   `session_timeout` の値は分で指定されます (この例では 10 分)。

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **ステップ 2 を繰り返してタイムアウトパラメータを確認します。**

▼ 未承認の SNMP プロトコルの無効化

デフォルトでは、ZFS Storage Appliance で SNMPv1 および SNMPv2c が有効になっています。 ZFS Storage Appliance では、製品のすべてのサポートされるバージョンにおいて SNMPv1/v2c をサポートします。バージョン 2013.1.2 以降、ZFS Storage Appliance では SNMPv3 もサポートしています。

注記 - SNMP プロトコルのバージョン 3 では、ユーザーベースのセキュリティーモデル (USM) のサポートが導入されました。この機能は、従来の SNMP コミュニティー文字列を、特定のアクセス権、認証、およびプライバシプロトコルで構成可能な実際のユーザーアカウントとパスワードで置き換えます。デフォルトで、ZFS Storage Appliance には統合された (読み取り専用) USM アカウントのユーザー名またはパスワードは含まれていません。セキュリティーのため、配備、管理、およびモニタリングの要件に基づいて USM 資格およびプロトコルを構成します。

必要でないかぎり使用していないまたは古いバージョンの SNMP プロトコルが無効になっていることを確認します。

1. **ZFS Storage Appliance にログインします。**
   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **SNMP プロトコルのどのバージョンがデバイスで使用されるのかを確認します。**

```
hostname:> configuration services snmp get version
version = v2
```

3. **SNMPv3 の使用を有効にします (使用可能な場合)。**
   SNMPv1/v2c と SNMPv3 の使用は相互に排他的であるため、SNMPv3 を有効にすると、SNMPv1/v2c は無効になります。

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **SNMP のバージョンを確認します。**

```
hostname:> configuration services snmp get version
version = v3
```

▼ SNMP コミュニティー文字列の構成

ZFS Storage Appliance が SNMPv1 または v2 を使用するように構成されている場合のみ、このタスクを実行します。

SNMP はデバイスの健全性をモニターするために使用されることが多いため、デバイスによって使用されるデフォルトの SNMP コミュニティー文字列を顧客定義の値に変更することが重要です。

1. **ZFS Storage Appliance にログインします。**
   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **SNMP コミュニティー文字列を変更します。**
   この例では、*string* を SNMP コミュニティー文字列の構成に関する米国国防総省の要件に準拠する値で置き換えます。

```
hostname:> configuration services snmp set community=string
community = value
```

3. **SNMP コミュニティー文字列を確認します。**

```
hostname:> configuration services snmp get community
```

▼ SNMP 承認ネットワークの構成

ZFS Storage Appliance が SNMPv1 または v2 を使用するように構成されている場合のみ、このタスクを実行します。

システム構成情報の開示を最小限に抑えるために、SNMP 照会は、承認されたネットワークまたはホストソースからのみ受け入れるべきです。

1. **ZFS Storage Appliance にログインします。**
   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **SNMP 承認ネットワークパラメータを構成します。**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **SNMP 承認ネットワークパラメータの値を確認します。**
   この例では、ネットワークパラメータを `127.0.0.1/8` に設定すると、すべてのネットワークベースの SNMP クエリーを実質的にブロックします。この値は、承認されたホストおよびネットワークを許可するように、必要に応じて調整する必要があります。

   値 `0.0.0.0/0` は、任意のネットワークの場所からの照会を許可します。

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

▼ 管理ネットワークアクセスの制限

これらのセキュリティー強化手順に加えて、ZFS Storage Appliance によって公開される管理インタフェースは、専用の隔離された管理ネットワーク上に配備される必要があります。この手順は、承認されていない、または意図しない管理ネットワークトラフィックから ZFS Storage Appliance を保護する際に役立ちます。管理ネットワークへのアクセスは、このレベルのアクセスを必要とする管理者のみにアクセス権を付与することで、厳密に制御する必要があります。

さらに、特定のネットワークインタフェース上の管理アクセスを有効または無効にするように ZFS Storage Appliance を構成できます。この変更はこの手順を使用して実装できます。

1. **ZFS Storage Appliance にログインします。**
   81 ページの「ZFS Storage Appliance へのログイン」を参照してください。

2. **管理ネットワークインタフェースを構成します。**

   この例では、値 *interface* を、この設定が適用される実際のネットワークインタフェースの名前で置き換えます。

   ```
   hostname:> configuration net interfaces select interface set admin=false
   ```

追加の ZFS Storage Appliance のリソース

ZFS Storage Appliance の追加のセキュリティーガイドラインについては、ZFS Storage Appliance 上で実行されているリリースに対応したセキュリティーガイドを参照してください。82 ページの「ZFS Storage Appliance ソフトウェアのバージョンの判別」を参照してください。

これらのガイドでは、製品のセキュリティーの特長、機能、および構成オプションに関する追加情報を提供します。

- 『*Oracle ZFS Storage Appliance* セキュリティーガイド』(リリース 2013.1.4.0)
  `http://docs.oracle.com//cd/E56047_01`
- 『*Oracle ZFS Storage Appliance* セキュリティーガイド』(リリース 2013.1.3.0)
  `http://docs.oracle.com/cd/E56021_01`
- 『*Oracle ZFS Storage Appliance* セキュリティーガイド』(リリース 2013.1.2.0)
  `http://docs.oracle.com/cd/E51475_01`

Exadata Storage Server のセキュリティー保護

Exadata Storage Server (ストレージサーバー) は、SuperCluster のストレージ構成要素です。各ストレージサーバーは、必要なすべての計算、ストレージ、およびソフトウェアの各コンポーネントを含む SuperCluster M7 の一部としてインストールおよび統合された状態で提供されます。

注記 - 承認されたメソッド、パッチ、または更新を適用する方法でのみ、構成を変更することが許可されます。その他のどのような方法でも、ストレージサーバーのソフトウェアは変更できません。

SuperCluster M7 には、少なくとも 3 台のストレージサーバーが存在します。メインの SuperCluster ラックおよびオプションの拡張ラックに、追加のストレージサーバーが取り付けられている可能性があります。各ストレージサーバーを個別にセキュリティー保護する必要があります。

次のトピックでは、ストレージサーバーをセキュリティー保護する方法について説明します。

▼ ストレージサーバー OS へのログイン

- **`celladmin` として、管理ネットワーク上のストレージサーバーのいずれかにログインします。**
  デフォルトのパスワードについては、94 ページの「デフォルトのアカウントとパスワード」を参照してください。

```
# ssh celladmin@Storage_Server_IP_address
```

デフォルトのアカウントとパスワード

この表には、ストレージサーバーのデフォルトアカウントとパスワードが一覧表示されています。

アカウント名	タイプ	デフォルトのパスワード	説明
root	管理者	welcome1	ストレージサーバー OS にアクセスして、一般的な管理アクションを実行したり、ストレージサーバーのソフトウェアを更新したりする際に使用されます。
celladmin	セル管理者	welcome	ストレージサーバーの設定および構成を実行する際に使用されます。さらに、プラットフォーム上のすべてのストレージサービスは、このアカウントを使用して動作します。
cellmonitor	モニター	welcome	モニタリングを行うためにのみ使用されます。このアカウントからストレージサーバー上に存在する構成やオブジェクトを変更できないように、このアカウントでは制限付きシェルが使用されます。

▼ ストレージサーバーのパスワードの変更

デフォルトのアカウントとパスワードのリストについては、94 ページの「デフォルトのアカウントとパスワード」を参照してください。

注記 - Oracle Engineered Systems Hardware Manager で管理される任意の SuperCluster コンポーネント (Exadata Storage Server OS など) のパスワードが変更された場合は、Oracle Engineered Systems Hardware Manager でもパスワードを更新する必要があります。詳細は、『*Oracle SuperCluster M7* シリーズ管理ガイド』を参照してください。

---

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **次の方法のいずれかを使用して、デフォルトのパスワードを変更します。**

   - **ログインしたサーバー上でアカウントのパスワードを変更します。**

     ```
     # passwd account_name
     ```

   - **すべてのストレージサーバーにわたってアカウントのパスワードを変更します。**

     `cell_group` は、すべてのストレージサーバーのホスト名を (1 行に 1 つずつ) 一覧表示した単純なテキストファイルです。

     この例では、これらのコマンド行の項目を置き換えます。

- *new_password* – サイトポリシーに準拠した新しいパスワードに置き換えます。
- *account_name* - Oracle Linux アカウントの名前で置き換えます。

```
# dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
```

▼ Exadata Storage Server ソフトウェアバージョンの判別

1. **ストレージサーバーのいずれかにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **このコマンドを入力します。**
   この例では、ストレージサーバーのソフトウェアバージョンが 12.1.2.1.1.150316.2 です。

   ```
   # imageinfo -ver
   12.1.2.1.1.150316.2
   ```

   ソフトウェアのバージョンを更新するには、My Oracle Support (https://support.oracle.com) から入手可能な最新の SuperCluster Quarterly Full Stack Download Patch をインストールします。

   注記 - SuperCluster の場合、追加の制限によって、ソフトウェアのどのバージョンを使用できるのかが制限されたり、それらのバージョンの更新方法が制限されたりすることがあります。これらの状況では、Oracle の担当者に連絡してください。

デフォルトの公開ネットワークサービス (ストレージサーバー)

サービス名	プロトコル	ポート	説明
SSH	TCP	22	ストレージサーバーのソフトウェアに統合されている Secure Shell サービスで CLI を使用して、システムへの管理アクセスを提供するために使用されます。 デフォルトでは、管理 (NET 0) および IB (BONDIB0) ネットワーク上の接続要求にのみ応答するように、Secure Shell サーバーが構成されています。

ストレージサーバーはリモートダイレクトメモリーアクセス (RDMA) インタフェース経由で Reliable Datagram Socket (RDSv3) プロトコルを使用して、SuperCluster 上の Oracle データベースドメインとも通信します。このようなポイントツーポイント通信では、TCP/IP が使用されないため、SuperCluster 上の Oracle データベースドメインと

ストレージサーバーの両方が存在する内部の IB ネットワークパーティションに通信が制限されます。

ストレージサーバーのセキュリティー構成の強化

注記 - ストレージサーバーには、製品の一部として Oracle ILOM が組み込まれています。その他の Oracle ILOM 実装と同様に、デバイスのデフォルトセキュリティー構成を改善するために、セキュリティー関連の構成の変更を実装できます。詳細は、37 ページの「Oracle ILOM のセキュリティー保護」を参照してください。

次のトピックでは、ストレージサーバーのセキュリティーを強化する方法について説明します。

セキュリティー構成の制限事項

`host_access_control` ユーティリティーは、ストレージサーバー上のセキュリティー構成の変更を実装することが許可およびサポートされている唯一の方法です。Oracle Support の通知 1068804.1 により、これらのデバイス構成を手動で変更することは許可されません。さらに、ストレージサーバーのセキュリティー構成を変更するには、このツールを使用する前に、まず Oracle SuperCluster Support から明示的な承認を得る必要があります。この承認を要求するには、Oracle Support でサービス要求を開きます。

Exadata ソフトウェアバージョン 11.2.3.3.0 の時点で使用可能な host_access_control コマンドを使用すると、次のように制限されたアクセスおよびセキュリティー構成セットの設定が実装されます。

- リモートの root アクセスを制限する。
- 特定アカウントへのネットワークアクセスを制限する。
- パスワードの有効期限と複雑性ポリシーを実装する。
- ログイン警告バナーを実装する。
- アカウントのロックアウトとセッションタイムアウトのポリシーを定義する。

▼ host_access_control による使用可能なセキュリティー構成の表示

host_access_control ユーティリティーで実行できる内容を確認するには、次の手順を実行します。

1. **ストレージサーバー OS にログインします。**
93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **(オプション) 詳細は、host_access_control ヘルプを表示してください。**

```
# /opt/oracle.cellos/host_access_control --help
```

▼ システムブートローダーのパスワードの構成

管理者がブートローダー (GRUB) エディタまたはコマンドインタフェースへのアクセスを試みるたびに、システムブートローダーのパスワードが必要となるようにストレージサーバーを構成できます。

1. **celladmin としてストレージサーバーにログインします。**
93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **システムブートローダーのパスワードを構成します。**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **設定を確認します。**

この例と同様の値がコマンドから返された場合は、ブートローダーのパスワードがインストールされています。

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

▼ Oracle ILOM システムコンソールアクセスの無効化

各ストレージサーバーには、リモートのモニタリングおよび管理を有効にするために Oracle ILOM が組み込まれています。Oracle ILOM を使用すると、ストレージサーバーのシステムコンソールへのリモートアクセスを提供することもできます。

Oracle ILOM からストレージサーバーへのアクセスを無効にする場合は、この手順を実行します。

1. **`celladmin` としてストレージサーバーにログインします。**
93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **Oracle ILOM システムコンソールへのアクセスを無効にします。**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **設定を確認します。**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

▼ SSH を使用したリモート `root` アクセスの制限

デフォルトでは、`root` ユーザーが各ストレージサーバーにリモートでアクセスすることが許可されています。

1. **`celladmin` としてストレージサーバーにログインします。**
93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **SSH を使用したリモート `root` アクセスを無効にします。**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **設定を確認します。**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

▼ システムアカウントのロックアウトの構成

デフォルトでは、認証の試みに 5 回連続失敗したあとにシステムアカウントがロックされるように、ストレージサーバーが構成されています。

このしきい値を変更するには、この手順を実行します。

1. **celladmin としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **しきい値を変更します。**
   米国国防総省のセキュリティー要件に準拠するには、値 3 を指定します。必要に応じて、ローカルサイトのポリシーに準拠した値に置き換えてください。

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --deny 3
   ```

3. **設定を確認します。**

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
   ```

▼ パスワードの複雑性ルールの構成

デフォルトでは、システムアカウントパスワードの複雑さを制御する重要な制限がストレージサーバーに実装されていません。

1. **celladmin としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **パスワードの複雑性ポリシーを定義します。**
   構文:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

N0,N1,N2,N3,N4 を 5 つの値のコンマ区切りセットで置き換えます。このように 5 つの値を使用することで、実際のシステムパスワードの複雑性ポリシーがまとめて設定されます。値は、次のとおりです (`passwdqc.conf(5)` のマニュアルページにも記載されています)。

- *N0* – 1 つの文字クラス (数字、小文字、大文字、および特殊文字) のみで構成されるパスワード用に使用されます。一般に、単純なパスワードはセキュアではないため、このパラメータは `disabled` に設定されます。
- *N1* – パスフレーズの要件を満たしていない 2 つの文字クラスで構成されるパスワード用に使用されます。このルールを適用するには、パスワードの長さが N1 文字以上である必要があります。
- *N2* – パスフレーズで構成されるパスワード用に使用されます。このルールを適用するには、パスワードの長さが N2 文字以上であり、パスフレーズの要件を満たしている必要があります。
- *N3* – 3 つの文字クラスで構成されるパスワード用に使用されます。このルールを適用するには、パスワードの長さが N3 文字以上である必要があります。
- *N4* – 4 つの文字クラスで構成されるパスワード用に使用されます。このルールを適用するには、パスワードの長さが *N4* 文字以上である必要があります。

米国国防総省のセキュリティー要件に準拠するには、*N0,N1,N2,N3,N4* パラメータを `disabled,disabled,disabled,disabled,15` に設定します。このように設定することで、4 つ以上の文字クラス (大文字、小文字、数字、および特殊) で構成され、長さが 15 文字以上であるパスワードのみが受け入れられるようになります。

注記 - 文字クラスの数を計算する際は、パスワード先頭の大文字とパスワード末尾の数字はカウントされません。

たとえば、米国国防総省の要件を満たすパスワードの複雑さを設定するには、次のように入力します。

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **この設定の現在のステータスを確認します。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

▼ パスワード履歴ポリシーの構成

デフォルトでは、ユーザーが最後の 10 個のパスワードを再使用できないようにするパスワード履歴ポリシーがストレージサーバーに定義されています。

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **現在の設定を表示します。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **パスワード履歴を変更します。**
   米国国防総省のセキュリティーと PCI-DSS の要件に準拠するには、パスワード履歴ポリシーを 5 に設定します。このように設定することで、アカウントに割り当てられている以前の 5 つのパスワードを再使用できなくなります。必要に応じて、ローカルサイトのポリシーに準拠した値に置き換えてください。

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --remember 5
   ```

4. **設定を確認するには、ステップ 2 を繰り返します。**

▼ 失敗した認証のロック遅延の構成

デフォルトでは、認証の試みに 1 回失敗したあとにシステムアカウントが 10 分間ロックされるポリシーがストレージサーバーに実装されています。

このしきい値を変更するには、この手順を実行します。

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **現在の設定を表示します。**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **しきい値を変更します。**
   米国国防総省のセキュリティー要件に準拠するには、値を 4 (秒) に設定します。必要に応じて、ローカルサイトのポリシーに準拠した値に置き換えてください。

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --lock 4
   ```

4. **設定を確認するには、ステップ 2 を繰り返します。**

▼ パスワードの有効期限制御ポリシーの構成

ストレージサーバーでは、さまざまなパスワードの有効期限制御 (パスワードが使用される最大日数、パスワードの変更間の最小日数、ユーザーに警告されるパスワードの有効期限前の日数を制御するパラメータを含む) がサポートされています。

米国国防総省のセキュリティーと PCI-DSS の要件に準拠するには、次の表に示す米国国防総省の値を使用します。

ポリシー	Oracle のデフォルト値	DOD 値
パスワードの最大有効期限	90 日	60 日
パスワードの最小有効期限	1 日	1 日
パスワードの最小長	8 文字	15 文字
パスワードの有効期限切れの警告	7 日	7 日

これらのパラメータのいずれかを変更するには、この手順を実行します。

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **現在の設定を表示します。**

```
# /opt/oracle.cellos/host_access_control password-policy --status
```

3. **サイトのパスワードポリシーに従って、これらのポリシーを構成します。**

   - **パスワードの最大有効期限パラメータを変更するには、次のように入力します。**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
```

   - **パスワードの最小有効期限パラメータを変更するには、次のように入力します。**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
```

   - **パスワードの最小長パラメータを変更するには、次のように入力します。**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
```

   - **パスワードの有効期限切れ警告パラメータを変更するには、次のように入力します。**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
```

4. **設定を確認するには、ステップ 2 を繰り返します。**

▼ 管理インタフェースの非アクティブタイムアウトの構成 (ログインシェル)

ストレージサーバーでは、事前に定義された秒数よりも長い時間非アクティブになっている管理セッションを終了する機能がサポートされています。

システムアカウントのログインシェルに管理インタフェースの非アクティブタイムアウトを定義するには、この手順を実行します。

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **現在の設定を表示します。**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

3. **管理インタフェースの非アクティブタイムアウトを定義します。**
   米国国防総省のセキュリティーおよび PCI-DSS の要件に準拠するには、値 `900` (秒) を指定します。必要に応じて、ローカルサイトのポリシーに準拠した値に置き換えてください。

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

4. **設定を確認するには、ステップ 2 を繰り返します。**

▼ 管理インタフェースの非アクティブタイムアウトの構成 (Secure Shell)

ストレージサーバーでは、事前に定義された秒数よりも長い時間非アクティブになっている管理 SSH セッションを終了する機能がサポートされています。

SSH セッションに管理インタフェースの非アクティブタイムアウトを定義するには、この手順を実行します。

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **現在の設定を表示します。**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
```

3. **SSH セッションに管理インタフェースの非アクティブタイムアウトを定義します。**
   米国国防総省のセキュリティー要件に準拠するには、値 `900` (秒) を指定します。必要に応じて、ローカルサイトのポリシーに準拠した値に置き換えてください。

```
# /opt/oracle.cellos/host_access_control idle-timeout --client 900
```

4. **設定を確認するには、ステップ 2 を繰り返します。**

▼ ログイン警告バナーの構成 (ストレージサーバー)

ストレージサーバーでは、ユーザーがシステムへの認証に成功する前に、お客様固有のメッセージを表示する機能がサポートされています。

認証前のログイン警告バナーを定義するには、この手順を実行します。

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **現在の設定を確認します。**

```
# /opt/oracle.cellos/host_access_control banner --status
```

3. **承認されたログイン警告バナーメッセージを含むテキストファイルを作成します。**

4. **認証前のログイン警告バナーを定義します。**
   米国国防総省のセキュリティー要件に準拠するには、*filename* を承認されたログイン警告バナーメッセージを含むファイルのパスと名前で置き換えます。

```
# /opt/oracle.cellos/host_access_control banner --file filename
```

5. **設定を確認するには、ステップ 2 を繰り返します。**

リモートネットワークアクセスの制限

フィルタリングルールセットを実装すると、ストレージサーバーへのインバウンドリモートネットワークアクセスを制限できます。カスタムのルールセットを定義すれば、ネットワークアクセスを微調整することもできます。

リモートアクセスを制限するには、次の手順を使用します。

ストレージサーバー管理ネットワークの分離

ストレージサーバーは、専用の隔離された管理ネットワーク上に配備されています。これは、承認されていない、または意図しないネットワークトラフィックからストレージサーバーを保護する際に役立ちます。管理ネットワークへのアクセスは、このレベルのアクセスを必要とする管理者のみにアクセス権を付与することで、厳密に制御する必要があります。

▼ リモートネットワークアクセスの制限

ストレージサーバー上のリモートネットワークアクセスは、複数の方法を使用して制限できます。ユーザーアカウントと起点によるアクセスを定義するトップダウン型のフィルタリングルールセットを実装すると、ストレージサーバーへのインバウンドネットワークアクセスを制限できます。米国国防総省および PCI-DSS の要件に従って、アクセスを許可または拒否するカスタムのルールセットを定義することもできます。

注意 - デフォルト以外のポリシーを実装するときは、システムへのアクセスが中断されないように注意してください。新しいルールを個別に追加すると、変更がすぐに有効になります。

ルールセットを実装するには、この手順を実行します。

1. **`celladmin` としてストレージサーバーにログインします。**
   93 ページの「ストレージサーバー OS へのログイン」を参照してください。

2. **アクティブなルールセットを調査します。**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **現在のルールセットをファイルにエクスポートし、バックアップコピーとして保存します。**
   このコマンドは、ルールセットを ASCII テキストファイルにエクスポートします。

```
# /opt/oracle.cellos/host_access_control access-export --file filename
```

4. **ルールセットを作成する際に使用する方法に基づいて、次のコマンドの 1 つ以上を実行してルールセットを構成します。**

   - **インバウンドネットワークの制限を削除する開いたルールセットを実装するには、次のように入力します。**

     ```
     # /opt/oracle.cellos/host_access_control access --open
     ```

   - **SSH を使用したインバウンドアクセスのみを許可する閉じたルールセットを実装するには、次のように入力します。**

     ```
     # /opt/oracle.cellos/host_access_control access --close
     ```

   - **既存のルールセットを変更するには、次のように入力します。**

     現在のルールセットを ASCII テキストファイルにエクスポートします。

     ```
     # /opt/oracle.cellos/host_access_control access-export --file filename
     ```

     エディタを使用してテキストファイルを編集して、ルールセットを構成します。

     テキストファイルからルールセットをインポートして、既存のルールセットをオーバーライドします。

     ```
     # /opt/oracle.cellos/host_access_control access-import --file filename
     ```

   - **特定のルールを個別に追加するには、次のように入力します。**

     この方法では、次のパラメータに基づいてアクセスが許可および拒否されます。

     - **ユーザー名** – 有効な値には、キーワード `all` または 1 つ以上の有効なローカルアカウントユーザー名が含まれます。
     - **起点** – 有効な値には、キーワード `all` またはシステムアクセスのソース (コンソール、仮想コンソール、Oracle ILOM、IP アドレス、ネットワークアドレス、ホスト名、または DNS ドメインを含む) を記述する個別のエントリが含まれます。

     この例では、ホスト `trusted.example.org` または `.trusted.domain.com` ドメイン内の任意のホストから接続が開始されたときに、ストレージサーバーへのアクセス権が `celladmin` ユーザーに付与されます。

     ```
     # /opt/oracle.cellos/host_access_control access --add --user celladmin \
     --origins trustedhost.example.org,.trusted.domain.com
     ```

追加のストレージサーバーリソース

Exadata データベースマシンのセキュリティーガイド (http://docs.oracle.com/cd/E50790_01/welcome.html) を参照してください。

IB および Ethernet スイッチのセキュリティー保護

SuperCluster で使用される Oracle Sun Data Center InfiniBand Switch 36 では、すべての内部コンポーネントにわたる高いパフォーマンス、高い拡張性、および完全な冗長性を備えたバックプレーンのためのネットワーク基盤を提供します。

IB スイッチは、計算サーバー、ストレージセル、および ZFS Storage Appliance を接続します。IB スイッチは、高度な管理およびモニタリング機能を提供するための組み込み Oracle ILOM を搭載しています。特に、Oracle ILOM は、ユーザー、ハードウェア、サービス、プロトコル、およびその他の構成パラメータのモニタリングおよび制御を可能にします。

SuperCluster M7 には少なくとも 2 つの IB スイッチを搭載し、大規模構成のために必要に応じて追加の IB スイッチを取り付けできます。各 IB スイッチを個別にセキュリティー保護する必要があります。

これらのトピックでは、SuperCluster M7 内の IB スイッチをセキュリティー保護する方法について説明します。

▼ IB スイッチへのログイン

このタスクでは、大部分の管理タスクが実行される、スイッチ上の Oracle ILOM インタフェースにログインする方法について説明します。

- **管理ネットワークで、IB スイッチ上の Oracle ILOM に `ilom-admin` としてログインします。**
  デフォルトのパスワードについては、110 ページの「デフォルトのアカウントとパスワード (IB スイッチ)」を参照してください。

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

▼ IB スイッチのファームウェアバージョンの判別

最新の機能やセキュリティー拡張機能を活用するには、IB スイッチが最新のサポートされているファームウェアバージョンで更新されていることを確認します。

1. **IB スイッチに `ilom-admin` としてログインします。**
   109 ページの「IB スイッチへのログイン」を参照してください。

2. **ファームウェアバージョンを表示します。**
   この例で、IB スイッチのファームウェアはバージョン `2.1.5-1` です。

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

IB スイッチファームウェアのバージョンを更新するには、`https://support.oracle.com` の My Oracle Support から入手可能な最新の SuperCluster Quarterly Full Stack Download Patch をインストールします。

注記 - SuperCluster M7 の場合、追加の制限によって、使用できる IB スイッチソフトウェアのバージョンが制限されることがあります。また、制限によってファームウェアの更新方法が決まります。これらの状況では、Oracle の担当者に連絡してください。

デフォルトのアカウントとパスワード (IB スイッチ)

アカウント名	タイプ	デフォルトのパスワード	説明
`root`	管理者	`welcome1`	IB スイッチの OS にアクセスするために使用されます。`ilom-admin`、`ilom-operator`、または顧客定義のアカウントが優先されるためこのアカウントは通常は使用されません。

アカウント名	タイプ	デフォルトのパスワード	説明
ilom-admin	管理者	ilom-admin	組み込みの Oracle ILOM ソフトウェアで管理機能を実行したり、ソフトウェアアップグレードを実行したり、ユーザーを構成やサービスを構成したり、IB スイッチ診断およびファブリック管理機能を実行したりするために使用されます。
ilom-operator	オペレータ	ilom-operator	Oracle ILOM のモニタリング、および IB ファブリック診断機能に対してのみ使用されます。
nm2user	読み取り専用	changeme	このアカウントは、IB スイッチのコマンド行管理インタフェースに対する読み取り専用権限を持ちます。このアカウントは、スイッチのハードウェアとソフトウェアのモニタリングをサポートするために Oracle Enterprise Manager によって使用されることがよくあります。

▼ root および nm2user パスワードの変更

IB スイッチでは、2 つの場所にシステムアカウントを保持します。root および nm2user アカウントは、スイッチのベースとなる OS によって構成および公開されます。アカウントの追加、削除、または変更は、このレイヤーでサポートされていませんが、デフォルトのパスワードを変更する必要があります。

ほかのアカウントとパスワードについては、112 ページの「IB スイッチのパスワードの変更 (Oracle ILOM)」を参照してください。

IB スイッチには、パスワードの複雑さ、有効期限、履歴、またはその他のルールを定義または強制する機能がありません。割り当てられたパスワードは米国国防総省のパスワードの複雑さの要件に準拠していること、米国国防総省のポリシーに従ってパスワードが更新されるようなプロセスが実装されていることを確認する必要があります。

新しいアカウントの作成、既存アカウントへの権限の割り当て、アカウントの削除といった IB スイッチアカウントの管理の詳細は、*Oracle Sun Data Center InfiniBand Switch 36* のハードウェアセキュリティーガイド、および *Oracle Sun Data Center InfiniBand Switch 36* に関する *Oracle Integrated Lights Out Manager* の補足情報を参照してください。118 ページの「追加の IB スイッチのリソース」を参照してください。

注記 - Oracle Engineered Systems Hardware Manager で管理される任意の SuperCluster コンポーネント (IB スイッチなど) のパスワードが変更された場合は、Oracle Engineered Systems Hardware Manager でもパスワードを更新する必要があります。詳細は、『*Oracle SuperCluster M7* シリーズ管理ガイド』を参照してください。

---

1. **IB スイッチに root としてログインします。**

```
# ssh root@IB_Switch_IP_address
```

デフォルトのパスワードについては、110 ページの「デフォルトのアカウントとパスワード (IB スイッチ)」を参照してください。

2. **root パスワードを変更します。**

```
$ passwd root
```

3. **nm2user パスワードを変更します。**

```
$ passwd nm2user
```

▼ IB スイッチのパスワードの変更 (Oracle ILOM)

IB スイッチでは、2 つの場所にシステムアカウントを保持します。このセクションでは、IB スイッチの Oracle ILOM インタフェースでパスワードを変更する方法について説明します。ほかのアカウントとパスワードについては、111 ページの「root および nm2user パスワードの変更」を参照してください。

デフォルトの IB スイッチアカウントおよび顧客定義のアカウントは、IB スイッチ上の組み込み Oracle ILOM を介して管理されます。

アカウントを表示したりパスワードを変更したりするには、この手順を実行します。

1. **IB スイッチに ilom-admin としてログインします。**
109 ページの「IB スイッチへのログイン」を参照してください。
デフォルトのパスワードについては、110 ページの「デフォルトのアカウントとパスワード (IB スイッチ)」を参照してください。

2. **IB スイッチ上の構成済み Oracle ILOM アカウントを表示します。**

```
-> show /SP/users
```

3. **ilom-admin アカウントのパスワードを変更します。**

```
-> set /SP/users/ilom-admin password=password
```

IB スイッチのネットワーク分離

IB スイッチの管理インタフェースは、専用の隔離された管理ネットワーク上に配備されます。これにより、承認されていない、または意図しないネットワークトラフィックから IB スイッチが保護されます。

この管理ネットワークへのアクセスは、このレベルのアクセスを必要とする管理者のみにアクセス権を付与することで、厳密に制御する必要があります。

デフォルトの公開ネットワークサービス (IB スイッチ)

サービス名	プロトコル	ポート	説明
SSH	TCP	22	統合された Secure Shell サービスで CLI を使用して、IB スイッチへの管理アクセスを有効にするために使用されます。
HTTP (BUI)	TCP	80	統合された HTTP サービスでブラウザインタフェースを使用して、IB スイッチへの管理アクセスを有効にするために使用されます。TCP/80 は通常、クリアテキストのアクセスに使用されますが、デフォルトでは TCP/443 で実行されるこのサービスのセキュアなバージョンに対して、IB スイッチが着信リクエストを自動的にリダイレクトします。
NTP	UDP	123	統合された Network Time Protocol (NTP) (クライアントのみ) サービスで、ローカルシステムクロックを 1 つ以上の外部時間ソースと同期させるために使用されます。
SNMP	UDP	161	統合された SNMP サービスで、IB スイッチの健全性をモニターし、受信したトラップ通知をモニターする管理インタフェースを提供するために使用されます。
HTTPS (BUI)	TCP	443	統合された HTTP サービスでブラウザインタフェースを使用して、IB スイッチへの暗号化された (SSL/TLS) チャネルを介した管理アクセスを有効にするために使用されます。
IPMI	TCP	623	統合された Intelligence Platform Management Interface (IPMI) サービスで、さまざまなモニタリングおよび管理機能のコンピュータインタフェースを提供するために使用されます。ハードウェアのインベントリデータ、フィールド交換可能ユニットの説明、ハードウェアのセンサー情報、およびハードウェアコンポーネントのステータス情報を収集するために Oracle Enterprise Manager Ops Center で使用されるため、このサービスは無効にしないでください。
サービスタグ	TCP	6481	Oracle サービスタグサービスによって使用されます。これは、サーバーを識別し、サービス要求を容易にするための Oracle の発見プロトコルです。このサービスは、IB スイッチソフトウェアを検索したりその他の Oracle の自動サービスソリューションと統合したりするために、Oracle Enterprise Manager Ops Center などの製品によって使用されます。

IB スイッチ構成の強化

これらのトピックでは、各種の構成設定を通じて IB スイッチをセキュリティー保護する方法について説明します。

- 114 ページの「不要なサービスの無効化 (IB スイッチ)」
- 115 ページの「HTTPS への HTTP リダイレクションの構成 (IB スイッチ)」

- 115 ページの「未承認の SNMP プロトコルの無効化 (IB スイッチ)」
- 116 ページの「SNMP コミュニティー文字列の構成 (IB スイッチ)」
- 117 ページの「デフォルトの自己署名付き証明書の交換 (IB スイッチ)」
- 118 ページの「管理 CLI セッションタイムアウトの構成 (IB スイッチ)」

▼ 不要なサービスの無効化 (IB スイッチ)

プラットフォームの運用および管理要件をサポートするために必要がないサービスを無効にします。デフォルトで IB スイッチはネットワークのデフォルトでのセキュリティー強化 (Secure By Default) 構成を採用します。この構成では、重要でないサービスはすでに無効になっています。ただし、顧客のセキュリティーポリシーおよび要件に基づいて、追加のサービスを無効にしなければならない場合があります。

1. **IB スイッチに `ilom-admin` としてログインします。**
   109 ページの「IB スイッチへのログイン」を参照してください。

2. **IB スイッチによってサポートされているサービスのリストを確認します。**

```
-> show /SP/services
```

3. **特定のサービスが有効になっているかどうかを確認します。**
   servicename を ステップ 2 のサービス名に置き換えます。

```
-> show /SP/services/servicename servicestate
```

   大半のサービスでは `servicestate` パラメータを認識および使用してサービスが有効と無効のどちらであるのかを記録しますが、`state` というパラメータを使用する `servicetag`、`ssh`、`sso`、`wsman` などのサービスがいくつかあります。使用される実際のパラメータにかかわらず、これらの例で示すように、サービス状態パラメータが値 `enabled` の値を返す場合、サービスは有効です。

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled
```

```
-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **必要がなくなったサービスを無効にするには、サービス状態を `disabled` に設定します。**

```
-> set /SP/services/http servicestate=disabled
```

5. **これらのいずれかのサービスを無効にする必要があるかどうかを確認します。**
   使用されるツールおよび方法に応じて、HTTP および HTTPS ブラウザサービスが必要ないか使用されていない場合は、無効にできます。次を入力します。

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

   - ブラウザ管理インタフェース (HTTP、HTTPS):
     -> **set /SP/services/http servicestate=disabled**
     -> **set /SP/services/http secureredirect=disabled**
     -> **set /SP/services/https servicestate=disabled**

▼ HTTPS への HTTP リダイレクションの構成 (IB スイッチ)

ブラウザベースの通信のすべてがスイッチと管理者との間で確実に暗号化されるように、IB スイッチはデフォルトで着信 HTTP 要求を HTTPS サービスにリダイレクトするように構成されています。

1. **IB スイッチに `ilom-admin` としてログインします。**
   109 ページの「IB スイッチへのログイン」を参照してください。

2. **セキュアなリダイレクションが有効になっていることを確認します。**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **デフォルトが変更されている場合は、セキュアなリダイレクションを有効にできます。**

```
-> set /SP/services/http secureredirect=enabled
```

▼ 未承認の SNMP プロトコルの無効化 (IB スイッチ)

デフォルトでは、IB スイッチをモニターおよび管理するために使用される SNMP サービスについて、SNMPv1、SNMPv2c、および SNMPv3 がすべて有効になっています。

必要でないかぎり古いバージョンの SNMP プロトコルが無効になっていることを確認します。

注記 - SNMP プロトコルのバージョン 3 では、ユーザーベースのセキュリティーモデル (USM) のサポートが導入されました。この機能は、従来の SNMP コミュニティー文字列を、特定のアクセス権、認証、およびプライバシプロトコルで構成可能な実際のユーザーアカウントとパスワードで置き換えます。デフォルトでは、IB スイッチに USM アカウントは含まれていません。独自の配備、管理、およびモニタリングの要件に基づいて、SNMPv3 USM アカウントを構成します。

---

1. **IB スイッチに `ilom-admin` としてログインします。**
109 ページの「IB スイッチへのログイン」を参照してください。

2. **それぞれの SNMP プロトコルのステータスを確認します。**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **必要に応じて、SNMPv1 と SNMPv2c を無効にします。**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

▼ SNMP コミュニティー文字列の構成 (IB スイッチ)

このタスクは、SNMP v1 または SNMPv2c が有効で使用するために構成されている場合のみ適用できます。

SNMP はデバイスの健全性をモニターするために使用されることが多いため、デバイスによって使用されるデフォルトの SNMP コミュニティー文字列を顧客定義の値に置き換えることが重要です。

1. **IB スイッチに `ilom-admin` としてログインします。**
109 ページの「IB スイッチへのログイン」を参照してください。

2. **新しい SNMP コミュニティー文字列を作成します。**
この例では、コマンド行でこれらの項目を置き換えます。

   - *string* – SNMP コミュニティー文字列の構成に関する米国国防総省の要件に準拠する顧客定義の値で置き換えます。

- *access* – これが読み取り専用と書き込み専用のどちらのアクセス文字列であるのかに応じて、`ro` または `rw` で置き換えます。

```
-> create /SP/services/snmp/communities/string permission=access
```

新しいコミュニティー文字列が作成されたら、デフォルトのコミュニティー文字列を削除する必要があります。

3. **デフォルトの SNMP コミュニティー文字列を削除します。**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **SNMP コミュニティー文字列を確認します。**

```
-> show /SP/services/snmp/communities
```

▼ デフォルトの自己署名付き証明書の交換 (IB スイッチ)

IB スイッチは、HTTPS プロトコルをデフォルトの状態で使用できるように、自己署名付き証明書を使用します。ベストプラクティスとして、自己署名付き証明書を、使用中の環境で使用することが承認され、認識された認証局によって署名された証明書で置き換えます。

IB スイッチは、SSL/TLS 証明書および非公開鍵へのアクセスに使用できるさまざまな方法 (HTTPS、HTTP、SCP、FTP、TFTP) をサポートし、情報を Web ブラウザインタフェースに直接渡します。詳細は、*Oracle Sun Data Center InfiniBand Switch 36* に関する *Oracle Integrated Lights Out Manager* の補足説明を参照してください。118 ページの「追加の IB スイッチのリソース」を参照してください。

1. **IB スイッチに `ilom-admin` としてログインします。**
109 ページの「IB スイッチへのログイン」を参照してください。

2. **IB スイッチでデフォルトの自己署名付き証明書を使用しているかどうかを確認します。**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **組織の証明書をインストールします。**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

▼ 管理 CLI セッションタイムアウトの構成 (IB スイッチ)

IB スイッチは、事前に定義された分数よりも長い時間非アクティブになっている管理 CLI セッションを切断してログアウトする機能がサポートされています。

デフォルトでは、CLI は 15 分後にタイムアウトします。

1. **IB スイッチに `ilom-admin` としてログインします。**
109 ページの「IB スイッチへのログイン」を参照してください。

2. **CLI に関連付けられた非アクティブタイムアウトパラメータを確認します。**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **非アクティブタイムアウトパラメータを設定します。**
n を分で指定された値で置き換えます。

```
-> set /SP/cli timeout=n
```

追加の IB スイッチのリソース

IB スイッチの管理およびセキュリティーの手順の詳細は、Sun Datacenter InfiniBand Switch 36 のドキュメントライブラリ (`http://docs.oracle.com/cd/E36265_01`) を参照してください。

▼ Ethernet スイッチのパスワードの変更

注記 - Oracle Engineered Systems Hardware Manager で管理される任意の SuperCluster コンポーネント (Ethernet スイッチなど) のパスワードが変更された場合は、Oracle Engineered Systems Hardware Manager でもパスワードを更新する必要があります。詳細は、『*Oracle SuperCluster M7* シリーズ管理ガイド』を参照してください。

---

1. **シリアルケーブルを Ethernet スイッチのコンソールからノートパソコンまたは類似のデバイスに接続します。**

   デフォルトのシリアルポートの速度は 9600 ボー、8 ビット、パリティーなし、1 ストップビット、ハンドシェークなしです。

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **スイッチを有効モードにします。**

```
sscsw-adm0> enable
```

3. **パスワードを設定します。**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **構成を保存します。**

```
sscsw-adm0# copy running-config startup-config
```

5. **セッションを終了します。**

```
sscsw-adm0# exit
```

6. **ノートパソコンを Ethernet スイッチから取り外します。**

コンプライアンスの監査

既知のベンチマークへのシステムのコンプライアンスを評価してレポートするには、Oracle Solaris コンプライアンスユーティリティーを使用します。

Oracle Solaris の `compliance` コマンドは、特定の要件へのコンプライアンスを検証するコード、ファイル、またはコマンド出力にベンチマークの要件をマップします。現在、Oracle SuperCluster では次の 2 つのセキュリティーコンプライアンスベンチマークのプロファイルがサポートされています。

- **推奨** – Center of Internet Security ベンチマークに基づいたプロファイルです。
- **PCI-DSS** – Payment Card Industry Data Security Standard (PCI DSS) のコンプライアンス要件を検証するプロファイルです。

これらのプロファイリングツールでは、セキュリティー制御がコンプライアンス要件にマップされるため、結果として生成されるコンプライアンスレポートによって大幅に監査時間を短縮できます。さらに、コンプライアンス機能では、セキュリティーチェックごとの根拠と、失敗したチェックを修正する手順を示すガイドも提供されています。ガイドはトレーニングに役立ち、将来のテストのガイドラインとしても役立ちます。デフォルトでは、各セキュリティープロファイルのガイドはインストール時に作成されます。SuperCluster Solaris 管理者はベンチマークを追加または変更したり、新規ガイドを作成したりできます。

次のトピックでは、コンプライアンスレポートを実行する方法と、FIPS-140 コンプライアンスについて説明します。

- 121 ページの「コンプライアンス評価の生成」
- 124 ページの「(オプション) `cron` ジョブを使用したコンプライアンスレポートの実行」
- 124 ページの「FIPS-140-2 レベル 1 コンプライアンス」

▼ コンプライアンス評価の生成

このタスクを実行するには、システムにパッケージを追加するためのソフトウェアインストールに関連する権利プロファイルが割り当てられている必要があります。ほとんどのコンプライアンスコマンドに対する管理権利が割り当てられている必要があります。

1. **コンプライアンスパッケージをインストールします。**

```
# pkg install compliance
```

このメッセージは、パッケージがインストールされていることを示します。

```
No updates necessary for this image.
```

詳細は、`pkg(1)` のマニュアルページを参照してください。

注記 - コンプライアンステストを実行する予定のあるすべてのゾーンにパッケージをインストールします。

---

2. **使用可能なベンチマーク、プロファイル、および以前の評価を一覧表示します。**

この例では、2 つのベンチマークが使用されています。

- **`pci-dss`** – `Solaris_PCI-DSS` と呼ばれる 1 つのプロファイルが含まれています。
- **`solaris`** – `Baseliine` および `Recommended` と呼ばれる 2 つのプロファイルが含まれています。

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **コンプライアンス評価を生成します。**

次の構文を使用して、`compliance` コマンドを実行します。

`compliance assess -b` *benchmark* `-p` *profile*

`-b`	特定のベンチマークを指定します。指定しない場合は、値がデフォルトの `solaris` に設定されます。
`-p`	プロファイルを指定します。プロファイル名では、大文字と小文字が区別されます。指定しない場合は、値がデフォルトの 1 番目のプロファイルに設定されます。

例:

- `Recommended` プロファイルの使用:

```
# compliance assess -b solaris -p Recommended
```

このコマンドは、3 種類のファイル (ログファイル、XML ファイル、および HTML ファイル) 形式の評価を含むディレクトリを `/var/share/compliance/assessments` 内に作成します。

- PCI-DSS プロファイルの使用:

```
# compliance assess -b pci-dss
```

注記 - pci-dss ベンチマークには 1 つのプロファイルしか存在しないため、コマンド行でプロファイルオプション (-p) を指定する必要はありません。

4. **コンプライアンスファイルが作成されたことを確認します。**

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

注記 - 同じ compliance コマンドを再度実行しても、ファイルは置き換えられません。評価ディレクトリを再使用する前に、ファイルを削除する必要があります。

5. **(オプション) カスタマイズされたレポートを作成します。**
   カスタマイズされたレポートは繰り返し実行できます。ただし、元のディレクトリでは 1 回しか評価を実行できません。
   この例では、レポートに表示される結果タイプを選択するために -s オプションが使用されています。
   デフォルトでは、notselected または notapplicable を除くすべての結果タイプがレポートに表示されます。コンマ区切りリストとして指定すると、結果タイプがデフォルトに加えて表示されます。結果タイプの前に - を付けると、個々の結果タイプを非表示にすることができます。一方で、リストを = で始めれば、正確にどの結果タイプが含まれるのかが指定されます。結果タイプは pass、fixed、notchecked、notapplicable、notselected、informational、unknown、error、または fail です。

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

   このコマンドは、失敗した項目と選択されていない項目を含むレポートを HTML 形式で作成します。このレポートは最新の評価に対して実行されます。

6. **完全なレポートを表示します。**
   テキストエディタによるログファイル表示、ブラウザによる HTML ファイル表示、XML ビューアによる XML ファイル表示が可能です。たとえば、前述の手順でカスタマイズされた HTML レポートを表示するには、次のブラウザエントリを入力します。

```
file:///var/share/compliance/assessments/filename_timestamp/report_A.html
```

7. **使用しているセキュリティーポリシーが合格するために必要な障害をすべて修正してください。**
   修正にシステムのリブートが含まれている場合、評価を再度実行する前にシステムをリブートします。

8. **障害が発生しなくなるまで、評価を繰り返します。**

▼ (オプション) cron ジョブを使用したコンプライアンスレポートの実行

- **crontab ファイルに適切なエントリを追加するには、スーパーユーザーとして crontab -e コマンドを使用します。**
  このリストには、crontab エントリの例が示されています。
  - 毎日午前 2:30 に、コンプライアンス評価が実行されます。

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```
  - 毎週日曜日の午前 1:15 に、コンプライアンス評価が実行されます。

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```
  - 毎月初日の午前 4:00 に、評価が実行されます。

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```
  - 毎月第 1 月曜日の午前 3:45 に、評価が実行されます。

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

FIPS-140-2 レベル 1 コンプライアンス

SuperCluster にホストされている暗号化アプリケーションは、FIPS 140-2 レベル 1 に準拠しているかどうかが検証される Oracle Solaris の暗号化フレームワーク機能に依存します。Oracle Solaris 暗号化フレームワークは、Oracle Solaris の主要な暗号化ストアであり、ユーザー空間とカーネルレベルのプロセスをサポートする 2 つの FIPS 140 検証済みモジュールを提供します。これらのライブラリモジュールは、アプリケーションに暗号化、復号化、ハッシュ処理、署名の生成と検証、証明書の生成と検証、およびメッセージ認証機能を提供します。これらのモジュールを呼び出すユーザーレベルのアプリケーションは、FIPS 140 モードで実行されます。

Oracle Solaris 暗号化フレームワークに加えて、Oracle Solaris にバンドルされている OpenSSL オブジェクトモジュールも、Secure Shell と TLS プロトコルに基づいたアプリケーションの暗号化をサポートする FIPS 140-2 レベル 1 に準拠しているかどうかが検証されます。クラウドサービスプロバイダは、FIPS 140 準拠モードでテナントホストが有効になるように選択できます。FIPS 140-2 プロバイダである Oracle Solaris および OpenSSL が FIPS 140 準拠モードで実行されている場合は、FIPS 140 検証済みの暗号化アルゴリズムが強制的に使用されます。

38 ページの「(必要な場合) FIPS-140 準拠の動作の有効化 (Oracle ILOM)」も参照してください。

この表は、SuperCluster M7 上の Oracle Solaris でサポートされている FIPS 承認済みのアルゴリズムが一覧表示されています。

鍵または CSP	証明書番号	
	v1.0	**v1.1**
対称鍵		
AES: 128 ビット、192 ビット、256 ビットの鍵サイズに対応した ECB、CBC、CFB-128、CCM、GMAC、GCM、CTR モード	#2311	#2574
AES: 256 ビットと 512 ビットの鍵サイズに対応した XTS モード	#2311	#2574
TripleDES: 鍵オプション 1 に対応した CBC および ECB モード	#1458	#1560
非対称鍵		
RSA PKCS#1.5 署名の生成/検証: 1024 ビット、2048 ビット (SHA-1、SHA-256、SHA-384、SHA-512 を使用)	#1194	#1321
ECDSA 署名の生成/検証: P-192、P-224、P-256、P-384、P-521、K-163、K-233、K-283、K-409、K-571、B-163、B-233、B-283、B-409、B-571	#376	#446
Secure Hashing Standard (SHS)		
SHA-1、SHA-224、SHA-256、SHA-384、SHA-512	#1425	#1596
(Keyed-) ハッシュベースのメッセージ認証		
HMAC SHA-1、HMAC SHA-224、HMAC SHA-256、HMAC SHA-384、HMAC SHA-512	#1425	#1596
乱数ジェネレータ		
swrand FIPS 186-2 乱数ジェネレータ	#1154	#1222
n2rng FIPS 186-2 乱数ジェネレータ	#1152	#1226

Oracle Solaris システムでは、FIPS 140-2 レベル 1 について検証された暗号化アルゴリズムのプロバイダが 2 つ提供されています。

- Oracle Solaris の暗号化フレームワーク機能は、Oracle Solaris システム上の主要な暗号化ストアであり、2 つの FIPS 140 モジュールを提供します。ユーザーランドモジュールは、ユーザー空間で動作するアプリケーションに暗号化を提供し、カーネルモジュールは、カーネルレベルのプロセスに暗号化を提供します。これらのライブラリモジュールは、アプリケーションに暗号化、復号化、ハッシュ処理、署名の生成と検証、証明書の生成と検証、およびメッセージ認証機能を提供します。これらのモジュールを呼び出すユーザーレベルのアプリケーション (`passwd` コマンドや IKEv2 など) は、FIPS 140 モードで実行されます。カーネルレベルのコンシューマ (Kerberos や IPsec など) は、独自の API を使用してカーネル暗号化フレームワークを呼び出します。
- OpenSSL オブジェクトモジュールは、SSH および Web アプリケーション用の暗号化を提供します。OpenSSL は、Secure Sockets Layer (SSL) および Transport Layer Security (TLS) プロトコル用のオープンソースのツールキットであり、暗号化ライブラリを提供します。Oracle Solaris では、SSH および Apache Web Server が OpenSSL FIPS 140 モジュールのコンシューマです。Oracle Solaris では、OpenSSL の FIPS 140 バージョンにすべてのコンシューマが使用できる Oracle Solaris 11.2 が

付属していますが、Oracle Solaris 11.1 に付属するバージョンは Solaris SSH のみが使用できます。FIPS 140-2 プロバイダモジュールは CPU を集中的に使用するため、デフォルトでは有効になっていません。管理者には、FIPS 140 モードでプロバイダを有効にし、コンシューマを構成する責任があります。

Oracle Solaris での FIPS-140 プロバイダの有効化の詳細は、見出し「Oracle Solaris 11 オペレーティングシステムのセキュリティー保護」(http://docs.oracle.com/cd/E36784_01) の下に表示される『*Using a FIPS 140 Enabled System in Oracle Solaris 11.2*』というタイトルのドキュメントを参照してください。

SuperCluster M7 シリーズシステムをセキュアな状態にする

次のトピックでは、システムの寿命期間全体にわたってセキュリティーを維持するために使用できる SuperCluster M7 シリーズの機能について説明します。

SuperCluster セキュリティーの管理

SuperCluster M7 では、さまざまな製品 (Oracle ILOM、Oracle Enterprise Manager Ops Center、Oracle Enterprise Manager、Oracle の Identity Management Suite など) のセキュリティー管理機能が使用されます。次のセクションで詳細に説明します。

セキュアな管理のための Oracle ILOM

Oracle ILOM は、数多くの SuperCluster M7 コンポーネントに組み込まれているサービスプロセッサです。次の帯域外管理アクティビティーを実行するには、Oracle ILOM を使用します。

- SuperCluster コンポーネントのセキュアな Lights-Out 管理を実行する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、Secure Shell 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。

- RBAC モデルを使用して職務の要件を分離します。実行できる機能を制限する特定の役割に個々のユーザーを割り当てます。
- 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。この機能を使用すると、未承認のアクティビティーや変更を検出して、これらのアクションを特定のユーザーに戻すことができます。

詳細は、Oracle Integrated Lights Out Manager のドキュメント (http://docs.oracle.com/en/hardware/?tab=4) を参照してください。

Oracle Identity Management Suite

Oracle Identity Management スイートでは、組織全体にわたるユーザー ID およびアカウントのエンドツーエンドのライフサイクルが管理されます。このスイートでは、シングルサインオン、Web ベースのアクセス制御、Web サービスのセキュリティー、識別情報の管理、強固な認証、および識別情報とアクセスの制御がサポートされています。

Oracle Identity Management では、Oracle SuperCluster 上で実行されているアプリケーションやサービスだけでなく、それを管理する基本インフラストラクチャーやサービスに関する識別情報およびアクセスも管理するための単一点を提供できます。

詳細は、Oracle Identity Management のドキュメントを参照してください。

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

Oracle Key Manager は、保存された情報を保護する暗号化鍵の管理とモニタリングを簡素化する包括的な鍵管理システム (KMS) です。

Oracle Key Manager では、高い拡張性と可用性を持つアーキテクチャーを備えたエンタープライズクラスの環境がサポートされているため、何千ものデバイスや何百万もの鍵を管理できます。この機能は、強化されたオペレーティング環境で動作し、鍵の管理およびモニタリング操作に対応した強力なアクセス制御および役割の分離を実施し、Oracle の Sun Crypto Accelerator 6000 PCIe カード (FIPS 140-2 認定を受けたハードウェアセキュアモジュール) でのセキュアな鍵の格納をオプションでサポートしています。

SuperCluster のコンテキストでは、Oracle Key Manager は、Oracle StorageTek でテープドライブを暗号化する際に使用される暗号化鍵、透過的なデータ暗号化を使用して暗号化された Oracle データベース、および Oracle Solaris 11 OS で使用できる暗号化済み ZFS ファイルシステムへのアクセスを承認、セキュリティー保護、および管理できます。

詳細は、Oracle Key Manager のドキュメントを参照してください。

http://docs.oracle.com/cd/E26076_02

Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager は、Oracle サービス担当者がラックレベルでハードウェアを管理するために使用される BUI ベースのツールです。詳細は、『*Oracle SuperCluster M7* シリーズオーナーズガイド*:* 管理』を参照してください。

Oracle Engineered Systems Hardware Manager には、次の 2 セットの認証情報が含まれています。

- **SuperCluster M7 コンポーネントパスワード**

  Oracle Engineered Systems Hardware Manager では、すべての SuperCluster M7 ハードウェアのすべての出荷時アカウントに対するパスワードのセキュアストアが保持されます。このソフトウェアでは、SuperCluster M7 コンポーネントを管理する際に、これらのパスワードが使用されます。

  これらのパスワードのいずれかを変更する際は、新しいパスワードで Oracle Engineered Systems Hardware Manager アプリケーションを更新する必要があります。
- **ローカル認証**

  Oracle Engineered Systems Hardware Manager には、2 つのローカルユーザーアカウントが用意されています。1 つのアカウントは、お客様が環境に合わせて Oracle Engineered Systems Hardware Manager を調整し、サービスアカウントを管理する際に使用されます。もう 1 つのアカウントは、Oracle サービス担当者が SuperCluster M7 ハードウェアを構成、サポート、および修理する際に使用されます。

Oracle Engineered Systems Hardware Manager では、次のローカル管理リソースが提供されています。

- **パスワードポリシー** – 企業ポリシーに従ってアプリケーションのパスワードを構成できることで、パスワードが企業規格に準拠します。

注記 - パスワードポリシーの設定については、企業のセキュリティー責任者に問い合わせてください。

- **証明書** –Oracle Engineered Systems Hardware Manager では、計算サーバーと Oracle Engineered Systems Hardware Manager サーバーおよび BUI 間の通信をセキュリティー保護する際に、証明書が使用されます。これらの証明書はインストール時に自動的に作成され、各 SuperCluster インスタンスに一意です。ただし、お客様が提供した証明書と鍵で置き換えることもできます。
- **ポート** – Oracle Engineered Systems Hardware Manager で使用されるネットワークポートは、企業ポリシーと競合する場合に備えて構成できます。ポート 8001 から 8004 までが使用されます。

構成手順については、『*Oracle SuperCluster M7* シリーズオーナーズガイド: 管理』を参照してください。

Oracle Enterprise Manager

Oracle Enterprise Manager スイートは、(Oracle Enterprise Manager Ops Center を使用した) アプリケーション、ミドルウェア、データベース、物理および仮想インフラストラクチャーのライフサイクル管理に重点を置いた包括的な統合クラウド管理ソリューションです。Oracle Enterprise Manager では、次の管理技術が提供されています。

- アプリケーション、ミドルウェア、およびデータベースの詳細なモニタリング、イベント通知、パッチ適用、変更管理、継続的な構成、コンプライアンス管理、およびレポートがサポートされています。
- データベースグループのアクセス制御と監査ポリシーのほかに、セキュリティー構成の設定を集中管理できます。これらの機能へのアクセスは承認された個人に制限できるため、管理アクセスでは、職務、最小特権、および説明責任を分離するためのコンプライアンス義務がサポートされます。
- さまざまな方法、詳細なアクセス制御、および包括的な監査を使用した強力な認証がサポートされているため、SuperCluster 環境の管理をセキュアな方法で実現できます。

詳細は、Oracle Enterprise Manager のドキュメント (`http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html`) を参照してください。

Oracle Enterprise Manager Ops Center (オプション)

Oracle Enterprise Manager Ops Center は、Oracle SuperCluster セキュリティー面の一部を管理する際に使用できるオプションの技術です。

Oracle Enterprise Manager スイートの一部である Oracle Enterprise Manager Ops Center は、サーバー、OS、ファームウェア、仮想マシン、ゾーン、ストレージ、およびネットワークファブリックに対応した単一の管理インタフェースを提供する集中型のハードウェア管理ソリューションです。

Oracle Enterprise Manager Ops Center を使用すると、管理アクセスを物理システムと仮想システムのコレクションに割り当てたり、管理者アクティビティーをモニターしたり、障害を検出したり、アラートを構成および管理したりできます。Oracle Enterprise Manager Ops Center では、既知の構成ベースライン、パッチレベル、およびセキュリティー上の脆弱性についてシステムを比較できる各種レポートがサポートされています。

詳細は、Oracle Enterprise Manager Ops Center のドキュメント (`http://docs.oracle.com/cd/E27363_01/index.htm`) を参照してください。

注記 - 以前のバージョンの Oracle Enterprise Manager Ops Center では、SuperCluster システムから Ops Center ソフトウェアがインストールされ、実行されていました。Oracle Enterprise Manager Ops Center 12c Release 2 (12.2.0.0.0) リリース以降では、SuperCluster システムの外部で Ops Center ソフトウェアがインストールされ、実行される必要があります。

セキュリティーのモニタリング

コンプライアンスレポートであるのか、インシデントレスポンスであるのかには関係なく、モニタリングおよび監査は、IT 環境への可視性を向上させるために使用する必要がある重要な機能です。多くの場合、モニタリングおよび監査が採用される範囲は、環境のリスクや重要な特性に基づきます。

SuperCluster M7 シリーズのシステムでは、サーバー、ネットワーク、データベース、およびストレージ層で包括的なモニタリングおよび監査機能が提供されるため、情報を監査およびコンプライアンスの要件をサポートするために使用できます。

次のセクションでは、ワークロードおよびデータベースのモニタリングと監査について説明します。

- 132 ページの「ワークロードのモニタリング」
- 132 ページの「データベースアクティビティーのモニタリングと監査」
- 133 ページの「ネットワークのモニタリング」

ワークロードのモニタリング

Oracle Solaris OS には、管理アクション、コマンド行の呼び出し、さらに個々のカーネルレベルのシステムコールをモニターできる包括的な監査機能が備わっています。この機能は高度な構成が可能であるため、大域、ゾーンごと、さらにユーザーごとの監査ポリシーが提供されます。

Oracle Solaris ゾーンを使用するようにシステムが構成されている場合は、各ゾーンの監査レコードを大域ゾーンに保存して、改ざんから保護できます。

Oracle Solaris の監査では、システムログ (`syslog`) 機能を使用してリモートの収集ポイントに監査レコードを送信する機能が提供されています。多くの商用の侵入検出および防止サービスでは、分析およびレポート用の追加入力として Oracle Solaris 監査レコードを使用できます。

Oracle VM Server for SPARC では、ネイティブの Oracle Solaris 監査機能を利用して、仮想化イベントおよびドメイン管理に関連付けられたアクションおよびイベントを記録します。

詳細は、Oracle Solaris セキュリティーガイドラインで Oracle Solaris セキュリティーのモニタリングと保守に関するセクションを参照してください。

`http://docs.oracle.com/cd/E26502_01`

データベースアクティビティーのモニタリングと監査

Oracle データベースでは詳細な監査がサポートされているため、監査レコードが生成される日時を選択的に決定するポリシーを確立できます。この機能は、ほかのデータベースアクティビティーに集中し、多くの場合に監査アクティビティーに関連するオーバーヘッドを削減する際に役立ちます。

Oracle Audit Vault and Database Firewall では、データベース監査の設定が集中管理され、セキュアなリポジトリへの監査データの統合が自動化されます。このソフトウェアには、特権ユーザーのアクティビティーやデータベース構造の変更を含む広範囲なアクティビティーをモニターするレポート機能が組み込まれています。Oracle Audit Vault and Database Firewall で生成されたレポートでは、さまざまなアプリケーションや管理データベースのアクティビティーへの可視性や、アクションの説明責任をサポートする詳細な情報が提供されます。

Oracle Audit Vault and Database Firewall では、不正なアクセスの試みやシステム権限の悪用を示している可能性のあるアクティビティーを事前に検出および警告できます。

これらの警告には、システム定義とユーザー定義の両方のイベントおよび条件 (特権ユーザーアカウントの作成や機密情報を含むテーブルの変更など) を含めることができます。

Oracle Audit Vault and Database Firewall Remote Monitor では、リアルタイムでデータベースセキュリティーをモニターできます。この機能はデータベース接続に対してクエリーを実行することで、悪意のあるトラフィック (アプリケーションバイパス、未承認のアクティビティー、SQL 侵入、その他の脅威など) を検出します。このソフトウェアは、正確な SQL 文法ベースのアプローチを使用しているため、疑わしいデータベースアクティビティーを迅速に特定する際に役立ちます。

詳細は、Oracle Audit Vault and Database Firewall のドキュメント (http://docs.oracle.com/cd/E37100_01/index.htm) を参照してください。

ネットワークのモニタリング

セキュリティーのガイドラインに基づいてネットワークを構成したあとは、定期的なレビューと保守が必要になります。

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。

- 発生する可能性があるインシデントをログで確認し、組織のセキュリティーポリシーに従ってアーカイブします。
- クライアントアクセスネットワークの定期的なレビューを実施して、ホストと Oracle ILOM の設定が変更されていないことを確認します。

詳細は、Oracle Solaris OS のセキュリティーガイドを参照してください。

- Oracle Solaris 11 OS – http://www.oracle.com/goto/Solaris11/docs
- Oracle Solaris 10 OS – http://www.oracle.com/goto/Solaris10/docs

ファームウェアとソフトウェアの更新

SuperCluster M7 シリーズシステムの更新は、QFSDP で提供されます。QFSDP をインストールすると、すべてのコンポーネントが一括して更新されます。これを実施することにより、Oracle で完全にテストされたソフトウェアバージョンの組み合わせで、すべてのコンポーネントを継続して実行できます。

My Oracle Support (http://support.oracle.com) から最新の QFSDP を取得します。

サポートされているソフトウェアとファームウェアの詳細は、『*Oracle SuperCluster M7* シリーズプロダクトノート』を参照してください。プロダクトノートにアクセスする手順については、MOS のノート 1605591.1 で入手できます。

注記 - Oracle サポートのアドバイスに従って、リアクティブ保守用に各コンポーネントを個別にアップグレード、更新、またはパッチ適用するだけにしてください。

索引

さ

た

な

は

ま

や

ら

わ

A

C

E

F

G

H

I

N

O