ORACLE
MINICLUSTER

Oracle MiniCluster S7-2
プラットフォームのセキュリティ

Oracle ホワイト・ペーパー | 2016 年 10 月

ORACLE

目次

はじめに

Oracle MiniCluster S7-2 は、多くのデータベースとエンタープライズ・アプリケーションを実行できるように設計、テスト、統合された高性能な多目的エンジニアド・システムです。この製品は、組織およびクラウド・サービス・プロバイダ内にデプロイされている各種のミッション・クリティカルなワークロードを実行させるのに最適です。

Oracle MiniCluster S7-2 プラットフォームは、業界のもっとも厳しいセキュリティ要件に準拠できるといったセキュリティの相乗効果も得ることが可能です。初回の起動時からコンプライアンスに対応できるようになっており、これは、今日の IT エンタープライズ・システムおよびクラウド・プロバイダ・アーキテクチャでは珍しいことです。Oracle MiniCluster S7-2 は情報セキュリティに対して総体的なアプローチを取っており、各スタック・レベル（連携して機能するように統合および検証されたコンピューティング、ネットワーク、ストレージ、データベース、関連のソフトウェア・セキュリティ・コンポーネントなど）で設計された多層防御型のセキュリティ制御が実装されています。このプラットフォームに事前統合された検証済みのセキュリティ対策は、高度なエンジニアリングの進化と統合によって、個々のコンポーネントの集合よりもずっと高度なものになっています。

このホワイト・ペーパーでは、Oracle MiniCluster S7-2 プラットフォームのセキュリティの原則と機能について説明します。特に、エンタープライズ環境およびクラウド・サービス・プロバイダ環境におけるもっとも困難なセキュリティ要件にも対応できるよう採用された包括的な一連のセキュリティ制御について詳しく説明します。各機能について個別に説明しますが、機能同士を階層化することで、セキュリティ対策を強化できるようになります。また、アーキテクチャ、デプロイメント、運用に関するガイダンスも提供します。これは、組織およびクラウド・サービス・プロバイダが、データベースとアプリケーションを集約して専用のコンピューティング・クラウド・サービスを提供するために、Oracle MiniCluster S7-2 プラットフォームを既存の IT セキュリティ環境に統合する場所と方法を理解するのに役立ちます。

Oracle MiniClusterのセキュリティの原則

Oracle MiniCluster S7-2 プラットフォームの各セキュリティ機能について知る前に、Oracle MiniCluster S7-2 エンジニアド・システムの開発の基盤となった原則について理解しておくことが重要です。Oracle MiniCluster S7-2 プラットフォームのセキュリティ・アーキテクチャの中心となるのは、存続性、多層防御、最小権限、アカウンタビリティ、コンプライアンスというセキュリティ原則です。Oracle MiniCluster S7-2 プラットフォームにより、時間をかけて有効性が証明されたこれらの原則が具現化され、統合性の高いセキュリティ機能のコレクションが提供されます。組織とクラウド・サービス・プロバイダは、このプラットフォームを導入することで、自身のセキュリティ要件に対応して、全世界のコンプライアンス義務に容易に対処できます。こうした非常に厳しいセキュリティ・ニーズに対する技術的なセキュリティ制御を適切にドキュメント化し、マッピングすることで、これを実現できます。

存続性

組織とクラウド・サービス・プロバイダがミッション・クリティカルなワークロード用にハードウェアおよびソフトウェア・プラットフォームを選択する際には、そのプラットフォームが内外のユーザーによる偶発的および悪意のある行為の両方から生じる損害を防止または最小限に抑えられることを確認する必要があります。Oracle MiniCluster S7-2 プラットフォームは、次の機能によって存続性の原則をサポートします。

» プラットフォームによって使用されるコンポーネントが、セキュアなデプロイメント・アーキテクチャによって連携して動作するように設計、構築、テストされています。Oracle MiniCluster S7-2 プラットフォームは、その構成製品と事前に統合および検証がなされており、ハードウェア支援型の暗号化サービス、エンタープライズ・クラスの監視およびコンプライアンス監査、サービス品質、およびセキュアな管理による包括的なアクセス制御と徹底的なデータ保護が可能な、セキュアな仮想マシン（VM）をサポートおよび提供します。

» デフォルトの状態で攻撃を受ける恐れのある構成製品を減らし、プラットフォーム全体が攻撃にさらされた場合の損失を最小限に抑えます。組織とクラウド・サービス・プロバイダは、コンプライアンスに対応した Oracle MiniCluster S7-2 プラットフォームのセキュリティ対策を利用して、組織のセキュリティ・ポリシーおよび規制要件を満たすことができます。

» 強力な認証およびアクセス制御、機密保護、整合性、可用性という従来のセキュリティ目標に対応できる、オープンかつ慎重に検討されたプロトコルおよび API の補完機能により、（運用および管理インタフェースを含む）プラットフォームを保護します。

多層防御

Oracle MiniCluster S7-2 プラットフォームは互いに独立しながらも強化しあう複数のセキュリティ制御を採用しており、組織のセキュアなオペレーティング環境をサポートしています。これにより、組織のワークロードやデータの機密保護、整合性、可用性を確保します。多層防御の原則を適切に導入すれば、階層的な防御体制を構築できるため、1 つのセキュリティ制御に脆弱性や障害が見つかっても組織はセキュアな運用を継続できます。Oracle MiniCluster S7-2 プラットフォームは、次の機能によって多層防御の原則をサポートします。

» データ保護をしっかりと補完することで、送信時、使用時、保管時、およびデータ破壊時に情報を保護します。セキュリティ制御はサーバー、ストレージ、ネットワーク、仮想化、データ

ベース、およびアプリケーションのレイヤーで利用できます。より重要なのは、各レイヤーの独自のセキュリティ制御を相互に統合して、階層化された強力なセキュリティ・アーキテクチャを構築できることです。

» 明確に定義されたオープンな標準、プロトコル、インタフェースの使用をサポートしています。つまり、Oracle MiniCluster S7-2 プラットフォームを組織の既存のセキュリティ・ポリシー、アーキテクチャ、実践方法、標準に統合することもできるということです。このような統合は非常に重要です。なぜなら、アプリケーションとデバイスは独立した存在ではなく、IT アーキテクチャのセキュリティの強度は、そのもっとも弱いコンポーネントと同レベルになるためです。

最小権限

アプリケーション、サービス、ユーザーに対して、タスクの実行に必要な機能へのアクセス権を付与することは、最小権限の原則の一面にすぎません。不要な機能、サービス、インタフェースへのアクセスを制限することも同じく重要です。最小権限の原則は、非常にシンプルな概念に基づいています。つまり、使用させたくない機能に関する権限をユーザーに与えないということです。Oracle MiniCluster S7-2 プラットフォームは、次の機能によって最小権限の原則に対応しています。

» 各ユーザーおよび管理者のロールに基づき、個々のサーバー、ストレージ、仮想化、オペレーティング・システム、データベース、およびその他のコンポーネントに対するアクセス権を付与できるようにします。権限が細かく定義されたロールベースの多要素アクセス制御モデルを使用することで、アクセスを必要最小限に制限できます。

» 情報、基盤リソース、ネットワーク通信に対するアプリケーションのアクセスや、ローカルまたはリモートのサービス・アクセスがニーズに基づいて制限されるよう、アプリケーションを制約します。原因が偶発的なものか、悪意のある攻撃かにかかわらず、アプリケーションが誤動作する可能性もあり、最小権限を適用しなければ、アプリケーションが本来の用途をはるかに超えて悪影響を与える可能性があります。

アカウンタビリティ

ほとんどの場合、セキュリティ・インシデントを防ぐだけでは不十分です。インシデントを検出し、イベントをレポートし、その発生をどのように防いだかを把握することも同じく重要です。同様に、イベントを防げない場合は、その発生を検出して適切に対処できるようにすることが必須です。アカウンタビリティを心がけている組織は、次の問いに対する答えを求めています。

» どのようなセキュリティ・インシデントが発生したか。

» いつ発生したか。

» どこで発生したか。

» イベントの原因は何であったか。

» ターゲットは何であったか。

» どのような影響があったか。

Oracle MiniCluster S7-2 プラットフォームは、次の内容によってアカウンタビリティの原則をサポートします。

» Oracle MiniCluster S7-2 へのアクセスが必要なすべてのユーザーと管理者は、複数名の承認ルールによる検査の対象になります。またすべての重要な操作は、職務分離と最小権限の原則に基づいて実行されます。

» Oracle MiniCluster S7-2 プラットフォーム内で使用される各コンポーネントは、アクティビティの監査と監視をサポートしています。たとえば、ログインおよびログアウトのイベントや管理アクションを記録する機能に加え、多くの場合は各製品に固有のその他のイベントを記録する機能などがあります。このような情報を収集して再検討することはセキュアな運用の維持にとって重要であり、セキュリティ・インシデントが発生した場合の根本原因の分析に役立ちます。

» 特に、Oracle MiniCluster S7-2 プラットフォームで使用される 2 種類の製品には、アクティビティを監査および監視する高度な機能があります。基盤となる Oracle Solaris オペレーティング・システムと Oracle Database は、いずれも監査に関する非常に細かい構成をサポートしています。このため、組織の基準や目標に応じて監査の構成を調整し、不要または不適切な監査イベントによる「煩雑さ」を最小限に軽減しながら重要な情報を確実に取得できます。

コンプライアンス

コンプライアンスは、リスクの軽減と、組織内外のセキュリティおよびプライバシー要件への適合のために設計された管理メカニズムです。Oracle MiniCluster S7-2 のシステム構成プロセスでは、複数の情報セキュリティ標準および規制遵守要件を選択できるため、所定の法律、業界標準、仕様に従って運用するという組織の責務を果たすことができます。Oracle MiniCluster S7-2 のコンポーネントはデプロイ時にインフラストラクチャ・セキュリティとデータ保護の標準に準拠しているため、セキュアなコンピューティング環境を確保できます。また、これらの標準に対応したテスト、メンテナンス、保護、レポートも簡単です。Oracle MiniCluster S7-2 には、システム構成の検証をサポートする、オンデマンドおよび定期的なコンプライアンス・レポートに便利な機能があります。この機能により、組織内外のセキュリティ・ポリシー、業界固有のセキュリティ標準、および規制条項への準拠が可能です。

Oracle MiniCluster S7-2 プラットフォームは、コンプライアンス対応のセキュアな環境でミッション・クリティカルなサービスをデプロイする組織およびクラウド・サービス・プロバイダに最適です。というのも、このプラットフォームは、前述のセキュリティ原則などのそれぞれに対応できる固有の機能（デフォルトでのセキュリティや少ない攻撃対象など）を備えているためです。Oracle MiniCluster S7-2 プラットフォームは、一連の包括的なセキュリティ機能によってセキュアなデプロイメント・アーキテクチャを実現できるため、組織内やクラウド・サービス・プロバイダ内でホストされる専用のコンピューティング環境への、ミッション・クリティカルなアプリケーションおよびデータベースのデプロイに最適です。

Oracle MiniCluster S7-2プラットフォームのセキュリティの概要

Oracle MiniCluster S7-2 はオラクルの SPARC S7 プロセッサのコンピューティング能力を搭載した多目的エンジニアド・システムとして構築されており、アクティブ/アクティブの独立した 2 台のコンピューティング・サーバーに 10GbE の冗長ネットワーク接続を備えています。そして、完全に冗長化された高性能な共有フラッシュ・ストレージを備えた、高可用性アーキテクチャを構成しています。コンピューティング・サーバーは、効率的な仮想化機能をもつ Oracle Solaris ベースのセキュアな仮想マシンと高可用性 Oracle Database を利用できるように、完全に最適化されています。また、別の 10GbE ネットワークの経路によって、SPARC S7 サーバー上の仮想マシン環境とホストされるアプリケーション間の相互通信がすべて管理されます。Oracle MiniCluster S7-2 では、これらのエンジニアド・コンポーネントが連携して機能することで、セキュアな単一テナント（アプリケーションとデータベースをホストする専用のコンピューティング・プラットフォーム環境）を実現しています。また、企業とクラウド・サービス・プロバイダは最初のインストール時から、セキュリティとコンプライアンスを確保できるように設計され、検証済みで、コンプライアンスに準拠した、徹底的に保護されたコンピューティングおよびアプリケーション環境が確立されます。

SPARC S7 プロセッサには常時オンのハードウェア支援型暗号化機能が搭載されており、Oracle MiniCluster S7-2 でホストされるエンティティは、高パフォーマンスな（保管時、使用時、送信時の）データ保護機能によって情報を保護できます。また、このプロセッサにはオラクルの Silicon Secured Memory（オラクルの SPARC M7 および SPARC S7 の機能）も搭載されており、メモリ・データの破損およびメモリ・スクレイピングに関連する攻撃を検出および防止できるため、アプリケーション・データの整合性を維持できます。Oracle MiniCluster S7-2 では、高可用性を備えた最大 24 台の仮想マシン（ノードあたり最大 4 台のデータベース仮想マシンおよびノードあたり最大 12 台のアプリケーション仮想マシン）をホストできます。これら 24 台の仮想マシンに加えて、管理専用の仮想マシンが 2 台と、共有サービス（NFSv4 ストレージ、Oracle key wallet、オブジェクト・ストアなど）をホストする専用の仮想マシンが 2 台あります。デフォルトでは、すべての仮想マシンは完全に暗号化されたストレージにあり、暗号化されたネットワーク接続を使用します。また、すべての仮想マシンは 250 種類を超える標準のセキュリティ制御で事前に構成および検証されています。これらのセキュリティ制御によって、必須ではない、または既知の脆弱性が存在するサービス、ポート、プロトコルを無効にすることで、システムが攻撃される可能性を減らし、プラットフォームの機密性、整合性、可用性を確保します。さらに、信頼できる接続のみを公開サービスで受け付けるように構成することで、機密性、整合性、可用性を確保し、多段階攻撃を防ぎます。

図 1 は、Oracle データベースのデプロイメントとアプリケーション・ワークロードを統合する Oracle MiniCluster S7-2 の一般的な構成を表しています。

図1.Oracle MiniCluster S7-2の一般的なデプロイメント

Oracle MiniCluster S7-2 アーキテクチャに組み込まれている各コア・コンポーネントのセキュリティ機能をよく理解することが重要です。これらの機能を簡単に示すため、8 つのカテゴリ（セキュアな仮想マシン、アクセス制御、データ保護、ユーザー管理、監視と監査、コンプライアンス、専用のコンピューティング・クラウドのデプロイメント、セキュリティ管理）にグループ化しています。

Oracle MiniCluster S7-2のセキュリティ機能

このリストは網羅的なものではなく、階層化されたセキュリティ戦略を導入しようとする組織およびクラウド・サービス・プロバイダでもっとも多く使用されている Oracle MiniCluster S7-2 の主要なセキュリティ機能に焦点を当てることを意図しています。

セキュアな仮想マシンとネットワーキング

Oracle MiniCluster S7-2 コンピュート・ノード内のセキュリティは、複数のレベルで提供されます。まず、ホスト・コンピューティング・サーバーのセキュアなベリファイド・ブート、独立した仮想マシンでの堅牢かつ最小限の OS の実行によって、ワークロードとデータに対する、権限のないユーザーやシステムからのアクセスを防ぎます。Oracle MiniCluster S7-2 の仮想マシンでは、Oracle Solaris Zones テクノロジーによって独立したコンピューティング環境をホストし、同じオペレーティング・システムで実行される各種アプリケーションを効果的かつ効率的にサンドボックス化して、他の仮想マシンで発生する意図しないアクティビティまたは悪意のあるアクティビティからアプリケーションを保護します。Oracle Solaris Zones の各インスタンスは同じカーネルで実行されま

すが、それぞれが固有の ID を持ち、それぞれのリソース、ネームスペース、プロセスは独立しています。基本的に、Oracle Solaris Zones テクノロジーによって、Oracle MiniCluster S7-2 の仮想マシンの強力な独立性と柔軟なリソース制御を、Type 1 ハイパーバイザで実行される従来の仮想マシンより少ない CPU およびメモリ・フットプリントで実現できます。Oracle MiniCluster S7-2 は単一テナントの専用コンピューティング環境用ですが、Oracle MiniCluster S7-2 の仮想マシンを使用して、ホストされるアプリケーションを論理的に分離することができます。この仮想マシンは、IT コンプライアンス・ポリシーに準拠し、リスク対象を限定するために不可欠な、細粒度のサンドボックスによる封じ込め機能を提供します。

Oracle MiniCluster S7-2 では、これらの仮想マシン内のセキュリティ制御レイヤーにアプリケーションをラッピングすることでアプリケーションのセキュリティを強化し、Oracle MiniCluster S7-2 の仮想アシスタント機能によってアプリケーション環境外から一元的に管理します。仮想アシスタントは、Oracle MiniCluster S7-2 のインストールおよび管理用のコンソールとして機能します。これにより、データベース VM の仮想マシン・グループの構成や Oracle Real Application Clusters（Oracle RAC）高可用性データベース・クラスタのインストールとデプロイメントに加え、アプリケーション VM の構築が行えます。さらに、セキュリティとコンプライアンスの管理、プッシュボタン方式による簡易なシステム全体へのパッチ適用、自動化して人的エラーを防止することによるプラットフォーム全体のセキュリティの向上も可能です。

セキュリティ・プロファイル

各仮想マシンはセキュリティ・プロファイルの概念に従って構成されます。これは、業界固有のセキュリティ要件を満たしてコンプライアンス対策を強化するためのものです。セキュリティ・プロファイルは、業界固有の標準または規制条項で定義されている一連の包括的なセキュリティ制御およびポリシーを定義します。これらはインストールの処理中に自動的に適用されます。適用時にセキュリティ・プロファイルはセキュリティ要件を実行し、必要なセキュリティ制御を割り当てます。たとえば、必須サービスのホワイトリスト化、不要なポート、プロトコル、サービスのブラックリスト化、オペレーティング・システムの堅牢化と最小化や、ユーザー、ロール、パスワード、ネットワーク、ストレージ構成に対する暗号化、権限、最小権限の適用などです。現在、Oracle MiniCluster S7-2 は PCI-DSS 3.2、FIPS 140-2 Level 1 準拠の DISA STIG、および Centre for Internet Security（CIS）相当のセキュリティ・ベンチマーク（HIPAA、FISMA、SOC-2 のセキュリティ要件に準拠）という 3 種類のセキュリティ・プロファイル・セットによって、プラットフォームのコンプライアンス対応を実現しています。Oracle MiniCluster S7-2 の初期インストール・プロセス中にいずれかのセキュリティ・プロファイルを選択して、コンプライアンス対応の仮想マシン環境を構築できます。ZFS プールおよび暗号化された ZFS データ・セットを使用することで、各仮想マシンのストレージをさらに細かく分割して暗号的に分離します。そうすることで、各アプリケーションおよびデータベースの仮想マシンに、固有の分離した暗号化ストレージを割り当てることができます。暗号化された ZFS データ・セットを使用すると、アプリケーションの対象外のファイル・システムに保存されているデータ（構成ファイル、アプリケーション・ログ、バックアップなど）の保護によって、アプリケーションの暗号化が補完されます。アプリケーション仮想マシンもデータベース仮想マシンも、オンデマンドの共有ストレージ（NFSv4 経由）を使用して、バイナリ、アプリケーション固有のデータ、バックアップを保存することができます。仮想アシスタント・コンソールからオンデマンドで Oracle MiniCluster S7-2 の共有ストレージの使用を無効にすることを強くお勧めします。本番環境にデプロイされたときのセキュリティ・コンプライアンスを確保するためです。物理ネットワーク・レベルでは、仮想マシン・グループへのクライアント・アクセスはデバイス管理およびノード間のサーバー通信の両方から分離されています。

ネットワークの分離

クライアント・アクセスはプラットフォームで実行しているサービスへ確実かつ高速にアクセスできる 10Gbps の Ethernet ネットワーク経由で行われます。クライアント・アクセス用の Ethernet ネットワークを経由して行われている仮想マシンとのネットワーク通信の分離を進めるため、物理的に分離する方法だけでなく専用の仮想 LAN（VLAN）も利用して、ニーズに応じて仮想マシン・グループとの間のネットワーク・トラフィックを分けることをお勧めします。同様に、物理的に分離されたサブネットへのアクセスに Oracle ILOM の管理アクセスも使用できるため、運用ネットワークと管理ネットワークをハード的に分離できます。また、プライベート・ネットワーク経由でのノード間通信も可能です。コンピュート・ノードとホストされる仮想マシン・デバイスも、このネットワーク経由で通信できます。さらに、ネットワークでは、通信の機密性と整合性を確保できるようにするため、暗号化されたプロトコル（IPSec/IKE、TLSv1.2、SSHv2 など）を使用することをお勧めします。オペレーティング・システムのカーネルによって実行される排他的ネットワーク・スタックと統合型仮想ネットワーク・スイッチを使用すると、ネットワークへのアクセスをポリシーに準拠させることができます。これにより、たとえば、ある仮想マシンで実行しているサービスが、他の仮想マシンで送受信されるネットワーク・トラフィックを傍受できないようにすることができます。

マルウェア対策システム

コンピューティング環境のマルウェア対策のため、Oracle MiniCluster S7-2 にデプロイされるアプリケーションは自動的に、マルウェア対策システムによって一般的なセキュリティ・エクスプロイトから保護されます。ハードウェア（ADI、ASLR、DEP）とソフトウェア（ベリファイド・ブート、署名付きパッケージ、ソフトウェアの整合性チェック）の一連のテクノロジーが相互に構築されているため、インフラストラクチャとアプリケーションの両方の整合性が確保されます。オラクルの SPARC M7 プロセッサと SPARC S7 プロセッサで新たに導入された Silicon Secured Memory 機能によって、さまざまなデータ・アクセス攻撃（バッファのオーバーフローやオーバーリードなど）からメモリを保護することで、マルウェア対策システムが強化されています。サーバー初期ブート中のベリファイド・ブート・プロセスは一連の信頼性の高い方法で実行され、ファームウェア、ブート・システム、カーネル、オペレーティング・システム・モジュールの、工場出荷時に署名された暗号化署名がチェックされます。これにより、コンピューティング環境におけるマルウェア、ランサムウェアの取り込み、重要なブート・コンポーネントおよびカーネル・コンポーネントに対する悪意のある改変または偶発的な変更のリスクが軽減されます。また、Oracle Solaris オペレーティング・システムが動作する仮想マシンは、ZFS ファイル・システムに保存されているコンテンツのリアルタイムなマルウェア対策スキャンを提供する VSCAN サービスをサポートします。VSCAN サービス・エンジンは、業界標準の ICAP プロトコルを使用しているサード・パーティのウイルス・スキャン・サービス・プロバイダを使用するように構成できます。VSCAN サービスでは、最新のウイルス定義を使ってファイル・システムをスキャンし、最後のスキャン時からファイル・システム内のファイルが変更されていないかどうかを検証します。ウイルスが検出されるとファイルに隔離済みのマークが付き、その情報を含む監査レコードが作成されます。

読取り専用の仮想マシン

Oracle MiniCluster S7-2 では、オプションで Mandatory Write Access Control（MWAC：強制書込みアクセス制御）カーネル・ポリシーを設定することで読取り専用の仮想マシンを有効にして、レジリエンスがある、整合性の高い改ざん防止オペレーティング・システム環境を構築できます。読取り専用の仮想マシンでは Oracle Solaris 本来のセキュリティ機能に基づいて構築されており、特別

なサンドボックス・モードが利用できます。このモードでは、システム構成はロックされるがアプリケーションは通常動作するような仮想マシン/ゾーンを保護できます。このモードの構成は簡単で、仮想マシンを再起動するだけで有効/無効にすることができます。これにより、ルート・ファイル・システムに含まれる一部（またはすべて）のオペレーティング・システムのディレクトリやファイルを変更できるのは、システムのプライマリ管理者だけとなります。この読取り専用セキュリティ対策を実施することで、不正な改変を防ぎ、変更管理手順をより厳密にし、カーネルベースのマルウェアとユーザーベースのマルウェア両方の侵入を防ぐことができます。ただし、読取り専用の仮想マシンでホストされるアプリケーションが、MWAC ポリシーの対象となるファイル・システムに対して、直接的な書込み依存性がないことを検証する必要があります。

アクセス制御

Oracle MiniCluster S7-2 は、システム、サービス、アプリケーション・データ、ワークロード、およびこれらすべてが実行されるインフラストラクチャを保護するために、包括的でありながら柔軟な一連のアクセス制御機能を備えています。

プラガブル認証

Oracle MiniCluster S7-2 では、アクセス制御アーキテクチャの基盤として、Oracle Solaris のロールベースのアクセス制御（RBAC）機能を利用しているため、一元的な権限によってオペレーティング・システムおよび仮想化の管理アクセスを管理、制御、監査できます。また、Oracle MiniCluster S7-2 では、ユーザーやアプリケーションがシステム・サービスにアクセスするためのさまざまなアクセス制御方法について、Oracle Solaris を利用しています。従来のユーザー名とパスワードの組み合わせは依然として広く使用されていますが、オプションで Oracle Solaris のプラガブル認証モジュール（PAM）アーキテクチャを使って、より厳密な多要素認証または 2 要素認証を統合できます。これにより、LDAP、Kerberos、ワンタイム・パスワード、公開鍵認証を使用できます。さらに、より厳密な認証方法によって、厳格なパスワード・ポリシーやパスワード暗号化を利用したユーザー認証を実施できるほか、Oracle Solaris やサード・パーティ・プロバイダの PAM モジュールを使用したワンタイム・パスワード（HMAC、Oracle Mobile Authenticator の OAuth2、Google Android Authenticator など）による 2 要素認証が可能な PAM 認証スキームを強化したオプションでもユーザー認証を実施できます。また、PAM 認証スキームによって、PKI および生体認証ベースのスマートカードを使ったサード・パーティの多要素認証プロバイダとの統合を実現することもできます。

Oracle Directory Server Enterprise Edition などの LDAP ディレクトリ・サービスと統合することで、仮想マシン全体でユーザー固有のセキュリティ・ポリシーを実施することもできます。また、仮想マシンへのシングル・サインオン・アクセス用に Kerberos と監査、暗号化、ユーザー管理機能を統合して、エンタープライズ認証ポリシーを厳密に実施したり、Oracle MiniCluster S7-2 がホストする Kerberos 対応のアプリケーションを保護したりすることもできます。

職務分離と最小権限

職務分離の原則は、共謀行為のリスクを低下させ、不注意によるエラーを防ぐため、Oracle MiniCluster S7-2 のすべての重要な管理操作やセキュリティ上重要な操作に適用されます。これにより、複数名による認可ワークフローを利用した職務分離が実施され、ユーザー・アカウントの管理、セキュリティの管理、リソースの削除などの機能は、その実行権限が認可されたユーザーに対してのみ付与されます。これはまた、システムのすべてのプログラムとユーザーに対してジョブの完了に最小限必要な権限で操作することを求める、最小権限のセキュリティ原則にも適合します。Oracle

MiniCluster S7-2 のソリューションは、特定の管理タスクのロールを幅広く使用しています。ユーザーが引き受けられるのは、認可されているロールのみです。権限プロファイルを作成してロールに割り当て、ロールが実行できるタスクを指定します。ユーザー・プロビジョニング操作と Oracle MiniCluster S7-2 の重要な管理/メンテナンス操作はすべて、複数名の認可ワークフローによってサポートされる、最小権限の原則と職務分離の原則に基づいて実行されます。システムの認可ワークフローには、ロールが異なる複数のユーザー（Oracle MiniCluster S7-2 システムの管理者であるスーパーバイザーと、Oracle MiniCluster S7-2 のインストールおよびインストール後の管理操作を管理するプライマリ管理者など）が参加して、すべてのセキュリティ上重要な操作を承認する必要があります。

ロールベースアクセス制御（RBAC）

Oracle MiniCluster S7-2 のコンピューティング環境は包括的な RBAC 機能に基づいて構築されているため、管理機能の委任、ユーザー・アクセスの制限、管理階層の実装、再ログインなしでのジョブへのロール割り当て、特定のアクションへのアプリケーションの追加、仮想マシン同士の分離、管理機能の昇格、ソフトウェアの制限ポリシーの設定、アプリケーションの読取り専用への制限などを柔軟に行うことができます。管理機能を、ロールとして付与可能なプロファイルに分離することで、匿名で非常に権限の強い root アクセスの必要性とリスクを排除できます。また、Oracle Solaris のアクセス制御を使用することで、タスクの完了に必要な最小限のアクセス権でアプリケーションを実行し、アプリケーションの誤動作や、マルウェアによるシステムの他のアプリケーションへの影響を少なくします。

RBAC は Oracle MiniCluster S7-2 のコンポーネントすべてに統合されており、オペレーティング・システム・レベルのアクセス制御のあらゆるニーズをサポートする、一貫性のあるアーキテクチャを実現します。Oracle MiniCluster S7-2 には root ユーザーが存在しません。代わりに root はロールとして、プライマリ管理者として登録されているユーザーに割り当てられます。特定のロールが認可されると、ユーザー・アカウントが作成されます。Oracle MiniCluster S7-2 では、Oracle MiniCluster S7-2 の管理操作と日常の操作をサポートするために、プライマリ管理者、セカンダリ管理者、テナント管理者、監査担当者という 4 種類のロールが定義されています。プライマリ管理者は root ロールとして機能し、Oracle MiniCluster S7-2 システムのほとんどの管理権限（すべてのコンピュート・ノード、ネットワーク、データベース、ストレージなど）を定義するものです。root ロールを持つユーザーは、インストールおよび重要な管理上の操作すべてを制限なく実行できます。プライマリ管理者は、操作の委任と、ユーザー（新しいプライマリ管理者およびセカンダリ管理者を含む）の追加および削除の承認を行うことができます。ユーザーは自分の資格証明でログインする必要があります。セカンダリ管理者の別名は mcadmin ロールで、Oracle MiniCluster S7-2 にデプロイされる仮想マシンのセカンダリ管理者の権限を定義するものです。このロールに割り当てられたユーザーは、管理およびサービスを行う仮想マシンの、日常的な管理操作をすべて処理します。テナント管理者の別名は tadmin ロールで、Oracle MiniCluster S7-2 の仮想マシンの管理者が持つ権限を定義するものです。このロールは、アプリケーションのインストールとデプロイメントをサポートする日常的な管理操作を担当する VM 管理者の権限を定義するものです。監査担当者のロールは、Oracle MiniCluster S7-2 内の監査証跡を管理、レビュー、レポートする権限を定義するものです。これらのロールによって実行されるアクションと操作はすべて、ロール ID ではなくユーザーID に基づいて記録および監査されます。つまり、従来の UNIX/Linux 環境では複数の管理者が root パスワードを知っており、スーパーユーザーによる管理アクションを実行したユーザーを特定することができませんでした。しかし、Oracle Solaris の RBAC が適用された Oracle MiniCluster S7-2 では、監査証跡内の特権アクションは、その管理ロールを持つユーザーに必ず起

因します。以上をまとめると、これらの機能を使用して、重要データを不正なアクセスや管理上の誤用から保護することで、重要な業務上の操作の実行ユーザーおよびその処理内容を確実に特定できます。ただし、データ・セットの物理的な損失や不適切な管理を防ぐことはできません。

ネットワークとストレージのアクセス制御

Oracle MiniCluster S7-2 でデプロイされる仮想マシンにはホストベースのファイアウォールが事前構成されており、ネットワークの外部境界および Oracle MiniCluster S7-2 ネットワーク内の内部境界でネットワーク通信を監視および制御します。Oracle MiniCluster S7-2 システムのすべての仮想マシンには、公開サービスに対するネットワーク・アクセスを制限する機能があります。具体的には、ホストベースのファイアウォールのパケット・フィルタリングによって、インバウンド/アウトバウンドのネットワーク・トラフィック・ポリシー（仮想マシン・レベル）やアクセス制御リストを適用し、物理デバイス、仮想デバイス、およびシステムの公開サービスの間でやり取りされる通信を制限します。ホストベースのファイアウォールでは、セキュリティ・ポリシーによってパケットが階層的に検査されます。このポリシーは、プロトコル、ポート、ソース、および宛先の IP アドレスに基づくパケットのフィルタリングによって、認可されたソース、宛先、トラフィックの種類を識別できるように構成されています。

Oracle MiniCluster S7-2 ではデフォルトでセキュリティ対策がデプロイされているため、Secure Shell（SSH）以外のネットワーク・サービスがインバウンド・ネットワーク・トラフィックを受け付けることはできません。他の有効なネットワーク・サービスが、仮想マシン内でリクエストを内部的にリッスンします。そのため、すべてのネットワーク・サービスはデフォルトで無効になっているか、ローカルのシステム通信のみをリッスンするように設定されています。このデフォルトのセキュリティ構成は、組織の要件に基づいて自由にカスタマイズできます。Oracle MiniCluster S7-2 内に存在するすべての仮想マシンでは、ホストベースのファイアウォールが事前構成されています。これは、Oracle Solaris の IP フィルタ機能を使って、ネットワークおよびトランスポート・レイヤーの（ステートフル）パケット・フィルタリングを実行するためです。IP フィルタには、ホストベースの一連のネットワーク・ファイアウォール機能（ステートフル・パケット・フィルタリング、ネットワーク・アドレス変換、ポート・アドレス変換など）があります。Oracle MiniCluster S7-2 でデプロイされる仮想マシンのデフォルトのファイアウォール・ポリシーは、「デフォルトですべて拒否（Default deny-all）」モードで構成されます。また、デフォルトのファイアウォール・ポリシーでは、ホワイトリスト・アプリケーション（Oracle Database や Oracle Fusion Middleware アプリケーションなど）と必須サービスのみが許可されるルールとなっています。ファイアウォール構成を変更して、組織の要件に合わせたり、ファイアウォール・ポリシー・ルールの変更、削除、新規追加によってデプロイ済みのアプリケーションをサポートしたりすることができます。各ルールでは、通信が許可される特定の送信元、宛先、プロトコルとポートの組み合わせを定義します。ファイアウォール・ルールで指定される送信元と宛先は、単一のホスト IP の場合と、サブネットまたはセキュリティ IP のリスト（外部ホストのリスト）の場合があります。たとえば、仮想マシンでの Oracle Secure Backup に対するファイアウォール・ルールを設定して、外部ホストとの間でポート 10000 経由の NDMP アクセスを許可することができます。

Oracle MiniCluster S7-2 でデプロイされる仮想マシンでは、データ・リンク保護が事前構成されています。これは、Oracle MiniCluster S7-2 ネットワークに悪意のある可能性のあるゲスト VM が追加されることによって発生しうる損害を防ぐためです。この機能によって、IP スプーフィング、MAC スプーフィング、L2 フレーム・スプーフィング（BPDU（ブリッジ・プロトコル・データ・ユニット）攻撃など）から保護されます。データ・リンク保護によって削除されたパケットは、Oracle Solaris のカーネル統計によって追跡できます。

データベースのアクセス制御

Oracle MiniCluster S7-2 では、オペレーティング・システムとデータベースのレベルで、さまざまなアカウントを使用してデータベース・インスタンスとシステム管理者のジョブ・ロールを分離しています。ストレージの場合、ユーザーやアクセスの制御は定義されていません。なぜなら、ストレージ・アレイは Oracle MiniCluster S7-2 コンピューティング・サーバーと緊密に統合された固定機能アプライアンスとして接続されており、この特定の用途向けに最適化されていると想定されるためです。共有上のディレクトリとファイルへのアクセスは、POSIX アクセス制御および拡張されたアクセス制御リストによって管理されます。さらに、これらの機能を組み合わせて、共有上のコンテンツの読取り、書込み、実行のアクセス権を持つユーザーを限定したり、実行可能な委任管理操作の種類（スナップショットやクローンの作成、データ・セット・プロパティの変更など）を制御したりすることができます。

Oracle Database 内では、ユーザーに特定の権限およびロールを割り当てて、認可されたデータ・オブジェクトのみに対するアクセス権を付与できます。これで、明示的に許可されていない場合にデータベースやスキーマ間でデータが共有されることを防止できます。Oracle Database で使用できるパスワードベースの認証に加えて、Oracle Advanced Security オプションを使用することにより、公開鍵の資格証明や既存の RADIUS または Kerberos インフラストラクチャを利用した強力な認証を実装できます。さらに、Oracle Enterprise User Security を使用して、データベースを既存の LDAP リポジトリと統合して認証や認可を行うこともできます。つまり、これらの機能を使用して、データベースに接続しているユーザーをより確実に識別できます。オプションで、Oracle Database Vault を使用して、管理ユーザーや特権ユーザーのアクセスを管理し、アプリケーション・データにアクセスできる方法、タイミング、場所を制御できます。Oracle Database Vault を使用すると、盗まれたログイン資格証明の悪用、アプリケーション・バイパス、アプリケーションおよびデータに対する不正な改変（アプリケーション・データのコピー作成を含む）を防ぐことができます。Oracle Database Vault はほとんどのアプリケーションおよび日常的なタスクに対して透過的であり、多要素の認可ポリシーをサポートできるため、業務を中断せずにセキュアにポリシーを実施できます。

データ保護

保管時、送信時、および使用時にデータを保護および検証したいという要望は、多くの場合、暗号化サービスの使用を前提にしています。暗号化と復号化からデジタル指紋、鍵管理、証明書検証まで、暗号化は最新の IT 組織およびクラウド・インフラストラクチャでもっとも広く導入されているセキュリティ制御の 1 つです。Oracle MiniCluster S7-2 には、完全かつ効率的で高パフォーマンスなエンド・ツー・エンドの暗号化によってデータを保護するための豊富な機能が含まれています。

図2.Oracle MiniCluster S7-2：組込みのデータ保護ライフサイクル

使用中のデータの保護

Oracle MiniCluster S7-2 コンピューティング・サーバーには SPARC S シリーズ・プロセッサが搭載されています。このプロセッサでは、パフォーマンスの低下なしで強力な暗号化サービスを実現するための統合型オンチップ暗号化アクセラレーション機能と、ハードウェアベースでメモリを保護するための Silicon Secured Memory 機能が組み込まれています。SPARC S7 プロセッサによって、15 種類の業界標準暗号化アルゴリズムのパフォーマンスを向上させ、乱数をセキュアかつ高速に生成することができます。これらの機能は、SPARC S7 プロセッサで直接実行されるオペレーティング・システムに提供されるか、または個々の仮想マシン経由で提供されます。Oracle Solaris オペレーティング・システムでは、デフォルトで（直接的または Oracle VM Server for SPARC 経由で仮想的に）SPARC S7 が利用され、Oracle Solaris 暗号化フレームワーク機能によって暗号化が非常に効率的に処理されるようになっています。この共有フレームワークに、Oracle Solaris オペレーティング・システムで暗号化を提供または使用するサービスが集まっています。Oracle Solaris 暗号化フレームワークを使用するユーザー、アプリケーション、サービスは、最適化されたアルゴリズムの使用だけでなく、ハードウェアの暗号化アクセラレーションとハードウェア・セキュリティ・モジュール（使用している場合）のシームレスな利用も保証されます。Oracle Solaris は、Secure Shell、IPSec/IKE、Kerberos、ZFS 暗号化などの暗号化サービスを完全に補完します。また、Oracle Solaris には、OpenSSL または Java を使用するアプリケーションがこの共通フレームワーク（利用可能な暗号化アクセラレーションを含む）を使用することを可能にする統合も含まれます。

ハードウェアベースのメモリ保護のための Silicon Secured Memory 機能では、動的ポインタ・チェックによってメモリ参照エラーを検出できます。このテクノロジーによって、不正なポインタ、無効な参照または古い参照、バッファのオーバーランを防ぎ、診断と修正に多くの開発時間が費やされる可能性のある、メモリ・スクレイピング、発見されにくいデータ破損、アプリケーションの問題を防止できます。アプリケーション固有のメモリ・アロケータ、たとえば Oracle Database 12c アプリケーションの SGA メモリ割当てや Oracle Solaris の汎用メモリ・アロケータ（malloc）などには、Silicon Secured Memory を利用する機能が実装されています。また、Oracle MiniCluster S7-2

でデプロイされる仮想マシンも、アドレス空間配置のランダム化（ASLR）をデフォルトで使用するように構成されています。これにより、タグ付きの実行可能な命令が接続されていないアドレス空間に書き込まれるため、侵入者がメモリをスキャンしたり、実行可能スタック上に命令を挿入したりする可能性を Oracle MiniCluster S7-2 によって減らすことができます。

送信中のデータの保護

暗号化によるセキュアなプロトコルを使った通信の機密保護と整合性を確保するため、Oracle MiniCluster S7-2 でデプロイされる仮想マシンでは、Secure Shell（SSH）、IPSec/IKE、SSL/TLS のプロトコルをサポートしやすくなっています。Secure Shell によって、システムおよび Oracle Integrated Lights Out Manager（Oracle ILOM）へのセキュアな管理アクセスを行っています。

IPsec/IKE によって仮想マシンとネットワーク・ピアの間の通信を保護できます。また、SSL/TLS によって、アプリケーションとその他のサービスの間でセキュアな通信を実現できます。IPsec/IKE 構成を有効にすると、ネットワーク上を流れる仮想マシン間トラフィックの IP ベースの通信と NFS トラフィック（必要な場合）の機密性と整合性を保護できます。セキュリティと暗号化の独立性を高めるため、各仮想マシン・インスタンスの個別のデジタル証明書を含む IPSec ピアの割り当てを検討することができます。Oracle MiniCluster S7-2 で構成された IPsec/IKE を使用して、1 組の仮想マシン間や、仮想マシンと VPN セキュリティ・ゲートウェイの間の 1 つまたは複数のデータ・フローを保護できます。これにより、共有ネットワーク上を流れるデータであっても、独立した暗号化境界によって保護できます。プライバシーおよびコンプライアンス規定の重要性を考えると、統合型のデータベースおよびアプリケーション・アーキテクチャを検討する組織は、データベースやアプリケーションとの間でやり取りされる情報を暗号化して保護することをしっかりと検討する必要があります。これにより、ネットワーク上を流れるデータが、権限のないユーザーに対して開示されることはありません。Oracle MiniCluster S7-2 は、送信中の情報を保護するため、Oracle Database ネイティブと SSL/TLS の両方の暗号化方法をサポートしています。また、アプリケーション、データベース・インスタンス、クラスタごとに個別の SSL 証明書を使用することで、組織は、データが共有のネットワークまたはインタフェース上を流れる必要がある場合でも保護する、独立した暗号化境界を実質的に構築できます。

Oracle MiniCluster プラットフォームが提供するネットワーク暗号化サービス（SSH、IPsec/IKE、SSL/TLS、Kerberos など）は自動的に高速化および最適化されるため、パフォーマンスが非常に優れています。また、Oracle ILOM および仮想マシンの個々のインスタンスとの管理接続およびサポート接続では、（SSH プロトコルや TLSv1.2 プロトコルを使った）強力な暗号化による保護もデフォルトで利用されるため、偶発的な機密情報の開示や、管理接続の乗っ取りを防ぐことができます。これにはインタラクティブ・セッションだけでなく、管理および監視ツール、バックアップおよびリカバリ・ソリューション、およびその他の同様のサービスで使用される通信も含まれます。

保管中のデータの保護

Oracle MiniCluster S7-2 ストレージでは、保管時のデータがデフォルトで保護されます。これは、インストール中に ZFS 暗号化によって自動的に構成されます。アプリケーションおよびデータベースの仮想マシンに接続されているストレージの ZFS データ・セットは、例外なくすべてデフォルトで暗号化されます。管理用仮想マシン（大域ゾーン）の場合、ルート・ファイル・システムだけは暗号化されません。また、管理用仮想マシンのユーザーは、暗号化されたホーム・ディレクトリを有効にして使用できます。デフォルトでは、デプロイされるすべての ZFS データ・セットで最新の Oracle Solaris 11 の暗号化サービス API が使用されます。このため、Oracle MiniCluster S7-2 プラットフォームで使用可能な AES アルゴリズムのハードウェア・アクセラレーションのメリットを自動

で享受できます。暗号化のポリシーは、データ・セット（ファイル・システムまたは ZVOL）の作成時に、データ・セット・レベルで設定されます。各 ZFS のオンディスク・ブロック（最小サイズは 512 バイト、最大サイズは 1MB）は、Galois/Counter Mode（GCM）の AES アルゴリズムで暗号化されます。インストール時に、Oracle Solaris PKCS#11 キーストアにラッピング鍵がセキュアに作成されます。ただし、ラッピング鍵は、ファイル・システムをオフラインにせずにいつでも変更できます。データ暗号化鍵はデータ・セットの作成時にランダムに生成されますが、必要に応じて変更できます。このように、Oracle MiniCluster S7-2 ストレージに書き込まれるデータはすべて暗号化された状態で保管されるため、アプリケーションやデータベースによる追加のアクションは不要です。

セキュアなデータ破壊

Oracle MiniCluster S7-2 がホストするサービスがプライマリ管理者の要求や専用コンピューティング・クラウド・コンシューマによって終了されると、Oracle MiniCluster S7-2 では仮想マシン環境およびその関連データが、一旦削除されたものは確実にアクセスも読取りもできなくなるような方法でセキュアに消去されます。Oracle MiniCluster S7-2 では、ファイル・システムに存在する仮想マシンとデータをセキュアに消去するため、許容可能な信頼度で安全に鍵を破壊し、ZVOL に保存されているデータと暗号化鍵をアクセス不可にするという、確実な削除メカニズムを採用しています。Oracle MiniCluster S7-2 では、セキュアな削除プロセスを開始する前に、要求者とプライマリ管理者が関与する 2 段階の承認プロセスと通知がトリガされます。

データベースの暗号化サービス

Oracle MiniCluster S7-2 は透過的データ暗号化（Transparent Data Encryption）をサポートしています。これは Oracle Advanced Security の機能で、データベース内の情報を暗号化するためのオプションです。透過的データ暗号化は、アプリケーション表領域の暗号化と、表内にある各列の暗号化の両方をサポートしています。一時表領域および REDO ログに保存されているデータが暗号化されます。データベースがバックアップされても、データはバックアップ先のメディアで暗号化されたままであるため、物理的な保存場所にかかわらず保管中の情報を保護できます。Oracle Advanced Security オプション（透過的データ暗号化を含む）では、SPARC S7 プロセッサの暗号化アクセラレーション機能を利用できます。このため、ソフトウェアのみの暗号化方法にはつきものの大幅なパフォーマンス低下なしで、組織は情報を保護できます。

Oracle Database には、ネイティブな暗号化または Transport-Layer Security（TLS）のいずれかによって SQL*Net と JDBC のトラフィックを暗号化し、ネットワーク上を流れる情報を保護する機能もあります。管理用とアプリケーションの両方の接続をこのメカニズムで保護し、送信中のデータを確実に保護できます。TLS 実装では、X.509 証明書によるサーバーのみの認証と X.509 による相互（クライアントとサーバー間）認証を含む、認証方式の標準セットをサポートしています。また、Oracle Database の Oracle Recovery Manager（Oracle RMAN）機能によって作成されたバックアップ、および Oracle MiniCluster S7-2 との間で生成された Data Pump（Oracle Database の機能）のエクスポートを、オンプレミスのストレージやオフプレミスのクラウド・サービス・プロバイダに暗号化することもできます。バックアップとエクスポートは、表領域の暗号化用と同じ鍵、パスワード、またはその両方で暗号化できます。

Oracle Database デプロイメントでは SSL/TLS がサポートされているため、オプションでそのデータベース・ネットワーク接続の相互認証を使って構成できます。Oracle ネイティブのネットワーク暗号化（SQL*Net）を使って暗号化し、オプションで整合性チェックを実行して、送信中のデータが変更されたり、不正な応答のためにデータが変更されたりするのを防ぐことができます。これらのネットワーク暗号化オプションは、強力な暗号（Advanced Encryption Standard（AES）など）や、最新のハッシング・アルゴリズム（SHA-2 など）による整合性チェックをサポートしています。保管データの暗号化用のマスター暗号化鍵はデータベースで自動的に作成され、テナント単位の Oracle ウォレットか、すべての仮想マシンで使用できる Oracle Solaris PKCS#11 キーストアを使用して保存されます。SQL コマンドを使用する、認可されたデータベース・セキュリティ管理者は、定期的に鍵を変更できます。古いマスター鍵は、将来的にリストアが必要となる可能性のある暗号化済みのバックアップ用に、Oracle ウォレットに保管されます。多くのデータベースと Oracle ウォレットを持つお客様は、Oracle Key Manager または Oracle Key Vault（別途ライセンス可能な製品）を使用して、暗号化鍵とウォレットを一元管理することを検討してもよいでしょう。Oracle Key Manager はセキュリティが強化されたハードウェア・アプライアンスです。Oracle Key Vault は、データセンターで、Oracle Cloud またはオンプレミスで実行される暗号化されたデータベースに接続して動作する、セキュリティが強化されたソフトウェア・アプライアンスです。

鍵管理サービス

データ自体だけでなく、データを保護するために使用する暗号化鍵の保護も重要です。大規模なデータセンター環境の大規模なサービス・コレクションでは特に、暗号化鍵の生成と管理がずっと課題となっていました。鍵管理システムによって、保管中の情報を保護するために使用される暗号化鍵を容易に管理および監視できます。Oracle MiniCluster S7-2 には、Oracle Solaris の PKCS#11 ソフトトークン・キーストアによる、パスフレーズで保護された一元的な鍵管理サービスがあり、暗号化鍵のセキュアな認可、制御、アクセス管理を行うことができます。これらの鍵は、Oracle MiniCluster S7-2 仮想マシンに接続されている暗号化された ZFS ファイル・システムで使用されます。また、Oracle MiniCluster S7-2 は、すべてのアプリケーションおよびデータベースの仮想マシンからアクセスできる一元的な Oracle ウォレットによって、鍵のライフサイクルの一元的な運用もサポートします。このため、アプリケーションおよびデータベース・インスタンスで、鍵と証明書を作成および保存できます。Oracle ウォレットは、透過的データ暗号化で構成された Oracle Database-Oracle RAC インスタンスをサポートします。たとえば、表領域の暗号化と列レベルの暗号化、暗号化された Oracle RMAN のバックアップとリストア、SSL/TLS 通信、および Oracle Fusion Middleware アプリケーションに適用される Web サービス・セキュリティなどです。

また、Oracle MiniCluster S7-2 ではセキュアな鍵のバックアップが定期的に作成され、暗号化鍵の喪失や、キーストアの障害によるデータへのアクセス喪失に備えた追加の保護として保管されます。プライマリ管理者は Oracle MiniCluster S7-2 コンソールを使って、鍵の使用方法のサマリー（ターゲットの使用、鍵のラベル、鍵の作成データ、鍵の有効期限、鍵のステータス、鍵の変更日、関連情報など）にアクセスできます。

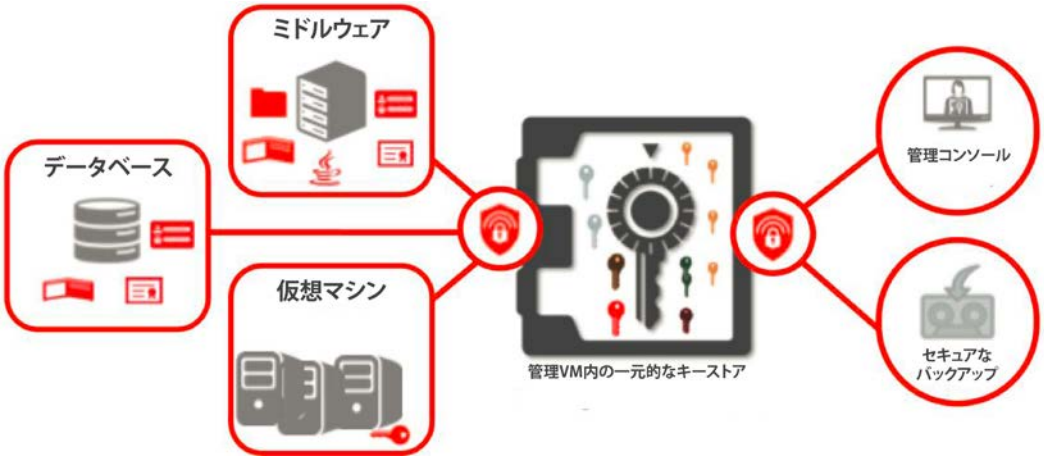

図3.Oracle MiniCluster S7-2：一元的な鍵管理サービス

Oracle MiniCluster S7-2 では、Oracle Key Manager（別途ライセンス可能な製品）の使用もお勧めします。Oracle Key Manager は、スケーラビリティと可用性の高いアーキテクチャを使ったエンタープライズ・クラスの環境をサポートする、包括的な鍵管理システム（KMS）です。Oracle Key Manager は数千台のデバイスと数百万個の鍵を管理できます。また堅牢なオペレーティング環境で動作して、強力なアクセス制御とロール分離を適用して鍵を管理します。Oracle Key Manager は動作の監視だけでなく、オプションでオラクルの Sun Crypto Accelerator 6000 PCIe カード（FIPS 140-2 に準拠したセキュアなハードウェア・モジュール）への鍵のセキュアな保管の監視と管理をサポートします。

Oracle MiniCluster S7-2 は Oracle Key Vault（OKV）の使用もサポートしています。これは別途ライセンス可能な製品であり、Oracle Database 表領域および Oracle Fusion Middleware アプリケーション用の鍵を管理するためのソフトウェア・アプライアンスです。Oracle Key Vault を使用すれば、暗号化鍵、データベースに適用される Oracle ウォレット、Java キーストア、Oracle MiniCluster 内のアプリケーションで使用される資格証明ファイルを外部管理および一元管理できます。Oracle Key Vault クライアントを Oracle MiniCluster 仮想マシンに手動でインストールして、外部でホストされている Oracle Key Vault アプライアンスを使用して暗号化鍵と管理の操作を実行することができます。また、Oracle MiniCluster ではハードウェア・セキュリティ・モジュール（HSM）も使用できます。HSM は、PKCS#11 と OASIS の Key Management Interoperability Protocol（KMIP）標準をサポートしています。サード・パーティの HSM を使用する場合は、そのベンダーが推奨するインストール・ガイドラインを参照してください。

適用される暗号化アルゴリズム

Oracle MiniCluster S7-2 プラットフォームでは、すべての暗号化アプリケーションで、NIST で承認されている暗号化アルゴリズムが使用されます。データ送信と保管データの識別、認証、保護には、次の暗号化アルゴリズムが使用されます。

暗号化アルゴリズムのリスト

アルゴリズム	鍵の長さ（ビット単位）	アプリケーション	Oracle MiniCluster S7-2 のセキュリティ機能
AES	128、192、256	暗号化、復号化	保管時のデータ保護（パスワード暗号化、ZFS データ・セット暗号化、Oracle 表領域暗号化、キーストア・バックアップ）、送信時のデータ保護はバルク暗号化のみ（TLSv1.2、IPSec/IKE、SSHv2）
RSA	2048、4096	認証、鍵交換	送信時の識別、認証、データ保護（TLSv1.2、IPSec/IKE、SSHv2）
SHA-2	256、384、512	メッセージ・ダイジェスト	送信時の識別、認証、データ保護（TLSv1.2、IPSec/IKE、SSHv2）

FIPS 140-2 Level 1への準拠

Oracle Solaris 暗号化フレームワーク機能は、Oracle MiniCluster S7-2 の中核となる暗号化ストアです。オラクルの SPARC S7 プロセッサを使用する Oracle Solaris カーネル暗号化フレームワークと Oracle Solaris ユーザーランド暗号化フレームワークは、どちらも NIST/CSE Cryptographic Module Validation Program（CMVP）によって FIPS 140-2 Level 1 への準拠が検証されています。つまり、Oracle MiniCluster S7-2 でホストされる暗号化アプリケーションは、前述の暗号化フレームワーク・モジュールで提供される NIST 承認済みの暗号化アルゴリズムを、暗号化、復号化、ハッシング、署名の生成と検証、証明書の生成と検証、およびアプリケーションのメッセージ認証機能に自動的に使用することになります。暗号化フレームワークのほか、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 FIPS 140-2 Level 1 への準拠が検証されています。このモジュールは、Secure Shell プロトコルと TLS プロトコルに基づくアプリケーションの暗号化をサポートします。組織とクラウド・サービス・プロバイダは、DISA STIG プロファイルの構成によって使用可能になる特別な FIPS 140 準拠モードで Oracle MiniCluster S7-2 仮想マシンを有効にするかどうかを、オプションで選択できます。Oracle MiniCluser S7-2 仮想マシンを FIPS 140-2 準拠モードで実行すると、ユーザーレベルのアプリケーションが Oracle Solaris モジュールおよび OpenSSL FIPS モジュールの提供する Oracle Solaris カーネル暗号化フレームワークまたは Oracle Solaris ユーザーランド暗号化フレームワークを自動で呼び出し、FIPS 140 検証済み暗号化アルゴリズムが適用されます。または、初期インストール・プロセス中に Oracle MiniCluster S7-2 の DISA STIG セキュリティ・プロファイルを有効にすると、すべての仮想マシンで、FIPS 140-2 Level 1 準拠モードおよび FIPS 検証済み暗号化アルゴリズムを使用するように自動的に構成されます。

監視と監査

コンプライアンス・レポートの作成でもインシデントへの対処においても、監視と監査は、組織が IT 環境に関するより多くの情報を把握するために必要な重要機能です。どの程度の監視および監査を導入するかは、多くの場合、保護対象となる環境のリスクや重要性によって決まります。Oracle MiniCluster S7-2 プラットフォームは、コンピューティング、ネットワーク、データベース、ストレージのレイヤーで包括的な監視および監査の機能を提供するように設計されているため、組織の監査とコンプライアンスの要件に役立つ豊富な情報を利用できます。

ワークロードの監視と監査

Oracle MiniCluster S7-2 では、監査レコードの生成、管理、保管、レポートを一元的に行います。Oracle MiniCluster S7-2 では、Oracle Solaris の監査機能を使用して、管理アクション、コマンドラインの呼出し、さらには個々のカーネル・レベルのシステム・コールまでも監視できます。すべての監査証跡は、専用の暗号化された ZFS ストレージに保存されます。Oracle MiniCluster S7-2 でデプロイされる仮想マシンはすべてこの監査機能を使って事前構成されているため、大域、ゾーン単位、ユーザー単位の監査ポリシーがあり、大域ゾーンの仮想マシンの監査レコードを保存して改ざんを防ぎます。Oracle MiniCluster S7-2 監査ログ・ストアはオプションで、システム・ログ（syslog）機能を使って監査レコードをリモート・コレクション・ポイントに送信する機能をサポートしています。また、多くの商用およびオープンソースの侵入検出および防止サービスを使用して、Oracle MiniCluster S7-2 に保存されている監査証跡を、分析およびレポート用の追加入力として活用できます。仮想マシンでは、Oracle Solaris のネイティブな監査機能を利用して、仮想化イベントとシステム管理に関連するアクションとイベントが記録されます。

データベースの監視と監査

Oracle Database はファイングレイン監査の概念をサポートしており、組織は、監査レコードの生成タイミングを決定する余地を広げるポリシーを定めることができます。このため、組織は、より関心の高いデータベース・アクティビティに注力しやすく、監査が必要となることの多い誤検知（フォールス・ポジティブ）を減らすことができます。

Oracle MiniCluster S7-2 は、Oracle Audit Vault and Database Firewall（別途ライセンス可能な製品）による、データベース監査設定管理の一元化と監視、およびセキュアなリポジトリへの監査データの自動収集をサポートしています。Oracle Audit Vault and Database Firewall にはレポート機能が組み込まれており、特権ユーザーのアクティビティやデータベース構造の変更などの幅広いアクティビティを監視できます。Oracle Audit Vault and Database Firewall で生成されるレポートによって、さまざまなアプリケーションおよび管理データベースのアクティビティが視覚化され、アクションのアカウンタビリティを立証する詳細情報を把握できます。

また、Oracle Audit Vault and Database Firewall では、不正アクセスやシステム権限の不正利用を試みた兆候のあるアクティビティを事前に出して、アラートを発することもできます。これらのアラートには、システムおよびユーザー定義のイベントや条件（特権ユーザー・アカウントの作成や機密情報が含まれる表の変更など）を含めることができます。

Oracle Audit Vault and Database Firewall のリモート・モニターを Oracle Database 11g Release 2 ドメインに常駐させ、データベース接続の調査によってデータベース・セキュリティをリアルタイムに監視し、アプリケーション・バイパス、不正なアクティビティ、SQL インジェクション、その他の脅威などの悪意のあるトラフィックを検出できます。Oracle Audit Vault and Database Firewall で

は高精度な SQL 文法ベースのアプローチによって、疑わしいデータベース・アクティビティを迅速に特定できます。

サービス品質

境界の突破やアクセス制御ポリシーの妨害以外にも、アプリケーションを攻撃する方法は多数あります。実際のところ、アプリケーションと情報の可用性が IT セキュリティ上の懸念事項と見なされる場合も多くあります。Oracle MiniCluster S7-2 プラットフォームには、サービスとデータの可用性に影響を与える可能性のある、リソース枯渇攻撃、サービス運用妨害（DoS）、偶発的な障害または故意による障害を検出および防止するための、多数の機能があります。

ワークロードのサービス品質

Oracle MiniCluster S7-2 は、仮想マシンに割り当てられる仮想 CPU、メモリ、および物理 I/O デバイスの再構成をサポートしています。これにより、組織は需要の変化に迅速に対処し、必要な箇所にリソースを移行できます。また、組織がドメインごとにリソース・ポリシーを定義することで、あるドメインのアクティビティによって他のドメインに必要なリソースが不足しないようにすることができます。同様に、Oracle MiniCluster S7-2 は Oracle Solaris オペレーティング・システムをサポートしており、グローバル、仮想マシン（ゾーン）、タスク、またはプロセス・レベルで適用できる一連の動的リソース制御が搭載されています。リソース制御を使用して、CPU とメモリの消費、コア・ファイル・サイズや、プロセス、ファイル記述子、その他の多くのパラメータの数を制限できます。組織の実際の構成とニーズに応じてこれらのパラメータの 1 つまたは複数を定義することで、Oracle Solaris オペレーティング・システム（ゾーンを含む）で実行されるアプリケーションとサービスが適切な割当てリソースを消費し、システムで実行される他のサービスに悪影響を与えないようにすることができます。また、Oracle Solaris 11 オペレーティング・システムは、データ・リンク・デバイス（仮想ネットワーク・インタフェースなど）やユーザー定義のトラフィック・フローに適用される帯域幅制限を定義する機能をサポートしています。このため、組織は事前定義したパケット属性に基づいてネットワーク・トラフィックに制限を適用できます。

ネットワークのサービス品質

Oracle MiniCluster S7-2 プラットフォームの各 SPARC S7 ノードには、パブリック・アクセス・ネットワークに接続された 10Gbps Ethernet インタフェースと、サーバー間のプライベート通信用の 10GbE インタフェースが搭載されています。これらのノードでは、Oracle Solaris の IP マルチパス（IPMP）と IEEE 802.3ad リンク・アグリゲーションを利用して Ethernet の冗長性を確保しています。このため、1 つの Ethernet インタフェースやスイッチに障害が発生してもネットワーク接続を継続できます。

また、Oracle Solaris 11 オペレーティング・システムはさまざまなネットワーク・レベルのリソース制御もサポートしています。このため、組織はさまざまなデータ・リンク・レベル（仮想 NIC、物理 NIC、リンク・アグリゲーションなど）で帯域幅制限を定義できます。このような制限は、これらの要素を経由するすべてのトラフィック、またはトラフィックのサブセットのみに適用できます。これにより、組織は、ネットワーク・トラフィックを分類して優先順位を付け、優先度の高いトラフィックを重要度の低いトラフィック・フローより優先させることができます。

データベースのサービス品質

Oracle MiniCluster S7-2 では、Oracle Real Application Clusters（Oracle RAC）の構成によって、共有キャッシュ・アーキテクチャを持つクラスタ化されたデータベースを作成できます。このため、シェアード・ナッシング方式の従来の制限事項をいくつか解消できます。その結果、Oracle RAC を使用してスケーラビリティと可用性の高いデータベース・アーキテクチャを実現できます。Oracle Database Quality of Service Management 機能は、システム全体のワークロード・リクエストを監視する、自動化されたポリシーベースのソリューションです。Quality of Service Management は正確なランタイム・パフォーマンスとリソース・メトリックを関連付け、このデータを分析してボトルネックを特定し、動的な負荷条件下でパフォーマンス目標を維持するための推奨リソース調整をします。

また、Oracle Database には、複数のデータベースが同じオペレーティング・システムで動作できるようにするための一連のツールが含まれています。たとえば、Oracle Database Resource Manager（Oracle DBRM）とインスタンス・ケージングは、きめ細かい方法による CPU リソースへの動的なアクセス制御機能をサポートしています。これにより、データベースで実行されるワークロードが、適正に割り当てられたコンピューティング・リソースにアクセスできます。また、Oracle DBRM によって並列度、アクション・セッションの数、その他の共有リソースを制御し、共有データベース・アーキテクチャに必要なリソースが 1 つのデータベースで独占されないようにすることもできます。

コンプライアンス・レポート

Oracle MiniCluster S7-2 には、すべての仮想マシンに対してコンプライアンス・レポートを生成する機能が含まれており、これは仮想アシスタント・コンソールからアクセスできます。この機能を使用すると、オンデマンドでコンプライアンス検証を実行でき、生成されるレポートによって、コンプライアンスの監査およびレポートの負担が軽減されます。米国国防総省の Security Content Automation Protocol（SCAP）エコシステムに基づき、Oracle MiniCluster S7-2 には Oracle Solaris コンプライアンス・ユーティリティが統合されています。これはセキュリティのレポートと構成を自動化するための相互に関連する標準のコレクションで、これらのツールを利用して、公共部門とエンタープライズ市場の両方でのシステム構成のコンプライアンス目標に関するレポートを作成します。監査担当者またはプライマリ管理者は、仮想アシスタント・コンソールを使用して、Oracle MiniCluster S7-2 がホストする仮想マシンのオペレーティング環境および適用されているセキュリティ制御のコンプライアンスを、すぐに評価してレポートできます。Oracle MiniCluster S7-2 のコンプライアンス・ユーティリティによって、業界標準ベンチマークの要件がセキュリティ・プロファイルにマッピングされ、適用されているセキュリティ制御がコンプライアンスに準拠しているかどうかが検証されます。Oracle MiniCluster S7-2 は現在、次の 3 種類のセキュリティ・コンプライアンス・ベンチマーク・プロファイルをサポートしています。

» Center of Internet Security ベンチマークは、（Oracle Solaris の推奨プロファイルにマッピングされる）CIS 相当のセキュリティ・プロファイルにマッピングされ、Health Insurance Portability and Accountability Act（HIPAA：医療保険の相互運用性と責任に関する法律）と Federal Information Security Management Act（FISMA：連邦情報セキュリティ マネジメント法）で定義されている業界固有のセキュリティ要件にも準拠しています。

» Payment Card Industry Data Security Standard（PCI DSS）ベンチマークは、PCI-DSS 3.2 仕様に基づく PCI-DSS プロファイルにマッピングされます。

» DISA-STIG セキュリティ・プロファイルは、U.S. Defense Information Systems Agency（米国国防情報システム局）が発行する Security Technical Implementation Guide（セキュリティ技術導入ガイド）による、組織のセキュリティ制御とコンプライアンスの要件を満たしています。

コンプライアンス・テストの間に、プロファイリング・ツールによって、セキュリティ・プロファイルで定義されている適用済みのセキュリティ制御が有効かつ使用中であることが検証されます。テストが正常に完了すると、コンプライアンス・レポートが生成されます。また、コンプライアンス機能によって、各セキュリティ・チェックの理由と、"failed"とチェックされたセキュリティの修正手順が含まれるガイドが提供されます。

Oracle MiniCluster S7-2 のアーキテクチャ・チームは、Oracle MiniCluster S7-2 のシステム・コンポーネントを定期的にレビューし、各リリース・サイクルの間は侵入および脆弱性のテスト手順を実行して、既知のセキュリティの問題を防止し、事前予防的メンテナンス・パッチによってシステムを更新し、セキュリティ・コンプライアンス・ポリシーのレポートを検証しています。

専用のコンピューティング・クラウドのデプロイメント

図 4 は、Oracle Public Cloud などの専用のコンピューティング・クラウド環境に Oracle MiniCluster S7-2 をデプロイする場合の論理的シナリオを示したものです。

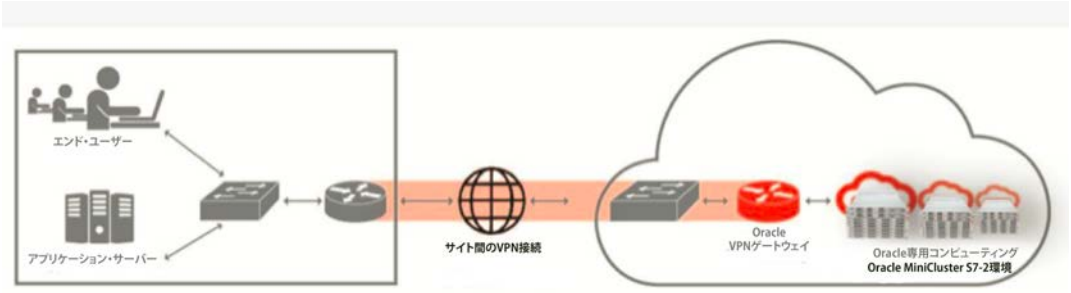

図4.Oracle専用コンピューティング・クラウド環境における、一般的なOracle MiniCluster S7-2のデプロイメント

クラウド・デプロイメントの場合、クラウド・サービス・プロバイダが、専用のコンピューティング・クラウド・サービス・ゾーン内でホストされている Oracle MiniCluster S7-2 システムとのセキュアな接続を確立します。この際、VPN ゲートウェイと、組織のデータセンターにインストールされている VPN ゲートウェイの間では、サイト間 VPN、すなわちセキュアな IPSec トンネルが使用されます。Oracle MiniCluster S7-2 でデプロイされる仮想マシンでは、ピアとの間で、事前構成された IPSec/IKE ベースの通信チャネルを利用できます。

セキュアなREST API接続

Oracle MiniCluster S7-2 には、エンタープライズ・データセンターおよび外部のクラウド・コンシューマの両方における接続要件をサポートするための、セキュアな TLSv1.2 チャネル経由の REST アプリケーション・プログラミング・インタフェース（API）があります。REST API を使用して、Oracle MiniCluster S7-2 の動作、仮想マシン・グループ、およびこれらをサポートするリソースをプログラム的にプロビジョニングおよび管理できます。Oracle MiniCluster S7-2 に対する REST API コールでは、基本認証（ユーザー名およびパスワード）とトークンベース認証を組み合わせて使用する必要があります。また、共有の ID 管理プロバイダと Oracle Web Services Manager を使用するように REST API コールを構成して、REST ベースのワークロードの認証、認可、メッセージ・レベルのセキュリティをサポートすることができます。認証リクエストが成功すると、サーバーから認証トークンが含まれる Cookie が返されます。このトークンの有効期間は、デフォルトでの 30 分間か、クラウド・サービス・プロバイダが定義した時間です。API コールを行うクライアントは、この Cookie を API コールに含める必要があります。トークンを更新するとセッションが延長されますが、セッションの有効期限を超過することはありません。

セキュリティ管理

個々のアプリケーションとサービスを適切に保護するには、セキュリティ制御と機能のコレクションが必要です。Oracle MiniCluster S7-2 の仮想アシスタントには、組織がデプロイしたサービスとシステムのセキュリティの維持をサポートするための包括的なセキュリティ管理機能があります。たとえば、セキュリティ・プロファイルの構成、ユーザー・プロビジョニング、ユーザー認可ワークフロー、暗号化鍵の使用サマリー、仮想マシン・グループのセキュアな作成と削除、SSH 鍵の再生成、鍵のセキュアなバックアップとリカバリ、オンデマンドのコンプライアンス・テスト、コンプライアンス・スコアと異常のレポートなどの機能があります。また、Oracle MiniCluster S7-2 では、Oracle Integrated Lights Out Manager、Oracle Enterprise Manager Ops Center、Oracle Enterprise Manager、Oracle Identity and Access Management Suite などのさまざまな製品のセキュリティ管理機能も利用しています。

Oracle Integrated Lights Out Manager

Oracle Integrated Lights Out Manager（Oracle ILOM）は、Oracle MiniCluster S7-2 のコンピュータ・サーバーに組み込まれているサービス・プロセッサです。これは、帯域外の管理アクティビティの実行に使用されます。

» Oracle Integrated Lights Out Manager には各種のセキュアなメカニズムがあり、組織は、コンピューティング・サーバーとストレージ・サーバー（TLSv1.2 で保護される Web ベースのアクセス、Secure Shell を使ったコマンドライン・アクセスのほか、IPMI v2.0、SNMPv3 を含む）をセキュアかつ自動的に管理できます。

» Oracle ILOM は、ロールベースのアクセス制御モデルを使った職務分離の要件をサポートしています。個々のユーザーは、実行できる機能が限定された特定のロールに割り当てられます。このため、組織は、完全な管理アクセス権を持つユーザーと、Oracle ILOM 設定の監査（読取り専用のアクセス）、リモート・ホスト・コンソールへのアクセス、またはホスト機能の制御のみを実行できればよいユーザーとを区別して決めることができます。

» Oracle ILOM ではアカウンタビリティを確保するため、すべてのログインと構成変更が記録されます。各監査ログ・エントリには、ユーザーのアクションとタイムスタンプが記載されます。

組織は、監査証跡によって不正なアクティビティや改変を検出し、これらのアクションを実行したユーザーを特定することができます。

Oracle Enterprise Manager

Oracle Enterprise Manager スイートは、アプリケーション、ミドルウェア、データベース、および物理/仮想インフラストラクチャのライフサイクルを管理するための、包括的な統合型クラウド管理ソリューションです。

» Oracle MiniCluster S7-2 に関連する内容として、アプリケーション、ミドルウェア、データベースの管理機能が、詳細な監視、イベント通知、パッチと変更の管理、および継続的な構成とコンプライアンスの管理とレポートをサポートしていることに注目することは重要です。

» Oracle Enterprise Manager では特に、組織は、データベース・グループのセキュリティ構成設定、およびアクセス制御と監査のポリシーを一元的に保持できます。これらの機能へのアクセスを認可されたユーザーに限定できるため、管理アクセスは職務分離、最小権限、およびアカウンタビリティのコンプライアンス規定を確実にサポートします。

» また、Oracle Enterprise Manager プラットフォームは各種の認証方式による強力な認証、きめ細かいアクセス制御、および包括的な監査もサポートしているため、Oracle MiniCluster S7-2 環境の管理制御にセキュアにアクセスできます。

Oracle Identity and Access Management Suite

Oracle Identity and Access Management Suite では、組織全体のユーザー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を管理します。Oracle Identity and Access Management Suite には、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、ID の管理、強力な認証、および ID とアクセスの管理のサポートが含まれます。

Oracle MiniCluster S7-2 に関連する内容として、Oracle Identity and Access Management は、Oracle MiniCluster プラットフォームで実行するアプリケーションとサービスの ID とアクセスを管理する単一ポイントとしてだけでなく、その管理に使用される仮想アシスタント・コンソールおよびサービスの単一ポイントとしても使用できます。

Oracle Key Manager

Oracle Key Manager は、保管中の情報を保護するために使用される暗号化鍵を容易に管理および監視するために設計された、包括的な鍵管理システム（KMS）です。Oracle Key Manager は、スケーラビリティと可用性の高いアーキテクチャを使ったエンタープライズ・クラスの環境をサポートしており、数千台のデバイスと数百万個の鍵を管理できます。Oracle Key Manager は堅牢なオペレーティング環境で動作し、強力なアクセス制御とロール分離を実施して鍵の管理および監視操作を行い、オプションでオラクルの Sun Crypto Accelerator 6000 PCIe カード（FIPS 140-2 Level 3 レベルのハードウェア・セキュア・モジュール）に鍵をセキュアに格納します。

Oracle MiniCluster S7-2 に関連する内容として、Oracle Key Manager では、透過的データ暗号化による Oracle Database の暗号化、および暗号化された ZFS ファイル・システムで使用される暗号化鍵へのアクセスを認可、保護、管理できます。

一般的な推奨事項と考慮事項

Oracle MiniCluster S7-2 プラットフォームには階層化された高機能なセキュリティ制御のコレクションが統合されており、組織独自のポリシーや要件に合わせて調整できます。これらの機能を利用し、既存の IT セキュリティ・アーキテクチャに合わせて拡張する最適な方法を、組織が理解することが重要です。また、組織とクラウド・サービス・プロバイダは、効果的な IT セキュリティを実現するには、セキュリティ・ポリシーによって整理され、堅牢なリスク管理およびガバナンスの実践によって信頼性を確認された人、プロセス、テクノロジーの統合が必要であるということを認識しておく必要があります。ここでは、組織とクラウド・サービス・プロバイダが知っておくべき一般的な推奨事項と考慮事項を、アーキテクチャ、デプロイメント、運用の面から説明します。

アーキテクチャ

次に示すアーキテクチャのベスト・プラクティスをお勧めします。

» 組織とクラウド・サービス・プロバイダは、Oracle MiniCluster S7-2 プラットフォームのコンポーネントとデプロイ済みサービスを既存の ID およびアクセス管理アーキテクチャと統合することで、ID およびアクセス管理に対して統一的にアプローチして、シングル・サインオン（SSO）と ID フェデレーションの要件に対処する必要があります。特に、Oracle Solaris オペレーティング・システムと Oracle Database は一連のオープンな標準プロトコルをサポートしているため、既存の ID およびアクセス管理のデプロイメントといっそう容易に統合できます。

» 組織とクラウド・サービス・プロバイダは、Intrusion Prevention System（IPS：侵入防止システム）を使用して、Oracle MiniCluster S7-2 プラットフォームを出入りするネットワーク・トラフィックを監視することを検討する必要があります。このようなシステムによって、疑わしい通信、攻撃の可能性があるパターン、および不正アクセスの試行を特定できます。Oracle MiniCluster S7-2 プラットフォーム内の可視性を高めるには、ホストベースの侵入検出および防止システムの使用を検討することをお勧めします。ホストベースのシステムは、Oracle Solaris オペレーティング・システムと Oracle Database のファイングレイン監査機能を利用することで、不適切なアクションや不正なアクティビティを検出できる可能性が高くなります。

» 同様に、組織とクラウド・サービス・プロバイダは、Oracle MiniCluster S7-2 プラットフォームを出入りする情報を保護できる、アプリケーションおよびネットワークのファイアウォールの使用を検討することもお勧めします。ネットワーク・ポートのフィルタリングが、システムやサービスに対する不正アクセスの最初の防衛線になる場合が多くあります。ホストベースの侵入検出サービスについては、Oracle MiniCluster S7-2 プラットフォームのコンポーネント間の通信をよりきめ細かく制御したい場合は、専用 VLAN の使用と IPSec チャネルの有効化によるネットワーク・レベルのセグメント化を検討することをお勧めします。

» また、組織とクラウド・サービス・プロバイダは、一元的な監査およびログのリポジトリによってセキュリティ関連の情報を集約し、相互の関連付け、分析、レポートの改善を検討する必要があります。最新のセキュリティ・イベントおよびインシデント管理（SIEM）システムは、ネットワーク・デバイス、オペレーティング・システム、データベース、アプリケーションからのデータ収集に使用できる一連のプロトコルをサポートしています。Oracle MiniCluster S7-2 と SIEM システムを統合し、監査情報を一元的な（かつ保護された）場所に収集して保存することで、組織はセキュリティ・インシデント対処プロセスおよびフォレンジック対処プロセスの品質と有効性を向上させることができます。このような分析に必要な情報は、不正侵入されるおそれのあるシステムやアプリケーションとは別に、安全に保管する必要があります。また、このようなアプローチの効果を最大限にするため、組織とクラウド・サービス・プロバイダが、ネットワーク・タイム・プロトコル・サービスを利用してデバイス、システム、ソフトウェア全体の時刻を合わせることも必要です。

デプロイメント

次に示すデプロイメントのベスト・プラクティスをお勧めします。

» 強力な認証とネットワーク通信の暗号化をサポートするプロトコルを利用することを強くお勧めします。これで通信の機密性と整合性を保護できます。また、Oracle MiniCluster S7-2 プラットフォームにデプロイされているサービスと通信する場合や、その管理インタフェースを使用してプラットフォームを管理する場合にも重要です。組織は、組織のポリシーに従った暗号化プロトコルと鍵の長さを使用するように、管理サービスと運用サービスを構成する必要があります。Oracle MiniCluster S7-2 プラットフォームの暗号化サービスには、ハードウェア・アクセラレーションという利点もあります。この機能によって、セキュリティだけでなく全体のパフォーマンスも向上します。

» Oracle MiniCluster S7-2 プラットフォームに事前統合されているセキュリティ制御の多くは、セキュアなデプロイメントのためにデフォルトで構成されていますが、組織とクラウド・サービス・プロバイダが独自の強化されたセキュリティ構成基準を採用している場合も多くあります。オラクルは自社製品のセキュリティ・ガイドを作成しており、Oracle MiniCluster S7-2 プラットフォーム関連の内容は、このドキュメントの末尾にある参考資料の項に含まれています。組織は、Oracle MiniCluster S7-2 のコンポーネントのセキュリティ構成を変更する前に、この情報を確認することが重要です。特に、組織の既存基準で改善できる点と、サポート上の問題から、特定のコンポーネントの変更可能な内容がどのように制限される可能性があるかを特定することが重要です。

» Oracle MiniCluster S7-2 プラットフォームに含まれるいくつかの製品には、デフォルトの管理パスワードが付属しています。組織とクラウド・サービス・プロバイダはできるだけ早く、これらのデフォルト・パスワードを、認可された管理者のみが知る値に変更することを強くお勧めします。

運用

次に示す運用上のベスト・プラクティスをお勧めします。

» セキュアなデプロイメントで使用するために Oracle MiniCluster S7-2 プラットフォームを構成することは比較的簡単ですが、組織は、プラットフォームおよびデプロイされるサービスのライフサイクル全体にわたって、セキュリティの確保が必要であることを理解しておくことが重要です。また、不正な改変や構成のずれ、および未適用のセキュリティ・パッチの検出用ツールを利用することもお勧めします。Oracle Enterprise Manager の一連のツールは、ハードウェアからデプロイされるアプリケーションやサービスにわたって、組織がこのような運用上の問題を管理するための統合ソリューションとなります。

» また、組織とクラウド・サービス・プロバイダは、Oracle MiniCluster S7-2 プラットフォームとデプロイされるサービスにアクセスするユーザーと管理者を定期的に評価し、アクセスと権限のレベルが適切であるかどうかを検証することをお勧めします。レビューを行わないと、個人に付与されるアクセス権のレベルは、時間の経過とともに際限なく拡大しがちです。（運用上および管理上の両方のアクセスに関する）アクセス権を調査し、各ユーザーのアクセス・レベルがそのロールと責務に対して適切であることを確認することをお勧めします。

結論

総括すると、Oracle MiniCluster S7-2 プラットフォームで使用できる一連の豊富なセキュリティ制御とセキュリティ機能によって、組織とクラウド・サービス・プロバイダがアプリケーションとデータベース・サービスをデプロイできる総体的なセキュリティ・アーキテクチャを提供します。ただし、より重要なのは、Oracle MiniCluster S7-2 プラットフォームのコンポーネントの緊密な統合と、セキュリティ構成および運用の柔軟性のレベルとのバランスが保たれ、組織が、組織のポリシーに基づいてプラットフォームのセキュリティ対策のカスタマイズもできることです。Oracle MiniCluster S7-2 は、堅牢ながらも柔軟なセキュリティ・アーキテクチャを備えており、アプリケーションとデータベースの統合、多層エンタープライズ・アプリケーションの運用、または専用のコンピューティング・クラウド・サービスの提供を行う組織に最適なプラットフォームです。

Oracle MiniCluster S7-2 プラットフォームには、オラクルの SPARC S7 ベースのサーバー、Oracle Solaris、Oracle Database、および Oracle Software Security Assurance に準拠したサード・パーティのソース・コードが統合されています。Oracle Software Security Assurance は、製品開発ライフサイクルのあらゆるフェーズを網羅する、既知の攻撃経路と脆弱性に対する包括的なセキュリティ・テストを含むプログラムです。Oracle Software Security Assurance は、製品の設計、構築、テスト、保守にセキュリティを組み込むオラクルの手法です。オラクルの目標は、オラクルの製品、およびオラクルの製品を利用するお客様のシステムを可能な限りセキュアな状態に維持することです。

参考資料

» Oracle MiniCluster S7-2 エンジニアド・システムの技術概要
http://www.oracle.com/jp/engineered-systems/supercluster/minicluster-s7-2/overview/index.html

製品のセキュリティ・ガイド

» オラクルの SPARC および Netra SPARC S7-2 シリーズサーバー・セキュリティガイド
https://docs.oracle.com/cd/E76977_01/html/E77180/index.html

» Oracle Integrated Lights Out Manager のドキュメント
https://docs.oracle.com/cd/E40703_01/

Oracle Solarisのセキュリティ

» Oracle Solaris 11 セキュリティと強化ガイドライン
https://docs.oracle.com/cd/E62101_01/html/E62714/

セキュリティ関連のホワイト・ペーパーとドキュメント

Oracle Solaris 11オペレーティング・システム

» Oracle Solaris 11 Network Virtualization and Network Resource Management
http://www.oracle.com/technetwork/server-storage/solaris11/documentation/o11-137-s11-net-virt-mgmt-525114.pdf

» Oracle Solaris Resource Manager を使用した効率的なリソース管理
http://www.oracle.com/technetwork/jp/articles/servers-storage-admin/o11-055-solaris-rm-419384-ja.pdf

Oracle Database

» Oracle Database 12c のセキュリティとコンプライアンス
http://www.oracle.com/technetwork/jp/database/security/security-compliance-wp-12c-1896112-ja.pdf

» Oracle Defense-in-Depth Guide
http://www.oracle.com/technetwork/jp/database/security/sol-home-086269-ja.html

» Oracle Database 11g Release 2 による費用効率に優れたセキュリティおよびコンプライアンス
http://www.oracle.com/technetwork/jp/content/owp-security-database-11gr2-1-129368-ja.pdf

» Oracle Database 11g Release 2 と Oracle Advanced Security
http://www.oracle.com/technetwork/jp/content/owp-security-advanced-security-11gr-1-131000-ja.pdf

» Oracle Advanced Security Transparent Data Encryption Best Practices
http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf

» Oracle Database 11g Release 2 の Oracle Database Vault
http://www.oracle.com/technetwork/jp/content/owp-security-database-vault-11gr2-130401-ja.pdf

» Oracle Database 11g Release 2 の Oracle Label Security
http://www.oracle.com/technetwork/jp/topics/security/owp-security-label-security-11gr2-326442-ja.pdf

» Effective Resource Management Using Oracle Database Resource Manager
http://www.oracle.com/technetwork/articles/servers-storage-admin/o11-056-oracledb-rm-419380.pdf

Oracle Middleware

» High Performance Security for Oracle WebLogic Applications Using Oracle's SPARC T5 and SPARC M5 servers
http://www.oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf

» Securing Oracle E-Business Suite Applications Using Oracle Solaris 11 on SPARC T5 and SPARC M5 Servers
http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-044-t5-ebssecurity-1964593.pdf

» High-Performance Security for Oracle WebLogic Applications Using Oracle's SPARC T5 and SPARC M5 Servers
http://www.oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf

» High-Performance Security for SOA and XML Web Services Using Oracle Web Services Manager and Oracle's SPARC Enterprise T-Series Servers
http://www.oracle.com/technetwork/articles/systems-hardware-architecture/hi-perf-soa-xml-svcs-172821.pdf

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

海外からのお問い合わせ窓口
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

Oracle MiniCluster S7-2 プラットフォームのセキュリティ 2016 年 10 月
著者：Ramesh Nagappan
共著者：Sujeet Vasudevan、Ramin Moazeni、Vamsee Kasavajhala