Oracle MiniCluster S7-2 セキュリティーガイド

Part No: E78267-02
2016 年 10 月

Part No: E78267-02

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方法

- **概要** – Oracle MiniCluster S7-2 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/minicluster-s7-2/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 MiniCluster S7-2 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、次のトピックについて説明します。

最低限必要なセキュリティータスク

MiniCluster は、エンジニアドシステムとして、デフォルトで出荷時から高度にセキュアなシステムとして構成され、次のセキュリティー機能を備えています。

- すべての仮想マシン (VM) 用の完全に自動化されたセキュリティーコントロールで事前構成されています。
- 暗号化がデフォルトで有効にされ、保存時と転送時のセキュアなデータを確保します。
- VM は、ホストベースのファイアウォールによって、強化された最小の OS で自動的に構成されます。
- アクセス制御では、最小の権限による役割ベースのアクセスを必要とします。
- すべての VM で、暗号化された ZFS ストレージを使用します。
- PKCS#11 および FIPS のサポートを使用した、集中管理された鍵管理機能があります。
- システムには、集中管理された監査ログによる包括的な監査ポリシーが含まれています。
- システムとすべての VM が、PCI-DSS、CIS 相当、または DISA-STIG セキュリティープロファイルのいずれかに対して構成されます。注記 – 後者のプロファイル

は現在確認中です。DISA-STIG プロファイルは、非本番環境で実験用にのみ使用してください。

- 簡単に実行できるコンプライアンスベンチマークをサポートする、簡単に表示できるコンプライアンスダッシュボードがあります。

MiniCluster のインストール直後に、セキュリティー管理者には次の 2 つの必須タスクがあります。

- Oracle ILOM root パスワードを変更します。27 ページの「Oracle ILOM root のデフォルトパスワードの変更」を参照してください

それ以外に、このガイドのセキュリティー情報を確認して、MiniCluster のセキュリティー機能を理解し、確認します。

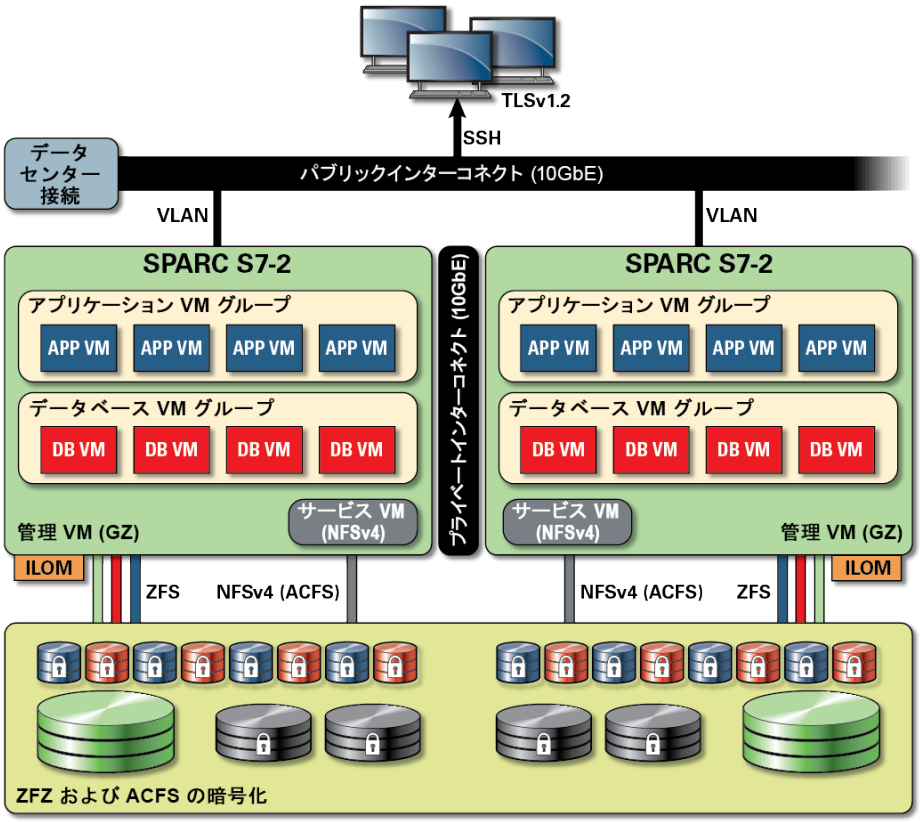
コアのセキュリティーの原則

MiniCluster はアプリケーションおよびデータベース統合のためのセキュアなクラウドインフラストラクチャープラットフォームであり、サービス (IaaS) ベースのクラウドサービスとして、専用のコンピュートインフラストラクチャーを提供する場合に適しています。多目的エンジニアドシステムとして構築され、Oracle の SPARC S7 プロセッサの計算能力、SPARC Solaris の効率的な仮想化機能、専用ストレージに統合された Oracle データベースの最適化されたデータベースパフォーマンスが組み合わされています。さらに、10 GbE ネットワークが採用されているため、クライアントが MiniCluster 上で実行されているサービスにアクセスできます。最後に、別の 10 GbE ネットワークによって、SPARC S7 サーバー上の仮想マシン環境とホストされているアプリケーション間のすべての通信が通る導管を提供します。

SPARC S7 プロセッサは、常時オンのハードウェア支援暗号化機能を備えており、MiniCluster でホストされるエンティティーが、保存時、使用時、および転送時に、高性能のデータ保護によって、それらの情報を保護するために役立ちます。さらに、プロセッサはシリコンセキュアメモリー機能も備えており、メモリーデータの破損やメモリースクレイピングに関連する攻撃を検出して防御することにより、アプリケーションデータの整合性を確保します。

デフォルトで、MiniCluster は、絶対に必要というわけではないサービス、ポート、プロトコルを無効にし、公開されたサービスを、信頼できる接続のみを受け入れるように構成して、システムの攻撃対象領域を減らす 250 以上のすぐ使用できるセキュリティーコントロールで事前構成されています。

システムは多様な構成および配備オプションをサポートしています。この図は、Oracle Database とアプリケーションのワークロードを統合する一般的な配備を示しています。



セキュアな仮想マシン

MiniCluster コンピュートノード内のセキュリティーは複数のレベルで提供されます。コンピュートノードのセキュアな検証済みのブート、分離された仮想マシンとして実行する強化された最小限の OS から始めて、承認されていないユーザーやシステムによってワークロードとデータがアクセスされないように防ぎます。MiniCluster では、Oracle Solaris Zones テクノロジを仮想マシンとして使用して、分離されたコンピュート環境をホストし、同じオペレーティングシステムで実行されているさまざまな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、ほかの仮想マシンで発生した意図しないまたは悪意のあるアクティビティーからそれらを保護します。同じカーネル上で実行していても、各 Solaris ゾーンには、それぞれ固有の識別情報、およびリソース、名前空間、プロセス分離があります。基本的に、Solaris ゾーンは、Type 1 ハイパーバイザーで実行している従来の仮想マシンよりも小さな CPU およびメモリーフットプリントで強力な分離と柔軟なリソースコントロールを含む組み込みの仮想化を提供します。各仮想マシンは、インストールプロセスで自動的に適用される包括的な一連のセキュリティーコントロールとポリシーを定義するセキュリティープロ

ファイルで構成されます。ZFS プールおよびデータセットの使用により、ストレージを仮想マシンのさらに細かいユニットに切り分け、分離して、それぞれ独自のセキュリティーポリシーを持つことができます。

アクセス制御

アプリケーションデータ、ワークロード、そのすべてが実行される基盤のインフラストラクチャーを保護するために、MiniCluster はユーザーと管理者の両方に包括的ながら柔軟なアクセス制御機能を提供します。MiniCluster は、システムサービスにアクセスするユーザーとアプリケーションに対するさまざまなアクセス制御方法として Oracle Solaris を利用します。従来のユーザー名とパスワードのペアも引き続き広く使用されていますが、Oracle Solaris の PAM (プラガブル認証モジュール) アーキテクチャーを使用して、より強力な認証方法を簡単に統合でき、LDAP、Kerberos、および公開鍵認証を使用できます。MiniCluster コンピュート環境は、包括的な役割ベースのアクセス制御 (RBAC) 機能に基づいて構築されているため、組織は必要に応じて、ユーザーおよび管理アクセスを委任する柔軟性が得られます。Oracle Solaris の RBAC 機能では、全能のスーパーユーザーの概念をなくすことで責務の分離を可能にし、ユーザーや管理者に権限を割り当てるためにまとめて使われる管理役割、承認、きめ細かい権限、および権利プロファイルの概念をサポートします。RBAC は、Oracle Solaris Service Management Facility (SMF) や仮想マシンを含むほかのコア Oracle Solaris サービスに統合され、すべてのオペレーティングシステムレベルのアクセス制御ニーズをサポートする一貫性のあるアーキテクチャーを提供します。MiniCluster はアクセス制御アーキテクチャーの基盤として Oracle Solaris の RBAC 機能を利用することで、組織が中央の認証局からオペレーティングシステムと仮想化管理アクセスを管理、制御、監査できるようにしています。すべてのクリティカルな操作は、多人数承認ワークフローによってサポートされている職務分掌の原則を使用して実行されます。セキュリティーが重要なすべての操作は複数のユーザーが承認する必要があります。これらの機能をまとめて使用して、ユーザーの識別情報およびクリティカルなビジネス操作の処理を高度に保証できます。

MiniCluster システムのすべてのデバイスが、アーキテクチャー上の方法 (ネットワーク分離など) を使用するか、またはパケットフィルタリングやアクセス制御リストを使用して、物理デバイスと仮想デバイス間に加え、システムによって公開されるサービスへの通信を制限することによって、サービスへのネットワークアクセスを制限する機能を備えます。MiniCluster は、インバウンドネットワークトラフィックを受け入れるために Secure Shell (SSH) 以外のネットワークサービスを有効にしないことで、デフォルトでセキュアな状態を配備します。ほかの有効にされているネットワークサービスは、Oracle Solaris オペレーティングシステム (仮想マシンまたはゾーン) 内で要求を内部で待機します。これにより、すべてのネットワークサービスはデフォルトで無効にされるか、ローカルシステム通信のみを待機するように設定されます。組織は要件に基づいてこの構成を自由にカスタマイズできます。MiniCluster は、Oracle Solaris IP フィルタ機能を使用して、ネットワークおよびトランスポート層 (ステートフル) パケットフィルタリングが事前に構成されています。IP フィルタは、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の幅広いホストベースのネットワーク機能を提供します。

データ保護

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、MiniCluster の SPARC S7 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シリコンセキュアメモリーテクノロジも採用しています。

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。さらにオペレーティングシステムレベルでは、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、MiniCluster によって使用される Oracle Solaris オペレーティングシステムおよび 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シリコンセキュアメモリー機能を使用でき、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。MiniCluster はパブリックおよびプライベートネットワーク上を流れる VM 固有および VM 間通信の機密性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) の使用をサポートしています。

MiniCluster では、ZFS データセット暗号化で集中管理された Oracle Solaris PKCS#11 キーストアを利用してラッピング鍵を安全に保護します。Oracle Solaris PKCS #11 キーストアを使用すると、すべての暗号化操作に対して、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、Oracle は、ZFS データセットの暗号化、Oracle Database Transparent Data Encryption (TDE)、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。データベース仮想マシンは、仮想マシン上に存在するデータベース間でウォレットを共有できるように、Oracle Solaris PKCS #11 キーストアを利用するか、または ACFS 共有ストレージ上にディレクトリを作成して、共有ウォレットアプローチを使用できます。各コンピュートノードで共有された集中管理型キーストアを使用すると、鍵がクラスタ内の各ノード間で同期されるため、システムは Oracle Grid インフラストラクチャーベースのクラ

スタ化データベースアーキテクチャーで Oracle TDE の鍵を適切に管理、保守、交換できます。MiniCluster は、その ZFS データセット (ファイルシステム/ZVOL) レベルで暗号化ポリシーと鍵管理を使用して、鍵の破棄による確実な削除を提供することで、仮想マシンと関連付けられた ZFS データセットのセキュアな削除も可能にします。

監査とコンプライアンス

MiniCluster 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。各仮想マシン (非大域ゾーン) は、各 MiniCluster (大域ゾーン) 監査ストア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、個々の仮想マシンが監査ポリシー、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、仮想マシンでの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。仮想マシンを使用するように構成されている場合、各仮想マシンの監査レコードを大域ゾーンに保存して、それらを改ざんから保護できます。大域ゾーンでは、ネイティブの Oracle Solaris 監査機能も利用して、仮想化イベントおよび MiniCluster 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。

MiniCluster は、仮想マシンに存在する Oracle Solaris 実行時環境のコンプライアンスを評価し、レポートするツールを提供します。コンプライアンスユーティリティーは、SCAP (Security Content Automation Protocol) 実装に基づいています。MiniCluster では 2 つのセキュリティー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。

- **デフォルトのセキュリティープロファイル** – CIS 相当プロファイル (Center of Internet Security ベンチマークに基づく) ですが、HIPAA、FISMA、SOX などの規制に規定されたセキュリティーコンプライアンス要件とより一致しています。
- **PCI-DSS プロファイル** – Payment Card Industry Data Security Standard
- **DISA STIG プロファイル** – Defense Information System Agency - Security Technical Implementation Guidance Standard。このプロファイルはデフォルトのセキュリティープロファイルに基づいて構築されており、追加の 75 個のセキュリティー制御、FIPS-140-2 暗号化、および S パスワードを設定するためのサポートが導入されています。注記 – このプロファイルは現在確認中です。このプロファイルは、非本番環境で実験用にのみ使用してください。

MiniCluster 管理者は、オンデマンドでコンプライアンスベンチマークを実行して、環境のコンプライアンスと異常を確認します。これらのプロファイリングツールは、セキュリティーコントロールを業界標準によって義務付けられたコンプライアンス要件にマップします。関連付けられたコンプライアンスレポートによって、監査時間とコストを大幅に削減できます。

MiniCluster v.1.1.18 の時点で、システムには次の監査機能が含まれています。

- **監査者役割** – この役割を MCMU ユーザーに対して指定すると、ユーザーは MCMU BUI で監査者の確認ページにアクセスできます。ユーザーは、その他の MiniCluster 管理タスクを表示したり実行したりはできません。
- **「Auditor Review」ページ** – 監査者役割を持つユーザーのみが表示できる特殊な MCMU BUI ページです。このページでは、監査プールステータスにアクセスでき、ゾーンごとにすべてのユーザーアクティビティーの監査レコードを生成できます。41 ページの「監査レポートの生成」を参照してください。

セキュリティー構成について

これらのトピックでは、MiniCluster のセキュリティーコントロールについて説明します。

組み込みセキュリティープロファイル

MiniCluster の初期化は MCMU BUI または CLI を使用して実行します。初期化時に、MCMU はインストーラがこれらのセキュリティープロファイルのいずれかを選択することを必要とします。

- **デフォルトのセキュリティープロファイル** – CIS (Center for Internet Security) およびセキュリティー技術導入ガイド(STIG) の評価で示されたベンチマークに匹敵する要件を満たします。
- **PCI-DSS プロファイル** – Payment Card Industry Security Standards Council によって定義された Payment Card Industry Data Security Standard (PCI DSS) 標準に準拠します。
- **DISA STIG プロファイル** – Defense Information System Agency - Security Technical Implementation Guidance Standard。このプロファイルはデフォルトのセキュリティープロファイルに基づいて構築されており、追加の 75 個のセキュリティー制御、FIPS-140-2 暗号化、および eeprom パスワードを設定するためのサポートが導入されています。注記 – このプロファイルは現在確認中です。このプロファイルは、非本番環境で実験用にのみ使用してください。

選択されたポリシーに基づいて、MCMU は 250 を超えるセキュリティーコントロールによって、大域ゾーンと非大域ゾーンを構成します。

初期化後、仮想マシンが作成されると、MCMU は仮想マシンごとに、いずれかのセキュリティープロファイルの選択を必要とします。セキュリティー要件に基づいて、仮想マシン上にセキュリティープロファイルを混在させることができます。

▼ VM セキュリティープロファイルの確認 (CLI)

ゾーンおよび仮想マシンに構成されているセキュリティープロファイルを確認または識別するには、次の手順を使用します。

注記 - この手順を実行するには、`root` 役割を持つユーザーアカウントでシステムにアクセスする必要があります。

注記 - 大域ゾーンに割り当てられたセキュリティープロファイルを識別するには、MCMU BUI で、「システム設定」->「ユーザー入力サマリー」を表示します。ページ下部にセキュリティープロファイルが表示されます。

---

1. **`mcinstall` として、大域ゾーンにログインします。**

   システムにアクセスする方法については、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

2. **`root` 役割になります。**

   例:

   ```
   # su root
   ```

3. **問題の VM のログファイル名を確認します。**

   この例では、VM ごとに 1 つのログファイルがあります。

   ```
   # cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
   # ls
   verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
   verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
   verify_dbvmg1-zone-1-mc4-n2.log   verify_dbvmg1-zone-4-mc4-n1.log
   verify_dbvmg1-zone-2-mc4-n1.log   verify_dbvmg1-zone-4-mc4-n2.log
   verify_dbvmg1-zone-2-mc4-n2.log
   #
   ```

4. **検証ログファイルを表示します。**

   ログファイルの最後の行を表示します。`(PCI-DSS)` が表示された場合、VM のセキュリティープロファイルは PCI-DSS です。プロファイルが一覧表示されない場合は、VM のセキュリティープロファイルは CIS 相当です。

   - PCI-DSS プロファイルでの VM の最後の 22 行の例:

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log

     (PCI-DSS) Checking /etc/cron.d/at.allow:
     Passed/Configured

     (PCI-DSS) Checking audit configuration (user audit flags):
     Passed/Configured
     ```

```
(PCI-DSS) Checking audit configuration (non-attributable audit flags):
Passed/Configured

(PCI-DSS) Checking audit configuration (audit_binfile plugin):
Passed/Configured

(PCI-DSS) Checking audit flags on root and tadmin roles:
Passed/Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

- CIS 相当プロファイルでの VM の最後の 22 行の例:

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
Checking if NDP routing daemon is disabled:
Passed/Configured

Checking if r-protocol services are disabled:
Passed/Configured

Checking if rpc/bind is enabled and configured correctly:
Passed/Configured

Checking if NFS v2/v3 is disabled:
Passed/Configured

Checking if GDM is enabled:
Failed/Not Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

データの保護

これらのトピックでは、MiniCluster のデータ保護テクノロジについて説明します。

ZFS データセット暗号化によるデータ保護

MiniCluster では、ZFS データセット暗号化を使用して、保存時のデータ保護が自動的に構成されます。暗号化は次のように構成されます。

- ルートおよびスワップファイルシステムを含め、すべての ZFS データセットが仮想マシンで暗号化されます。
- ルートおよびスワップファイルシステムを除き、すべての ZFS データセットが大域ゾーンで暗号化されます。

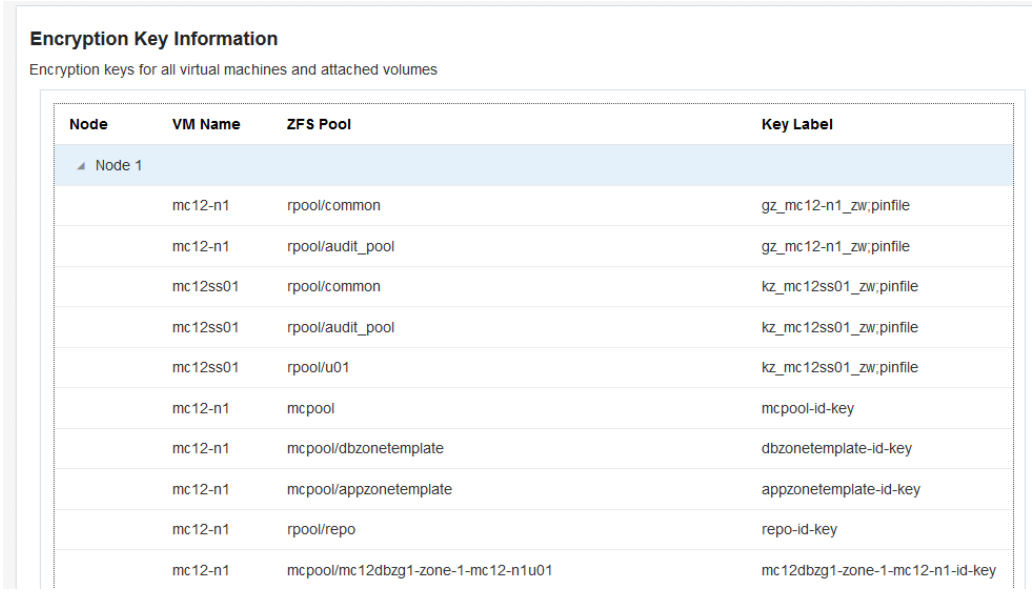
暗号化構成を確認するには、暗号化鍵を表示します。21 ページの「ZFS データセット暗号化鍵を表示する (BUI)」を参照してください。

▼ ZFS データセット暗号化鍵を表示する (BUI)

暗号化鍵の詳細を表示するには、次の手順を使用します。

1. **MCMU BUI にアクセスします。**
   MCMU BUI にアクセスする方法の詳細については、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。
2. **ナビゲーションパネルで、「システム設定」->「セキュリティー」を選択します。**

ノードをクリックして詳細を表示します。



Encryption Key Information

Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
◢ Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw;pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw;pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw;pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

Secure Shell サービス

MiniCluster では、MiniCluster コンピュートノード (大域ゾーン) および仮想マシンインスタンス (非大域ゾーン) にセキュアにログインできるように、SSH ネットワークプロトコルの使用が必要になります。

ユーザーがはじめて SSH を使用してログインすると、システムは自動的にユーザーの新しい SSH 鍵ペアを生成します。

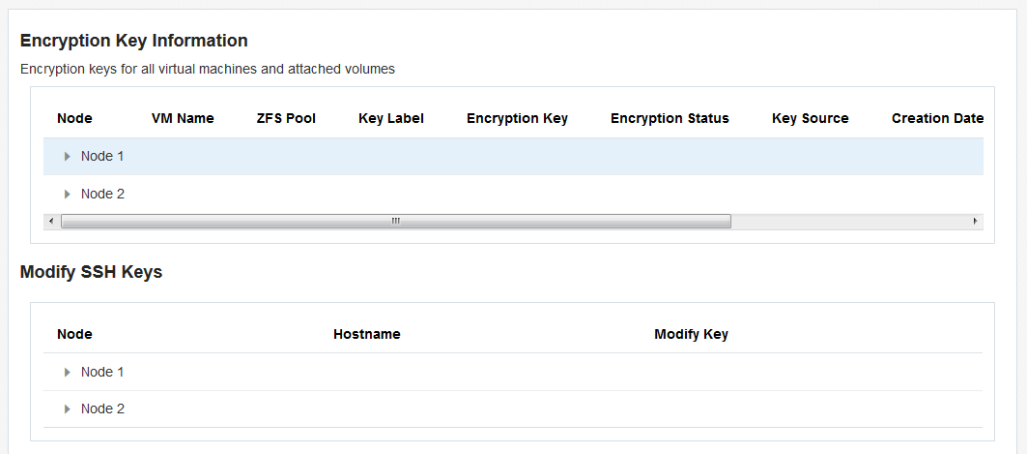
▼ SSH 鍵の変更 (BUI)

これらの構成のいずれかでゾーンまたは VM の SSH 鍵を変更するには、次の手順を使用します。

- 新しい鍵を挿入してパスワードなしの SSH を承認する - VM ユーザー名、VM マシン名、RSA 公開鍵を入力する必要があります。
- VM 用の新しい鍵を自動生成する

注記 - MCMU CLI を使用してこの手順を実行するには、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

1. **MCMU BUI にアクセスします。**
2. **ナビゲーションパネルで、「システム設定」->「セキュリティー」を選択します。**



3. **「SSH 鍵の変更」パネルで、表示を展開するノードをクリックします。**

4. **変更する予定がある VM については、「選択」をクリックします。**

5. **ドロップダウンメニューからオプションを選択して、「次へ」をクリックします。**
   選択肢は、次のとおりです。
   - パスワードなしの SSH を承認するための新しい鍵の挿入
   - マシン用の新しい鍵の自動生成
6. **「次へ」をクリックします。**
7. **パスワードなしの SSH を承認するように選択した場合は、この情報を入力してから、「次へ」をクリックします。**
   - マシンのユーザー名
   - マシンのホスト名
   - マシンの RSA 公開鍵
8. **「SSH の設定」をクリックします。**
   変更が適用されます。

IPsec によるセキュアな通信

ネットワーク上を流れるゾーン間 IP ベース通信および NFS トラフィックの機密性と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) の使用が推奨されます。IPsec は、ネットワークレベルのピア認証、データの起点の認証、データ機密性、データ整合性、およびリプレイ保護をサポートしているために推奨されます。Oracle MiniCluster プラットフォームで使用すると、IPsec と IKE は自動的にハードウェア支援の暗号化アクセラレーションを利用できるため、このネットワークチャネル上を流れる機密情報を保護するための暗号化の使用のパフォーマンスへの影響が最小化します。

▼ IPsec および IKE の構成

IPsec を構成する前に、通信ピア間で使用される特定のホスト名や IP アドレスが定義されている必要があります。

この手順の例では、10.1.1.1 および 10.1.1.2 の IP アドレスを使用して、1 つのテナントによって操作されている 2 つの Solaris 非大域ゾーンを指定しています。これらの 2 つのアドレス間の通信は IPsec を使用して保護されます。例は、IP アドレス 10.1.1.1 によって関連付けられた非大域ゾーンの観点からのものです。

次の手順を使用して、指定した (仮想マシン) 非大域ゾーンのペア間に IPsec と IKE を構成して使用します。

1. **IPsec セキュリティーポリシーを定義します。**
   通信ゾーンのペア間に適用するセキュリティーポリシーを定義します。
   この例では、10.1.1.1 と 10.1.1.2 間のすべてのネットワーク通信が暗号化されます。

   ```
   {laddr 10.1.1.1 raddr 10.1.1.2}
   ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
   ```

2. **ポリシーを `/etc/inet/ipsecinit.conf` ファイルに格納します。**

3. **IPsec ポリシーが構文的に正しいことを確認します。**
   例:

   ```
   # ipsecconf -c -f ipsecinit.conf
   ```

4. **Internet Key Exchange (IKE) サービスを構成します。**
   `/etc/inet/ike/config` ファイルにホストとアルゴリズム設定に続いてサービスを構成します。

   ```
   { label "ipsec"

   local_id_type ip

   remote_addr 10.1.1.2

   p1_xform { auth_method preshared oakley_group 5

   auth_alg sha256 encr_alg aes } }
   ```

5. **事前共有鍵を構成します。**
   IPsec を有効にする前に、互いに認証できるように、両方のピアノードで鍵材料を共有する必要があります。

   Oracle Solaris の IKE 実装は、事前共有鍵と証明書を含むさまざまな鍵のタイプをサポートしています。簡単にするため、この例では、`etc/inet/secret/ike.preshared` ファイルに格納されている事前共有鍵を使用します。ただし、強力な形式の認証を使用することを求めている組織では、そのようにします。

   /etc/inet/secret/ike.preshared ファイルを編集して、事前共有された鍵情報を入力します。例:

   ```
   {
   localidtype IP
   localid 10.1.1.1
   remoteid type IP
   key "This is an ASCII phrAz, use strOng p@sswords"
   }
   ```

6. **両方のピアで IPsec および IKE サービスを有効にします。**
   暗号化通信を可能にする前に、両方の通信ピアでサービスが有効にされている必要があります。

   例:

   ```
   # svcadm enable svc:/network/ipsec/policy:default
   ```

```
# svcadm enable svc:/network/ipsec/ike:default
```

アクセスの制御

次のトピックでは、MiniCluster で利用できるアクセス制御機能について説明します。

▼ Oracle ILOM root のデフォルトパスワードの変更

システムの出荷時には、両方のノードの Oracle ILOM root アカウントにデフォルトのパスワードが割り当てられています。これにより、予測可能な初期アクセスアカウントを使用してインストールプロセスを実行できます。最適なセキュリティーを確保するために、インストール後すぐにデフォルトのパスワードを変更してください。

1. **ノード 1 の Oracle ILOM に root としてログインします。**

   Oracle ILOM に接続するには、ssh コマンドを使用します。

   Oracle ILOM のホスト名を取得するには、ユーティリティー BUIで「システム設定」->「システム情報」の順に選択します。ホスト名は「ILOM」列の下に一覧表示されます。

   構文:

   ```
   % ssh root@node1_ILOM_hostname_or_IPaddress
   ```

   Oracle ILOM の root のデフォルトパスワード welcome1 を入力します。

2. **Oracle ILOM の `root` パスワードを変更します。**

```
-> set /SP/users/root password
Enter new password: *********
Enter new password again: ***********
```

3. **この手順を繰り返して、ノード 2 の Oracle ILOM の `root` パスワードを変更します。**

4. **Oracle Engineered Systems Hardware Manager を新しいパスワードに更新します。**

『Oracle MiniCluster S7-2 管理ガイド』 の 「コンポーネントパスワードを更新する」を参照してください。

▼ EEPROM パスワードの構成

それぞれの MiniCluster ノードには、OpenBoot PROM と呼ばれることもある EEPROM があります。これは、システムのブートを容易にする一部の構成パラメータとドライバを含む、低レベルのファームウェアです。デフォルトでは、EEPROM パスワード機能は無効になっています。

パスワード機能を有効にして、パスワードを設定するには、セキュアな環境でこの手順を使用してください。パスワードは自動的に有効になり、両方のノードに適用されます。

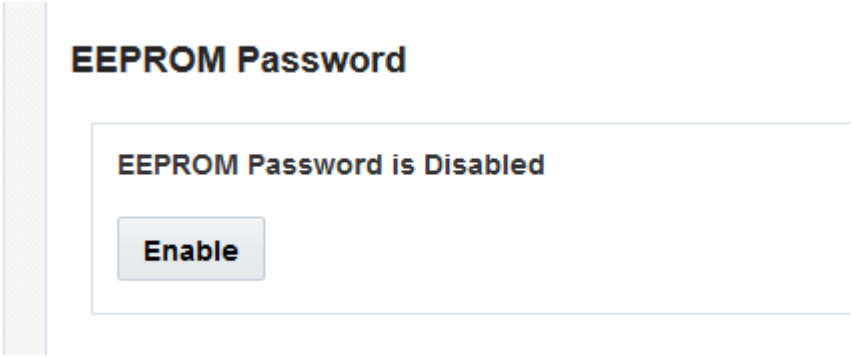
この手順は、パスワードが OpenBoot `ok` プロンプトで設定されるか、`eeprom` コマンドを使用して Oracle Solaris 内で設定される古い方法より優先されます。

注意 - パスワードを覚えておくことが重要です。パスワードを忘れた場合は、システムを再度ブート可能にするためにサポートサービスに電話する必要があります。

注記 - この手順では、MCMU BUI を使用してパスワードを設定する方法について説明します。または、`mcmu security -e` コマンドを使用することもできます。

1. **`mcinstall` などのプライマリ管理者として MCMU にログインします。**

2. **ナビゲーションパネルで、「システム設定」->「セキュリティー」を選択します**



3. **次のいずれかのアクションを実行します。**

   - パスワードを有効にして設定するには – 「有効」をクリックしてパスワードを 2 回入力し、「パスワードの設定」をクリックします。
   - この機能を無効にするには – 「無効」をクリックしてから、「確認」をクリックします。
   - 既存のパスワードを変更するには – パスワードを変更して、新しいパスワードを 2 回入力し、「更新」をクリックします。

ユーザープロビジョニング

MiniCluster のインストール時に、`mcinstall` という最初の MCMU ユーザーを作成して登録するよう求められます。ユーザーの電子メールアドレス、電話番号など、人口統計上の情報が収集されます。`mcinstall` ユーザーは最初のプライマリ管理者アカウントです。ユーティリティーでは、はじめて `mcinstall` でログインしたとき、セキュリティープロファイルに関連付けられている Oracle Solaris パスワードポリシーに従って `mcinstall` の新しいパスワードを作成するよう求められます。

`mcinstall` ユーザーの登録時には、MCMU スーパーバイザとしての役割を果たす人物を指定する必要があります。スーパーバイザは名前と電子メールアドレスのみで識別されます。スーパーバイザは MCMU ユーザーではなく、ログイン資格情報はありません。

スーパーバイザと mcinstall ユーザーのどちらにも、実際の個人名および有効な電子メールアドレスが関連付けられます。

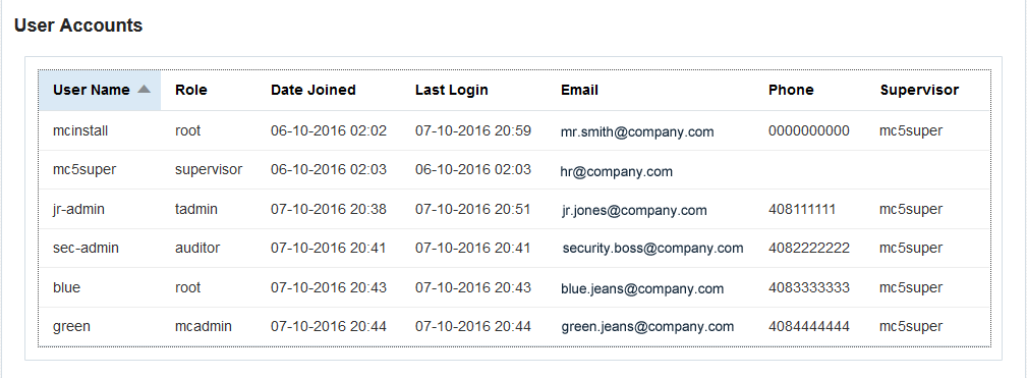
新しい MCMU ユーザーがプロビジョニングされるときは、各ユーザーアカウントにプライマリ管理者またはセカンダリ管理者の役割が割り当てられます (31 ページの「役割ベースのアクセス制御 」を参照)。新しいアカウントが有効になるには、その前に、`mcinstall` ユーザーとスーパーバイザの両方が、電子メールで受信した URL を通して新しいユーザーアカウントを承認する必要があります (30 ページの「MCMU ユーザーの承認プロセス」を参照)。ユーザーは最初のログイン時に、MCMU パスワードポリシーに準拠したパスワードを設定するよう強制されます。33 ページの「ユーザー認証およびパスワードポリシー」を参照してください。

MCMU ユーザーの承認プロセス

すべての MCMU ユーザーアカウントには、MCMU スーパーバイザとプライマリ管理者の 2 者による承認が必要です。プロセスは次のとおりです。

1. 見込みユーザー (またはその代理の MCMU 管理者) が MCMU 登録ページにアクセスし、次に示す必須の詳細を入力します。
   - MCMU ユーザー名
   - 電子メールアドレス
   - 氏名
   - 電話番号
   - MCMU 役割
2. MCMU から MCMU スーパーバイザおよびプライマリ管理者に、許可または拒否を求める電子メールが送信されます。電子メールには、MCMU の承認/拒否機能への URL が含まれ、一意の鍵識別子が含まれています。
3. スーパーバイザとプライマリ管理者の両方がアカウントを承認すると、ユーザーアカウントが有効になり、MCMU から新しいユーザーに、アカウントのアクティブ化を確認する電子メールが送信されます。ユーザーは、MCMU BUI または CLI からアクセスできる MCMU アカウントを受け取ります。ユーザーは、Oracle Solaris ユーザーアカウントも受け取ります。ユーザーが企業 LDAP 内に存在している場合で、MiniCluster に LDAP クライアントが構成されているときは、Oracle Solaris アカウントに LDAP のみを使用できます。

登録されたユーザーはすべて MCMU リポジトリに格納されます。MCMU 管理者は、MCMU の「システム設定」->「ユーザーアカウント」を表示して、ユーザーの役割やスーパーバイザなどを確認できます。例:



User Accounts

User Name ▲	Role	Date Joined	Last Login	Email	Phone	Supervisor
mcinstall	root	06-10-2016 02:02	07-10-2016 20:59	mr.smith@company.com	0000000000	mc5super
mc5super	supervisor	06-10-2016 02:03	06-10-2016 02:03	hr@company.com		
jr-admin	tadmin	07-10-2016 20:38	07-10-2016 20:51	jr.jones@company.com	408111111	mc5super
sec-admin	auditor	07-10-2016 20:41	07-10-2016 20:41	security.boss@company.com	4082222222	mc5super
blue	root	07-10-2016 20:43	07-10-2016 20:43	blue.jeans@company.com	4083333333	mc5super
green	mcadmin	07-10-2016 20:44	07-10-2016 20:44	green.jeans@company.com	4084444444	mc5super

このセクションの以降のトピックでは、これらのタスクを実行する方法について説明します。

役割ベースのアクセス制御

MiniCluster には `root` ユーザーは存在しません。代わりに、root 役割が、プライマリ管理者として登録されている MCMU ユーザーに割り当てられます。

MCMU ユーザーを作成するとき、次の役割の 1 つをユーザーに割り当てます。

- **プライマリ管理者 (`root` 役割)** – `root` 役割は、MiniCluster システム (その計算ノード、ネットワーク、データベース、ストレージをすべて含む) のプライマリ管理者の権利と権限を定義します。`root` 役割を持つユーザーは、すべてのインストール操作およびすべての重要な管理操作を制約なしで実行できます。プライマリ管理者は、操作を委任したり、新しいプライマリ管理者やセカンダリ管理者を含むユーザーの追加と削除を承認したりできます。ユーザーは、自分の資格情報を使用してログインする必要があります。実行されるすべてのアクションと操作は、役割識別子ではなくユーザー識別子に基づいて記録および監査されます。
- **セカンダリ管理者 (`mcadmin` 役割)** – この役割は、MiniCluster ドメインおよび非大域ゾーンのセカンダリ管理者の権利と権限を定義します。デフォルトでは、この役割は MCMU への読み取り専用アクセスのみを有効にします。実行されるすべてのアクションと操作は、役割識別子ではなくユーザー識別子に基づいて記録および監査されます。
- **テナント管理者 (`tadmin` 役割)** – この役割は、MiniCluster VM の管理者の権利と権限を定義します。この役割は、日常の管理操作に関与してアプリケーションのインストールと配備をサポートする VM 管理者の権利と権限を定義します。すべてのアクションは、役割識別子ではなくユーザー識別子に基づいて監査されます。
- **監査者 (`auditor` 役割)** – この役割を持つユーザーは、監査プールステータスを表示してユーザーアクティビティーのレポートを生成できる、MCMU BUI の「Audit Review」ページにのみアクセスできます。この役割を持つユーザーのみが「Audit

Review」ページにアクセスできます。監査者は、MCMU (「監査」ページを除く) にアクセスすることも、カーネルゾーンまたは VM にログインすることもできません。

ユーザーアカウント

MiniCluster には、次の表に示すユーザーアカウントが含まれています。

ユーザー	パスワード	役割	説明
`mcinstall`	パスワードはインストール時に構成されます。MCMU からリセットおよび変更できます。	`root`	インストールプロセスでは、MCMU プライマリ管理者として `mcinstall` を作成して、パスワードを作成する必要があります。このアカウントは、MCMU のプライマリ管理者になることを意図しています。 このユーザーアカウントは次のアクティビティーに使用されます。 ■ `installmc` の実行によってインストール時にシステムの初期化を実行する。 ■ MCMU BUI と `mcmu` CLI を使用して、VM を含むシステムを管理する。 ■ アプリケーション VM 上および大域ゾーンとカーネルゾーンで、`root` 役割になって (su で root に切り替えて) スーパーユーザー権限を取得する。
MCMU スーパーバイザ – インストール時に決定されたアカウント名	なし	なし	MiniCluster ソフトウェアでは、スーパーバイザユーザーはユーザー名と電子メールアドレスのみです。ログイン資格情報ではありません。このアカウントを使用して、MCMU ユーザーの承認プロセスを 2 段階にすることができます。 このユーザーは、新しい MCMU ユーザーが作成されるたびに電子メールを受け取ります。新しいユーザーのアカウントが有効になるには、スーパーバイザとプライマリ管理者がユーザーを承認する必要があります。 このアカウントを使用して、プライマリ管理者以外の人物をスーパーバイザとして割り当てることにより、MCMU ユーザーの承認プロセスを 2 段階にすることができます。
(オプション) テナント管理者 – ユーザーの登録時に決定されたアカウント名	最初のログイン時に決定されます。	`tadmin`	このユーザーは、VM でのみすべてのインストール後アクティビティーを実行できます。 このユーザーは、大域ゾーンまたはカーネルゾーンにアクセスすることも、MCMU BUI または CLI を実行することもできません。
(オプション) セカンダリ管理者 – ユーザーの登録時に決定されたアカウント名	最初のログイン時に決定されます。	`mcadmin`	MCMU ユーザーが作成され、セカンダリ管理者として割り当てられており、非大域ゾーンへの読み取り専用アクセスを持つ場合。
`oracle`	パスワードは `mcinstall` のパスワードと同じです。	`root`	このユーザーアカウントは次のアクティビティーに使用されます。

ユーザー	パスワード	役割	説明
			■ データベース VM への初期ログインアカウントとして使用して、データベース VM にデータベース、データ、およびほかのアカウントを必要に応じて構成する。 ■ データベース VM 上で、root 役割になって (su で root に切り替えて) スーパーユーザー権限を取得する。

最初のログインで使用されるデフォルトの MCMU パスワードは `welcome1` です。ユーザーは `welcome1` を一度入力すると、パスワードポリシーに準拠した新しいパスワードを作成するよう強制されます。33 ページの「ユーザー認証およびパスワードポリシー」を参照してください。

すべての MCMU ユーザーによって実行されるすべてのアクションが、ユーザーの識別子に基づいて記録されます。監査レポートの詳細は、39 ページの「監査およびコンプライアンスレポート」を参照してください。

注記 - MCMU ユーザーアカウントは、アプリケーションやデータベースの使用といったシステムの日常的使用には使用されません。これらのユーザーアカウントは、Oracle Solaris、アプリケーション、VM 上のデータベース、およびサイトのネームサービスを介して管理されます。

ユーザー認証およびパスワードポリシー

MiniCluster でプロビジョニングされたすべてのユーザーに役割が割り当てられ、セキュリティープロファイルによって厳密なパスワードポリシーとパスワード暗号化が適用されます。

デフォルトのセキュリティーポリシーでは、MCMU パスワードに次の要件が規定されます。

- 14 文字以上であること
- 数字を 1 つ以上含むこと
- 大文字の英字を 1 つ以上含むこと
- 前のパスワードと 3 文字以上異なること
- 10 個前までのパスワードと一致しないこと

すべてのユーザーは、自分のパスワードのみを使用して Oracle Solaris アカウントにログインします。

▼ Oracle Solaris ユーザーの役割の確認

1. **MiniCluster の大域ゾーンにログインし、root 役割になります。**

詳細は、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

2. **使用可能な役割のリストを確認します。**

```
# logins -r
```

3. **認証に必要なユーザーの役割とパスワードを確認します。**

```
# grep root /etc/user_attr
root::::audit_flags=lo\:no;type=role;roleauth=user
mcinstall::::auths=solaris.system.maintenance;roles=root
```

VM のセキュアな削除

MCMU プライマリ管理者だけが VM および VM グループを削除できます。VM コンポーネントが削除されると、対応する鍵が自動的に削除され、プライマリ管理者に電子メールが送信されます。

この機能を検証するには、VM コンポーネントを削除する前に、プライマリ管理者として MCMU BUI にログインし、暗号化鍵を表示します (「システム設定」->「セキュリティー」)。VM コンポーネントを削除してから、鍵を再度表示します。削除されたコンポーネントの VM および関連付けられた鍵ラベルが表示されなくなります。

▼ ホストベースのファイアウォール規則の確認

大域ゾーン、カーネルゾーン、および非大域ゾーンを含むすべてのコンピュート環境に、IPFilter ファイアウォールが自動的に構成されます。手動で行う必要はありません。

使用されている IPFilter を確認するには、次の手順を実行します。

1. **ノード 1 の大域ゾーンに `mcinstall` としてログインし、`root` 役割になります。**

   Oracle ILOM のログイン手順については、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **IPFilter 構成を確認します。**

   /etc/ipf/ipf.conf ファイル内の規則が、次の画面出力に一致していることを確認します。

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. **IPF サービスがオンラインになっていることを確認します。**

```
# svcs | grep svc:/network/ipfilter:default
online         22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:            in 0    out 0
 IPv6 packets:          in 0 out 0
 input packets:         blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:         blocked 0 passed 596143 nomatch 595516 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0  not fragmented 0
fragment reassembly(in):        bad v6 hdr 0     bad v6 ehdr 0  failed reassembly 0
fragment state(out):    kept 0  lost 0  not fragmented 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  0       (out):  0
IN Pullups succeeded:   0       failed: 3462
OUT Pullups succeeded:  0       failed: 0
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
IPF Ticks:      92894
Packet log flags set: (0)
        none
```

4. **ファイアウォール規則を変更せずにデータベースおよびアプリケーションにアクセスできることを確認します。**

▼ 検証済みブート環境の確認

Oracle Solaris 検証済みブートは、悪意を持って、または誤って変更されたクリティカルなブートおよびカーネルコンポーネントを取り込むリスクを軽減するマルウェア対策および整合性機能です。この機能は、出荷時に署名されているファームウェア、ブートシステム、およびカーネルの暗号化署名をチェックします。

デフォルトでは、MiniCluster 大域ゾーンには Oracle Solaris 検証済みブートが構成されています。システムに検証済みブートが構成されていることを確認するには、次の手順を実行します。

1. **いずれかのノードの Oracle ILOM にログインします。**

   Oracle ILOM のログイン手順については、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

2. **Oracle ILOM で検証済みブートの構成を確認します。**

   `boot_policy` が `warning` に設定されていることを確認します。

```
-> show /HOST/verified_boot

 /HOST/verified_boot
    Targets:
        system_certs
        user_certs

    Properties:
        boot_policy = warning

    Commands:
        cd
        show
```

3. **検証済みブートのポリシー設定を確認します。**

   `module_policy` が `enforce` に設定されていることを確認します。

```
-> show /HOST/verified_boot module_policy

  /HOST/verified_boot
    Properties:
        module_policy = enforce
```

4. **ホストコンソールを起動して大域ゾーンにアクセスします。**

   `mcinstall` としてログインします。

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

Serial console started.  To stop, type #.

Minicluster Setup successfully configured
mc4-n1 console login: mcinstall
Password: **************
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3    June 2016
```

```
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. **システムが検証済みブートの構成でブートした証拠を大域ゾーンで探します。**

   `messages` ファイルで、`NOTICE: Verified boot enabled; policy=warning` という文字列を探します。

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
 policy=warning
```

▼ 共有ストレージへのアクセスの制限

MiniCluster には、SSD と HDD の組み合わせを使用するストレージアレイが含まれています。VM に共有ストレージを提供するように HDD を構成できます。

MiniCluster には、大域ゾーンとカーネルゾーンにのみ適用される共有ストレージの分離を容易にする切り替えスイッチである、共有ストレージの分離機能が含まれています。これは、セキュリティーとコンプライアンス対応の VM グループ環境を、大域ゾーンとカーネルゾーンとのファイルの共有から分離するために役立ちます。これにより確実に、VM グループは NFS マウントに接続されなくなり、NFS サービスが無効になります。

非常にセキュアな環境では、データベース VM とアプリケーション VM に対して共有ストレージを有効にしないでください。共有ストレージが有効になっている場合、ファイルシステムは読み取り専用として VM からアクセス可能であることが必要です。共有ストレージを有効または無効にする方法については、`http://docs.oracle.com/cd/E69469_01` で入手可能な『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

`/sharedstore` ディレクトリは、共有ストレージのマウントポイントです。

- **セキュリティーニーズに応じて、次の推奨事項を考慮して共有ストレージを構成してください。**
  - 共有ストレージがデータベース VM および VM アプリケーションで使用不可になっていること、または読み取り専用であることを確認します。
  - 本番配備では、両方のカーネルゾーンにパブリックネットワークからアクセスできたり、クライアントアクセスに直接アクセスできたりしないようにします。パブリックネットワークやクライアントアクセスからのすべての直接アクセスと共有ストレージサービスの使用を終了する必要があります。仮想マシンで NFS から `/sharedstore` ファイルシステムにアクセスする必要がある場合、IPSEc/IKE チャネルを介して容易になるようにします。

監査およびコンプライアンスレポート

次のトピックでは、MiniCluster で利用できる監査およびコンプライアンスレポートの機能について説明します。

▼ 監査ポリシーの確認

監査ポリシーは、コンプライアンスプロファイル (デフォルトの CIS 相当または PCI-DSS) の選択時に、大域ゾーンと非大域ゾーンのインストールにおいて構成されています。

監査ポリシーが有効になっていることを確認するには、次の手順を実行します。

1. **大域ゾーンに `mcinstall` としてログインし、`root` 役割になります。**

   Oracle ILOM のログイン手順については、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **監査サービスがオンラインになっていることを確認します。**

```
# svcs | grep svc:/system/auditd
online         22:14:37 svc:/system/auditd:default
```

3. **監査プラグインがアクティブになっていることを確認します。**

```
# auditconfig -getplugin audit_binfile
```

```
Plugin: audit_binfile (active)
        Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. **アクティブな監査ポリシーを確認します。**

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. **すべての役割が cusa 監査ポリシーにキャプチャーされていることを確認します。**

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ 監査ログの確認

1. **大域ゾーンに `mcinstall` としてログインし、`root` 役割になります。**

   Oracle ILOM のログイン手順については、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **`auditreduce` コマンドを次のように使用します。**

   これは監査ログを表示するための構文です。

   `auditreduce -z` *vm_name audit_file_name* `| praudit -s`

```
# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce  -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```

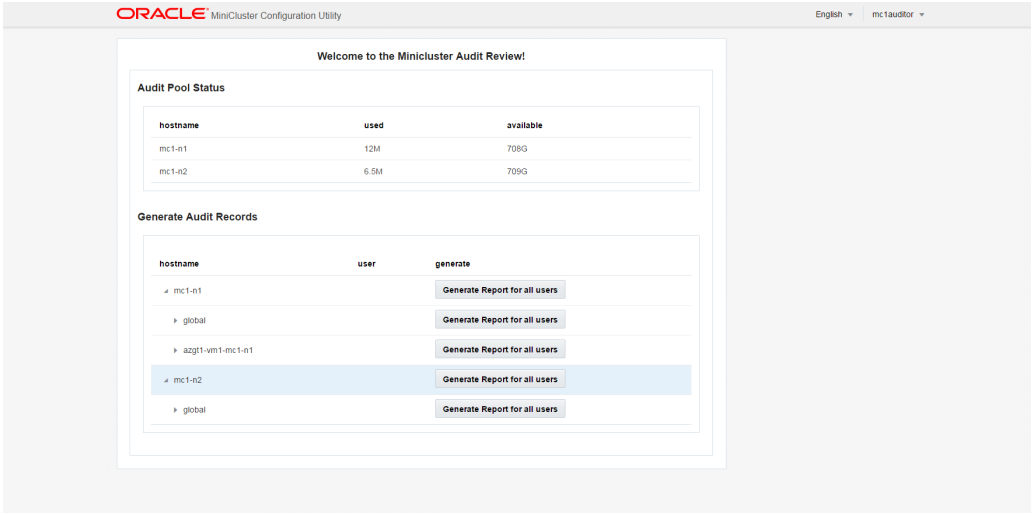
▼ 監査レポートの生成

あるノードまたは個々の VM と大域ゾーンに関する監査レポートを生成するには、この手順を使用します。

1. **監査者役割を割り当てられているユーザーとして MCMU にログインします。**
   MCMU ユーザーと役割の詳細は、`http://docs.oracle.com/cd/E69469_01` で入手可能な『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

2. **ナビゲーションパネルで、「システム設定」->「セキュリティー」を選択します。**
   「Audit Review」ページが表示されます。

注記 - 監査者役割が割り当てられた MCMU ユーザーのみがこのページを表示できます。

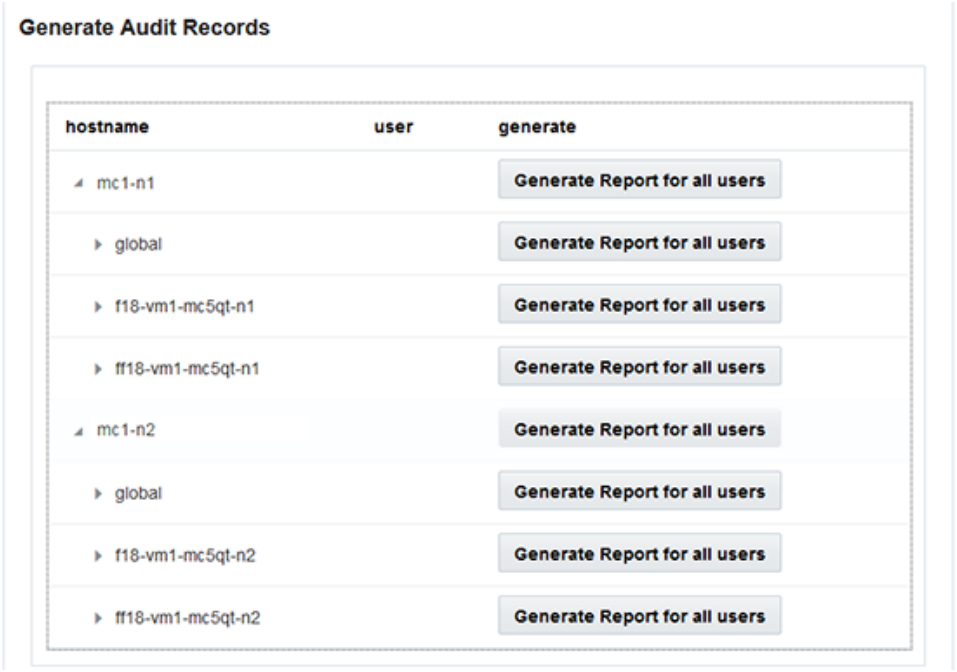


3. **「監査プールステータス」セクションを確認します。**
   このセクションには、各ノード上の監査プールに使用される容量と、使用できる容量が一覧表示されます。

4. **ノード全体のレポートを生成するには、いずれかのノードの「生成」ボタンをクリックして、ステップ 6 に進みます**
   または、特定の VM またはゾーンのレポートを生成できます。ステップ 5 を参照してください

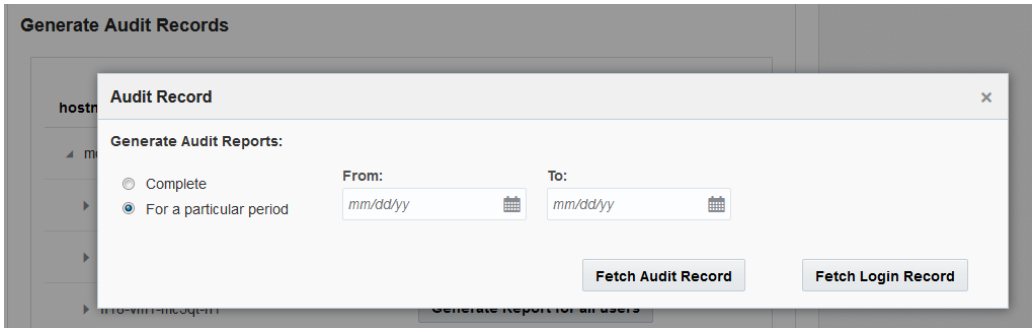
5. 特定の VM または大域ゾーンのレポートを生成するには、次のステップを実行します。

   a. ノードの横にある三角形をクリックして、ビューを展開します。



   b. VM または大域ゾーンの場合、「すべてのユーザーのレポートの生成」をクリックします。

6. **「監査レコード」ダイアログボックスで、監査レコードのパラメータを構成します。**



選択肢は、次のとおりです。

- **完全** - すべての監査レコードを含むレポートが必要な場合に選択します。
- **特定の期間中** – 特定の期間を指定する場合に選択してから、開始日と終了日を入力します。

7. **いずれかの「フェッチ」ボタンをクリックします。**

選択肢は、次のとおりです。

- **監査レコードのフェッチ** – 完全な監査レコードを生成します。
- **ログインレコードのフェッチ** – ログイン、ログアウト、ユーザーアクションなどのユーザーアクティビティーを生成します。

8. **「ここをクリック」ボタンをクリックして、「XML ファイルのダウンロード」を選択します。**

この XML ファイルは、Oracle Audit Vault などの監査分析アプリケーションにインポートできます。

9. **「閉じる」をクリックします。**

▼ (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。

また、44 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。**

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
```

FIPS-140-2 レベル 1 コンプライアンス

MiniCluster 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。

43 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。

この表には、MiniCluster 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。

セキュリティーコンプライアンスの評価

次のトピックでは、MiniCluster のセキュリティーベンチマーク機能について説明します。

セキュリティーコンプライアンスのベンチマーク

システムのインストール時に、セキュリティープロファイル (PCI-DSS、CIS 相当、および DISA-STiG) が選択され、システムはそのセキュリティープロファイルに適合するように自動的に構成されます。システムがセキュリティープロファイルに従って動作し続けていることを確認するために、MCMU にはセキュリティーベンチマークを実行してベンチマークレポートにアクセスするための手段が用意されています。MCMU BUI および CLI を使用してベンチマークを管理できます。

セキュリティーベンチマークを実行することには次の利点があります。

- データベース VM およびアプリケーション VM の現在のセキュリティー状態を評価できます。
- セキュリティーコンプライアンステストでは、インストール時に構成されたセキュリティーレベルに基づいて、PCI-DSS、CIS 相当の規格 (デフォルト)、および DISA-STiG がサポートされます。
- セキュリティーコンプライアンステストは、システムのブート時に自動的に実行され、オンデマンドまたはスケジュールされた間隔で実行することもできます。
- コンプライアンススコアおよびレポートは MCMU プライマリ管理者だけが使用でき、MCMU BUI から簡単にアクセスできます。
- コンプライアンスレポートは、改善のための推奨事項を提供します。

注記 - DISA-STIG プロファイルは現在確認中です。このプロファイルは、非本番環境で実験用にのみ使用してください。

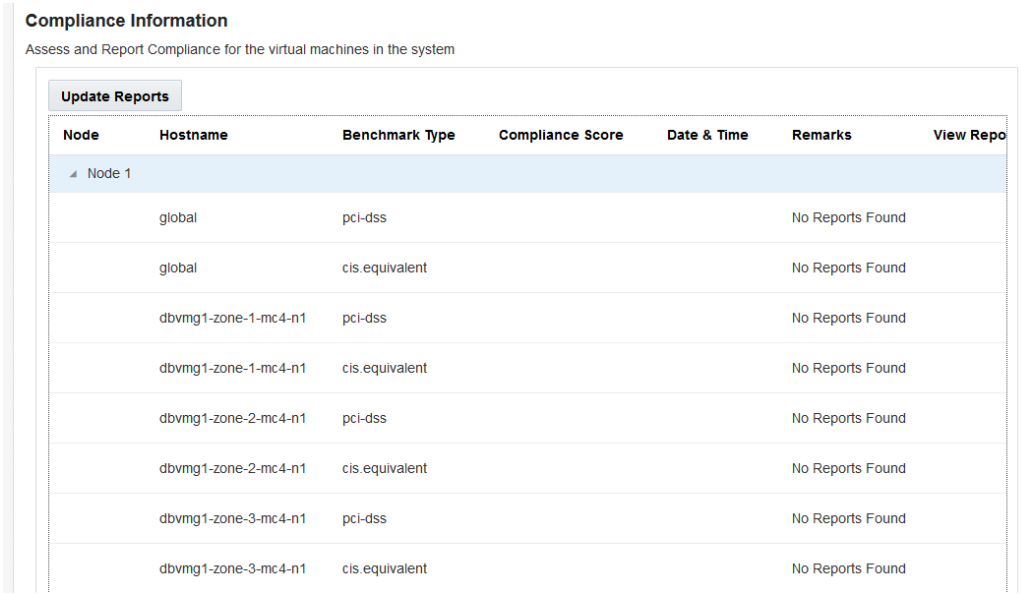
▼ セキュリティーコンプライアンスベンチマークのスケジュール (BUI)

MCMU BUI を使用してセキュリティーベンチマークをスケジュールするには、次の手順を使用します。代わりに MCMU CLI を使用する場合は、手順について『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

1. **プライマリ管理者として MCMU BUI にログインします。**
   手順については、『*Oracle MiniCluster S7-2* 管理ガイド』を参照してください。

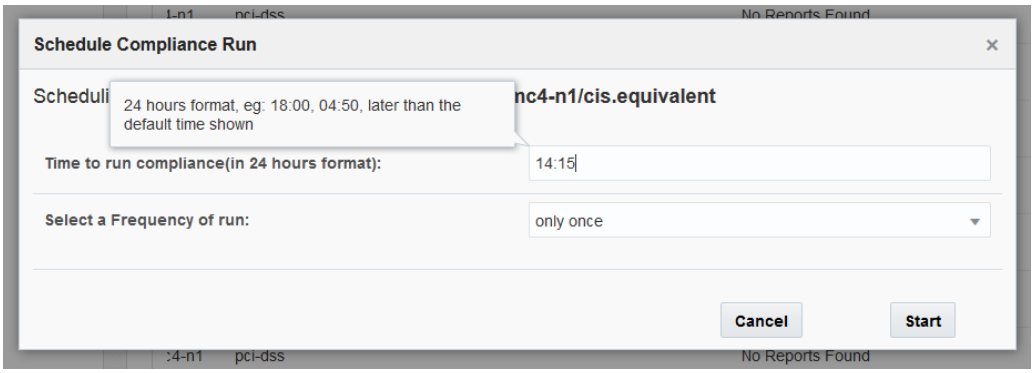
2. **ホームページで、「コンプライアンス情報」パネルまで下へスクロールします。**

3. **ノードをクリックしてその詳細を展開します。**
   各ゾーンおよび VM には、セキュリティープロファイル (CIS 相当または PCI-DSS) が構成されています。ベンチマークをスケジュールするときは、コンポーネントのセキュリティープロファイルに対応するベンチマークを選択してください。



4. **右へスクロールし、いずれかの VM の「スケジュール」ボタンをクリックします。**

コンプライアンスの実行のスケジュールページが表示されます。



5. **時間と頻度を指定し、「開始」をクリックします。**
   セキュリティーコンプライアンステストがスケジュールされた時間に実行されたあとで、レポートを表示します。49 ページの「ベンチマークレポートの表示 (BUI)」を参照してください。

▼ ベンチマークレポートの表示 (BUI)

許容可能なコンプライアンス結果は次のとおりです。

	CIS 相当	PCI-DSS
大域ゾーン	約 88%	約 88%
VM	約 90%	約 93%

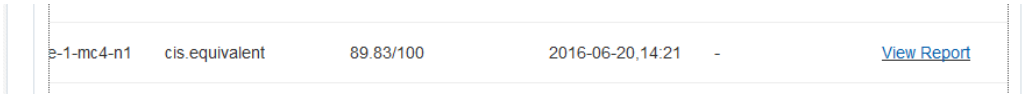
Oracle Solaris の問題に起因する、コンプライアンステストの既知の障害は次のとおりです。

- パッケージ整合性 (コア os、rad-python)
- GDM
- ルーティングデーモン
- SSH ループバックアドレス – 軽減では問題は修正されません。
- ネームサービスが DNS を認識しない
- LDAP クライアント

MiniCluster の顧客によって要求された構成の問題に起因する、コンプライアンステストの既知の障害は次のとおりです。

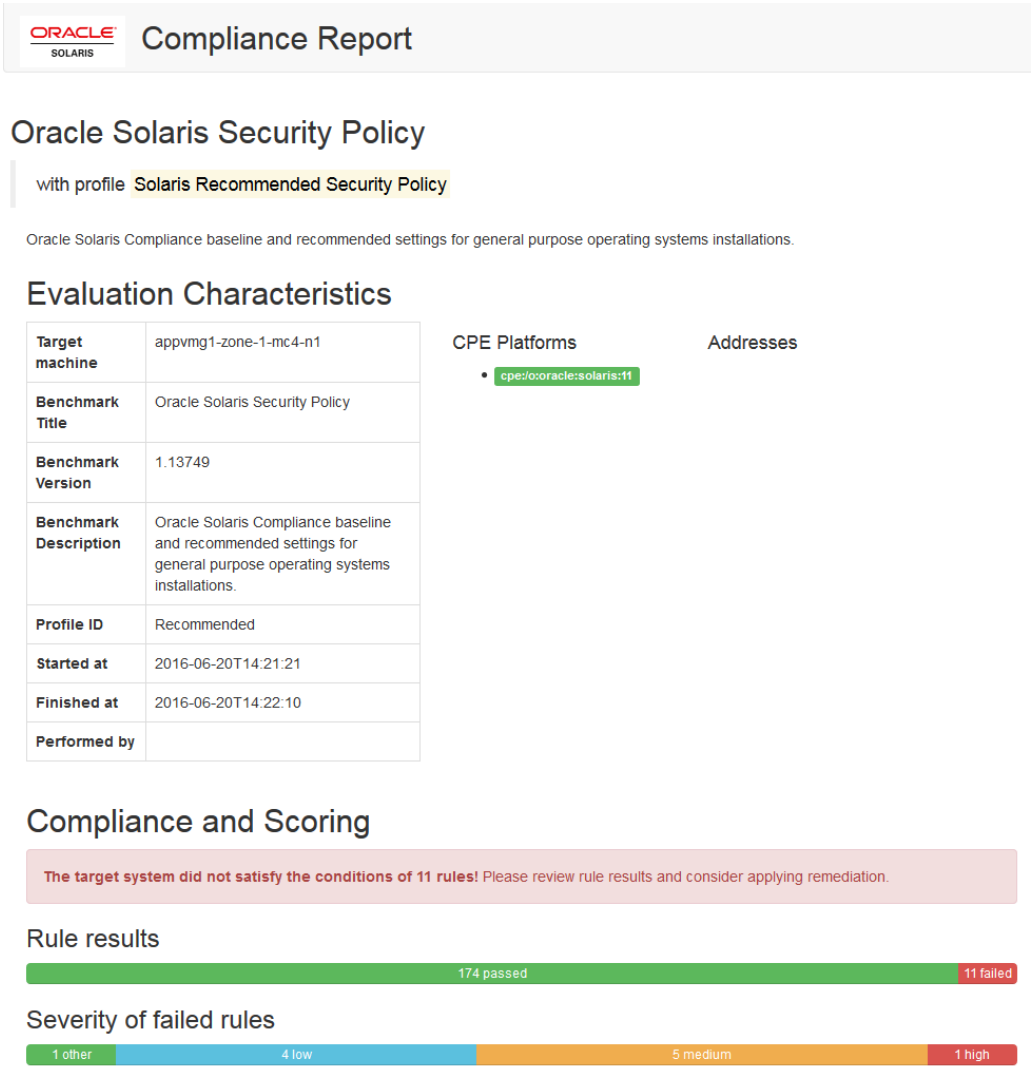
- NFS クライアントサービス – 一部のサービスを使用可能にする必要があります。
- eeprom パスワードの設定 – オプション設定

1. **MCMU BUI にログインします。**
2. **ホームページで、「コンプライアンス情報」パネルまで下へスクロールします。**
3. **「レポートの更新」をクリックします。**
   更新プロセスが完了するまでに約 1 分かかります。
4. **ノードの表示を展開し、コンプライアンスレポートを特定します。**



5. **右へスクロールし、「レポートの表示」をクリックします。**
   ベンチマークレポートが表示されます。

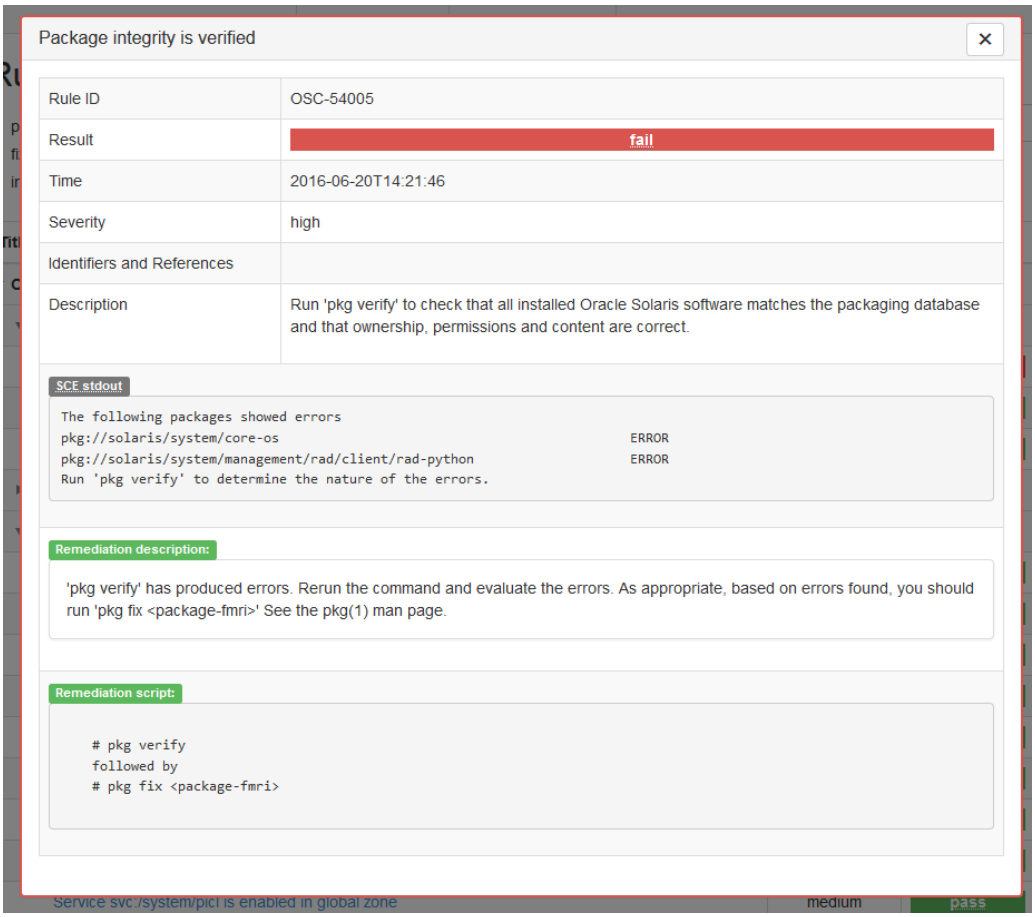
規則の概要では、結果に基づいて表示するテストのタイプを選択できます。検索フィールドで検索文字列を指定することもできます。



6. **レポートに基づいて、セキュリティー制御、コンプライアンススコア、異常、および改善手順を確認できます。**

7. **テストの名前をクリックして、詳細および推奨される改善の情報を取得します。**

注記 - レポートの下部にある、すべての結果の詳細を表示のテキストをクリックすると、すべてのテストの詳細をすべて表示できます。



SPARC S7-2 サーバーのセキュリティーコントロールについて

これらのトピックでは、ハードウェアおよび OpenBoot 環境のセキュリティーコントロールについて説明します。

ハードウェアのセキュリティーについて

物理的な分離とアクセス制御は、セキュリティーアーキテクチャーを構築するべき基盤となります。物理サーバーを確実にセキュアな環境に設置することで、不正アクセスから保護します。同様に、すべてのシリアル番号を記録すると、盗難、転売、またはサプライチェーンのリスク (つまり、偽造されたり危険にさらされたりしたコンポーネントが組織のサプライチェーンに流入されること) を防止するために役立ちます。

これらのセクションでは、MiniCluster の一般的なハードウェア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

- サーバーと関連装置は、アクセスが制限された鍵の掛かった部屋に設置してください。
- 鍵付きのドアがあるラックに装置を設置する場合は、ラック内のコンポーネントの保守を行うとき以外はラックのドアに常に鍵を掛けておいてください。ドアに鍵を掛けることで、ホットプラグまたはホットスワップデバイスへのアクセスも制限されます。

- 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のアクセスは、承認された人だけ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、改ざんや誤ってドアの鍵が掛かっていないままになることを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。物理アクセスは、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。
- コンソールを外付けの KVM に接続して、リモートコンソールアクセスを有効にします。KVM デバイスでは多くの場合、ツーファクタ認証、集中管理されたアクセス制御、および監査がサポートされます。KVM のセキュリティーガイドラインとベストプラクティスの詳細は、KVM デバイスに付属のドキュメントを参照してください。

シリアル番号

- すべてのハードウェアのシリアル番号を記録しておいてください。
- 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は、システム緊急時にシステムマネージャーが簡単に取り出せるセキュアな場所に保管しておいてください。これらの印刷ドキュメントが、唯一の所有権証明になる場合があります。

ワイヤレスの無線周波数識別 (Radio Frequency Identification、RFID) リーダーを使用すると、より簡単にアセットを追跡できます。次の場所にある *RFID* を使用した *Oracle Sun* システムアセットの追跡方法に関する Oracle のホワイトペーパーを参照してください。

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

ハードドライブ

ハード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、すべてのデータをディスク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 サービスを利用してください

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

OpenBoot へのアクセス制限

これらのトピックでは、OpenBoot プロンプトでアクセスを制限する方法について説明します。

OpenBoot のパスワードの構成方法については、28 ページの「EEPROM パスワードの構成」を参照してください。

- 55 ページの「OpenBoot プロンプトの表示」
- 56 ページの「失敗したログインをチェックする」
- 56 ページの「電源投入バナーを提供する」

OpenBoot のセキュリティー変数の設定の詳細は、次の場所にある OpenBoot のドキュメントを参照してください。

http://www.oracle.com/goto/openboot/docs

▼ OpenBoot プロンプトの表示

この手順では、MiniCluster コンピュートノードで OpenBoot プロンプトを表示し、セキュリティーコントロールを構成する方法について説明します。

OpenBoot プロンプトに到達するには、システムをシャットダウンする必要があります。『*Oracle MiniCluster S7-2* 管理ガイド』に説明するように、VM を正常にシャットダウンするための適切な手順に従います。

1. **ノードで Oracle ILOM にログインし、次のコマンドを実行します。**

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

`mcinstall` ユーザーとしてホストコンソールにログインし、`root` に `su` します。

2. **すべての VM がシャットダウンしたら、root 役割として、大域ゾーンを停止します。**

```
# init 0
```

```
.
.
.
{0} ok
```

▼ 失敗したログインをチェックする

1. **次の例に示すように、`security-#badlogins` パラメータを使用して、ユーザーが OpenBoot 環境にアクセスしようとして失敗したかどうかを判別します。**

   ```
   {0} ok printenv security-#badlogins
   ```

   このコマンドが Ø より大きい値を返す場合、OpenBoot 環境にアクセスしようとして失敗したことが記録されています。

2. **このコマンドを入力して、パラメータをリセットします。**

   ```
   {0} ok setenv security-#badlogins 0
   ```

▼ 電源投入バナーを提供する

これは直接の予防的コントロールまたは発見的コントロールではありませんが、次の理由でバナーを使用できます。

- 所有権を譲渡します。
- サーバーの許容される用途をユーザーに警告します。
- OpenBoot パラメータへのアクセスまたは変更が承認された人に制限されていることを示します。

- **次のコマンドを使用して、カスタムの警告メッセージを有効にします。**

  ```
  {0} ok setenv oem-banner banner-message
  {0} ok setenv oem-banner? true
  ```

  バナーメッセージは最大 68 文字です。出力可能な文字がすべて受け入れられます。

索引

V

Z