ORACLE
MINICLUSTER

Oracle MiniCluster S7-2 セキュリティ技術導入ガイド（STIG）コンプライアンス・レビュー

Oracle ホワイト・ペーパー | 2017 年 1 月

ORACLE

目次

はじめに 2

対象読者と前提知識 2

検証方法 3

Oracle MiniCluster - DISA STIG セキュリティ・チェックリスト 4

Oracle Database 12c セキュリティ・チェックリスト 5

STIG の検証結果と解決策 6

- 検証結果の概要 6
  - Oracle Solaris セキュリティ・チェックリストの検証結果 6
  - Oracle Database 12c セキュリティ・チェックリストの検証結果 8
  - 解決策の概要 8
  - 構成設定 9
  - パッチとアップデート 10
  - ソフトウェアのアンインストール 10
  - プロセスまたはプロシージャ 11
  - セキュリティ・ソフトウェア 12

その他のセキュリティ・プラクティス 12

- 管理ネットワークのセキュリティに関する推奨事項 12
  - SPARC S7 コンピュート・ノード 12
- ソフトウェアとファームウェアへのパッチ適用 12
- Oracle MiniCluster の Oracle Database セキュリティ 13

結論 13

付録 14

- Oracle MiniCluster S7-2 プラットフォームについて 14

参考資料 16

- 製品セキュリティ・ガイド 16

はじめに

米国国防情報システム局（DISA）は、国防総省（DOD）の情報システム向けの一連のセキュリティ・ガイドラインの作成および管理を行っています。これらのガイドラインは、セキュリティ技術導入ガイド（STIG）と呼ばれ、展開されているシステムのセキュリティ体制を強化するための構成設定と実行すべき手順が記載されています。多くの政府機関が、まずシステムをこのガイドラインに準拠させてからネットワークに接続するよう求めています。このホワイト・ペーパーは、DISA STIG セキュリティ・ガイドラインに準拠するための手引きとして、前述の DISA STIG セキュリティ・ガイドラインを Oracle MiniCluster S7-2 に正しく実装できることを検証し、報告したものです。

このホワイト・ペーパーに記載された推奨事項は、オラクルが実施したプロジェクトの中で、オラクル・エンタープライズ・テクノロジー・センターで運用中の Oracle MiniCluster S7-2（Oracle MiniCluster）version 1.1.21 に STIG を正しく適用し、テストした結果を踏まえて作成されたものです。すべての取り組みは、導入する DISA STIG セキュリティのベスト・プラクティスを確実にするためのものですが、オラクルの推奨事項が認定機関に認められることを保証するものではありません。

対象読者と前提知識

本文書は、Oracle MiniCluster、Oracle MiniCluster software version 1.1.21（DISA STIG Profile）、Oracle Solaris 11、Oracle Database 11gR3、Oracle Database 12c、Oracle Enterprise Manager とそのセキュリティ機能に精通しているセキュリティの実務者を対象としたものです。

検証方法

STIG の適用とテストの対象として、フル構成の Oracle MiniCluster を使用しました。Oracle MiniCluster プラットフォーム・アーキテクチャの説明は、付録を参照してください。Oracle MiniCluster システムは、全自動の DISA STIG プロファイル・ツールを使ってインストールおよび事前構成されるため、お客様のサイトに提供するのと同様、手動操作を一切必要としません。さらに、Oracle Database STIG スクリプトは、Oracle MiniCluster データベース仮想マシン（Oracle Solaris 11.3 の非大域ゾーン）上の Oracle Database 12c データベースにロードしました。インストール後、システムやデータベース、アプリケーション・サービスが正しく運用されているかを検証するために、次のテストを実施しました。

- Oracle MiniCluster が生成する DISA-STIG コンプライアンス対応レポートを検証（推奨の手動操作を行った場合に期待される総合評価は 95%以上）
- システムの再起動の際にエラーが発生しないことを検証
- FIPS-140-2 レベル 1 への準拠を検証
- 管理コンソール、サーバーおよび外付けストレージに正しく接続できることをテスト
- SQL*Net および TLS で暗号化された SQL*Net 経由でデータベースに正しく接続できることをテスト
- Oracle ZFS の暗号化と鍵管理についてパフォーマンスを低下させずに正しく検証できることをテスト
- エラーがないかシステム・ログを確認
- データベース・コンソール・ユーティリティによるクラスタ全体とデータベースの状態を検証
- アプリケーション仮想マシンの Oracle Enterprise Manager 12c 管理スイートと、データベース仮想マシンの Enterprise Manager エージェントのインストールとテスト
- 構成変更の前後で、“Order Entry“ベンチマークを実行する Swingbench 負荷生成ツールから接続とロードを行うことによって、データベース・インスタンスの機能および性能をテスト
- プライマリ、セカンダリ、テナントの管理者および監査担当者のロール・ベース・アクセス制御を検証
- 一元化された監査ストアおよび監査レポートを検証
- 一元化されたキーストアおよび FIPS 認定アルゴリズムを検証
- ホストベースのファイアウォール（Oracle Solaris IPFilter）を検証
- DISA STIG が推奨するパスワード・ポリシーを検証
- ホワイトリスト登録サービスを検証
- 不要なパッケージ、ポート、プロトコル、サービスの無効化を検証

対象システムは、上記のすべてのテストで安定して動作し続け、結果は良好でした。

Oracle MiniCluster - DISA STIGセキュリティ・チェックリスト

DISA から公開された *Oracle Solaris 11 STIG Version 1 Release 9* に関するドキュメントは、潜在的不一致項目（PDI）を特定する基準、および是正措置や例外処理に関するドキュメントとして利用しました。審査は、Oracle MiniCluster DISA-STIG プロファイルの構成（Virtual Assistant コンソールで Oracle MiniCluster をインストールする時とデータベースおよびアプリケーション仮想マシン・グループを作成する時に有効化される）を使って実施され、総合的なコンプライアンス対応レポートとログに成功したテストと手動操作を必要とする不合格のテストとに分けて記録されました。DISA の Oracle Solaris 11 STIG ドキュメントは、下記のページを参照してください。

http://iase.disa.mil/stigs/os/unix-linux/Pages/solaris.aspx

Oracle Solaris 11 は、Oracle MiniCluster の基盤となる必須オペレーティング・システムですが、Oracle Solaris 10 の仮想マシンでも利用できます。Oracle Solaris 11 は、ラベル・セキュリティと仮想化を含む Operating System Protection Profile（OSPP）の Common Criteria EAL4+の認証レベルを獲得しています。Oracle Solaris Zone は、各物理ノードで複数の仮想マシンを実行できるようにする仮想化技術です。データベース仮想マシン・グループと汎用アプリケーション仮想マシン・グループを別々に作成できるよう、複数の Oracle Solaris Zone をテストで使用しました。すべてのグループは仮想マシン・グループ用の Oracle MiniCluster DISA- STIG プロファイルでインストールする際に保護されています（図 1）。

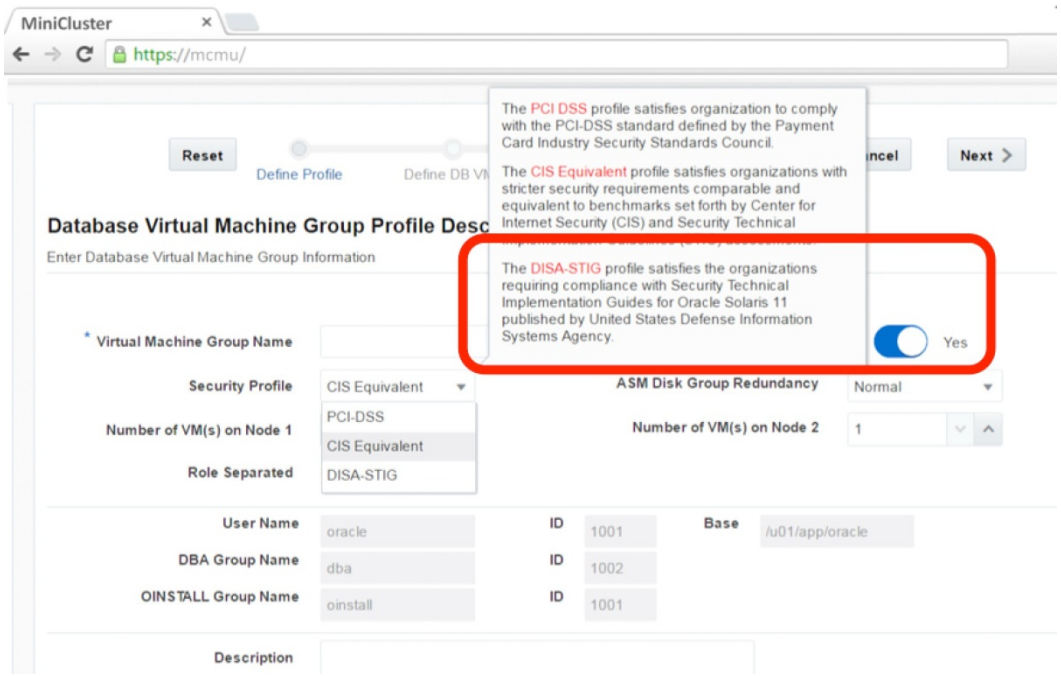
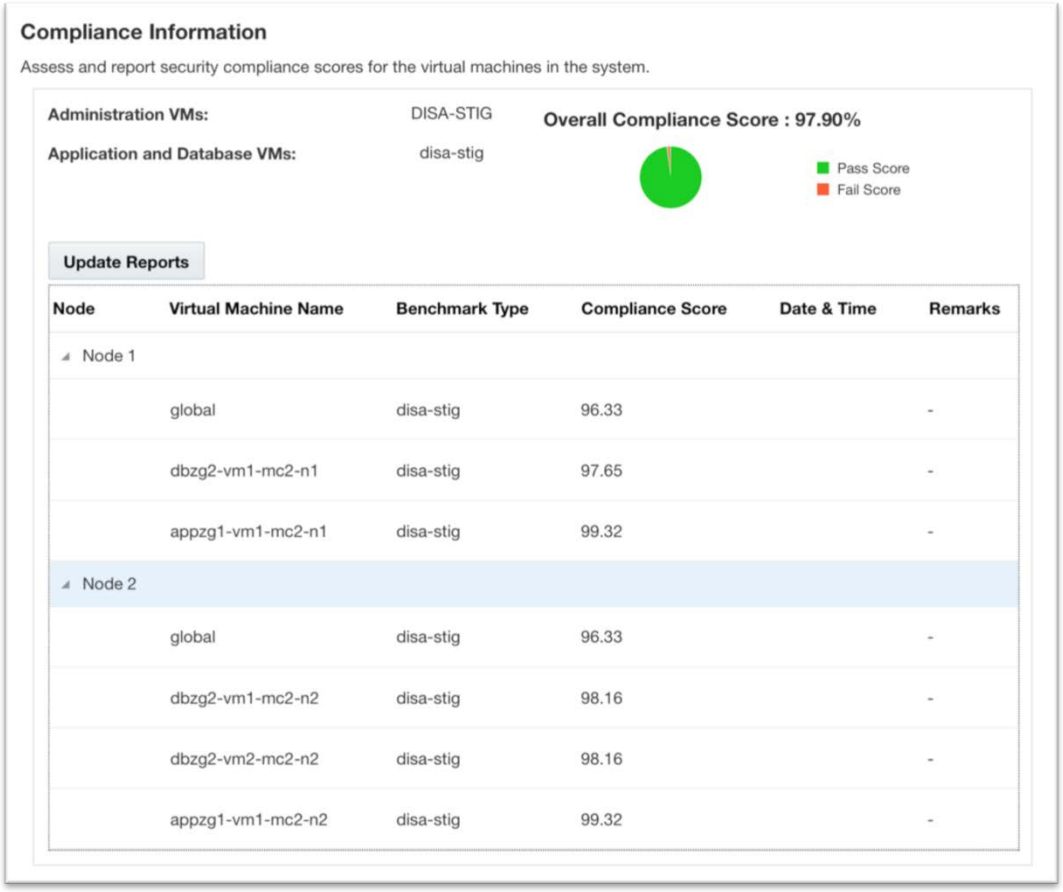


図1：Oracle MiniCluster Virtual Assistant－DISA-STIGプロファイルの選択

DISA-STIG プロファイルを使ってインストールが完了すると、Oracle MiniCluster Virtual Assistant は、Oracle MiniCluster システム・ノード（大域ゾーン）、データベースおよびアプリケーション仮想マシン・グループを最初に起動するときに利用可能な DISA- STIG コンプライアンス対応レポートを表示します。コンプライアンスの全体スコアを記載したコンプライアンス対応レポートと STIG レポートは、Oracle MiniCluster Virtual Assistant の「Compliance Information」の項で参照できます（図 2）。



Node	Virtual Machine Name	Benchmark Type	Compliance Score	Date & Time	Remarks
Node 1					
	global	disa-stig	96.33		-
	dbzg2-vm1-mc2-n1	disa-stig	97.65		-
	appzg1-vm1-mc2-n1	disa-stig	99.32		-
Node 2					
	global	disa-stig	96.33		-
	dbzg2-vm1-mc2-n2	disa-stig	98.16		-
	dbzg2-vm2-mc2-n2	disa-stig	98.16		-
	appzg1-vm1-mc2-n2	disa-stig	99.32		-

図2：Oracle MiniCluster Virtual Assistant－コンプライアンス対応

Oracle Database 12cセキュリティ・チェックリスト

Oracle Database Security Readiness Review（Oracle Database セキュリティ準備審査：SRR）スクリプトも DISA から提供されています。このスクリプトは、Oracle Database 12c システム全体のセキュリティと整合性を脅かす恐れのある潜在的な問題を特定することを目的としています。Oracle Database 12c セキュリティ・チェックリストでは、データベース用の STIG で指定された一連の既知のセキュリティ関連項目を確認します。Oracle MiniCluster プラットフォームにインストールされた Oracle Database のセキュリティ審査は、SRR Oracle Database 12c スクリプトに組み込まれた Oracle Enterprise Manager STIG 検証チェック（本レポートに記載）を使用して実施されました。このレポートでは、Oracle Database 12.1.0.3 での Oracle Database SPR の STIG Version 1 release 1.8 の適用を検証します。

STIGの検証結果と解決策

以降の項では、Oracle MiniCluster システムで動作するデータベースとアプリケーションの DISA STIG セキュリティ構成について説明します。

オラクルでは、DISA-STIG プロファイルで事前構成された Oracle MiniCluster に関する Oracle MiniCluster と Solaris 11 をベースとした STIG の 275 以上の項目と、Oracle のデータベース SRR に従って Oracle Database の 180 項目以上を審査しました。このテストでは、次のカテゴリを使って検証結果のステータスを記録しました。

- 未解決の検証結果：Oracle MiniCluster のデフォルト・セットアップでは、技術的な解決策を提供できません
- 手動操作が必要：適切な対策がデフォルト、または手動で適用されています。

検証結果の概要

STIG テストの検証結果は、以下のカテゴリに分類されています。

- Oracle Solaris セキュリティ・チェックリストの検証結果
- Oracle Database 12c セキュリティ・チェックリストの検証結果

Oracle Solarisセキュリティ・チェックリストの検証結果

Oracle Solaris セキュリティ・チェックリストの検証結果は、表 1 に示すように、いくつかのカテゴリに分類されます。

表1：Oracle MiniCluster/Solarisセキュリティ・チェックリストの検証結果のカテゴリ

カテゴリ	説明
292	Oracle MiniCluster/Solaris の審査項目の総数
74	MiniCluster CIS/Secure にデフォルトで追加されたセキュリティ構成
183	成功したセキュリティ・テストの数－合格
9	Oracle MiniCluster のインストール後に不合格となったセキュリティ・テストの数（修正前）
27	手動操作が必要、サイト固有のポリシーまたは手続きが必要な項目の数
3	未解決の検証結果の数（修正後）

すべてのコンピュート・ノードに関する STIG 対応レポートは、Oracle MiniCluster Virtual Assistant にアクセスしてダウンロードできます。次に標準的なレポートを示します（図 3 参照）。

図3：Oracle MiniCluster－標準的なDISA STIG対応レポート（大域ゾーンの概要）

Oracle MiniCluster のデフォルト・インストール（大域ゾーン）後に手動操作が通常必要とされる未解決項目は以下のとおりです。

- SRG-OS-999999 SOL-11.1-020350 2 RC no write
- SRG-OS-999999 SOL-11.1-020380 2 SS exec owner
- SRG-OS-999999 SOL-11.1-030040 3 miscDisab
- SRG-OS-999999 SOL-11.1-030050 2 wrappers
- SRG-OS-000002 SOL-11.1-040020 3 pass temp
- SRG-OS-000148 SOL-11.1-040490 2 outbound
- SRG-OS-999999 SOL-11.1-050140 3 wrappers
- SRG-OS-999999 SOL-11.1-050470 2 spoof `
- SRG-OS-000157 SOL-11.1-060070 2 ssh ipsec
- SRG-OS-000158 SOL-11.1-060080 2 ssh ipsec
- SRG-OS-000159 SOL-11.1-060090 2 ssh ipsec
- SRG-OS-000160 SOL-11.1-060100 2 ssh ipsec
- SRG-OS-000161 SOL-11.1-060110 2 ssh ipsec
- SRG-OS-000162 SOL-11.1-060120 2 ssh ipsec
- SRG-OS-000033 SOL-11.1-060130 2 ssh ipsec
- SRG-OS-000157 SOL-11.1-060190 2 ipsec
- SRG-OS-999999 SOL-11.1-070090 2 homeOwn
- SRG-OS-999999 SOL-11.1-070190 3 SUID
- SRG-OS-999999 SOL-11.1-070200 2 all owned
- SRG-OS-999999 SOL-11.1-080010 1 O/S ver

- SRG-OS-999999 SOL-11.1-080160 1 SNMP
- SRG-OS-000056 SOL-11.1-090020 2 ntp.conf
- SRG-OS-999999 SOL-11.1-090030 2 auditReduce
- SRG-OS-999999 SOL-11.1-090040 3 extraAccts
- SRG-OS-000099 SOL-11.1-090050 2 backups
- SRG-OS-000100 SOL-11.1-090060 2 backups
- SRG-OS-000101 SOL-11.1-090070 2 backups

不合格のテスト項目のうち、手動操作によって（Oracle MiniCluster BUI または CLI を使用して）解決できる可能性のある項目は以下のとおりです。

- SRG-OS-999999 SOL-11.1-080130 3 EEPROM
- SRG-OS-000047 SOL-11.1-010420 2 auditCrash
- SRG-OS-999999 SOL-11.1-050370 3 ipfilter

Oracle MiniCluster のデフォルト・インストールでは解決できない既知の不合格テスト項目（大域ゾーン）。

- SRG-OS-000256 SOL-11.1-020030 2 pkgVerify
- SRG-OS-999999 SOL-11.1-070080 3 userHome
- SRG-OS-999999 SOL-11.1-100030 2 zone dev

Oracle Database 12cセキュリティ・チェックリストの検証結果

Oracle Database 12c のセキュリティ・チェックリストでは、表 2 に示すカテゴリに分類された合計 180 項目が評価されました。

表2：Oracle Databaseチェックリストの検証結果のカテゴリ

カテゴリ	説明
180	Oracle Database の審査項目の総数
24	未解決項目の数（修正前）
0	未解決項目の数（修正後）
119	手動、サイト固有のポリシーまたは手続きが必要な項目の数
46	デフォルト構成における所見なしの項目の数

解決策の概要

このセクションでは、未解決の検証結果を解決するために実施すべき対策の概要を説明しています。わかりやすくするために、解決策は以下のカテゴリに分類され、STIG 適用対象の Oracle MiniCluster のデータベース・サーバーに適用されます。

- **構成設定**：オペレーティング・システム、ユーティリティ、データベースに対する構成設定を変更

- **パッチとアップグレード**：パッチの適用またはソフトウェアやファームウェアをアップグレード
- **ソフトウェアのアンインストール**：対象システムからインストール済みのソフトウェアを削除
- **プロセスまたはプロシージャ**：ドキュメント作成およびプロセスまたはプロシージャの導入
- **セキュリティ・ソフトウェア**：対象システムへのソフトウェアやユーティリティのインストールと設定。たとえば、アンチウィルス・ソフトやホストの侵入検知ツールなど

構成設定

Oracle MiniCluster/Solaris 11 のセキュリティ構成の設定と変更には、以下のようなものがあります。

- 基本サービスのホワイトリストへの登録
- 不要なサービスのブラックリストへの登録と無効化
- ログインとパスワードのシステムの設定、ログイン設定および tty の設定
- 個別のアカウントやグループの削除、変更または無効化
- ファイルやディレクトリの所有権および権限の変更または削除
- bashrc などのファイルの初期化
- 監査サブシステムの設定（新しいルールや監査ログのローテーションを取り入れるため）
- cron やスケジューリング・システムの設定
- ファイアウォール、TCP ラッパー、およびネットワーク構成の設定
- コア・ダンプの構成
- パッケージ化されたユーティリティの無効化または削除
- 国防総省（DoD）の承認済みログイン・バナーやメッセージ、警告の追加
- 公開されたポリシーに基づくパスワード付きコンテンツの作成
- /etc/hosts での許可および拒否の設定
- 端末のロックアウト設定
- NTP サーバーの構成
- FIPS 140 モードの設定
- 暗号化された ZFS データセットの作成
- Swap の暗号化
- 監査ストアの一元化
- ロールベースのアクセス制御の設定
- PKCS#11 ベースのキーストアの一元化

Oracle Solaris 12c の設定と変更には、以下のようなものがあります。

- データベース監査の有効化と構成
- ユーザー・プロファイルに対するリソース制限の設定
- システム・パラメータの変更によるデータベース・アクセスの強化
- STIG によるパスワードの複雑さの要件に準拠するため、お客様に応じたパスワード検証機能の導入
- SQL*Net の設定の変更による有効期間や接続時間の延長、許可クライアントの制限および cnt バージョンの規制強化
- ファイルやディレクトリの所有権および権限の設定
- STIG によるパスワードの複雑さのルールに準拠するため、アカウントのパスワード変更
- パスワード・システム構成と認証設定の変更
- SYSMAN の権限付与およびスキーマ設定
- 機密データの暗号化の実施
- STIG チェックリストに基づく TNS リスナーの構成

パッチとアップデート

Oracle MiniCluster の事前予防的なメンテナンスのために最重要なアップデートは、四半期ごとのメンテナンス・アップデートです。これは Oracle MiniCluster 用の四半期ごとのフルスタック・ダウンロード・パッチ（QFSDP）としてリリースされます。

リアクティブ・メンテナンスの場合（問題発生時の修正、または四半期ごとのアップデートの間の重要なセキュリティ修正）、オラクル・エンジニアド・システム・サポートと相談のうえ、必要に応じて、影響を受けるコンポーネントをアップデートできます。

ソフトウェアのアンインストール

Oracle Solaris 11 ソフトウェアの場合、アンインストールの対象には、ネットワーク・プロトコル（FTP、NIS、TFTP/installadm、telnet、UUCP、finger）、VNC およびインスタント・メッセージング（pidgin）などがあります。Oracle Database 12c ソフトウェアの場合、STIG チェックリストの推奨項目がアンインストールされます。これには、不要なデータベース・コンポーネントまたはライセンスされていないデータベース・コンポーネントのアンインストールや削除だけでなく、任意のデータベース・スキーマやオブジェクト、これらの専用サポート・アプリケーションの削除も含まれます。こうした変更は通常、データベース・システムの意図的な操作や機能に対応するために適宜実行されます。このカテゴリの Oracle Database 12c のコンポーネントの例としては、Oracle Partitioning、Oracle Real Application Clusters（Oracle RAC)、および Data Guard、Oracle Active Data Guard の機能と Oracle Database、Enterprise Edition などが挙げられます。必須コンポーネントは、アプリケーション設計仕様書に記載され、システムのセキュリティ計画に一覧表示されています。

プロセスまたはプロシージャ

プロセスとプロシージャの作成および実装は、サイトに大きく依存し、ローカルのセキュリティ・ポリシーに左右されます。このカテゴリの大半の項目は、「未解決でお客様のアクションを必要とする」と判断された検証結果です。以下は、STIG チェックリスト・スクリプトで特定された潜在的なエラーが含まれた箇所に対する個別の推奨是正措置を要約したものです。

- Oracle Solaris 11 セキュリティの適用とガイドラインの強化。これは、次の標準ドキュメント・セットに記載されています。
  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- あらゆる外付けデバイスの接続を含めた、システムの物理的なセキュリティの確保
- ベンダー推奨のパッチとセキュリティ・パッチの定期的な適用
- ベースライン・バックアップの維持とベースラインに対するファイル・システムの検証
- 情報保証責任者による、STIG の推奨事項とローカル・ポリシーに則った STIG ポリシーとの相違点とシステムの文書化
- ユーザー・パスワードとアカウント・ポリシーに関するアクションの実行
- クライアント・アクセス・ネットワークと管理ネットワークの明確な区分の維持

Oracle Database 12c データベース・スコープのプロセスまたはプロシージャは以下のとおりです。

- 管理ポリシーと運用ポリシーおよびプロセスの作成と文書化
- コンプライアンス標準に対する構成の検証
- データベースのバックアップとリカバリの導入とテスト
- データベース変更と構成管理
- コンプライアンス要件に基づいたデータ・ラベリング、暗号化、鍵管理、検証（必要に応じて）
- 監査情報の導入と管理
- アカウント、アクセス制御および認可プロシージャとポリシーの文書化と適用
- STIG 推奨事項と DBMS 種別レベルに対する監査と準拠
- ネットワーク構成とネットワーク構成のセキュリティ、リモート管理の暗号化、ネットワーク境界の保護。

セキュリティ・ソフトウェア

Oracle Solaris 11 でインストールされるセキュリティ・ソフトウェアやユーティリティは以下のとおりです。

- システム脆弱性ツールのインストールと構成
- 認定ウィルス・スキャン・ソフトウェアのインストールと構成

その他のセキュリティ・プラクティス

このセクションでは、Oracle MiniCluster 全体のセキュリティを強化するために利用できるその他のセキュリティ・プラクティスについて説明します。プラクティスの内容は、システムへのパッチ適用から管理ネットワークの要素に対するアクセス制御まで多岐に渡ります。

管理ネットワークのセキュリティに関する推奨事項

Oracle MiniCluster の管理サブネットは、システム・コンポーネントへの重要なアクセスを提供するため、適切に保護する必要があります。管理ネットワークにより、システムのさまざまなコンポーネントへのアクセスポートを持つ Oracle Integrated Lights Out Manager（Oracle ILOM）へアクセスが可能になります。Oracle ILOM ポートにアクセスできるということは、システムに物理的にアクセスできるのと同じです。Oracle ILOM ポートにアクセスできるユーザーは、システムの電源を切ったり、新しい ILOM ソフトウェアをインストールしたり、ILOM の root パスワードを変更したりできます。Oracle ILOM のセキュリティ制御によって、機能を制限したロールを作成できます。管理ネットワークへのアクセスは、限られた人数の十分なスキルを持つ専門の管理スタッフだけが SSH を使用して行うよう、制限する必要があります。Oracle ILOM へは、コマンドラインで SSH を使用するか、または SSL で暗号化された Web セッションでアクセスできます。

SPARC S7コンピュート・ノード

Oracle Solaris STIG に従って適切に構成すれば、コンピュート・ノードは DISA のガイドラインに則って、ユーザー・パスワード・ポリシーとロール・パスワード・ポリシーを自動的に適用し、デフォルトで複雑なパスワードを使用します。さらに、Oracle ILOM の管理者パスワードおよび EEPROM パスワードを DISA 標準に合わせて手動で設定し、Oracle ILOM コンソールや Oracle MiniCluster Virtual Assistant の Web インターフェース経由で不正にシステムの電源をオンオフされないようにする必要があります。ロールは、Oracle MiniCluster 仮想マシン（Solaris 11 ゾーン）や Oracle ILOM で効果的に使用されており、完全な root 権限を与えなくてもシステム管理が可能になります。

ソフトウェアとファームウェアへのパッチ適用

適切で効果的なパッチ管理は、あらゆるシステムのセキュリティにおいて不可欠な構成要素です。オラクル推奨パッチやセキュリティ・パッチを適用することは、基本的なセキュリティを確立するうえでの最低限の推奨事項です。

Oracle MiniClusterのOracle Databaseセキュリティ

オラクルは、当初から業界最先端のデータ保護技術をデータの保存場所、つまりデータベースに投入してきました。オラクルは、総合的なセキュリティ・ソリューションの製品ラインナップを取り揃え、データのプライバシーの確保、内部脅威に対する保護、法規制の順守を実現します。Oracle Database の主要なセキュリティ製品は以下のとおりです。

- Oracle Transparent Data Encryption
- Oracle Database Vault
- Oracle Audit Vault and Database Firewall
- Oracle Configuration Manager
- Oracle Total Recall
- Oracle Advanced Security
- Oracle Data Masking Pack
- Oracle Label Security
- Oracle Secure Backup

オラクルの強力な特権ユーザー、複数ファクタのアクセス制御、データ種別、透過的データ暗号化、監査、監視、データ・マスキングを利用すれば、信頼性の高いデータ・セキュリティ・ソリューションを導入できます。しかも、既存のアプリケーションを一切変更する必要がないので時間とコストを節約できます。

結論

STIG が推奨する構成設定を、Oracle MiniCluster ソフトウェア 1.1.21（DISA STIG プロファイル）によってシステムに悪影響を与えずに、Oracle MiniCluster プラットフォームに適用するという目標を無事達成し、このホワイト・ペーパーを作成しました。あらゆる状況やあらゆる構成に STIG の推奨事項を適用するための 1 つの定式というものはありません。その一方で、国防総省の DISA が作成した推奨事項に準拠するよう要請された、または準拠することを決めた政府や民間組織のニーズを満たすには、STIG の推奨事項を最初の起動時に Oracle MiniCluster プラットフォームに適用することが合理的かつ可能であることが、このプロジェクトで実施した導入とテストによって明らかになりました。

付録

Oracle MiniCluster S7-2プラットフォームについて

オラクルの SPARC S7 プロセッサの処理能力を持った多用途のエンジニアド・システム Oracle MiniCluster S7-2 は、10GbE の冗長ネットワークによって接続された独立したアクティブ/アクティブの 2 台のコンピュート・サーバーで構成されています（図 4）。このため、高性能共有フラッシュ・ストレージによる完全に冗長化された高可用性アーキテクチャの構築が可能になります。コンピュート・サーバーは、Oracle Solaris をベースとしたセキュアな仮想マシンの効率的な仮想化機能と高可用性 Oracle Database を利用するために、完全に最適化されています。さらに、別の 10GbE ネットワークによって、複数の SPARC S7 サーバー上の仮想マシン環境とホストされた複数のアプリケーション間のすべての相互通信が管理されます。このようにそれぞれが最適化されたコンポーネントが連携することで、Oracle MiniCluster S7-2 は、ホスティングする複数のアプリケーションやデータベースにセキュアな単一テナント、すなわち専用のコンピュート・プラットフォーム環境を提供します。この統合環境により、企業やクラウド・サービス・プロバイダーが初期インストール時からセキュアでガイドラインに準拠した状態をより確実に維持することが可能になります。これにより、検証済みで、ガイドラインに準拠した、完全に新しい設計によるセキュアなコンピュート環境とアプリケーション環境が構築可能になります。

＊オプションのストレージ・エクスパンジョン搭載時

図4：Oracle MiniCluster S7-2ハードウェア・アーキテクチャ

SPARC S7 プロセッサには、ハードウェアによる暗号化機能が搭載され、Oracle MiniCluster S7-2 上にホストされているエンティティが持つ情報を（保存中、使用中、送信中でも）高性能データ保護機能で保護できるようになっています。このプロセッサには、オラクルのシリコン・セキュアド・メモリも搭載されています。これは、オラクルのプロセッサ SPARC M7 と SPARC S7 の機能であり、メモリ・データ破損やメモリ・スクレイピングに関連する攻撃を検知し、防御することによって、アプリケーション・データの整合性を保全します。Oracle MiniCluster S7-2 は、高い可用性を備えた仮想マシンを最大 24 台ホスティングできます（ノードあたり仮想データベース・マシンが最大 4 台と仮想アプリケーション・マシンが 12 台）。この 24 台の仮想マシンに加えて、管理専用の VM が 2 台と NFSv4 ストレージやオラクル・キー・ウォレット、オブジェクト・ストアといった共有サービスをホストする専用の仮想マシンを 2 台備えています。デフォルトで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配置され、暗号化されたネットワーク接続を利用します。さらに仮想マシンはすべて、250 以上の標準セキュリティ制御機能を使って、事前に構成と検証が行われます。この制御によって、必ずしも必要ではない、または既知の脆弱性を持つサービスやポート、

プロトコルを無効にしてシステムの攻撃対象領域を減らすことで、プラットフォームの機密保護、整合性、可用性を実現します。さらに公開サービスが信頼された接続のみを受け入れるよう構成することで、いかなる多段攻撃に対しても堅牢なセキュリティ制御が可能になります。

図 5 は、Oracle データベースとアプリケーションのワークロードを統合しデフォルトのセキュリティ構成を持つ、Oracle MiniCluster S7-2 の標準的なコンフィギュレーションを表しています。

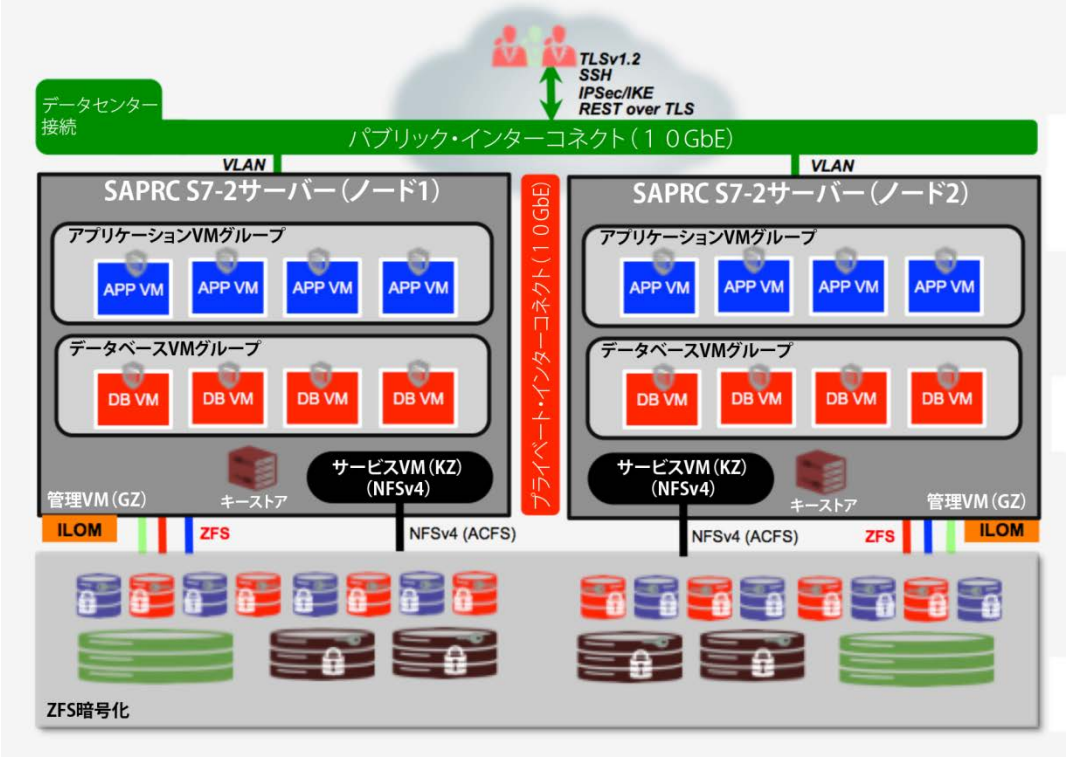


図5：Oracle MiniCluster S7-2：ソフトウェア・ワークロード向けのデフォルト・セキュリティ構成が適用された標準構成

参考資料

Oracle Solaris と Oracle Database 用の STIG コンプライアンス文書の詳細と最新バージョンは、以下の DISA のウェブサイトから入手できます。

- http://iase.disa.mil/stigs/os/unix-linux/Pages/solaris.aspx
- http://iase.disa.mil/stigs/app-security/database/Pages/oracle.aspx

製品セキュリティ・ガイド

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

  http://www.oracle.com/jp/products/servers-storage/miniclusters7-security-3459326-ja.pdf?ssSourceSiteId=otnjp
- Oracle MiniCluster S7-2 セキュリティ・ガイド

  https://docs.oracle.com/cd/E78248_01/html/E78267/index.html
- Oracle Integrated Lights Out Manager (Oracle ILOM) Security Guide Firmware Releases 3.0, 3,1, 3.2

  http://docs.oracle.com/cd/E37444_01/pdf/E37451.pdf
- Oracle Solaris 10 のセキュリティ・ガイドライン

  https://docs.oracle.com/cd/E24845_01/pdf/E23420.pdf
- Oracle Solaris 11 のセキュリティと強化ガイドライン

  http://docs.oracle.com/cd/E62101_01/pdf/E62714.pdf
- Oracle Database 12c セキュリティ・ガイド

  https://docs.oracle.com/cd/E49329_01/network.121/b71285/toc.htm
- Oracle's Common Criteria status page

  http://www.oracle.com/technetwork/topics/security/oracle-common-criteria-095703.html

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

Copyright © 2017, Oracle and/or its affiliates.All rights reserved.本文書は情報提供のみを目的として提供されており、記載内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

Oracle および Java は Oracle およびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

Intel および Intel Xeon は Intel Corporation の商標または登録商標です。すべての SPARC 商標はライセンスに基づいて使用される SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMD ロゴおよび AMD Opteron ロゴは、Advanced Micro Devices の商標または登録商標です。UNIX は、The Open Group の登録商標です。0615

Oracle MiniCluster セキュリティ技術導入ガイド（STIG）コンプライアンス・レビュー（2017 年 1 月）
著者：Ramesh Nagappan 共著者：Kevin Rohan

Oracle is committed to developing practices and products that help protect the environment.