Oracle® VM Server for SPARC 3.0 セキュリティーガイド

Part No: E37592
2012 年 11 月

ORACLE

130417@25097

目次

はじめに

『Oracle VM Server for SPARC 3.0 セキュリティーガイド』では、Oracle VM Server for SPARC 3.0 ソフトウェアを安全にインストール、構成、および使用する方法についての情報を示します。

関連ドキュメント

次の表に、Oracle VM Server for SPARC 3.0 リリース向けに提供される、またこのリリースに関連するドキュメントを示します。

表 P–1 関連ドキュメント

用途	タイトル
Oracle VM Server for SPARC 3.0 ソフトウェア	『Oracle VM Server for SPARC 3.0 管理ガイド』 『Oracle VM Server for SPARC 3.0 セキュリティーガイド』 『Oracle VM Server for SPARC 3.0 リファレンスマニュアル』 『Oracle VM Server for SPARC 3.0 リリースノート』
Oracle VM Server for SPARC 3.0 `drd`(1M) および `vntsd`(1M) マニュアルページ	Oracle Solaris OS リファレンスマニュアル: ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
Oracle Solaris OS: インストールと構成	Oracle Solaris OS インストールおよび構成ガイド: ■ Oracle Solaris 10 Documentation ■ Oracle Solaris 11 Documentation
Oracle VM Server for SPARC および Oracle Solaris OS のセキュリティー	Oracle VM Server for SPARC のホワイトペーパーおよび Oracle Solaris OS セキュリティーガイド: ■ Secure Deployment of Oracle VM Server for SPARC (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf`) ■ 『Oracle Solaris 10 Security Guidelines』 ■ 『Oracle Solaris 11 Security Guidelines』

使用しているサーバー、ソフトウェア、またはOracle Solaris OSに関連するドキュメントは、http://www.oracle.com/technetwork/indexes/documentation/index.html で参照できます。必要なドキュメントや情報を検索するには、「Search」ボックスを使用します。

Oracle VM Server for SPARCのディスカッションフォーラムへは、http://forums.oracle.com/forums/forum.jspa?forumID=1047 からアクセスできます。

Oracleサポートへのアクセス

Oracleユーザーは My Oracle Support から電子サポートにアクセスできます。詳細については、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info にアクセスしてください。または、聴覚に障害がある場合は http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs にアクセスしてください。

表記上の規則

次の表では、このマニュアルで使用される表記上の規則について説明します。

表 P–2 表記上の規則

字体	説明	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 machine_name% you have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	machine_name% **su** Password:
aabbcc123	可変部分: 実際に使用する特定の名前または値で置き換えます。	ファイルを削除するコマンドは、rm *filename* です。
AaBbCc123	書名、新しい単語、および強調する単語を示します。	『ユーザーズガイド』の第 6 章を参照してください。 キャッシュは、ローカルに格納されたコピーです。 ファイルを保存しないでください。 注: 一部の強調された項目はオンラインでは太字で表示されます。

コマンド例のシェルプロンプト

次の表に、Oracle Solaris OS に含まれるシェルの UNIX システムプロンプトおよびスーパーユーザープロンプトを示します。コマンド例のシェルプロンプトは、標準ユーザーと特権ユーザーのどちらがコマンドを実行するべきであるのかを示しています。

表 P–3 シェルプロンプト

シェル	プロンプト
Bash シェル、Korn シェル、および Bourne シェル	`$`
スーパーユーザーの Bash シェル、Korn シェル、および Bourne シェル	`#`
C シェル	`machine_name%`
スーパーユーザーの C シェル	`machine_name#`

◆ ◆ ◆ 第 1 章

Oracle VM Server for SPARC のセキュリティーの概要

この章では、Oracle VM Server for SPARC ソフトウェアによって使用される次のセキュリティー機能について説明します。

Oracle VM Server for SPARC によって使用されるセキュリティー機能

Oracle VM Server for SPARC ソフトウェアは、それぞれに独自の Oracle Solaris 10 または Oracle Solaris 11 OS がインストールされた複数の Oracle Solaris 仮想マシン (VM) を、1 つの物理システム上で実行できるようにする仮想化製品です。各 VM は論理ドメインとも呼ばれます。ドメインは独立したインスタンスであり、Oracle Solaris OS の各種バージョンおよび各種のアプリケーションソフトウェアを実行できます。たとえば、複数の異なるパッケージリビジョンをドメインにインストールしたり、複数の異なるサービスをドメインで有効にしたり、パスワードが異なる複数のシステムアカウントをドメインに作成したりできます。Oracle Solaris のセキュリティーについては、『Oracle Solaris 10 Security Guidelines』および『Oracle Solaris 11 Security Guidelines』を参照してください。

論理ドメインを構成したり、状態情報を取得したりするには、`ldm` コマンドを制御ドメインで実行する必要があります。制御ドメインおよび `ldm` コマンドへのアクセスを制限することは、システムで実行されているドメインのセキュリティーにとって重要です。ドメイン構成データへのアクセスを制限するには、Oracle VM Server for SPARC のセキュリティー機能を使用しますが、そのような機能の例としては、コンソールおよび `solaris.ldoms` 承認を対象とした、Oracle Solaris の役割に基づくアクセ

ス制御 (RBAC) 機能があります。『Oracle VM Server for SPARC 3.0 管理ガイド』の「Logical Domains Manager プロファイルの内容」を参照してください。

Oracle VM Server for SPARC ソフトウェアは次のセキュリティー機能を使用します。

- Oracle Solaris 10 OS および Oracle Solaris 11 OS で利用できるセキュリティー機能は、Oracle VM Server for SPARC ソフトウェアを実行するドメインでも利用できます。『Oracle Solaris 10 Security Guidelines 』および『Oracle Solaris 11 Security Guidelines 』を参照してください。
- Oracle Solaris OS のセキュリティー機能は Oracle VM Server for SPARC ソフトウェアに適用できます。Oracle VM Server for SPARC のセキュリティー確保についての詳しい情報は、『Secure Deployment of Oracle VM Server for SPARC』を参照してください。
- Oracle Solaris 10 OS および Oracle Solaris 11 OS には、システムに適用可能なセキュリティー修正が含まれています。Oracle Solaris 10 OS の修正はセキュリティーパッチまたはアップデートとして入手します。Oracle Solaris 11 OS の修正は SRU (Support Repository Update) として入手します。
- Oracle VM Server for SPARC の管理コマンドおよびドメインコンソールへのアクセスを制限する方法と、Oracle VM Server for SPARC の監査機能を有効にする方法については、『Oracle VM Server for SPARC 3.0 管理ガイド』の第 3 章「Oracle VM Server for SPARC のセキュリティー」を参照してください。

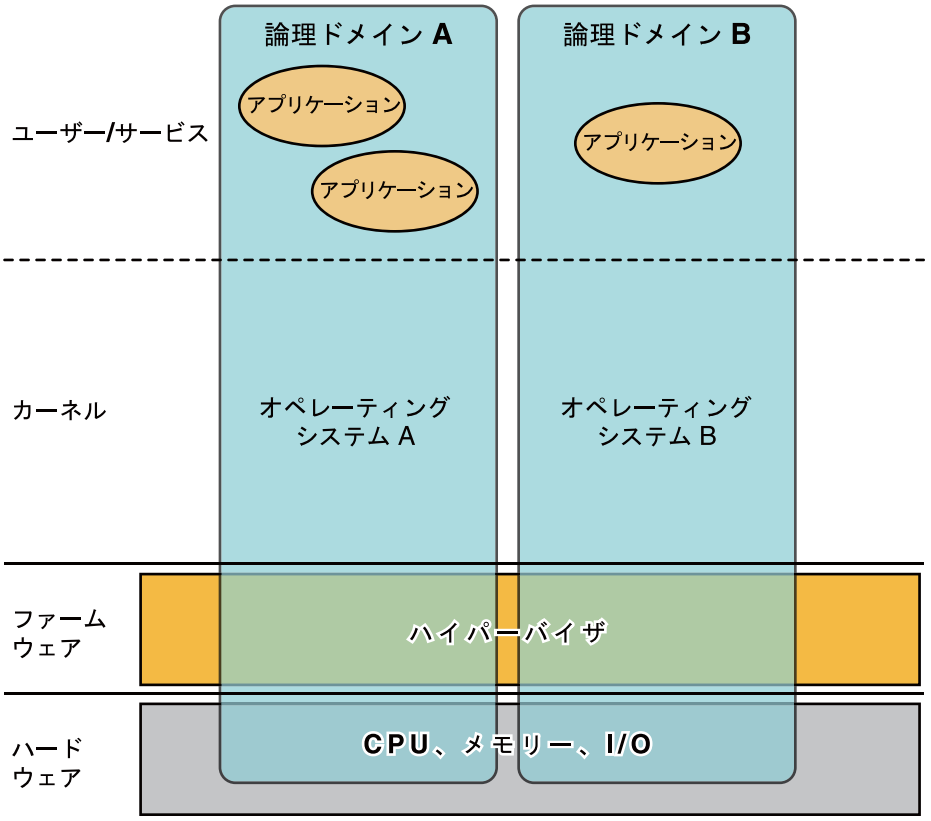
Oracle VM Server for SPARC 製品の概要

Oracle VM Server for SPARC は、Oracle SPARC T シリーズサーバーに高度な効率性とエンタープライズクラスの仮想化機能を提供します。Oracle VM Server for SPARC ソフトウェアを使用すると、最大で 128 台の仮想サーバーを単一のシステム上に作成できます。これは論理ドメインと呼ばれます。こうした構成により、SPARC T シリーズサーバーおよび Oracle Solaris OS が提供する大規模なスレッドを活用できるようになります。

論理ドメインは、個別に論理グループ化されたリソースを含む仮想マシンです。論理ドメインは、単一のコンピュータシステム内で独自のオペレーティングシステムおよび ID を持っています。各論理ドメインは、サーバーの電源の再投入を実行する必要なしに、作成、削除、再構成、およびリブートを単独で行うことができます。異なる論理ドメインでさまざまなアプリケーションソフトウェアを実行でき、パフォーマンスおよび安全性の目的から、これらを独立した状態にしておくことができます。

Oracle VM Server for SPARC ソフトウェアの使用については、『Oracle VM Server for SPARC 3.0 管理ガイド』および『Oracle VM Server for SPARC 3.0 リファレンスマニュアル』を参照してください。必要なハードウェアおよびソフトウェアについては、『Oracle VM Server for SPARC 3.0 リリースノート』を参照してください。

図 1–1　2つの論理ドメインをサポートするハイパーバイザ



Oracle VM Server for SPARC ソフトウェアは次のコンポーネントを使用してシステム仮想化を提供します。

- ハイパーバイザ。ハイパーバイザは小規模なファームウェアレイヤーであり、オペレーティングシステムのインストール先とすることができる、安定した仮想化マシンアーキテクチャーを提供します。ハイパーバイザを使用する Oracle Sun サーバーでは、論理ドメイン上のオペレーティングシステムの動作をハイパーバイザが制御できるようにするためのハードウェア機能が用意されています。

  特定の SPARC ハイパーバイザがサポートするドメインの数と各ドメインの機能は、サーバーによって異なります。ハイパーバイザは、サーバー全体の CPU、メモリー、および I/O リソースのサブセットを特定の論理ドメインに割り当てることができます。この割り当てにより、それぞれが独自の論理ドメイン内にある複数のオペレーティングシステムを同時にサポートできます。別個の論理ドメインの間で、任意の粒度でリソースを再配置できます。たとえば、CPU は CPU スレッド単位で論理ドメインに割り当てることができます。

システムコントローラ (SC) とも呼ばれるサービスプロセッサ (SP) は物理マシンを監視および実行しますが、論理ドメインは管理しません。Logical Domains Manager が論理ドメインを管理します。

- 制御ドメイン。Logical Domains Manager がこのドメインで動作することにより、ほかの論理ドメインを作成および管理したり、仮想リソースをほかのドメインに割り当てることが可能になります。制御ドメインは、サーバーごとに 1 つだけ存在できます。制御ドメインは、Oracle VM Server for SPARC ソフトウェアをインストールするときに最初に作成されるドメインです。制御ドメインの名前は `primary` です。
- サービスドメイン。サービスドメインは、仮想スイッチ、仮想コンソール端末集配信装置 (コンセントレータ)、仮想ディスクサーバーなどの仮想デバイスサービスをほかのドメインに提供します。どのドメインも、サービスドメインとして構成できます。
- **I/O** ドメイン。I/O ドメインは、PCI EXPRESS (PCIe) コントローラ内のネットワークカードなどの物理 I/O デバイスに直接アクセスできます。I/O ドメインは PCIe ルートコンプレックスを所有するか、直接 I/O (Direct I/O、DIO) 機能を使用して PCIe スロットまたはオンボードの PCIe デバイスを所有することができます。『Oracle VM Server for SPARC 3.0 管理ガイド』の「PCIe エンドポイントデバイスの割り当て」を参照してください。

  I/O ドメインは、I/O ドメインがサービスドメインとしても使用される場合に、仮想デバイスの形式でほかのドメインと物理 I/O デバイスを共有できます。
- ルートドメイン。ルートドメインには PCIe ルートコンプレックスが割り当てられます。このドメインは PCIe ファブリックを所有し、ファブリックのエラー処理など、ファブリックに関連するすべてのサービスを提供します。ルートドメインは I/O ドメインでもあり、物理 I/O デバイスを所有し、それらに直接アクセスできます。

  保持できるルートドメインの数は、プラットフォームアーキテクチャーによって決まります。たとえば、Oracle の Sun SPARC Enterprise T5440 サーバーを使用している場合、最大で 4 つのルートドメインを保持できます。
- ゲストドメイン。ゲストドメインは非 I/O ドメインであり、1 つ以上のサービスドメインによって提供される仮想デバイスサービスを利用します。ゲストドメインには物理 I/O デバイスが存在しません。仮想ディスクや仮想ネットワークインタフェースなどの仮想 I/O デバイスのみが存在します。

多くの場合、Oracle VM Server for SPARC システムに存在するただ 1 つの制御ドメインが、I/O ドメインやサービスドメインによって実行されるサービスを提供します。冗長性とプラットフォーム保守性を向上させるには、Oracle VM Server for SPARC システム上で複数の I/O ドメインを構成することを検討してください。

Oracle VM Server for SPARC に適用される一般的なセキュリティー原則

ゲストドメインをさまざまな方法で構成し、ゲストドメインの独立性、ハードウェア共有、およびドメインの接続性をさまざまなレベルで提供できます。これらの要因は Oracle VM Server for SPARC 構成全体のセキュリティーレベルに影響し、次に示す一般的なセキュリティー原則のいくつかを構成に適用できます。

- 攻撃対象領域を最小化する。
  - 運用ガイドラインを作成し、システムのセキュリティーを定期的に評価できるようにすることで、意図しない構成エラーを最小化します。『Secure Deployment of Oracle VM Server for SPARC』の「Counter Measure #1: Operational Guidelines」を参照してください。
  - ドメインの独立性を最大化するために、仮想環境のアーキテクチャーを慎重に計画します。『Secure Deployment of Oracle VM Server for SPARC』の「Threat #2: Errors in the Architecture of the Virtual Environment」で説明されている対応策を参照してください。
  - どのリソースを割り当てるか、またリソースを共有するかどうかを慎重に計画します。『Secure Deployment of Oracle VM Server for SPARC』の「Counter Measure #7: Carefully Assigning Hardware Resources」および「Counter Measure #8: Careful Assignment of Shared Resources」を参照してください。
  - 『Secure Deployment of Oracle VM Server for SPARC』の「Threat #4: Manipulation of the Execution Environment」および「Counter Measure #28: Securing the Guest OS」で説明されている対応策を適用することによって、論理ドメインが不正な操作から確実に保護されるようにします。
  - 必要なときにのみゲストドメインをネットワークに公開します。仮想スイッチを使用して、ゲストドメインのネットワーク接続を適切なネットワークのみに制限できます。
  - 『Oracle Solaris 10 Security Guidelines 』および『Oracle Solaris 11 Security Guidelines 』で説明されている、攻撃対象領域を最小化するための Oracle Solaris 10 および Oracle Solaris 11 向けの手順を実行します。
  - 『Secure Deployment of Oracle VM Server for SPARC』の「Counter Measure #15: Validating Firmware and Software Signatures」および「Counter Measure #16: Validating Kernel Modules」の説明に従って、ハイパーバイザのコアを保護します。
  - 制御ドメインをサービス拒否攻撃から保護します。『Secure Deployment of Oracle VM Server for SPARC』の「Counter Measure #17: Console Access」を参照してください。
  - 承認されていないユーザーが Logical Domains Manager を実行できないようにします。『Secure Deployment of Oracle VM Server for SPARC』の「Threat #8: Unauthorized Use of Configuration Utilities」を参照してください。

- 承認されていないユーザーまたはプロセスがサービスドメインにアクセスできないようにします。『Secure Deployment of Oracle VM Server for SPARC』の「Threat #9: Manipulation of a Service Domain」を参照してください。
- I/O ドメインまたはサービスドメインをサービス拒否攻撃から保護します。『Secure Deployment of Oracle VM Server for SPARC』の「Threat #10: Denial-of-Service of IO Domain or Service Domain」を参照してください。
- 承認されていないユーザーまたはプロセスが I/O ドメインにアクセスできないようにします。『Secure Deployment of Oracle VM Server for SPARC』の「Threat #11: Manipulation of an IO Domain」を参照してください。
- 不必要なドメインマネージャーサービスを無効化します。Logical Domains Manager は、ドメインのアクセス、監視、および移行のためのネットワークサービスを提供します。次に示すネットワークサービスのいずれかが使用されていないときは、そのサービスを無効化します。
  - TCP ポート `8101` 上の移行サービス

    このサービスを無効化するには、`ldmd(1M)` マニュアルページの `ldmd/incoming_migration_enabled` および `ldmd/outgoing_migration_enabled` プロパティーの説明を参照してください。
  - TCP ポート `6482` の XMPP (eXtensible Messaging and Presence Protocol) サポート

    このサービスを無効化するには、『Oracle VM Server for SPARC 3.0 管理ガイド』の「XML トランスポート」を参照してください。
  - UDP ポート `161` の SNMP (Simple Network Management Protocol)

    Oracle VM Server for SPARC 管理情報ベース (MIB) を使用してドメインを監視するかどうかを決定します。この機能を使用するには、SNMP サービスが有効である必要があります。選択に基づいて次のいずれかを実行します。
    - **Oracle VM Server for SPARC MIB** を使用するために **SNMP** サービスを有効化します。安全な方法で Oracle VM Server for SPARC MIB をインストールします。『Oracle VM Server for SPARC 3.0 管理ガイド』の「Oracle VM Server for SPARC MIB ソフトウェアパッケージのインストール方法」および『Oracle VM Server for SPARC 3.0 管理ガイド』の「セキュリティーの管理」を参照してください。
    - **SNMP** サービスを無効化します。このサービスを無効化するには、『Oracle VM Server for SPARC 3.0 管理ガイド』の「Oracle VM Server for SPARC MIB ソフトウェアパッケージを削除する方法」を参照してください。
  - マルチキャストアドレス `239.129.9.27` およびポート `64535` の発見サービス

    Logical Domains Manager デーモン `ldmd` が実行されている間はこのサービスを無効化できません。代わりに、Oracle Solaris の IP フィルタ機能を使用してこのサービスへのアクセスをブロックし、Logical Domains Manager の攻

撃対象領域を最小化します。アクセスをブロックしてユーティリティーの無断使用を防ぐことは、サービス拒否攻撃や、これらのネットワークサービスを悪用しようとするその他の試みへの対抗策として有効です。『Oracle Solaris Administration: IP Services』の第 20 章「IP Filter in Oracle Solaris (Overview)」および『Oracle Solaris Administration: IP Services』の「Using IP Filter Rule Sets」を参照してください。

『Secure Deployment of Oracle VM Server for SPARC』の「Counter Measure #14: Securing the ILOM」および「Counter Measure #20: Hardening LDoms Manager」も参照してください。

- 操作を実行するための最小限の権限を付与します。
  - 同じセキュリティー要件と権限を共有する個別のゲストシステムのグループであるセキュリティークラスにシステムを分離します。単一のセキュリティークラスに属するゲストドメインのみを単一のハードウェアプラットフォームに割り当てることによって、分離ブランチを作成し、ドメインの範囲が別のセキュリティークラスに及ばないようにします。『Secure Deployment of Oracle VM Server for SPARC』の「Counter Measure #2: Carefully Assigning Guests to Hardware Platforms」を参照してください。
  - RBAC を使用して、`ldm` コマンドでドメインを管理する機能を制限します。ドメインを管理する必要があるユーザーのみにこの機能を付与するようにしてください。すべての `ldm` サブコマンドにアクセスする必要があるユーザーには、LDoms Management 権利プロファイルを使用する役割を割り当てます。リスト関連の `ldm` サブコマンドのみにアクセスする必要があるユーザーには、LDoms Review 権利プロファイルを使用する役割を割り当てます。『Oracle VM Server for SPARC 3.0 管理ガイド』の「権利プロファイルと役割の使用」を参照してください。
  - RBAC を使用して、コンソールへのアクセスを、Oracle VM Server for SPARC の管理者がアクセスする必要があるドメインのコンソールにのみ制限します。すべてのドメインに対する汎用アクセスを許可しないでください。『Oracle VM Server for SPARC 3.0 管理ガイド』の「権利プロファイルと役割の使用」を参照してください。
- システムの動作状態を監視します。

  Oracle VM Server for SPARC の監査を有効化します。『Oracle VM Server for SPARC 3.0 管理ガイド』の「監査の有効化と使用」を参照してください。

Oracle VM Server for SPARC ソフトウェアを安全な方法で配備するための推奨事項については、『Secure Deployment of Oracle VM Server for SPARC』の「Recommended Deployment Options」を参照してください。

◆ ◆ ◆ 第 2 章

Oracle VM Server for SPARC の安全なインストールと構成

この章では、Oracle VM Server for SPARC のインストールおよび構成に関連するセキュリティー上の考慮事項について説明します。

インストール

Oracle VM Server for SPARC ソフトウェアは、Oracle Solaris 10 または Oracle Solaris 11 パッケージとして自動的かつ安全にインストールされます。インストールの完了後、役割に基づくアクセス制御 (RBAC)、監査、および承認の各機能をドメインで構成するためには管理者権限が必要です。これらの機能はデフォルトで有効になっていません。

インストール後の構成

Oracle VM Server for SPARC ソフトウェアをインストールしたあとで、使用上のセキュリティーを最大化するために次のタスクを実行します。

- 仮想スイッチ、仮想ディスクサーバー、仮想コンソール端末集配信装置 (コンセントレータ) サービスなど、必要な仮想 I/O サービスを制御ドメインで構成します。『Oracle VM Server for SPARC 3.0 管理ガイド』の第 4 章「サービスおよび制御ドメインの設定」を参照してください。
- ゲストドメインを構成します。『Oracle VM Server for SPARC 3.0 管理ガイド』の第 5 章「ゲストドメインの設定」を参照してください。

  仮想スイッチを使用すると、管理ネットワークおよび本番ネットワークを利用してゲストドメインを構成できます。この場合、本番ネットワークのインタフェースを仮想スイッチのネットワークデバイスとして使用することによって仮想スイッチが作成されます。『Secure Deployment of Oracle VM Server for SPARC』の「Counter Measure #13: Dedicated Management Network」を参照してください。

ゲストドメインの仮想ディスクのいずれかが危険にさらされると、そのドメインのセキュリティーが低下します。したがって、仮想ディスク (ネットワーク接続ストレージ (NAS)、ローカルに格納されたディスクイメージファイル、または物理ディスク) は必ず、セキュリティーで保護された場所に配置してください。

`vntsd` デーモンはデフォルトで無効です。このデーモンが有効になると、制御ドメインにログインしているすべてのユーザーが、ゲストドメインのコンソールに接続することを許可されます。このようなアクセスを防ぐには、`vntsd` デーモンが無効であることを確認するか、または RBAC を使用して、認可されたユーザーのみにコンソール接続アクセスを制限します。

- サービスプロセッサ (SP) はデフォルトで安全に構成されます。Integrated Lights Out Management (ILOM) ソフトウェアを使用した SP の管理については、`http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html` のプラットフォーム別ドキュメントを参照してください。

◆ ◆ ◆ 第 3 章

Oracle VM Server for SPARC のセキュリティー機能

この章では、Oracle VM Server for SPARC ソフトウェアによって使用されるセキュリティー機能の概要を示します。

認証、アクセス制御、および監査については、『Oracle VM Server for SPARC 3.0 管理ガイド』の第 3 章「Oracle VM Server for SPARC のセキュリティー」を参照してください。

セキュリティーモデル

Oracle VM Server for SPARC ソフトウェアは、Oracle Solaris OS に組み込まれたセキュリティーモデルおよび機能を基盤としています。Oracle Solaris OS のセキュリティーガイドラインについては、『Oracle Solaris 11 Security Guidelines 』および『Oracle Solaris 10 Security Guidelines 』を参照してください。

認証の構成と使用

Oracle Solaris のベアメタルインストールと同様に、アカウントを持つすべてのユーザーが、制御ドメインを含む論理ドメインにログインできます。Oracle VM Server for SPARC ソフトウェアはユーザーアカウントを作成しません。『Oracle VM Server for SPARC 3.0 管理ガイド』の「Logical Domains Manager のインストール」を参照してください。Oracle Solaris ユーザーをセキュリティーで保護する方法については、『Oracle Solaris 11 Security Guidelines』の「Securing Users」を参照してください。

Logical Domains Manager を使用して制御ドメインに対するドメイン管理操作を実行するには、構成データの読み取りと書き込みのための特別な権限がユーザーに付与されている必要があります。『Oracle VM Server for SPARC 3.0 管理ガイド』の「Logical Domains Manager プロファイルの内容」および『Oracle VM Server for SPARC 3.0 管理ガイド』の「権利プロファイルと役割の使用」を参照してください。

RBAC の構成と使用

Oracle Solaris OS の役割に基づくアクセス制御 (Role-Based Access Control、RBAC) 機能を使用して、ユーザーアカウントに対する承認と権利プロファイルを管理し、役割を割り当てることができます。RBAC については、『System Administration Guide: Security Services』の第 9 章「Using Role-Based Access Control (Tasks)」を参照してください。

Logical Domains Manager をインストールすると、必要な承認と権利プロファイルがローカルファイルに追加されます。『Oracle VM Server for SPARC 3.0 管理ガイド』の「権利プロファイルと役割の使用」を参照してください。

ネームサービスでユーザー、承認、権利プロファイル、および役割を構成するには、『System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)』を参照してください。

監査の構成と使用

ベアメタルシステムで実行されている Oracle Solaris OS と同じように、ゲストドメイン内の Oracle Solaris インスタンスを管理および監査するようにしてください。Oracle Solaris OS の監査機能をカスタマイズし、特定の環境にとって重要な機能およびシステムサービスのみを監査できます。Oracle VM Server for SPARC では、仮想化ソフトウェアクラスが必ず監査されるようにします。その他の監査関連タスクを実行できます。『Oracle Solaris 11 Security Guidelines』の「Using the Audit Service」および『Oracle Solaris 11 Security Guidelines』の「How to Audit Significant Events in Addition to Login/Logout」を参照してください。

Logical Domains Manager は監査イベントを作成し、格納とその後の検査のために Oracle Solaris の監査サブシステムに渡します。履歴は、何が、いつ、誰によって行われ、どのような影響があるかを示すログに保持されます。システム内のすべてのドメインの監査情報をシステムの制御ドメインから参照することはできません。

そのため、システム内のドメインごとに、システムで実行されている次の Oracle Solaris OS のバージョンに基づいてこの監査機能を有効または無効にできます。

- **Oracle Solaris 10 OS**。`bsmconv` および `bsmunconv` コマンドを使用します。`bsmconv(1M)` マニュアルページおよび`bsmunconv(1M)` マニュアルページと、『Solaris のシステム管理 (セキュリティサービス)』の Oracle Solaris 10 バージョンを参照してください。
- **Oracle Solaris 11 OS**。`audit` コマンドを使用します。`audit(1M)` マニュアルページおよび『Solaris のシステム管理 (セキュリティーサービス)』の Oracle Solaris 11 バージョンを参照してください。

詳細は、『Oracle VM Server for SPARC 3.0 管理ガイド』の「監査の有効化と使用」を参照してください。

その他のセキュリティー機能の構成と使用

Oracle VM Server for SPARC は、特定の仮想化機能の使用をセキュリティーで保護します。有効にした場合、vntsd デーモンはデフォルトでもっとも安全な構成で構成されます。制御ドメインからの接続のみを受け入れ、ネットワーク経由の接続は受け入れません。必要な場合、よりセキュリティーの低いオプションを構成し、ネットワーク接続を許可できます。vntsd(1M) のマニュアルページの vntsd/listen_addr プロパティーの説明を参照してください。

ネットワーク接続を受け入れるように vntsd を構成するときは注意してください。最適なセキュリティーのためにもっとも望ましいのは、制御ドメインからの接続のみを許可するか、または vntsd を無効化することです。13 ページの「Oracle VM Server for SPARC に適用される一般的なセキュリティー原則」を参照してください。

Oracle VM Server for SPARC のドメイン移行機能ではセキュリティー対策を使用します。ソースマシン上の Logical Domains Manager はドメインの移行要求を受け入れ、ターゲットマシン上で実行されている Logical Domains Manager とのセキュアなネットワーク接続を確立します。移行の実行は、この接続が確立されてからです。これらのセキュリティーで保護された接続は、認証および暗号化機能を使用して作成されます。『Oracle VM Server for SPARC 3.0 管理ガイド』の「移行処理のセキュリティー」を参照してください。

特に、ドメイン移行処理では、デフォルトで SSL (Secure Sockets Layer) を使用して、ネットワーク経由で送受信されるすべてのトラフィックを暗号化します。暗号化装置をサポートするシステムの制御ドメインに暗号化装置を割り当てると、移行のパフォーマンスを向上させることができます。

ドメイン移行が必要でないときは、ldmd プロセスが移行ポートで待機しないよう、移行機能を無効にできます。

ドメインの移行を使用する場合は、移行中にパスワード認証を必要とするように ldmd デーモンが構成されていることを確認してください。これはデフォルトの動作です。

◆ ◆ ◆ 第 4 章

4 開発者向けのセキュリティーの考慮事項

この章では、Oracle VM Server for SPARC ソフトウェア向けのアプリケーションを作成する開発者にとって役立つ情報を提供します。

Oracle VM Server for SPARC XML インタフェース

XMPP (eXtensible Messaging and Presence Protocol) を使用する、XML (eXtensible Markup Language) 通信機構によって Oracle VM Server for SPARC ソフトウェアと連携する外部プログラムを作成できます。

攻撃者がこのネットワークプロトコルの弱点を突いてシステムへのアクセスを試みる可能性があるため、XMPP を無効化することの検討が必要な場合があります。XMPP の無効化については、『Oracle VM Server for SPARC 3.0 管理ガイド』の「XML トランスポート」を参照してください。Logical Domains Manager が使用するセキュリティー機構については、『Oracle VM Server for SPARC 3.0 管理ガイド』の「XMPP サーバー」を参照してください。

XMPP を無効にすると、一部の主要な Oracle VM Server for SPARC の機能 (ドメインの移行、メモリーの動的再構成、`ldm init-system` コマンドなど) が使用できなくなることに注意してください。

◆ ◆ ◆ 付 録 A

安全な配備のためのチェックリスト

このチェックリストは、Oracle VM Server for SPARC 環境を強化するために実行できる手順を要約したものです。詳細については次のものを含む各種ドキュメントを参照してください。

- 『Oracle VM Server for SPARC 3.0 管理ガイド』
- 『Oracle Solaris 10 Security Guidelines 』
- 『Oracle Solaris 11 Security Guidelines 』
- Secure Deployment of Oracle VM Server for SPARC

Oracle VM Server for SPARC セキュリティーチェックリスト

- ❒ 仮想化環境でない場合と同様に、Oracle Solaris の強化手順をゲストドメインに対して実行します。
- ❒ LDoms Management および LDoms Review 権利プロファイルを使用して、適切な権限をユーザーに委任します。
- ❒ 役割に基づくアクセス制御 (RBAC) を使用して、コンソールへのアクセスを、Oracle VM Server for SPARC の管理者がアクセスする必要があるドメインのコンソールにのみ制限します。
- ❒ Oracle VM Server for SPARC に対して Oracle Solaris OS の監査機能を有効化します。
- ❒ 不必要なドメインマネージャーサービスを無効化します。
- ❒ 1 つの物理プラットフォームには同じセキュリティークラスのゲストシステムのみを配備します。
- ❒ 実行環境の管理とゲストドメインの間にネットワーク接続がないことを確認します。
- ❒ 必要なリソースのみをゲストシステムに割り当てます。