Red Hat Enterprise Linux 6

仮想化セキュリティーガイド

仮想化環境のセキュリティー保護

Last Updated: 2017-10-12

Red Hat Enterprise Linux 6 仮想化セキュリティーガイド

仮想化環境のセキュリティー保護

Scott Radvan
Red Hat Engineering Content Services
sradvan@redhat.com

Tahlia Richardson
Red Hat Engineering Content Services
trichard@redhat.com

Paul Moore
Red Hat エンジニアリング

Kurt Seifried
Red Hat エンジニアリング

David Jorm
Red Hat エンジニアリング

Thanks go to the following people for enabling the creation of this guide:

法律上の通知

概要

本ガイドは、Red Hat が提供する仮想化セキュリティーテクノロジーについての概要を説明します。仮想化環境内のホスト、ゲスト、および共有インフラストラクチャー/リソースのセキュリティーを保護するための推奨事項を提供します。

目次

第1章 はじめに

1.1. 仮想化環境と非仮想化環境

仮想化環境は、攻撃者にとって以前は価値がなかった新たな攻撃ベクトルの発見と既存のエクスプロイトの洗練の両方の機会を与えます。このため、仮想マシンを作成し、これを維持する際には、物理ホストとそのホスト上で実行されるゲストの両方のセキュリティーを確保するための対策を講じることが重要となります。

非仮想化環境

非仮想化環境では、ホストは物理的に相互分離しており、各ホストには Web サーバーや DNS サーバーなどのサービスで構成される自己完結型の環境があります。これらのサービスは、独自のユーザースペース、ホストカーネル、物理ホストと直接通信して、ネットワークにサービスを直接提供します。下図は、非仮想化環境を示しています。

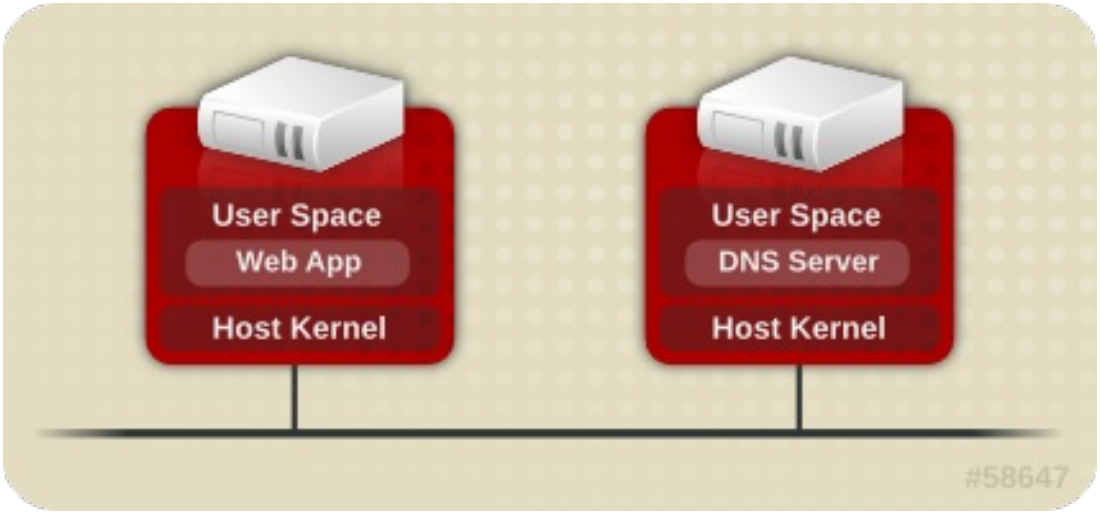


図1.1 非仮想化環境

仮想化環境

仮想化環境では、複数のオペレーティングシステムを (「ゲスト」として) 単一のホストカーネルおよび物理ホストに格納することができます。下図は仮想化環境を示しています。

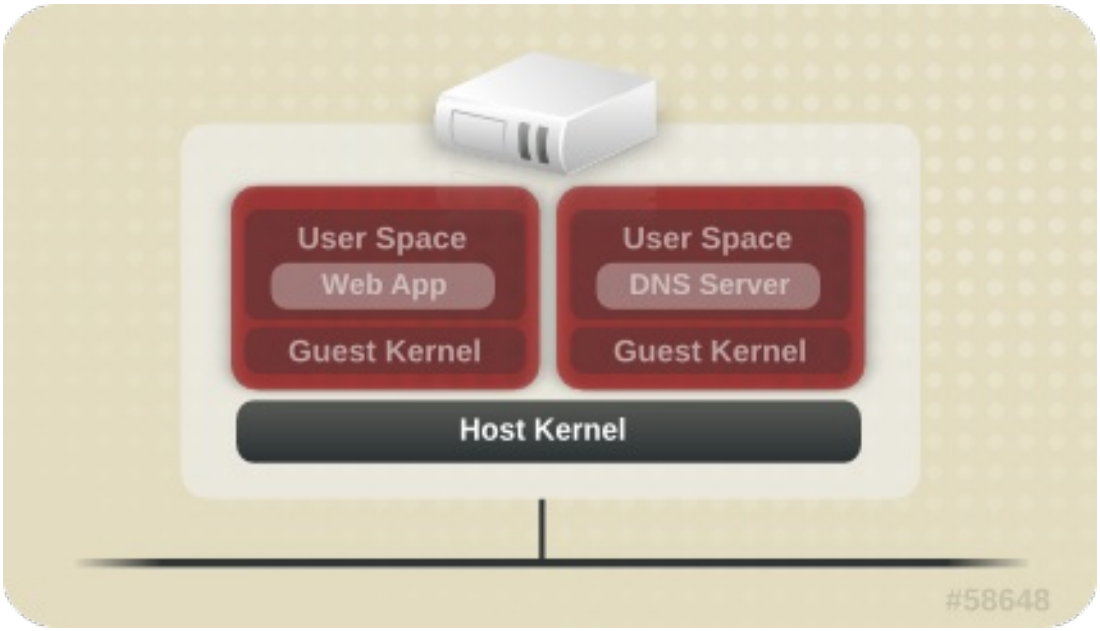


図1.2 仮想化環境

サービスが仮想化されていない場合は、マシンは物理的に分離されています。したがって、エクスプロイトは影響を受けたマシンに抑えられます。ただし、ネットワーク攻撃は明らかな例外となります。仮想化環境内でサービスがグループ化されると、システムの脆弱性が高まります。ハイパーバイザーのセキュリティーに不備がある場合、ゲストインスタンスによるエクスプロイトを受ける可能性があり、そのゲストはホストのみならず、そのホスト上で実行されている他のゲストも攻撃できるようになる可能性があります。これは単に理論上の事柄ではなく、攻撃はすでにハイパーバイザー上に存在しています。それらの攻撃がゲストインスタンスを超えて、他のゲストが攻撃にさらされる可能性もあり得ます。

1.2. 仮想化セキュリティーが重要である理由

インフラストラクチャーに仮想化をデプロイすると、数多くのメリットがもたらされますが、新たなリスクが生じる可能性もあります。仮想化のリソースとサービスのデプロイにあたっては以下のようなセキュリティーに関する考慮事項を検討した上でデプロイを行う必要があります。

- ホスト/ハイパーバイザーは第一のターゲットであり、ゲストとデータの単一障害点となることが多くあります。
- 仮想マシンは望ましくない方法で相互干渉する場合があります。これを防ぐためのアクセス制御が導入されていないとすると、悪意のあるゲストが脆弱なハイパーバイザーをバイパスし、他のゲストのストレージなど、ホストシステム上の他のリソースに直接アクセスする可能性があります。
- 仮想化システムを迅速にデプロイすると、十分なパッチ、モニタリング、メンテナンスなどのリソース管理の必要性が増大するため、リソースとサービスのトラッキングおよび維持管理が難しくなる場合があります。
- 仮想化環境における技術スタッフの知識不足、技能の格差、経験不足などの問題が存在する可能性があります。このような問題は、多くの場合、脆弱性へとつながります。
- ストレージなどのリソースが複数のマシンに散在し、それらのマシンに依存している場合があります。このような場合には環境が過度に複雑化してしまい、システムの管理とメンテナンスが不十分となる可能性があります。

- 仮想化によって、環境内に存在する従来のセキュリティーリスクは排除されません。仮想化レイヤーのみでなく、ソリューションスタック全体のセキュリティーを保護する必要があります。

本ガイドは、仮想化環境のセキュリティー保護に役立つ、Red Hat Enterprise Linux および Red Hat Enterprise Virtualization の仮想化推奨プラクティスの数々をご紹介し、お客様のセキュリティーリスクを軽減することを目的としています。

1.3. SVIRT を使用した SELINUX の活用

sVirt は仮想化を SELinux (Security-Enhanced Linux) によって提供されている既存のセキュリティーフレームワークに組み込むことにより、*強制アクセス制御*(MAC) を仮想マシンに適用します。sVirt の主な目的は、ハイパーバイザーのセキュリティーの脆弱性を利用した攻撃からホストとゲストを保護することです。SELinux は異なるプロセス全体にわたってアクセスポリシーを適用することでシステムを保護します。sVirt は、各ゲストをプロセスとして扱うことによりこの機能をホストとゲストにまで拡張し、悪意のあるゲストが制限付きリソースにアクセスするのを防ぐために設計されたのと同様のポリシーを管理者が適用できるようにします。sVirt についての詳しい情報は 4章*sVirt* を参照してください。

1.4. 他の参考文献

Red Hat では、様々な仮想化製品のドキュメントを豊富に提供しています。Red Hat Enterprise Linux およびその技術を組み込みこんだ仮想化製品については、以下のようなガイドで解説しています。

- 『Red Hat Enterprise Linux 仮想化スタートガイド』: 仮想化の概念、利点、ツールについて概説し、Red Hat の仮想化関連ドキュメントおよび製品の概要を記載しています。
- 『Red Hat Enterprise Linux 仮想化ホスト設定およびゲストインストールガイド』: 仮想化ソフトウェアのインストールおよび仮想化ホスト上のゲストマシンの設定について記載しています。
- 『Red Hat Enterprise Linux 仮想化管理ガイド』: virt-manager または virsh のいずれかを使用した、ホスト、ネットワーク、ストレージ、デバイス、ゲストの管理について説明し、libvirt および QEMU についての参考情報と、トラブルシューティング情報も記載しています。
- 『Red Hat Enterprise Linux 仮想化セキュリティーガイド』: Red Hat が提供する仮想化セキュリティーテクノロジーについての概要を説明しています。また、仮想化環境内のホスト、ゲスト、共有インフラストラクチャー/リソースのセキュリティーを保護するための推奨事項も記載しています。
- 『Red Hat Enterprise Linux 仮想化のチューニングと最適化ガイド』: システムおよびゲスト仮想マシンで、仮想化パフォーマンスの機能とオプションを最大限に活用するためのヒント、コツ、アドバイスを記載しています。
- 『Red Hat Enterprise Linux V2V ガイド』 には、KVM、Xen、および VMware ESX/ESX(i) ハイパーバイザーから Red Hat Enterprise Virtualization および libvirt で管理されている KVM への仮想マシンのインポートについて記載しています。

Red Hat Enterprise Virtualization ドキュメントスイートは、Red Hat Enterprise Virtualization プラットフォームおよび関連製品のインストール、アプリケーション開発、設定、使用方法に関する情報を提供します。

- 『Red Hat Enterprise Virtualization インストールガイド』: Red Hat Enterprise Virtualization 環境を準備し、セットアップする方法、および Red Hat Enterprise Virtualization 環境を最新リリースにアップグレードする方法について記載しています。さらに、ハイパーバイザーをセッ

トアップする方法や、Red Hat Enterprise Virtualization 環境の初期設定を実行する方法についても概説しています。

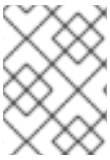
- 『Red Hat Enterprise Virtualization 管理ガイド』: Red Hat Enterprise Virtualization 環境を最初にセットアップした後に設定し、管理する方法について記載しています。これには、ハイパーバイザーやストレージドメイン、および外部プロバイダーを環境に追加する方法や、仮想マシン、仮想ディスクおよびテンプレートなどのリソースを管理する方法、およびバックアップを取る方法や復元する方法などが含まれます。

- 『Red Hat Enterprise Virtualization ユーザーガイド』: 基本タブや拡張タブで提供される機能を含む Red Hat Enterprise Virtualization 環境のユーザーポータルの使い方、仮想マシンおよびテンプレートの作成および使用方法、さらにはリソース使用を監視する方法について記載しています。

- 『Red Hat Enterprise Virtualization テクニカルガイド』: Red Hat Enterprise Virtualization に特有の REST API、Python、Java ソフトウェア開発キット、およびコマンドラインツールの使用方法について記載しています。さらに、Red Hat Enterprise Virtualization の背後にある基盤となる技術コンセプトについて概説しています。

- 『Red Hat Enterprise Virtualization Manager リリースノート』: 現行リリースに固有の Red Hat Enterprise Virtualization Manager に関する情報が記載されています。

- 『Red Hat Enterprise Virtualization テクニカルノート』: 現行リリースと旧リリース間の変更点を記載しています。



注記

これらの製品のガイドはすべて、Red Hat カスタマーポータル: https://access.redhat.com/site/documentation/ で提供しています。

第2章 ホストのセキュリティー

2.1. ホストのセキュリティーが重要である理由

仮想化テクノロジーをデプロイする際、ホストのセキュリティーは最優先事項になります。**Red Hat Enterprise Linux** のホストシステムは、物理デバイス、ストレージ、ネットワークへのアクセスに加えて、すべての仮想化ゲスト自体を管理し、これらを制御します。そのため、ホストシステムのセキュリティーが侵害されると、ホストシステムのみでなくゲストとそのデータまでもが攻撃を受ける可能性があります。

仮想化ゲストのセキュリティーはホストシステムにかかっています。**Red Hat Enterprise Linux** ホストシステムのセキュリティー保護は、セキュアな仮想化プラットフォームの確立に向けた第一歩です。

2.2. RED HAT ENTERPRISE LINUX のホストセキュリティー推奨プラクティス

ホストのセキュリティーは、セキュアな仮想化インフラストラクチャーの極めて重要な要素であるため、以下の推奨プラクティスは **Red Hat Enterprise Linux** ホストシステムのセキュリティー保護の開始点とし役立ちます。

- ゲストシステムの使用と管理のサポートに必要なサービスのみを実行します。ファイルサービスや印刷サービスなどのサービスを追加で提供する必要がある場合には、それらのサービスを **Red Hat Enterprise Linux** ゲストで実行することを検討した方がよいでしょう。

- システムへの直接のアクセスはシステムの管理を行う必要がある人に制限してください。共有の **root** アクセスを無効にして、代わりに **sudo** などのツールを使用して、管理ロールに基づいて管理者に特権的アクセスを付与することを検討してください。

- **SELinux** がご使用のインストールに応じて適切に設定され、**enforcing** モードで稼働していることを確認します。これは、適正なプラクティスである上、**sVirt** によって提供される高度な仮想化セキュリティー機能は **SELinux** に依存しています。**SELinux** と **sVirt** に関する詳しい情報は *4章sVirt* を参照してください。

- ホストシステムで監査が有効化され、**libvirt** が監査レコードを生成するように設定されていることを確認します。監査が有効化されると、**libvirt** はゲストの設定変更および起動/停止イベントの監査レコードを生成します。これは、ゲストの状態をトラッキングするのに役立ちます。また、**libvirt** の監査イベントは、標準の監査ログ検査ツール以外に、専用の **auvirt** ツールでも確認することができます。

- システムのリモート管理はすべてセキュアなネットワークチャネル上のみで実行されるようにしてください。**SSH** のようなツールや、**TLS** または **SSL** などのネットワークプロトコルは認証とデータ暗号化の両方を提供し、承認済みの管理者のみがシステムをリモートで管理できるようにするのに役立ちます。

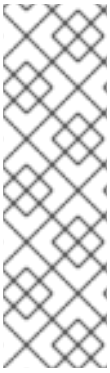
- ご使用のインストールに応じてファイアウォールが適切に設定されており、ブート時にアクティブ化されることを確認します。システムの使用および管理に必要なネットワークポートのみを許可する必要があります。

- ディスク全体またはブロックデバイス (例: **/dev/sdb**) への直接のアクセスをゲストに許可するのは控えて、代わりにゲストストレージにはパーティション (例: **/dev/sdb1**) や **LVM** ボリュームを使用します。

- スタッフが仮想化環境における十分なトレーニングを受けており、知識が十分にあることを確認してください。

警告

SR-IOV が利用不可能な場合に USB デバイス、物理ファンクションまたは物理デバイスを仮想マシンに割り当てると、デバイスのファームウェアを上書きするのに十分なデバイスへのアクセスが提供される場合があります。これにより、攻撃者が悪意のあるコードによってデバイスのファームウェアを上書きし、仮想マシン間でデバイスを移動する際やホストのブート時に問題を生じさせる潜在的なセキュリティー上の問題が提示されます。適用できる場合は、SR-IOV 仮想ファンクションデバイス割り当てを使用することをお勧めします。



注記

本ガイドは、大半の仮想化環境でみられるセキュリティー関連の課題、脆弱性、解決策と推奨される対処方法について説明することを目的としています。ただし、Red Hat Enterprise Linux システムのセキュリティーを保護する際には従うべき推奨プラクティスが数多くあり、これらはスタンドアロン、仮想化ホスト、ゲストインスタンスを問わずに適用されます。これらの推奨プラクティスにはシステム更新、パスワードのセキュリティー、暗号化、ファイアウォールの設定などが含まれます。この情報については、https://access.redhat.com/site/documentation/ の『Red Hat Enterprise Linux セキュリティガイド』で詳しく説明しています。

2.2.1. パブリッククラウドオペレーター向けの特殊な考慮事項

パブリッククラウドサービスオペレーターは、従来の仮想化ユーザーのリスクを超える数多くのセキュリティーリスクにさらされます。悪意のあるゲストの脅威や、仮想化インフラストラクチャー全体にわたる顧客データの機密性および整合性に対する要件により、ホスト/ゲスト間ならびにゲスト間における仮想ゲストの分離は極めて重要となります。

パブリッククラウドオペレーターは上記の Red Hat Enterprise Linux 仮想化推奨プラクティスに加えて、以下の点も考慮する必要があります。

- ゲストからハードウェアへの直接のアクセスを無効にしてください。PCI、USB、FireWire、Thunderbolt、eSATA などのデバイスパススルーメカニズムは、管理を難しくする上、多くの場合は基礎となるハードウェアに依存してゲスト間の分離を強制します。
- クラウドオペレーターのプライベート管理ネットワークを顧客のゲストネットワークと分離して、顧客ネットワークを相互に分離することにより、以下が可能になります。
  - ゲストがネットワークを介してホストシステムにアクセスできないようにする。
  - 顧客がクラウドプロバイダーの内部ネットワークを介して別の顧客のゲストシステムに直接アクセスできないようにする。

2.3. RED HAT ENTERPRISE VIRTUALIZATION のホストセキュリティー推奨プラクティス

2.3.1. Red Hat Enterprise Virtualization のネットワークポート

Red Hat Enterprise Virtualization では、管理用およびその他の仮想化機能用にさまざまなネットワークポートを使用します。Red Hat Enterprise Linux が Red Hat Enterprise Virtualization とともにホスト

として機能するには、これらのポートを開放しておく必要があります。対象のポートと Red Hat Enterprise Virtualization での用途は以下の一覧のとおりです。

- ICMP エコー要求の受信と ICMP エコー応答の送信を許可する必要があります。
- ポート 22 (TCP) は SSH アクセスと初期インストール用に開放する必要があります。
- ポート 161 (UDP) は SNMP (Simple Network Management Protocol) に必要です。
- ポート 5900 から 65535 (TCP) はゲストコンソールアクセスに使用されます。
- ポート 80 または 443 (TCP) は **vdsm-reg** サービスによるホスト情報の通信には、Manager のセキュリティー設定に応じて使用されます。
- ポート 16514 (TLS) またはポート 16509 (TCP) は libvirt によって生成される移行関連の通信をサポートするために使用されます。
- ポート 49152 から 49215 (TCP) は、移行に使用されます。移行には、同時に発生する移行数に応じて、この範囲内の任意のポートを使用することができます。
- VDSM による管理、ストレージ、ホスト間通信には、デフォルトでポート 54321 (TCP) を使用します。このポートは変更可能です。

警告

外部でのデバイス管理が不可欠な場合以外は、ネットワーク境界に位置するポート 161 (UDP) での SNMP のフィルタリングには特に注意を払ってください。

第3章 ゲストのセキュリティー

3.1. ゲストのセキュリティーが重要である理由

ホストシステムのセキュリティーは、そのホスト上で実行されているゲストを確実にセキュリティー保護するために極めて重要となりますが、ホストのセキュリティーによって個別のゲストマシンの適切なセキュリティー保護の必要性がなくなる訳ではありません。システムを仮想化ゲストとして実行する場合、従来の非仮想化システムに関連するセキュリティー上のリスクはすべて依然として存在します。ゲストシステムのセキュリティーが侵害されると、ビジネスデータや顧客の機密情報など、ゲストシステムにアクセス可能なリソースはいずれも攻撃を受けやすくなる可能性があります。

3.2. ゲストセキュリティーの推奨プラクティス

『Red Hat Enterprise Linux セキュリティガイド』 に記載の Red Hat Enterprise Linux システムのセキュリティー保護に関する推奨プラクティスはすべて、従来の非仮想化システムと仮想化ゲストとしてインストールされたシステムの両方に適用されますが、仮想化環境内でゲストを実行する場合に極めて重要となるセキュリティー関連のプラクティスがいくつかあります。

- ゲストの管理はすべてリモートで実行される可能性が高いため、システムの管理は必ずセキュリティー保護されたネットワークチャネルで行うようにしてください。SSH などのツールや TLS または SSL などのネットワークプロトコルは、認証とデータの暗号化の両方を提供し、承認された管理者のみがシステムをリモートで管理できるようにします。

- 一部の仮想化テクノロジーでは、特殊なゲストエージェントまたはドライバーを使用して仮想化固有の機能を有効にします。このようなエージェントやアプリケーションは、Red Hat Enterprise Linux の標準のセキュリティー機能 (例: SELinux) を使用して確実に保護してください。

- 仮想化環境では、ゲストシステムの保護境界線の外部から機密データがアクセスされるリスクがより高くなります。保管されている機密データは **dm-crypt** や **GnuPG** などの暗号化ツールを使用して保護してください。ただし、暗号化キーの機密性の確保には特に注意が必要です。

第4章 SVIRT

4.1. 概要

KVM 下の仮想マシンは Linux プロセスとして実装されているため、KVM は標準の Linux セキュリティーモデルを活用して分離とリソースの制御を行います。Linux カーネルには、米国国家安全保障局によって開発されたプロジェクトである SELinux (Security-Enhanced Linux) が搭載されており、柔軟性の高いカスタマイズ可能なセキュリティーポリシーを通して、強制アクセス制御 (MAC)、マルチレベルセキュリティー (MLS)、およびマルチカテゴリーセキュリティー (MCS) を追加します。SELinux は、Linux カーネル上で実行されるプロセス (仮想マシンプロセスを含む) を対象とした、リソースの厳重な分離および隔離を行います。sVirt プロジェクトは SELinux を基盤として、仮想マシンの分離と制御された共有をさらに促進します。たとえば、粒度の細かいパーミッションを適用して仮想マシンをグループ化し、リソースを共有することができます。

セキュリティーの観点からすると、ハイパーバイザーは攻撃者の格好の的です。これは、ハイパーバイザーがセキュリティー侵害を受けると、そのホストシステム上で実行されている全仮想マシンのセキュリティーも被害を受けることになる可能性があるためです。仮想化テクノロジーに SELinux を組み込むと、ホストシステムや他の仮想マシンへのアクセスを試みる悪意のある仮想マシンに対するハイパーバイザーのセキュリティーを強化するのに役立ちます。

以下の図は、ゲストを分離することによって、セキュリティー侵害されたハイパーバイザー (またはゲスト) がさらなる攻撃を加えたり、別のインスタンスにまで被害を拡げたりする能力を抑える仕組みを示しています。

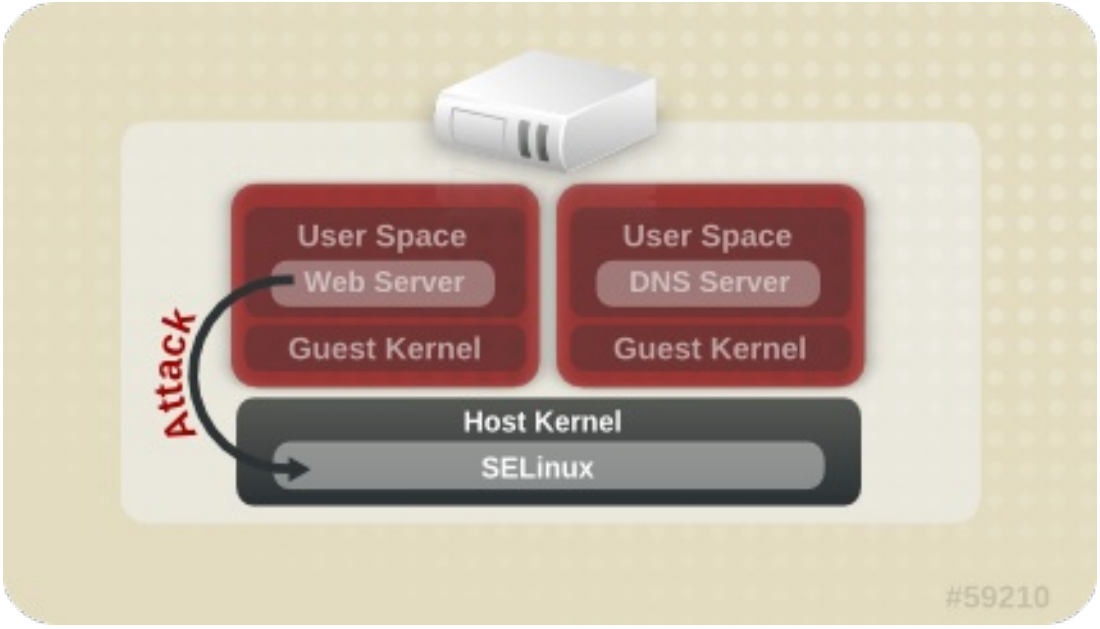


図4.1 SELinux によって分離される攻撃パス

注記

SELinux に関するさらに詳しい情報は、https://access.redhat.com/site/documentation/ の 『Red Hat Enterprise Linux Security-Enhanced Linux』 を参照してください。

4.2. SELINUX と強制アクセス制御 (MAC)

Security-Enhanced Linux (SELinux) は、Linux カーネルにおける MAC の実装です。標準の任意アクセス制御 (DAC) がチェックされたあとに、許可された操作をチェックします。SELinux は、実行中のプ

ロセスとそれらの動作 (例: ファイルシステムオブジェクトへのアクセスを試みるなど) に対して、ユーザーがカスタマイズ可能なセキュリティーポリシーを適用することができます。Red Hat Enterprise Linux では SELinux がデフォルトで有効化されており、アプリケーションやシステムサービス (例: ハイパーバイザー) の脆弱性の悪用によって生じる可能性のある潜在的被害の範囲を制限します。

sVirt は、仮想化管理用の抽象化レイヤーである libvirt と一体化して、仮想マシン用の MAC フレームワークを提供します。このアーキテクチャーは、libvirt によってサポートされている全仮想化プラットフォームと、sVirt によりサポートされている全 MAC 実装が相互運用可能となります。

4.3. SVIRT の設定

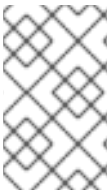
SELinux ブール値は、オン/オフ切り替えが可能な変数で、機能やその他の特殊条件を迅速に有効化/無効化することができます。ブール値は、一時的な変更の場合は **setsebool *boolean_name* {on|off}**、再起動時に変更を永続化する場合は **setsebool -P *boolean_name* {on|off}** のいずれかを実行することによって切り替えることができます。

以下の表は、libvirt で始動された場合に KVM に影響する SELinux ブール値を示しています。これらのブール値 (オンまたはオフ) の現在の状態は、コマンド **getsebool -a|grep virt** を実行することにより確認できます。

表4.1 KVM SELinux のブール値

SELinux のブール値	説明
staff_use_svirt	staff ユーザーが sVirt ドメインを作成し、それに移行することを許可します。
unprivuser_use_svirt	非特権ユーザーが sVirt ドメインを作成し、それに移行することを許可します。
virt_sandbox_use_audit	サンドボックスコンテナーが監査メッセージを送信することを許可します。
virt_sandbox_use_netlink	サンドボックスコンテナーがネットリンクシステム呼び出しを使用することを許可します。
virt_sandbox_use_sys_admin	サンドボックスコンテナーが sys_admin システム呼び出しを使用することを許可します (例: mount)。
virt_transition_userdomain	仮想プロセスがユーザードメインとして実行されることを許可します
virt_use_comm	virt がシリアル/パラレル通信ポートを使用するのを許可します。
virt_use_execmem	制限された仮想マシンが実行可能なメモリーおよび実行可能なスタックを使用することを許可します。
virt_use_fusefs	virt が FUSE マウントされたファイルを読み取るのを許可します。

SELinux のブール値	説明
virt_use_nfs	virt が NFS マウントされたファイルを管理するのを許可します。
virt_use_rawip	virt が rawip ソケットと通信することを許可します。
virt_use_samba	virt が CIFS マウントされたファイルを管理するのを許可します。
virt_use_sanlock	隔離された仮想化ゲストが sanlock と対話するのを許可します。
virt_use_usb	virt が USB デバイスを使用するのを許可します。
virt_use_xserver	仮想マシンが X Window System と対話するのを許可します。



注記

SELinux のブール値についてさらに詳しくは、https://access.redhat.com/site/documentation/ の 『Red Hat Enterprise Linux Security Enhanced Linux』 を参照してください。

4.4. SVIRT のラベル

SELinux の保護下にある他のサービスと同様に、sVirt はプロセスベースのメカニズム、ラベル、制限を使用してセキュリティーを強化し、ゲストインスタンスを制御します。ラベルは、現在実行中の仮想マシンに基づいて、システム上のリソースに自動的に適用されます (動的) が、管理者が手動で指定して (静的)、特別な要件がある場合でも対応することが可能です。

4.4.1. sVirt ラベルのタイプ

以下の表には、仮想マシンのプロセス、イメージファイル、共有コンテンツなどのリソースに割り当てることができる、異なる sVirt ラベルについての説明をまとめています。

表4.2 sVirt ラベル

タイプ	SELinux コンテキスト	説明/効果
仮想マシンプロセス	system_u:system_r:svirt_t:*MCS1*	*MCS1* は無作為に選択されたフィールドです。現在は、約 500,000 のラベルがサポートされています。

タイプ	SELinux コンテキスト	説明/効果
仮想マシンのイメージ	system_u:object_r:svirt_image_t:*MCS1*	これらのイメージファイルやデバイスの読み取り/書き込みができるのは、同じ *MCS1* フィールドが付いた **svirt_t** プロセスのみです。
仮想マシンの共有読み取り/書き込みコンテンツ	system_u:object_r:svirt_image_t:s0	**svirt_t** プロセスはすべて、**svirt_image_t:s0** のファイルおよびデバイスに書き込むことができます。
仮想マシンの共有読み取り専用コンテンツ	system_u:object_r:svirt_content_t:s0	**svirt_t** プロセスはすべて、このラベルがついたファイル/デバイスを読み取ることができます。
仮想マシンのイメージ	system_u:object_r:virt_content_t:s0	イメージが存在する場合に使用されるシステムのデフォルトラベルです。**svirt_t** 仮想プロセスは、このラベルの付いたファイル/デバイスを読み取ることはできません。

4.4.2. 動的設定

動的ラベル設定は、sVirt を SELinux と併用する場合のデフォルトのラベルオプションです。以下の例は、動的ラベリングを示しています。

```
# ps -eZ | grep qemu-kvm

system_u:system_r:svirt_t:s0:c87,c520 27950 ?  00:00:17 qemu-kvm
```

この例では、**qemu-kvm** プロセスに **system_u:system_r:svirt_t:s0** のベースラベルが付いています。libvirt システムは、このプロセス用に一意の MCS ラベル **c87,c520** を生成しています。ベースラベルと MCS ラベルを組み合わせることにより、そのプロセス用の完全なセキュリティーラベルが形成されます。同様に、libvirt は同じ MCS ラベルとベースラベルを使用してイメージラベルを形成します。このイメージラベルは次に、ディスクイメージやディスクデバイス、PCI デバイス、USB デバイス、kernel/initrd ファイルなど、仮想マシンがアクセスする必要のある全ホストファイルに自動的に適用されます。各プロセスは、異なるラベルを使用して、他の仮想マシンから分離されます。

以下の例は、**/var/lib/libvirt/images** 内のゲストディスクイメージに適用された、仮想マシンの一意のセキュリティーラベル (この場合は、対応する MCS ラベルが **c87,c520**) を示しています。

```
# ls -lZ /var/lib/libvirt/images/*

  system_u:object_r:svirt_image_t:s0:c87,c520   image1
```

以下の例は、ゲストの XML 設定内の動的ラベルを示しています。

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_t:s0:c87,c520</label>
```

```
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

4.4.3. ベースラベルを使用した動的設定

デフォルトのダイナミックモードのベースセキュリティーラベルを上書きするには、以下の例に示したように、XML ゲスト設定内の **<baselabel>** オプションを手動で設定することができます。

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <baselabel>system_u:system_r:svirt_custom_t:s0</baselabel>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

4.4.4. 動的リソースラベルを使用した静的設定

一部のアプリケーションは、セキュリティーラベルの生成を完全に制御する必要がありますが、リソースのラベル付けは依然として libvirt が行う必要があります。以下のゲスト XML 設定は、動的リソースラベルを使用した静的設定の例を示しています。

```
<seclabel type='static' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
</seclabel>
```

4.4.5. リソースラベルを使用しない静的設定

MLS (マルチレベルセキュリティー) または厳重に管理された環境で主に使用される、リソース再ラベルを使用しない静的設定が可能です。静的ラベルにより管理者は、仮想マシン用に MCS/MLS フィールドなどの特定のラベルを選択することができます。静的なラベルが付いた仮想マシンを実行する管理者は、イメージファイルに正しいラベルを設定する責任を担います。仮想マシンは常にそのラベルで起動し、sVirt システムは静的なラベルの付いた仮想マシンのコンテンツは決して変更しません。以下のゲスト XML 設定は、このシナリオの例を示しています。

```
<seclabel type='static' model='selinux' relabel='no'>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
</seclabel>
```

第5章 仮想化環境におけるネットワークセキュリティー

5.1. ネットワークセキュリティーの概要

大半の状況では、ネットワークはシステム、アプリケーション、管理インターフェースへの唯一のアクセス方法です。ネットワークは、仮想化システムの管理とそれらのシステムでホストされているアプリケーションの可用性において極めて重要な役割を果たすので、仮想化システムとデータをやり取りするネットワークチャネルをセキュアな状態に確保することは非常に重要です。

ネットワークのセキュリティー保護により、管理者は機密データのアクセスを制御して、情報の漏えいや改ざんから保護することができます。

5.2. ネットワークセキュリティー推奨プラクティス

ネットワークセキュリティーはセキュアな仮想化インフラストラクチャーの重要な要素です。ネットワークのセキュリティー保護については、以下の推奨プラクティスを参照してください。

- システムのリモート管理はすべてセキュアなネットワークチャネル上のみで実行されるようにしてください。SSH のようなツールや、TLS または SSL などのネットワークプロトコルは認証とデータ暗号化の両方を提供し、システムへのセキュアなアクセスとその制御を行います。
- ゲストアプリケーションによる機密データの転送はセキュアなネットワークチャネルで行われるようにします。TLS や SSL などのプロトコルが利用できない場合には、IPsec などを使用することを検討してください。
- ファイアウォールを設定して、ブート時にアクティブ化されるようにします。システムの使用と管理に必要なネットワークポートのみを許可してください。ファイアウォールルールの定期的なテストと確認を行なってください。

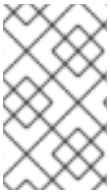
5.2.1. SPICE への接続のセキュリティー保護

SPICE リモートデスクトッププロトコルは SSL/TLS をサポートしています。これは、SPICE のすべての通信チャネル (main、display、inputs、cursor、playback、record) で有効化する必要があります。

5.2.2. ストレージへの接続のセキュリティー保護

仮想化システムのネットワークストレージへの接続は、さまざまな方法で行うことができます。各アプローチにはセキュリティー上のさまざまな利点と懸念点がありますが、セキュリティー上の同一の原則がそれぞれに適用されます。使用前にはリモートのストアプールを認証し、転送中のデータの機密性と整合性を保護します。

データは保管時にもセキュアな状態を維持する必要があります。Red Hat は、データを保管する前に暗号化および/またはデジタル署名することを推奨しています。



注記

ネットワークストレージについてさらに詳しくは、https://access.redhat.com/site/documentation/ にある 『Red Hat Enterprise Linux 仮想化管理ガイド』 のストレージの概念に関する章を参照してください。

付録A 追加情報

A.1. SELINUX および SVIRT

SELinux および sVirt に関する詳細情報:

- SELinux のメイン Web サイト: http://www.nsa.gov/research/selinux/index.shtml
- SELinux のドキュメンテーション: http://www.nsa.gov/research/selinux/docs.shtml
- sVirt のメイン Web サイト: http://selinuxproject.org/page/SVirt
- Dan Walsh 氏のブログ: http://danwalsh.livejournal.com/
- 非公式の SELinux FAQ: http://www.crypt.gen.nz/selinux/faq.html

A.2. 仮想化セキュリティー

仮想化セキュリティーに関する追加情報

- NIST (National Institute of Standards and Technology) 完全仮想化セキュリティーガイドライン: http://www.nist.gov/itl/csd/virtual-020111.cfm

付録B 改訂履歴

改訂 0.4-21.3 **Mon Nov 3 2014** **Aiko Sasaki**
校閲完了

改訂 0.4-21.2 **Fri Oct 31 2014** **Aiko Sasaki**
翻訳完了

改訂 0.4-21.1 **Fri Oct 31 2014** **Aiko Sasaki**
翻訳ファイルを XML ソースバージョン 0.4-21 と同期

改訂 0.4-21 **Fri Oct 10 2014** **Scott Radvan**
6.6 GA リリース向けバージョン

改訂 0.4-20 **Fri Oct 10 2014** **Scott Radvan**
USB および PF セキュリティーの脆弱性に関する警告を追加 (BZ#1150077)。

改訂 0.4-19 **Wed May 14 2014** **Tahlia Richardson**
ブール値の一覧を更新 (BZ#1093284)。
ドキュメンテーション QE フィードバックを適用 (BZ#1093286、BZ#1097058)。

改訂 0.4-18 **Tues Nov 19 2013** **Tahlia Richardson**
6.5 GA リリース向けのバージョン

改訂 0.4-17 **Mon Sept 30 2013** **Tahlia Richardson**
Hypervisor 導入ガイドをドキュメンテーションスイートの一覧から削除。
更新されたドキュメンテーションスイートの一覧および更新されたリンク (以前に変更済み) による発行。

改訂 0.4-16 **Sun Feb 17 2013** **Scott Radvan**
6.4 GA リリース向けバージョン

改訂 0.4-15 **Wed Feb 13 2013** **Scott Radvan**
6.4 リリースのレビュー

改訂 0.4-14 **Tue Jan 22 2013** **Scott Radvan**
『他の参考文献』を「はじめに」に追加。

改訂 0.4-13 **Tue Jan 22 2013** **Scott Radvan**
6.4 リリースのレビュー

改訂 0.4-12 **Sun Nov 25 2012** **Scott Radvan**
ブール値に関する説明が 'semanage boolean -l' コマンドで表示される情報と一致するように変更。

改訂 0.4-11 **Sun Oct 28 2012** **Scott Radvan**
サブタイトルを修正。

改訂 0.4-10 **Tue Oct 16 2012** **Scott Radvan**
6.4 に関する正確性をレビュー。

改訂 0.4-9 **Thu Sep 27 2012** **Scott Radvan**
新規ドキュメンテーションサイトへのリンクを修正。

改訂 0.4-08 **Fri Jul 20 2012** **Laura Bailey**
ドキュメントが用語の使用ポリシーに適合していることを確認。

改訂 0.4-07 **Sun Jun 17 2012** **Scott Radvan**

6.3 GA リリースに向けて発行。

改訂 0.4-06 **Fri Jun 15 2012** **Scott Radvan**
Draft の透かしを削除し、6.3 ブランチ用に準備。

改訂 0.4-05 **Fri Jun 08 2012** **Scott Radvan**
静的ラベルの出力例を並べ替え。

改訂 0.4-04 **Fri Jun 08 2012** **Scott Radvan**
SME のレビューにしたがって若干修正。

改訂 0.4-03 **Tue Jun 05 2012** **Scott Radvan**
QE レビューからの修正を追加 (BZ#828032)。

改訂 0.4-02 **Mon Jun 04 2012** **Scott Radvan**
追加情報の章を追加し、寄稿者とリンクを記載。

改訂 0.4-01 **Mon Jun 04 2012** **Scott Radvan**
メジャーバージョンアップ、校正および若干の編集。

改訂 0.2-06 **Wed May 30 2012** **Scott Radvan**
「第 5 章 - 仮想化環境におけるネットワークセキュリティー」の初回執筆。

改訂 0.2-05 **Tue May 15 2012** **Scott Radvan**
ゲスト内における root アクセスが望ましくない旨の記述を Guest_Security.xml に追加。

改訂 0.2-04 **Mon May 14 2012** **Scott Radvan**
ネットワーク境界における SNMP についての警告を追加。

改訂 0.2-03 **Mon May 14 2012** **Scott Radvan**
「ゲストセキュリティー」のセクションを追加。ネットワークポートのセクションを拡張して、エコー要求 (ping) および TCP/UDP について記載。パブリッククラウドの推奨事項にパススルーメカニズムについての追加情報を記載。ブール値のセクションを拡張し、マウント済みファイルシステムについて記述。

改訂 0.2-02 **Tue May 08 2012** **Scott Radvan**
『概要」を「はじめに」に変更。

改訂 0.2-01 **Tue May 08 2012** **Scott Radvan**
メジャーバージョンアップ。「ホストのセキュリティー」の章に SME からの情報を追加し、編集および校正。

改訂 0.1-15 **Thu Mar 29 2012** **Scott Radvan**
「Red Hat Enterprise Virtualization のネットワークポート」のセクションを Host_Security.xml にインポート。

改訂 0.1-14 **Thu Mar 29 2012** **Scott Radvan**
ベストプラクティスのセクションのタイトルを変更。ベストプラクティスという用語を置き換え。

改訂 0.1-13 **Wed Mar 28 2012** **Scott Radvan**
新たなパブリッシングツールチェーンを使用してビルド。

改訂 0.1-12 **Mon Mar 20 2012** **Scott Radvan**
SME レビューに向け、新セクション「1.2. 仮想化セキュリティーが重要である理由」を初めて公開。

改訂 0.1-11 **Mon Mar 20 2012** **Scott Radvan**
「Red Hat Enterprise Linux のホストセキュリティーベストプラクティス」を「ホストセキュリティー」の章に移動。

改訂 0.1-10 **Mon Mar 20 2012** **Scott Radvan**
SME の協力の下で目次を大幅に再編成。

改訂 0.1-09 **Mon Feb 14 2012** **Scott Radvan**
序文の表現

改訂 0.1-08 **Mon Feb 13 2012** **Scott Radvan**
新バージョンのパブリッシングツール

改訂 0.1-07 **Tue Feb 01 2012** **Scott Radvan**
sVirt の章を SME レビュー向けに発行。

改訂 0.1-06 **Tue Jan 31 2012** **Scott Radvan**
Draft の透かしを追加し、作成段階/社外秘の状態である旨を付記。

改訂 0.1-05 **Mon Jan 30 2012** **Scott Radvan**
「はじめに」の章に追記。sVirt のラベルのセクションを配置。本ガイドでは記載していないシステムのセキュリティー強化トピックについての勧告を追加。

改訂 0.1-04 **Mon Jan 30 2012** **Scott Radvan**
sVirt の章の表現を若干変更。「第 1 章: はじめに」を再編成し、フローを改善。

改訂 0.1-03 **Fri Jan 20 2012** **Scott Radvan**
sVirt の章をさらに再編成。開発者からの初回のフィードバックと修正の取り込み。

改訂 0.1-02 **Tue Jan 17 2012** **Scott Radvan**
文書のフローを大幅に再編成。一貫性のあるファイル名に変更。

改訂 0.1-01 **Tue Jan 17 2012** **Scott Radvan**
初版作成。既存のテキストとコメントをインポート。