



Cisco Security Manager 4.2 展開計画ガイド

OL-25358-01-J

【注意】 シスコ製品をご使用になる前に、安全上の注意 (www.cisco.com/jp/go/safety_warning/) をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

概要

本書では、Cisco Security Manager 4.2 サーバの展開計画に関するガイドラインについて説明します。このマニュアルは、推奨されるサーバハードウェア、クライアントハードウェア、リファレンスネットワークに基づいたサイジングおよびソフトウェア、Security Manager、Security Manager サーバの高度なチューニング オプションに含まれているアプリケーションセットの展開オプションとライセンスングに関する内容で構成されています。Security Manager のソフトウェア機能の詳細については、<http://www.cisco.com/go/csmanager> の製品マニュアルを参照してください。

このマニュアルは、『*User Guide for Cisco Security Manager 4.2*』や『*Installation Guide for Cisco Security Manager 4.2*』など、Security Manager の他のユーザ マニュアルを補足するものです。

Cisco Security Manager 4.2 のアプリケーション

Cisco Security Manager 4.2 のインストールには、次のアプリケーションが含まれます。

- 「[Configuration Manager](#)」
- 「[Event Viewer](#)」
- 「[Report Manager](#)」

Configuration Manager

Configuration Manager を使用すると、250 以上のさまざまなタイプおよびモデルの Cisco セキュリティ デバイス上でセキュリティ ポリシーを集中管理できます。Security Manager は、次のデバイス全体で、ファイアウォール、IPS、および VPN（サイト間、リモート アクセス、および SSL）サービスの統合プロビジョニングをサポートします。

- IOS/ISR/ASR ルータ
- Catalyst スイッチ
- ASA および PIX セキュリティ アプライアンス
- ファイアウォール、VPN、および IPS に関連する Catalyst Service Module
- IPS アプライアンス、およびルータと ASA デバイスに関するさまざまなサービス モジュール

Security Manager でサポートされるデバイスおよび OS バージョンの一覧については、Cisco.com で『[Supported Devices and Software Versions for Cisco Security Manager](#)』を参照してください。

Event Viewer

高パフォーマンスで、使い勝手の良い統合 Event Viewer を使用すると、IPS、ASA、および FWSM デバイスからイベントを集中監視し、関連する設定ポリシーに相互に関連付けることができます。このことは、問題の特定や、設定のトラブルシューティングに役立ちます。さらに、Configuration Manager を使用して、設定を調整し、展開することができます。Event Viewer は、Cisco ASA、IPS、および FWSM デバイスのイベント管理をサポートします。

プライマリ イベント データ ストアだけでなく、拡張イベント データ ストアにイベントをコピーして格納できます。拡張イベント データ ストアは、大量のイベントのバックアップおよびアーカイブに使用できます。これは、Event Viewer がプライマリ イベント データ ストアと拡張イベント データ ストアの両方からイベント データを収集できる場合、イベントの履歴のレビューおよび分析に役立ちます。拡張イベント データ ストアは、Security Manager の管理設定でイベント管理を有効にできます。

サポートされているプラットフォームと詳細については、Cisco.com で『[User Guide for Cisco Security Manager 4.2](#)』の「Monitoring and Diagnostics」を参照してください。

Report Manager

この新しい統合型の Report Manager アプリケーションでは、ASA、IPS、および Remote Access VPN レポートの生成とスケジュール作成を実行できます。ASA および IPS デバイスのレポートは、Event Viewer で収集されたイベントを集約することによって作成されます。Security レポートは、管理対象デバイスによって報告されたネットワークの使用状況やセキュリティの問題を効率的に監視、追跡、および監査できます。ユーザは、Report Manager を使用して、Cisco ASA および IPS デバイスのレポートを作成およびカスタマイズできます。

サポートされているプラットフォームと詳細については、Cisco.com で『*User Guide for Cisco Security Manager 4.2*』の「Monitoring and Diagnostics」を参照してください。

Common Services 3.3

Common Services は、データ ストレージ、Web ログイン ポータル、ユーザ ロール定義、アクセス権限、セキュリティ プロトコル、およびナビゲーション用のフレームワークを提供します。また、インストール、データ管理、イベントおよびメッセージ処理、およびジョブおよびプロセス管理用のフレームワークも提供します。Common Services には、アプリケーションにとって必要なサーバ側のコンポーネントが用意されています。具体的には次のものが含まれています。

- SSL ライブラリ
- 組み込み型 Sybase SQL データベース
- Apache Web サーバ
- Tomcat サブレット エンジン
- CiscoWorks Web ポータル
- バックアップ/復元機能
- RBAC の機能。Common Services によって提供される RBAC 機能には、次のものがあります。
 - RBAC と組み合わされているローカル認証
 - 外部 AAA サーバ (ACS および AD など) と統合するための追加機能

Common Services は、Security Manager に含まれているすべてのアプリケーションにとって必要です。Common Services 3.3 の詳細については、http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.3/user/guide/cs_33_ug.html のマニュアルを参照してください。

Auto Update Server 4.2

AUS を使用して、自動アップデート機能を使用している PIX Security Appliance (PIX) および Adaptive Security Appliance (ASA) デバイス上のデバイス コンフィギュレーション ファイルおよびソフトウェア イメージをアップグレードすることができます。AUS は、デバイス設定、設定アップデート、デバイス OS アップデート、および定期設定確認に使用可能な設定のプル モデルをサポートします。加えて、自動アップデート機能と組み合わせて動的 IP アドレスを使用するサポート対象デバイスは、AUS を使用してコンフィギュレーション ファイルをアップグレードしたり、デバイス情報とステータス情報を渡したりできます。

この方法では、Security Manager は定期的な間隔、特定の日付と時間、およびオンデマンドのタイミングで、設定のアップデートを AUS サーバへ展開し、管理対象のデバイスは、新しい設定のアップデートをダウンロードするよう AUS サーバに連絡します。

AUS は、リモートセキュリティ ネットワークのスケラビリティを向上させ、リモートセキュリティ ネットワークの維持コストを削減し、アドレス指定されたリモート ファイアウォールを動的に管理できるようにします。

AUS はブラウザベースのグラフィカル ユーザ インターフェイスを使用しており、Common Services 3.3 が必要です。AUS の詳細については、<http://www.cisco.com/go/csmanager> のマニュアルを参照してください。

Resource Manager Essentials 4.3

ライフサイクル管理をサポートするために、RME には、デバイス インベントリと監査変更、コンフィギュレーション ファイル、ソフトウェア イメージ、および（設定のアーカイブおよびトラッキングのための）基本的な syslog 分析を管理する機能が備わっています。64 ビット OS がサポートされるようにするには、RME のインストールを、Security Manager 4.2 にバンドルされている RME パッケージから行う必要があります。CiscoWorks LAN Management Solution (LMS) に付属の RME には、64 ビット OS との互換性がありません。

RME はブラウザベースのグラフィカル ユーザ インターフェイスを使用しており、Common Services 3.3 が必要です。RME の詳細については、http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2073/products_data_sheets_list.html のデータシートを参照してください。

RME をサポートしているデバイスの情報は、http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2073/products_device_support_tables_list.html で入手できます。

Performance Monitor 4.2

Performance Monitor は、セキュリティ デバイスとセキュリティ サービスに重点を置いたヘルスおよびパフォーマンス モニタ アプリケーションです。Performance Monitor は、ネットワークのパフォーマンスの問題が重大になる前に事前に検出する機能をサポートしており、オーバーロード状態のネットワークの部分や、潜在的に余分なリソースを必要とするネットワークの部分の特定を支援し、ヘルスとパフォーマンスに関する豊富な履歴情報を事後調査と分析に提供します。Performance Monitor は、モニタリングのリモートアクセス VPN、サイト間 VPN、ファイアウォール、Web サーバ ロードバランシング、および SSL 終了をサポートしています。Performance Monitor はブラウザベースのグラフィカル ユーザ インターフェイスを使用しており、Common Services 3.3 が必要です。

Performance Monitor の詳細については、<http://www.cisco.com/go/csmanager> のマニュアルを参照してください。

関連アプリケーション

Security Manager に統合して追加の機能とメリットを提供するその他のアプリケーションがシスコから提供されています。

Cisco Secure Access Control Server (ACS) 4.2.x

Security Manager ユーザの認証および許可に対して ACS を使用するために、オプションで Security Manager を設定することができます。ACS は、ロールベース アクセス コントロール (RBAC)、および特定のデバイス セットにユーザを制限する機能に基づいて、きめ細かいロールについてのカスタム ユーザ プロファイルの定義をサポートしています。

Security Manager と ACS の統合の設定については、『[Installation Guide for Cisco Security Manager 4.2](#)』を参照してください。ACS の詳細については、<http://www.cisco.com/go/acs> を参照してください。

Cisco CNS Configuration Engine 3.5 および 3.5(1)

Security Manager は、デバイスの設定を展開するためのメカニズムとして、Cisco Configuration Engine 3.5 および 3.5(1) の使用をサポートしています。Security Manager は、差分コンフィギュレーション ファイルを Cisco Configuration Engine に渡して、保存を依頼し、デバイスから読み取れるようにします。Cisco IOS ルータ、および Dynamic Host Configuration Protocol (DHCP) サーバを使用する PIX ファイアウォールや ASA ファイアウォールなどのデバイスは、設定（およびイメージ）のアップデートについて Cisco Configuration Engine に通知します。Security Manager は、CNS コンフィギュレーション エンジンを通じてスタティック IP アドレスを持っているデバイスの管理もサポートします。このような場合には、検出はライブで行われ、デバイスへの展開は CNS コンフィギュレーション エンジンを通じて行われます。

Configuration Engine の詳細については、<http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/index.html> を参照してください。

ハードウェアおよびソフトウェアの最小要件

各 Cisco Security Manager サーバのインストールには、ポリシー、イベント、およびレポート管理用の専用の物理サーバまたは仮想マシンが 1 台必要です。Auto Update Server、Performance Monitor、Resources Manager Essentials などのオプションのコンポーネントは、同じシステムにインストールすることも、別のシステムにインストールすることもできます。

表 1 は、Cisco Security Manager サーバ ソフトウェア、および他のオプションのモジュールをインストールする場合のハードウェアとソフトウェアの最小仕様を示しています。Security Manager ソフトウェアは、最小仕様を備えたシステムにインストールできますが、この場合のパフォーマンスと容量は、より小規模な展開（最大 25 のデバイスを管理）に制限されます。より大規模な展開については、「推奨されるハードウェアおよびソフトウェア仕様」の項で推奨されている仕様で物理サーバを使用する必要があります。

表 1 サーバの最小ハードウェアとソフトウェア

サーバの最小ハードウェア	
推奨サーバ	Cisco UCS C210 M2 または同等品
CPU	1 x Intel Xeon Four-core 5600 シリーズ この Four-core (quad-core) CPU は最小です。コア数が多くなると、パフォーマンスがさらに向上します。
メモリ (RAM)	<p>Security Manager のすべての機能を使用するには、最小 16 GB が必要です。メモリがそれ以下の場合、イベント管理やレポート管理などの機能が影響を受けます。</p> <p>特に、オペレーティング システムが使用できる RAM の容量が 8 GB 未満であると、Event Viewer および Report Manager がインストール中に無効化されます。</p> <p>OS が使用できるメモリが 8 ~ 12 GB の場合は、Event Viewer および Report Manager を使用しないと判断し、オフにすることができます。このようなシステムでは、コンフィギュレーション管理は便利です。</p> <p>推奨はされませんが、インストールの完了後に Security Manager クライアントからロー メモリ システムに対して Event Viewer および Report Manager をイネーブルにできます ([Tools] > [Security Manager Administration] > [Event Management] を選択)。ロー メモリ システム上で Event Viewer および Report Manager をイネーブルにすると、アプリケーション全体のパフォーマンスに深刻な影響が及ぶ可能性があることに注意してください。</p> <p>AUS、RME、または Performance Monitor を別のサーバにインストールする場合は、次の最小要件が適用されます。</p> <ul style="list-style-type: none"> • AUS または Performance Monitor 専用のサーバ : 4 GB。4 GB 以上を推奨します。 • RME 専用のサーバ : 3 GB

表 1 サーバの最小ハードウェアとソフトウェア (続き)

ハードドライブスペース	<p>必要なディスク領域の確保に適した HDD の組み合わせ (以下を参照) を使用します。</p> <ul style="list-style-type: none"> OS パーティションには、100 GB を推奨します。 アプリケーション (Security Manager) パーティションには、150 GB を推奨します。Security Manager のインストールのみに必要な最小空きディスク領域は 5 GB です。この容量を満たしていない場合は、インストールは中断されます。 <p>(注) OS とアプリケーションを別々のパーティションにインストールすることを強くお勧めします。</p> <p>(注) Veritas を HA (ハイ アベイラビリティ) モードで使用する場合は、上記のアプリケーションパーティション、およびその他のすべてのイベントストアパーティションには当てはまらない場合があります。詳細については、該当する Security Manager のハイ アベイラビリティに関するマニュアル (http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html)、および Veritas マニュアルを参照してください。</p> <ul style="list-style-type: none"> 別個のパーティション上にある Event Viewer のログストレージ用に追加の 1.0 TB : これは、Event Viewer を使用する予定がある場合にのみ必要です。このパーティションは、直接接続されている記憶装置上に作成することを推奨します。 追加の 1.0 TB 以上 : これは、イベント記録を有効にする場合にのみ必要です。イベント記録機能は、(長期の保存などのために) プライマリストレージの容量を超えるログストレージが必要な場合に、イベントのセカンダリストレージを作成します。セカンダリイベントストアのサイズは、設定したプライマリストレージのサイズよりも大きくする必要があります。したがって、イベント記録を使用するには、追加の 1.0 TB 以上のディスク領域が必要です。プライマリ イベントストアとセカンダリ イベントストアは両方とも SAN 上に置くことができますが、最適なパフォーマンスを達成するためには、直接接続されているストレージ (DAS) 上にプライマリ ストアを作成することをお勧めします。 <p>パフォーマンスをさらに向上させるには、RAID 10 を推奨します。必要に応じて、RAID 5 を使用できます。</p> <p>ヒント</p> <p>連続 10,000 イベント/秒 (EPS) の場合は、1 日に約 86 GB の圧縮ディスクスペースが消費されます。イベントストア (プライマリ/セカンダリ) に割り当てられたディスク領域の 90% がいっぱいになった段階で、ログロールオーバーが発生します。ディスクのサイズが小さいほど、ロールオーバーの発生が早くなります。予想 EPS レートとロールオーバー要件に基づいて、イベント管理の使用時に最小ディスクサイズを増減できます。</p>
サポートされているデバイス	最大 25 台
ネットワークアダプタ	1 Gbps
サーバの最小ソフトウェア	
オペレーティングシステム	<p>Microsoft Windows 2008 Enterprise Server 64 ビット版 SP2</p> <p>Microsoft Windows 2008 Enterprise Server 64 ビット版 R2</p>

表 2 は、Cisco Security Manager クライアント ソフトウェアのインストールのためのハードウェアとソフトウェアの最小仕様を示しています。Security Manager クライアント ソフトウェアは専用のマシンにインストールすることをお勧めします。

表 2 クライアントの最小ハードウェアとソフトウェア

クライアントの最小ハードウェア	
CPU	デュアルコア 2.0 GHz 以上
メモリ	2 GB 以上推奨
HDD	10 GB の空き容量
表示	1280 x 1024
ネットワーク アダプタ	1 Gbps
クライアントの最小ハードウェア	
オペレーティング システム	Windows XP SP3、Windows Vista SP2、Windows 2003/2008 Enterprise Server SP2、Windows 2008 Enterprise R2、Windows 7
ブラウザ	次のいずれかです。 <ul style="list-style-type: none"> • Internet Explorer 7.0 • Internet Explorer 8.0 (互換表示でのみサポート) ヒント 互換表示を使用するには、Internet Explorer 8 を開いて、[Tools] > [Compatibility View Settings] に移動し、[website to be displayed in Compatibility View] として Security Manager サーバを追加します。
	Firefox 3.6.x

仮想マシンのハードウェアおよびソフトウェア要件

仮想マシンのハードウェアおよびソフトウェア要件については、表 3 の「VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開」を参照してください。

推奨されるハードウェアおよびソフトウェア仕様

単一プロセッサ (コア) サーバから複数プロセッサ (コア) サーバへ移行する場合には、Security Manager を使用するとパフォーマンスの改善が見られます。このリリースでの新しいイベント管理、レポート管理、およびその他の新機能については、最適なパフォーマンスを得るために、適切なハードウェアおよびソフトウェア仕様を使用することをお勧めします。また、将来の拡張用にサーバのサイジングもお勧めします。

最良のパフォーマンスを得るためには、最小要件として、2.66 MHz Intel Xeon quad-core プロセッサ (Hyper-Threading 機能あり) 以上を備えた Security Manager サーバが推奨されます。イベント管理を使用する場合には、Security Manager アプリケーションに対して専用のハード ディスクまたはストレージ ボリュームを用意すること、およびイベント ストレージに対して専用のディスクまたはボリュームを用意することを強くお勧めします。Security Manager クライアント システムでは、このマニュアルの「ハードウェアおよびソフトウェアの最小要件」の項に記載されているハードウェアの最小仕様を使用できます。

次の仕様は、さまざまな規模の展開に対して、Security Manager サーバで推奨される仕様を示しています。

- 「VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開」
- 「小規模な企業での展開」
- 「中規模な企業での展開」
- 「大規模な企業での展開」

これらの仕様は、デバイス数に基づいてこのような展開をサポートするための、適切なハードウェアおよびソフトウェアの一般的なガイドラインです。このマニュアルの「展開シナリオ」で説明している他の要因によっては、パフォーマンスの結果が異なる場合があります。Security Manager に対するこれらのハードウェアおよびソフトウェア要件は、Security Manager を新しくインストールする場合も、Security Manager の古いバージョンからバージョン 4.2 にアップグレードする場合も同じです。

VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開

VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開で推奨される Security Manager の仕様は、表 3 に示してあります。

表 3 VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開

(注)	VMware のパフォーマンスは、同じホスト システム上の他の VM によって生成される負荷によってゲートされます。そのため、これらの VM のサイジングの数字は、他の VM による大きな負荷が掛かっていないシステムに基づいた数字になります。
推奨されるホストサーバ	Cisco UCS C210 M2 または同等品
UCS 部品番号	R210-2121605W
仮想 CPU	6 vCPU vCPU を増やすと、パフォーマンスが向上します。
メモリ (RAM)	<p>Security Manager のすべての機能を使用するには、最小 16 GB が必要です。メモリがそれ以下の場合、イベント管理やレポート管理などの機能が影響を受けます。</p> <p>特に、オペレーティング システムが使用できる RAM の容量が 8 GB 未満であると、Event Viewer および Report Manager がインストール中に無効化されます。</p> <p>OS が使用できるメモリが 8 ~ 12 GB の場合は、Event Viewer および Report Manager を使用しないと判断し、オフにすることができます。このようなシステムでは、コンフィギュレーション管理は便利です。</p> <p>推奨はされませんが、インストールの完了後に Security Manager クライアントからローメモリシステムに対して Event Viewer および Report Manager をイネーブルにできます ([Tools] > [Security Manager Administration] > [Event Management] を選択)。ローメモリシステム上で Event Viewer および Report Manager をイネーブルにすると、アプリケーション全体のパフォーマンスに深刻な影響が及ぶ可能性があることに注意してください。</p> <p>AUS、RME、または Performance Monitor を別のサーバにインストールする場合は、次の最小要件が適用されます。</p> <ul style="list-style-type: none"> • AUS または Performance Monitor 専用のサーバ : 4 GB。4 GB 以上を推奨します。 • RME 専用のサーバ : 3 GB

表 3 VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開 (続き)

<p>ハードドライブスペース</p>	<p>必要なディスク領域の確保に適した HDD の組み合わせ (以下を参照) を使用します。</p> <ul style="list-style-type: none"> OS パーティションには、100 GB を推奨します。 アプリケーション (Security Manager) パーティションには、150 GB を推奨します。Security Manager のインストールのみに必要な最小空きディスク領域は 5 GB です。この容量を満たしていない場合は、インストールは中断されます。 <p>(注) OS とアプリケーションを別々のパーティションにインストールすることを強くお勧めします。</p> <p>(注) Veritas を HA (ハイ アベイラビリティ) モードで使用する場合は、上記のアプリケーションパーティション、およびその他のすべてのイベントストアパーティションには当てはまらない場合があります。詳細については、該当する Security Manager のハイアベイラビリティに関するマニュアル (http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html)、および Veritas マニュアルを参照してください。</p> <ul style="list-style-type: none"> 別個のパーティション上にある Event Viewer のログストレージ用に追加の 1.0 TB : これは、Event Viewer を使用する予定がある場合にのみ必要です。このパーティションは、直接接続されている記憶装置上に作成することを推奨します。 追加の 1.0 TB 以上 : これは、イベント記録を有効にする場合にのみ必要です。イベント記録機能は、(長期の保存などのために) プライマリストレージの容量を超えるログストレージが必要な場合に、イベントのセカンダリストレージを作成します。セカンダリイベントストアのサイズは、設定したプライマリストレージのサイズよりも大きくする必要があります。したがって、イベント記録を使用するには、追加の 1.0 TB 以上のディスク領域が必要です。プライマリイベントストアとセカンダリイベントストアは両方とも SAN 上に置くことができますが、最適なパフォーマンスを達成するためには、直接接続されているストレージ (DAS) 上にプライマリストアを作成することをお勧めします。 <p>パフォーマンスをさらに向上させるには、RAID 10 を推奨します。必要に応じて、RAID 5 を使用できます。</p> <p>ヒント</p> <p>連続 10,000 イベント/秒 (EPS) の場合は、1 日に約 86 GB の圧縮ディスクスペースが消費されます。イベントストア (プライマリ/セカンダリ) に割り当てられたディスク領域の 90% がいっぱいになった段階で、ログロールオーバーが発生します。ディスクのサイズが小さいほど、ロールオーバーの発生が早くなります。予想 EPS レートとロールオーバー要件に基づいて、イベント管理の使用時に最小ディスクサイズを増減できます。</p>
<p>ホスト サーバの HDD RAID</p>	<p>VM 内の RAID は、基礎となるホストシステムの HDD 構成に加えて、仮想化されたファイルシステムが使用されるため、当てはまりません。また、ソフトウェアベースの RAID は、VMware ESX VM では使用できません。詳細については、VMware, Inc. 発行のマニュアルを参照してください。</p>
<p>ネットワークアダプタ</p>	<p>1 Gbps</p>

表 3 VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開 (続き)

オペレーティング システム	Microsoft Windows 2008 Enterprise Server 64 ビット版 SP2 Microsoft Windows 2008 Enterprise Server 64 ビット版 R2
推奨されるサイジング	
デバイスの最大数	最大 25 台
サポートされる最大累積 EPS	5000 イベント/秒 (この値は、syslogs と IPS SDEE の比率 9:1 (つまり、4500 syslog + 500 SDEE) です)
最大同時利用者数	同時利用者は多くても 2 人 (コンフィギュレーションのみのユーザが 1 人と、イベント画面およびレポート画面を使用するユーザが 1 人)

小規模な企業での展開

表 4 に、小規模な企業での展開用に推奨される Security Manager サーバの仕様を示します。

表 4 小規模な企業での展開

推奨サーバ	Cisco UCS C210 M2 または同等品
UCS 部品番号	R210-2121605W
CPU	1 x Hex Core (X5670 または同等シリーズを推奨)
メモリ (RAM)	<p>Security Manager のすべての機能を使用するには、最小 16 GB が必要です。メモリがそれ以下の場合、イベント管理やレポート管理などの機能が影響を受けます。</p> <p>特に、オペレーティング システムが使用できる RAM の容量が 8 GB 未満の場合は、イベント管理および Report Manager がインストール中に無効化されます。</p> <p>OS が使用できるメモリが 8 ~ 12 GB の場合は、イベント管理およびレポート管理を使用しないと判断し、オフにすることができます。このようなシステムでは、コンフィギュレーション管理は便利です。</p> <p>推奨はされませんが、インストールの完了後に Security Manager クライアントからローメモリシステムに対してイベント管理およびレポート管理をイネーブルにできます ([Tools] > [Security Manager Administration] > [Event Management] を選択)。ローメモリシステム上でイベント管理およびレポート管理をイネーブルにすると、アプリケーション全体のパフォーマンスに深刻な影響が及ぶ可能性があることに注意してください。</p> <p>AUS、RME、または Performance Monitor を別のサーバにインストールする場合は、次の最小要件が適用されます。</p> <ul style="list-style-type: none"> • AUS または Performance Monitor 専用のサーバ : 4 GB。4 GB 以上を推奨します。 • RME 専用のサーバ : 3 GB

表 4 小規模な企業での展開 (続き)

<p>ハードドライブスペース</p>	<p>必要なディスク領域の確保に適した HDD の組み合わせ (以下を参照) を使用します。</p> <ul style="list-style-type: none"> OS パーティションには、100 GB を推奨します。 アプリケーション (Security Manager) パーティションには、150 GB を推奨します。Security Manager のインストールのみに必要な最小空きディスク領域は 5 GB です。この容量を満たしていない場合は、インストールは中断されます。 <p>(注) OS とアプリケーションを別々のパーティションにインストールすることを強くお勧めします。</p> <p>(注) Veritas を HA (ハイ アベイラビリティ) モードで使用する場合は、上記のアプリケーションパーティション、およびその他のすべてのイベントストアパーティションには当てはまらない場合があります。詳細については、該当する Security Manager のハイ アベイラビリティに関するマニュアル (http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html)、および Veritas マニュアルを参照してください。</p> <ul style="list-style-type: none"> 別個のパーティション上にある Event Viewer のログストレージ用に追加の 1.0 TB : これは、Event Viewer を使用する予定がある場合にのみ必要です。このパーティションは、直接接続されている記憶装置上に作成することを推奨します。 追加の 1.0 TB 以上 : これは、イベント記録を有効にする場合にのみ必要です。イベント記録機能は、(長期の保存などのために) プライマリストレージの容量を超えるログストレージが必要な場合に、イベントのセカンダリストレージを作成します。セカンダリ イベントストアのサイズは、設定したプライマリストレージのサイズよりも大きくする必要があります。したがって、イベント記録を使用するには、追加の 1.0 TB 以上のディスク領域が必要です。プライマリ イベントストアとセカンダリ イベントストアは両方とも SAN 上に置くことができますが、最適なパフォーマンスを達成するためには、直接接続されているストレージ (DAS) 上にプライマリストアを作成することをお勧めします。 <p>パフォーマンスをさらに向上させるには、RAID 10 を推奨します。必要に応じて、RAID 5 を使用できます。</p> <p>ヒント</p> <p>連続 10,000 イベント/秒 (EPS) の場合は、1 日に約 86 GB の圧縮ディスクスペースが消費されます。イベントストア (プライマリ/セカンダリ) に割り当てられたディスク領域の 90% がいっぱいになった段階で、ログロールオーバーが発生します。ディスクのサイズが小さいほど、ロールオーバーの発生が早くなります。予想 EPS レートとロールオーバー要件に基づいて、イベント管理の使用時に最小ディスクサイズを増減できます。</p>
<p>ネットワークアダプタ</p>	<p>1 Gbps</p>
<p>オペレーティングシステム</p>	<p>Microsoft Windows 2008 Enterprise Server 64 ビット版 SP2 Microsoft Windows 2008 Enterprise Server 64 ビット版 R2</p>

表 4 小規模な企業での展開 (続き)

推奨されるサイジング	
デバイスの最大数	最大 100 台
サポートされる最大累積 EPS	5000 イベント/秒 (この値は、syslogs と IPS SDEE の比率 9:1 (つまり、4500 syslog + 500 SDEE) です)
最大同時利用者数	同時利用者は多くても 4 人 (コンフィギュレーションのみのユーザが 2 人と、イベント画面およびレポーティング画面を使用するユーザが 2 人)

中規模な企業での展開

表 5 に、中規模な企業での展開用に推奨される Security Manager サーバの仕様を示します。

表 5 中規模な企業での展開

推奨サーバ	Cisco UCS C210 M2 または同等品
UCS 部品番号	R210-2121605W
CPU	1 x Hex Core (X5670 または同等シリーズを推奨)
メモリ (RAM)	<ul style="list-style-type: none"> Configuration Manager のみを使用する場合は 16 GB すべての機能を使用する場合は 24 GB
ハードドライブスペース	<p>必要なディスク領域の確保に適した HDD の組み合わせ (以下を参照) を使用します。</p> <ul style="list-style-type: none"> OS パーティションには、100 GB を推奨します。 アプリケーション (Security Manager) パーティションには、150 GB を推奨します。Security Manager のインストールのみに必要な最小空きディスク領域は 5 GB です。この容量を満たしていない場合は、インストールは中断されます。 <p>(注) OS とアプリケーションを別々のパーティションにインストールすることを強くお勧めします。</p> <p>(注) Veritas を HA (ハイアベイラビリティ) モードで使用する場合は、上記のアプリケーションパーティション、およびその他のすべてのイベントストアパーティションには当てはまらない場合があります。詳細については、該当する Security Manager のハイアベイラビリティに関するマニュアル (http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html)、および Veritas マニュアルを参照してください。</p> <ul style="list-style-type: none"> 別個のパーティション上にある Event Viewer のログストレージ用に追加の 1.0 TB : これは、Event Viewer を使用する予定がある場合にのみ必要です。このパーティションは、直接接続されている記憶装置上に作成することを推奨します。 追加の 1.0 TB 以上 : これは、イベント記録を有効にする場合にのみ必要です。イベント記録機能は、(長期の保存などのために) プライマリストレージの容量を超えるログストレージが必要な場合に、イベントのセカンダリストレージを作成します。セカンダリイベントストアのサイズは、設定したプライマリストレージのサイズよりも大きくする必要があります。したがって、イベント記録を使用するには、追加の 1.0 TB 以上のディスク領域が必要です。プライマリイベントストアとセカンダリイベントストアは両方とも SAN 上に置くことができますが、最適なパフォーマンスを達成するためには、直接接続されているストレージ (DAS) 上にプライマリストアを作成することをお勧めします。 <p>パフォーマンスをさらに向上させるには、RAID 10 を推奨します。必要に応じて、RAID 5 を使用できます。</p> <p>ヒント</p> <p>連続 10,000 イベント/秒 (EPS) の場合は、1 日に約 86 GB の圧縮ディスクスペースが消費されます。イベントストア (プライマリ/セカンダリ) に割り当てられたディスク領域の 90% がいっぱいになった段階で、ログロールオーバーが発生します。ディスクのサイズが小さいほど、ロールオーバーの発生が早くなります。予想 EPS レートとロールオーバー要件に基づいて、イベント管理の使用時に最小ディスクサイズを増減できます。</p>

表 5 中規模な企業での展開 (続き)

ネットワークアダプタ	1 Gbps
オペレーティングシステム	Microsoft Windows 2008 Enterprise Server 64 ビット版 SP2 Microsoft Windows 2008 Enterprise Server 64 ビット版 R2
推奨されるサイジング	
デバイスの最大数	最大 200 台
サポートされる最大累積 EPS	10,000 イベント/秒 (この値は、syslogs と IPS SDEE の比率 9:1 (つまり、9000 syslog + 1000 SDEE))
最大同時利用者数	同時利用者は多くても 7 人 (コンフィギュレーションのみのユーザが 5 人と、イベント画面およびレポート画面を使用するユーザが 2 人)

大規模な企業での展開

表 6 に、大規模な企業での展開用に推奨される Security Manager サーバの仕様を示します。

表 6 大規模な企業での展開

推奨サーバ	Cisco UCS C210 M2 または同等品
UCS 部品番号	R210-2121605W
CPU	2 x Hex Core (X5670 または同等シリーズを推奨)
メモリ (RAM)	<ul style="list-style-type: none"> Configuration Manager のみを使用する場合は 24 GB すべての機能を使用する場合は 32 GB

表 6 大規模な企業での展開 (続き)

<p>ハードドライブスペース</p>	<p>必要なディスク領域の確保に適した HDD の組み合わせ (以下を参照) を使用します。</p> <ul style="list-style-type: none"> OS パーティションには、100 GB を推奨します。 アプリケーション (Security Manager) パーティションには、150 GB を推奨します。Security Manager のインストールのみに必要な最小空きディスク領域は 5 GB です。この容量を満たしていない場合は、インストールは中断されます。 <p>(注) OS とアプリケーションを別々のパーティションにインストールすることを強くお勧めします。</p> <p>(注) Veritas を HA (ハイ アベイラビリティ) モードで使用する場合は、上記のアプリケーションパーティション、およびその他のすべてのイベントストアパーティションには当てはまらない場合があります。詳細については、該当する Security Manager のハイ アベイラビリティに関するマニュアル (http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html)、および Veritas マニュアルを参照してください。</p> <ul style="list-style-type: none"> 別個のパーティション上にある Event Viewer のログストレージ用に追加の 1.0 TB : これは、Event Viewer を使用する予定がある場合にのみ必要です。このパーティションは、直接接続されている記憶装置上に作成することを推奨します。 追加の 1.0 TB 以上 : これは、イベント記録を有効にする場合にのみ必要です。イベント記録機能は、(長期の保存などのために) プライマリストレージの容量を超えるログストレージが必要な場合に、イベントのセカンダリストレージを作成します。セカンダリ イベントストアのサイズは、設定したプライマリストレージのサイズよりも大きくする必要があります。したがって、イベント記録を使用するには、追加の 1.0 TB 以上のディスク領域が必要です。プライマリ イベントストアとセカンダリ イベントストアは両方とも SAN 上に置くことができますが、最適なパフォーマンスを達成するためには、直接接続されているストレージ (DAS) 上にプライマリストアを作成することをお勧めします。 <p>パフォーマンスをさらに向上させるには、RAID 10 を推奨します。必要に応じて、RAID 5 を使用できます。</p> <p>ヒント</p> <p>連続 10,000 イベント/秒 (EPS) の場合は、1 日に約 86 GB の圧縮ディスクスペースが消費されます。イベントストア (プライマリ/セカンダリ) に割り当てられたディスク領域の 90% がいっぱいになった段階で、ログロールオーバーが発生します。ディスクのサイズが小さいほど、ロールオーバーの発生が早くなります。予想 EPS レートとロールオーバー要件に基づいて、イベント管理の使用時に最小ディスクサイズを増減できます。</p>
<p>ネットワークアダプタ</p>	<p>1 Gbps</p>
<p>オペレーティングシステム</p>	<p>Microsoft Windows 2008 Enterprise Server 64 ビット版 SP2 Microsoft Windows 2008 Enterprise Server 64 ビット版 R2</p>

表 6 大規模な企業での展開 (続き)

推奨されるサイジング	
デバイスの最大数	最大 500 台
サポートされる最大累積 EPS	10,000 イベント/秒 (この値は、syslogs と IPS SDEE の比率 9:1 (つまり、9000 syslog + 1000 SDEE))
最大同時利用者数	同時利用者は多くても 10 人 (コンフィギュレーションのみのユーザが 5 人と、イベント画面およびレポート画面を使用するユーザが 5 人)



(注) イベント記録を有効にする場合は、プライマリストアと同サイズまたはそれ以上の追加のストレージ容量が必要です。



(注) 上記のサイジングのガイドラインは、平均 3000 ~ 5000 のルールを持つファイアウォールデバイスに基づいています。ルール数がこれよりも大幅に多い場合は、展開でサポートされるデバイスの数を減らすか、すぐ上のハードウェアを考慮する必要があります。

展開シナリオ

Security Manager アプリケーションについては、さまざまな展開が考えられます。展開のシナリオを決定する場合には、システムのパフォーマンスに影響を与える可能性のある、次の重要な要因について考慮する必要があります。

Security Manager は何台のデバイスを管理できますか。

各 Security Manager のインストールには、管理するデバイスの数にハードリミットはありませんが、Security Manager サーバごとに 500 デバイス未満にすることを推奨します (推奨されるハードウェアとソフトウェアを使用している場合)。1 台のサーバ当たりの適切なデバイス数を管理するには、前の項に記載されている推奨仕様に従う必要があります。管理対象デバイスが非常に大きな構成になっている場合には、デバイスの数は少なくなることがあります。たとえば、多数のファイアウォールデバイスが 20,000 ~ 50,000 のルールを持つ場合、大量の IPS シグニチャセットを持つ場合、または数千の支店で大規模かつ複雑な VPN ポリシーを持つ場合には、Security Manager の実行で実現できるパフォーマンスが準最適を下回ることがあります。多数のデバイスおよびネットワークを管理するには、必要に応じて複数の Security Manager サーバを展開する必要があります。

複数の Security Manager サーバにわたって、ポリシー、オブジェクト、およびデバイスをどのように管理できますか。

共有されているポリシー、オブジェクト、およびデバイスは、Policy Export/Import 機能を使用して、ある Security Manager サーバから別の Security Manager サーバにエクスポート/インポートできます。この機能を使用すると、共有されているポリシーやオブジェクトを複数のサーバにわたって簡単に同期できます。また、必要に応じて、管理対象デバイスのあるサーバから別のサーバに移行 (移動) するのにも使用できます。

Security Manager では、どのようなタイプのデバイスが管理されますか。デバイスのタイプによってパフォーマンスも変わりますか。

多くのタイプのデバイスを Security Manager で管理できますが、最も多く見られるのはファイアウォール、IPS センサー、VPN デバイスで、この種のデバイスは、さまざまなタイプのデバイスでパフォーマンスがどのように異なるかを示す良い例となります。

他のタイプのデバイスよりもポリシー変更が頻繁に必要なタイプのデバイスもあります。たとえば、ファイアウォールや IPS センサーなどのデバイスは、VPN デバイスよりもポリシー変更が頻繁に必要です。したがって、ファイアウォールや IPS センサーは、VPN デバイスよりもはるかに多くのリソースを必要とします。そのため、通常、Security Manager はファイアウォールまたは IPS 環境よりも VPN 環境でより多くのデバイスを管理できます。

構成の一般的なサイズはどのくらいですか。

小規模な環境では、一般的なサイズは 100 ～数千行です。中規模な環境では、一般的なサイズは 1000 ～ 5000 の ACL ですが、大規模な環境では、5000 ～ 50,000 以上の ACL になることがあります。より規模の大きい環境では、将来的な成長に対して十分な余裕を確保しておくために、1 台の Security Manager サーバ当たりのデバイス数を減らすことを考慮する必要があります。

Security Manager はいくつのイベントを管理できますか。ファイアウォールおよび IPS ロギングの正しい設定はどのようなものですか。

イベント管理は、多数のユーザおよびデバイスを持つ大規模な環境において、特に大量のシステムリソースを消費することがあります。適切なハードウェアおよびソフトウェアの仕様を備えた 1 つの Security Manager サーバでは、1 秒間に最大 10,000 のイベントを管理できますが、運用に必要な重要ログだけを送信するようにデバイスを設定することをお勧めします。ファイアウォールデバイスで推奨されるロギングレベルは 0（緊急）～5（通知）です。0 では、Security Manager に送信されるログの量が最小になります。追加のロギングについては、トラブルシューティングおよびデバッグの目的で必要なときのために、1 つのデバイスに対して常に有効にしておくことができます。ロギングのレベルで 7（デバッグ）または 6（情報）を使用する場合は注意してください。これらは、必要に応じてデバイスのコンソールまたは Device Manager のみでオンにして、使用後はオフにする必要があります。IPS デバイスでは、シグニチャの設定を、Low（低）、Medium（中）、High（高）、または Informational（情報）から調整できます。これらの設定は環境によって異なり、システムパフォーマンスに影響を与えることがあります。詳細については、IPS 設定ガイドを参照してください。

何人のユーザがこれらのアプリケーションを使用しますか。

アクティブなユーザセッションはサーバに負荷をかけるため、展開のサイズを決定する場合には、要因として考慮する必要があります。たとえば、あるアプリケーションではデバイス数が上限に達することはないが、同時ユーザセッション数のために最大負荷近くなることもある場合は、1 台のサーバをそのアプリケーション専用にすることが妥当です。Security Manager は 5 人を超える同時ユーザをサポートしますが、ユーザは Event Viewer 内の最大 5 つのリアルタイム イベントビューをいつでも開くことができます。Event Server は、自身に接続している Event Viewer のインスタンスの数を制限しませんが、アクティブなすべての Event Viewer にわたる同時リアルタイム イベントビューの数に 5 というハードリミットを設定します。

Security Manager に含まれているアプリケーションのうち、どのアプリケーションを展開する必要がありますか。

(Auto Update Server や RME などの) アプリケーションは、サイトの障害または機能停止の場合でも、可用性を高くしておいたり、運用を継続させたりする必要がありますか。専用サーバにインストールされている特定のアプリケーションで、規模の制限に達した場合には、複数のアプリケーションインスタンスを異なるサーバへ展開することを考慮する必要があります。

アプリケーションパフォーマンスに影響を与える要因

アプリケーションのパフォーマンスに影響を与える要因には、多くのものがあります。具体的には次のものがありますが、これ以外にも考えられます。

- サーバおよびクライアントのハードウェア（プロセッサ、メモリ、ストレージのテクノロジーなど）。
- 管理対象デバイスの数、およびデバイスのタイプ、デバイスの複雑さ、構成のサイズ（多数のACLなど）。
- イベント管理エンジン、管理デバイスによって報告されるイベントボリューム、およびログレベル。
- ポリシーオブジェクトの数と複雑さ。
- 同時ユーザの数と、それらのユーザが実行している特定のアクティビティ。
- デバイスの数が多い場合の、コンフィギュレーションの展開頻度、またはIPSシグニチャのアップデート頻度。
- 展開ジョブ内のデバイスの数。
- ネットワークの帯域幅と遅延（Security Manager クライアントとサーバ間、サーバと管理対象デバイス間など）。
- VMware ESX などの仮想テクノロジーの使用。
- AAA サービスに対する ACS サーバの使用。
- スケジュール済みレポートの数。
- レポートエンジン、管理対象デバイスによって報告されるイベントボリューム、およびイベント集約。

Security Manager クライアントとサーバが地理的にかなり離れていると、遅延が生じて、クライアントの応答性が低下することがあります。たとえば、カリフォルニアにあるサーバで、インドにあるクライアントを使用することは、大きな遅延が生じるため推奨されません。このような場合には、クライアントがサーバと同じデータセンター内（または、少なくとも近隣）に設置される、リモートデスクトップまたはターミナルサーバ配置を採用することをお勧めします。

単一サーバのインストール

単一サーバは、最も簡単な展開シナリオで、Security Manager の対象のアプリケーションをすべて同じサーバにインストールします。ネットワークのセキュリティ管理者が1人、または2人の小規模なセキュリティ環境では、通常は単一サーバの展開で十分です。

複数サーバのインストール

デバイスが数百台または数千台あるような大規模な環境では、単一サーバですべてのデバイスを効率よく管理できないことがあります。パフォーマンス上の理由から、Security Manager の対象のアプリケーションを複数のサーバ間に展開することを選択できます。アプリケーション配布の例としては、たとえば次のようになります。

サーバ A：ファイアウォール ポリシーおよびデバイス管理

- Common Services
- Security Manager
- イベント/ログ モニタリング

- Report Manager
- Auto Update Server (オプション)

サーバ B : IPS ポリシーおよびデバイス管理

- Common Services
- Security Manager
- イベント/ログ モニタリング
- Report Manager

サーバ C : VPN ポリシーおよびデバイス管理

- Common Services
- Security Manager
- イベント/ログ モニタリング
- Report Manager

サーバ A は、すべての ASA/PIX/FWSM ファイアウォール デバイスのコンフィグレーションおよびイベント管理専用です。サーバ B は、すべての IPS デバイスのコンフィグレーションおよびイベント管理専用で、サーバ C は、ASA/IOS/ISR VPN デバイスの VPN ポリシー管理専用です。サーバ C は、ファイアウォール デバイスは VPN トポロジの一部であるため、ファイアウォール デバイスの管理も行います。この展開方法では、各サーバはそれ自身の中ではほとんど同じポリシー データしか使用しないため、サーバ間でポリシー データを共有する必要性はほとんどありません。ただし、**Security Manager** サーバと管理デバイスが非常に離れた場所に展開されているようなネットワークでは、この展開は適していません。このようにすると、モニタリング、設定の検出、および展開に影響を与えることがあります。

もうひとつの方法として、地域ごとにデバイスを分けて、各 **Security Manager** は、地域内（米国西部、米国中部、米国東部、ヨーロッパ、アジアなど）の少数のデバイスのみを管理する、というものがあります。この方法では、管理コンソール、イベント モニタリング、および管理デバイスの設定展開について、ローカルな **Security Manager** サーバから最適なパフォーマンスを提供できます。

複数のサーバ展開では、ポリシーのインポート/エクスポート機能を使用して、共有ポリシーおよびオブジェクトを異なるサーバ間でエクスポートおよびインポートできます。ポリシーのインポート/エクスポートを使用して、デバイスを別のサーバに移行（移動）することもできます。これは、さまざまなサーバの多数のデバイスにわたってポリシーとオブジェクトの同期を保持しながら、管理をスケールアップするのに役立ちます。

大規模な小売店舗での展開

業種別小売店舗に見られるような大規模なルータ展開を持つ顧客には、管理についての選択肢が複数あります。通常、このような環境では、高度に分散化されたモデルに展開された多数のルータがあります。これらの環境に対する管理を必要とする顧客に推奨されるのは、Cisco CNS Configuration Engine (<http://www.cisco.com/en/US/products/sw/netmgts/ps4617/index.html>) および Cisco Virtual Office MEVO (<http://www.cisco.com/en/US/netsol/ns855/index.html>) を高度にスケーラブルなソリューションであると評価することです。

Security Manager でのイベント管理が必要ない環境（CS-MARS またはサードパーティのログ管理を使用）では、イベント管理エンジンをオフにして、ポリシー管理のパフォーマンスを改善できますが、その場合には、Event Server とともに Report Manager も無効化されます。

VMware の仮想マシン環境でのインストール

Security Manager は、VMware ESX 4.1 および VMware ESXi 4.1 での動作をサポートしています。VMware Server や VMware Workstation などの VMware の他の環境はサポートしていません。

VMware のゲスト オペレーティング システムとして、Security Manager でサポートされている任意のサーバ オペレーティング システムを使用できます。VMware の認定作業では、通常の仮想化されていないサーバ上で稼動している Security Manager で実行されたものと同じパフォーマンス テストおよび耐久性テストを行う必要がありました。テスト結果として、VMware ESX Server 4.0 で Security Manager を実行すると、イベント管理機能をオンにしない場合、アプリケーション パフォーマンスが少し低下することがわかりました。これは、関連するリファレンス ネットワークのサイズや、特定のテスト ケースによって異なります。VMware 環境で Security Manager を展開することは、小さいサイズのネットワークにのみ適しています。

パフォーマンスが常に大きく低下するようなエリアでは、多数の (約 5,000 ~ 50,000 の) ルールを使用して、多数の PIX デバイス、ASA デバイス、またはデバイスへの展開を行っていました。このような場合には、展開にかかる時間が、容認できる範囲を超えてしまいます。VMware のパフォーマンスのベスト プラクティスについては、次のマニュアル

(http://www.vmware.com/pdf/Perf_Best_Practices_vSphere4.1.pdf) を参照してください。

ただし、通常、デフォルトの値または設定は最適になっているため、詳細な VMware パラメータは調整すべきではありません。

また、仮想化の効率を向上させることに特化して設計されたテクノロジーが含まれているプロセッサを使用した、最新世代のサーバを使用することが推奨されます。たとえば、Intel® Virtualization Technology (IVT) が含まれている Intel® Xeon® X5500 シリーズの Quad-core プロセッサ上で、VMware ESX Server 4.0 で実行している Security Manager をテストした場合には、良好な結果が得られました。AMD は、仮想化の機能拡張に対して 64 ビット x86 アーキテクチャ プロセッサを提供しており、これは AMD Virtualization (AMD-V) と呼ばれます。

仮想マシンのハードウェアおよびソフトウェア要件については、表 3 の「VMware ESX 4.1 または VMware ESXi 4.1 による小規模な展開」を参照してください。

ハイ アベイラビリティ / 障害回復

Security Manager をハイ アベイラビリティまたは障害回復の構成に展開して、サーバ、ストレージ、ネットワーク、またはサイトの障害時にアプリケーションの可用性および存続可能性を大幅に向上させることができます。これらの展開オプションについては、適用可能な Security Manager ハイ アベイラビリティに関するマニュアル

(http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html) および Veritas マニュアルに詳しい説明が記載されています。

設置に関する注意事項

Security Manager のインストールの詳細については、『*Installation Guide for Cisco Security Manager 4.2*』を参照してください。

インストール可能なモジュール

Security Manager サーバのインストールには、さまざまなコンポーネントが含まれており、いくつかのコンポーネントはオプションになっています。Security Manager のインストーラは、次のコンポーネントのインストールを行います。

- Common Services 3.3 (必須)
- Security Manager 4.2 Server (必須)
- AUS 4.2 (オプション)
- Security Manager 4.2 Client (クライアントが専用クライアント マシンにインストールされている場合はオプション)

個別のインストーラを使用して、コンポーネントを個々にインストールできます。次にスタンドアロンインストーラを示します。

- Security Manager クライアントのインストーラ。クライアントのスタンドアロン インストーラとしても使用できます。このインストーラにアクセスする最も一般的な方法は、Web ブラウザ (https://server_hostname_or_ip) を使用してサーバにログインし、クライアント インストーラをクリックする方法です。
- RME インストーラ。RME のインストールを行います。このインストーラでは、Security Manager のインストーラを使用して、Common Services 3.3 を事前にインストールしておくことが必要です。スタンドアロンダウンロードではなく、Security Manager 4.2 Bundle の RME インストールパッケージを使用する必要があります。

Performance Monitor のインストーラは別個のインストール モジュールであり、Common Services 上に Performance Monitor をインストールします。このインストーラでは、Security Manager のインストーラを使用して、Common Services 3.3 を事前にインストールしておくことが必要です。Security Manager のインストーラ、RME のインストーラ、Performance Monitor のインストーラの詳細な使用方法は、『[Installation Guide for Cisco Security Manager 4.2](#)』に記載されています。

IP アドレス、ホスト名、および DNS 名

Cisco Security Manager では、DHCP アドレスではなく、スタティック IP アドレスが必要です。Security Manager サーバの IP アドレスは変更できます。変更後に、システムのレポートが必要です。Security Manager の TCP/IP 設定で DNS サーバを設定する場合は、Security Manager サーバのホスト名と DNS 名が同じで、設定されている DNS サーバで解決可能であることを確認してください。Security Manager をインストールする前に、サーバに対して永続的な DNS 名とコンピュータ ホスト名を選択する必要があります。これは、ホスト名と DNS 名はインストールの後に修正できないためです。インストール後に Security Manager サーバのホスト名を変更すると、Security Manager の再インストールが必要になる場合があります。

クライアントの展開

推奨される通常の手順では、Security Manager クライアントを個別のクライアント マシンにインストールし、実行します。Security Manager がサポートしているのは、所定のマシン上への単一バージョンのクライアントのインストールのみです。そのため、同一マシン上に、たとえば Security Manager 3.3 と 4.2 の両方のクライアントをインストールすることはできません。サーバにクライアントをインストールして使用することはできますが、これは、規模の小さいネットワークにのみ適しており、規模の大きい企業ネットワークにはお勧めできません。

「アプリケーションパフォーマンスに影響を与える要因」の項に記載されているように、エンドユーザとサーバの場所がかなり離れていて、相当な遅延が発生する場合（大陸間の距離がある場合）でも容認できるパフォーマンスを保持するために、サーバに近い場所にあるターミナルサーバ上に、クライアントを展開することをお勧めします。

Security Manager サーバのチューニング

Security Manager には、いくつかの詳細なパラメータが用意されています。このパラメータを修正して、アプリケーションのパフォーマンスを調整できます。50 以上のデバイスを管理する中規模および大規模な展開では、最適なパフォーマンスを得るために、Security Manager で次のパラメータを変更できます。

Windows オペレーティング システムのスワップ ファイル サイズ

仮想メモリ（ページング ファイル）は、「インストールされているメモリ」の 1.5 倍である必要があります (<http://support.microsoft.com/kb/2267427>)。これは、Windows プラットフォームに関する Microsoft の推奨事項です。Cisco の推奨事項ではありません。システムにインストールされている RAM が負荷を処理するには十分ではない場合のみ、メモリ ページングが必要になります。



注意

Windows Server 2008 では、[Automatically manage paging file size for all drives] チェックボックスを選択解除する（チェックをはずす）必要があります。このチェックボックスへのナビゲーションパスは、[Computer] > [Properties] > [Advanced System Settings] > [Performance] > [Settings] > [Advanced] > [Virtual Memory] > [Change] です。

Sybase データベースのレジストリ パラメータ

中規模または大規模な展開では、最適なパフォーマンスとスケーラビリティが得られるように、次のパラメータを調整する必要があります。

- ステップ 1** Security Manager のサーバで、`<NMSROOT>%databases%vms%orig%odbc.tmp` にある次のファイルを見つけ、テキスト エディタで下記のパラメータを変更します。
- a. 「`__Switches`」パラメータには、「`-gb high`」があるはずですが（あった場合は **Enter** を押します）。
 - b. 「`net stop crmdmgtd`」を使用して CSM をシャットダウンし、Security Manager が完全にシャットダウンするまで待ってから、次のステップに移ります。

図 1 odbc.tpl パラメータの編集

```

1  CWEUID=AuNEpmBTZNE=
2  CWEPWD=6YAqdtZ2Kkp1U6pPcU5JYA==
3  Start=dbsrv10
4  DatabaseName=vms
5  EngineName=csmEng
6  CommLinks=tcip(HOST=localhost;DOBOARDCAST=NO;ServerPort=10033
7  CWENCRYPTION=YES
8  AutoStop=yes
9  # note __ values are not passed through for odbc registration
10 # These __ values are skipped by odbcdsn.pl.
11 # These __ values are used for configuring db engine startup ;
12  Cache 512
13  Switches=-gd all -gp 4096 -gb high
14  _DbNTSvcLongName=Cisco Security Manager database engine
15  JdbcDriver=com.sybase.jdbc2.jdbc.SybDriver
16  DmPrefix=vms
17
18

```

ステップ 2 このステップは、次の 2 つのサブステップから構成されています。

- a. <NMSROOT>\objects\db\conf にある perl ユーティリティを使用して、Windows レジストリにデータベースパラメータを再登録します。以下にコマンドと構文の例を示します。

「perl configureDb.pl action=reg dsn=vms dmprefix=vms」

図 2 データベースパラメータの再登録

```

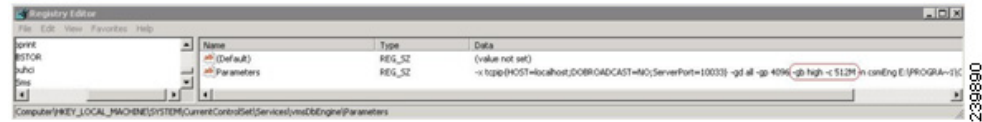
Administrator: Command Prompt
E:\PROGRAM~1\NCSOpx\objects\db\conf>perl configureDb.pl
Usage:
configureDb.pl action={install|uninstall} <dsn=database>
configureDb.pl action={reg|unreg} <dsn=database> <dnprefix=prefix> [dmonitor=no
]
configureDb.pl action=upgrade <dsn=database>
configureDb.pl action=upgrade <dsn=database> <portid=number>
configureDb.pl action=validate <dsn=database>
configureDb.pl action=rebuild <dsn=database>
configureDb.pl action=upgradeall
Example: configureDb.pl action=reg dsn=cnf dnprefix=Cnf
Note: portid is 16 bits long integer which should be smaller than 65535
E:\PROGRAM~1\NCSOpx\objects\db\conf>perl configureDb.pl action=reg dsn=vms dnpre
fix=vms
INFO: a datasource with the name vms was already present. It will be preserved.
INFO: Starting the DataBase
Starting database engine csmEng
INFO: Process created
INFO: Started the Database engine : csmEng Retry 0
INFO: Started the Database engine : csmEng Retry 1
INFO: Started the Database engine : csmEng Retry 2
INFO: Started the Database engine : csmEng Retry 3
INFO: Started the Database engine : csmEng Retry 4
INFO: Started the Database engine : csmEng Retry 5
INFO: Started the Database engine : csmEng Retry 6
INFO: Started the Database engine : csmEng Retry 7
INFO: Started the Database engine : csmEng Retry 8
INFO: Started the Database engine : csmEng Retry 9
INFO: Getting message
INFO: Connect the database dsn=vms
INFO: Connected the Database
INFO: Command Executed
INFO: Connecting the Database vms
INFO: Company=Cisco Systems|Application=NMIC|Signature=010fa55157edbe14d818eb4f
e3db41447146f1521632125eb777a87cf8b29a954f559d4221b792ff8
INFO: Preparing AUTH cmd
INFO: AUTH Executed
INFO: AUTH cmd Finished
INFO: Stopping the Database engine vms
Stopping database engine csmEng
SQL Anywhere Command File Hiding Utility Version 10.0.1.3830
E:\PROGRAM~1\NCSOpx\objects\db\conf>

```

- b. 上記のパラメータが正しく再登録されていることを確認し、次の場所にある Windows Registry の設定をチェックします。

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmsDbEngi
ne\Parameters (「-gb high -c 512M」 というエントリがあるはず)

図 3 データベース パラメータの再登録の確認



ステップ 3 コマンドプロンプトから「`net start crmdmgtd`」を使用して Security Manager を起動し、Security Manager が完全に機能するまで待ちます。

Security Manager のライセンスについて

Security Manager の展開を計画して、管理対象デバイスの数とタイプに応じた基本ライセンスとデバイス ライセンスが揃っていることを保証するためには、Security Manager のライセンスについて理解しておくことが重要です。

重要なライセンシング情報については、次のマニュアルを参照してください。

- 『[Installation Guide for Cisco Security Manager 4.2](#)』
- http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html にある、Security Manager の最新メジャー リリースの製品速報

ライセンスの例

ここでは、Security Manager のライセンスを理解しやすいように、いくつかの代表的なライセンスの例を示します。

例 1

管理対象ネットワークの説明：15 台の Cisco Integrated Services Router。

必要なライセンス：Enterprise Standard - 25 Device ライセンスが必要です。関連する Catalyst 6500 サービス モジュールがなく、デバイス数が 50 未満のため、Standard-25 ライセンスを注文します。

例 2

管理対象ネットワークの説明：5 台の IDSM-2 モジュールがあり、各モジュールには仮想センサーが 2 つずつある。

必要なライセンス：Enterprise Standard - 10 Device ライセンスが必要です (5 台のモジュールに 10 個の仮想センサーがあるため)。Standard-25 でも十分に思えますが、Catalyst 6500 サービス モジュールが含まれているため、Security Manager を使用して Catalyst 6500 スイッチを管理する必要がある場合は、最小でも Pro-50 ライセンスが必要です。

例 3

管理対象ネットワークの説明：シングルおよびフェールオーバー モードで動作する 250 の ASA ペアがある (500 台のデバイス)。

必要なライセンス：Enterprise Professional - 50 Device、および 2 つの Enterprise Incremental - 100 ライセンスが必要です。追加のデバイスの管理が必要な場合は、50、100、または 250 のデバイス単位で増分デバイス ライセンスを注文できます。

例 4

管理対象ネットワークの説明：Security Manager Standard Edition の 25 台のデバイスがあり、追加で、シングル モードで稼動している 20 台の ASA デバイスを管理する必要があります。

必要なライセンス：Enterprise Standard 25 to Professional 50 Upgrade ライセンスが必要です。

例 5

管理対象ネットワークの説明：アクティブ/スタンバイ、またはアクティブ/アクティブのペアの組み合わせで展開されており、それぞれ 5 つのセキュリティ コンテキストを持つ、10 ペアのフェールオーバー ASA デバイス (20 台のデバイス)。

必要なライセンス：Enterprise Professional - 50、および Enterprise Professional Incremental 50 Device。

冗長性を得るためフェールオーバー デバイスのペアを展開する場合は、Security Manager にアクティブ デバイスおよびコンテキストを追加するだけで済みます。必要なデバイスのライセンス数は、(10 台のデバイス) × (5 つのコンテキスト) + (10 台のシャーシ) で、合計 60 個のデバイスライセンスになります。



(注) 使用可能なライセンスの種類やサポートされているアップグレードパスに関する詳細の他、購入可能な Cisco Software Application Support サービス契約については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html で Security Manager の最新メジャー リリースの製品速報を参照してください。



(注) 上記のすべての例では、Cisco Technical Assistance Center (TAC) およびアプリケーションのマイナー リリース アップデートを無料で使用できるようにするために、対応する Cisco Service Application Support (SAS) の注文を検討する必要があります。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2011 Cisco Systems, Inc.
All rights reserved.

Copyright © 2011, シスコシステムズ合同会社.
All rights reserved.