

VPN/Security Management Solution 2.2 クイック スタートガイド

1 使用許諾契約補遺

シスコシステムズ ネットワーク管理ソフトウェア用使用許諾契約補遺: CiscoWorks VPN/SECURITY MANAGEMENT SOLUTION (無制限バージョンおよび制限付きバージョン)

重要：よくお読みください：本使用許諾契約 補遺 (SLA; Supplemental License Agreement) は、お客様とシスコ間のソフトウェア使用許諾契約に基づいてお客様に提供される、当該のソフトウェアの使用許諾に関する補足的な制限事項を記載したものです。本 SLA で下線を引いた条項は、別途に記載のない限り、ソフトウェア使用許諾契約の同条項で規定された意味を包含するものとします。ソフトウェアに適用される契約条件に矛盾が存在する場合は、本 SLA の条項が優先します。

ソフトウェアをインストール、ダウンロード、アクセス、またはその他の方法で使用することで、お客様は本 SLA の条項の制約を受けることに同意されることとなります。本 SLA の条項に同意されない場合には、ソフトウェアをインストール、ダウンロード、またはその他の方法で使用することはできません。以下で「サーバ」という用語は、セントラルプロセッサユニットを指しています。

使用許諾に関する補足の制限事項

- **デバイス数 20 台の制限付きバージョン。**このバンドルで提供されるコンポーネント全体で、最大 20 台のデバイスを管理できます。ただし、Management Center for Cisco Security Agents は、この限りではありません。Management Center for Cisco Security Agents では、別途ライセンスを購入してネットワーク環境に展開された Cisco Security Agent を管理できるデバイス数に制限はありません。ここでは、ネットワーク環境において IP アドレスを持つデバイスを、1 台のデバイスとして定義します。デバイスの定義の詳細については、コンポーネントのインストールガイドを参照してください。制限付きバージョンの上限である 20 台を超えるデバイスを使用する必要がある場合、このソフトウェアの無制限バージョンにアップグレードする必要があります。
- **インストールと使用。**ソフトウェア コンポーネントは、適用されるネットワーク管理ソフトウェア製品の既存の機能をインストール、アップデート、補完、または交換するという目的のみ、お客様に提供されます。お客様は、次のソフトウェア コンポーネントをインストールおよび使用できます。



- Common Services : このバンドル内の他のコンポーネントで使用される共有リソースを含みます。このバンドル内の一部のコンポーネントを複数のサーバにインストールする場合、お客様のネットワーク管理環境内に各コンポーネントとともに Common Services のコピーをインストールできません。
- Management Center for Cisco Security Agents (CSA MC) : お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。

注 別途ライセンスを購入されたシスコ セキュリティ エージェントについては、CSA MC を使用して管理できるデバイスの台数に制限はありません。

- Cisco Security Agents : VMS サーバのみとともに使用するためのサーバエージェントが 3 ライセンス含まれています。VMS 以外のサーバとともにエージェントを使用することはできません。追加のエージェントを別途購入する必要があります。
- Management Center for Performance : お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。
- Management Center for IDS Sensors : お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。
- Monitoring Center for Security: お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。
- Management Center for Firewalls: お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。
- Auto Update Server : お客様のネットワーク管理環境内にある 1 台のサーバにインストールできません。
- Management Center for VPN Routers : お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。
- Resource Manager Essentials (RME) : お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。
- VPN Monitor : お客様のネットワーク管理環境内にある 1 台のサーバにインストールできます。

•複製と配布。お客様は、ソフトウェアを複製または配布することはできません。

その他の権利および制限事項

「シスコシステムズ ソフトウェア使用許諾契約」を参照してください。



2 VPN/Security Management Solution の概要

CiscoWorks VPN/Security Management Solution (VMS) は、ネットワーク セキュリティ用 SAFE blueprint の中核機能であり、企業の Virtual Private Network (VPN; バーチャルプライベート ネットワーク)、ファイアウォール、ネットワークとホスト ベースの Intrusion Detection System (IDS; 侵入検知システム) の設定、監視、トラブルシューティングを行うための Web ベースのツールを組み合わせたものです。CiscoWorks VMS の堅牢でスケーラブルな基盤と機能セットは、規模の大小を問わず、あらゆる VPN とセキュリティの実装ニーズに対応する能力を業界で初めて提供します。

このガイドでは、ネットワーク管理者を対象に、VPN/Security Management Solution のインストールに関連した基本的な作業を簡単に説明します。このガイドでは、作業の詳細やソフトウェアが提供する機能全体の説明は行いません。VMS を効果的に展開する方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/sw/cscowork/ps2330/products_white_paper09186a0080088841.shtml にある『CiscoWorks VPN/Security Management Solution 展開ガイド』を参照してください。

ここでは、パッケージの内容リストと「新機能」情報を説明します。表 1 は、個々のコンポーネントの機能を説明しています。

VMS の内容

VMS 2.2 には、『VPN/Security Management Solution 2.2 クイック スタート ガイド』および次の 4 つのサブボックスが含まれています。

- **VMS Management and Monitoring Centers for Windows (VMCM) :** VMCM 起動ディスクが含まれており、次のコンポーネントが提供されています。
 - CiscoWorks Common Services
 - Management Center for Firewalls
 - Auto Update Server
 - Management Center for VPN Routers
 - Management Center for IDS Sensors
 - Monitoring Center for Security
 - Management Center for Cisco Security Agents

- **CiscoWorks VPN Monitor for Windows :** リリース ノートと VPN Monitor の CD-ROM が含まれています。

- **CiscoWorks Common Services for Solaris**



–CiscoWorks Common Services

- VMS Management and Monitoring Centers for Solaris (VMMC)** : VMMC 起動ディスクが含まれており、次のコンポーネントが提供されています。

- Management Center for Firewalls
- Auto Update Server
- Management Center for VPN Routers
- Management Center for IDS Sensors
- Monitoring Center for Security
- Monitoring Center for Performance

- CiscoWorks Resource Manager Essentials** : リリース ノートおよび Windows と Solaris 用の Resource Manager Essentials の CD-ROM が含まれています。

新機能

VMS 2.2 には、2 つの新しいコンポーネントが追加されました。Management Center for Cisco Security Agents 4.0.1 (CSA MC) は、ネットワークおよびシステムに攻撃が拡散するのを防止するエージェントを実装することにより、本格的な分散型のセキュリティをお客様の業務環境に実現します。これらのエージェントでは、Management Center によって提供される一連のルールが使用され、エージェントは、ネットワーク管理者によってネットワーク上の各クライアント ノードに選択的に割り当てられます。

また、このバージョンの VMS には、Monitoring Center for Performance 2.0 (Performance Monitor) が導入されているので、企業ネットワークのセキュリティに寄与するサービスの動作状況やパフォーマンスの監視およびトラブルシューティングも行えます。Performance Monitor を使用すれば、ユーザに IPSec または他のセキュリティテクノロジーの専門知識がなくても、ネットワークで重要なイベントが発生した時点で切り分けとトラブルシューティングを行って、サービスのアベイラビリティを向上させることができます。

VMS 2.2 では、VMS Management and Monitoring Centers 2.2 (VMMC) という 1 枚のインストール CD-ROM (起動ディスク) で、すべての Management Center (MC) をインストールできます。CiscoWorks Common Services (Common Services) は、Service Pack 2 (SP2) を含むようにアップグレードされました。すべての Management Center がアップグレードされました。

VMS の各機能が拡張されています。これらは、ファイアウォール管理、ルータ管理、IDS 管理、セキュリティモニタリングです。



主な機能拡張は次のとおりです。

- Solaris による IDS 管理、セキュリティ モニタリング、ファイアウォール/ルータ管理をサポート。
- アクティブな VPN に関連するメトリックを相互に関連付けてグラフ化。Solaris システム上の VPN によって接続されたすべてのネットワークとユーザをデバイスごとに識別可能。
- Cisco Catalyst Firewall Service Module (FWSM) および Cisco PIX Security Appliance の syslog レポート機能を Security Monitor でサポート。
- Cisco Catalyst の Firewall モジュールと VPN サービス モジュールをサポート。
- ファイアウォール サービス、ハイ アベイラビリティ VPN、および複数のハブ アンド スポーク環境をサポートするセキュリティルータ用の拡張サポート。
- IDS 4.1 のサポート。
- Cisco IDS Host Sensor を Okena テクノロジー準拠のシスコ セキュリティ エージェントに置き換え、ホストベース IDS 機能によるサーバの保護、および分散型ファイアウォールによるデスクトップの保護を強化。
- インストール作業の簡素化により、CiscoWorks VMS のほとんどの機能を 1 枚の CD-ROM からインストール可能。

表 1： VMS のコンポーネントとアトリビュート

コンポーネント	実現される機能
CiscoWorks Common Services 2.2 (Service Pack 2 適用)	VMS コンポーネント用の共有ソフトウェアとサービスを提供。 CiscoWorks Common Services 2.2 は、次の機能を提供します。Common Services 2.2：一連の共有アプリケーション サービス。 CiscoView 5.5：グラフィカルなデバイス管理ツール。 Integration Utility 1.5：サードパーティ製 Network Management System (NMS; ネットワーク管理システム) をサポートする統合モジュール。 Java Plug-in 1.4.1_02 のサポート。
Management Center for Firewalls 1.2.2 (Firewall MC)	PIX Firewall および Cisco Catalyst Firewall Services Module (FWSM) の設定。
Auto Update Server 1.1 (AUS)	動的にアドレスが設定されるデバイス PIX Firewall デバイスおよび IOS デバイスの管理。
Management Center for VPN Routers 1.2.1 (Router MC)	セキュリティルータ、Catalyst 6000 VPN サービス モジュール、および IOS ファイアウォールの設定。
Management Center for IDS Sensors 1.2.3 for Windows (IDS MC)	ネットワーク ベース IDS センサーおよび Catalyst 6000 Intrusion Detection Service Module (IDSM) の設定。
Monitoring Center for Security 1.2.3 for Windows (Security Monitor)	ネットワークベースおよびホストベースの IDS イベント、FWSM および PIX Firewall の syslog の監視。



コンポーネント	実現される機能
Management Center for Cisco Security Agents 4.0.1 (CSA MC)	サーバを保護するための Cisco Security Agents の設定と管理、および分散型ファイアウォールによるデスクトップの保護。
VPN Monitor 1.2.1	IPSec ベース、サイトツーサイト、およびリモート アクセスの VPN の監視。
Resource Manager Essentials 3.5 (RME)	ネットワーク インベントリおよびデバイス変更、ネットワーク構成、およびソフトウェア イメージの更新の管理。
Monitoring Center for Performance 2.0 (Performance Monitor)	企業ネットワークのセキュリティに影響を及ぼすサービスの状態およびパフォーマンスの監視とトラブルシューティング。

3 サーバおよびクライアントのシステム要件

Performance Monitor 以外のすべての VMS コンポーネントは Windows システムにインストールできます。VPN Monitor および CSA MC 以外のすべてのコンポーネントは Solaris システムにもインストールできます。ここでは、VMS のシステム要件と CSA MC のブラウザ要件について説明します。

注： VMS と LAN Management Solution (LMS) を共存させることは可能ですが、パフォーマンスを最適化するために、別々のサーバにインストールすることをお勧めします。Cisco.com の http://www.cisco.com/en/US/products/sw/cscowork/ps2330/products_white_paper09186a0080088841.shtml にある『CiscoWorks VPN/Security Management Solution 展開ガイド』を参照してください。

VMS のシステム要件

表 2 は VMS のサーバ要件、表 3 は VMS のクライアント要件をそれぞれ示しています。

注 VMS のコンポーネントを正しくインストールするために、ターミナル サービスがオフになっていることを確認してください。Microsoft のマニュアルを参照してください。

次のサービスが 1 つでも実行されている Windows サーバには、VMS のコンポーネントをインストールしないでください。

- プライマリ ドメイン コントローラ。
- バックアップドメイン コントローラ。



- ターミナル サーバ。

表 2：VMS のサーバ要件

コンポーネント	最小要件
ハードウェア	<ul style="list-style-type: none">• 次のいずれか：<ul style="list-style-type: none">- 1 GHz 以上の Pentium プロセッサを搭載した IBM PC 互換機 または <ul style="list-style-type: none">- 440 MHz 以上のプロセッサを搭載した Sun UltraSPARC 60 MP または <ul style="list-style-type: none">- Sun UltraSPARC III (Sun Blade 2000 Workstation または Sun Fire 280R Workgroup Server) <ul style="list-style-type: none">• 16 ビット カラー対応のビデオ カードとカラー モニタ。• CD-ROM ドライブ。• 100BaseT 以上の接続。
オペレーティング システム	<p>次のオペレーティング システムのいずれかが必要です。</p> <ul style="list-style-type: none">• Windows 2000 Professional、Server、および Advanced Server (Service Pack 4)。 <hr/> <p>注 Advanced Server ではターミナルサービスをオフにする必要があります。Microsoft のマニュアルを参照してください。</p> <hr/> <ul style="list-style-type: none">• 次のパッチを適用済みの Sun Solaris 2.8。<ul style="list-style-type: none">- 109742 は 108528-13 に置き換えられています。- 109322 は 108827-15 に置き換えられています。- 109279 は 108528-13 に置き換えられています。- 108991 は 108827-15 に置き換えられています。- 111626-01.- 111327-02.- 110945-02.- 110934-01.- 110898-02.- 110700-01.- 109326-05.- 108827-30.- 108652-51.- 108528-18.- 108921-14.- 108940-24.- 110951-01.- 110662-02.- 110615-01.- 110286-02.- 109324-02.- 111085-02.- 108964-06.



コンポーネント	最小要件
ファイルシステム	NTFS。
メモリ	最小 1 GB。
仮想メモリ	最小 2 GB。
ハード ドライブ容量	9 GB 以上の空きハード ドライブ容量。 注 実際に必要なハード ドライブの容量は、インストールする CiscoWorks Common Services クライアント アプリケーションの数およびそれらのクライアントアプリケーションを使用して管理するデバイスの数により異なります。
Java	Sun Java Plug-in 1.4.1_02。

表 3：VMS のクライアント要件

コンポーネント	最小要件
ハードウェアとソフトウェア	次のいずれか 1 つが必要です。 <ul style="list-style-type: none"> • Pentium 300 MHz 以上のプロセッサを搭載し、次のいずれかを実行する IBM PC 互換機 <ul style="list-style-type: none"> - Windows 2000 Server または Service Pack 4 適用済み Professional Edition。 - Service Pack 1A 適用済み Windows XP Professional。 • 333 MHz のプロセッサを搭載し、Solaris 2.8 オペレーティングシステムを実行する Solaris SPARCstation または Sun Ultra 10
ハード ドライブ容量	<ul style="list-style-type: none"> • 400 MB の仮想メモリ (Windows の場合)。 • 512 MB のスワップ領域 (Solaris の場合)。
メモリ	256 MB 以上。
Web ブラウザ	<p>次のいずれかの HTML ブラウザをインストールする必要があります。</p> <ul style="list-style-type: none"> • Windows オペレーティングシステムの場合、Microsoft Internet Explorer 6.0 Service Pack 1 • いずれかの Windows プラットフォームの場合、Netscape Navigator 4.79/7.1。 <hr/> <p>注意： AUS、CSA MC、Firewall MC、および Router MC を使用するには、Windows プラットフォームの場合は Navigator 7.1、Solaris プラットフォームの場合は Navigator 7.0 が必要です。</p>



ブラウザ要件

すべての VMS コンポーネントは、Windows プラットフォーム上の Internet Explorer 6.0 (Service Pack 1 適用済み) をサポートしています。CSA MC は、Explorer バージョン 5.5 以降をサポートしています。どのコンポーネントを使用する場合でも、cookie と JavaScript を有効にする必要があります。これは、インターネットのセキュリティ設定で、最高でも「中」の設定を使用することに相当します。この機能は Tools メニューの Internet Options メニューにあります。Security タブを選択してください。

表 4 に各コンポーネントによる Netscape Navigator のサポート状況を示します。これらの要件は、VMS 全体の要件と異なります。

表 4 : Netscape Navigator のサポート

コンポーネント	Windows のブラウザ要件	Solaris のブラウザ要件
CiscoWorks Common Services (Common Services)	<ul style="list-style-type: none"> • Netscape Navigator 4.79 • Netscape Navigator 7.1 	<ul style="list-style-type: none"> • Netscape Navigator 4.76 • Netscape Navigator 7.0
Management Center for Firewalls (Firewall MC)	<ul style="list-style-type: none"> • Netscape Navigator 7.1 	<ul style="list-style-type: none"> • Netscape Navigator 7.0
Auto Update Server (AUS)	<ul style="list-style-type: none"> • Netscape Navigator 7.1 	<ul style="list-style-type: none"> • Netscape Navigator 7.0
Management Center for IDS Sensors (IDS) および Security Monitor	<ul style="list-style-type: none"> • Netscape Navigator 4.79 	<ul style="list-style-type: none"> • Netscape Navigator 4.76
Management Center for VPN Routers (Router MC)	<ul style="list-style-type: none"> • Netscape Navigator 7.1 	<ul style="list-style-type: none"> • Netscape Navigator 7.0
Management Center for Cisco Security Agents (CSA MC)	<ul style="list-style-type: none"> • Netscape Navigator 7.1 (cookies および Java Script を有効に設定)¹ 	<ul style="list-style-type: none"> • Netscape Navigator 7.0 (cookies および Java Script を有効に設定)²
Resource Manager Essentials (RME)	<ul style="list-style-type: none"> • Netscape Navigator 4.79 • Netscape Navigator 7.1 	<ul style="list-style-type: none"> • Netscape Navigator 4.76 • Netscape Navigator 7.0
VPN Monitor	<ul style="list-style-type: none"> • Netscape Navigator 7.1 	<ul style="list-style-type: none"> • Netscape Navigator 7.0
Monitoring Center for Performance (Performance Monitor)	<ul style="list-style-type: none"> • Netscape Navigator 4.79 	<ul style="list-style-type: none"> • Netscape Navigator 4.76

1. この機能には次のメニューからアクセスできます。Edit > Preferences > Advanced.

2. この機能には次のメニューからアクセスできます。Edit > Preferences > Advanced.



注 CiscoWorks Desktop Server から CSA MC のユーザ インターフェイスにアクセスする場合は、SSL 経由のアクセスとなります。[「Windows にインストールする際の特記事項」のセクション](#)を参照してください。

4 Windows への VMS のインストール

ここでは、CiscoWorks VMS Management and Monitoring Centers (VMMC) のコンポーネント アプリケーション、VPN Monitor、および RME のインストール手順について説明します。また、Cisco IDS Host Sensor and Console (Cisco HIDS) をアンインストールする手順についても説明します。

注意 このクイック スタート ガイドの情報は、初めて VMS コンポーネントをインストールする場合のみを対象に提供されています。実稼働中の展開済みシステムでは、これらの手順を実行しないでください。実行するとシステムに悪影響を及ぼす可能性があります。アップグレード手順については、[「8 関連資料」のセクション](#)にある個々のコンポーネントのインストール マニュアルを参照してください。

始める前に

- すべてのシステム要件が満たされていることを確認します。[「VMS のシステム要件」のセクション](#)を参照してください。
 - 開かれているプログラムやアクティブなプログラムをすべて閉じます。インストール中には他のプログラムを実行しないでください。
-

注 インストール中にターミナル サービスが動作していないことを確認してください。Microsoft のマニュアルを参照してください。



Windows にインストールする際の特記事項

ここには、インストールを開始する前に読む必要のある重要な情報が記載されています。

- CSA MC を展開する際には、CSA MC システムに、CSA MC と VMS バンドルの一部である Security Monitor のみをインストールすることをお勧めします。CSA MC をインストールすると、CSA MC など、一部の CiscoWorks のデーモンおよび動作を保護するために必要なポリシーが含まれるエージェントも自動的にインストールされます。このエージェントが実施するポリシーは、かなり制限が多く、推奨される展開形態で使用する場合に適切な設定になっています。

CiscoWorks サーバ上で VMS 以外の製品またはソフトウェアを実行している場合は、それらの実行がこの制限ポリシーによって妨げられる場合があります。VMS 以外の製品をインストールする場合は、システムを保護するエージェントから制限ポリシーを削除して、よりオープンなポリシーを使用する必要がある場合があります。制限ポリシーを使用しなくても、システムは引き続き保護されますが、より多くの製品をシステムで実行して、ネットワーク リソースにアクセスできるようになります。そのため、システムのセキュリティは本質的に低くなります。VMS 以外のソフトウェアが実行されるシステムに CSA MC を展開する場合は、CiscoWorks VMS Systems グループに移動して、そのグループから CiscoWorks Restrictive VMS Module を削除します。

注 必要に応じて、CiscoWorks Restrictive VMS Module を削除する代わりに編集することもできます。適切に編集すれば、インストールされている他の製品に必要なアクションを実行できるようになります。詳細については、http://www.cisco.com/en/US/products/sw/cscowork/ps5212/products_user_guide_book09186a008019b759.html にある「Using Management Center for Cisco Security Agents 4.0」を参照してください。

- Common Services をインストールした後、SP2 などのコンポーネント パッチが自動的にインストールされるため、Common Services のインストール処理が延長されます。
- インストール作業を行えるのは、管理者特権のあるユーザのみです。
- CiscoWorks のアプリケーションは、システムドライブの \Program Files\CSCOpX というデフォルト ディレクトリにインストールされます。インストール中に別のディレクトリを選択すると、そのディレクトリにアプリケーションがインストールされます。
- インストール中にエラーが発生した場合は、オペレーティング システムがインストールされているドライブのルート ディレクトリにあるインストール ログを調べてください。インストールするたびに新しいログ ファイルが作成されます。たとえば、CiscoWorks Common Services をインストールすると、システムドライブに \CiscoWorks_setupxxx.log というファイルが作成されます。xxx は最後にインストールされた CiscoWorks アプリケーションのログ ファイルを示します。
- Cancel をクリックすれば、いつでもインストールを終了することができます。ただし、システムに加えられた変更（新しいファイルのインストールやシステム ファイルの変更など）は元には戻りません。



- クライアント ブラウザと管理サーバの間でセキュリティ保護されたアクセスを使用したい場合は、CiscoWorks デスクトップから SSL を有効または無効にできます。
- SSL が有効な場合は、次のようになります。

-http ではなく https で始まる URL になり、安全な接続であることが示される。

-サーバ名に続くポート番号が 1741 ではなく 1742 になる。

SSL 準拠ではないアプリケーションがサーバにインストールされている場合は、CiscoWorks サーバで SSL を有効にすることはできません。

注 SSL をサポートしない CiscoWorks コンポーネントを使用する場合以外は、インストール時に SSL を有効にしておくことをお勧めします。SSL をサポートしないコンポーネントがある場合は、CSA MC をサーバにインストールすることはできません。SSL に関する詳細については、『User Guide for CiscoWorks Common Services 2.2』を参照してください。

- VMMC 起動ディスクは、リモートドライブからアクセスすると正常に動作しない可能性があります。リモート インストールは避けるようにお勧めします。リモート マウント ポイントからインストールすると、ネットワークの不整合が原因でインストール エラーが発生する場合があります。

Windows 2000 の保護

システムの安全性は、システムで最もセキュリティの弱いコンポーネントによって決まります。サーバソフトウェアをインストールする前に、次の基本的な手順を実行して、インストール先のサーバとオペレーティングシステムのセキュリティを確保する必要があります。

- オペレーティング システムは、専用のパーティションにインストールしてください。**オペレーティング システムを 1 つのパーティションにインストールし、ユーザのソフトウェアとデータを別のパーティションにインストールすると、ユーザのデータおよびアプリケーションをウィルスやセキュリティ侵犯の危険から保護できます。
- 推測されにくいパスワードを使用してください。**強固なパスワードとは、8 文字以上で、数字、英字（大文字と小文字の両方）および記号を含むパスワードです。Local Security Policy を編集すれば、Windows 2000 によって強固なパスワードが要求されるように設定できます。
- ネットワーク共有は作成しないでください。**ネットワーク共有を作成する必要がある場合は、強固なパスワードを設定して共有リソースのセキュリティを確保してください。ただし、ネットワーク共有は使用しないように強くお勧めします。また、NETBIOS は完全に無効にしてください。
- 不要なアカウントは無効にしてください。**デフォルトの Guest アカウントは削除します。他のアカウントはすべて、必ず強固なパスワードで保護します。ログイン時にはパスワードが要求されるように設定します。



- レジストリのセキュリティを設定してください。**レジストリに対するリモート アクセスは無効にするか制限します。
- すべてのホットフィックスとセキュリティ パッチを適用してください。**Microsoft の Web サイトを定期的に参照して、最新のセキュリティ パッチを適用します。Windows Update を定期的に使用して、最新の重要な更新を必ずサーバにインストールします。
- 使用しないサービスや不要なサービスは無効にしてください。**Windows の実行に最低限必要なサービスは、DNS Client、Event Log、Plug & Play、Protected Storage、および Security Accounts Manager です。ご使用のソフトウェアに必要なその他の Windows サービスについては、ソフトウェアのマニュアルを参照してください。IIS はインストールしないでください。
- Internet Protocol (TCP/IP) 以外のすべてのネットワーク プロトコルを無効にしてください。**他のプロトコルは、サーバにアクセスするのに利用される場合があります。使用されるネットワーク プロトコルを制限すれば、サーバへのアクセス ポイントを制限できます。サーバでネットワーク共有を使用しない場合は、NETBIOS を無効にします。
- システムのセキュリティを定期的に監視してください。**システム アクティビティのログを取得して確認します。Microsoft Security Configuration Tool Set (MSCTS) や Fport などのセキュリティ ツールを使用して、システムのセキュリティ設定を定期的に検討します。MSCTS は Microsoft の Web サイトから入手できます。
- サーバへの物理的接触を制限してください。**サーバに取り外し可能なメディア ドライブがある場合、サーバがまずハード ドライブからブートするように設定します。フロッピー ディスクからサーバをブートできれば、データを盗むことも可能です。通常、ブートの順序はシステムの BIOS で設定します。BIOS は必ず強固なパスワードで保護してください。
- リモート アクセス ツールやリモート管理ツールをサーバにインストールしないでください。**これらのツールはサーバへの侵入経路になるので、セキュリティ リスクと見なされます。
- ウィルス スキャン アプリケーションをサーバ上で実行してください。**ウィルス スキャン ソフトウェアを使用すれば、サーバがトロイの木馬に感染するのを防止できます。ウィルス シグニチャは定期的に更新してください。

インストールの順序

ここでは、推奨されるインストール手順の概要を説明します。ここに説明されているインストール手順の順序を読んでから、詳細な指示について、以降の該当するセクションを参照することをお勧めします。

ステップ 1 必要に応じて、Cisco HIDS および Console をアンインストールします。[「Cisco IDS Host Sensor と Console をアンインストールする」のセクション](#)を参照してください。-

注 CSA MC またはエージェントのインストーラがシステム上に Cisco IDS Host Sensor のいずれかのソフトウェアを検知した場合は、インストールが中止されます。



ステップ 2 Cisco.com または VMMC 起動ディスクにある vmmc_verify_digest.exe 実行ファイルを使用して、CD-ROM にあるすべてのメディアが信頼できるエラーのないメディアであることを確認します。[「VMMC ファイルの整合性を確認する」のセクション](#)を参照してください。

ステップ 3 VMMC 起動ディスクから Common Services をインストールします。[「CiscoWorks Common Services および Service Pack 2 を Windows にインストールする」のセクション](#)を参照してください。

注 Common Services のインストールの完了後、システムを再起動すれば、自動的に SP2 のインストールが開始されます。SP2 のインストールが完了するまで待つ必要があります。約 7 分かかります。

ステップ 4 VMMC 起動ディスクから、必要な VMMC アプリケーションを任意の順序でインストールします。次のいずれかを参照してください。

[「Cisco IDS Host Sensor と Console をアンインストールする」のセクション。](#)

[「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Windows にインストールする」のセクション。](#)

[「CiscoWorks Common Services および Service Pack 2 を Windows にインストールする」のセクション。](#)

[「Management Center for Firewalls を Windows にインストールする」のセクション。](#)

[「Auto Update Server を Windows にインストールする」のセクション。](#)

[「Management Center for VPN Routers を Windows にインストールする」のセクション。](#)

[「Management Center for IDS Sensors および Monitoring Center for Security を Windows にインストールする」のセクション。](#)

[「Management Center for Cisco Security Agents を Windows にインストールする」のセクション。](#)

注 CSA MC を最初にインストールしてから、別のコンポーネントをインストールしようとする、CSA MC のエージェント コンポーネントによって許可されなかったり、応答の必要な複数の問い合わせが表示される場合があります。エージェント ソフトウェアを無効にして再び有効にする方法については、[「他のコンポーネントをインストールするために CSA MC のエージェント ソフトウェアを無効にする」のセクション](#)を参照してください。

ステップ 5 RME をインストールします。[「Resource Manager Essentials を Windows にインストールする」のセクション](#)を参照してください。



ステップ 6 VPN Monitor をインストールします。[「VPN Monitor をインストールする」のセクション](#)を参照してください。

ステップ 7 登録およびセットアップに関する重要な情報について、[「6 インストール後の作業」のセクション](#)を参照します。

Cisco IDS Host Sensor と Console をアンインストールする

VMS のコンポーネントをインストールする前に、Cisco IDS Host Sensor および Cisco IDS Host Sensor Console をアンインストールすることをお勧めします。特に、CSA MC またはエージェントのインストーラがシステム上に Cisco IDS Host Sensor のいずれかのソフトウェアを検知した場合には、インストールが中止されます。

Cisco HIDS をアンインストールする

始める前に

Console をアンインストールする前に、Console のホストにインストールされている Host Sensor (Agent) のモードを変更する必要があります。次に、Agent のモードを変更する手順を示します。

注 Cisco HIDS を正しくアンインストールするための手順および追加情報は、Cisco.com の <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/host/hos t25/install/> にも掲載されています。

Console をアンインストールするには、次の手順に従います。

ステップ 1 次の手順で Agent のモードを変更します。

- a. Console にログインします。
- b. **Agents** をクリックして、Agent Management ビューを表示します。
- c. Console ホストにインストールされている Agent を選択します。



d. Agent が SecureSelect-Warning モードの場合は、Console を閉じます。

e. Agent のモードを SecureSelect-Warning モードに変更するには、Agent を右クリックして **Set to SecureSelect-Warning Mode** を選択します。

f. Console を閉じます。

ステップ 2 Windows のタスクバーで、**Start > Programs > Cisco HIDS > Cisco HIDS Uninstall** の順に選択します。

Install Shield ウィザードが表示されます。

ステップ 3 Uninstall Setup ウィンドウで **Yes** をクリックして、Cisco IDS Host Console を削除します。publickey と serverkey が PreserveKeys フォルダにコピーされます。

ステップ 4 **OK** をクリックして、Console を削除します。

ステップ 5 **Finish** をクリックしてコンピュータを再起動すれば、アンインストールが完了します。

VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Windows にインストールする

VMMC の起動ディスクを使用すれば、1 枚の CD-ROM から Management Center のコンポーネントをどれでもインストールできます。ここで説明するステップに従って、起動ディスクに収録されているコンポーネントのマニュアルを見つけてインストールを開始した後、インストールするコンポーネントに関する以降の VMMC インストール手順を実行します。

注 VMMC のインストールを始める前に、ファイルの整合性を確認することを強くお勧めします。[「VMMC ファイルの整合性を確認する」のセクション](#)を参照してください。



ステップ 1 VMMC の起動ディスクを CD-ROM ドライブに挿入します。ディレクトリ階層の一番上に各 VMMC コンポーネントに対応するフォルダがあります。ここで、いずれかのコンポーネントのフォルダをダブルクリックして、コンポーネントの **Documentation** ディレクトリを表示すれば、必要なすべてのコンポーネント情報やすべてのインストール ファイルのリストを表示できます。

ステップ 2 システムの autorun が有効になっている場合は、CiscoWorks VMS Management and Monitoring Centers Installer ウィンドウが自動的に開きます。

ステップ 3 autorun が有効になっていない場合は、**Start > Run** の順にクリックします。Run ダイアログ ボックスで、e:\autorun.exe と入力します。e には、CD-ROM ドライブを指定します。

CiscoWorks VMS Management and Monitoring Centers 2.2 のセットアッププログラムのスプラッシュ画面が表示されます。

ステップ 4 Install をクリックします。

CiscoWorks の InstallShield ウィザードにより、すべての VMMC コンポーネントのリストが表示され、インストールするコンポーネントのチェック ボックスをオンにするように求められます。すべてを選択するオプションと、インストールをキャンセルするオプションもあります。

ステップ 5 インストールするコンポーネントをすべて選択します。

注 選択された項目の中にシステムの再起動が必要なものがあれば、**Select All** を使用することはできません。Select All オプションを動作させるには、まず、再起動が必要なコンポーネント（Common Services および CSA MC）をインストールする必要があります。

ステップ 6 Next をクリックします。InstallShield ウィザードにより、選択したコンポーネントが表示され、再選択、キャンセル、または続行するかが確認されます。

ステップ 7 Install をクリックして続行します。

ステップ 8 起動ディスクにより、前述のメニューで選択した順序に従ってインストール スクリプトの実行が開始されます。



注 Common Services、Router MC、IDS MC の 1 つまたはいずれかの組み合わせをインストールする場合は、システムの再始動を求められます。残りのコンポーネントのインストールを続行する前に、再始動することをお勧めします。ステップ 2 とステップ 3 を繰り返して、VMMC の Install Shield ウィザードを再始動して、他の VMMC ツールをインストールします。

注 CSA MC により、自動的にシステムが再始動されます。ステップ 2 とステップ 3 を繰り返して、VMMC の Install Shield ウィザードを再始動して、他の VMMC ツールをインストールします。

ステップ 9 一般的なインストール手順について、各コンポーネントに該当する以降のセクションを参照します。

VMMC ファイルの整合性を確認する

VMMC の起動ディスクには、起動ディスクの全ファイルの整合性をチェックできる `vmmc_verify_digest.exe` 実行ファイルが収録されています。アカウントをお持ちの場合は、Cisco.com からこのツールを入手することもできます。最大限のセキュリティを確保するために、このツールはこの場所からダウンロードすることをお勧めします。

VMMC のファイルの信頼性と整合性を確認するには、次の手順に従います。

ステップ 1 次のいずれかを行います。

- <http://www.cisco.com/public/sw-center/cw2000/vms-planner.shtml> を開いて `verify_digests.exe` ファイルを安全に入手し、DOS コマンド プロンプトで、**run vmmc_verify_digest.exe** と入力します。

または



- VMMC の起動ディスクを CD-ROM ドライブに挿入して、DOS コマンド プロンプトで `run vmmc_verify_digest.exe` と入力します。
-

注意 ダイジェスト ファイルをダウンロードする際には、安全にダウンロードするために、ブラウザが https モードになっていることを確認してください。

`vmmc_verify_digest.exe` ファイルにより、確認する必要があるファイルのリストがチェックされます。この処理が終わると、ファイルのあるディレクトリをたずねるメッセージが表示されます。

注 CD またはローカル ディレクトリのファイルの確認後は、任意のキーを押せば処理が終了します。

ステップ 2 CD-ROM のフォルダを参照して起動ディスクの場所を選択してから、Enter キーを押します。Verify_digests.exe によって、各ファイルの妥当性が検査されます。

注 CD-ROM のドライブ文字を入力して起動ディスク自体のファイルをチェックすることも、ファイルをシステムにコピーして、コピー先のディレクトリのファイルをチェックすることもできます。

ファイルの信頼性が確認されれば、出力に **OK** と表示されます。いずれかのファイルが信頼できない（システムからのものでない）か破損していれば、**Failure** と表示されます。

ステップ 3 次のいずれかを行います。

- 不具合のメッセージが示された場合は、VMMC のインストールに進む前にシステム管理者に連絡します。

または

- File not found** のメッセージが表示されたら、ファイルの場所をチェックします。これは、ダイジェスト プログラムがファイルを見つけられなかったことを示しています。



ステップ 4 不具合のメッセージが示されなかった場合、インストールを続行します。

CiscoWorks Common Services および Service Pack 2 を Windows にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 VMMC の Install Shield ウィザードで Common Services のチェックボックスをオンにすると、Common Services が常に最初にインストールされます。

注 Common Services のインストールを手動で実行するには、VMMC の起動ディスクを CD-ROM ドライブに挿入して、Common Services のトップレベル ディレクトリを探して、setup.exe ファイルをダブルクリックします。

ステップ 2 表示されるメッセージに従って、必要な情報を入力します。Express インストールを選択することをお勧めします。別のインストール オプションを選択する必要があるのは、システム ドライブ :\\Program Files\\CSCOpx 以外のディレクトリをインストール先に指定する場合だけです。詳細については、『Installation and Setup Guide for CiscoWorks Common Services (includes CiscoView) for Windows』を参照してください。

注 Common Services の最新アップデートを適用するために、この時点で CiscoWorks VMS Update1 をインストールする必要があります。

ステップ 3 Patches > VMSUpdate フォルダにある setup.exe ファイルをクリックして、CiscoWorks VMS Update 1 をインストールします。

ステップ 4 他の VMS コンポーネントをインストールする前に、システムを再起動する必要があります。

再起動が完了し、1 つ以上の VMS コンポーネントのインストールを開始すると、「Please wait, installer is checking your system...」という画面が表示されます。



その後、次のエラー メッセージが表示されます。Common Services SP2 is not installed. Installation of Common Services SP2 will begin now. その後、次のインストーラ メッセージが表示されます。Installing Common Services SP2. This will take approximately 7 minutes. Please wait....

SP2 のインストールが終わったら、2 個のパッチ アップデートのインストールが始まります。ユーザの介入は必要ありませんが、Installing Patch CSCec43722-1 というスプラッシュ画面が表示されます。このインストール作業が行われている間は、最小化された DOS ウィンドウがデスクトップに表示されます。パッチのインストール中にこのウィンドウを最大化すると、インストール中のパッチが表示されます。

パッチ アップデート CSCec43722-1 のインストール後、すぐに引き続き 2 番目のパッチ アップデートのインストールが始まり、Installing Patch CSCed18592-1 というスプラッシュ画面が表示されます。このパッチのインストール中にも最小化された DOS ウィンドウがデスクトップ上に表示されます。

注 これらのパッチのインストールは、連続してすばやく行われ、ユーザが介入する必要はありません。

ステップ 5 [「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Windows にインストールする」のセクション](#)に示されているステップのうち、必要なものを繰り返します。

Management Center for Firewalls を Windows にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 VMMC の Install Shield ウィザードで Managing PIX Firewalls, Catalyst Firewall SM チェックボックスをオンにすると、Common Services と SP2 のインストールが終わるとすぐに、Firewall MC のインストールが始まります。

注 Common Services 2.2 がシステムにインストールされている場合は、VMMC の起動ディスクを CD-ROM ドライブに挿入し、Firewall MC のトップレベル ディレクトリを見つけて setup.exe ファイルをダブルクリックすれば、Firewall MC を手動でインストールできます。



ステップ 2 表示されるメッセージに従って、必要な情報を入力します。詳細については、『Installing Management Center for Firewalls 1.2.2 on Windows 2000 and Solaris 2.8』を参照してください。

ステップ 3 アクティビティ承認者電子メール通知機能を使用するには、CiscoWorks の電子メール サーバを設定する必要があります。電子メール設定オプションは、Common Services の Typical インストールではなく、Advanced インストールにあります。インストール中に電子メール サーバを設定しなかった場合は、CiscoWorks のデスクトップで、VPN/Security Management Solution > Administration > Common Services > Preferences の順に選択すれば設定できます。

ステップ 4 Firewall MC および選択された他のインストールが終わったら、「インストール後の作業」のセクションにある CiscoWorks Desktop Server の設定に関する説明を参照します。

Auto Update Server を Windows にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 VMMC の Install Shield ウィザードで Auto Update Server チェックボックスをオンにすると、表示された順序で AUS のインストールが開始されます。

注 Common Services 2.2 がシステムにインストールされている場合は、VMMC の起動ディスクを CD-ROM ドライブに挿入し、AUS のトップレベルディレクトリを見つけて setup.exe ファイルをダブルクリックすれば、AUS を手動でインストールできます。

ステップ 2 表示されるメッセージに従って、必要な情報を入力します。詳細については、『Installing Auto Update Server 1.1 on Windows 2000 and Solaris』を参照してください。

AUS および選択された他のインストールが終わったら、[「6 インストール後の作業」のセクション](#)にある CiscoWorks Desktop Server の設定に関する説明を参照します。



Management Center for VPN Routers を Windows にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 VMMC の Install Shield ウィザードで Managing VPN Routers, Catalyst VPN SM, IOS Firewalls チェックボックスをオンにすると、表示された順序で Router MC のインストールが開始されます。

注 Common Services 2.2 がシステムにインストールされている場合は、VMMC 起動ディスクを CD-ROM ドライブに挿入し、Router MC のトップレベルディレクトリを見つけて setup.exe ファイルをダブルクリックすれば、Router MC を手動でインストールすることができます。

ステップ 2 表示されるメッセージに従って、必要な情報を入力します。詳細については、『Release Notes for Management Center for VPN Routers 1.2.1 on Windows 2000 and Solaris』を参照してください。

ステップ 3 Router MC のデータベースに対する内部アクセス用のパスワードを Password フィールドと Confirm Password フィールドの両方に入力します。入力したパスワードは、自動的にバックグラウンドで使用されて、特定のシステム イベント（バックアップおよび復元処理など）が行えるようになります。

ステップ 4 アクティビティ承認者電子メール通知機能を使用するには、CiscoWorks の電子メール サーバを設定する必要があります。電子メール設定オプションは、Common Services の（Typical インストールではなく）Advanced インストールにあります。インストール中に電子メールサーバを設定しなかった場合は、CiscoWorks のデスクトップで、VPN/Security Management Solution > Administration > Common Services > Preferences の順に選択すれば設定できます。

ステップ 5 他の VMS コンポーネントをインストールする前に、システムを再起動する必要があります。システムが再起動されると、再び VMMC の Install Shield ウィザードに戻ります。[「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Windows にインストールする」](#)のセクションに示されているステップのうち、必要なものを繰り返します。

Router MC および選択された他のインストールが終わったら、[「6 インストール後の作業」](#)のセクションにある CiscoWorks Desktop Server の設定に関する説明を参照します。



Management Center for IDS Sensors および Monitoring Center for Security を Windows にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

Security Monitor を他の Management Center と同じ場所にインストールすることは可能ですが、Security Monitor は実稼動ネットワークの管理アプリケーションとは別のサーバにインストールすることをお勧めします。Firewall MC と IDS Sensors の一方または両方をモニタリングすることにより、トラフィック処理の負荷が高くなる可能性があるためです。

ステップ 1 VMMC の Install Shield ウィザードで Managing IDS Sensors, Catalyst IDS SM, and Security Monitoring チェックボックスをオンにすると、表示された順序で IDS MC と Security Monitor のインストールが開始されます。

注 Common Services 2.2 がシステムにインストールされている場合は、VMMC の起動ディスクを CD-ROM ドライブに挿入し、IDS MC と Security Monitor のトップレベルディレクトリを見つけて `setup.exe` ファイルをダブルクリックすれば、IDS MC と Security Monitor を手動でインストールすることができます。

ステップ 2 IDS MC と Security Monitor の両方をインストールするには、Typical インストール オプション ボタンを選択します。

ステップ 3 IDS MC か Security Monitor のいずれかをインストールするには、Custom インストール オプション ボタンを選択します。次に、Next をクリックします。

a. IDS MC をインストールするには、IDS MC only オプション ボタンを選択して、**Next** をクリックします。

b. Security Monitor をインストールするには、Security Monitor only オプション ボタンを選択して、**Next** をクリックします。

ステップ 4 表示されるメッセージに従って、必要な情報を入力します。データベースの場所を選択して、データベースのパスワードを入力し、UDP ポートを指定するように求められます。詳細については、『Installing Management Center for IDS Sensors 1.2 and Monitoring Center for Security 1.2』を参照してください。



ステップ 5 他の VMS コンポーネントをインストールする前に、システムを再始動する必要があります。システムが再起動されると、再び VMMC の Install Shield ウィザードに戻ります。[「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Windows にインストールする」](#)のセクションに示されているステップのうち、必要なものを繰り返します。

ステップ 6 IDS MC、Security Monitor および選択された他のインストールが終わったら、[「6 インストール後の作業」](#)のセクションにある CiscoWorks Desktop Server の設定に関する説明を参照します。

Management Center for Cisco Security Agents を Windows にインストールする

CSA MC をインストールすると、CSA MC などの CiscoWorks のデーモンおよび動作を保護するのに必要なポリシーが含まれるエージェントも自動的にインストールされます。このエージェントによって適用されるポリシーは、CSA MC、VMS コンポーネント、および一般的な CiscoWorks の動作を保護するためのポリシーです。

Cisco HIDS をアンインストールする

CSA MC は、Common Services または他のアプリケーションの前後にいつでも起動ディスクからインストールできます。ただし、Cisco IDS Host Sensor ソフトウェアと Management Center for Cisco Security Agents (CSA MC) の間に互換性がない可能性があるため、CSA MC またはエージェント ソフトウェアをインストールする前に、Cisco IDS Host Sensor および Cisco IDS Host Sensor Console ソフトウェアをアンインストールする必要があります。[「Cisco IDS Host Sensor と Console をアンインストールする」](#)のセクションを参照してください。

注 CSA MC をインストールするシステムには、Cisco IDS Host Sensor Console または Cisco IDS Host Sensor がインストールされてはなりません。CSA MC またはエージェントのインストーラがシステム上に Cisco IDS Host Sensor のいずれかのソフトウェアを検知した場合は、インストールが中止されます。

CSA MC のコンポーネントの登録

適切な製品ライセンスがない場合は、CSA MC のインストールを実行できません。まだライセンスを取得していない場合は、(添付のライセンス関連書類の封筒に同封されている) CSA MC の資格証明書に貼付された PAK ラベルを利用して、製品ライセンスを取得する必要があります。詳細については、[「Windows のコンポーネント登録」](#)のセクションを参照してください。



始める前に

CSA MC には、一部独自のシステム要件があります。このコンポーネントをインストールする前に、[「ブラウザ要件」のセクション](#)を参照してください。

他のコンポーネントをインストールするために CSA MC のエージェント ソフトウェアを無効にする

Cisco Security Agent (CSA) を使用して VMS を保護している場合に、各種 VMS コンポーネントをインストールまたはアンインストールするには、他の VMS コンポーネントをインストールまたはアンインストールする前に、そのエージェント サービスを無効にする必要があります (CSA MC をインストールまたはアンインストールする場合は、この作業は必要ありません。)

エージェント サービスを無効にするには、次の手順に従います。

ステップ 1 コマンド プロンプトから、**net stop "Cisco Security Agent"** と入力します。

ステップ 2 エージェント サービスを停止するかどうかを尋ねられた場合は、**Yes** を選択します。

ステップ 3 **net start "Cisco Security Agent"** と入力すれば、いつでもサービスを有効にできます。

注 エージェント サービスを無効にせずに CiscoWorks のシステム設定を変更しようとする、エージェントによってそのアクションが許可されなかったり、応答の必要な複数の問い合わせが表示される場合があります。

CSA MC をインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。



ステップ 1 VMMC の Install Shield ウィザードで **Managing Cisco Security Agents - Servers and Desktops** チェックボックスをオンにすると、ウィザードでチェックボックスをオンにした順序に従って **CSA MC** のインストールが開始されます。

注 **CSA MC** のインストールを手動で実行するには、VMMC の起動ディスクを **CD-ROM** ドライブに挿入し、**CSA MC** のトップレベル ディレクトリを探して、**setup.exe** ファイルをダブルクリックします。

ステップ 2 表示されるメッセージに従って、必要な情報を入力します。詳細については、「**Management Center for Cisco Security Agents をインストールする**」を参照してください。

ステップ 3 さまざまな **VMS** コンポーネントのインストールまたはアンインストールを行う際に **Cisco Security Agent** を使用して **VMS** を保護している場合は、[「他のコンポーネントをインストールするために CSA MC のエージェント ソフトウェアを無効にする」](#)のセクションを参照してください。

ステップ 4 添付のライセンス関連書類の封筒に同封されている **CSA MC** の資格証明書に貼付された **PAK** ラベルを利用して、製品ライセンスを取得する必要があります。詳細については、[「Windows のコンポーネント登録」](#)のセクションを参照してください。

注意 適切な製品ライセンスがない場合は、**CSA MC** のインストールを実行できません。

ステップ 5 インストールが完了したら、第 3 章「**Quick Start Configuration**」で説明されているセットアップの指示を読みます。**CiscoWorks Desktop Server** のセットアップに関する詳細については、この文書の[「6 インストール後の作業」](#)のセクションを参照してください。

RME Gatekeeper のリモート アクセスに関する問題

RME Gatekeeper デーモンに対するリモート アクセスが行えなくても、**VMS** のコンポーネントは正しく動作します。そのため、このデーモンに対するリモート クライアント アクセスは、**CiscoWorks VMS** モジュール ポリシーでは通常無効にされています。**RME Gatekeeper** デーモンに対するリモート アクセスが必要な **VMS** システムに **VMS** 以外の製品がインストールされている場合は、**CSA MC** の **VMS** ポリシーを次の手順に従って変更してください。



ステップ 1 CSA MC の CiscoWorks VMS モジュール ポリシー内で *CiscoWorks RME Gatekeeper daemon, server for UDP and TCP services* と記述されたルールを探します。

ステップ 2 このルールを有効にして、ルールプログラムを再作成します。

注 ルールを有効にしてルールプログラムを再作成する方法については、「Using Management Center for Cisco Security Agents 4.0」を参照してください。

Resource Manager Essentials を Windows にインストールする

注 RME は、RME のコンポーネント CD-ROM に収録されています。

ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM か Cisco.com で『Installation and Setup Guide for Resource Manager Essentials on Windows』を探して、前提条件およびセットアップ情報を確認します。

ステップ 2 第 1 章「Installing RME」の「Performing a New Installation」のセクションのステップに従います。

注 RME データベースのパスワードの変更を求めるメッセージが表示されたら、パスワードを変更することをお勧めします。

ステップ 3 インストールが完了したら、次の手順に従って RME が正しくインストールされたことを確認します。



- a. [「6 インストール後の作業」のセクション](#)に説明されているインストールとセットアップの指示に従って、CiscoWorks のデスクトップにアクセスします。

- b. **System Configuration > About the Server > Applications and Versions** の順に選択します。CiscoWorks の About the Server ページが表示されます。

- c. Applications Installed テーブルをチェックします。システム上に RME がインストールされ、有効にされている必要があります。

ステップ 4 『Installation and Setup Guide for Resource Manager Essentials on Windows』の第2章「Preparing to Use RME」に説明されているステップに従います。

ステップ 5 必要なパッチを適用するために、VMware の起動ディスクを再び挿入します。

ステップ 6 VMware 起動ディスクの Patches フォルダにある setup.exe ファイルをクリックして、Incremental Device Update (IDU) 5.0 for Resource Manager Essentials 3.5 をインストールします。

注 最新の IDU は、<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme> からダウンロードすることもできます。詳細については、『Installation and Setup Guide for Resource Manager Essentials on Windows, Software Release 3.5』を参照してください。

ステップ 7 Patches > VMSUpdate フォルダにある setup.exe をクリックして CiscoWorks VMS 2.2 Update 1 をインストールします。

ステップ 8 CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の [「6 インストール後の作業」のセクション](#)を参照してください。

注 RME Gatekeeper デーモンに対するリモート アクセスが行えなくても、VMS のコンポーネントは正しく動作します。そのため、このデーモンに対するリモート クライアント アクセスは、「CiscoWorks VMS module」ポリシーの拒否ルールでは通常無効にされています。詳細については、「RME Gatekeeper のリモート アクセスに関する問題」のセクションを参照してください。



VPN Monitor をインストールする

注 VPN Monitor は、VPN Monitor のコンポーネント CD-ROM に収録されています。

ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM か Cisco.com で『Installing VPN Monitor on Windows 2000 and Solaris』を探して、前提条件およびセットアップ情報を確認します。

ステップ 2 第 2 章「Installing and Uninstalling VPN Monitor on Windows 2000 and Windows NT」の「Installing VPN Monitor on Windows 2000 and Windows NT」のセクションに説明されているステップに従います。

ステップ 3 『Installation and Setup Guide for Resource Manager Essentials on Windows』の第 2 章「Preparing to Use RME」に説明されているステップに従います。

ステップ 4 CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の[「6 インストール後の作業」のセクション](#)を参照してください。

99 % の CPU 使用率に関するアップデート (CSCdt73198)

注意 同じサーバ上で、他の CiscoWorks のソリューション (LMS や RWAN など) を実行している場合は、このアップデートはインストールしないでください。

VMS サーバを実行しているシステムでは、特定の条件下で CPU 使用率が高くなる可能性があります。この高い CPU 使用率は、次の条件のいずれかによって発生する可能性があります。

- ネットワーク接続がダウンした。
- サーバが接続されているスイッチのダウンまたは再起動、あるいはその両方が発生した。
- サーバからイーサネット ケーブルが取りはずされた。
- ネットマスクまたは IP アドレス、あるいはその両方が変更された。



この問題に対するアップデートは、VMMC の起動ディスクに収録されています。

ステップ 1 VMMC インストール起動ディスクの CSCd73198-1 という名前の Patches ディレクトリに移動します。

ステップ 2 このディレクトリにある Readme ファイルの指示に従います。

5 Solaris への VMS のインストール

ここでは、Common Services、VMMC Solaris 起動ディスクに収録されている VMS Management and Monitoring Center (VMMC) のすべてのコンポーネント アプリケーション (Firewall MC、AUS、Router MC、IDS MC、Security Monitor、Performance Monitor)、および RME のインストール手順について説明します。

注意 このクイック スタート ガイドの情報は、初めて VMS コンポーネントをインストールする場合のみを対象に提供されています。実稼働中の展開済みシステムでは、これらの手順を実行しないでください。実行するとシステムに悪影響を及ぼす可能性があります。アップグレード手順については、「関連資料」のセクションにある個々のコンポーネントのインストール マニュアルを参照してください。

始める前に

- すべてのシステム要件が満たされていることを確認します。[「VMS のシステム要件」のセクション](#)を参照してください。
- 開かれているプログラムやアクティブなプログラムをすべて閉じます。インストールプロセス中に他のプログラムを実行しないでください。

Solaris にインストールする際の特記事項

ここには、インストールを開始する前に読む必要のある重要な情報が記載されています。

- CiscoWorks のアプリケーションは、次のデフォルト ディレクトリにインストールされます。
-/opt/CSCOpX



インストール中に別のディレクトリを選択すると、そのディレクトリにアプリケーションがインストールされます。

- デフォルトと異なるインストールディレクトリを選択した場合、選択したディレクトリへのリンクとして `/opt/CSCOpX` ディレクトリが作成されます。インストール後にこのリンクを削除すると、コンポーネントが正常に動作しなくなる可能性があります。
- インストール中にエラーが発生した場合は、インストール ログ ファイル `/var/tmp/ciscoinstall.log` を調べてください。
- **Ctrl-C** を押せば、いつでもインストールを中止できます。ただし、システムに加えられた変更（新しいファイルのインストールやシステム ファイルの変更など）は元には戻りません。

注 **Ctrl-C** でインストールを中止することはお勧めしません。中止した場合は、手動でインストールディレクトリをクリーンアップする必要があります。

-
- クライアントブラウザと管理サーバの間でセキュリティ保護されたアクセスを使用したい場合は、CiscoWorks デスクトップから **SSL** を有効または無効にできます。

SSL が有効な場合は、次のようになります。

- **http** ではなく **https** で始まる URL になり、安全な接続であることが示される。
- サーバ名に続くポート番号が **1741** ではなく **1742** になる。

SSL 準拠ではないアプリケーションがサーバにインストールされている場合は、CiscoWorks サーバで **SSL** を有効にすることはできません。

注 **SSL** をサポートしない CiscoWorks コンポーネントを使用する場合以外は、インストール時に **SSL** を有効にしておくことをお勧めします。**SSL** に関する詳細については、『**User Guide for CiscoWorks Common Services 2.2**』を参照してください。

-
- リモート マウント ポイントからインストールすると、ネットワークの不整合が原因でインストールエラーが発生する場合があります。



Solaris でのインストールの順序

ここでは、推奨されるインストール手順の概要を説明します。ここに説明されているインストール手順の順序を読んでから、詳細な指示について、以降の該当するセクションを参照することをお勧めします。

ステップ 1 Common Services をインストールします。[「CiscoWorks Common Services および SP2 を Solaris にインストールする」のセクション](#)を参照してください。

ステップ 2 VMMC 起動ディスクから、必要な VMMC アプリケーションを任意の順序でインストールします。次のいずれかを参照してください。

[「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Solaris にインストールする」のセクション。](#)

[「CiscoWorks Common Services および SP2 を Solaris にインストールする」のセクション。](#)

[「Management Center for Firewalls を Solaris にインストールする」のセクション。](#)

[「Management Center for VPN Routers を Solaris にインストールする」のセクション。](#)

[「Auto Update Server を Solaris にインストールする」のセクション。](#)

[「Monitoring Center for Performance を Solaris にインストールする」のセクション。](#)

[「Management Center for IDS Sensors および Monitoring Center for Security を Solaris にインストールする」のセクション。](#)



ステップ 3 RME をインストールします。[「Resource Manager Essentials を Solaris にインストールする」のセクション](#)を参照してください。

ステップ 4 セットアップに関する重要な情報について、[「6 インストール後の作業」のセクション](#)を参照します。

CiscoWorks Common Services および SP2 を Solaris にインストールする

注 Common Services と Service Pack 2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM または Cisco.com で『Installation and Setup Guide for CiscoWorks Common Services (includes CiscoView) for Solaris』を探します。

ステップ 2 第 2 章「Installing CiscoWorks Common Services」の「Preparing to Install CiscoWorks Common Services」のセクションを読みます。そのセクションで説明されているとおり、次の点を確認してください。

- CiscoWorks Common Services のインストール先サーバの root アクセス権を持っている。
- サーバの IP アドレスを知っている。
- CiscoWorks Common Services が使用する TCP ポートが、既存のアプリケーションと競合しない。

ステップ 3 CiscoWorks Common Services の管理者によって使用されるパスワードを決定します。パスワードを作成する際に従う必要のあるルールについては、付録 C 「Password Information」の「Admin Password」のセクションを参照してください。

ステップ 4 第 2 章「Installing CiscoWorks Common Services」の「Performing a New Installation」のセクションのステップに従います。

注 Common Services の最新アップデートを適用するために、この時点で CiscoWorks VMS Update1 をインストールする必要があります。



ステップ 5 次のように入力して、VMMC 起動ディスクから CiscoWorks VMS Update 1 をインストールします。

```
cd Patches
cd VMS_Update1
sh ./setup.sh
```

ステップ 6 この文書の [「6 インストール後の作業」のセクション](#) のステップに従います。

ステップ 7 インストールが完了したら、次の作業を行って CiscoWorks Common Services を使用する準備をします。

- a. CiscoWorks サーバを設定します。
 - b. クライアントを設定します。
-

VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Solaris にインストールする

Common Services のインストールが完了したら、VMMC の起動ディスクを使用して Management Center の任意のコンポーネントをインストールできます。ここで説明するステップに従って、起動ディスクに収録されているコンポーネントのマニュアルを見つけてインストールを開始した後、インストールするコンポーネントに応じて以降の VMMC インストール手順を実行します。

ステップ 1 VMMC の起動ディスクを CD-ROM ドライブに挿入します。ディレクトリ階層の一番上に各 VMMC コンポーネントに対応するフォルダがあります。ここで、任意のコンポーネントのディレクトリを表示して、コンポーネントの文書ディレクトリを表示すれば、必要なすべてのコンポーネント情報やすべてのインストールファイルのリストを表示できます。

ステップ 2 root のアクセス権で、VMMC の CD-ROM を Common Services をインストールしたシステムにマウントします。

ステップ 3 インストールプログラムを実行します。

- ローカル インストールの場合は、次のように入力します。



```
cd /cdrom/cdrom0/
```

```
./setup.sh
```

- リモート インストールの場合は、次のように入力します。

```
cd remotedir
```

```
./setup.sh
```

remotedir は CD-ROM がマウントされているリモートの場所です。

Common Services と Service Pack 2 がインストールされているかどうか、このインストール スクリプトによってただちに検出されます。Common Services をインストールする前に VMMC 起動ディスクを挿入した場合は、Common Services の CD-ROM を挿入するように求めるエラー メッセージが表示されます。Common Services のインストールが正しく完了すれば、次のメッセージが表示されます。Common Services SP2 is not installed. This patch will now be installed. Press Enter to continue.

ステップ 4 Enter キーを押して SP2 をインストールします。

SP2 のインストールが完了したら、次のメッセージが表示されます。CSCec43722-1 patch is not installed.This patch will now be installed. Press Enter to continue.

ステップ 5 Enter キーを押して CSCec43722-1 のパッチ アップデートをインストールします。

パッチ アップデート CSCec43722-1 のインストール後、すぐに引き続き 2 番目のパッチ アップデートのインストールが始まり、Installing Patch CSCed18592-1 という画面が表示されます。

注 これらのパッチのインストールは、連続してすばやく行われ、ユーザが介入する必要はありません。

スクリプトの処理が進むと、「ようこそ」のメッセージと 2 画面分の情報テキストが表示された後、次のような VMMC コンポーネントのリストが最後に表示されます。

1) Management Center for Firewalls



- 2) Router-MC
- 3) Auto Update Server
- 4) Suite for Performance Monitor Application
- 5) IDS MC/Security Monitor
- 6) All of the above

Select one or more items using its number separated by comma or enter q to quit:

ステップ 6 インストールするコンポーネントに対応する番号を 1 つ以上入力するか、6 を入力してすべてのコンポーネントを選択します。

確認メッセージが表示されます。次に例を示します。

Entered value is 3

INFO: You entered option 3) Auto Update Server.

インストール スクリプトは選択された順に実行され、ただちにスクリプトのメッセージがすばやく画面に表示され始めます。

ステップ 7 一般的なインストール手順について、各コンポーネントに該当する以降のセクションを参照します。

情報エラー メッセージが各コンポーネントのインストール処理の最後に表示されますが、すぐに次のコンポーネントのインストールが開始されるので読めません。選択したすべてのインストールが完了したら、次のメッセージが表示されます。

Software Installation Tool Completed, followed by a section of informational and error messages titled Summary of Installations.

このメッセージは、コンポーネントごとに整理されて再度表示されます。これらのメッセージにより、インストールが正しく完了したことが確認され、どの製品に再起動が必要か、問題が発生したかなどについての説明が表示されます。



ステップ 8 使用するクライアント システムを準備します。CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の「[インストール後の作業](#)」のセクションを参照してください。

Management Center for Firewalls を Solaris にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 「[関連資料](#)」のセクションで説明されているように、コンポーネント CD-ROM か Cisco.com で『Installing Management Center for Firewalls 1.2.2 on Windows 2000 and Solaris 2.8』を探して、前提条件およびセットアップ情報を確認します。

ステップ 2 [「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Solaris にインストールする」](#)のセクションに示されているステップ 1～3 に従います。

ステップ 3 インストール スクリプトによって表示されるメッセージに従います。

注意 システムのベースラインを確立し、データが損失しても Management Center (MC) を再インストールしなくても済むように、この時点で、すべてのシステム ファイルとデータベース ファイルのバックアップを作成することをお勧めします。「CiscoWorks Common Services 2.2 を Solaris にインストールする」に説明されている backup コマンドを使用して、システム ファイルとデータベースのバックアップを作成します。バックアップ データは必ずテープか CD-ROM に保存します。インストールが完了したら、CD-ROM をアンマウントします。

ステップ 4 インストールが完了したら、CD-ROM をアンマウントします。

ステップ 5 使用するクライアント システムを準備します。CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の「[6 インストール後の作業](#)」のセクションを参照してください。



Management Center for VPN Routers を Solaris にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM か Cisco.com で『Installing Management Center for VPN Routers 1.2.1 on Windows 2000 and Solaris』を探して、前提条件およびセットアップ情報を確認します。

ステップ 2 [「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Solaris にインストールする」のセクション](#)に示されているステップ 1～3 に従います。

ステップ 3 インストール スクリプトによって表示されるメッセージに従います。

ステップ 4 インストールが完了したら、CD-ROM をアンマウントします。

ステップ 5 使用するクライアントシステムを準備します。CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の [「6 インストール後の作業」のセクション](#)を参照してください。

Auto Update Server を Solaris にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。

注意 リモート マウント ポイントからインストールすると、ネットワークの不整合が原因でインストールエラーが発生する場合があります。



ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM か Cisco.com で『Installing Auto Update Server 1.1 on Windows 2000 and Solaris』を探して、前提条件およびセットアップ情報を確認します。

ステップ 2 [「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Solaris にインストールする」のセクション](#)に示されているステップ 1～3 に従います。

ステップ 3 インストール スクリプトによって表示されるメッセージに従います。これらにどう応答するかが変わってくるので、次の重要事項に注意してください。

- サポートされていないバージョンのプラットフォームまたは Service Pack が正しく適用されていないシステムに AUS をインストールしようとする、メッセージが表示されます。インストールを続行することはできませんが、そのコンポーネントを使用する前に、ご使用のプラットフォームまたは Service Pack をアップデートする必要があります。
- サーバのディスク容量またはメモリが不足している場合は、メッセージが表示された時点でインストールを中止し、システム管理者に相談してください。
- AUS は、インターネットからもアクセス可能な DMZ に展開するコンポーネントなので、最大限のセキュリティを確保するために、変更を求めるメッセージが表示されたらデータベース パスワードを変更することをお勧めします。

ステップ 4 インストールが完了したら、CD-ROM をアンマウントします。

ステップ 5 使用するクライアント システムを準備します。CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の[「6 インストール後の作業」のセクション](#)を参照してください。

Monitoring Center for Performance を Solaris にインストールする

注 Common Services と SP2 は、他の VMS コンポーネントよりも前にインストールする必要があります。



ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM か Cisco.com で『Installing Monitoring Center for Performance 2.0 on Solaris』を探して、前提条件およびセットアップ情報を確認します。

ステップ 2 [「VMS Management and Monitoring Center 2.2 のアプリケーションを起動ディスクから Solaris にインストールする」のセクション](#)に示されているステップ [1](#) ~ [3](#)に従います。

ステップ 3 インストール スクリプトによって表示されるメッセージに従います。

ステップ 4 インストールが完了したら、CD-ROM をアンマウントします。

ステップ 5 使用するクライアントシステムを準備します。CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の [「6 インストール後の作業」のセクション](#)を参照してください。

Management Center for IDS Sensors および Monitoring Center for Security を Solaris にインストールする

注 Common Services は、他の VMS コンポーネントよりも前にインストールする必要があります。

ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM か Cisco.com で『Installing Management Center for IDS Sensors 1.2 and Monitoring Center for Security 1.2』を探します。

ステップ 2 前提条件を読んで、次の項目を確認します。

- IDS MC と Security Monitor のインストール先サーバの root アクセス権を持っている。
-

注 Security Monitor を他の Management Center と同じ場所にインストールすることは可能ですが、Security Monitor は実稼動ネットワークの管理アプリケーションとは別のサーバにインストールすることをお勧めします。PIX Firewall と IDS Sensors の一方または両方をモニタリングすることにより、トラフィック処理の負荷が高くなる可能性があるためです。



- サーバの IP アドレスを知っている。
- これらのアプリケーションが使用する TCP ポートが、既存のアプリケーションと競合しない。
- このインストール マニュアルに示されたとおりに、他のシステム パラメータを調整した。

ステップ 3 インストーラにより、IDS MC のデータベースのパスワードと PostOffice の設定を求められます。インストールを続行するには、これらの情報を入力する必要があります。

ステップ 4 第 2 章「Installing, Upgrading, and Uninstalling IDS MC and Security Monitor」の「Installing IDS MC and Security Monitor」のセクションに説明されているステップに従います。

選択したすべてのコンポーネントのインストールが完了したら、次のメッセージが IDS MC/Security Monitor の Possible Warnings/Errors Encountered フィールドに表示されます。WARNING:/etc/system file has been updated. Please reboot the system to make the changes effect.

ステップ 5 インストール後に行う作業を開始する前に、システムを再起動します。

ステップ 6 第 3 章「Preparing to Use IDS MC and Security Monitor」に説明されているセットアップ手順を読みま。CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の [「6 インストール後の作業」のセクション](#)を参照してください。

Resource Manager Essentials を Solaris にインストールする

ステップ 1 [「8 関連資料」のセクション](#)で説明されているように、コンポーネント CD-ROM か Cisco.com で『Installation and Setup Guide for Resource Manager Essentials on Solaris』を探して、前提条件およびセットアップ情報を確認します。

ステップ 2 Common Services をインストールしたシステムに root としてログインします。

ステップ 3 次のいずれかの方法で RME の CD-ROM をマウントします。

- CiscoWorks Server のシステムに CD-ROM をマウントする。
- リモートの Solaris システムに CD-ROM をマウントし、CiscoWorks Server システムからアクセスする。



ステップ 4 インストールを開始します。

- ローカル インストールの場合は、次のように入力します。

```
cd /cdrom/cdrom0/
```

```
sh ./setup.sh
```

- リモート インストールの場合は、次のように入力します。

```
cd remotedir
```

```
sh ./setup.sh
```

remotedir は CD-ROM がマウントされているリモートの場所です。

ステップ 5 第 1 章「Installing Essentials」の「Performing a New Installation」のセクションのステップに従います。

注 RME データベースのパスワードの変更を求めるメッセージが表示されたら、パスワードを変更することをお勧めします。

ステップ 6 デバイスと機能に関する最新のアップデートを適用するために、VMMC の起動ディスクを再び挿入します。

ステップ 7 次のように入力して、VMMC の起動ディスクから RME Incremental Device Update 5.0 をインストールします。

```
cd Patches
```

```
cd IDU5.0
```



```
sh ./setup.sh
```

注 最新の IDU は、<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme> からダウンロードすることもできます。詳細については、『Installation and Setup Guide for Resource Manager Essentials on Windows, Software Release 3.5』を参照してください。

ステップ 8 次のように入力して、VMMC 起動ディスクから CiscoWorks VMS Update 1 をインストールします。

```
cd VMS_Update1
```

```
sh ./setup.sh
```

ステップ 9 インストールが完了したら、次の手順に従って RME が正しくインストールされたことを確認します。

a. CiscoWorks デスクトップにアクセスします。(CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の [「6 インストール後の作業」のセクション](#)を参照してください)

b. **System Configuration > About the Server > Applications and Versions** の順に選択します。CiscoWorks の About the Server ページが表示されます。

c. Applications Installed テーブルをチェックします。システム上に RME がインストールされ、有効にされている必要があります。次に RME のインストール マニュアルの第 2 章「Preparing to Use Essentials」に説明されているステップに従います。CiscoWorks Desktop Server のセットアップに関する詳細については、この文書の [「6 インストール後の作業」のセクション](#)を参照してください。

6 インストール後の作業

各コンポーネントのインストール マニュアルを参照して、すべてのセットアップ作業が完了していることを確認することが重要です。インストールが完了したら、次の作業を行います。

- 必要に応じてコンポーネントのセットアップ作業を行う。コンポーネントの文書と入手場所については、[「7 次のステップ」のセクション](#)を参照してください。



- Common Services および CSA MC を登録する。詳細については、[「Windows のコンポーネント登録」登録](#)のセクションおよび「[Solaris のコンポーネント登録](#)」のセクションを参照してください。
-

注意 Common Services を登録すれば、Common Services に依存するすべての Management Center がアクティブになります。登録を行わないと、これらのコンポーネントは 90 日で使用期限切れになります。

VMS のインストール ガイドの指示に従えば、VMS をアンインストールできます。各アプリケーションを、インストールとは逆の順序でアンインストールします。

注 依存関係にあるアプリケーションをアンインストールするまでは、CiscoWorks Common Services 2.2 をアンインストールしないでください。

Windows のコンポーネント登録

Common Services を登録すれば、Management Center がアクティブになります。Common Services のインストール時には、90 日間の無制限ライセンス ファイルが提供され、VMS アプリケーションの使用を開始できますが、手続きをしない場合は有効期限が切れます。CSA MC のインストール時には、一時ライセンスが提供されますが、CSA MC を登録して実稼動ライセンスを入手するまでは、アプリケーションは使用できません。そのため、すぐに実稼動ライセンスを入手してインストールすることをお勧めします。

Common Services と CSA MC の両方に Product Authorization Key (PAK) が必要です。Common Services の PAK は、PAK ラベルにあらかじめ印刷されており、VMMC の箱に添付されています。CSA MC の PAK ラベルは、同じく VMMC の箱に入っているライセンス封筒にある、CSA MC の資格証明書に添付されています。

CSA MC の実稼動ライセンスを入手するには、次のいずれかの方法でソフトウェアを登録してください。

ステップ 1 Cisco.com に登録済みのお客様は、次の Web サイトをご利用ください。

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl>

または



Cisco.com に登録していないお客様は、次の Web サイトをご利用ください。

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl>

ステップ 2 登録すると、登録時に指定した電子メールアドレスにソフトウェアライセンスが送信されます。この文書は、VMS のコンポーネント ソフトウェアの記録とともに保管しておいてください。

注 VMMC の箱に入っている『Registration and Licensing Notes for CiscoWorks Common Services 2.2』および、VMMC 起動ディスクの封筒に入っている CSA MC の資格証明書を参照してください。

Solaris のコンポーネント登録

Common Services を登録すれば、Management Center がアクティブになります。Common Services のインストール時には、90 日間の無制限ライセンス ファイルが提供され、VMS アプリケーションの使用を開始できますが、手続きをしない場合は有効期限が切れます。すぐに実稼動ライセンスを入手してインストールすることをお勧めします。

注 Common Services と CSA MC の両方に Product Authorization Key (PAK) が必要です。Common Services の PAK は、PAK ラベルにあらかじめ印刷されており、VMMC の箱に添付されています。

次の Web サイトのいずれかで、ご使用のソフトウェアを登録してください。VMMC の箱に添付された、PAK ラベルに印刷されている Product Authorization Key (PAK) を入力する必要があります。次のサイトで実稼動ライセンスを入手できます。

Cisco.com に登録済みのお客様は、次の Web サイトをご利用ください。

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl>

または

Cisco.com に登録していないお客様は、次の Web サイトをご利用ください。

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl>



登録すると、登録時に指定した電子メールアドレスにソフトウェア ライセンスが送信されます。この文書は、VMS のコンポーネント ソフトウェアの記録とともに保管しておいてください。

注 『CiscoWorks Common Services 2.2 に関する登録およびライセンス ノート』を参照してください。

7 次のステップ

必要な製品のインストールおよびインストール後に必要な作業を完了したら、VMS の使用を開始できます。詳細については、次のユーザ ガイドを参照してください。

- *User Guide for CiscoWorks Common Services 2.2*
- *Using Management Center for Firewalls 1.2*
- *Using Auto Update Server 1.1*
- *Using Management Center for VPN Routers 1.2.1*
- *Using Management Center for IDS Sensors 1.2*
- *Using Monitoring Center for Security 1.2*
- *Using Management Center for Cisco Security Agents 4.0*
- *User Guide for VPN Monitor*
- *User Guide for Resource Manager Essentials, Software Release 3.5*
- *Using Monitoring Center for Performance 2.0*

これらのマニュアルには、次の方法でアクセスできます。

- VMMC 2.2 起動ディスクの Documentation ディレクトリでは PDF 形式で提供。
- Cisco.com では HTML 形式と PDF 形式で提供。次の手順でアクセスできます。

a. Cisco.com にログインします。

b. Products & Services > Network Management CiscoWorks > CiscoWorks VPN/Security Management Solution の順に選択します。

c. 該当するコンポーネントを選択します。

d. Technical Documentation > User Guides の順に選択します。



e. このリリース用に書かれたマニュアルを選択します。

- VMS の各コンポーネントに内蔵されているオンライン ヘルプで提供。

8 関連資料

インストール マニュアルとユーザ マニュアルは、各コンポーネントの documentation ディレクトリにある VMMC リストに PDF 形式で提供されています。各コンポーネントのリリース ノートには、各コンポーネントのすべての資料のリストが、発注情報とともに記載されています。VMS の資料はすべて Cisco.com にも掲載されています。**Products & Services > Network Management CiscoWorks > CiscoWorks VPN/Security Management Solution > Versions and Options > CiscoWorks VPN/Security Management Solution 2.2** の順に選択してください。

注 印刷文書および電子文書に記載されている情報が正確であることは最善を尽くして検証されていますが、更新された情報を確認するために Cisco.com のドキュメントを参照することも必要です。

印刷文書

- VPN/Security Management Solution 2.2 クイック スタート ガイド
- Readme for Management Center for Cisco Security Agents 4.0.1*
- CiscoWorks Common Services 2.2 に関する登録およびライセンス ノート
- Release Notes for CiscoWorks Common Services 2.2 (includes CiscoView 5.5) on Solaris 2000*
- Release Notes for CiscoWorks Common Services 2.2 (includes CiscoView 5.5) on Windows 2000*
- Release Notes for Management Center for Firewalls 1.2.2 on Windows 2000 and Solaris 2.8*
- Release Notes for Auto Update Server 1.1 on Windows 2000 and Solaris*
- Release Notes for Management Center for VPN Routers 1.2.1 on Windows 2000 and Solaris*
- Release Notes for Management Center for IDS Sensors 1.2.3 and Monitoring Center for Security 1.2.3*
- Release Notes for Management Center for Cisco Security Agents 4.0*
- Release Notes for Monitoring Center for Performance 2.0 on Solaris*
- Release Notes for Resource Manager Essentials on Solaris, Software Release 3.5*
- Release Notes for Resource Manager Essentials on Windows, Software Release 3.5*
- Release Notes for VPN Monitor 1.2.1 on Windows and Solaris*

オンライン ヘルプおよびその他すべての資料



•オンライン ヘルプには次の 2 つの方法でアクセスできます。

- ナビゲーション ツリーでオプションを選択してから、**Help** をクリックする。
- ダイアログ ボックスの **Help** ボタンをクリックする。

PDF :

- Installation and Setup Guide for CiscoWorks Common Services (includes CiscoView) on Windows*
- User Guide for CiscoWorks Common Services 2.2*
- Installing Management Center for Firewalls 1.2.2 on Windows 2000 and Solaris 2.8*
- Using Management Center for Firewalls 1.2*
- Supported Devices, OS Versions, and Commands for Management Center for Firewalls 1.2.1*
- Installing Auto Update Server 1.1 on Windows 2000 and Solaris*
- Using Auto Update Server 1.1*
- Supported Devices and Software Versions for AUS 1.1*
- Installing Management Center for VPN Routers 1.2.1 on Windows 2000 and Solaris*
- Using Management Center for VPN Routers 1.2.1*
- Supported Devices Table for Management Center for VPN Routers 1.2*
- Installing Management Center for IDS Sensors 1.2 and Monitoring Center for Security 1.2*
- Using Management Center for IDS Sensors 1.2*
- Supported Devices and Software Versions for Management Center for IDS Sensors 1.2*
- Using Monitoring Center for Security 1.2*
- Supported Devices and Software Versions for Monitoring Center for Security 1.2*
- Management Center for Cisco Security Agents をインストールする*
- Using Management Center for Cisco Security Agents*
- Installing Monitoring Center for Performance 2.0 on Solaris*
- Using Monitoring Center for Performance 2.0*
- Supported Devices and Software Versions for Monitoring Center for Performance 2.0*
- Installation and Setup Guide for Resource Manager Essentials on Windows, Software Release 3.5*
- Installation and Setup Guide for Resource Manager Essentials for Solaris, Software Release 3.5*
- User Guide for Resource Manager Essentials, Software Release 3.5*
- Supported Device Table for Resource Manager Essentials 3.5*

注 Adobe Acrobat Reader 4.0 以降が必要です。



9 資料の入手

マニュアル、技術サポート、およびその他の技術リソースは、さまざまな方法で入手できます。ここでは、シスコシステムズから技術情報を入手する方法を説明します。

Cisco.com

次の URL にアクセスすると、シスコの最新資料をワールドワイド ウェブ上で入手できます。

<http://www.cisco.com/univercd/home/home.htm>

シスコの Web サイトには、次の URL でアクセスできます。

<http://www.cisco.com>

世界各国のシスコの Web サイトには、次の URL でアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

購入された製品に付属している Cisco Documentation CD-ROM には、シスコのマニュアルと補足資料が収録されています。Documentation CD-ROM は定期的に更新されるため、印刷資料よりも新しい情報が掲載されている場合があります。この CD-ROM パッケージは、単独の製品として入手できるほか、年間または四半期単位の購読手続きによって入手することもできます。

Cisco.com の登録ユーザ様は、次の URL で Cisco Ordering Tool を使用して、単体の Documentation CD-ROM（製品番号 DOC-CONDOCCD=）をご注文いただけます。

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

すべてのユーザ様は、次の URL にあるオンラインの Subscription Store から、年単位または四半期単位の登録をご注文いただけます。

<http://www.cisco.com/go/subscription>

左のナビゲーション バーにある Subscriptions & Promotional Materials をクリックしてください。



資料のご注文

資料の注文方法については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

シスコの資料は、以下の方法でご注文いただけます。

- Cisco.com の登録ユーザ様（シスコ直販のお客様）は、Networking Products MarketPlace からシスコ製品の資料をご注文いただけます。

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Cisco.com にまだ登録されていないユーザ様の場合は、米国シスコシステムズ本社（カリフォルニア州）にお電話をいただき、地域顧客営業担当を通じて資料をご注文いただけます。米国内からは 408 526-7208 まで、北米の他地域からは 800 553-NETS (6387) までお電話ください。

10 資料に関するご意見

技術資料に関するご意見を電子メールでお送りいただく場合は、bug-doc@cisco.com へご送付ください。

文書の表紙の後にレスポンスカードがある場合は、それにご記入いただくか、下記の住所にご意見をお送りいただくこともできます。

Cisco Systems

Attn: Customer Document Ordering

170 West Tasman Drive

San Jose, CA 95134-9883

お客様からのご意見を心よりお待ちしております。

11 技術サポート

有効な Cisco サービス契約をお持ちのすべてのお客様、パートナー様、販売店様、代理店様に対しては、オンラインおよび電話での 24 時間体制による Cisco Technical Assistance Center (TAC) の技術サポート サービスをご提供いたします。Cisco.com では、技術サポートのオンライン窓口として Cisco TAC Web サイトをご用意しています。有効な Cisco サービス契約をお持ちでない場合は、担当の販売代理店までご連絡ください。



Cisco TAC Web サイト

Cisco TAC Web サイトでは、シスコの製品とテクノロジーに関する技術的な問題のトラブルシューティングと解決を支援するために、オンラインドキュメントおよびツールを提供しています。Cisco TAC Web サイトは、365 日 24 時間ご利用いただけます。Cisco TAC Web サイトへは、次の URL からアクセスできます。

<http://www.cisco.com/tac>

Cisco TAC Web サイトにあるすべてのツールへのアクセスには、Cisco.com のユーザ ID とパスワードが必要です。有効なサービス契約を締結しているが、ログイン ID またはパスワードをお持ちでないというお客様は、次の URL で登録を行ってください。

<http://tools.cisco.com/RPF/register/register.do>

TAC ケースのオープン

P3 および P4 のケースの場合は、オンラインの TAC Case Open Tool を使用すると、最もすばやくケースをオープンできます。(P3 および P4 のケースとは、ネットワークの機能低下がごくわずかである状況や、製品情報を入力する必要がある状況に該当します)。TAC Case Open Tool で現在の状況を入力すると、当面の解決策として、推奨リソースが自動的に提示されます。提示されたリソースで問題が解決されない場合は、Cisco TAC エンジニアが割り当てられます。オンラインの TAC Case Open Tool へは、次の URL からアクセスできます。

<http://www.cisco.com/tac/caseopen>

P1 または P2 のケース (P1 および P2 のケースとは、実稼動ネットワークがダウンしているか、著しく機能が低下している場合です) またはインターネットにアクセスできない場合は、電話で Cisco TAC にご連絡ください。P1 および P2 のケースの場合は、お客様の円滑な業務を維持するために、Cisco TAC のエンジニアがただちに割り当てられます。

電話でケースをオープンする場合の連絡先は次のとおりです。

アジア太平洋 : +61 2 8446 7411 (オーストラリア : 1 800 805 227)

EMEA : +32 2 704 55 55

米国 : 1 800 553-2447

Cisco TAC の全連絡先のリストは、次の URL で参照できます。

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>



TAC ケース プライオリティの定義

シスコでは、すべてのケースの報告形式を標準化するために、以下のようにケースのプライオリティを定義しています。

プライオリティ 1 (P1) : 既存のネットワークが「ダウン」しているか、お客様の事業運営に重大な影響がある。お客様とシスコの両方が、必要なすべてのリソースを 24 時間体制で保証して問題の解決を図る。

プライオリティ 2 (P2) : 既存のネットワークの運用パフォーマンスが著しく低下しているか、シスコ製品のパフォーマンスが不適切であるためにお客様の事業運営に重大な悪影響が及んでいる。お客様とシスコの両方が、通常の営業時間にフルタイムのリソースを割り当てて問題の解決を図る。

プライオリティ 3 (P3) : ネットワークの運用パフォーマンスに影響があるが、ほとんどの事業運営は引き続き適切に行える。サービスを満足できるレベルに回復するために、お客様とシスコの両方が、通常の営業時間にリソースを割り当てて解決を図る。

プライオリティ 4 (P4) : お客様が、シスコ製品の機能、インストール、設定などに関して、情報または支援を必要としている。事業運営には、ほとんど、またはまったく影響がない。

12 補足資料と情報の入手

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報は、さまざまなオンラインソースや出版ソースから入手できます。

- Cisco Product Catalog には、シスコシステムズが提供しているネットワーク製品の説明があり、製品の発注およびカスタマー サポート サービスにも利用できます。Cisco Product Catalog には、次の URL でアクセスできます。

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press では、ネットワーキング、トレーニング、および認定に関する一般的な書籍を幅広く発行しています。これらの出版物は、新しいユーザにとっても、経験豊富なユーザにとっても有益なものです。Cisco Press の最新の書籍と他の情報については、次の URL にある Cisco Press にアクセスしてください。

<http://www.ciscopress.com>

- Packet はシスコの季刊誌で、ネットワーク技術の最新トレンド、最新テクノロジー、およびシスコの製品とソリューションをネットワーク業界の専門家に提供します。ネットワークの展開やトラブルシューティングに関するヒント、設定例、お客様の事例、チュートリアルとトレーニング、認定情報、および多数の詳細なオンライン リソースへのリンクが掲載されています。Packet には、次の URL でアクセスできます。

<http://www.cisco.com/packet>

- iQ Magazine はシスコの隔月誌で、インターネット ビジネス戦略に関する最新情報を管理職に提供します。iQ Magazine には、次の URL でアクセスできます。

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal は、シスコシステムズが発行している季刊誌です。パブリックまたはプライベートなインターネットおよびイントラネットのデザイン、開発、および運用に携わる工学専門家を対象にしています。Internet Protocol Journal には、次の URL でアクセスできます。

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- トレーニング：シスコでは、高度なネットワーキング トレーニングを提供しています。現在提供しているトレーニングの一覧は、次の URL に表示されています。

<http://www.cisco.com/en/US/learning/index.html>

©2004 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-6670-2992

電話でのお問合せは、以下の時間帯で受け付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先