仮想マシンの高可用性とディザスタリカバリ

このマニュアルでは、VMware ベースの高可用性（HA）環境やディザスタリカバリ（DR）環境に Cisco Security Management Suite（Security Manager）をインストールする方法について説明します。Security Manager は、次のシナリオをサポートしています。

- ホストベースのフェールオーバー（ローカル HA） （1 ページ）
- フォールトトレランス （3 ページ）
- ディザスタ カバリ （7 ページ）

上記のシナリオで Security Manager を設定する手順は次のとおりです。

- ホストベースのフェールオーバー（ローカル HA） （1 ページ）
- フォールトトレランス （3 ページ）
- ディザスタ カバリ （7 ページ）

ホストベースのフェールオーバー（ローカル HA）

この設定では、Security Manager は VMware クラスタ内の ESXi ホスト上の仮想マシンにインストールされます。既存の ESXi ホストでハードウェア障害が発生した場合、ホストベースのフェールオーバー設定により、VMware クラスタ内の別のホストで同じ仮想マシン（VM）が自動的に起動します。

VMware HA エージェントは、プライマリホストとセカンダリホスト間で 1 秒ごと（デフォルト）に送信されるハートビートをモニターして、ホストの障害を検出します。冗長ハートビートネットワークを設定することをお勧めします。これにより、信頼性の高い障害検出が可能になり、隔離状態の発生を防ぐことができます。

同じオペレーティングシステムとアプリケーションボリュームを持つ同じプライマリ VM が、別の ESXi ホストで起動されます。ホストベースのフェールオーバー設定では、ホスト名と IP アドレスは同じままです。この設定は、物理ホスト間の共有 SAN インフラストラクチャで機能します。別のホストへのフェールオーバーのこのプロセスには数分かかる場合があります。

（注） 次の設定は参照目的でのみ使用されます。VMware インフラストラクチャを設定するための特定の手順については、VMware のドキュメントを参照する必要があります。この章で説明する手順は、Security Manager 固有の手順ではありません。

VMware HA クラスタ作成の前提条件

VMware クラスタを作成するには、次の前提条件を満たす必要があります。

- すべての仮想マシンとその構成ファイルは、ストレージ エリア ネットワーク（SAN）などの共有ストレージに存在する必要があります。
- ESXi ホストは、同じ仮想マシンネットワークにアクセスできるように設定する必要があります。
- VMware HA クラスタ内の各ホストには、ホスト名と静的 IP アドレスが割り当てられている必要があります。
- ホスト間に CPU の互換性が必要です。理想的なクラスタは、ハードウェアとメモリのサイズが完全に一致するクラスタです。
- 冗長なサービスコンソールと VMkernel ネットワーク設定を使用することをお勧めします。

ホストベースのフェールオーバー用 Security Manager の設定

ホストベースのフェールオーバー用に Security Manager を設定するには、次の手順を実行します。

ステップ 1 『*Deployment Planning Guide for Cisco Security Manager 4.27*』[英語] で説明されている要件を満たす 2 つの物理ホストを設定します。

（注） 各ホストの CPU には互換性がある必要があります。

ステップ 2 ステップ 1 で作成した各ホストに VMware ESXi をインストールします。

ステップ 3 vCenter でクラスタを作成し、ESXi ホストをクラスタに追加します。

ステップ 4 ESXi ホストで vSphere HA 設定を構成します。詳細については、VMware のマニュアルを参照してください。

ステップ 5 ESXi ホストの 1 つに VM を作成します。詳細については、『*Deployment Planning Guide for Cisco Security Manager 4.27*』[英語] を参照してください。

ステップ 6 ステップ 5 で作成した VM に Security Manager をインストールします。詳細については、『*Installation Guide for Cisco Security Manager 4.27*』[英語] を参照してください。

ステップ 7 Security Manager を起動します。

Security Manager が VM にインストールされている ESXi ホストでハードウェア障害が発生した場合、VM はクラスタ内の他の ESXi ホストに移動され、VM が起動します。この移動は完了するまでに数分かかるため、ダウンタイムが発生します。

制限事項

ホストベースのフェールオーバー設定には、次の制限があります。

- 障害が発生したホストで仮想マシンを手動で再起動する必要があります。
- 障害が発生したホスト上の VM でアプリケーションの稼動が停止し、アプリケーションデータが破損した場合、フェールオーバー後に VM を手動で再起動しても、アプリケーションは使用できないままになる可能性があります。
- VMware クラスタ内のホストがハートビートネットワークへの接続を失っても、ホスト自体が実行されている場合、そのホストはクラスタから分離されます。この場合、VMware High Availability ソリューションは、ホストがクラスタから分離されていると判断する前に 12 秒間待機します。

（注） アプリケーションベースのモニタリングは、Security Manager ではサポートされていません。つまり、Security Manager プロセスが実行を停止しても、自動的に再起動されません。手動で問題を解決し、プロセスを再起動してから、手動で Security Manager を再起動する必要があります。

フォールトトレランス

VMware Fault Tolerance 設定では、ホストでハードウェア障害が検出されると、別のホストに 2 番目の VM が作成され、サービスを中断することなく、2 番目の VM で Security Manager の実行が開始されます。VMware Fault Tolerance は、新しいレベルのゲスト冗長性を実現します。VMware Fault Tolerance では、VM の 2 つのコピーがそれぞれ別のホストに保持されます。この機能は、Security Manager がインストールされている VM で耐障害性をオンにすることで有効にできます。

VMware Fault Tolerance とホストベースのフェールオーバー（HA）ソリューションの主な違いは、ESX/ESXi ホストに障害が発生した場合に VM の動作が中断されることです。耐障害性システムは新しいホストに即座に移行しますが、高可用性システムは別のホストで再起動する前にホストで VM に障害が発生したことを確認します。障害が発生したホスト上の VM はプライマリ VM と呼ばれ、引き継ぐ VM はセカンダリ VM と呼ばれます。プライマリ VM からセカンダリ VM へのフェールオーバーは動的で、セカンダリ VM はプライマリ VM が終了した正確なポイントから実行を継続します。このプロセスは自動的に実行され、データの損失、ダウンタイム、またはサービスの中断は発生しません。動的なフェールオーバーの後、セカンダリ VM が新しいプライマリ VM になり、新しいセカンダリ VM が自動的に生成されます。

（注） 次の設定は参照目的でのみ使用されます。VMware インフラストラクチャを設定するための特定の手順については、VMware のドキュメントを参照する必要があります。この章で説明する手順は、Security Manager 固有の手順ではありません。

耐障害性システムの作成

前提条件

耐障害性システムを作成するには、次の前提条件を満たす必要があります。

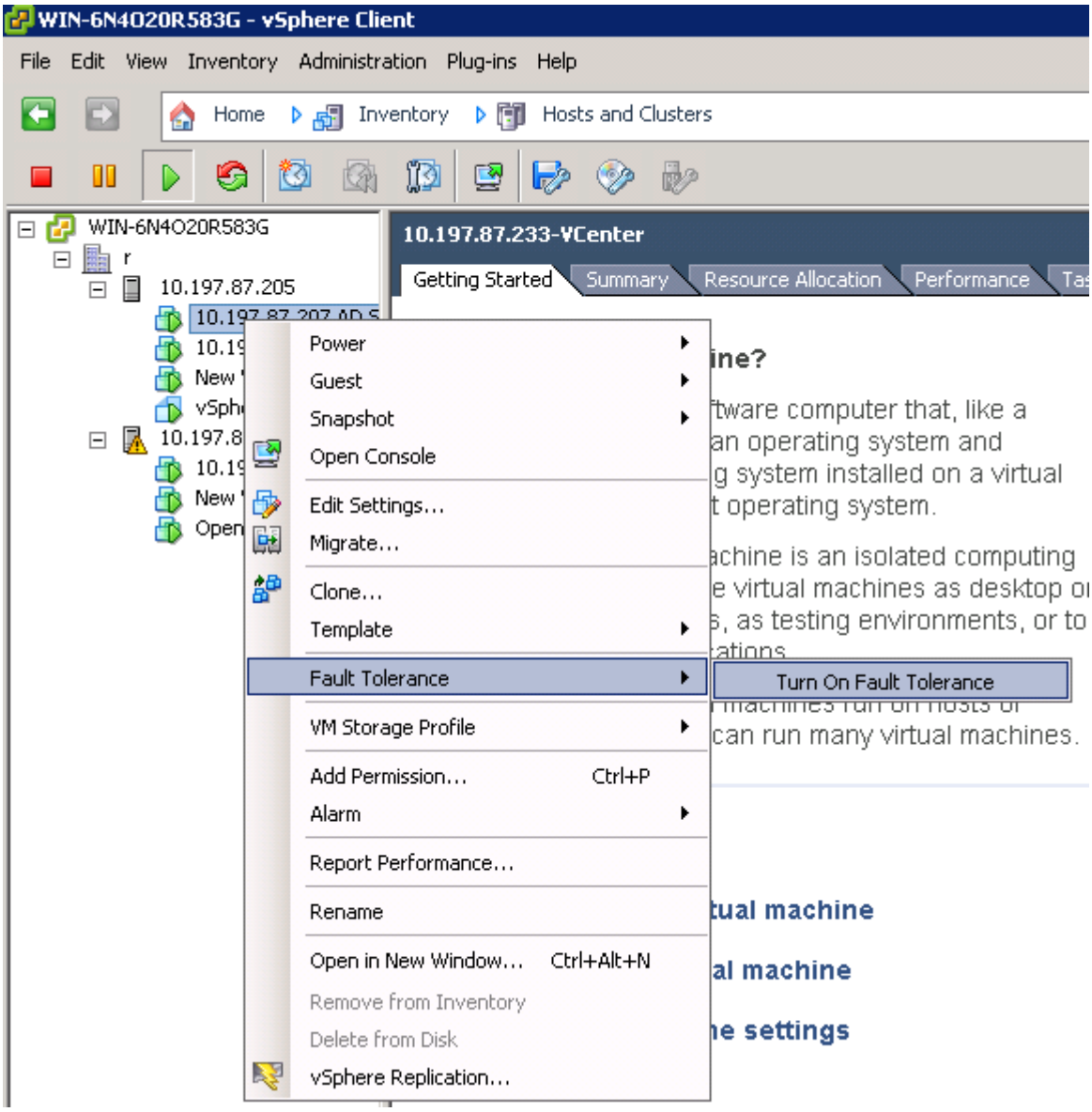
- 耐障害性環境で使用される VMware ソフトウェアのすべてのバージョンが、vSphere 互換性マトリックスのリストに従って互換性があることを確認します。詳細については、『VMware Compatibility Guide』を参照してください。
- ハードウェアおよびゲスト オペレーティング システム レベルでは、特定のプロセッサとオペレーティングシステムのみがサポートされます。サポートの詳細については、『VMware Guest OS Compatibility Guide』（http://www.vmware.com）[英語] を参照してください。さらに、既存の VMware 設定がフォールトトレランスに適しているかどうかを確認するには、https://www.vmware.com/support/shared_utilities [英語] でサイト調査を実行します。
- クラスタ内の各ホストの BIOS でハードウェア仮想化を有効にします。ハードウェア仮想化を有効にするプロセスは BIOS ごとに異なるため、ハードウェア仮想化を有効にする具体的な手順については、ハードウェアベンダーにお問い合わせください。
- VMware Fault Tolerance で使用されるすべての ESX ホストが VMware High Availability（HA）クラスタのメンバーであることを確認します。VMware Fault Tolerance を機能させるには、VMware HA を有効にする必要があります。VMware HA の有効化については、『vSphere Availability Guide』（http://www.vmware.com）[英語] を参照してください。
- プライマリおよびセカンダリ耐障害性ノードを実行する ESX ホストが同じビルドの ESX を実行していることを確認します。さらに、パッチには VMware 耐障害性機能の改善が含まれているため、リリースされたパッチを必ず適用してください。
- VMware Fault Tolerance を有効にするには、使用している環境で次のように設定されていることを確認します。
  - 仮想マシンは、共有ストレージ、つまり、クラスタ内のすべての ESX ホストに表示されるストレージに存在する必要があります。
  - ストレージは、ローカルストレージではなく、FC SAN、iSCSI、または NFS である必要があります。
  - 仮想マシンにはスナップショットを含めることはできません。スナップショットがある場合は、続行する前にコミットする必要があります。
- 耐障害性環境でネットワーキングを設定するには、次のタスクを実行してください。

- 耐障害性ロギング用に別の VMkernel ポートグループを定義します。ポートグループを作成する手順については、『ESX Configuration Guide』[英語] を参照してください。
- 耐障害性ロギングおよび VMotion ポートグループを定義し、アップリンク用の物理ネットワークカードを割り当てます。このネットワークカードのサイズは 1GB 以上である必要があります。10GB のネットワークカードを使用することをお勧めします。
- 耐障害性ロギングでのジャンボフレームの使用を有効にします。詳細な手順については、『ESX Configuration Guide』の「Advanced Networking」のセクション [英語] を参照してください。
- VMware では、可用性を確保するために完全な冗長 NIC を有効にすることを推奨していますが、耐障害性は冗長 NIC がなくても機能できます。

前提条件のリストに従って環境を設定したら、次の図に示すように、耐障害性をオンにします。

図 423485

図 *1*: 耐障害性オン設定



（注） VMware ESXi バージョン 5.102 から ESXi バージョン 6.0 までの小規模展開では、Security Manager に少なくとも 6 つの仮想 CPU が必要です。詳細については、『*Cisco Security Manager Deployment Planning Guide*』[英語] を参照してください。

（注） vCenter Server バージョン 5.x の耐障害性仮想マシンは、保護された仮想マシンごとに 1 つの仮想 CPU をサポートします。 vCenter Server バージョン 6.0 は、ライセンスに応じて最大 4 つの仮想 CPU をサポートします。

ディザスタ カバリ

Security Manager は、VMware vCenter Site Recovery Manager ツールを VMware vSphere Replication とともに使用して、ディザスタリカバリと管理を行います。

Site Recovery Manager は、VMware vSphere Replication とネイティブに統合され、ビジネス要件に応じてサイト間で仮想マシンを確実にコピーするために、さまざまな高性能アレイベースのレプリケーション製品をサポートします。Site Recovery Manager は、仮想マシンのリカバリの計画、テスト、および実行に役立つディザスタ リカバリ ソリューションを提供する VMware vCenter Server の拡張機能です。Site Recovery Manager は、複製されたデータストアを検出して管理し、vCenter Server インスタンス間のインベントリの移行を自動化できます。

システム要件

ハードウェア要件

ハードウェア要件については、*VMware Site Recovery Manager 6.1 Documentation Center*（http://www.vmware.com）[英語] を参照してください。

ソフトウェア要件

次に、ディザスタリカバリ用の VMware Site Recovery Manager ソリューションを設定するためのソフトウェア要件の概要を示します。

- Virtual Center 6.0 ライセンスがプライマリ（保護された）サイトとリカバリサイトの両方に適用されている。
- ESXi Server 6.0 ライセンスがプライマリサイトとリカバリサイトの両方に適用されている。
- VSphere SRM 6.0ライセンスがプライマリサイトとリカバリサイトの両方に適用されている。
- Site Recovery Manager 用の SQL Server データベースがプライマリサイトとリカバリサイトの両方にインストールされている。

（注） すべての VMware ツールがバージョン 6.0 である必要があります。

（注） VMware Disaster Recovery ソリューションは VMware Site Recovery Manager でテスト済みです。ただし、他の VMware ソリューションも Security Manager で動作する場合があります。

VMware Site Recovery Manager の設定

vCenter サーバーに Site Recovery Manager をインストールするには、次の手順を実行します。

ステップ 1 **install.exe** をクリックして、Site Recovery Manager のインストールを開始します。

ステップ 2 VMware エンドユーザーライセンス契約書に同意します。

ステップ 3 [VMware vCenter Site Recovery Manager—vSphere Replication（VMware vCenter Site Recovery Manager—vSphere Replication）] ウィンドウで、[vSphere Replicationのインストール（Install vSphere Replication）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 vCenter サーバーのアドレス、ポート（デフォルトでは 81）、ユーザー名、およびパスワードを入力します。

ステップ 5 セキュリティ警告を受け入れます。

ステップ 6 [VMware vCenter Site Recovery Manager：証明書タイプの選択（VMware vCenter Site Recovery Manager—Certificate Type Selection）] ウィンドウで、[証明書ソース（Certificate Source）] として [証明書の自動生成（Automatically Generate a Certificate）] を選択します。

ステップ 7 vCenter サーバー情報を入力します。

[VMware vCenter Site Recovery Managerエクステンション（VMware vCenter Site Recovery Manager Extension）] ウィンドウで、次のように入力します。

- [ローカルサイト名（Local Site name）]：VCenter サイトの完全修飾ドメイン名。
- [管理者の電子メール（Administrator Email）]：組織の要件に応じた管理者の電子メール。
- [追加の電子メール（Additional Email）]：入力する追加の電子メール ID。
- [ローカルホスト（Local Host）]：現在のホストの IP アドレス。これは自動的に入力されます。
- リスナーポート
  - [SOAPポート（SOAP Port）]：デフォルトは 8095 です。
  - [HTTPポート（HTTP Port）]：デフォルトは 9085 です。
- [APIリスナーポート（API Listener Port）]：デフォルトは 9007 です。

ステップ 8 Site Recovery Manager サーバーには、リカバリ計画やインベントリ情報などのデータを保存するために使用する独自のデータベースが必要です。Site Recovery Manager データベースは、Site Recovery Manager インストールの重要な部分です。Site Recovery Manager をインストールする前に、Site Recovery Manager データベースを作成し、データベース接続を確立する必要があります。

[VMware vCenter Site Recovery Manager—データベース設定（VMware vCenter Site Recovery Manager—Database Configuration）] ウィンドウで、次のように入力し、[次へ（Next）] をクリックします。

- ドロップダウンリストから、[データベースクライアントタイプ（Database Client type）] を選択します。
- [データソース名（Data Source Name）] を入力します。[ODBC DSN設定（ODBC DSN Setup）] をクリックして、システム DSN を設定します。
- [データベースユーザー名（Database Username）] と [パスワード（assword）] を入力します。
- [接続数（Connection Count）] と [最大接続数（Maximum Connections）] を入力します。

図 *2*：データベースの設定

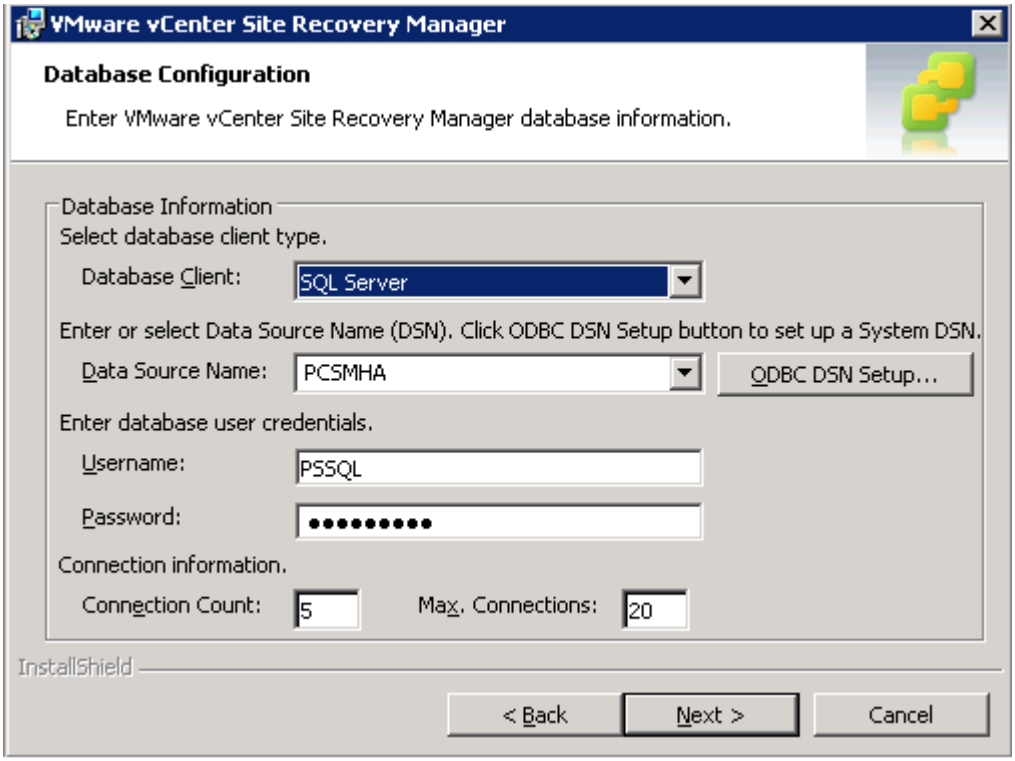
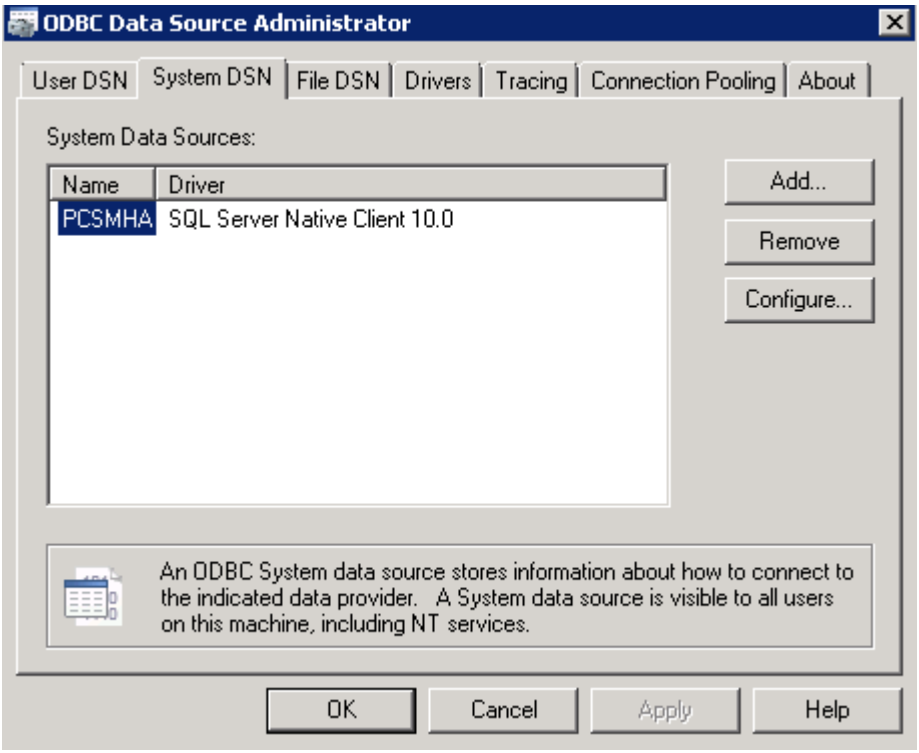


図 *3 : OBDC DSN* の設定



ステップ 9 [次へ（Next）] をクリックして、Site Recovery Manager のインストールを完了します。

（注） 各 Site Recovery Manager サイトには、Site Recovery Manager データベースの独自のインスタンスが必要です。サイトごとに個別の Site Recovery Manager データベースを実行するには、異なるデータベース サーバー インスタンスを使用します。同じデータベース サーバー インスタンスを使用して両方のサイトのデータベースを実行する場合や、データベースサーバーで問題が発生すると、Site Recovery Manager サイトは機能せず、リカバリを実行できなくなります。

vCenter の設定

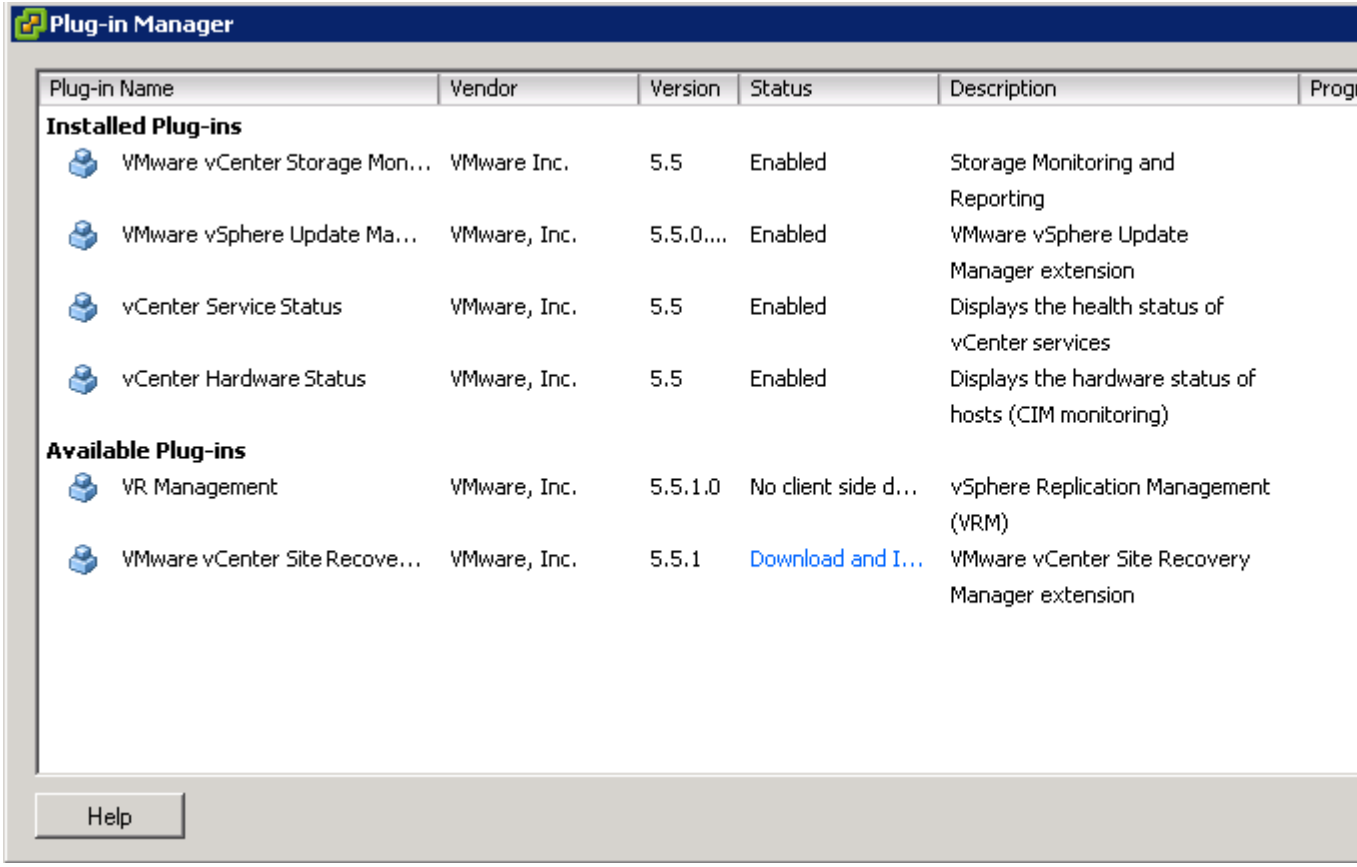
保護サイトで vCenter を設定するには、次の手順を実行します。

vCenter サーバーの詳細は、ステップ 7 で指定したものです。vCenter サーバー情報を入力すると、Site Recovery Manager 5.5 プラグインマネージャが有効になります。

ステップ 1 プラグインマネージャから、VMware vCenter Site Recovery Manager 拡張機能をダウンロードしてインストールします。

（注） 上記の手順は、Site Recovery Manager バージョン 5.5 にのみ適用されます。Site Recovery Manager バージョン 6.0 では、vSphere Web クライアントをサポートしているため、プラグインをインストールする必要はありません。

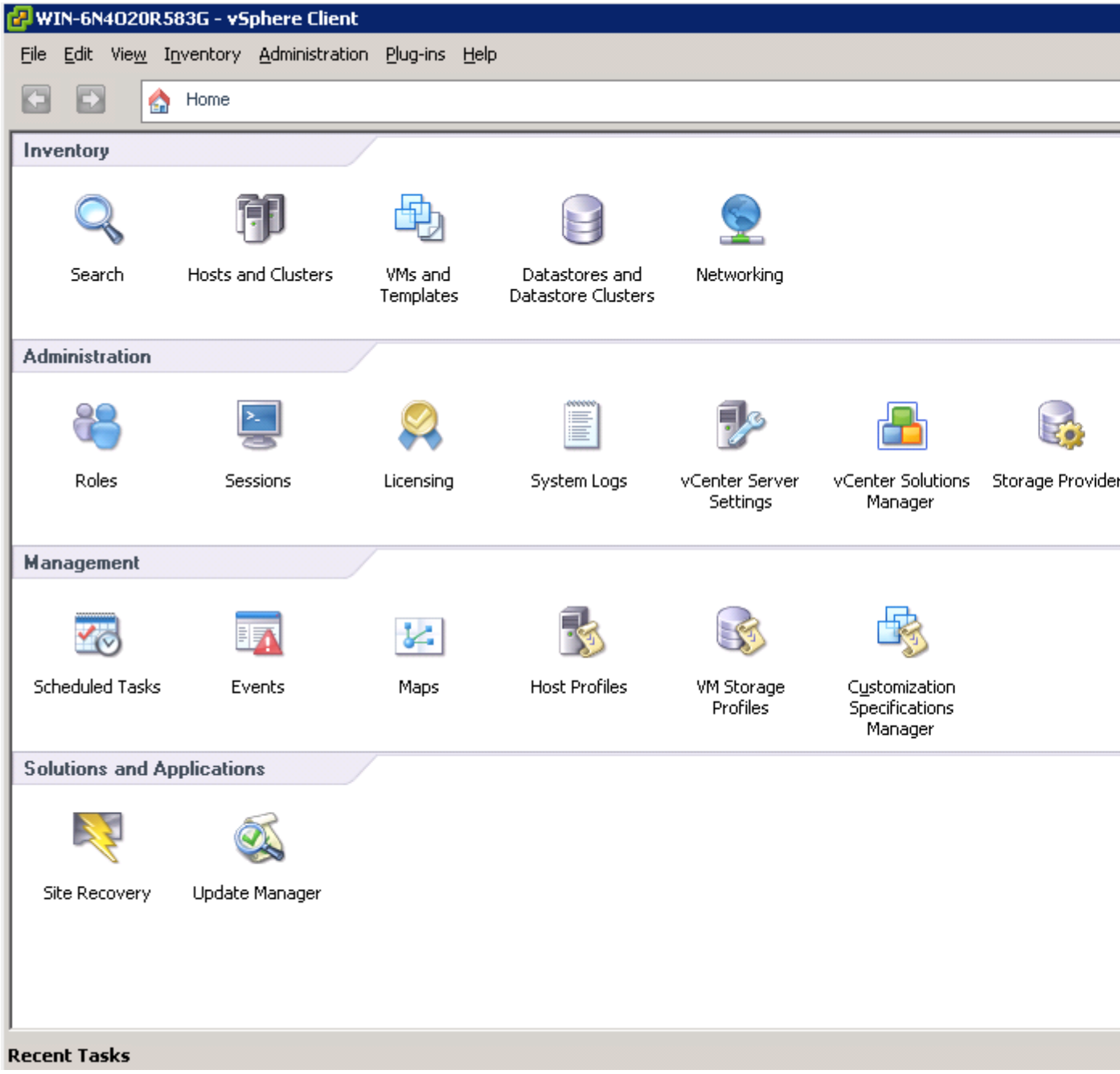
図 *4* : プラグインマネージャ



ステップ 2 Site Recovery Manager を設定および管理するには、ホームページで [サイトのリカバリ（Site Recovery）] をクリックします。

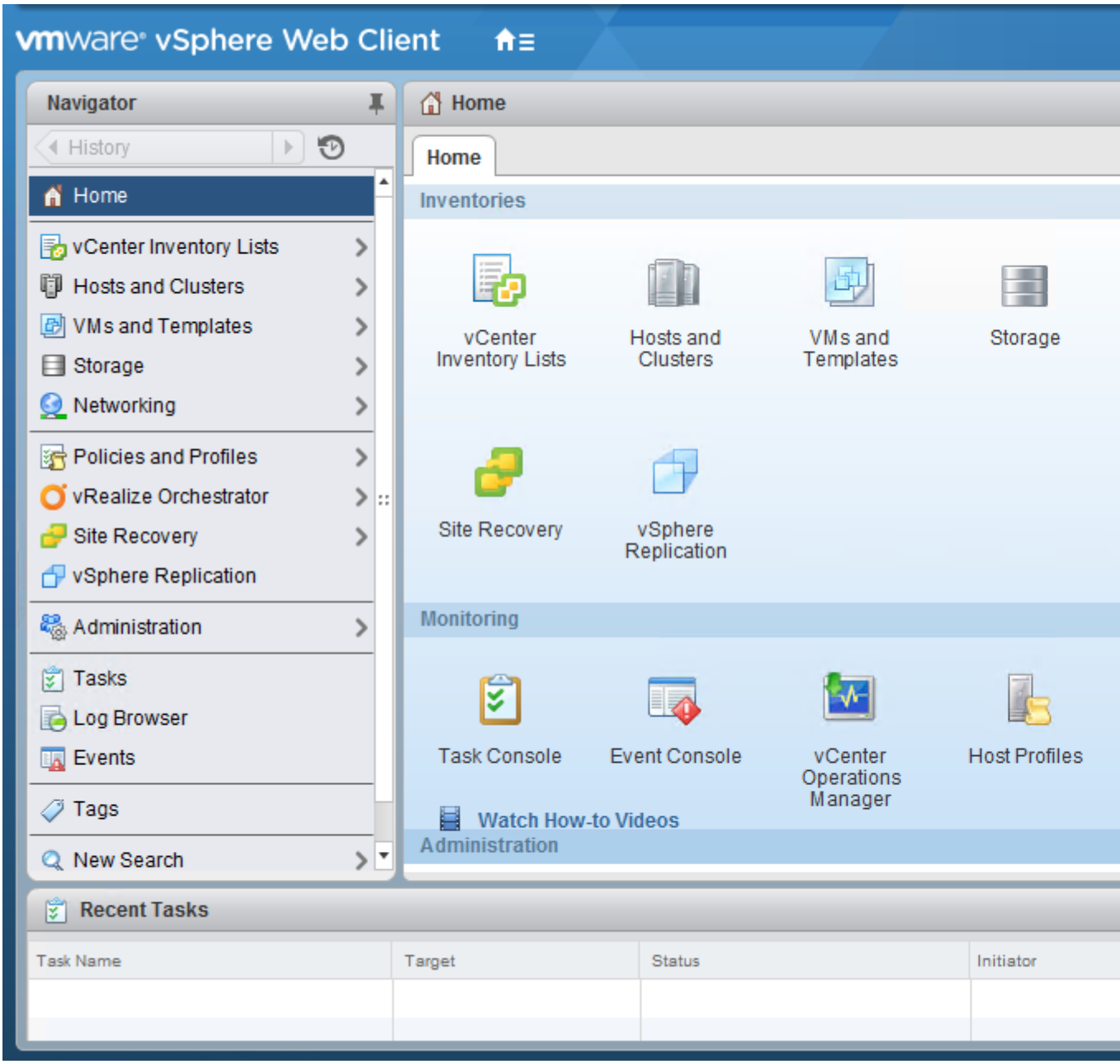
（注） 上記の手順は、Site Recovery Manager バージョン 5.5 にのみ適用されます。Site Recovery Manager バージョン 6.0 では、vSphere Web クライアントをサポートしているため、プラグインをインストールする必要はありません。

図 *5 : Site Recovery Manager 5.5*



次の図は、Site Recovery Manager バージョン 6.0 へのアクセスに使用できる vSphere Web クライアントを示しています。

図 *6 : VMware vSphere Web* クライアント



リカバリサイトの設定

VMware Site Recovery Manager の設定 （8 ページ） と vCenter の設定 （10 ページ） で説明されているタスクをリカバリサイトで実行します。

複製の設定

保護サイトとリカバリサイトで次のタスクを実行します。次の手順は、Site Recovery Manager バージョン 5.5 および 6.0 に適用されます。

- 保護サイトとレプリケーションサイトの設定
- インベントリの設定
- vSphere Replication のインストールと設定
- 保護グループの設定
- リカバリプランの設定

詳細については、*VMware vCenter Site Recovery Manager* バージョン *5.5* および *6.0* ドキュメントセンターにある『VMware User Guide』[英語] を参照してください。

ディザスタリカバリ環境での Security Manager のインストール

保護サイトとリカバリサイトの両方で Site Recovery Manager を設定した後、保護サイトの VM に Security Manager をインストールする必要があります。Security Manager をインストールするには、『*Installation Guide for Cisco Security Manager 4.27*』[英語] を参照してください。

VMware Site Recovery Manager ツールは、リカバリサイトにインストールを複製します。保護サイトとリカバリサイト間の同期は、保護サイトの帯域幅とデータサイズに基づいて実行されます。保護サイトホストで Site Recovery Manager を有効にすると、vSphere Replication は、ソースの VM とそのレプリカのリカバリサイトへの最初の完全同期を実行します。

完全同期が初めて完了すると、Site Recovery Manager で設定された目標復旧時点（RPO）の時間間隔に基づいて vSphere レプリケーションが実行されます。

（注） 環境、つまり帯域幅とデータサイズに基づいて RPO 時間間隔を設定する必要があります。

注意 アプリケーションでの作業を開始する前に、Security Manager サービスがリカバリサイトで起動するまで少なくとも 15 分の猶予時間を確保することをお勧めします。猶予時間が許可されていない場合、Security Manager は正常に起動せず、アプリケーションの再インストールが必要になる可能性があります。

（注） Security Manager が Access Control Server（ACS）と統合されている場合は、認証のために、（Security Manager がインストールされている）保護サイトとリカバリサイトの両方の IP アドレスを AAA クライアントとして ACS サーバーに提供する必要があります。

（注） Cisco Security Manager 4.21 以降では、以前の ACS サーバーの代わりに Cisco Identity Services Engine（ISE）を認証に使用できます。

翻訳について
このドキュメントは、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。