

管理ガイド

Site Recovery Manager 1.0 Update 1



Site Recovery Manager 管理ガイド

アイテム : JA-000096-00

最新情報を反映したテクニカル ドキュメントは、当社の Web サイトにてご覧いただけます。

<http://www.vmware.com/support/>

VMware Web サイトでは、最新の製品アップデート情報も提供しています。

本書に関するご意見は、次のアドレスまでお寄せください。

docfeedback@vmware.com

© 2008 VMware, Inc. All rights reserved. 本ソフトウェアは、米国特許 (No. 6,397,242、6,496,847、6,704,925、6,711,672、6,725,289、6,735,601、6,785,886、6,789,156、6,795,966、6,880,022、6,944,699、6,961,806、6,961,941、7,069,413、7,082,598、7,089,377、7,111,086、7,111,145、7,117,481、7,149,843、7,155,558、7,222,221、7,260,815、7,260,820、7,269,683、7,275,136、7,277,998、7,277,999、7,278,030、7,281,102、7,290,253、7,356,679、7,409,487、7,412,492、7,412,702、7,424,710、7,428,636、7,433,951、7,434,002 および 7,447,854) により保護されています。特許出願中。

VMware、VMware ボックスロゴとデザイン、Virtual SMP および VMotion は、VMware, Inc. の米国およびその他の国における登録商標または商標です。ここに記載されているその他の名称およびマークは各社の商標です。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目次

はじめに	7
Site Recovery Manager の概要	9
VMware Infrastructure の Site Recovery Manager 対応	9
Site Recovery Manager の機能	10
Site Recovery Manager の要件	11
Site Recovery Manager の環境	12
アレイベース レプリケーション	13
Site Recovery Manager のプロセスの概要	14
SRM のインストール	14
保護サイトと復旧サイトのセットアップ	15
仮想マシンの設定	16
システム要件	19
SRM インストールの前提条件	19
SRM のハードウェアとソフトウェアの要件	20
SRM データベース要件	21
Microsoft SQL Server 設定	22
Oracle Server 設定	23
構成の上限	23
SRM ライセンス	23
ライセンス ファイルのインポート	24
Site Recovery Manager の インストールまたは更新	25
Site Recovery Manager のインストール	26
Site Recovery Manager のアップデート	29
Site Recovery Manager プラグインのインストール	29
データベース証明書のアップデート	30
以前のリリースに戻す	30
SRM の管理	33
VI クライアントを使用して SRM を管理する	33
保護サイトと復旧サイトの接続	34

クリデンシヤル ベースの認証	35
サティファイケツト ベースの認証	36
SRM ユーザー、グループ、権限、およびロール	37
SRM 権限	37
SRM デフォルト ロール	38
ロールの追加	39
VirtualCenter アクセス権限の割り当て	40
新規ユーザー グループおよびロールを SRM に追加する	40
アクセス権限の変更	41
アクセス権限の削除	42
SRM ログ ファイルへのアクセス	42
保護サイトの構成	45
保護サイトの構成	45
VMware Infrastructure の構成の要件	46
アレイ マネージャの設定	46
アレイ マネージャの修復	48
インベントリ環境設定の設定	49
保護グループの作成	50
仮想マシン プロパティの設定	51
保護仮想マシンにプロパティを設定する	52
メッセージおよびコマンド ステップの追加	54
バッチ ファイルまたはコマンドの実行	54
IP アドレス マッピング	55
バッチ IP プロパティのカスタマイズ	56
復旧サイトの構成	61
復旧プランの作成	61
復旧プランの管理	63
復旧プランの編集	64
復旧プランのテスト	64
テストの一時停止、再開、またはキャンセル	65
復旧プランの実行	66
復旧プランの削除	66
復旧プランでの仮想マシンの設定	67
復旧プランの表示	68
復旧プラン履歴の表示	69
復旧履歴の結果をエクスポートする	69
カスタマイズ仕様の使用	69

フェイルバック	71
フェイルバック シナリオ	71
その他のフェイルバックの考慮事項	77
アラートと監視	79
SRM アラーム	79
SRM アラーム トリガについて	80
SRM アラーム設定を編集する	80
E メールによるアラーム通知の準備	82
保護サイトと復旧サイトの変更	83
VirtualCenter サーバへの変更	83
保護サイトでの変更	83
復旧サイトへの変更	84
プリインストール チェックリスト	85
フェイルバック チェックリスト	87
srn-config コマンドを使用して SRM サーバ接続を修復する	89
ページング ファイルおよび他の一時データの複製を	91
スワップファイルに複製されなかったデータストアを指定する	91
ページング ファイル ストレージに複製されない仮想ディスクを作成する	92
用語集	95
索引	97

はじめに

本マニュアル『Site Recovery Manager 管理ガイド』では、VMware VirtualCenter サーバの災害復旧用プラグイン、VMware Site Recovery Manager (SRM) のインストールおよび構成について説明します。本書には、サイトの構成と管理、復旧プラン、フェイルオーバーのテストと実行、アラート、システム管理、およびトラブルシューティングについての概念が記されています。

対象読者

本書は、Site Recovery Manager をインストールまたは使用する方を対象としています。本書に記載されている情報は、Windows または Linux のシステム管理者としての経験があり、仮想マシンテクノロジーおよびデータセンター操作に詳しい方を対象としています。本書は、VMware ESX 3.x、VirtualCenter サーバ 2.5、および VI クライアントを含む VMware VI にも精通していることを前提としています。またユーザーは、ストレージ ネットワーク テクノロジー、具体的にはファイバチャネルや iSCSI ストレージエリア ネットワークおよび VI によってこれらのネットワークと通信する方法についても実用的な知識を有している必要があります。

VMware Infrastructure ドキュメント

VI クライアントに詳しくない場合は、VirtualCenter サーバと ESX Server が組み合わされて構成されている VMware Infrastructure ドキュメントを参照してください。ドキュメントは次の URL から入手できます。

<http://www.vmware.com/support/pubs/>

本書へのフィードバック

ドキュメントの向上にご協力ください。本書に関するコメントがございましたら、docfeedback@vmware.com までご連絡ください。

テクニカル サポートおよびエデュケーション リソース

ここでは、お客様にご利用いただけるテクニカル サポート リソースを紹介します。本書の最新のバージョンおよびその他の文書は、<http://www.vmware.com/support/pubs> でご覧いただけます。

オンライン サポートおよび電話サポート

テクニカル サポート リクエストの提出、製品情報や契約情報の表示、および製品の登録には、オンライン サポートをご利用いただけます。詳しくは、<http://www.vmware.com/support> をご覧ください。

該当するサポート契約を結んでいるお客様の場合、迅速な対応が必要な Severity1 の問題に関しては電話でのサポートをご利用ください。詳しくは、http://www.vmware.com/support/phone_support.html をご覧ください。

サポート サービス

ヴェイムウェアのサポート サービスがお客様のビジネス ニーズにどのように対応できるかを確認するには、<http://www.vmware.com/support/services> をご覧ください。

ヴェイムウェア プロフェッショナル サービス

ヴェイムウェア エデュケーション サービス コースでは、広範なハンズオン ラボ、ケース スタディ、業務の際のリファレンスとしてお使いいただける資料を提供しています。このコースは、オンサイト、クラスルームおよびオンラインで有効になります。オンサイトパイロットプログラムおよび実装のベスト プラクティスのために、ヴェイムウェア コンサルティング サービスは、仮想環境をアセス、プラン、ビルドおよび管理するように、オフオファリングを提供しています。エデュケーション クラス、サティフィケートプログラム、およびコンサルティング サービスの詳細は、<http://mylearn1.vmware.com/mgrreg/index.cfm> をご覧ください。

Site Recovery Manager の概要

災害とは、事業を大規模に停止させてしまうすべての出来事を指します。IT リソースに影響を与える災害は、データを復旧し、システムの使用を検証している間はビジネスの停止となることを意味します。

しかし準備さえしておけば、災害の破壊的な影響を軽減することができます。VMware Site Recovery Manager を使用することにより、組織の IT インフラストラクチャを迅速に復旧し、そしてビジネスの停止期間を劇的に短縮することができます。

本章では、SRM の紹介と以下の内容について説明します。

- 「[VMware Infrastructure の Site Recovery Manager 対応](#)」 (P.9)
- 「[Site Recovery Manager の機能](#)」 (P.10)
- 「[Site Recovery Manager の要件](#)」 (P.11)
- 「[Site Recovery Manager の環境](#)」 (P.12)
- 「[Site Recovery Manager のプロセスの概要](#)」 (P.14)

VMware Infrastructure の Site Recovery Manager 対応

VMware Infrastructure の以下の機能は SRM をサポートします。

- カプセル化：仮想マシンは共有ストレージのファイルのグループにカプセル化されます。
- 共有ストレージから起動：共有ストレージのレプリケーションとは、ハードウェアに依存しない仮想マシンを完全にレプリケートし、必要に応じてすぐにパワーオンできる準備が整っていることを意味します。

- **VMware Distributed Resource Scheduler (DRS)** およびリソース プール：
VMware DRS は、使用可能な IT リソースに応じてリソース プール全体にリソースを割り当て、コンピュータの能力のバランスを取ります。障害に先だって復旧仮想マシンの割り当てについて判断する必要がありません。
- ハードウェアからの独立：仮想マシンを使用すると、仮想マシンはドライバを設置する必要がなく、任意のどのハードウェアからでも起動できるため災害による障害はほぼゼロとなります。
- インスタント リパーキング：システムの再インストールという制約がなく、ハードウェアはわずか数分間のうちにまったく異なるオペレーティング システム上で、まったく異なる業務を実行できます。
- **Virtual Local Area Networks (VLAN)**：Virtual LAN を使用すると、仮想マシンのネットワーク トラフィックを隔離できるため、業務を中断することなくテストを実行できます。
- 変更管理と監査能力：VMware Infrastructure の変更管理機能は、災害対策戦略にとって非常に役立ちます。タスクを追跡することにより SRM への変更を確認できます。

Site Recovery Manager の機能

Site Recovery Manager は、災害復旧プランの設定、フェイルオーバー、およびテストを自動化する災害復旧用ワークフロー製品です。

- 応答準備によるエラー削減：SRM では、復旧戦略を前もって、マッピング、テスト、およびリハーサル済みであるため、災害が発生した場合の人的ミスの可能性を減らします。
- 無停止テスト：復旧プランのテストではアレイ スナップショットおよび代替 VLAN と隔離されたネットワーク トラフィックを使用するため、毎日の本番ワークフローを中断することなくテストを実行できます。
- レパレージド ストレージ：SRM では、セットアップ時の構成エラーをなくすためアレイベース レプリケーションと統合化されており、通常これは非常に意味のあることです。
- 復旧した仮想マシンのネットワーク再構成：各仮想マシンは適切な VLAN に接続され、SRM に事前設定されている適切なゲスト IP 設定を使用して再構成されます。これはつまりユーザーが復旧時に各仮想マシンを手動で再構成する必要がないということです。

- 復旧した仮想マシンの CPU およびメモリのクォリティ：各仮想マシンはインストール先サイトの再構成されたリソース プールで復旧されるため、復旧時には適切な CPU およびメモリ リソースが使用されます。このようにして、復旧された仮想マシンは、何百もの各仮想マシンをマッピングしてホストする仮想マシンを事前に指定する必要なく、期待どおりの業務を実行することができます。
- 復旧された仮想マシンの予測可能な管理：仮想マシンはリモートサイトの VirtualCenter の階層にしたがって構成されているため、管理者は各仮想マシンの用途を一目で理解できます。
- インスタントアップデート：復旧プランの変更はテストおよびフェイルオーバーのワークフローに即座に反映されます。
- 監視とアラート：SRM はリモート サイトの無応答や、復旧テストの開始と終了などのイベントを監視します。このことは E メールメッセージによって SRM システム管理者に通知されます。

Site Recovery Manager の要件

SRM を使用するには、以下の条件を満たす必要があります。

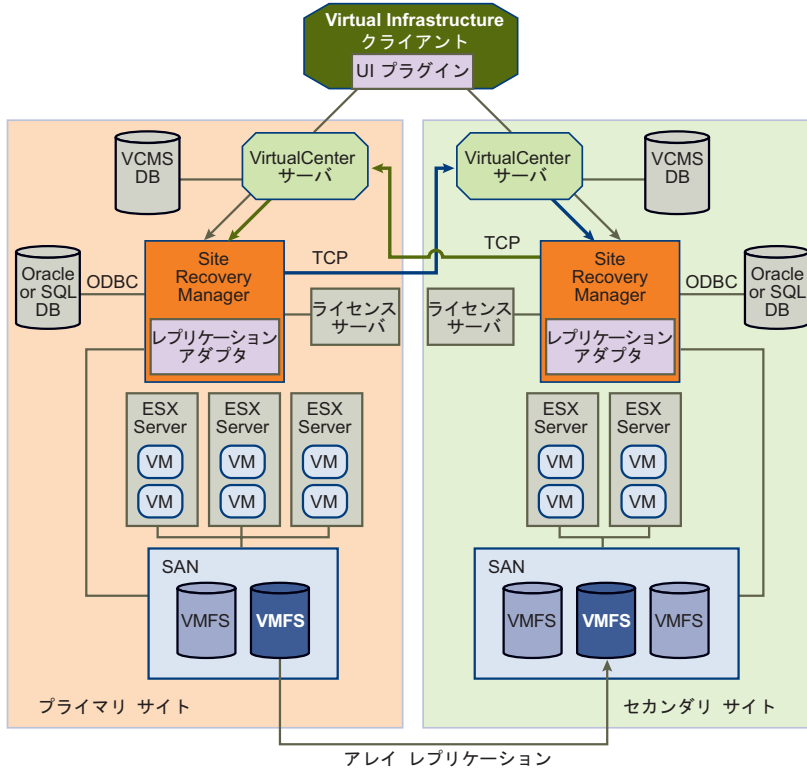
- 保護サイトおよび復旧サイトに VirtualCenter サーバがインストールされている。
- 保護サイトと復旧サイトの間にアレイ ベース レプリケーションが事前設定されている。
- SRM サーバ、VirtualCenter サーバ、および VI クライアントとの間の TCP 接続が可能なネットワーク構成。
- 保護サイトおよび復旧サイトに Oracle データベースまたは SQL Server データベースが備わっており、SRM 専用データ ストアとの接続で ODBC を使用。
- 保護サイトおよび復旧サイトの VirtualCenter ライセンス サーバに SRM ライセンスがインストールされている。

構成の最小要件の詳細については、「SRM インストールの前提条件」(P.19) を参照してください。

Site Recovery Manager の環境

図 1-1 の図は、SRM の主要なコンポーネントを示しています。

図 1-1. SRM 環境の前提条件



これらのコンポーネントの説明は次のとおりです。

- **VirtualCenter Server** : 仮想化された IT 環境を設定、プロビジョニング、および管理するための中心となるポイント。
- **Site Recovery Manager サーバ** : SRM および 1 つまたは複数のマネージャがインストールされている物理ホストまたは仮想ホスト。
- **ライセンス サーバ** : ライセンスを保存および割り当てるサーバ。
- **Oracle または SQL データベース** : SRM オブジェクトの永続的なストレージ。
- **ESX サーバ** : プロセッサ、メモリ、ストレージ、およびネットワーク リソースを複数の仮想マシン内で抽象化する、物理サーバで実行される仮想化レイヤー。

- **SAN** : アレイベース レプリケーションをサポートするストレージエリア ネットワーク (ファイバチャネルまたは iSCSI アレイ)。
- **Virtual Machine File System (VMFS)** : 仮想マシンの格納用に最適化されたクラスタファイルシステム。

アレイベース レプリケーション

SRM では、保護サイトの 1 つまたは複数のストレージアレイがデータを復旧サイトのピアアレイに複製するアレイベース レプリケーションをサポートしています。ストレージレプリケーションアダプタ (SRA) は、アレイベンダーが提供して SRM によるアレイベース レプリケーションの使用をサポートするアレイ固有のプログラムです。SRA は SRM リリースの一部ではありません。アレイベンダーは SRA を提供してサポートします。また、VMware Web サイトからダウンロードすることもできます。SRM サーバホスト上の SRM で使用するアレイ固有の SRA をインストールする必要があります。

LUN レプリケーションとデータストア

各ストレージアレイは LUN のセットをサポートします (1 つまたは複数の物理デバイスを充たす論理ストレージ単位)。指定された LUN は複製されているか、または複製されていない場合があります。VMFS (Virtual Machine File System) データストアは複数の LUN にまたがるため、SRM はデータストア内のすべての LUN が複製されていることを確認する必要があります。

仮想マシン保護を設定する前に、SRM は含まれているデータストアグループおよび仮想マシンのリストを表示します。データストアグループのリストが予想したものと異なる場合は、続行する前に修正してください。Storage VMotion (ESX 3.5 以上) を使用して個々の仮想マシンを移動できます。間違った LUN がレプリケートされている場合は、レプリケーションを再構成します。

注 この確認ステップは、災害復旧プランにおいてもっとも大きなエラーのソースの 1 つを排除するための重要なチェックポイントです。

保護グループ

保護グループとは、一緒にフェイルオーバーする仮想マシンのグループのことです。各レプリケートされたデータストアに対して 1 つの保護グループを作成する必要があります。保護サイトで保護グループが作成された後、SRM のセットアップを完了するには保護グループおよびその仮想マシンを復旧サイトの復旧プランに追加する必要があります。

新しい仮想マシンがレプリケートされたデータストアに作成された場合、トリガされた場合に通知するイベントが作成されます (およびそれらのイベントにアラームを関連付けることができます)。この場合、保護グループに移動して、まだ構成されていない仮想マシンを見つけ、各仮想マシンごとに設定を変更します。

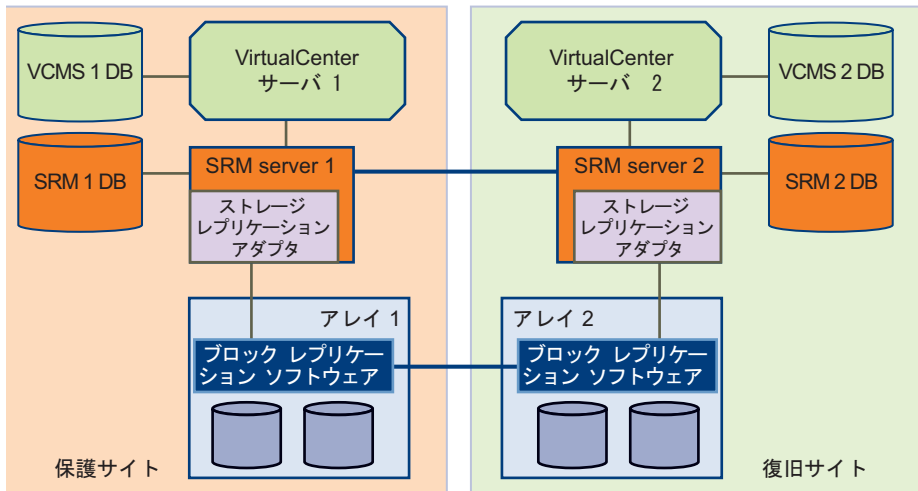
Site Recovery Manager のプロセスの概要

SRM を使用して、常に本番サイトをレプリケートする復旧サイトをセットアップできます。災害復旧プランを作成し、テストされたプロセスの結果が復旧の目標を満たすものとします。災害が発生した場合、フェイルオーバー プロセスによって優先度による順番にしたがってリソースをサービスに戻すことができます。

SRM のインストール

SRM には各サイトでインストールする必要があるサーバ コンポーネントおよびサーバからダウンロードして VI クライアントにインストールするクライアント プラグインが含まれています。これは、SRM サービスを管理するために使用します。図 1-2 の図に、SRM のインストールを示します。

図 1-2. SRM インストール アーキテクチャ



各サイトには VirtualCenter サーバホストがあります。これは、VirtualCenter サービスを実行する Windows マシンです。SRM サーバは可能であれば専用のサーバ ホストにインストールされている必要がありますが、必要に応じて VirtualCenter サーバホストにインストールすることもできます。ストレージ レプリケーション アダプタは SRM サーバ ホストにインストールされています。各サイトの SRM データベースは仮想マシン構成、保護グループ、および復旧プランについての情報を保持しています。SRM のデータベース スキーマの要件が異なるため、SRM は Virtual Center データベースを使用することができません。VirtualCenter データベース サーバを使用して SRM データベースを作成してサポートすることができます。

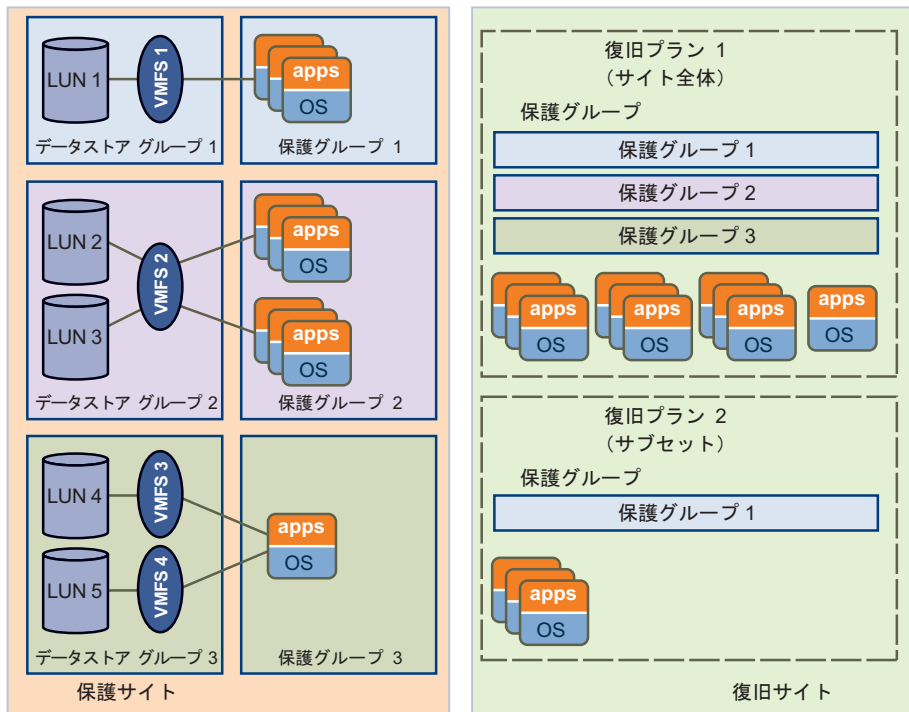
SRM のインストールには以下のタスクが含まれます。

- 1 両方のサイトに SRM データベースを設定します。
- 2 両方のサイトに SRM サーバをインストールして各サーバを対応するデータベースに接続します。
- 3 各サイトで SRM サーバ上のアレイにストレージレプリケーションアダプタをインストールします。
- 4 各サイトで 1 つまたは複数の VirtualCenter クライアントに SRM クライアントプラグインをインストールします。
- 5 SRM クライアントを使用して保護サイトと復旧サイトに接続します。
- 6 SRM クライアントを使用して各サイトにアレイ マネージャを設定します。

保護サイトと復旧サイトのセットアップ

インストール後に、保護サイトと復旧サイトをセットアップします。

図 1-3. 保護サイトの復旧サイトに対するリソースの計算の関係



保護サイトでは、仮想マシンは保護グループに割り当てられます。保護グループは、同じデータストアグループ（レプリケートされた同じ LUN のセット）を使用して一緒にフェイルオーバーする仮想マシンの集まりです。

保護グループを使用して仮想マシンがフェイルオーバー後に復元される順番を制御します。たとえば、重要なビジネス アプリケーションを保護グループ 1 に割り当てて、優先度の低いアプリケーションを保護グループ 2 に、そしてオプションのアプリケーションを保護グループ 3 に割り当てることができます。復旧プランでは、保護グループ 1 が最初にフェイルオーバーされて、次にグループ 2、そしてグループ 3 と続きます。

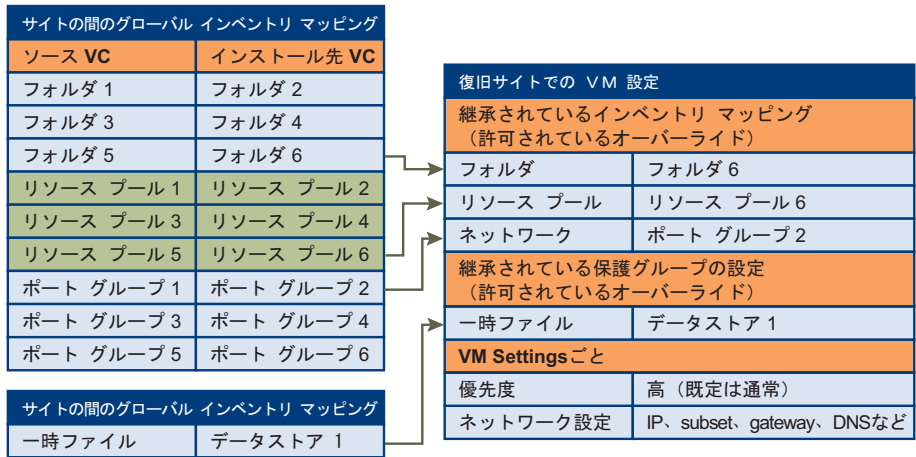
復旧サイトで、1 つまたは複数の復旧プランを作成します。復旧プランはフェイルオーバー中に発生した内容を制御する手順の順序付けられたセットです。複数の復旧プランを開発して複数の災害シナリオに対応することができます。保護サイトと復旧サイトのセットアップには、以下のタスクが含まれています。

- 1 使用可能なデータストア グループについて理解する。SRM ではストレージ レプリケーション アダプタからの情報を使用してデータストア グループを決定します。
- 2 保護仮想マシンにインベントリ マップを作成します。
- 3 各データベース グループに保護グループを作成します。
- 4 保護グループの設定を設定する。保護グループ内のすべての仮想マシンに対してデフォルトの構成を提供します。
- 5 復旧プラン (必要な場合はプロンプト、スクリプト、および通知を含む) を作成します。

仮想マシンの設定

SRM では、保護サイトのフォルダ、リソース プール、およびネットワークなどの仮想マシンのリソースが復旧サイトの同じリソースにマッピングされる方法を制御するインベントリの環境設定を指定することができます。このインベントリ マッピングによって、保護仮想マシンが適切にパワーオンされるように設定されていて、復旧サイトのネットワークに接続されていることを確認することができます。

図 1-4. 保護サイトから復旧サイトへの仮想マシンのマッピング



グローバルな環境設定が保護グループのすべての仮想マシンに適用されています。また、個々の仮想マシンにネットワーク構成情報などのカスタム設定も適用することができます。

仮想マシンの設定には以下のタスクが含まれています。

- 1 インベントリ マッピングの設定
- 2 保護グループの設定
- 3 仮想マシン設定の設定

システム要件

この章では、VMware Site Recovery Manager (SRM) のハードウェア要件、オペレーティングシステム要件、およびライセンス要件について説明します。この章では、この情報を使用してユーザの環境が確実にインストールの要件を満たすようにします。

SRM の互換性の要件の完全なリストについては、「Site Recovery Manager 互換性マトリックス」を参照してください。

本章の内容は、次のとおりです。

- 「SRM インストールの前提条件」 (P.19)
- 「SRM のハードウェアとソフトウェアの要件」 (P.20)
- 「SRM データベース要件」 (P.21)
- 「構成の上限」 (P.23)
- 「SRM ライセンス」 (P.23)

SRM インストールの前提条件

VMware Infrastructure は以下の要件を満たす必要があります。

- VirtualCenter サーバ2.5 Update 1 以上およびVI クライアント 2.5 がインストールされていて、保護サイトと復旧サイトで実行している。VirtualCenter サーバホストには静的 IP アドレスが必要（可能な場合）。
- レプリケートされたアレイにホストされたデータストアである、VirtualCenter サーバが管理する ESX ホストに常駐する仮想マシン。
- レプリケートされたデータストアは、複数のデータセンターからアクセスすることはできません。

ストレージアレイは以下の要件を満たす必要があります。

- 保護サイトおよび復旧サイトにアレイベース レプリケーションおよびストレージレプリケーションアダプタがインストールされ、設定されていること。
- また、アレイの管理にはベンダーで提供されているその他のコンポーネントをインストールする必要があります。これらのコンポーネントのいくつかは、SRM サーバと同じホストにインストールする必要がありますが、その他のコンポーネントは SRM サーバによるネットワーク アクセスのみを必要とします。

SRM は時々ストレージアレイを再スキャンする必要がある場合があります。ESX ホストで `Scsi.RescanAllHbas` のデフォルトの値を変更することによって、アレイの再スキャン時間を改善することができます。ESX ホストの再スキャン時間が 10 分以上かかる場合は、このオプションの値を **1** に設定します。

- リモートの ESX がフェイルオーバーした場合に備えて、レプリケートされた LUN に対してマスキングおよびゾーニングが設定されていること。VMware では、ストレージを設定してレプリケートされた LUN のクローンまたはスナップショットを作成することをお勧めします。スナップショットまたはクローンは、復旧 ESX ホストにマスキングする必要があります。
- SRM サーバと VirtualCenter サーバが同じホストにインストールされている場合を除いて、以下のポートを Windows ファイアウォールの例外リスト追加して SRM と VirtualCenter 間の通信を有効にする必要があります。
 - SRM 通信 SOAP ポート (デフォルトは 8095)
 - SRM クライアントダウンロード HTTP ポート (デフォルトは 8096)
 - SRM 外部 API SOAP ポート (デフォルトは 9007)

SRM のハードウェアとソフトウェアの要件

SRM ハードウェアは、以下の要件を満たす必要があります。

- プロセッサ：2.0GHz 以上の Intel または AMD x86 プロセッサ。
- メモリ：最低 2GB。
- ディスク ストレージ：最低 2GB。
- ネットワーク：ギガビットを推奨。

VMware SRM は次の Microsoft Windows オペレーティング システムで実行されます。

- Windows XP Professional with SP2
- Windows 2003 Server R2
- Windows 2003 Server SP1 (64 ビット以外のすべてのリリース)

- Windows 2000 Server SP4 with Update Rollup 1

VI クライアントには SRM プラグインがインストールされています。SRM プラグインは、Microsoft Windows オペレーティングシステム上で実行するよう設計されており、これらのオペレーティングシステムの 32 ビットバージョン用に設計されています。

- Windows 2000 Professional with SP4 Update Rollup 1 (MSI インストーラ バージョン 3.1.4000.2435 以降)

- Windows XP Professional 32-bit with SP2 (MSI インストーラ バージョン 3.1.4000.2435 以降)

- Windows 2003 with SP1 (64 ビット以外のすべてのリリース)

- Windows 2003 Server R2

- Windows Vista Business

- Windows Vista Enterprise

VI クライアントは Microsoft .NET 2.0 Framework が必要です。システムにこれがインストールされていない場合、VI クライアントのインストーラによってインストールされます。

注 SRM サーバホストには静的 IP アドレスが必要 (可能な場合)。

SRM データベース要件

各サイトの SRM データベースは仮想マシン構成、保護グループ、および復旧プランについての情報を保持しています。SRM のデータベーススキーマの要件が異なるため、SRM は VirtualCenter データベースを使用することができません。VirtualCenter データベースサーバを使用して SRM データベースを作成してサポートすることができます。

各サイトには SRM データベースの固有のインスタンスが必要です。SRM をインストールする前にデータベースが存在する必要があります。SRM のインストールが完了した後でデータベースを再初期化することはできません。再初期化すると、SRM が失敗する原因となります。SRM データベースを再初期化する必要がある場合は、再初期化が完了してから、新しいデータベース接続を指定して SRM を再インストールします。

各データベースには基本インストールの後で追加の設定が必要です。「[Microsoft SQL Server 設定](#)」(P.22) および「[Oracle Server 設定](#)」(P.23) を参照してください。

表 2-1 に SRM がサポートするデータベースをリストします。

表 2-1. SRM によってサポートされているデータベース

データベース タイプ	サービス パック、パッチ、およびドライバの要件
Microsoft SQL Server 2005 Enterprise (64 ビットバージョンの SP2 もサポートされています)	SP1 または SP2 Windows 2000 および Windows XP の場合、クライアントに MDAC 2.8 SP1 を適用。 クライアントに SQL ネイティブクライアントのドライバを使用。
Microsoft SQL Server 2005 Standard	クライアントに SQL ネイティブクライアントのドライバを使用。
Microsoft SQL Server 2005 Express	クライアントに SQL ネイティブクライアントのドライバを使用。
Microsoft SQL Server 2000 Enterprise	SP4
Microsoft SQL Server 2000 Standard	SP4
Oracle 9i release 2 Standard Oracle 9i release 2 Enterprise	サーバおよびクライアントにパッチ 9.2.0.8.0 を適用。 ドライババージョン 10.02.x.x
Oracle 10g Enterprise Release 1	ドライババージョン 10.02.x.x
Oracle 10g Enterprise Release 2 (64 ビットバージョンもサポートされています)	最初にクライアントおよびサーバにパッチ 10.2.0.3.0 を適用。 その後クライアントにパッチ 5699495 を適用。 ドライババージョン 10.02.x.x

Microsoft SQL Server 設定

Microsoft SQL Server では、SRM と使用する場合に次の設定要件が必要です。

- スキーマ名はユーザー名と同じである必要があります。ユーザー アカウントと関連付けられているデフォルトのスキーマが必要です。
- バルク挿入の管理者権限が必要です。
- Windows 認証を使用している場合は、SRM サーバとデータベース サーバが同じホストで実行している必要があります。
- SQL Server がローカルにインストールされている場合、データベース サーバで [共有メモリ (Shared Memory)] の設定を無効にする必要があります。
- SRM データベースのユーザーには、接続、表の作成、ビューの作成の権限が付与されている必要があります。

Oracle Server 設定

Oracle Server では、SRM と使用する場合に以下の設定要件が必要です。

- Oracle 9i サーバを使用している場合、SRM の「バルク挿入 (Bulk Insert)」機能を無効にする必要があります。vmware-dr.xml 設定ファイルを編集し、EnableBulkInsert の設定を「false」に変更します。このファイルのデフォルトの場所は、C:\Program Files\VMware\VMware Site Recovery Manager\config\ です。設定ファイルを変更したら、このデータベースを使用している各 SRM サーバに [VMware Site Recovery Manager Service] サービスを再開始します。
- サポートされているすべてのデータベース バージョンにドライバ バージョン 10.02.x.x を使用します。
- SRM データベースのユーザーには、接続、リソース、表の作成、ビューの作成の権限が付与されている必要があります。

構成の上限

仮想および物理機器を選択し、構成する場合、SRM に設定されている制限を超えることはできません。表 2-2 に、単一の SRM サーバによってサポートされている保護仮想マシン、保護グループ、およびレプリケートされた LUN の制限を表示します。SRM では、新しい保護グループを作成する場合、保護仮想マシンおよび保護グループの制限を超えないように保護します。SRM の以前のバージョンで作成された設定がこれらの制限を超える場合は、SRM は警告を表示しますが、設定の実行を許可します。それらの設定は、できる限り早急にサポートされている制限内に再設定してください。

表 2-2. SRM 構成の上限

アイテム	最大
保護される仮想マシン	500
保護グループ	150
レプリケートされる LUN	150
復旧プランの実行	3

レプリケートされた LUN の制限および復旧プランの実行は助言であり、強制するものではありません。

SRM ライセンス

SRM には 2 つのタイプのライセンス キーがあります。

- サイトで保護仮想マシンを実行できる ESX CPU の数を指定する保護が有効なライセンス キー (SRM_PROTECTED_HOST)。このキーを保護サイトにインストールしてフェイルオーバーを有効にします。復旧サイトと保護サイトにインストールして双方向操作 (フェイルバック) を有効にします。

- 保護サイトと復旧サイトにインストールする必要があるサイト有効ライセンスキー (PROD_SRM)。これらのキーは保護イネーブルキーを購入したときに提供されます。

ライセンスキーを取得するには、VMware Web サイトの [Site Recovery Manager 製品情報 (Site Recovery Manager Product Information)] ページに移動します。

SRM ライセンスは、ホストライセンスが最初にインストールされて、SRM ホストプログラムが再開される度に有効なライセンスをチェックします。ライセンスサーバから取得したライセンスは5分ごとにチェックされます。ライセンスが順守されていない場合は、VirtualCenter はライセンスアラームをトリガします。VMware では、ライセンスの管理者に電子メールで通知できるように、トリガされたライセンスイベントのアラートを設定することをお勧めします。詳細については、「アラートと監視」(P.79) を参照してください。

ライセンス ファイルのインポート

VMware ライセンスサーバがインストールされると、ライセンスサーバに SRM ライセンス ファイルをインポートできます。保護サイトおよびリカバリサイトでサイトごとのライセンスをインストールする必要があります。保護イネーブルライセンスをインストールしてフェイルオーバーを有効にし、復旧サイトと保護サイトで双方向操作 (フェイルバック) を有効にする必要があります。

VMware ライセンスサーバに関する詳細については、『ESX Server 3 インストールガイド』を参照してください。

SRM ライセンスを有効にするには

- 1 ライセンスサーバアプリケーションを実行しているコンピュータにログインします。
保護サイトおよび復旧サイトはそれぞれ固有のライセンスサーバを持っている必要があります。
- 2 PROD_SRM キーが含まれている SRM ライセンス ファイルを
C:\Program Files\VMware\VMware License Server\Licenses\ にコピーします。
ライセンス ファイルには .lic 拡張子が必要です。
- 3 これが保護仮想マシンを有効にして実行するサイトである場合は、SRM_PROTECTED_HOST キーが含まれている SRM ライセンス ファイルを
C:\Program Files\VMware\VMware License Server\Licenses\ にコピーします。
- 4 [スタート]>[プログラム]>[VMware]>[VMware ライセンスサーバ]>[VMware ライセンスサーバツール] を選択して VMware ライセンスサーバツールを起動します。
- 5 [開始、停止または再読み取り] タブをクリックします。
- 6 [ライセンスファイルの再読み取り (ReRead License File)] をクリックして新しいライセンスファイルをロードします。
- 7 SRM サーバを再起動します。

Site Recovery Manager の インストールまたは更新

3

SRM サーバを保護サイトおよび復旧サイトでインストールする必要があります。SRM サーバをインストールしたら、クライアント プラグインをいずれかのサーバから VI クライアントにダウンロードし、そのクライアントを使用していずれかのサイトで SRM を設定して管理します。

SRM では各サイトで **VirtualCenter** サーバのサポートが必要です。インストール中、SRM インストーラはこのサーバに接続できるようにする必要があります。専用のサーバホストに **SRM** をインストールできない場合は、それを **VirtualCenter** サーバがインストールされていた同じホストにインストールできます。

SRM のインストールには以下のタスクが含まれます。

- 1 保護サイトで SRM をインストールします。
- 2 復旧サイトで SRM をインストールします。
- 3 VI クライアントを使用して保護サイトまたは復旧サイトに **VirtualCenter** サーバを接続し、**SRM** プラグインをダウンロードします。

SRM のアップデートには以下のタスクが含まれます。

- 1 保護サイトと復旧サイトで SRM データベースをバックアップします。
- 2 保護サイトで SRM を更新します。
- 3 復旧サイトで SRM を更新します。
- 4 SRM プラグインがインストールされていない VI クライアントを使用して、保護サイトまたは復旧サイトで **VirtualCenter** サーバに接続して新しい SRM プラグインをダウンロードします。

本章の内容は、次のとおりです。

- 「[Site Recovery Manager のインストール](#)」 (P.26)

- 「[Site Recovery Manager のアップデート](#)」 (P.29)
- 「[Site Recovery Manager のアップデート](#)」 (P.29)

Site Recovery Manager のインストール

SRM をインストールする前に、[第 2 章「システム要件」](#) (P.19) にリストされているすべての要件を完了していることを確認してください。特に、各サイトには以下の情報が必要です。

- 実行している **VirtualCenter** サーバのホスト名または IP アドレス：SRM と VirtualCenter は同じホストまたは別々のホストに置くことができます。SRM のインストール中に、VirtualCenter ホスト名または IP アドレスを指定する必要があります。
- **VirtualCenter** 管理者のユーザー名とパスワード：SRM のインストール中は、VirtualCenter 管理者に有効なユーザー名とパスワードを指定する必要があります。
- **SRM** データベースのユーザー名とパスワード：詳細については、「[SRM データベース要件](#)」 (P.21) を参照してください。

注 インストール中に、SRM は、SRM サーバおよび VirtualCenter サーバ ホストのホスト名を保存します。これらのホスト名のいずれかを変更する必要がある場合は、SRM を再インストールする必要があります。

SRM をインストールするには

- 1 SRM をインストールするサーバ ホストにログインします。
SRM をインストールするには、ホストの [管理者] グループのメンバーとしてログインする必要があります。
- 2 SRM インストール ファイルをホスト上のフォルダにダウンロードする、またはこのファイルが含まれているネットワーク上のフォルダを開きます。
- 3 SRM インストーラ アイコンをダブルクリックしてインストールを開始します。
インストーラはインストールされたホスト上の VMware ソフトウェアのセットを確認します。SRM の既存のインストールが検出された場合は、既存のインストールを更新するかどうかを確認するプロンプトが表示されます。SRM のアップデートの詳細については、「[SRM を更新するには](#)」 (P.29) を参照してください。
- 4 [インストール ウィザードへようこそ (**Welcome to the installation wizard**)] 画面で [次へ (**Next**)] をクリックします。
- 5 [使用許諾契約書 (**License Agreement**)] 画面で、[使用許諾契約書に同意する (**I accept the terms in the license agreement**)] を選択し、[次へ (**Next**)] をクリックします。
- 6 [インストール先フォルダ (**Destination Folder**)] 画面で、SRM をインストールするフォルダを選択して [次へ (**Next**)] をクリックします。

インストール フォルダのパス名は 240 文字よりも長くすることはできません。また、ASCII 以外の文字を含めることはできません。

- 7 SRM をインストールするサイトで **VirtualCenter** サーバに関する以下の情報を入力します。

- **VirtualCenter** アドレス: **VirtualCenter** サーバのホスト名または IP アドレスを入力します。

VirtualCenter サーバと **SRM** サーバは同じドメインである必要があります。ホスト名を小文字で入力します。インストールが完了して保護サイトと復旧サイト間の接続を設定したら、ここで入力したホスト名または IP アドレスとまったく同じホスト名または IP アドレスを入力する必要があります。

- **VirtualCenter** ポート: デフォルトを受け入れるか、別のポートを入力します。
- **VirtualCenter** ユーザー名: 指定された **VirtualCenter** サーバで管理者権限のあるユーザー ID を入力します。
- **VirtualCenter** パスワード: 指定されたユーザー ID のパスワードを入力します。

[次へ (Next)] をクリックします。インストーラは指定された **Virtual Center** サーバに接続して入力された情報を検証します。

- 8 サーバ接続の認証に使用される証明書のソースを選択します。

- **SRM** が証明書の作成とインストールを行うようにするには、[証明書を自動的に生成 (Automatically generate certificate)] を選択して [次へ (Next)] をクリックします。

組織および組織単位のテキスト値を入力します。一般的には、会社名と会社内のグループの名前です。結合した値の最大長は 80 文字を超えることはできません。

- 既存の **PKCS #12** 証明書ファイルを使用するには、[**PKCS #12** 証明書ファイルを使用 (Use a PKCS #12 certificate file)] を選択して [次へ (Next)] をクリックします。

証明書ファイルにパスを入力します。証明書ファイルには証明書に一致する 1 つの秘密キーが含まれている必要があります。

必要に応じて証明書のパスワードを入力します。

- 9 以下の追加の情報を入力します。

- ローカル サイト名: この **SRM** インストールの一意の名前。1 つのサイトでの **SRM** のインストールごとに一意の識別子を指定する必要があります。
- 管理者 E メール: **SRM** を監視し、アラートまたは通知に対して応答する担当者またはグループの E メールアドレス。

- 追加の E メール（オプション）：同様にアラートまたは通知を受け取る担当者またはグループの E メールアドレス。
- ローカルホスト：ローカルホストの名前または IP アドレス。この値は SRM インストーラによって取得され、間違っている場合にのみ変更する必要があります（たとえば、ローカルホストが複数のネットワーク インターフェイスを持っていて、SRM インストーラによって検出されたものが使用したいものでない場合など）。
- リスナ ポート：ネットワーク トラフィック用の SOAP ポート番号または HTTP ポート番号。SOAP は SRM からのリクエストを受け取るのに使用され、HTTP は SRM プラグインをダウンロードするのに使用されます。デフォルトの値が入力されます。
- API リスナポート：SRM API からのネットワーク トラフィック用の SOAP ポート番号または HTTP ポート番号。デフォルトの値が自動的に入力されます。詳細については、[Site Recovery Manager API ドキュメント](#)を参照してください。

デフォルトのポートの値は、SRM がインストールされているシステムで他のアプリケーションによって使用中でない限り、修正なしで機能します。他のサービスがすでにポートを使用している場合、またはネットワーク管理者が固有のポートを SRM で使用するよう割り当てたい場合は、これらの値を変更することができます。

- 10 以下のデータベース構成情報を入力して [次へ (Next)] をクリックします。
 - データベース クライアント：フィールドの右側にある矢印をクリックして、サイト用のデータベース クライアントを選択します。
 - データ ソース名：SRM のこのインストールで使用する DSN。[ODBC DSN セットアップ (ODBC DSN Setup)] をクリックして既存の DSN を表示するかまたは新しく作成します。
 - ユーザー名：指定されたデータベースの有効なユーザー ID。
 - パスワード：指定されたユーザー ID のパスワード。
 - 接続数：初期接続プール サイズ。このプールの接続数は SRM インストーラによって作成されます。これらの接続がすべて使用中で新しい接続が必要な場合は、作成されても最大接続数によって指定されている接続数を超えることはありません。SRM にとってはプールからの接続を使用する方が新しい接続を作成するよりも速くなります。
 - 最大接続数：データベースに対して同時に開く最大接続数。データベース管理者がデータベースに対して開くことができる接続数を制限している場合は、ここに入力した値はその数を超えてはなりません。
- 11 [インストール (Install)] をクリックします。
- 12 ウィザードが完了したら、[終了 (Finish)] をクリックします。

Site Recovery Manager のアップデート

Site Recovery Manager を更新する場合、Virtual Center サーバ接続、証明書、およびデータベース構成に関する情報は、既存のインストールから読み込まれて新しいインストールで再利用されます。

注 更新を開始する前に、現在の SRM データベースをバックアップします。更新ウィザードは、データベースがバックアップされたことを確認するように要求し、確認されるまで一時停止します。

SRM を更新するには

- 1 SRM サーバ ホストにログインします。

SRM をインストールするには、ホストの管理者グループのメンバーとしてログインする必要があります。

- 2 SRM インストール ファイルをホスト上のフォルダにダウンロードするか、またはこのファイルが含まれているネットワーク上のフォルダを開きます。
- 3 SRM インストール ファイルをダブルクリックして更新を開始します。

インストーラはインストールされたホスト上の VMware ソフトウェアのセットを確認します。SRM の既存のインストールが検出された場合は、既存のインストールを更新するかどうかを確認するプロンプトが表示されます。

[はい (Yes)] をクリックして更新を続行します。

- 4 [更新ウィザードへようこそ (Welcome to the update wizard)] 画面で [次へ (Next)] をクリックします。ウィザードには、SRM データベースをバックアップしたことを確認するプロンプトが表示されます。
 - インストールを一時停止してデータベースをバックアップする場合は、[いいえ (No)] をクリックします。
 - データベースがバックアップされていてインストールを続行する場合は、[はい (Yes)] をクリックします。インストーラは既存のインストールから構成データを読み込んでそれを使用して更新を完了します。
- 5 ウィザードが完了したら、[終了 (Finish)] をクリックします。

Windows をシャットダウンして再起動するようにプロンプトが表示される場合があります。

Site Recovery Manager プラグインのインストール

SRM をインストールまたは更新したら、保護サイトまたは復旧サイトで VI クライアントを使用して VirtualCenter サーバに接続し、サーバからプラグインをダウンロードしてそれを VI クライアントで有効にします。

SRM プラグインをダウンロードしてインストールするには

- 1 VI クライアントを開始して保護サイトまたは復旧サイトで VirtualCenter サーバに接続します。
- 2 VI クライアントメニュー バーで、[プラグイン (Plugins)] > [プラグインの管理 (Manage Plugins)] を選択します。
- 3 [使用可能 (Available)] タブで、[VMware VirtualCenter Site Recovery プラグイン (VMware VirtualCenter Site Recovery plug-in)] を指定し、[ダウンロードとインストール (Download and install)] をクリックします。
- 4 ダウンロードが完了したら、プラグイン インストール ウィザードが表示されます。[次へ (Next)] をクリックしてウィザードを開始します。
- 5 [使用許諾契約書に同意します (I accept the terms in the license agreement)] をクリックして、[次へ (Next)] をクリックします。
- 6 [インストール (Install)] をクリックします。
- 7 [終了 (Finish)] をクリックします。
Windows をシャットダウンして再起動するようにプロンプトが表示される場合があります。
- 8 [インストール済み (Installed)] タブをクリックします。
- 9 Site Recovery プラグインの [有効 (Enabled)] チェックボックスをオンにします。
[Site Recovery] アイコンがツールバーに表示されます。

データベース証明書のアップデート

インストール中に、SRM は指定されたデータベース証明書を暗号化して保存します。これらの証明書が変更された場合 (たとえば、データベースのユーザー名またはパスワードが変更された場合など) は、インストール ディレクトリにある `installcreds.exe` ユーティリティを実行することによって、保存されている証明書を変更する必要があります。

以前のリリースに戻す

以前のリリースに戻す場合は、SRM とそのデータベースの両方をアンインストールする必要があります。

以前のリリースに戻すには

- 1 保護サイトおよび復旧サイトで SRM をアンインストールします。
サイトがペアリングされている場合は、両方のサイトで SRM をアンインストールする必要があります。SRM をホストのペアの 1 つのメンバーからアンインストールした場合、残りのメンバーのデータベースは不整合なものになります。
- 2 影響を受けた VirtualCenter クライアントから SRM プラグインをアンインストールする。

- 3 データベース ベンダが提供する手順に従って以前のリリースで使用されていたデータベースを復元します。

SRM の管理

本章では、VMware Infrastructure Client について説明し、サイト ペアの設定、ユーザーの管理、ログ ファイルへのアクセスなど、アプリケーションを使用して SRM を管理および操作する方法について説明します。

本章の内容は、次のとおりです。

- 「VI クライアントを使用して SRM を管理する」 (P.33)
- 「保護サイトと復旧サイトの接続」 (P.34)
- 「クリデンシャルベースの認証」 (P.35)
- 「サティフィケートベースの認証」 (P.36)
- 「SRM ユーザー、グループ、権限、およびロール」 (P.37)
- 「SRM ログ ファイルへのアクセス」 (P.42)

VI クライアントを使用して SRM を管理する

VI クライアントは VirtualCenter サーバへのインターフェースです。ログインすると、ログイン先のサーバのタイプによってサポートされている機能のみが表示されます。SRM プラグインをインストールしたら、VI クライアントはサイト復旧オプションを表示します。

VI クライアントセッションから SRM にログインするには

- 1 VI クライアントを使用して、保護サイトまたは復旧サイトの VirtualCenter サーバにログインします。
- 2 ツールバーの [Site Recovery] アイコンをクリックします。

VI クライアントでの **Site Recovery** には、以下のコンポーネントが含まれます。

- インベントリ : 左側に配置され、保護グループや復旧プランを含む、SRM で利用可能なインベントリ オブジェクトが表示されます。
- [概要 (**Summary**)] タブ : 保護サイトと復旧サイトに関連する情報が表示されます。
- [セットアップ (**Setup**)] ペイン : サイトのフェイルオーバーを設定するのに使用されるオプションが表示されます。
- [アラーム (**Alarms**)] タブ : SRM 用に設定済みのアラームのリストが表示されます。
- [権限 (**Permissions**)] タブ : 選択したオブジェクトに対する権限を持つユーザーやグループ、および割り当てられた権限のレベルを一覧表示します。

保護サイトと復旧サイトの接続

SRM の使用を開始する場合は、保護サイトと復旧サイトの間に安全な接続を確立します。VI クライアントを使用して両方のサイトをペアリングして管理します。VI クライアントは一度に 1 つの **VirtualCenter** サーバにのみ接続することができるため、1 つの VI クライアントを起動して各サイトを管理します。復旧サイトに接続する前に、以下のものがが必要です。

- 復旧サイト **VirtualCenter** サーバの名前（または IP アドレス）とポート番号。
- クリデンシャル ベースの認証に使用されている場合は、復旧サイトの保護 SRM 管理者 (**Protection SRM Administrator**) のロール。
- リモート サーバへの管理者ログイン。

SRM との接続および **VirtualCenter** または **SRM** の別のインスタンスが認証されている必要があります。管理者の認証情報または信頼された証明書を使用して接続を認証できますが、認証方法を組み合わせることはできません。選択した認証方法は、各サイトで **VirtualCenter** サーバと **SRM** 間の接続、および保護サイトと復旧サイトで **SRM** サーバ間の接続を安全に行うために使用する必要があります。信頼された証明書を使用する場合は、どちらのサイトも証明書で同じ件名（インストール中に入力する組織および組織単位の情報で構成された）を使用する必要があります。

- クリデンシャル ベース : ユーザー名とパスワードを使用します。アカウントは管理者アカウントである必要があります。**VirtualCenter** サーバの権限はこれらの認証情報を指定します。**VirtualCenter** サーバへの通信に指定した認証情報を保存します。
- サティフィケート ベース : 信頼された証明機関によって署名された証明書を指定します。証明書は一般的に信頼された証明機関によって署名され、**VirtualCenter** サーバおよび保護サイトと復旧サイトで **SRM** にインストールされます。この構成は最も安全な接続です。

クリデンシャル ベースの認証

インストール時に自動生成された証明書を指定することによって、黙示的にクリデンシャル ベースの認証を指定することになります。この場合は、SRM サーバはインストール中に指定された証明書を保存してローカル VirtualCenter サーバとのすべての後続の通信を認証します。この SRM のインスタンスがリモート SRM サーバにペアリングされると、ペアリング プロセスの一部として指定された証明書が保存されてリモート SRM サーバとのすべての後続の通信を認証します。

VirtualCenter および SRM サーバへの認証情報の転送を含め、SRM とのすべての通信は SSL 暗号化を使用して保護されます。

クリデンシャル ベースの認証を使用したペアリング サイト

自動生成証明書を使用している保護サイトと復旧サイトの接続は、保護サイトと復旧サイトの接続設定のデフォルトです。

保護サイトと復旧サイトを接続するには

- 1 VI クライアントを使用して、保護サイトの VirtualCenter サーバにログインします。
- 2 ツールバーの [Site Recovery] アイコンをクリックします。
- 3 [保護セットアップ (Protection Setup)] ペインで、[設定 (Configure)] をクリックします。
- 4 リモート VirtualCenter サーバの IP アドレスまたはホスト名とポート番号を入力して [次へ (Next)] をクリックします。



注意 VirtualCenter サーバにホスト名を入力する場合は、小文字を使用します。VirtualCenter ホスト名は、インストール時と同じように、ペアリングの間もまったく同じように（完全修飾されているか否か）入力する必要があります。

- 5 リモート サイトの証明書を受け入れます。
この証明書のプロンプトは、SRM サーバがリモート VirtualCenter サーバの証明書を信頼しなかった場合に表示されます。
- 6 管理者のユーザー名とパスワードを入力します。
- 7 リモート サイトの証明書を受け入れます。
この証明書のプロンプトは、SRM サーバがリモート SRM サーバの証明書を信頼しなかった場合に表示されます。
- 8 各ステップにチェックマークが付いていることを確認し、[終了 (Finish)] をクリックします。

- 9 リモート VirtualCenter サーバの管理者のユーザー名とパスワードを入力します。
- 10 リモート サイトの証明書を受け入れます。
- 11 VI クライアントを使用して、復旧サイトの VirtualCenter サーバにログインします。
- 12 ツールバーの **[Site Recovery]** アイコンをクリックします。

これによってリモート VirtualCenter サーバにログインするのに必要な認証情報が送信されます。

- 13 リモート サイトの証明書を受け入れます。

ペアが正しく確立されると、保護サイトと復旧サイトのペインに接続情報が表示されます。

サティフィケート ベースの認証

サティフィケート ベースの認証には、SRM インストールに関係するすべてのサーバで、一般的に信頼された証明機関によって署名された証明書を使用する必要があります。これには VirtualCenter サーバと SRM サーバとが含まれます。これらの証明書は「信頼された証明書」と呼ばれます。

インストール時に信頼された証明書を指定することによって、サティフィケート ベースの認証を黙示的に選択することになります。この場合は、SRM サーバはインストール中に指定された証明書を使用してローカル VirtualCenter サーバとのすべての後続の通信を認証します。SRM サーバは最初のインストール中には指定された証明書を保存しません。

サティフィケート ベースの認証を使用したペアリング サイト

VMware では、サティフィケート ベースの認証を使用することをお勧めします。

保護サイトと復旧サイトに接続するには

- 1 VI クライアントを使用して、保護サイトの VirtualCenter サーバにログインします。
- 2 ツールバーの **[Site Recovery]** アイコンをクリックします。
- 3 **[セットアップ (Setup)]** ペインで、**[設定 (Configure)]** をクリックします。
- 4 リモート VirtualCenter サーバの IP アドレスまたはホスト名とポート番号を入力して **[次へ (Next)]** をクリックします。
- 5 各ステップにチェックマークが付いていることを確認し、**[閉じる (Close)]** をクリックします。
- 6 保護サイトから、**[リモート VirtualCenter Server (Remote VirtualCenter Server)]** ダイアログ ボックスにリモートの認証情報を入力します。

- 7 VIクライアントを使用して、復旧サイトの VirtualCenter サーバにログインします。
- 8 ツールバーの [Site Recovery] アイコンをクリックすると、必要な認証情報が送信されてペアの作成が完了します。

ペアリングが正常に行われたら、接続情報が表示されます。

SRM ユーザー、グループ、権限、およびロール

SRM は、VirtualCenter サーバと同じ権限モデルを使用します。オブジェクトに適用または継承された権限のセットは、オブジェクトに許可されている操作およびそれらの操作を実行できるロールのリストを決定します。SRM インベントリの管理対象オブジェクトには、特定の権限が適用されています。権限を制御して SRM 操作を実行するための方法には2つあります。

- ユーザーの追加：事前定義されたロールにユーザーを割り当てます。
- ロールの追加：ロールを作成し、管理者を追加してロールに正しい権限を追加します。

権限とロールを管理するには、管理者アカウントを使用して VirtualCenter サーバにログインする必要があります。

注 SRM を設定するには、ユーザーは VirtualCenter 権限と SRM 権限の両方を持っている必要があります。SRM 保護管理者や SRM 復旧管理者などの SRM ロールには VirtualCenter に対して特別な権限がないため、すべての SRM 操作を実行するための適切な権限がありません。また、その逆も同様です。VirtualCenter ロールは SRM 権限を提供しません。SRM ユーザーに必要な応じて VirtualCenter および SRM の特定のロールがあることを確認してください。

[権限 (Permissions)] タブは選択したオブジェクトに対する権限を持つユーザーやグループ、および割り当てられた権限のレベルを一覧表示します。

[ロール (Roles)] メニュー項目を有効にするには、[管理者 (Administration)] ビューにいる必要があります。[権限 (Permissions)] タブには以下が表示されます。

- [ユーザーやグループ (User/Group)] : SRM に存在するユーザーまたはグループ。
- [ロール (Role)] : 既存のユーザーまたはグループに割り当てられた権限のセット。
- [定義 (Defined in)] : ペア ユーザーまたはグループおよびロールが定義されているオブジェクト。

SRM 権限

保護サイトおよび復旧サイトで完全な管理者権限を取得するためには、以下の権限を定義する必要があります。

保護サイト：

- VirtualCenter ルートで読み取り専用（伝達なし）。
- Datacenter インベントリ オブジェクトで読み取り専用（伝達なし）。
- 仮想マシン レベル（伝達）で保護仮想マシン管理者ロール。
- SRM Site Recovery ルート レベル（伝達なし）で保護 SRM 管理者ロール。
- SRM 保護グループ レベル（伝達）で保護グループ管理者ロール。

復旧サイト：

- VirtualCenter ルート レベル（伝達なし）でインベントリ復旧管理者ロール。
- VirtualCenter データセンターレベル（伝達なし）でデータセンター復旧管理者ロール。
- VirtualCenter ホスト レベル（伝達なし）でホスト復旧管理者ロール。
- VirtualCenter リソース プールおよび VirtualCenter フォルダ レベル（伝達）で仮想マシン復旧管理者。
- SRM ルート レベル（伝達なし）で SRM 復旧管理者。
- SRM 復旧プラン レベル（伝達）でプラン復旧管理者。

SRM デフォルト ロール

以下の SRM 固有のロールが SRM のインストール中に VirtualCenter サーバ上で定義されています。

- 保護グループ管理者：保護グループをセットアップおよび変更します。
- 保護 SRM 管理者：保護サイトと復旧サイトのペアを作成し、インベントリ マッピングを設定します。
- 保護仮想マシン管理者：保護されている仮想マシンの保護特性をセットアップおよび変更します。
- データセンター復旧管理者：使用可能なデータストアを表示し、復旧仮想マシンのカスタマイズを実行します。
- ホスト復旧管理者：復旧時に仮想マシンのコンポーネントを構成します。
- インベントリ復旧管理者：復旧サイトのカスタマイズ仕様を表示します。

- プラン復旧管理者：保護および復旧仮想マシンを再構成します。また復旧のセットアップおよび実行権限を許可します。
- SRM 復旧管理者：SAN アレイを構成して保護プロファイルを作成します。
- 仮想マシン復旧管理者：復旧仮想マシンの作成およびリソース プールにシャドウ仮想マシンを追加します。また、復旧プランの実行時に復旧仮想マシンの再構成およびカスタマイズ権限をユーザーに許可します。

VirtualCenter サーバは、ユーザーに SRM の参照権限を許可するのに使用できる読み取り専用システム ロールを定義します。また、管理者ロールを使用して保護コンポーネントと復旧コンポーネントの両方の完全な制御をユーザーに許可できます。

インベントリ マッピングをセットアップするには、保護されたサイトのユーザーに以下のロールが割り当てられている必要があります。

- SRM ルート オブジェクト上の「保護 SRM 管理者」ロール。
- プライマリ サイトと復旧サイトの両方にマッピングされた VirtualCenter オブジェクトの「読み取り専用」ロール。

ロールの追加

一部のデフォルト ロール（管理者など）は事前設定されており、変更はできません。組み合わせの異なるアクセス権限が必要な場合は、必要に応じて別のロールを作成するか、用意されているサンプル ロールをニーズに合うように編集します。

ロールを追加するには

- 1 VI クライアントに、管理者権限を持つユーザーとしてログインします。
- 2 VI クライアントから、ナビゲーション バーの [管理 (Administration)] ボタンをクリックします。
- 3 [ロール (Roles)] タブをクリックします。
- 4 [ロールの追加 (Add Role)] をクリックします。
- 5 新しいロールの名前を入力します。
- 6 新しいロールに割り当てる権限を選択（たとえば、Site Recovery など）し、[OK] をクリックします。必要に応じてプラス記号 (+) をクリックしてリストを展開します。

VirtualCenter アクセス権限の割り当て

新しいユーザーとグループに関連するインベントリ オブジェクトのロールと権限を割り当てます。

ユーザーまたはグループに権限を割り当てるには

- 1 VI クライアントに、管理者権限を持つユーザーとしてログインします。
- 2 VI クライアントから、ナビゲーションバーの [インベントリ (**Inventory**)] ボタンをクリックします。
- 3 [権限 (**Permissions**)] タブをクリックします。
- 4 [権限 (**Permissions**)] タブを右クリックし、[権限の追加 (**Add Permission**)] を選択します。
- 5 [追加 (**Add**)] をクリックします。
- 6 このロールが割り当てられているユーザーまたはグループを識別します。
 - a [ドメイン (**Domain**)] ドロップダウン メニューから、ユーザーまたはグループが属しているドメインを選択します。
 - b [検索 (**Search**)] ボックスに名前を入力するか、[名前 (**Name**)] リストから名前を選択します。
ユーザー名またはグループ名が決定している場合は、[名前 (**Name**)] フィールドに名前を入力できます。
 - c [追加 (**Add**)] をクリックして [ユーザー (**Users**)] または [グループ (**Groups**)] リストに名前を追加します。
 - d 手順 a から手順 c を繰り返して追加のユーザーまたはグループを追加し、終了したら、[**OK**] をクリックします。
- 7 このロールを選択したインベントリ オブジェクトのすべての子オブジェクトに適用するには、[子オブジェクトへ伝達 (**Propagate to Child Objects**)] を選択します。
- 8 ユーザーおよびグループが適切な権限に割り当てられていることを確認し、[**OK**] をクリックします。
- 9 [**OK**] をクリックします。
サーバーは、オブジェクトの権限のリストに、権限を追加します。

新規ユーザー グループおよびロールを SRM に追加する

新しいユーザーとグループに関連する SRM インベントリ オブジェクトのロールと権限を割り当てます。

ユーザーまたはグループに権限を割り当てるには

- 1 VI クライアントに、管理者権限を持つユーザーとしてログインします。
- 2 ナビゲーションバーで [Site Recovery] をクリックします。

保護サイトと復旧サイトがペアになっている場合、復旧サイトのログイン情報を入力する必要があります。

- 3 SRM インベントリ オブジェクトの [権限(Permissions)] タブをクリックします。
- 4 [権限 (Permissions)] タブを右クリックし、[権限の追加 (Add Permission)] を選択します。
- 5 [追加 (Add)] をクリックします。
- 6 このロールが割り当てられているユーザーまたはグループを識別します。
 - a [ドメイン (Domain)] ドロップダウン メニューから、ユーザーまたはグループが属しているドメインを選択します。
 - b [検索 (Search)] ボックスに名前を入力するか、[名前 (Name)] リストから名前を選択します。
 - c [追加 (Add)] をクリックして、[ユーザー (Users)] または [グループ (Groups)] リストに名前を追加します。
 - d 手順 a から手順 c を繰り返してさらにユーザーまたはグループを追加します。
 - e 終了したら [OK] をクリックします。
- 7 [割り当てられた権限 (Assigned Permissions)] ダイアログボックスで、[割り当てられたロール (Assigned Role)] ドロップダウンメニューからロールを選択します。このメニューには、そのホストに割り当てられているすべての使用可能なロールが表示されます。
- 8 このロールを選択したインベントリ オブジェクトのすべての子オブジェクトに適用するには、[子オブジェクトへ伝達 (Propagate to Child Objects)] を選択します。このタスクを追加した各ユーザーまたはグループに実行します。
- 9 [OK] をクリックします。
サーバは、オブジェクトの権限のリストに、権限を追加します。

アクセス権限の変更

インベントリ内にあるオブジェクトのアクセス権限を変更できます。

ユーザーまたはグループの権限を変更するには

- 1 VI クライアントから、インベントリ オブジェクトをクリックします。
- 2 オブジェクトを選択し、[権限 (Permissions)] タブをクリックします。
- 3 変更するユーザーまたはグループおよびロール ペアを選択するには、項目を右クリックします。
- 4 ユーザーまたはグループの該当するロールを選択するには、[プロパティ (Properties)] を選択します。
- 5 ドロップダウンメニューから選択して [OK] をクリックします。

- 6 割り当てたインベントリ オブジェクトの子に権限を伝達するには、[伝達 (Propagate)] チェックボックスをクリックします。

アクセス権限の削除

使用可能なリストからユーザー、グループ、またはロールの権限を削除すると、ユーザーまたはグループおよびロール ペアが選択されたインベントリ オブジェクトから削除されます。ロールは使用可能アイテムのリストから削除されません。

ユーザーまたはグループの権限ロールを削除するには

- 1 VI クライアントから、インベントリ オブジェクトを選択します。
- 2 [権限 (Permissions)] タブをクリックします。
- 3 削除するユーザーまたはグループおよびロール ペアを選択するには、項目を右クリックします。
- 4 [削除 (Delete)] を選択します。

VirtualCenter サーバは権限の設定を削除します。

SRM ログ ファイルへのアクセス

サーバから SRM ログおよび設定ファイルを取得してそれらをデスクトップの圧縮 (Zip) フォルダに収集します。

SRM サーバホストにログインしたときにログ ファイルを取得するには

[スタート (Start)] > [プログラム (Programs)] > [VMware] > [VMware Site Recovery Manager] > [Site Recovery Manager のログ バンドルの生成 (Generate Site Recovery Manager log bundle)] をクリックします。

個々のログ ファイルは srm-support-MM-DD-YYYY-HH-MM.zip という名前のファイルに収集されます。ここで、MM-DD-YYYY-HH-MM は、ログ ファイルが取得された月、日、年、時間、分を示します。

VI クライアントにログインしたときにログ ファイルを取得するには

- 1 Windows コマンドプロンプトを開始します。
- 2 ディレクトリを C:\Program Files\VMware\VMware Site Recovery Manager\bin に変更します。
- 3 次のコマンドを実行します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>cscript srm-support.wsf
```

個々のログファイルは `srm-plugin-support-MM-DD-YYYY-HH-MM.zip` という名前のファイルに収集されます。ここで、`MM-DD-YYYY-HH-MM` は、ログファイルが取得された月、日、年、時間、分を示す文字列です。

5

保護サイトの構成

本章では、保護グループの作成、ストレージアレイ マネージャの構成、インベントリ環境設定、および仮想マシン設定の編集を含む、VMware Site Recovery Manager (SRM) 保護サイトの構成に必要な手順について説明します。

本章の内容は、次のとおりです。

- 「[保護サイトの構成](#)」 (P.45)
- 「[アレイ マネージャの設定](#)」 (P.46)
- 「[アレイ マネージャの修復](#)」 (P.48)
- 「[インベントリ環境設定の設定](#)」 (P.49)
- 「[保護グループの作成](#)」 (P.50)
- 「[仮想マシンプロパティの設定](#)」 (P.51)
- 「[メッセージおよびコマンド ステップの追加](#)」 (P.54)
- 「[IP アドレス マッピング](#)」 (P.55)

保護サイトの構成

保護サイトでの保護の設定には、以下の手順が含まれます。

- 1 ストレージレプリケーションアダプタをインストールします。

必要に応じてストレージベンダーのドキュメントを参照してください。アレイ マネージャを設定する前に、必要なアレイ スクリプトを追加して SRM サービスを再起動する必要があります。

- 2 アレイ マネージャを設定して SRM がレプリケートされた LUN を検出してデータストア グループを作成できるようにします。
- 3 インベントリ環境設定を設定して継承するすべての保護グループのグローバルマッピングを設定します。
- 4 一緒にフェイルオーバーする仮想マシンを定義する保護グループを作成します。
- 5 個々の仮想マシンを設定し、保護グループからインベントリ マッピングと設定が継承されるように仮想マシンのデフォルトを設定します。

VMware Infrastructure の構成の要件

アレイ マネージャの設定を開始する前に、以下の VMware Infrastructure の構成が必要です。

- 保護サイトと復旧サイトのデータセンター。
- 保護サイトおよび復旧サイトの ESX ホスト。

復旧サイトで特定のタイプのスナップショットの使用（仮想マシンがパワーオンまたは一時停止したときに撮られるスナップショット）をサポートする必要がある場合は、VMware ナレッジベースの条項 VMotion CPU Compatibility Requirements for Intel Processors (条項 1991) および VMotion CPU Compatibility Requirements for AMD Processors (条項 1992) で定義されているように、互換性のある CPU が両方のサイトの ESX ホストで必要です。また、ホストでは同じ BIOS 機能が有効になっている必要があります。サーバの BIOS 構成が一致しない場合は、それ以外が同一であっても互換性のエラー メッセージが引き続き表示されます。チェックすべき最も一般的な機能は、非実行メモリ保護 (NX または XD) と仮想テクノロジー (VT または AMD-V) です。

- 保護サイトで保護される仮想マシン。

データセンター、ホスト、リソース プールの設定に関する詳細については、『VMware Infrastructure Server Configuration Guide』を参照してください。

アレイ マネージャの設定

保護サイトと復旧サイトが相互に接続されたら、アレイ マネージャを設定して SRM が使用可能なアレイおよびレプリケートされた LUN を識別できるようにします。アレイ マネージャはアレイ ベンダーから供給されるストレージ レプリケーションアダプタを使用します。アレイ マネージャを設定する場合は、使用するアレイに関する情報を入力します。SRM はこの情報を使用してサポートしている SRM サーバおよびレプリケートされた LUN で使用可能なアレイを検出します。詳細については、「[アレイ ベース レプリケーション](#)」(P.13) を参照してください。

アレイ マネージャを設定するには、マネージャのストレージ レプリケーション アダプタが SRM サーバ ホストにインストールされている必要があります。また、アレイ マネージャを設定するときに入力する必要がある情報が含まれているアレイ ベンダーからのドキュメントも必要です。

SRM はアレイを 24 時間ごとに再スキャンして追加または削除された LUN を検出します。アレイ マネージャをサイトに設定したら、アレイ マネージャに必要な IP アドレスや管理者の認証情報などの情報を変更したり、あるいは LUN を追加または削除してその変更を SRM に次に予定されている再スキャンまでに認識させない限り、通常はそれらを再設定する必要はありません。

アレイ マネージャを設定するには、以下の条件が配備されている必要があります。

- VI クライアントは保護サイトに接続されている必要があります。
- 保護 SRM 管理者のロール。

アレイ マネージャを設定するには

- 1 VI クライアントを使用して、保護サイトの VirtualCenter サーバにログインします。
- 2 VI クライアントのツールバーで [Site Recovery] アイコンをクリックします。
- 3 復旧サイトで有効なユーザー名とパスワードを入力するようにプロンプトが表示されます。
- 4 [Site Recovery for <protected-site-hostname>] ウィンドウの [概要 (Summary)] ページで、[保護セットアップ (Protection Setup)] の下の [アレイ マネージャ (Array Managers)] 行を検索します。[構成 (Configure)] をクリックして [アレイ マネージャの設定 (Configure Array Managers)] ウィザードを開きます。
- 5 [追加 (Add)] をクリックして [アレイ マネージャの追加 (Add Array Manager)] ウィンドウを開きます。
- 6 [アレイ マネージャの追加 (Add Array Manager)] ウィンドウで、ストレージアレイに接続するために SRM が必要とする情報を入力します。
 - アレイ マネージャの表示名を入力します。このアレイ マネージャが管理するアレイを識別しやすくする説明的な名前を使用します。
 - [マネージャ タイプ (Manager Type)] リストからストレージ レプリケーション アダプタを選択します。使用したいマネージャ タイプがリストに表示されない場合は、それをサポートするストレージ レプリケーション アダプタが SRM ホストにインストールされていません。
 - マネージャ タイプを選択したら、[アレイ マネージャの追加 (Add Array Manager)] ウィンドウはそのマネージャ タイプに必要な情報を入力するフィールドに変更します。これらのフィールドの値に関する詳細については、ストレージアレイ ベンダーからのドキュメントを参照してください。

- 7 [接続 (Connect)] をクリックして入力した情報を確認し、アレイ マネージャがサポートするアレイのリストを返します。

サポートされているすべてのアレイが選択されています。SRM で使用しないアレイの選択をオフにします。
- 8 SRM で使用するストレージアレイの選択が終了したら、[OK] をクリックします。

アレイ マネージャは選択されたアレイに問い合わせたレプリケートされる LUN を検出します。選択されたアレイに関する詳細およびサポートするレプリケートされた LUN の数は [アレイ マネージャの設定 (Configure Array Managers)] ウィンドウの [レプリケートされるアレイ ペア (Replicated Array Pairs)] 領域に表示されます。
- 9 [次へ (Next)] をクリックして復旧サイトでストレージアレイを設定します。

これらのアレイを追加する手順は、手順 5 から手順 7 に表示されている保護サイトでアレイを追加する手順と同じです。復旧サイトでのストレージアレイの追加を終了すると、SRM は各アレイ ペアの両方のメンバーと通信できることを確認し、[アレイ マネージャの設定 (Configure Array Managers)] ウィンドウの [レプリケートされるアレイ ペア (Replicated Array Pairs)] 領域の [アレイ ID (Array ID)] 列に緑色のチェックマーク アイコンを表示します。緑色のチェックマークが表示されない場合は、[アレイ マネージャの追加 (Add Array Manager)] ウィンドウで入力したいいくつかの情報を修正する必要がある場合があります。
- 10 [次へ (Next)] をクリックして [レプリケートされたデータストアのレビュー (Review Replicated Datastores)] ページを表示します。

ツリーを参照して正確なデータストア グループおよびレプリケートされた LUN がリストされていることを確認します。登録済みの仮想マシンを含むレプリケートされたデータストアだけがこのページに表示されます。
- 11 アレイ マネージャの設定に納得したら、[終了 (Finish)] をクリックします。

アレイ マネージャの修復

保護サイトにアクセスできない場合にアレイ マネージャの詳細を編集する必要がある場合は、アレイ マネージャの修復機能を使用します。保護サイトにアクセスできる場合は、「アレイ マネージャの設定」(P.46) の手順に従って編集することができます。

アレイ マネージャを修復するには、以下の条件が配備されている必要があります。

- VI クライアントは復旧サイトに接続されている必要があります。
- 復旧 SRM 管理者のロール。

アレイ マネージャを修復するには

- 1 インベントリで、[復旧プラン (Recovery Plans)] をクリックします。
- 2 [概要 (Summary)] タブのコマンド領域で、[アレイ マネージャの修復 (Repair Array Managers)] をクリックします。これで、[アレイ マネージャの設定 (Configure Array Managers)] ウィンドウの [復旧サイトのアレイ マネージャ (Recovery Site Array Managers)] ページが開きます。[追加 (Add)]、[削除 (Remove)]、または [編集 (Edit)] ボタンを使用して復旧サイトのアレイ マネージャを修正します。

インベントリ環境設定の設定

インベントリ環境設定を設定することにより、保護サイトと復旧サイトのカウンタパートとの間のコンピュータリソース、仮想マシンフォルダ、およびネットワークのマッピングを提供します。これらのマッピングは、保護された個々の仮想マシンで指定されている値によって置き換えられます。マッピングする前に、復旧サイトに関連付ける保護サイトのコンピュータリソース、仮想マシンフォルダ、およびネットワークを決定します。復旧サイトで、対応するコンピュータリソース、仮想マシンフォルダ、およびネットワークを作成します。

リソースのマッピングはオプションです。マッピングにより、復旧サイトにレプリケートされる仮想マシンにデフォルトのロケーションおよびネットワークが提供されます。保護グループを作成してマップが存在しない場合は、保護される各仮想マシンを個々に設定する必要があります。

インベントリ環境設定を設定するには、以下の条件が配備されている必要があります。

- VI クライアントは保護サイトに接続されている必要があります。
- 保護 SRM 管理者のロール。

インベントリ環境設定を設定するには

- 1 VI クライアントを使用して、保護サイトの VirtualCenter サーバにログインします。
- 2 VI クライアントのツールバーで [Site Recovery] アイコンをクリックします。
- 3 [インベントリ マッピング (Inventory Mappings)] タブをクリックします。
- 4 [設定 (Configure)] をクリックします。
- 5 復旧サイトにマッピングするネットワークを選択し、[設定 (Configure)] をクリックします。
- 6 ツリーを展開して該当するネットワークを選択し、[OK] をクリックします。
- 7 [設定 (Configure)] をクリックします。
- 8 [インベントリ マッピング (Inventory Mappings)] タブから復旧サイトにマップする [コンピュータリソース (Compute Resources)] を選択し、[設定 (Configure)] をクリックします。

- 9 復旧サイトで作成したコンピュータ リソースを選択し、[OK] をクリックします。
- 10 [設定 (Configure)] をクリックします。
- 11 復旧サイトにマップする仮想マシン フォルダを選択します。
- 12 この仮想マシン用に復旧サイトで作成した仮想マシン フォルダを選択し、[OK] をクリックします。

保護グループの作成

保護グループは、テストおよび復旧の際に、復旧サイトで一緒にフェイルオーバーする仮想マシンのグループです。保護グループを作成すると、SRM は、保護グループの各仮想マシンに復旧サイトでブレースホルダ仮想マシンを作成します。これらのブレースホルダ仮想マシンをパワーオンすることはできませんが、それらを設定してイベントリ内で移動させることができます。

1つの保護グループは1つのデータストア グループを保護します。グループ内の仮想マシンは特定の共通特性を共有しています。これらの仮想マシンを設定して保護グループに追加することによって、追加の仮想マシンを保護できます。復旧サイトへのデータ移動は、グループを作成するときに指定したレプリケーション プロバイダに任されています。

保護グループはデータストア グループの範囲内にあるため、Storage VMotion を使用して仮想マシンのストレージを移動することによって、そのストレージが別のデータストアに移動した場合は、仮想マシンを保護グループから削除することができます。

注 オペレーティングシステムによってはファイルシステムの書き込みをキャッシュに格納するため、実行している仮想マシンの基礎となるレプリケートされたストレージのファイルによっては、レプリケートされたときに最新でない場合があります。そのため、復旧した仮想マシンが最新のレプリケーションの結果を使用してパワーオンしたときに、保護仮想マシンのファイルの状態の変更がすべて含まれていない場合があります。

1つの保護グループを1つまたは複数の復旧プランに入れることができます。

保護グループを作成するには、以下の条件が配備されている必要があります。

- VI クライアントは保護サイトに接続されている必要があります。
- 保護グループ管理者のロール。
- 完全設定済みのアレイ マネージャ。

保護グループを作成するには

- 1 VI クライアントを使用して、保護サイトの VirtualCenter サーバにログインします。
- 2 VI クライアントのツールバーで [Site Recovery] アイコンをクリックします。

- 3 インベントリの [保護グループ (Protection Groups)] をクリックします。
- 4 [概要 (Summary)] タブの [コマンド (Commands)] ペインで、[保護グループの作成 (Create Protection Group)] をクリックします。
- 5 [保護グループ名 (Protection Group Name)] フィールドに、グループの名前を入力します。
- 6 [次へ (Next)] をクリックします。
- 7 データストア グループを選択して保護グループに追加します。
保護グループに関連付けることができるのは 1 つのデータストア グループのみです。関連付けは後で変更することはできません。
- 8 [次へ (Next)] をクリックします。
- 9 この保護グループの仮想マシンのファイルを保存する復旧サイトのデータストアを選択します。
データストアはメタ データを .vmdk ファイルではなく、仮想マシンに保存します。メタ データには .vmsd、.vmx、および .vmxf ファイルが含まれていて、復旧サイトで VirtualCenter インベントリに仮想マシンを追加できるようにデータストアに書き込まれます。
選択されたデータストア グループの仮想マシンにインベントリ マッピングが定義されている場合、SRM はこれらの仮想マシンの保護を開始します。インベントリ マッピングが定義されていない場合は、空の保護グループが作成され、仮想マシンのステータスは [設定されていない (Not Configured)] となります。
- 10 [終了 (Finish)] をクリックします。
保護グループはインベントリの [保護グループ (Protection Groups)] に追加されます。
仮想マシンの設定は、保護グループの [仮想マシン (Virtual Machines)] で実行されます。詳細については、「[仮想マシン プロパティの設定](#)」(P.51) を参照してください。

仮想マシン プロパティの設定

SRM は、復旧サイト インベントリにブレースホルダ仮想マシンを作成します。これらの各ブレースホルダは保護サイトの仮想マシンを表し、その仮想マシンに復旧サイトでインベントリ エントリを提供します。

保護仮想マシンのプロパティのカスタマイズは復旧サイトのオブジェクトであり、復旧サイトに接続している間に設定する必要があります。保護仮想マシンのリソース設定は、復旧サイトでは全く意味を持たない任意の単位を使用するため、レプリケートされません。

[仮想マシンのプロパティ (virtual machine properties)] ウィザードを使用して、以下のタスクを実行できます。

- 保護グループの仮想マシンリストから未設定の仮想マシンを追加します。

- 保護グループまたは復旧グループにリストされている仮想マシンを編集します。保護グループがすでに存在する場合は [仮想マシン (Virtual Machines)] タブから仮想マシンを編集できます。
- 復旧サイトで仮想マシンを設定するには、「[復旧プランでの仮想マシンの設定](#)」(P.67)を参照してください。

保護仮想マシンにプロパティを設定する

保護仮想マシンのプロパティは、マシンの保護グループに指定したインベントリ環境設定から最初を取得されたものです。インベントリ環境設定を指定していない場合、または仮想マシンを再設定する必要がある場合は、以下の方法を行うことができます。

- 保護グループを作成するときに使用できる [仮想マシンの設定 (Configure virtual machines)] ページから再設定する。
- 保護グループがすでに存在する場合は、[仮想マシン (Virtual Machines)] タブから再設定する。

仮想マシン保護プロパティを設定するには、以下の条件が配備されている必要があります。

- VI クライアントは復旧サイトに接続されている必要があります。
- 保護仮想マシン管理者のロール。

保護グループにすべての仮想マシンを設定するには

- 1 VI クライアントを使用して、復旧サイトの VirtualCenter サーバにログインします。
- 2 VI クライアントのツールバーで [Site Recovery] アイコンをクリックします。
- 3 インベントリ リストで保護グループを選択します。
- 4 [仮想マシン (Virtual Machines)] タブで、[すべて設定 (Configure All)] をクリックします。

このアクションは既存のインベントリ マッピングを [設定されていない (Not Configured)] のステータスを持つすべての仮想マシンに適用します。この処理が完了した後で、自動的に設定されなかったすべての仮想マシンは、[マッピングが見つかりません (Mapping Missing)] または [マッピングが無効 (Mapping Invalid)] のステータスになります。「[個々の仮想マシンのプロパティを設定するには](#)」(P.52) に説明があるように、これらのマシンを個々に設定する必要があります。

個々の仮想マシンのプロパティを設定するには

- 1 VI クライアントを使用して、復旧サイトの VirtualCenter サーバにログインします。
- 2 VI クライアントのツールバーで [Site Recovery] アイコンをクリックします。
- 3 インベントリ リストで保護グループを選択します。

- 4 [仮想マシン (Virtual Machines)] タブから、設定するマシンを選択し、[保護の設定 (Configure Protection)] をクリックします。
- 5 復旧サイトで仮想マシンを配置する仮想マシンフォルダを選択し、[次へ (Next)] をクリックします。
- 6 復旧サイトで仮想マシンを管理するホストを選択し、[次へ (Next)] をクリックします。
- 7 復旧サイトで仮想マシンを配置するリソース プールを選択し、[次へ (Next)] をクリックします。
- 8 この仮想マシンで使用するコンポーネント レベルの保護をクリックし、[次へ (Next)] をクリックします。

SRM は、仮想ディスク、フロッピー ディスク、または ISO 画像などの添付されたデバイスにアクセスできない場合は、仮想マシンを保護できません。仮想マシンはデバイスなしで操作するか、または、フェイルオーバー中に仮想マシンをデバイスに添付できるようにデバイスはデータストアにコピーされます。

- 9 復旧仮想マシン ファイルを格納するデータストアをクリックし、[次へ (Next)] をクリックします。

[この VM のカスタマイズ仕様を指定 (Specify a Customization Specification for this VM)] 画面が表示されます。カスタマイズ仕様を使用すると、復旧された仮想マシンの IP アドレスやネットワーク マスクなどのネットワーク情報を変更できます。その他の仮想マシンのプロパティはカスタマイズできません。

- 10 [カスタマイズ仕様 (Customization Specification)] ページで [参照 (Browse)] をクリックして使用可能なカスタマイズ仕様を表示します。
- 11 仮想マシンを選択して適用し、[OK] をクリックします。

[この VM のカスタマイズ仕様を指定 (Specify a Customization Specification for this VM)] 画面の [説明 (Description)] に指定されたカスタマイズ オプションの説明が表示されます。

このオプションを設定するには、復旧サイトで VI クライアントを使用してカスタマイズ仕様を作成する必要があります。仕様が設定されていないと、「使用可能なカスタマイズ仕様が見つかりません (No available Customization Specification found)」というメッセージが表示されます。カスタマイズ仕様が指定された仮想マシンにオペレーティング システムがない場合、カスタマイズ スクリプトのステップは復旧テストまたはフェイルオーバーのときに失敗します。

「[カスタマイズ仕様の使用](#)」(P.69) を参照してください。

- 12 [次へ (Next)] をクリックします。
- 13 ドロップダウン メニューから復旧の優先順位を選択し [次へ (Next)] をクリックします。
 - 高：仮想マシンを番号順に開始します。
 - 通常および低：この ESX ホストで他の仮想マシンと同時に仮想マシンを開始します。

- 14 [次へ (**Next**)] をクリックします。

この仮想マシンをパワーオンする前に実行する、ユーザー定義のメッセージおよびコマンドを追加します。これらのユーザー定義メッセージおよびコマンドは削除したり、並べ替えることができます（「[メッセージおよびコマンド ステップの追加](#)」(P.54) を参照）。

- 15 [終了 (**Finish**)] をクリックします。

メッセージおよびコマンド ステップの追加

仮想マシンのプロパティを設定する際、保護サイトまたは復旧サイトのいずれかで、復旧プランにメッセージまたはコマンドを追加できます。パワーオンする前または後でメッセージまたはコマンド ステップを追加できます。

メッセージ ステップはテキスト形式の情報です。復旧プランを実行中にメッセージ ステップを検出した場合、復旧はメッセージのテキストを確認するまで一時停止します。その後プランは続行されます。

コマンド ステップは、**Site Recovery Manager** で提供されているデフォルト ステップと一緒に復旧プランに挿入することができるライブ スクリプトです。復旧プランを実行中にコマンド ステップが検出されると、そのスクリプトが実行されます。

メッセージ ステップおよびコマンド ステップを追加するには、以下の条件が必要です。

- VI クライアントは保護サイトまたは復旧サイトのいずれかに接続されている必要があります。
- 復旧仮想マシン管理者のロールまたは復旧プラン管理者のロール。

バッチ ファイルまたはコマンドの実行

Windows バッチ ファイルまたはコマンドを実行するには、フルパスを使用して Windows コマンドを開始します。たとえば、`c:\alarmscript.bat` に配置されているスクリプトを実行するには、次のコマンド行を使用します。

```
c:\windows\system32\cmd.exe /c c:\alarmscript.bat
```

復旧プランにバッチ ファイルまたはコマンドを追加する場合は、次の要件に注意してください。

- スクリプトは、SRM サーバがインストールされているホストに配置されている必要があります。
- バッチ ファイルまたはコマンドへの SRM 呼び出しは、VI クライアントにログインするユーザーとしてではなく、SRM サーバ ホストのローカル管理者として実行します。

- 出力に 127 よりも大きい ASCII 値を持つ文字が含まれているバッチ ファイルまたはコマンドでは、UTF-8 符号化を使用して SRM サーバ ホストのローカル管理者として実行する必要があります。
- スクリプト出力の最後の 4KB のみがログファイルおよび復旧履歴に取得されます。多くの出力を生成するスクリプトでは、ログされるように標準出力に送信するのではなく、出力をファイルにリダイレクトすることができます。
- コマンドまたはスクリプトが 0 以外のステータスで終了した場合、復旧は終了します。コマンドによっては、正常に終了した場合でも、0 以外のステータスで終了する場合があります。コマンドが 0 のステータスで終了するように強制するには、次の例のように、それに `|| exit 0` を付けます。

```
c:\windows\system32\cmd.exe /C chkdsk || exit 0
```

ESX ホストでコマンド行タイムアウトを変更する

デフォルトでは、SRM は完了までに 300 秒以上要する呼び出しスクリプトを終了します。スクリプトの実行が一般的に時間がかかる場合は、タイムアウトの値を増やすこともできます。コマンド行タイムアウトを変更するには、`vmware-dr.xml` 設定ファイルを編集して `calloutCommandLineTimeout` パラメータの値を変更し、新しいタイムアウト値を秒で指定します。

SRM の電源状態のタイムアウトを変更する

仮想マシン（たとえば、パワーダウン）の電源状態を変更する要求が 120 秒以内に完了しない場合は、デフォルトでは、SRM はエラーを報告します。電源状態のタイムアウトを変更するには、`vmware-dr.xml` 設定ファイルを編集して `powerStateChangeTimeout` パラメータの値を変更し、新しいタイムアウト値を秒で指定します。

IP アドレス マッピング

SRM IP アドレス マップ レポータは、保護サイトと復旧サイトのネットワーク構造を説明する XML ドキュメントを生成します。これは、ネットワーク管理者に 2 つのサイトのネットワークが相互に関連付けられる方法および復旧サイトの仮想マシンによって使用されるネットワークおよび IP アドレスを決定するために使用される方法のビューを提供します。

SRM IP アドレス マップ レポータは、SRM サーバ設定ファイルの情報を使用して `VirtualCenter` および `SRM` に接続します。保護サイトまたは復旧サイトのいずれの設定ファイルも使用できます。レポータはファイルに定義されたサイトに接続してそのサイトとペアリングされたサイトの両方に問い合わせます。ユーティリティは、最初にサイトで、次に復旧プランでグループ化されたマッピングの完全なリストを生成します。

次の書式のコマンドを使用して復旧サイトの設定ファイルに対してツールを実行することができます。

```
dr-ip-reporter.exe -cfg <DR サーバ設定 XML> -out <出力 XML ファイルパス> [-plan <復旧プラン名>] [-i]
```

- `-plan <復旧プラン名>` を指定して特定の復旧プランを参照します。

- `-i` を指定して指紋確認プロンプトをオフにします。

すべての復旧プランにマッピングを報告するには

- 1 ディレクトリを `C:\Program Files\VMware\VMware Site Recovery Manager\bin` に変更します。
- 2 次のコマンドを実行します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>dr-ip-reporter.exe
-cfg ..\config\vmware-dr.xml -out c:\tmp\report.xml
```

特定の復旧プランにマッピングを報告するには

- 1 ディレクトリを `C:\Program Files\VMware\VMware Site Recovery Manager\bin` に変更します。
- 2 次のコマンドを実行します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>dr-ip-reporter.exe
-cfg ..\config\vmware-dr.xml -out c:\tmp\report.xml -plan Plan-B
```

バッチ IP プロパティのカスタマイズ

SRM には、復旧プランの任意またはすべての仮想マシンで IP プロパティ (ネットワーク設定) を指定できるツールが含まれています。指定するには、ツールが生成するカンマ区切り値 (CSV) ファイルを編集します。最初に、このファイルにはプランの各プレースホルダ仮想マシンの単一行が含まれています。ファイルを編集して各プレースホルダ仮想マシンの各ネットワーク アダプタに行を追加し、各アダプタのネットワーク設定をカスタマイズします。終了したら、編集したファイルをプレースホルダ仮想マシンにカスタマイズ仕様を作成するコマンドへの入力として使用します。

CSV ファイルを生成するには

- 1 ディレクトリを `C:\Program Files\VMware\VMware Site Recovery Manager\bin` に変更します。
- 2 次のコマンドを実行します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>dr-ip-customizer.exe
-cfg ..\config\vmware-dr.xml -csv c:\tmp\example.csv -cmd generate
```

3つのプレースホルダ仮想マシンを定義する SRM 復旧プラン設定で、生成されたファイルは次のように表示されます。

```
VM ID,VM Name,Adapter ID,MAC Address,DNS Domain,Net BIOS,Primary WINS,Secondary
WINS,IP Address,Subnet Mask,Gateway(s),DNS Server(s), DNS Suffix(es)
shdw3,srm3,0,,,,,,,,,
shdw2,srm2,0,,,,,,,,,
shdw1,srm1,0,,,,,,,,,
```

ファイルには各列の意味を定義するヘッダー行および復旧プランで検索された各プレースホルダ仮想マシンの単一行が含まれています。値が投入される唯一の行を次に示します。

- VM ID (プレースホルダ仮想マシンの ID)
- VM 名 (プレースホルダ仮想マシンのホスト名)
- アダプタ ID (常に 0 でグローバル IP 設定を指定、任意のアダプタ固有のものではありません)

CSV ファイルを編集して IP プロパティをカスタマイズする

例 5-1 の表には、スプレッドシートプログラムを使用して `dr-ip-customizer` の出力を開いて、復旧プランのプレースホルダ仮想マシンにネットワーク設定を定義する追加の行を作成した結果を示します。

例 5-1.

VM ID	VM 名	アダプタ ID	MAC アドレス	DNS ドメイン	NetBIOS	プライマリ WINS	セカンダリ WINS	IP アドレス	サブネットマスク	ゲートウェイ	DNS サーバ	DNS サーバ フィックス
shdw1	srm1	0									10.10.10.1	example.com
shdw1		1	00-1f-3a-38-29-9c	example.com				dhcp				
shdw2	srm2	0										
shdw2		1	00-1f-3a-38-29-9c	example.com		10.10.10.10		10.13.99.5	255.255.0.0	10.10.10.100	10.10.10.1	
shdw2		1									10.10.10.2	
shdw3	srm3	0										
shdw1	srm1	0									10.10.10.1	example.com
shdw1		1	00-1f-3a-38-29-9c	example.com				dhcp				
shdw2	srm2	0										
shdw2		1	00-1f-3a-38-29-9c	example.com		10.10.10.10		10.13.99.5	255.255.0.0	10.10.10.100	10.10.10.1	
shdw3		1									10.10.10.2	
shdw2		1	00-1a-3f-b8-f3-79	example.com		10.10.10.10		10.13.99.22	255.255.0.0	10.10.10.100	10.10.10.1	
shdw3		1									10.10.10.2	

以下のルールは、`dr-ip-customizer` ユーティリティが作成した CSV ファイルを変更する場合に適用されます。

- [MAC アドレス (MAC Address)] フィールドは同じ仮想マシン上のアダプタを区別する場合にのみ適用されます。これは、読み取り専用です。MAC アドレスを変更すると、カスタマイズが適用された場合、仮想マシンの設定を無効にします。

- [VM 名 (VM Name)] フィールドはファイルのカスタマイズするユーザーの参照を目的としています。このフィールドは CSV ファイルが作成される場合に生成されますが、修正が復旧プランに適用された場合には無視されます。
- アダプタ ID が 0 である行で、修正可能なフィールドは、DNS サーバと DNS サフィックスのみです。指定されている場合は、これらの値は、その VM ID の他のすべてのアダプタに継承されます。
- プレースホルダ仮想マシンで特定のアダプタのプロパティを定義するには、VM ID 列にその仮想マシンの ID およびアダプタ ID 列のアダプタ ID (プレースホルダ仮想マシンでアダプタがインストールされている仮想 PCI スロット) が含まれている新しい行を作成し、次にその他の列に値を指定します。
- 列に複数の値を指定する場合は、そのアダプタに追加の行を作成してその行の列に値を含めます。例 5-1 では、追加の行がプレースホルダ仮想マシン shdw2 と shdw3 のセカンダリ DNS サーバを定義します。
- プレースホルダ仮想マシンを DHCP クライアントとして作成するには、例 5-1 の 2 行目に示されているように、IP アドレス フィールドに **dhcp** と入力します。
- DHCP クライアントでない 0 以外のアダプタ ID の場合：
 - IP アドレス、サブネットマスク、ゲートウェイ、および DNS サーバに値を指定する必要があります。ただし、これらのプロパティのグローバル値が存在する (in the row for Adapter ID zero for that VM ID) 場合は、指定する必要はありません。グローバル値が指定されている場合は、0 以外の各アダプタ ID に指定する値によって上書きされます。
 - NetBIOS 列には、空欄でない場合、以下のいずれかの文字列が含まれている必要があります。
 - disableNetBIOS
 - enableNetBIOS
 - enableNetBIOSViaDhcp
 - MAC アドレス列にはアダプタ ID 列に指定されたアダプタの MAC アドレスが含まれている必要があります。アドレスは、ダッシュまたはコロンで区切られた 16 進数字の組み合わせで書き込まれます。大文字小文字は区別されません。
- 列にカンマを入力した場合、カスタマイズされた IP プロパティに適用すると、エラーが発生します。

カスタマイズされた IP プロパティを適用するには

- 1 ディレクトリを C:\Program Files\VMware\VMware Site Recovery Manager\bin に変更します。
- 2 次のコマンドを実行します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>dr-ip-customizer.exe  
-cfg ..\config\vmware-dr.xml -csv c:\tmp\example.csv -cmd create
```

カスタマイズされた IP プロパティをリセットまたは元に戻すには

- 1 ディレクトリを C:\Program Files\VMware\VMware Site Recovery Manager\bin に変更します。
- 2 次のコマンドを実行します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>dr-ip-customizer.exe  
-cfg ..\config\vmware-dr.xml -csv c:\tmp\example.csv -cmd drop
```

カスタマイズされた IP プロパティを更新するには

- 1 CSV ファイルを編集して変更するプロパティを修正します。
- 2 ディレクトリを C:\Program Files\VMware\VMware Site Recovery Manager\bin に変更します。
- 3 次のコマンドを実行します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>dr-ip-customizer.exe  
-cfg ..\config\vmware-dr.xml -csv c:\tmp\example.csv -cmd recreate
```

復旧サイトの構成

復旧プランは、データセンターの操作を保護サイトから復旧サイトに切り替えるためのステップの一覧です。この章では、復旧プランを作成および変更するのに必要なステップについて説明します。

復旧サイトでの保護の設定には、以下のタスクが含まれます。

- 復旧プランを作成します。
- 復旧プランで復旧する保護グループを選択します。
- SRM は該当する復旧ステップを使用して復旧プランを作成します。必要に応じて復旧プランをカスタマイズします。

本章の内容は、次のとおりです。

- 「[復旧プランの作成](#)」 (P.61)
- 「[復旧プランの管理](#)」 (P.63)
- 「[復旧プランのテスト](#)」 (P.64)
- 「[復旧プランの実行](#)」 (P.66)
- 「[復旧プランでの仮想マシンの設定](#)」 (P.67)
- 「[カスタマイズ仕様の使用](#)」 (P.69)

復旧プランの作成

復旧プランは、プラン名およびプランに含める保護グループを入力するように求める復旧プラン ウィザードを使用して作成されます。SRM 復旧プランを使用すると、以下を行うことができます。

- 複数の復旧プランを作成することができます。たとえば、サイト全体の障害に対してはあるプランを指定しておき、大規模な部分的な障害に対しては別のプランを指定するとか、あるいは各ビジネス単位ごとに1つの復旧プランを指定することもできます。
- 保護グループは、1つ以上の復旧プランに含めることができます。
- テスト用に空の復旧プランを作成できます。

詳細については、「[保護グループの作成](#)」(P.50)を参照してください。

復旧プランを作成する間に、復旧中にサスペンドさせる仮想マシンを選択します。サスペンドさせる仮想マシンは、復旧ホストで実行するローカル仮想マシンです。重要でないリソースをサスペンドすることで、スペースを節約してホスト上のCPUとメモリリソースを解放します。

パワーオンされるマシンは、フェイルオーバーされるマシンです。復旧を実行する場合、仮想マシンはプランに設定されている応答時間に応じてパワーオンします。仮想マシンは、[高 (High)]、[標準 (Normal)]、[低 (Low)]、または[パワーオンなし (No Power On)]に分類され、プランが実行されるときに正しい順序で開始されるようにします。

復旧プランを作成するには、以下の条件が配備されている必要があります。

- VIクライアントは復旧サイトに接続されている必要があります。
- 復旧プラン管理者のロール。

復旧プランを作成するには

- 1 VIクライアントを使用して、復旧サイトのVirtualCenterサーバにログインします。
- 2 VIクライアントのツールバーで[Site Recovery]アイコンをクリックします。
- 3 インベントリで[復旧プラン (Recovery Plans)]をクリックします。
- 4 [概要 (Summary)]タブの[コマンド (Commands)]ペインで、[復旧プランの作成 (Create Recovery Plan)]をクリックします。
- 5 復旧プランの名前とオプションの説明を入力して、[次へ (Next)]をクリックします。
- 6 プランに含める保護グループを選択して[次へ (Next)]をクリックします。
復旧プランには1つ以上の保護グループを含めることができます。
- 7 プランの仮想マシンの応答時間を設定します (応答は、VMware ツールがインストールされていない仮想マシンでは検出できません)。
 - ネットワーク設定の変更：ネットワーク設定を変更する復旧手順の後で、指定された間隔内に仮想マシンが予期されたIPアドレスを取得しない場合は、エラーが報告されて復旧プランは次の仮想マシンで続行されます。

- **OS Heartbeat** を待機: 仮想マシンがパワーオンされた後で指定された間隔内に OS Heartbeat を報告しない場合は、エラーが報告されて復旧プランは次の仮想マシンで続行されます。
- 8 [次へ (Next)] をクリックします。
 - 9 復旧プランのテスト時に使用するネットワークを選択するか、[自動 (Auto)] を選択して [ネットワークのテスト (Test Network)] ドロップダウンメニューから隔離された新規のネットワークを作成します。
復旧プランに **Linux** を実行する仮想マシンが含まれていて、**DHCP** クライアントである場合は、ネットワークに **DHCP** サーバが含まれていることを確認してください。
復旧サイトで **VMware HA** を使用する場合は、**ESX** ホストにまたがるテスト **VLAN** を作成して使用する必要があります。**HA** クラスタは他のテスト ネットワーク設定では正常に動作しません。
 - 10 [次へ (Next)] をクリックします。
 - 11 [仮想マシンおよびデータセンター] を展開します。
 - 12 プランがテストまたは実行された場合にサスペンドするローカル仮想マシンを選択して、[終了 (Finish)] をクリックします。

復旧プランの管理

ナビゲーション ペインで復旧プランを選択すると、ページのメインの表示エリアに復旧プランの詳細が表示されます。ページには次のタブが表示されます。

- [概要 (Summary)]: 名前、説明、およびプランの編集やテストなどプランに対して実行可能なコマンドを含む、復旧プランの概要を示します。[概要 (summary)] タブはデフォルトです。
- [仮想マシン (Virtual Machines)]: この復旧プランで保護される仮想マシンを表示します。
- [復旧ステップ (Recovery Steps)]: 復旧プランのステップを一覧表示します。
- [履歴 (History)]: 復旧プランが実行されたかどうか、実行された日付、実行された期間、およびプランの結果を表示します。XML、HTML、または CSV 形式で結果のコピーをエクスポートするオプションを提供します。
- [権限 (Permissions)]: 復旧プランのメンテナンスが許可されているユーザーの一覧を表示します。

ナビゲーションペインで復旧プランを選択すると、次のコマンドが [概要 (Summary)] タブに表示されます。

- [復旧プランの編集 (Edit Recovery Plan)]: プラン名と説明、プランに含まれる保護グループ、仮想マシン応答時間、プランのテストで使用するネットワーク、復旧プランの一部としてサスペンドされる仮想マシンの変更を行います。

- [復旧プランの削除 (**Remove Recovery Plan**)] : 復旧プランを削除します。
- [復旧プランのテスト (**Test Recovery Plan**)] : 復旧プランのテストを実行します。
- [復旧プランの実行 (**Run Recovery Plan**)] : 復旧プランを実行します。

復旧プランの編集

プラン名と説明、プランに含まれる保護グループ、仮想マシン応答時間、プランのテストで使用するネットワーク、復旧プランの一部としてサスペンドされる仮想マシン、メッセージおよびコマンドを変更できます。

復旧プランを編集するには、次の条件が配備されている必要があります。

- VI クライアントは復旧サイトに接続されている必要があります。
- 復旧プラン管理者のロール。

復旧プランを編集するには

- 1 [概要 (**Summary**)] タブで、[復旧プランの編集 (**Remove Recovery Plan**)] をクリックします。
- 2 プラン名または説明を変更して [次へ (**Next**)] をクリックします。
- 3 必要に応じて復旧サイトに含める保護グループを変更し [次へ (**Next**)] をクリックします。
- 4 必要に応じて復旧プランの仮想マシンの応答時間を変更し [次へ (**Next**)] をクリックします。
- 5 プランのテスト用に最初に指定したネットワークを変更します。
変更を終えたら、[次へ (**Next**)] をクリックします。
- 6 復旧が発生または復旧テスト時にサスペンドさせるローカル仮想マシンを変更します。
- 7 [終了 (**Finish**)] をクリックします。

復旧プランは変更されました。インベントリで再びプランを選択すると、[概要 (**Summary**)] タブ、[履歴 (**History**)] タブ、および [復旧ステップ (**Recovery Steps**)] タブに変更が反映されています。

復旧プランのテスト

実際の復旧をシミュレートするテストを何度でも実行できます。テストを実行する場合、テスト復旧を実行して復旧プランを編集し、問題を修正することができます。SRMは、テストおよび実際の復旧時の両方で実行されるのと全く同じプランを実行しますが、次の例外があります。

- 復旧テストは保護サイトに接続せず、仮想マシンをシャットダウンしません。

- 復旧テストは、保護サイトと復旧サイトのインフラストラクチャが保護されるように、テスト ネットワークを作成します。テストが完了したら、テスト ネットワークは削除されます。このアクションにより、両方のサイトのインフラストラクチャが確実に保護されるようにします。しかしながら、実際のネットワークを選択して復旧をテストすることもできます。

復旧サイトの仮想マシンは、通常、ターゲット データストアから複製された復旧サイトのデータストアから開始され、本番環境から隔離されたストレージ インフラストラクチャに対してテストが確実に実行されるようにします。

復旧プランをテストするには、以下の条件が配備されている必要があります。

- VI クライアントは復旧サイトに接続されている必要があります。
- 復旧プラン管理者のロール。

復旧プランをテストするには

- 1 ナビゲーション バーでテストするプランを選択します。
- 2 [概要 (Summary)] タブで、[復旧プランのテスト (Test Recovery Plan)] をクリックします。
- 3 [続行 (Continue)] をクリックして復旧テストを続行します。

[最近のタスク (Recent Tasks)] 領域 (開いている場合) の、[名前 (Name)] フィールドに [テストモードで復旧プランを実行 (Run Test Mode Recovery Plan)] と表示され、[ステータス (Status)] フィールドに完了したパーセンテージが表示されます。

テストの一時停止、再開、またはキャンセル

復旧プランはいつでも一時停止、再開、またはキャンセルすることができます。テストを一時停止またはキャンセルした場合、新しいステップは開始されず、進行中のステップは次のルールに従います。

- パワーオンやハートビートの待機など、停止できないステップは、完了するまで実行してから、停止またはキャンセルを完了します。
- ストレージデバイスを追加または削除するステップは、キャンセルした場合はクリーンアップ操作によって、あるいは一時停止して再開する場合は後続のステップによって元に戻されます。

テストを一時停止またはキャンセルするのに必要な時間は、要求が行われた場合に進行中のステップのタイプおよび数によって異なります。テストを再開するのに必要な時間は、一時停止の要求が行われた場合に進行中のステップのタイプおよび数によって異なります。

復旧プランの実行

実際の復旧プランを実行すると、復旧サイト ネットワーク上の復旧サイトで仮想マシンが開始されます。このプロセスは簡単にあるいは自動で元に戻すことはできません。復旧プランを実行すると、仮想マシンおよび保護サイトと復旧サイトのインフラストラクチャが永久に変更されます。復旧プランを実行すると、次の変更が発生します。

- 復旧中に、保護サイトが復旧サイトに接続された場合、仮想マシンは保護サイトで適切にシャットダウンされます。
- サイト間の接続が失われると、SRM は保護サイトの保護仮想マシンに対して何のアクションも取りません。復旧サイトのデータストアでは、読み取り機能と書き込み機能が有効になっていて、SRM は、復旧プランのスタートアップの順番に従って復旧サイトの仮想マシンの起動を開始します。
- サイト間の接続が切断されて、保護サイトがダウンしている場合、仮想マシンはすでにシャットダウンの状態になっています。

復旧プランを実行するには、以下の条件が配備されている必要があります。

- VI クライアントは復旧サイトに接続されている必要があります。
- 復旧プラン管理者のロール。

復旧プランを実行するには

- 1 復旧サイトの [インベントリ (Inventory)] で実行するプランを選択します。
- 2 [概要 (Summary)] タブで、[復旧プランの実行 (Run Recovery Plan)] をクリックします。
- 3 確認して、[復旧プランの実行 (Run Recovery Plan)] をクリックします。

プランが実行されると、[復旧ステップ (Recovery Steps)] タブの各ステップのステータスが更新されます。

復旧プランの削除

レポートを削除すると SRM からプランが永久に削除されます。削除された後で復旧プランを取得することはできません。

復旧プランを削除するには、以下の条件が配備されている必要があります。

- VI クライアントは復旧サイトに接続されている必要があります。
- 復旧プラン管理者のロール。

復旧プランを削除するには

- 1 ナビゲーションバーで削除するプランを選択します。
- 2 [概要 (Summary)] タブで、[復旧プランの削除 (Remove Recovery Plan)] をクリックします。
- 3 [はい (Yes)] をクリックして確認し、プランを削除します。

復旧プランでの仮想マシンの設定

[仮想マシン (Virtual Machines)] タブでは、この復旧プランに含まれている仮想マシンを参照し、設定できます。

仮想マシンを復旧プランに設定するには、以下の条件が配備されている必要があります。

- VI クライアントは復旧サイトに接続されている必要があります。
- 復旧プラン管理者のロール。

プランで仮想マシン プロパティを編集するには

- 1 [仮想マシン (Virtual Machines)] タブで、[編集 (Edit)] をクリックします。
- 2 [参照 (Browse)] をクリックして使用可能なカスタマイズ仕様を表示します。
- 3 矢印をクリックして、仮想マシンに適用するカスタマイズプロパティを選択します。

このオプションを設定するには、復旧サイトで VI クライアントを使用してカスタマイズ仕様を作成する必要があります。仕様が設定されていないと、「使用可能なカスタマイズ仕様が見つかりません (No available Customization Specification found)」というメッセージが表示されます。

- 4 [OK] をクリックします。
- 5 デフォルトの復旧優先度を指定して、[次へ (Next)] をクリックします。

復旧優先度は仮想マシンのプロパティであり、復旧プランのプロパティではありません。仮想マシンの復旧優先度は復旧プランの一部になった後で変更することはできません。

- 6 この仮想マシンをパワーオンする前に実行する、メッセージまたはコマンドの追加、ステップの削除または順番変更をします。

[「メッセージおよびコマンド ステップの追加」 \(P.54\)](#) を参照してください。

- 7 [次へ (Next)] をクリックします。
- 8 この仮想マシンをパワーオンした後に実行するメッセージまたはコマンドの追加、ステップの削除または順番変更をします。

- 9 [終了 (**Finish**)] をクリックします。

復旧プランの表示

復旧プランを表示するには、災害対策用に推奨されるステップがリストされた [復旧ステップ (**Recovery Steps**)] タブをクリックします。いくつかのステップは、ツリー形式でサブステップが含まれています。

プラス記号 (+) をクリックしてサブステップを含むビューを展開します。高レベルのステップだけを表示させるにはマイナス記号 (-) をクリックします。

復旧ステップとサブステップの他に、その他の情報の列が表示されます。以下の情報が復旧プランに表示されます。いくつかのフィールドは、復旧プランがテストまたは実行されるまで空白のままです。

- 復旧ステップ：復旧時に実行されるステップおよびサブステップ
- ステータス：復旧プランがテストまたは実行されるまで空白のままです。ステップが正しく完了すると、[ステータス (**Status**)] カラムには [成功 (**Success**)] という用語が表示されます。
- タスク開始：プランがテストまたは実行されるとこのステップの開始日付と時刻が表示されます。
- タスク完了：プランがテストまたは実行されるとこのステップの完了日付/時刻が表示されます。
- モード：テストまたは実際の復旧時にステップが実行中であるかどうかを記します。[復旧 (**Recovery**)] は、復旧時にのみ実行されるステップを示します。テストが実行されている場合、「テスト」という用語が表示されてテストにのみ適用されます。

復旧プランに表示する情報カラムを選択するには

- 1 テキストバーを右クリックします。
- 2 そのカラムの参照をオフにするカラム名を選択解除します。

[復旧 (**Recovery**)] タブに、アイコンのツールバーが表示されます。復旧プランの編集やエクスポートなどのアクションのためのアイコンがあり、各アイコンの上にカーソルを置くとそれらの簡単な説明が表示されます。

復旧プランのステップをエクスポートするには

- 1 [復旧ステップ (**Recovery Steps**)] タブの [エクスポート (**Export**)] アイコンをクリックします。
- 2 選択したファイル名を使用してディレクトリにファイルを保存します。

レポートは、XML、.doc、XLW、HTML、および CSV 形式でエクスポートされます。

復旧プラン履歴の表示

復旧プランをテストまたは実行したら、情報が [履歴 (History)] タブに表示されます。

復旧プランを表示するには

- 1 [履歴 (History)] タブで、復旧プランを選択して [表示 (View)] をクリックします。
- 2 プランの閲覧を終えたら、Windows の [閉じる (Close)] ボタンをクリックします。

復旧履歴の結果をエクスポートする

[履歴 (History)] タブを使用して、復旧プランの結果をエクスポートします。

復旧プランをエクスポートするには

- 1 [履歴 (History)] タブで、エクスポートする復旧プランを選択して [エクスポート (Export)] アイコンをクリックします。
- 2 [ファイル名 (File name)] フィールドに復旧プランの名前を入力して、[保存 (Save)] をクリックします。
- 3 [名前をつけて保存 (Save As)] ダイアログボックスを閉じます。

カスタマイズ仕様の使用

SRM は、登録情報、タイムゾーン、管理者のパスワード、復旧プランの仮想マシンの IP アダプタのプロパティなど、VirtualCenter から継承したデフォルトの設定を使用します。カスタマイズ仕様を編集することによって、プラン内の仮想マシンの IP アダプタのプロパティを更新することができますが、その他のプロパティは更新できません。

仮想マシンにカスタマイズ仕様を適用するには、「[仮想マシン プロパティの設定](#)」(P.51) を参照してください。

カスタマイズ仕様を作成するには

- 1 VI クライアントで、[編集 (Edit)] > [カスタマイズ仕様 (Customization Specifications)] を選択します。
- 2 [新規 (New)] を選択します。
- 3 [ネットワーク (Network)] ページが表示されるまで [次へ (Next)] をクリックします。
- 4 ネットワーク設定を変更するには、[カスタム設定 (Custom settings)] を選択し、[次へ (Next)] をクリックします。
- 5 カスタマイズするネットワークを選択し、[カスタマイズ (Customize)] をクリックします。

- 6 ネットワーク設定に変更を行い、[OK] をクリックします。
- 7 [次へ (Next)] をクリックして [終了 (Finish)] をクリックします。
[カスタマイズ仕様マネージャ (Customization Specification Manager)] ページにスクリプトが表示され、保護サイトで使用できるようになりました。
- 8 [閉じる (Close)] ボックスをクリックします。

カスタマイズ仕様をインポートするには

- 1 [編集 (Edit)] > [カスタマイズ仕様 (Customization Specifications)] を選択します。
- 2 [インポート (Import)] を選択します。
- 3 インポートするスクリプトを参照し、[開く (Open)] をクリックします。

フェイルバック

VMware Site Recovery Manager (SRM) を使用したフェイルバックの管理は、計画済みのサーバ移行と同じように管理できる手動のプロセスです。SRM を使用すると、保護サイトで操作を再開する準備ができた後で、復旧サイトから保護サイトにサービスをフェイルバックできます。

注 フェイルバックを試行する前に、アレイベンダーのドキュメントを参照してください。すべてのアレイが必要な操作をサポートしているわけではありません。詳細については、VMware Web サイトを参照してください。

本章の内容は、次のとおりです。

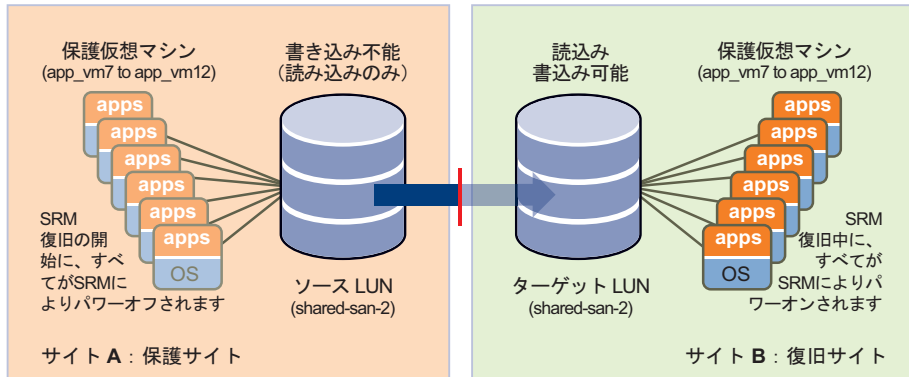
- 「フェイルバック シナリオ」 (P.71)
- 「その他のフェイルバックの考慮事項」 (P.77)

フェイルバック シナリオ

以下のステップでは、これらの仮想マシンがサイト B で復旧された後で SRM をサイト A でフェイルバック ツールとして使用するシナリオについて説明します。app_vm7 から app_vm12 までの (shared-san-2 という名前のデータストア グループによってホストされている) 6 つのマシンがサイト B からサイト A にフェイルバックします。

図 7-1 では、サイト A からサイト B でフェイルオーバーを実行した後のストレージ構成を図示しています。

図 7-1. 実際のフェイルオーバーを shared-san-2 データストアのサイト A から サイト B で実行した後のストレージ構成



このフェイルバック シナリオでは、サイト B からサイト A への正常なフェイルバックの手順について説明します。これには、サイト B からのフェイルバックの後でサイト A の再保護を行うための手順も含まれています。

注 保護サイトに保護を有効にするライセンス キー (SRM_PROTECTED_HOST) を購入していない場合は、フェイルバックを実行する前に、そのキーを復旧サイトから保護サイトに転送する必要があります。詳細については、「[SRM ライセンス](#)」(P.23) を参照してください。

以下の用語および略語が使用されます。

- サイト A : 元の保護サイト。
- サイト B : 元の復旧サイト。
- PG 1 : サイト A で定義された元の保護グループ。
- PG 2 : サイト B からサイト A へのフェイルバックを容易にするためにサイト B で定義された新しい保護グループ。
- PG 3 : サイト B へのフェイルオーバーを容易にするためにサイト A で定義された新しい保護グループ。PG 3 は基本的に PG 1 と同じ保護グループです。
- RP 1 : サイト B で定義された元の復旧プラン。
- RP 2 : サイト B からサイト A へのフェイルバックを容易にするためにサイト A で定義された新しい復旧プラン。
- ソース LUN : 代替データセンターに複製された VMFS データストア。
- ターゲット LUN : 代替データセンターの結果データストア。

- クローン LUN：フェイルオーバーのテストの間にもみ使用されるターゲット LUN のクローン。

このシナリオでは、復旧サイトから元の保護サイトに戻ってフェイルバックを実行するための一般的な手順について説明します。

これらのステップを追跡する方法については、[付録 B、「以下のチェックリストを使用してフェイルバックの手順を実行しながら追跡します。」](#) (P. 87) を参照してください。

フェイルバックの準備を行うには

- 1 フェイルオーバー用にサイト B に復旧されたすべてのサイト B の仮想マシンをシャットダウンします。
- 2 サイト B に復旧されたすべての保護仮想マシンのリストを作成します。後のステップでこの情報が必要になります。
- 3 VirtualCenter データストア ブラウザで、サイト B で保護グループの作成中に作成された仮想マシン構成ファイルが含まれているサイト A のディレクトリをクリーンアップします。

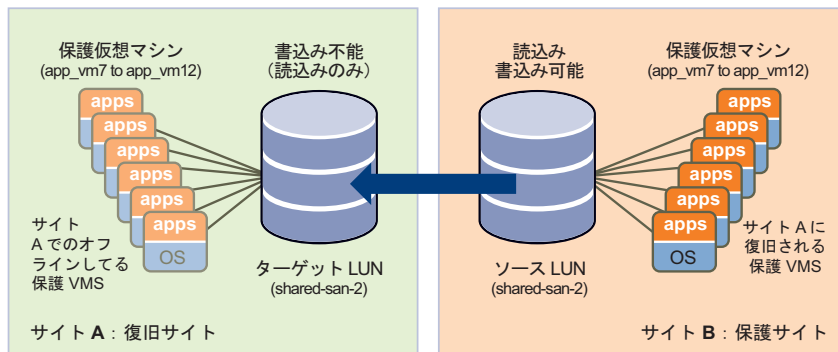


注意 これらの仮想マシンを保持しているデータストアはプレースホルダ マシンに使用されます。実際の仮想マシンではこれらのファイルを削除しないでください。

これは、サイト A - PG 1 で元の保護グループの作成中に選択された場所です。具体的には、.vmsd、.vmx、および .vmxf ファイルを削除します。このクリーンアップ手順の間の参照として上記の[手順 2](#)で作成したリストを使用してください。

ソース LUN がサイト B になるようにストレージ構成の変更を完了するには

ストレージ チームと協力してストレージ構成の変更を完了し、ソース LUN がサイト B に関連付けられるようにしてターゲット LUN がサイト A に関連付けられるようにします。



サイト A のインベントリから期限切れの保護された仮想マシンを削除するには

- 1 サイト A で、すべてのホストでホスト バス アダプタ (HBA) を再スキャンします。これにより、割り当てられている保護グループと同様に、インベントリに無効なマシンとして表示されるため、保護仮想マシンを簡単に識別することができます。
- 2 サイト A で、復旧プランから PG 2 をリムーブし、次に PG 2 を削除します。
- 3 サイト A でサイト B に復旧されたすべての保護仮想マシンを選択します。選択した仮想マシンを右クリックして [**インベントリから削除 (Remove from Inventory)**] を選択してサイト A のインベントリからハイライトされた保護仮想マシンを削除します。

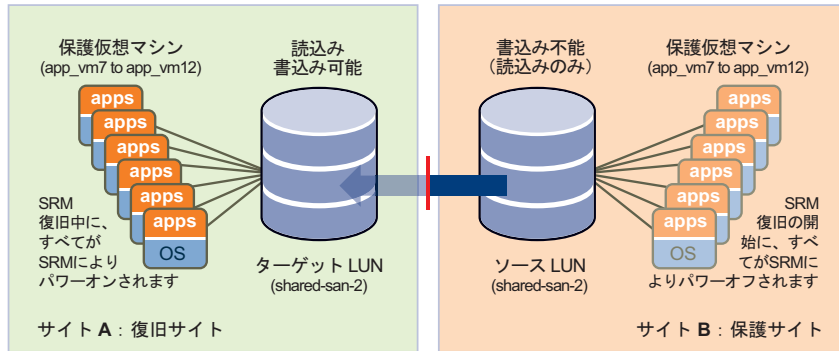
サイト B からサイト A にフェイルバックするには

- 1 サイト B でアレイ マネージャの設定ウィザードを完了します。現在ソース LUN はサイト B に設定されていて、ターゲット LUN はサイト A に設定されています。これで、復旧サイトのアレイ マネージャは保護サイトのアレイ マネージャになり、保護サイトのアレイ マネージャは復旧サイトのアレイ マネージャになります。
- 2 サイト B でインベントリ マッピングを設定します。

これらのインベントリ環境設定は、フェイルバック後にサイト A で再開始されるときに保護仮想マシンに割り当てられます。
- 3 サイト B で、PG 2 をサイト A へのフェイルバックに設定します。
- 4 サイト A で、RP 2 を設定します。

サイト A で指定された仮想マシンを保護するためにサイト B で作成した RP 1 を削除しないでください。
- 5 [**テスト (Test)**] をクリックし、保護サイトのターゲット LUN のクローンまたはスナップショットを使用して復旧プランをテストします。テストが正常に行われた場合は、[**実行 (Run)**] をクリックして RP 2 の実際の復旧を実行します。

以下の図に RP 2 に対する復旧が完了した後のストレージ構成を示します。



二次災害の場合に備えてフェイルオーバー用に **サイト A** を準備するには

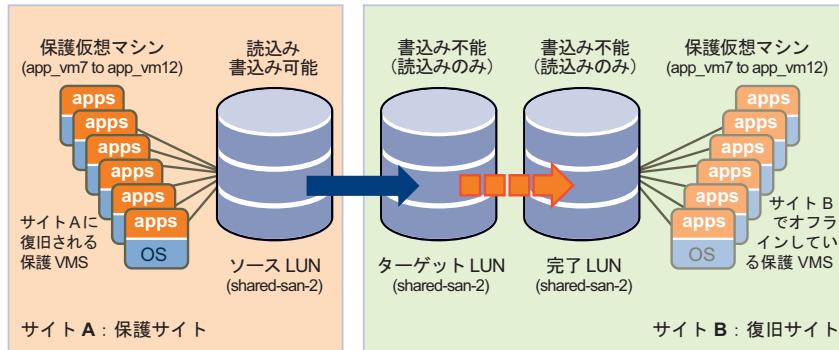
- 1 「[サイト B からサイト A にフェイルバックするには](#)」で実行された SRM 復旧操作の間にサイト B からフェイルバックされたサイト A のすべての保護仮想マシンをシャットダウンします。

シャットダウンにより、アレイのレプリケーション方向を交換する前に、LUN のすべての I/O が停止されていることを確認できます。

- 2 サイト B で保護グループの作成中に作成された仮想マシンの設定ファイルが含まれているサイト A でディレクトリのクリーンアップを実行します。（「[フェイルバックの準備を行うには](#)」というタイトルの[手順 3](#)を参照してください。）
- 3 **VirtualCenter** データストア ブラウザで、サイト A で保護グループの作成中に作成された仮想マシン構成ファイルが含まれているサイト B のディレクトリをクリーンアップします。

ソース LUN がサイト A になるようにストレージ構成の変更を完了するには

ストレージチームと協力して 2 番目のストレージ構成の変更を完了します。以下の図で示すように、ソース LUN をサイト A と再度関連付けて、ターゲット LUN をサイト B およびクローン LUN と再度関連付けます。



これで、ストレージ構成は、SRM のセットアップ前の元の設定に戻りました。ストレージアレイベンダーは、ターゲット LUN からクローン LUN のデータ同期化方法（周期的または連続的な同期化のスナップショット）を決定します。シミュレートされたフェイルオーバーが SRM のテスト オプションを使用して開始された場合、最終的なデータ同期化はターゲット LUN からクローン LUN で実行されます。

二次災害の場合に備えてフェイルオーバー用にサイト B を準備するには

- 1 サイト B で、すべてのホストでホスト バス アダプタ (HBA) を再スキャンします。これにより、割り当てられている保護グループと同様に、インベントリに無効なマシンとして表示されるため、保護仮想マシンを簡単に識別することができます。
- 2 サイト B で、復旧プランから PG 2 をリムーブし、次に PG 2 を削除します。
- 3 サイト B で、サイト B のインベントリからサイト A に復旧されたすべての保護仮想マシンを削除します。このシナリオでは、これは **app_vm7 ~ app_vm12** です。（「[サイト A のインベントリから期限切れの保護された仮想マシンを削除するには](#)」を参照してください。）
- 4 保護仮想マシンにサイト A で PG 3 を作成します。

PG 3 は、元は RP 1 に関連付けられていた保護グループで、復旧モードで実行され、サイト B で保護仮想マシンをスタートアップさせる結果となった復旧プラン、PG 1 と同一である必要があります。

5 サイト A の保護グループをサイト B の RP 1 と再度関連付けます。

RP 2 を削除する必要はありません（サイト A からサイト B への復旧を容易にするためにサイト A で作成された復旧プラン）。

サイト A で保護仮想マシンの再保護を完了しました。RP 1 に対するフェイルオーバーテストを実行し、サイト A が保護されていて別の障害が発生した場合に必要なサイト B の復旧の準備ができているか確認することをお勧めします。

その他のフェイルバックの考慮事項

フェイルバック中に考慮すべき問題がいくつかあります。

- サイト ペアリング：サイト A およびサイト B は 1 回のみペアリングする必要があります。SRM ではペアリングされたサイト間で双方向関係を保持します。
- DNS アップデート：サイト A とサイト B が拡張 VLAN によって結合されていない場合は、手動で DNS アップデートを指定する必要があります。というのも、仮想マシンがサイト A とサイト B の間で移動し、その IP アドレスが新しいネットワークに適用するように変更されているためです。

アラートと監視

この章では、SRM (Site Recovery Manager) イベントおよびアラーム通知の設定オプションについて説明します。本章の内容は、次のとおりです。

- 「SRM アラーム」 (P.79)
- 「SRM アラーム トリガについて」 (P.80)
- 「SRM アラーム設定を編集する」 (P.80)
- 「E メールによるアラーム通知の準備」 (P.82)

SRM アラーム

SRM アラームは、SRM によって上げられた選択済みのイベントに応答して発生する通知です。Site Recovery が VI クライアントで選択された場合、これらのイベントトリガアラームが使用可能となり、設定できます。SRM イベントに特有のアラームは、SRM のインストール時に定義されます。

SRM アラームでは E メールで通知メッセージを送信します。SRM アラームを編集する前に、E メールメッセージアラーム通知をサポートする VirtualCenter サーバの設定方法の詳細については、「E メールによるアラーム通知の準備」(P.82) を参照してください。

[Site Recovery] ビューの [アラーム (Alarms)] タブには、指定されたイベントで有効化されている SRM のアラームのリストが表示されます。これらのアラームは SRM に固有で、VirtualCenter サーバからは利用できません。(SRM アラームは、Virtual Center のイベントログに表示されている場合でも、VI クライアントの [トリガアラーム (Triggered Alarms)] ペインには表示されません。)

注 SRM アラームはどのようなイベントにも 5 分ごとに 1 回以上はトリガしません。5 分間の間の同じイベントの複数のインスタンスに対しては 1 つのアラームのみをトリガします。

SRM アラーム トリガについて

アラーム トリガにはいくつかの形式があります。

- 以下のような問題が発生すると、SRM は VirtualCenter サーバのアラームに関連付けることのできるイベントを生成します。
 - SRM サーバで問題が発生すると、SNMP トラップ、E メールなどが生成されます。
 - アラームは、SRM プラグインから SRM イベントに関連付けられます。
- 保護サイトまたは復旧サイトで、SRM サーバまたは VirtualCenter サーバに以下のような障害が発生すると、VirtualCenter アラームに関連付けることのできるイベントを生成します。
 - ローカル サイトでの問題（たとえばリソース制約など）。
 - リモート サイトでの問題（たとえば SRM または VirtualCenter ホストをリモート サイトで ping できなかったなど）。リモート サイトの障害は SRM イベントに反映され、復旧をトリガしません。復旧は手動で起動する必要があります。
 - ディスク容量が不足している。
 - CPU の制限を越えている。
 - メモリが不足している。
 - リモート サイトが応答しない。
 - リモート サイトの VirtualCenter サーバまたは SRM サーバに障害が発生している。
 - 復旧テストが開始、正常に終了、失敗、またはキャンセルされた。
 - 仮想マシンの復旧が開始、終了、成功、失敗、または警告を出した。

以下にアラームの通知方法を示します。

- 通知 E メールメッセージを送信する
- 通知トラップを送信する
- スクリプトを実行する

SRM アラーム設定を編集する

SRM アラームを変更することができます。簡単な変更は、アラームを有効または無効にすることです。アラームが無効な場合、アラーム リスト アイコンに X が表示されます。

SRM アラームを編集するには、以下の条件が設定されている必要があります。

- VI クライアントは保護サイトまたは復旧サイトに接続されている必要があります。
- 必要な最小権限は [アラームの変更 (Modify Alarm)] (アラームの権限) です。

アラームを編集するには

- 1 VI クライアントを使用して、保護サイトの VirtualCenter サーバにログインします。
- 2 VI クライアントのツールバーで [Site Recovery] アイコンをクリックします。
- 3 [アラーム (Alarms)] タブをクリックします。
- 4 イベントを右クリックして、[設定の編集 (Edit Settings)] を選択します。
- 5 [アクション (Action)] をクリックしてイベントがトリガされたときに取られるアクションを選択し、関連する情報を指定します。

オプション	説明
通知 E メールを送信する	<p>[値(Value)] フィールドに通知受信者の E メールアドレスを入力します。SMTP で E メールを送信します。SMTP は、E メール送信時に準備ができていない必要があります。</p> <p>E メール メッセージの件名と本文テキストは、VirtualCenter サーバによって生成されます。[宛先 (To list)] (受信者) だけはユーザーが入力する必要があります。メッセージが送信される E メール ドレスを指定します。</p> <p>VirtualCenter サーバの E メール メッセージの SMTP アラーム通知の準備の詳細については、「VMware Infrastructure Basic System Administration」を参照してください。</p>
通知トラップを送信する	<p>VirtualCenter サーバは、デフォルトの SNMP 通知の受信者です。SNMP トラップ ビューアは、送信トラップを閲覧する必要があります。</p> <p>VirtualCenter サーバホストでは、SNMP トラップを受信するように設定する必要があります。</p> <p>VirtualCenter サーバの E メール メッセージの SNMP アラーム、SMTP アラーム通知の準備の詳細については、「VMware Infrastructure Basic System Administration」を参照してください。</p>
スクリプトを実行する	<p>スクリプトが .exe ファイルの場合は、そのスクリプトを実行するためのパスを指定します。スクリプトが .bat ファイルの場合は、<code>c:\windows\system32\cmd.exe</code> コマンドの引数としてそのスクリプトのパスを指定します。たとえば、<code>c:\alarmscript.bat</code> にあるスクリプトを実行するには、スクリプトのパスを「<code>c:\windows\system32\cmd.exe /c c:\alarmscript.cmd</code>」と指定します。</p>

- 6 アラームを完了するには、[OK] をクリックします。
- 7 VirtualCenter によってアラームの設定が確認され、選択したオブジェクトのアラーム リストにアラームが追加されます。

E メールによるアラーム通知の準備

E メール メッセージを使用してアラーム通知を送信するには、以下を行う必要があります。

- SMTP サーバおよび E メール メッセージ アドレス情報を定義します。
- E メール通知を受信するユーザーの E メール アドレスを指定します。

E メール メッセージのアラーム通知を準備するには、以下の条件が設定されている必要があります。

- VI クライアントは VirtualCenter サーバに接続されている必要があります。
- 必要な最小権限は、[設定 (Settings)] (グローバル権限) です。

SMTP サーバおよび E メール メッセージ アドレス情報を定義するには

- 1 VI クライアントで、[管理 (Administration)] > [VirtualCenter Management Server の構成 (VirtualCenter Management Server Configuration)] を選択します。
- 2 ナビゲーション リストで [メール (Mail)] をクリックします。
- 3 E メール メッセージ通知の、SMTP サーバおよび SMTP ポートを以下のように設定します。
 - SMTP サーバ - E メール メッセージの送信に使用する SMTP ゲートウェイの、ホスト名または IP アドレス。
 - 送信者アカウント - たとえば、srm_alarms@example.com などの送信者の E メールアドレス。
- 4 [OK] をクリックします。
- 5 SRM ビューで、[アラーム (Alarms)] タブをクリックします。
- 6 アラームを選択してメール通知イベントを追加します。
- 7 アラームを右クリックして、[設定の編集 (Edit Settings)] を選択します。
- 8 [アクション (Actions)] タブを選択します。
- 9 [追加 (Add)] をクリックします。
- 10 [通知 E メールを送信する (Send a notification email)] アクションのタイプを変更します。
- 11 通知を送信する E メール アドレスに対するアクションの値を設定します。

保護サイトと復旧サイトの変更

SRM は、保護サイトと復旧サイトで VirtualCenter サーバへの変更を監視して処理します。

本章の内容は、次のとおりです。

- 「VirtualCenter サーバへの変更」 (P.83)
- 「保護サイトでの変更」 (P.83)
- 「復旧サイトへの変更」 (P.84)

VirtualCenter サーバへの変更

SRM サーバは、仮想マシンやネットワークなどの特定のインベントリ オブジェクトの使用可能性に依存しています。VirtualCenter サーバに変更を加えることは SRM に影響を与える可能性があります。

VirtualCenter サーバインベントリにおけるオブジェクトの名前変更および移動は、テストあるいは復旧時にリソースがアクセス不能にならないかぎり SRM への影響はありません。

保護サイトでの変更

SRM では、作業を中断することなく保護サイトで以下の変更をサポートしています。

- デバイスの追加、変更、削除あるいは仮想マシンの移動など、保護されている仮想マシンの変更。
仮想マシンがすでに保護グループに属している場合、保護サイトで仮想マシンのメモリ サイズを変更しても復旧サイトには反映されません。
- 保護されている仮想マシンの削除。
- インベントリ マッピングが存在するオブジェクトの削除。

SRM では保護サイトと復旧サイトで SRM の再インストールが必要です。

- VirtualCenter サーバを保護サイトで再インストールし、VirtualCenter データベースを再初期化します。
- SRM を保護サイトで再インストールし、SRM データベースを再初期化します。

復旧サイトへの変更

SRM では、作業を中断することなく復旧サイトで以下の変更をサポートしています。

- 復旧仮想マシンの削除。
- 復旧仮想マシンを別のフォルダ、リソース プールまたはネットワークに移動。
- インベントリ マッピングが存在するオブジェクトの削除。
- 復旧サイトでの VirtualCenter サーバの再インストール (VirtualCenter データベースの再初期化)。

SRM では、SRM が復旧サイトで再インストールされている場合は、保護サイトと復旧サイトで SRM を再インストールする必要があります (SRM データベースの再初期化)。

プリンストール チェックリスト



以下のチェックリストを使用して、ストレージプラットフォームが SRM との統合の準備ができていないかどうかを確認することができます。

説明	保護	復旧
VMware Web サイトから SRM ソフトウェア、ストレージレプリケーションアダプタ (SRA)、および製品情報をダウンロードします。		
Microsoft SQL Server または Oracle Database サーバのサポートされているリリースが設定されていて使用する準備ができていないことを確認します。		
VirtualCenter サーバにデータベース インスタンスを作成します。		
db 所有者の VirtualCenter インスタンスにデータベース ユーザーを作成して表の権限を作成します。		
VirtualCenter データベースに DSN を作成します。		
VirtualCenter サーバの互換バージョンがインストールされていて使用する準備ができていないことを確認します。		
VI クライアントを使用して VirtualCenter サーバへのアクセスを設定します。		
ESX のサポートされたバージョンがインストールされていて VirtualCenter に統合されていることを確認します。ESX には、VMFS データストアとして設定されていて、復旧サイトの対応する SAN にデータ複製用に設定されている SAN の LUN へのアクセス権が必要です。		

説明	保護	復旧
SRM にデータベース インスタンスを作成します。		
SRM データベース インスタンスに適切な権限のデータベース ユーザーを作成します。		
SRM データベースに DSN を作成します。		
SRM をインストールする物理システムまたは仮想システムを特定します。		
SRA を SRM ホストのアレイ プロバイダからインストールします。		

フェイルバック チェックリスト

B

以下のチェックリストを使用してフェイルバックの手順を実行しながら追跡します。

フェイルバックの準備

- サイト B 保護仮想マシンをパワーダウンします。
- サイト B サイト B に復旧された保護仮想マシンのリストを作成します。
- サイト B 保護されたマシンをサイト A の保護グループに割り当てたときに作成された仮想マシン構成ファイルに含まれているサイト B のディレクトリをクリーンアップします。

ソース LUN がサイト B になるようにストレージ構成の変更を完了する

- スト レージ ストレージ チームと協力してストレージ構成の変更を完了し、ソース LUN がサイト B に関連付けられるようにしてターゲット LUN がサイト A に関連付けられるようにします。

サイト A のインベントリから期限切れの保護仮想マシンを削除する

- サイト A すべてのホストでホストバス アダプタ (HBA) を再スキャンします。
- サイト A サイト A で VirtualCenter インスタンスに接続し、元の保護グループ (PG 2) を削除します。
- サイト A サイト A のインベントリからサイト B に復旧されたすべての保護仮想マシンを削除します。

サイト B からサイト A へのフェイルバック

- サイト B サイト B でアレイ マネージャの設定ウィザードを完了します。現在ソース LUN はサイト B に設定されていて、ターゲット LUN はサイト A に設定されています。
- サイト B インベントリ環境設定をサイト B に設定します。これらは、フェイルバックの後でサイト A で再起動されるときに保護仮想マシンに割り当てられるインベントリの環境設定です。

- _____ サイト B サイト B の VirtualCenter インスタンスに接続して PG 2 を設定します。
- _____ サイト A サイト A の VirtualCenter インスタンスに接続して RP 2 を設定します。
- _____ サイト A RP 2 に対して復旧を実行します。

二次災害の場合に備えてフェイルオーバー用に サイト A を準備する

- _____ サイト A 前の手順でサイト B からフェイルバックしたサイト A の保護仮想マシンをシャットダウンします。
- _____ サイト A サイト B で保護グループの作成中に作成された仮想マシン構成ファイルが含まれているサイト A のディレクトリをクリーンアップします。

ソース LUN がサイト A になるようにストレージ構成の変更を完了する

- _____ ストレージ ストレージ チームと協力して 2 つ目のストレージ構成の変更を完了し、ソース LUN が再度サイト A に関連付けられるようにしてターゲット LUN およびクローン LUN がサイト B に関連付けられるようにします。

二次災害の場合に備えてフェイルオーバー用に サイト B を準備する

- _____ サイト B すべてのホストでホストバス アダプタ (HBA) を再スキャンします。
- _____ サイト B サイト B の VirtualCenter インスタンスに接続して PG 2 を削除します。
- _____ サイト B サイト B の VirtualCenter インスタンスに接続してサイト B ですべての保護仮想マシンを削除します。これらの仮想マシンはサイト A に復旧されています。
- _____ サイト A 保護仮想マシンにサイト A で PG 3 を作成します。
- _____ サイト B PG 3 (サイト A のステップ 18 から) をサイト B で RP 1 と再度関連付けます。
- _____ サイト B RP 1 に対してテストのフェイルオーバーを実行し、サイト A が再度保護されていることを確認します。

srm-config コマンドを使用して SRM サーバ接続を修復する



srm-config コマンドは、SRM サーバとそれをサポートする VirtualCenter サーバとの間にネットワーク接続を設定します。管理者は、VirtualCenter サーバまたは SRM サーバの IP アドレスが変更された場合、あるいは認証情報ベースの認証に使用されるユーザー ID またはパスワードが変更された場合に、このコマンドを使用して SRM サーバ接続を修復することができます。

注 ここに説明されている手順のいずれかを完了したら、「[保護サイトと復旧サイトの接続](#)」(P. 34) の説明に従ってサイトのペアを再設定する必要があります。

SRM サーバの IP アドレスが変更された後で接続を修復する

- 1 SRM サーバ ホストにログインして Windows コマンド シェルを開始します。
- 2 C:\Program Files\VMware\VMware Site Recovery Manager\config\extension.xml ファイルをテキスト エディタで開きます。
- 3 開いているファイルで、<url> タグを指定し、そのコンテンツを新しい IP アドレスと SRM サーバのポートに変更します。

```
<config>
  <extension>
    <key></key>
    <version></version>
    <description></description>
    <servers>
      <server>
        <url>http://10.17.186.120:8095</url>
```

- 4 ディレクトリを C:\Program Files\VMware\VMware Site Recovery Manager\bin に変更します。
- 5 次のコマンドを実行して拡張登録を更新します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>srms-config.exe -cmd  
updateext -cfg ..\config\vmware-dr.xml -extcfg ..\config\extension.xml
```

Virtual Center サーバの IP アドレスが変更された後で接続を修復する

- 1 SRM サーバ ホストにログインして Windows コマンド シェルを開始します。
- 2 ディレクトリを C:\Program Files\VMware\VMware Site Recovery Manager\bin に変更します。
- 3 次のコマンドを実行します。ここで、<vc-ip-addr> は Virtual Center ホストの IP アドレスです。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>srms-config.exe -cmd  
updatevc -cfg ..\config\vmware-dr.xml -vc <vc-ip-addr>
```

証明書が信頼されなかったことを示すエラーをコマンドが返した場合は、次のコマンドを実行します。ここで、<vc-ip-addr> は Virtual Center ホストの IP アドレスで、<thumbprint-string> はエラー メッセージで返された指紋の文字列です。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>srms-config.exe -cmd  
updatevc -cfg ..\config\vmware-dr.xml -vc <vc-ip-addr> -thumbprint <thumbprint-string>
```

ユーザー ID またはパスワードが変更された場合に認証情報ベースの認証を再初期化する

- 1 SRM サーバ ホストにログインして Windows コマンド シェルを開始します。
- 2 ディレクトリを C:\Program Files\VMware\VMware Site Recovery Manager\bin に変更します。
- 3 次のコマンドを実行してユーザー ID とパスワードを更新します。プロンプトが表示された場合は、コマンド行に新しい <userID> とパスワードを入力します。

```
C:\Program Files\VMware\VMware Site Recovery Manager\bin>srms-config.exe -cmd  
updateuser -cfg ..\config\vmware-dr.xml -u <userID>
```

ページング ファイルおよび他の一時データの複製を



SRM では、Windows ページング ファイルまたは仮想マシンのスワップファイルなどの一時データを複製することができますが、それらのデータは複製する必要はありません。それらのデータの複製を防止することで、ネットワーク帯域幅を不必要な消費しないようにします。

スワップファイルに複製されなかったデータストアを指定する

各仮想マシンにはスワップファイルが必要ですが、通常は他の仮想マシンのファイルと同じデータストアに作成されます。SRM を使用すると、このデータストアは複製されます。スワップファイルが複製されないようにするには、それらを複製されないデータストアに作成します。この手順は、保護サイトと復旧サイトの両方で、すべての保護クラスタに実行する必要があります。詳細については、VMware Infrastructure ドキュメントを参照してください。

複製されないデータストア (ESX 3.5) にスワップファイルを作成するには

- 1 VI クライアントで、ESX クラスタを右クリックして [設定の編集 (Edit Settings)] をクリックします。
- 2 クラスタの [設定 (Settings)] ウィンドウで、[スワップファイルの場所 (Swapfile Location)] をクリックして [ホストによって指定されたデータストアにスワップファイルを保存する (Store the swapfile in the datastore specified by the host)] を選択し、[OK] をクリックします。
- 3 クラスタ内の各仮想マシンの場合は、
 - a [構成 (Configuration)] タブをクリックします。
 - b [スワップファイルの場所 (Swapfile location)] 行で、[編集 (Edit)] をクリックします。
 - c [仮想マシンのスワップファイルの場所 (Virtual Machine Swapfile Location)] ウィンドウで、複製されないデータストアを選択して [OK] をクリックします。

複製されないデータストア (ESX 3.0.2) にスワップファイルを作成するには

- 1 選択したクラスタで、仮想マシンを選択してシャットダウンします。
- 2 仮想マシンの .vmx ファイルのバックアップ コピーを作成します。
- 3 .vmx ファイルを編集して `sched.swap.dir` パラメータの値を変更し、保護サイトで複製されないデータストアのパス名を指定します。
このパス名を持つデータストアは復旧サイトにも存在するはずですが、存在しない場合は、仮想マシンは復旧サイトでパワーオンできません。
- 4 `vmx` ファイルを編集して `sched.swap.derivedName` 行を削除します。
- 5 修正された .vmx ファイルを保存します。
- 6 仮想マシンをパワーオンします。
- 7 クラスタ内の各仮想マシンで手順を繰り返します。

ページング ファイル ストレージに複製されない仮想ディスクを作成する

デフォルトの構成では、Windows はページング ファイルをシステム ディスク (通常は C:) に作成します。複製データストアを使用する場合は、この場所に作成されたページング ファイルは常に複製されます。ページング ファイルを複製しないようにするには、複製されないデータストアに仮想ディスク (.vmdk ファイル) を作成し、保護グループの各仮想マシンで、そのディスクにページング ファイルが作成されるように Windows を構成します。SRM は、このようにして設定されたすべての仮想マシンが少なくとも 1 つの複製されない仮想ディスク (ページング ファイル ディスク) に依存していることを検出し、その仮想マシンをその保護グループから削除します。復旧した仮想マシンを使用するように復旧サイトでその仮想ディスク ファイルのコピーを明示的に指定する必要があります。

保護グループ内の各仮想マシンでのこの手順の繰り返しを単純化するには、仮想ディスク ファイルのテンプレートを作成して複製し、両方のサイトで仮想マシンに複製されないページング ファイル ディスクを指定します。

仮想マシンに複製されないページング ファイル ストレージを使用するように強制するには

- 1 保護サイトで、一時仮想マシンを作成します。
- 2 一時仮想マシンで、新しいディスクを作成します。
ディスク ファイルを通常仮想マシンのテンプレートを保存する場所に保存します。
- 3 一時仮想マシンをパワーオンし、新しいディスクにパーティションを作成してフォーマットします。
- 4 新しいディスクを一時仮想マシンから切断します。
- 5 復旧サイトでテンプレート ディスクをテンプレート フォルダにコピーします。

.vmdk ファイルおよびそのフラットの対（たとえば、pagedisk.vmdk および pagedisk-flat.vmdk）をコピーする必要があります。

- 6 保護サイトで、保護グループ内の仮想マシンの場合は、
 - a vmkfstools コマンドを使用して複製されないデータストアにテンプレート ディスクのクローンを作成します。
 - b VI クライアントを使用して複製したディスクを仮想マシンに接続します。
 - c 仮想マシンをパワーオンしてドライブ文字を複製したディスクに割り当てます。
 - d 複製した仮想ディスクにページング ファイルが作成されるように仮想マシンを設定します。
 - e 仮想マシンをシャットダウンして再開始し、ページング ファイルが新しい場所（複製した仮想ディスク）に書き込まれるようにします。
システム ディスクから古い使用されていないページング ファイルを削除できます。
 - f vmkfstools コマンドを使用して手順 5 にコピーしたテンプレートを復旧サイトで複製されないデータストアの .vmdk ファイルに複製します。
 - g VI クライアントを使用して仮想マシンが含まれている保護グループを表示します。
仮想マシンは複製されないディスクをページング ファイルに使用するため、SRM は仮想マシンが複製された LUN にファイルがバックアップされていない 1 つまたは複数のデバイスを使用していることを通知します。その後、この構成問題が解決されるまで、仮想マシンを保護グループから削除します。
 - h VI クライアントで、[この VM にストレージを設定する (Configure Storage for this VM)] ページを使用してページング ファイルディスクのストレージを手順 f で複製した .vmdk ファイルに割り当てます。
保護サイトで複製されないディスクを使用するように仮想マシンを設定したら、SRM は仮想マシンのストレージが設定されているとみなし、保護グループに戻します。

保護サイトで行った変更が復旧サイトで複製されたら、復旧プランのテストを実行して復旧された仮想マシンが複製されないページング ファイルを使用していることを確認することができます。

用語集

アレイベース レプリケーション

仮想マシンのレプリケーションで、仮想マシンの内部、VMkernel、あるいはサーバ ビス コンソールからではなく、ストレージ サブシステム自身によって管理および実行されます。

フェイルバック

システム障害によってコンピュータ サーバ、システム、ネットワークが自動的にスタンバイ用のサーバ、システムまたはネットワークに切り替えられた後、システムを元の状態に戻すプロセス。

フェイルオーバー

災害が宣言された後、保護サイトの代わりに復旧サイトで操作を引き継ぐときに発生するイベント。

インベントリ マッピング

保護サイト上のリソース プール、ネットワーク、および仮想マシン フォルダを復旧サイトの宛先カウンターパートにマッピングすること。

LUN (logical unit number)

ストレージアレイでのディスク ボリュームの識別子。

保護サイト

復旧サイトにレプリケートされるデータ元の仮想マシンが格納されているデータセンター。

保護グループ

テストおよび復旧の際に、一緒にフェイルオーバーされる仮想マシンのグループ。

復旧プラン

プランで定義されている優先度の順番に従って、指定された保護グループの保護された仮想マシンを復旧するために必要な手順。

復旧サイト

保護サイトが使用できない間に代わって業務を実行する復旧仮想マシンが含まれているデータセンター。

復旧仮想マシン

保護サイトからレプリケートされた仮想マシンを表す保護仮想マシンを示すプロセスホルダ。

ストレージレプリケーションアダプタ (SRA)

ストレージデバイスと Site Recovery Manager を確実に統合するためのストレージベンダから提供されるソフトウェア。これらのベンダ固有のスクリプトは、アレイ検出、レプリケートされた LUN 検出、テストフェイルオーバー、および実際のフェイルオーバーをサポートします。

ストレージアレイ

複数のディスク ドライブを含むストレージ システム。

索引

A

- API リスナ ポート
 - HTTP **28**
 - SOAP **28**

D

- DNS アップデート **77**

H

- HTTP ポート **28**

L

- LUN
 - クローン **76**
 - ソース LUN **73**
 - ターゲット LUN **73**
 - マスキングおよびゾーニング **20**
 - レプリケーションの確認 **13**

M

- Microsoft .NET 2.0 Framework **21**

P

- PKCS#12 証明書ファイル **27**

S

- SMTP サーバ **82**
- SMTP ポート **82**
- SNMP トラップ **81**
- SOAP
 - ポート **28**
- SRM
 - インストール手順 **15**

環境 **12**

- 使用の要件 **11**

SRM アーキテクチャ コンポーネント

- ESX サーバ **12**
- Oracle または SQL データベース **12**

SAN **13**

- SRM サーバ **12**
- VirtualCenter Server **12**
- VMware ファイル システム (VMFS) **13**

ライセンス サーバ **12**

SRM の機能 **10**

- CPU およびメモリのクオリティ **11**
- インスタント アップデート **11**
- 応答準備 **10**
- 監視とアラート **11**
- ネットワーク再構成 **10**
- 無停止の変更 **10**
- 予測可能な管理 **11**
- レバレッジドストレージ **10**

SRM バルク挿入機能 **23**

- デフォルトのファイルの場所 **23**

V

VI Client

- SRM の管理に使用 **33**
- から SRM にログインする **33**

VMFS (Virtual Machine File System) **13**

VMware Infrastructure

- Distributed Resource Scheduler **10**
- SRM をサポートする方法 **9**

VLAN と SRM テスト 10

カプセル化 9

監査能力 10

共有ストレージ 9

ハードウェアからの独立 10

ハードウェア リパーバシング 10

変更管理 10

リソース プール 10

あ

アラーム

E メール メッセージの SMTP 通知
の前提条件 82

通知 79

定義済み 79

トリガするイベント 80

編集する 81

編集の前提条件 81

メッセージ アドレス情報の定義 82

アラームのトリガ イベント 80

アレイ スクリプト 45

アレイ マネージャ

修復 49

い

インストール

SRM に必要なオペレーティング シ
ステム 20

SRM プラグインに必要なオペレー
ティング システム 21

SRM プラグインの手順 30

VMware Infrastructure の要件 19

前提条件 26

手順 26, 29

のアレイ要件 20

インベントリ マッピング

使用方法 17

インベントリ環境設定

設定 49

設定の前提条件 49

用途 49

え

エクスポート形式（復旧プラン対
応） 63

お

オペレーティング システム
20

か

カスタマイズ仕様 69

インポート 70

作成 69

仮想マシン 16

カスタマイズ設定 69

重要でないリソースをサスペン
ド 62

設定 17, 67

設定の前提条件 67

パワーオンの分類 62

復旧後の再開の優先度 16

保護されたサイト インベントリか
らの削除 74

マッピングの環境設定 16

仮想マシンをサスペンド 62

く

クローン 20

マスキング 20

こ

構成

復旧サイト 61

VMware Infrastructure の要件 46

インベントリ環境設定 49

仮想マシン保護プロパティの前提条
件 52

保護サイト **45**
 コマンド ステップ
 追加のための前提条件 **54**
 用途 **54**

さ

災害

の定義 **9**

最大

仮想マシンの応答時間 **62**
 接続数 **28**

し

システム要件 **20**

信頼された証明書 **34**

す

スクリプト

DOS コマンドの実行 **54**

アラーム通知 **81**

バッチ ファイルの実行 **54**

ストレージ レプリケーション アダプ
 タ **20, 45**

スナップショット **20**

マスキング **20**

ち

チェックリスト

フェイルバック **87**

プリンストール **85**

つ

通知 **79**

て

データストア

メタ データ **51**

データストア グループ

および保護グループ **13**

データソース名 (DSN) **28**

データベース

Oracle **11**

SQL **11**

データベース要件

Oracle Server **23**

に

認証

安全な接続を参照 **34**

は

バッチ ファイル **54**

パワーオンの分類

高、標準、低、またはなし **62**

ふ

フェイルバック

管理する **71**

シナリオ **71**

準備 **73**

ソース LUN をサイト A に変更す
 る **76**

ソース LUN をサイト B に変更す
 る **73**

チェックリスト **87**

ディレクトリのクリーンアップ **73,**
75

復旧サイトから保護サイトにフェイ
 ルバックする **74**

別のフェイルオーバー用にサイト A
 を準備する **75**

別のフェイルオーバー用にサイト B
 を準備する **76**

フェイルバック中のディレクトリのク
 リーンアップ **73, 75**

復旧サイト

中断による変更 **84**

無停止の変更 **84**

復旧プラン

- エクスポート **68, 69**
- エクスポート形式 **63, 68**
- 削除 **67**
- 削除するための前提条件 **66**
- 作成 **61, 62**
- 作成のための前提条件 **62**
- 実際に実行する **66, 74**
- 実際に実行するための前提条件 **66**
- 詳細の表示 **63**
- 定義済み **16, 61**
- テスト **65, 74**
- テストの前提条件 **65**
- 表示 **68**
- 編集する **64**
- 履歴の表示 **69**
- プリインストール チェックリスト **85**
- プレースホルダ仮想マシン
用途 **51**
- へ
- ペアリング **77**
 - の前提条件 **34**
 - 保護サイトと復旧サイト **34**
- ほ
- 保護グループ **13**
 - およびデータストア グループ **13**
 - 作成 **50**
 - 作成のための前提条件 **50**
 - 定義済み **15, 50**
 - 保護サイトで **15**
- 保護サイト
 - 中断による変更 **84**
 - 無停止の変更 **83**
- 保護サイトと復旧サイト
 - セットアップ **15, 16**
- 保護サイトと復旧サイトの接続
 - ペアリングを参照 **34**
- ホストのシステム要件 **20**
- ホストバス アダプタ (HBA) **74, 76**
- め
- メタ データ **51**
- メッセージ ステップ
 - 追加のための前提条件 **54**
 - 用途 **54**
- ら
- ライセンス
 - SiteRecoveryManager.lic ファイル **24**
 - VMware ライセンス サーバ ツール **24**
 - 詳細を検索 **24**
 - ライセンス サーバ **24**
- り
- リスナ ポート
 - HTTP **28**
 - SOAP **28**