

# Site Recovery Manager 管理

Site Recovery Manager 8.2

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**ヴィエムウェア株式会社**  
〒108-0023 東京都港区芝浦 3-1-1  
田町ステーションタワー N 18 階  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2008-2019 VMware, Inc. All rights reserved. 著作権および商標情報。

# 目次

VMware Site Recovery Manager の管理について 8

更新情報 9

## 1 Site Recovery Manager の特権、ロール、および権限 10

Site Recovery Manager が権限を処理する方法 11

Site Recovery Manager と vCenter Server の管理者ロール 12

Site Recovery Manager と vSphere Replication のロール 12

共有リカバリ サイト構成での権限の管理 13

Site Recovery Manager のロールと権限の割り当て 15

Site Recovery Manager ロール リファレンス 17

## 2 仮想マシンのレプリケーション 22

Site Recovery Manager でのアレイベース レプリケーションの使用 22

アレイベース レプリケーションの構成 23

vSphere Replication と Site Recovery Manager の使用 30

仮想マシンのレプリケートと複数の特定の時点のインスタンスの有効化 31

Site Recovery Manager でのアレイベース レプリケーションと vSphere Replication の使用 32

## 3 マッピングの構成 34

アレイベース レプリケーション保護グループおよび vSphere Replication 保護グループ用のインベントリ マッピング 35

ストレージ ポリシー保護グループのインベントリ マッピング 35

一時的なブレースホルダ マッピングの構成 37

一時的なブレースホルダ マッピングの構成後に仮想マシンへのアクセス権をユーザーが取得 39

インベントリ マッピングの構成 39

ストレージ ポリシーのマッピングについて 41

ストレージ ポリシーのマッピングの選択 42

## 4 ブレースホルダ仮想マシンについて 44

リカバリ中のブレースホルダ仮想マシンへの処理 45

ブレースホルダ データストアの選択 46

## 5 保護グループの作成および管理 48

アレイベース レプリケーション保護グループとデータストア グループについて 49

Site Recovery Manager によるデータストア グループの計算方法 50

vSphere Replication 保護グループ 51

ストレージ ポリシー保護グループについて 52

ストレージ ポリシー保護グループの前提条件	53
ストレージ ポリシー保護グループの制限事項	54
ストレージ ポリシー保護グループと保護されていない仮想マシン	57
暗号化された仮想マシンの保護	58
保護グループの状態の概要	58
仮想マシンの保護状態の概要	60
保護グループの作成	61
vSphere Replication 保護グループの作成	61
ストレージ ポリシー保護グループの作成	62
アレイベース レプリケーション保護グループの作成	63
フォルダ内の保護グループの整理	65
データストア グループまたは仮想マシンの保護グループへの追加および保護グループからの削除	65
アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用	67
アレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成	68
アレイベース保護グループまたは vSphere Replication 保護グループ内の仮想マシンの設定の変更	69
仮想マシンからの保護の削除	70
仮想マシンからの保護の削除	71

## 6 復旧プランの作成、テスト、実行 72

復旧プランのテスト	73
ネットワークとデータセンター ネットワークのテスト	74
リカバリ プランの実行による計画移行またはディザスタ リカバリの実行	75
強制復旧による復旧の実行	76
復旧プランのテストと実行の相違点	77
リカバリ サイトの複数のホストでの仮想マシンのテスト リカバリの実行	78
復旧プランの作成、テスト、実行	79
復旧プランの作成	79
フォルダによるリカバリ プランの整理	80
復旧プランの編集	81
復旧プランのテスト	81
リカバリ プランをテストした後のクリーンアップ	82
復旧プランの実行	83
仮想マシンの特定の時点のスナップショットのリカバリ	84
テストまたは復旧のキャンセル	85
ストレージ ポリシー保護グループ内の仮想マシンのリカバリの無効化	85
ストレージ ポリシー保護グループ内の整合性グループのリカバリの無効化	86
リカバリ プランのステップのエクスポート	87
リカバリ プランの履歴レポートの表示とエクスポート	87
復旧プランの削除	88
リカバリ プランの状態の概要	89

## 7 リカバリ プランの構成 92

リカバリ プランの手順 92

カスタム リカバリ手順の作成 93

カスタム リカバリ ステップの種類 94

Site Recovery Manager がカスタム リカバリ手順のエラーを処理する方法 95

コマンド 手順を記述するためのガイドライン 96

コマンド ステップの環境変数 96

トップレベルのメッセージ プロンプトまたはコマンド手順の作成 99

個別の仮想マシンのメッセージ プロンプトまたはコマンド ステップの作成 100

リカバリ プラン実行時の仮想マシンのサスペンド 101

仮想マシンの復旧優先順位の指定 102

仮想マシンの依存関係の構成 103

計画移行用の vSphere vMotion の有効化 104

仮想マシンの起動およびシャットダウン オプションの構成 104

仮想マシンの保護とリカバリに関する制限事項 105

## 8 仮想マシンの IP プロパティのカスタマイズ 108

個々の仮想マシンの IP プロパティの手動カスタマイズ 109

仮想マシンへの IP カスタマイズ ルールの適用 110

複数の仮想マシンの IP プロパティのカスタマイズ 111

DR IP Customizer ツールを使用した複数の仮想マシンの IP プロパティのカスタマイズ 111

IP カスタマイズ ルールの定義による複数仮想マシンの IP プロパティのカスタマイズ 131

## 9 復旧後の仮想マシンの再保護 133

Site Recovery Manager がアレイベース レプリケーションを使用して仮想マシンを再保護する方法 134

Site Recovery Manager が vSphere Replication をを使用して仮想マシンを再保護する方法 135

Site Recovery Manager がストレージ ポリシー保護を使用して仮想マシンを再保護する方法 135

再保護を実行するための前提条件 136

仮想マシンの再保護 137

再保護の状態の概要 138

## 10 フェイルバックの実行による事前リカバリ サイト構成のリストア 139

フェイルバックの実行 140

## 11 他のソフトウェアとの Site Recovery Manager の相互運用性 142

Site Recovery Manager と vCenter Server 143

Site Recovery Manager と VMware vSAN ストレージおよび vSphere Replication の併用 144

リカバリ時の Site Recovery Manager と DPM および DRS の連携方法 144

復旧時の Site Recovery Manager と Storage DRS および Storage vMotion の連携方法 145

Storage DRS または Storage vMotion を使用するサイトでの Site Recovery Manager とアレイベース  
レプリケーションの併用 145

Storage DRS または Storage vMotion を使用するサイトでの Site Recovery Manager と vSphere Replication の併用	146
Site Recovery Manager と vSphere High Availability の連携方法	147
Site Recovery Manager が拡張されたストレージと相互作用する方法	147
Site Recovery Manager と NSX Data Center for vSphere の使用	149
Site Recovery Manager と vSphere PowerCLI	150
Site Recovery Manager および仮想マシンの暗号化	150
Site Recovery Manager と vRealize Orchestrator	151
Microsoft Cluster Server およびフォールトトレラント仮想マシンの保護	151
Site Recovery Manager を SIOC データストアと併用	153
Site Recovery Manager をアドミッションコントロール クラスタと併用	154
Site Recovery Manager と RDM ディスク デバイスに接続された仮想マシン	155
Site Recovery Manager と Active Directory ドメイン コントローラ	155

## 12 Site Recovery Manager の高度な構成 156

Site Recovery Manager の設定の再構成	156
接続設定の変更	156
Site Recovery Manager 履歴レポート収集の設定の変更	157
ローカル サイトの設定の変更	158
ログ設定の変更	159
リカバリ設定の変更	161
リモート マネージャ設定の変更	165
リモート サイトの設定の変更	166
レプリケーション設定の変更	166
SSO 設定の変更	167
ストレージ設定の変更	168
ABR ストレージ ポリシー設定の変更	169
ストレージ プロバイダ設定の変更	169
vSphere Replication 設定の変更	172
テレメトリ設定の変更	173
大規模な Site Recovery Manager 環境を実行するように設定を変更する	174
大規模な Site Recovery Manager 環境の設定	176

## 13 Site Recovery Manager のイベントとアラーム 179

Site Recovery Manager がサイト間の接続を監視する方法	179
Site Recovery Manager アラームの作成	180
Site Recovery Manager のイベント参照	180

## 14 Site Recovery Manager ログ ファイルの収集 191

Site Recovery Manager インターフェイスを使用する Site Recovery Manager ログ ファイルの収集	191
手動での Site Recovery Manager ログ ファイルの収集	192
Site Recovery Manager Server ログ ファイルのサイズと数の変更	192

Site Recovery Manager コア ダンプの構成 194

## 15 Site Recovery Manager のトラブルシューティング 196

- リカバリ サイトで多数の仮想マシンを同時にパワーオンするとエラーが起こる場合がある 196
- 仮想マシンの保護グループへの追加が未解決のデバイス エラーにより失敗する 197
- 保護の構成がブレースホルダの作成エラーにより失敗する 197
- ブレースホルダを短い時間内に削除し、再作成を行うと失敗する 198
- ホストが不正な状態にあるため計画移行が失敗する 198
- ストレージ ポリシー保護グループを同期できなかったために、計画移行に失敗する 199
- 一部の仮想マシンでネットワークのカスタマイズ時にタイムアウト エラーによりリカバリが失敗する 199
- リカバリが利用できないホストまたはデータストアのエラーで失敗する 200
- 再保護が vSphere Replication のタイムアウト エラーで失敗する 201
- VMware Tools の待機中にリカバリ プランがタイムアウトする 201
- vSphere Replication 保護グループの同期の失敗 202
- データストアの再スキャンがストレージ デバイスの準備ができていないため失敗する 202
- 計画移行中にリカバリが 36% で停止する 203
- レプリケート対象外に関するエラーが発生してリカバリが失敗する 203
- 制限されたユーザー権限によってリカバリが失敗する 204
- サポートされていない VMware Tools と ESXi の組み合わせによってリカバリが失敗する 205

# VMware Site Recovery Manager の管理について

VMware Site Recovery Manager は、VMware vCenter Server の拡張機能で、ビジネスの継続性と、vCenter Server 仮想マシン リカバリの計画、テスト、実行を支援するディザスタ リカバリ ソリューションを提供します。Site Recovery Manager では、レプリケートされるデータストアを検出および管理して、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。

## 対象者

本書は、vSphere やレプリケーション テクノロジー（ホスト ベースのレプリケーションやレプリケートされたデータストアなど）に詳しい Site Recovery Manager 管理者を対象としています。このソリューションは、vSphere インベントリの保護を構成する管理者のニーズに対応します。また、保護インベントリに仮想マシンを追加するユーザーや既存のインベントリが Site Recovery Manager で使用できるように正しく構成されていることを確認する必要があるユーザーも対象となります。



# 更新情報

この『Site Recovery Manager 8.2 管理』は、製品のリリースごとに、または必要に応じて更新されます。

以下の表に、『Site Recovery Manager 8.2 管理』ガイドの更新履歴を示します。

リビジョン	説明
2020 年 8 月 05 日	VMware では、多様性の受け入れを尊重しています。お客様、パートナー、社内コミュニティとともにこの原則を推進するために、コンテンツで使用される用語の一部を置き換えています。VMware は多様性の受け入れに適切でない言葉遣いを削除するため、このガイドを更新しました。
2019 年 8 月 14 日	<ul style="list-style-type: none"><li>■ 新しいトピック <a href="#">Site Recovery Manager および仮想マシンの暗号化</a>を追加。</li><li>■ <a href="#">DR IP Customizer ツールの構文</a>のトピックの情報が更新されました。</li><li>■ <a href="#">DR IP Customizer の実行による複数の仮想マシンの IP プロパティのカスタマイズ</a>のトピックの情報が更新されました。</li></ul>
2019 年 5 月 09 日	初期リリース。

# Site Recovery Manager の特権、ロール、および権限

# 1

Site Recovery Manager はユーザーに代わって操作を実行することにより、災害復旧を行います。これらの操作には、復旧プランや保護グループなどのオブジェクトの管理、仮想マシンのレプリケーションや電源オフなどの操作が含まれます。Site Recovery Manager はロールと権限を使用するため、正しいロールと権限をもつユーザーだけが操作を実行できます。

Site Recovery Manager は複数のロールを vCenter Server に追加し、各ロールには Site Recovery Manager と vCenter Server のタスクを実行するための権限が含まれています。Site Recovery Manager でタスクの実行を許可するには、ロールをユーザーに割り当てます。

## 権限

たとえば、復旧プランを作成したり、保護グループを変更したりなどのアクションを実行する権利。

## ロール

権限の集合。デフォルトのロールにより、Site Recovery Manager のタスク セットを実行するために特定のユーザー（たとえば、保護グループを管理したり、復旧を実行したりするユーザー）が必要とする特権が付与されます。一人のユーザーは1つのオブジェクトでロールを1つだけもつことができますが、すべてがオブジェクトについてロールをもっている複数のグループにユーザーが属する場合は、ロールを組み合わせることができます。

## 権限

特定のユーザーまたは特定のオブジェクトのユーザー グループに付与されるロール。ユーザーまたはユーザーグループは、プリンシパルとも呼ばれます。権限は、ロール、オブジェクト、およびプリンシパルの組み合わせです。たとえば、ある権限は、特定の保護グループを変更する特権です。

Site Recovery Manager が vCenter Server に追加するロール、およびタスクを実行するためにユーザーに必要な特権の詳細については、[Site Recovery Manager ロール リファレンス](#) を参照してください。

### ■ Site Recovery Manager が権限を処理する方法

保護の構成やリカバリ プランでの各手順の実行などの操作を実行する権限がユーザーにあるかどうかは、Site Recovery Manager によって決定されます。この権限のチェックでユーザーの有効な認証が確保されますが、操作が実行されるセキュリティ コンテキストは含まれません。

### ■ Site Recovery Manager と vCenter Server の管理者ロール

Site Recovery Manager をインストールする際に、ユーザーまたはユーザー グループに vCenter Server インスタンスに対する vCenter Server の管理者ロールがある場合、そのユーザーまたはユーザー グループは Site Recovery Manager のすべての権限を取得します。

## ■ Site Recovery Manager と vSphere Replication のロール

vSphere Replication を Site Recovery Manager とともにインストールする場合、vCenter Server の管理者ロールは Site Recovery Manager と vSphere Replication の権限のすべてを継承します。

## ■ 共有リカバリ サイト構成での権限の管理

共有リカバリ サイトを使用するための権限の構成を Site Recovery Manager で行うことができます。共有リカバリ サイトの vCenter Server 管理者は、各ユーザーが Site Recovery Manager を構成して使用するための十分な権限を保有し、別のユーザーに属しているリソースにアクセスできないように権限を管理する必要があります。

## ■ Site Recovery Manager のロールと権限の割り当て

Site Recovery Manager のインストール時に、vCenter Server 管理者ロールを持つユーザーに Site Recovery Manager での管理者ロールが付与されます。この時点では、他のユーザーにアクセス権が明示的に付与されないかぎり、vCenter Server 管理者のみが Site Recovery Manager にログインできます。

## ■ Site Recovery Manager ロール リファレンス

Site Recovery Manager は一連のロールを含んでいます。各ロールには、該当するロールのユーザーが各種アクションを完了するための権限セットが含まれています。

# Site Recovery Manager が権限を処理する方法

保護の構成やリカバリ プランでの各手順の実行などの操作を実行する権限がユーザーにあるかどうかは、Site Recovery Manager によって決定されます。この権限のチェックでユーザーの有効な認証が確保されますが、操作が実行されるセキュリティ コンテキストは含まれません。

Site Recovery Manager はサイトへの接続に使用されるユーザー ID のセキュリティ コンテキストまたはローカル システム ID などの Site Recovery Manager サービスが実行されている ID のコンテキストで操作を実行します。

Site Recovery Manager は、ユーザーにターゲット vSphere リソースに対する適切な権限があることを確認すると、Site Recovery Manager は vSphere 管理者ロールを使用してユーザーに代わって操作を実行します。

仮想マシンの保護を構成する操作では、ユーザーが操作を要求すると Site Recovery Manager はユーザー権限を検証します。操作には 2 段階の検証が必要です。

- 1 構成中に、Site Recovery Manager は、システムを構成するユーザーが vCenter Server オブジェクトに対する構成を完了するために必要な権限を保有していることを確認します。たとえば、ユーザーは仮想マシンを保護し、リカバリされた仮想マシンが使用するセカンダリ vCenter Server のリソースを使用する権限を保有している必要があります。
- 2 構成を実行するユーザーには、構成しているタスクを完了するための適正な権限が必要です。たとえば、ユーザーは復旧プランを実行するための権限をもつ必要があります。その後に Site Recovery Manager は、ユーザーに代わって vCenter Server 管理者としてタスクを完了します。

結果として、復旧などの特定のタスクを完了するユーザーは、必ずしも vSphere リソースで動作を行う権限が必要ではなくなります。ユーザーには、Site Recovery Manager でリカバリを実行するための権限のみが必要です。Site Recovery Manager は、保護サイトとリカバリ サイトに接続する際に提供されるユーザー認証情報を使用して操作を実行します。

Site Recovery Manager は、vCenter Server が使用するモデルと同様のモデルを使用する内部 Site Recovery Manager オブジェクトの権限のデータベースを維持します。Site Recovery Manager は vCenter Server オブジェクトに対しても、自身の Site Recovery Manager 権限を検証します。たとえば、Site Recovery Manager は 容量の割り当て のような複数の低レベル権限はチェックせずに、ターゲット データベースで リソース.リカバリ使用 権限があるかどうかをチェックします。Site Recovery Manager は、リモートの vCenter Server インスタンスの権限についても確認します。

Site Recovery Manager を vSphere Replication とともに使用するには、Site Recovery Manager ロールと vSphere Replication ロールをユーザーに割り当てる必要があります。vSphere Replication ロールについては、『vSphere Replication の管理』を参照してください。

## Site Recovery Manager と vCenter Server の管理者ロール

Site Recovery Manager をインストールする際に、ユーザーまたはユーザー グループに vCenter Server インスタンスに対する vCenter Server の管理者ロールがある場合、そのユーザーまたはユーザー グループは Site Recovery Manager のすべての権限を取得します。

Site Recovery Manager のインストール後に vCenter Server の管理者ロールをユーザーまたはユーザー グループに割り当てる場合、Site Recovery Manager のオブジェクトに対する Site Recovery Manager のロールをこれらのユーザーに手動で割り当てる必要があります。

vCenter Server の管理者ロールを保有しないユーザーまたはユーザー グループに Site Recovery Manager のロールを割り当てることができます。この場合、これらのユーザーには Site Recovery Manager の操作を実行する権限はありますが、vCenter Server のすべての操作を実行する権限はありません。

## Site Recovery Manager と vSphere Replication のロール

vSphere Replication を Site Recovery Manager とともにインストールする場合、vCenter Server の管理者ロールは Site Recovery Manager と vSphere Replication の権限のすべてを継承します。

ユーザーまたはユーザー グループに Site Recovery Manager のロールを手動で割り当てる場合、または vCenter Server 管理者でないユーザーまたはユーザー グループに Site Recovery Manager のロールを割り当てる場合、これらのユーザーは vSphere Replication 権限を取得できません。Site Recovery Manager のロールには、vSphere Replication のロールの権限は含まれません。たとえば、Site Recovery Manager リカバリ管理者ロールにはリカバリ プランを実行する権限があり、ここには vSphere Replication の保護グループを含むリカバリ プランも含まれますが、仮想マシンの vSphere Replication を構成する権限は含まれません。Site Recovery Manager および vSphere Replication のロールを分離することにより、異なるユーザー間での責任を分散できます。たとえば、あるユーザーが VRM 管理者ロールで仮想マシンの vSphere Replication の構成に責任を負い、別のユーザーが Site Recovery Manager リカバリ管理者ロールでリカバリの実行に責任を負うということも可能です。

場合によっては、vCenter Server 管理者でないユーザーに Site Recovery Manager と vSphere Replication の両方の操作を実行する権限が必要なこともあります。Site Recovery Manager および vSphere Replication のロールの組み合わせを単一のユーザーに割り当てるには、ユーザーを 2 つのユーザー グループに追加します。

## 例：Site Recovery Manager および vSphere Replication のロールの 1 人のユーザーへの割り当て

ユーザー グループを 2 つ作成することにより、ユーザーを vCenter Server 管理者にすることなく Site Recovery Manager のロールと vSphere Replication のロールの両方の権限を 1 人のユーザーに付与できます。

- 1 ユーザー グループを 2 つ作成します。
- 2 Site Recovery Manager のロールを 1 つのユーザー グループ (Site Recovery Manager 管理者など) に割り当てます。
- 3 vSphere Replication のロールをもう 1 つのユーザー グループ (VRM 管理者など) に割り当てます。
- 4 ユーザーを両方のユーザー グループに追加します。

このユーザーは Site Recovery Manager 管理者ロールと VRM 管理者ロールのすべての権限を持つことになります。

## 共有リカバリ サイト構成での権限の管理

共有リカバリ サイトを使用するための権限の構成を Site Recovery Manager で行うことができます。共有リカバリ サイトの vCenter Server 管理者は、各ユーザーが Site Recovery Manager を構成して使用するための十分な権限を保有し、別のユーザーに属しているリソースにアクセスできないように権限を管理する必要があります。

共有リカバリ サイトでは、ユーザーは Site Recovery Manager Server インスタンスのペアの所有者を指します。適切な権限のあるユーザーは、共有リカバリ サイトにアクセスして、各自の保護サイトのリカバリ プランを作成、テスト、および実行できる必要があります。共有リカバリ サイトの vCenter Server 管理者は、ユーザーごとに個別のユーザー グループを作成する必要があります。ユーザーのユーザー アカウントを vCenter Server 管理者グループのメンバーにすることはできません。共有リカバリ サイトでは、1 つの組織がすべての保護サイトとリカバリサイトを管理する構成のみがサポートされています。

---

**注意：** 特定の Site Recovery Manager ロールではユーザーが Site Recovery Manager Server でコマンドを実行できるため、これらのロールは信頼できる管理者レベルのユーザーのみに割り当てる必要があります。Site Recovery Manager Server でコマンドを実行できる Site Recovery Manager ロールのリストについては、[Site Recovery Manager ロール リファレンス](#) を参照してください。

---

共有リカバリ サイトでは、複数の顧客が単一の vCenter Server インスタンスを共有します。場合によっては、複数の顧客がリカバリ サイトで単一の ESXi ホストを共有することもあります。保護サイトのリソースは、共有リカバリ サイトの共有リソースにマッピングできます。たとえば、すべての顧客が同じ組織に属していて、各顧客の仮想マシンを個別に用意する必要がない場合は、リカバリ サイトのリソースを共有できます。

また、共有リカバリ サイトに隔離されたリソースを作成し、共有リカバリ サイトの各顧客専用のリソースに保護サイトのリソースをマッピングすることもできます。たとえば、すべての顧客が異なる組織に属していて各顧客の仮想マシンを個別に用意する必要がある場合は、この構成を使用できます。

## ユーザーのリソースの共有に関するガイドライン

共有リカバリ サイトでユーザーのリソースを共有する権限を構成するときは、次のガイドラインに従ってください。

- すべてのユーザーには、共有リカバリ サイトの vCenter Server のすべてのフォルダへの読み取りアクセス権が必要です。
- データセンターまたはホストを名前変更、移動、または削除する権限をユーザーに付与しないでください。
- ユーザー専用のフォルダとリソース プールの外部に仮想マシンを作成する権限をユーザーに付与しないでください。
- ユーザー専用ではないオブジェクトのロールの変更や権限の割り当てをユーザーに許可しないでください。
- 異なる組織のリソース間での望ましくない権限の伝達を避けるため、共有リカバリ サイト上の vCenter Server のルート フォルダ、データセンター、およびホストに対する権限を伝播しないでください。

## ユーザーのリソースの隔離に関するガイドライン

共有リカバリ サイトでユーザーのリソースを隔離する権限を構成するときは、次のガイドラインに従ってください。

- ユーザーごとに、vCenter Server インベントリ内の個別の仮想マシン フォルダを割り当てます。
  - このフォルダに対して、他のユーザーが仮想マシンを配置できないようにする権限を設定します。たとえば、管理者ロールを設定し、ユーザーのフォルダの伝播オプションをそのユーザーに対して有効にします。この構成によって、複数のユーザーが同じ名前の仮想マシンを保護する場合に発生する可能性がある名前の重複エラーを回避できます。
  - ユーザーのすべてのプレースホルダ仮想マシンをこのフォルダに配置して、権限を継承できるようにします。
  - 他のユーザーにこのフォルダへのアクセス権限を割り当てないでください。
- 各ユーザーに専用のリソース プール、データストア、およびネットワークを割り当て、フォルダに対する権限の構成と同様に権限を構成します。

---

**注意：** ユーザーのリソースを隔離するためのデプロイは、vSphere サイト間の信頼を前提にしています。ユーザーのリソースは隔離できますが、ユーザー自体を隔離することはできません。すべてのユーザーを完全に隔離する必要がある場合、これは適切なデプロイではありません。

---

## 共有リカバリ サイト構成でのタスクとイベントの表示

vSphere Client の [最近のタスク] パネルで、オブジェクトの表示権限があるユーザーは、他のユーザーがそのオブジェクトで開始したタスクを表示できます。すべてのユーザーは、他のユーザーが共有リソースに対して実行するすべてのタスクを表示できます。たとえば、共有ホスト、データセンター、または vCenter Server ルート フォルダで実行されたタスクは、すべてのユーザーが表示できます。

Site Recovery Manager Server のすべてのインスタンスによって共有リカバリ サイトで生成されるイベントには、同じ権限が付与されています。Site Recovery Manager Server の 1 つのインスタンスによるイベントを表示できるすべてのユーザーは、共有リカバリ サイトで実行されているすべての Site Recovery Manager Server インスタンスによるイベントを表示できます。

## Site Recovery Manager のロールと権限の割り当て

Site Recovery Manager のインストール時に、vCenter Server 管理者ロールを持つユーザーに Site Recovery Manager での管理者ロールが付与されます。この時点では、他のユーザーにアクセス権が明示的に付与されないかぎり、vCenter Server 管理者のみが Site Recovery Manager にログインできます。

ほかのユーザーに Site Recovery Manager へのアクセスを許可するためには、vCenter Server 管理者が Site Recovery Manager ユーザー インターフェイスでそれらのユーザーに権限を付与する必要があります。サイト単位でサイト全体の権限割り当てを行います。両方のサイトに対応する権限を追加する必要があります。

Site Recovery Manager は、Site Recovery Manager オブジェクトおよび vCenter Server オブジェクトに対する権限が必要です。リモート vCenter Server インストールで権限を構成するには、vSphere Web Client の別のインスタンスを開始します。保護サイトとリカバリ サイトに接続した後、両方のサイトで同じ Site Recovery Manager ユーザー インターフェイスから Site Recovery Manager 権限を変更できます。

Site Recovery Manager では、vCenter Server のロールと権限に加え、Site Recovery Manager 固有のタスクや操作を詳細に制御できる権限が追加されます。各 Site Recovery Manager のロールに含まれている権限の詳細については、[Site Recovery Manager ロール リファレンス](#)を参照してください。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。

### 3 左ペインで [権限] をクリックし、サイトを選択して、[追加] をクリックします。

- a [ドメイン] 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含まれるドメインを選択します。
- b [ユーザー/グループ] リストから特定のユーザー/グループを検索して選択します。

デフォルトでは、vCenter Single Sign-On は最大 5,000 行を返し、2 つに分けて配布されます。半数はユーザー用、もう半数はソリューション ユーザーとグループ用です。この設定は、vCenter Server の詳細設定から変更できます。

- c [ロール] ドロップダウン メニューからロールを選択し、ユーザーまたはユーザー グループに割り当てます。

[ロール] ドロップダウン メニューには、vCenter Server とそのプラグインによって使用可能になるすべてのロールが含まれています。Site Recovery Manager ではいくつかのロールが vCenter Server に追加されます。

オプション	操作
ユーザーまたはユーザー グループがすべての Site Recovery Manager の構成および管理操作を実行できるようにします。	SRM 管理者ロールを割り当てます。
ユーザーまたはユーザー グループが保護グループを管理および変更し、仮想マシンで保護を構成できるようにします。	SRM 保護グループ管理者ロールを割り当てます。
ユーザーまたはユーザー グループがリカバリを実行し、リカバリをテストできるようにします。	SRM リカバリ管理者ロールを割り当てます。
ユーザーまたはユーザー グループがリカバリ プランを作成、変更、およびテストできるようにします。	SRM リカバリ プラン管理者ロールを割り当てます。
ユーザーまたはユーザー グループがリカバリ プランをテストできるようにします。	SRM リカバリ テスト管理者ロールを割り当てます。

### 4 選択したロールを、このロールが影響する可能性のあるインベントリ 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、[子へ伝達] を選択します。

たとえば、あるロールにフォルダを変更する権限が含まれている場合にこのオプションを選択すると、フォルダ内のすべての仮想マシンでその権限が有効になります。より複雑な階層を持つ権限を作成する場合、このオプションを選択解除することができます。たとえば、このオプションを選択解除すると、階層ツリーの特定のノードのルートから伝達された権限がオーバーライドされますが、そのノードの子オブジェクトの権限はオーバーライドされません。

- 5 [追加] をクリックして、ロールとそれに関連付けられた権限をユーザーまたはユーザー グループに割り当てます。
- 6 手順 3 から手順 5 までを繰り返し、他の Site Recovery Manager サイト上のユーザーまたはユーザー グループにロールおよび権限を割り当てます。



## 結果

所定の Site Recovery Manager ロールをユーザーまたはユーザー グループに割り当てました。このユーザーまたはユーザー グループには、構成した Site Recovery Manager サイト上のオブジェクトに対して、ロールによって定義されるアクションを実行するための権限があります。

## 例： Site Recovery Manager ロールの結合

ユーザーまたはユーザー グループに割り当てられるのは 1 つのロールのみです。vCenter Server 管理者ではないユーザーに複数の Site Recovery Manager ロールの権限が必要な場合は、複数のユーザー グループを作成できます。たとえば、リカバリ プランを管理する権限とリカバリ プランを実行する権限が 1 人のユーザーに必要な場合があります。

- 1 ユーザー グループを 2 つ作成します。
- 2 SRM リカバリ プラン管理者ロールを 1 つのグループに割り当てます。
- 3 SRM リカバリ管理者ロールをもう 1 つのグループに割り当てます。
- 4 ユーザーを両方のユーザー グループに追加します。

SRM リカバリ プラン管理者ロールと SRM リカバリ管理者ロールの両方を持つグループのメンバーである場合、そのユーザーはリカバリ プランの管理とリカバリの実行を行えます。

## Site Recovery Manager ロール リファレンス

Site Recovery Manager は一連のロールを含んでいます。各ロールには、該当するロールのユーザーが各種アクションを完了するための権限セットが含まれています。

ロールの権限およびアクションのセットが重複している場合があります。たとえば、Site Recovery Manager 管理者ロールと Site Recovery Manager 保護グループ管理者が、保護グループを作成する権限を持っています。この権限を持つユーザーは、保護グループを管理するためのタスク セットの一部を完了できます。

保護オブジェクトとリカバリ オブジェクトが同じ権限を持つよう、Site Recovery Manager オブジェクト上のユーザーには、両方のサイトで同じロールを割り当てるようにしてください。

すべてのユーザーは少なくともシステム読み取り権限を、vCenter Server のルート フォルダと両方のサイトの Site Recovery Manager ルート ノードで持っている必要があります。

---

**注：** Site Recovery Manager Server をアンインストールすると、Site Recovery Manager はデフォルトの Site Recovery Manager ロールを削除しますが、Site Recovery Manager の権限は維持されます。Site Recovery Manager のアンインストール後も、Site Recovery Manager の権限は表示され、他のロールに割り当てることができます。これは標準的な vCenter Server の動作です。vCenter Server からのエクステンションを登録解除しても権限は削除されません。

---

表 1-1. Site Recovery Manager ロール

ロール	このロールで許可されるアクション	このロールに含まれる権限	このロールがアクセスできる vCenter Server インベントリ内のオブジェクト
Site Recovery Manager 管理者	<p>Site Recovery Manager 管理者は、すべての Site Recovery Manager 構成および管理操作を実行するための権限を付与します。</p> <ul style="list-style-type: none"> <li>■ 詳細設定を構成します。</li> <li>■ 接続を構成します。</li> <li>■ インベントリ環境設定を構成します。</li> <li>■ プレースホルダ データストアを構成します。</li> <li>■ アレイ マネージャを構成します。</li> <li>■ 保護グループを管理します。</li> <li>■ リカバリ プランを管理します。</li> <li>■ リカバリ プランを実行します。</li> <li>■ 再保護操作を実行します。</li> <li>■ 仮想マシンの保護を構成します。</li> <li>■ 保護グループを編集します。</li> <li>■ 保護グループを削除します。</li> <li>■ ストレージ ポリシー オブジェクトを表示します。</li> </ul> <p>Site Recovery Manager 管理者ユーザーは、継承された権限を編集できません。特定のユーザーのアクセスを制限したり、ユーザーにアクセス権を付与するには、Site Recovery Manager 管理者が新しいロールを追加する必要があります。</p>	<p>Site Recovery Manager.詳細設定.変更 Site Recovery Manager.アレイ マネージャ.構成 Site Recovery Manager.診断.エクスポート Site Recovery Manager.内部.内部アクセス Site Recovery Manager.インベントリ環境設定.変更 Site Recovery Manager.プレースホルダ データストア.構成 Site Recovery Manager.保護グループ.プランへの割り当て Site Recovery Manager.保護グループ.作成 Site Recovery Manager.保護グループ.変更 Site Recovery Manager.保護グループ.削除 Site Recovery Manager.保護グループ.プランからの削除 Site Recovery Manager.復旧履歴.履歴の削除 Site Recovery Manager.リカバリ履歴.削除されたプランの表示 Site Recovery Manager.リカバリ プラン.コマンドの構成 Site Recovery Manager.リカバリ プラン.作成 Site Recovery Manager.リカバリ プラン.変更 Site Recovery Manager.リカバリ プラン.リカバリ Site Recovery Manager.リカバリ プラン.削除 Site Recovery Manager.リカバリ プラン.再保護 Site Recovery Manager.リカバリ プラン.テスト Site Recovery Manager.リモート サイト.変更 データストア.レプリケーション.保護 データストア.レプリケーション.保護解除.停止 リソース.リカバリ使用 仮想マシン.SRM 保護.保護 仮想マシン.SRM 保護.停止 Site Recovery Manager.プロファイル駆動型ストレージ.プロファイル駆動型ストレージ ビュー</p>	<ul style="list-style-type: none"> <li>■ 仮想マシン</li> <li>■ データストア</li> <li>■ vCenter Server フォルダ</li> <li>■ リソース プール</li> <li>■ Site Recovery Manager サービス インスタンス</li> <li>■ ネットワーク</li> <li>■ Site Recovery Manager フォルダ</li> <li>■ 保護グループ</li> <li>■ リカバリ プラン</li> <li>■ アレイ マネージャ</li> </ul>
Site Recovery Manager 保護グループ 管理者	<p>Site Recovery Manager 保護グループ管理者ロールを使用して、ユーザーは保護グループを管理できます。</p>	<p>Site Recovery Manager.保護グループ.作成 Site Recovery Manager.保護グループ.変更 Site Recovery Manager.保護グループ.削除 データストア.レプリケーション.保護</p>	<ul style="list-style-type: none"> <li>■ Site Recovery</li> </ul>

表 1-1. Site Recovery Manager ロール（続き）

ロール	このロールで許可されるアクション	このロールに含まれる権限	このロールがアクセスできる vCenter Server インベントリ内のオブジェクト
	<ul style="list-style-type: none"> <li>■ 保護グループを作成します。</li> <li>■ 保護グループを変更します。</li> <li>■ 保護グループに仮想マシンを追加します。</li> <li>■ 保護グループを削除します。</li> <li>■ 仮想マシンの保護を構成します。</li> <li>■ 仮想マシンから保護を削除します。</li> </ul> <p>このロールのユーザーはリカバリを実行またはテストできないか、リカバリ プランを作成または変更できません。</p>	<p>データストア、レプリケーション、保護解除、停止</p> <p>リソース、リカバリ使用</p> <p>仮想マシン、SRM 保護、保護</p> <p>仮想マシン、SRM 保護、停止</p>	<p>ry</p> <p>Manag</p> <p>er フォ</p> <p>ルダ</p> <ul style="list-style-type: none"> <li>■ 保護グループ</li> </ul>
Site Recovery Manager リカバリ管理者	<p>Site Recovery Manager リカバリ管理者ロールを使用して、ユーザーはリカバリおよび再保護操作を実行できます。</p> <ul style="list-style-type: none"> <li>■ リカバリ プランから保護グループを削除します。</li> <li>■ リカバリ プランをテストします。</li> <li>■ リカバリ プランを実行します。</li> <li>■ 再保護操作を実行します。</li> <li>■ 仮想マシンにカスタム コマンド ステップを構成します。</li> <li>■ 削除されたリカバリ プランを表示します。</li> <li>■ 仮想マシンのリカバリ プロパティを編集します。</li> </ul> <p>このロールのユーザーは仮想マシンに保護を構成できないか、リカバリ プランを作成または削除できません。</p>	<p>Site Recovery Manager、保護グループ、プランからの削除</p> <p>Site Recovery Manager、リカバリ プラン、変更</p> <p>Site Recovery Manager、リカバリ プラン、テスト</p> <p>Site Recovery Manager、リカバリ プラン、リカバリ</p> <p>Site Recovery Manager、リカバリ プラン、再保護</p> <p>Site Recovery Manager、リカバリ プラン、コマンドの構成</p> <p>Site Recovery Manager、リカバリ履歴、削除されたプランの表示</p>	<ul style="list-style-type: none"> <li>■ 保護グループ</li> <li>■ リカバリプラン</li> <li>■ Site Recovery Manager サービスインスタンス</li> </ul>

表 1-1. Site Recovery Manager ロール（続き）

ロール	このロールで許可されるアクション	このロールに含まれる権限	このロールがアクセスできる vCenter Server インベントリ内のオブジェクト
Site Recovery Manager リカバリ プラン管理者	<p>Site Recovery Manager リカバリ プラン管理者ロールを使用して、ユーザーはリカバリ プランを作成およびテストできます。</p> <ul style="list-style-type: none"> <li>■ 復旧プランに保護グループを追加します。</li> <li>■ リカバリ プランから保護グループを削除します。</li> <li>■ 仮想マシンにカスタム コマンド ステップを構成します。</li> <li>■ リカバリ プランを作成します。</li> <li>■ リカバリ プランをテストします。</li> <li>■ リカバリ プラン テストをキャンセルします。</li> <li>■ 仮想マシンのリカバリ プロパティを編集します。</li> </ul> <p>このロールのユーザーは仮想マシンに保護を構成できないか、リカバリ操作または再保護操作を実行できません。</p>	<p>Site Recovery Manager.保護グループ.プランへの割り当て Site Recovery Manager.保護グループ.プランからの削除 Site Recovery Manager.リカバリ プラン.コマンドの構成 Site Recovery Manager.リカバリ プラン.作成 Site Recovery Manager.リカバリ プラン.変更 Site Recovery Manager.リカバリ プラン.削除 Site Recovery Manager.リカバリ プラン.テスト リソース.リカバリ使用</p>	<ul style="list-style-type: none"> <li>■ 保護グループ</li> <li>■ リカバリ プラン</li> <li>■ vCenter Server フォルダ</li> <li>■ データストア</li> <li>■ リソース プール</li> <li>■ ネットワーク</li> </ul>

表 1-1. Site Recovery Manager ロール（続き）

ロール	このロールで許可されるアクション	このロールに含まれる権限	このロールがアクセスできる vCenter Server インベントリ内のオブジェクト
Site Recovery Manager テスト管理者	<p>Site Recovery Manager テスト管理者ロールを使用して、ユーザーはリカバリプランのテストのみを行います。</p> <ul style="list-style-type: none"> <li>■ リカバリ プランをテストします。</li> <li>■ リカバリ プラン テストをキャンセルします。</li> <li>■ 仮想マシンのリカバリプロパティを編集します。</li> </ul> <p>このロールのユーザーは仮想マシンへの保護の構成、保護グループまたはリカバリプランの作成、リカバリ操作または再保護操作の実行を行えません。</p>	<p>Site Recovery Manager.リカバリ プラン.変更</p> <p>Site Recovery Manager.リカバリ プラン.テスト</p>	<ul style="list-style-type: none"> <li>■ リカバリ プラン</li> </ul>
Site Recovery Manager リモート ユーザー	<p>Site Recovery Manager リモート ユーザー ロールでは、サイト間の Site Recovery Manager 操作に必要な最小限の権限がユーザーに付与されます。</p>	<p>データストア.データストアの参照</p> <p>データストア.低レベルのファイル操作</p> <p>データストア.仮想マシン ファイルの更新</p> <p>データストア.仮想マシン メタデータの更新</p> <p>ホスト.vSphere Replication.レプリケーションの管理</p> <p>仮想マシン.スナップショット管理.スナップショットの削除</p> <p>仮想マシン.vSphere Replication.レプリケーションの構成</p> <p>仮想マシン.vSphere Replication.レプリケーションの管理</p> <p>仮想マシン.vSphere Replication.レプリケーションの監視</p>	<ul style="list-style-type: none"> <li>■ 仮想マシン</li> <li>■ データストア</li> </ul>

# 仮想マシンのレプリケーション

# 2

保護グループを作成する前に、保護する仮想マシンでレプリケーションを構成する必要があります。

アレイ ベースのレプリケーションまたは vSphere Replication を使用するか、またはその両方を使用することで、仮想マシンをレプリケートできます。

この章には、次のトピックが含まれています。

- Site Recovery Manager でのアレイベース レプリケーションの使用
- vSphere Replication と Site Recovery Manager の使用
- Site Recovery Manager でのアレイベース レプリケーションと vSphere Replication の使用

## Site Recovery Manager でのアレイベース レプリケーションの使用

アレイベース レプリケーションを使用する場合、保護サイトの 1 つ以上のストレージ アレイでリカバリ サイトのピア アレイにデータをレプリケートできます。ストレージ レプリケーション アダプタ (SRA) を使用すると、Site Recovery Manager をさまざまなアレイと統合できます。

Site Recovery Manager でアレイベース レプリケーションを使用するには、Site Recovery Manager を構成する前にレプリケーションを構成しておく必要があります。

ストレージ アレイで整合性グループがサポートされている場合、Site Recovery Manager は vSphere Storage DRS および vSphere Storage vMotion との互換性があります。Storage DRS と Storage vMotion を使用して、Site Recovery Manager によって保護されている整合性グループ内に仮想マシン ファイルを移動できます。ストレージ アレイで整合性グループがサポートされていない場合、Storage DRS と Storage vMotion を Site Recovery Manager と組み合わせて使用することはできません。

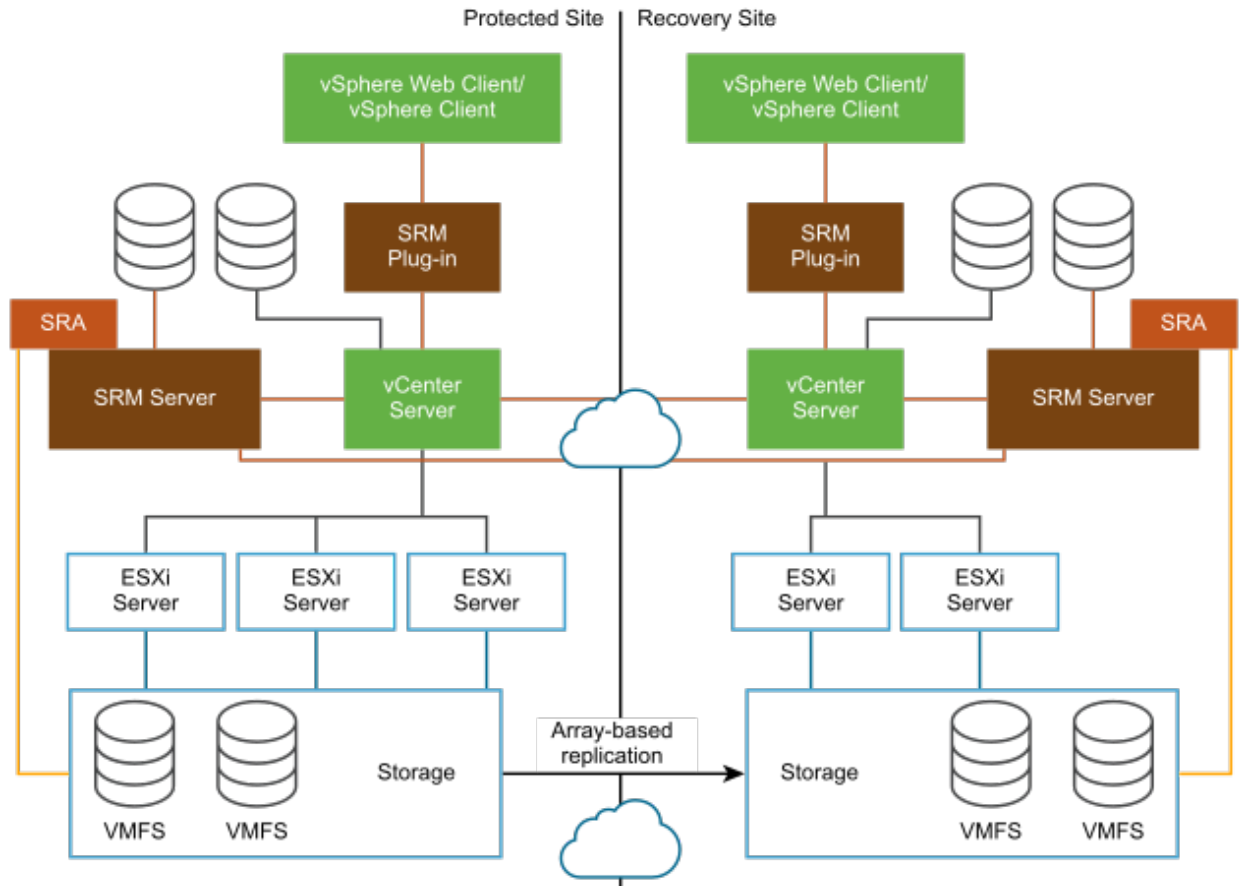
VMware vSphere Flash Read Cache ストレージを使用するディスクを含む仮想マシンを保護できます。仮想マシンのリカバリ先ホストに Flash Read Cache の構成が行われていない場合があるため、Site Recovery Manager はリカバリ サイトで仮想マシンを起動する際にディスク上の Flash Read Cache を無効にします。Site Recovery Manager は予約をゼロに設定します。vSphere Flash Read Cache を使用するように構成された仮想マシンでリカバリ処理を実行する前に、vSphere Web Client の仮想マシンのキャッシュ予約をメモしてください。リカバリ後、仮想マシンを Flash Read Cache ストレージのあるホストに移行し、仮想マシンに元の Flash Read Cache 設定を手動でリストアすることができます。

ストレージ ポリシー保護グループを使用して仮想マシンを保護する場合、アレイベース レプリケーションを使用してそれらの仮想マシンをレプリケートする必要があります。

## ストレージ レプリケーション アダプタ

ストレージ レプリケーション アダプタは、Site Recovery Manager リリースには含まれません。アレイ ベンダーはこれらを開発してサポートします。Site Recovery Manager Server ホストの Site Recovery Manager で使用する各アレイに固有の SRA をインストールする必要があります。Site Recovery Manager は複数の SRA の使用をサポートします。

図 2-1. Site Recovery Manager アーキテクチャとアレイベース レプリケーションの併用



## アレイベース レプリケーションの構成

アレイベース レプリケーションを使用してレプリケートした仮想マシン（ストレージ ポリシー保護グループを使用して保護する仮想マシンを含む）を保護するには、ストレージ レプリケーション アダプタ (SRA) を各サイトで構成する必要があります。

## ストレージ レプリケーション アダプタのインストール

アレイベース レプリケーション、またはストレージ ポリシー保護を伴うアレイベース レプリケーションを使用して仮想マシンを保護する場合は、Site Recovery Manager で使用する各ストレージ アレイに固有のストレージ レプリケーション アダプタ (SRA) をインストールする必要があります。SRA はアレイ ベンダーが提供するプログラムで、Site Recovery Manager が特定の種類のアレイと連動できるようにするためのものです。

保護サイトとリカバリ サイトの Site Recovery Manager Server ホストに適切な SRA をインストールする必要があります。複数のタイプのストレージ アレイを使用する場合は、両方の Site Recovery Manager Server ホスト上の各タイプのアレイに SRA をインストールする必要があります。

**注：** 複数のタイプのストレージ アレイを使用するように Site Recovery Manager を構成できますが、異なるベンダーの複数のアレイに単一仮想マシンの仮想マシン ディスクを保存することはできません。同一アレイに 1 台の仮想マシンのすべてのディスクを保存する必要があります。

ストレージ レプリケーション アダプタには、専用のインストール手順の説明書が付属しています。特定の Site Recovery Manager バージョンに対応するバージョンの SRA をインストールする必要があります。両方のサイトで同じバージョンの SRA をインストールします。SRA のバージョンを混在させないでください。

vSphere Replication を使用している場合、SRA は必要ありません。

#### 前提条件

- <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra> に掲載されている『VMware 互換性ガイド』で Site Recovery Manager の部分を参照して、使用しているストレージのタイプで利用できる SRA について確認してください。
- <https://my.vmware.com/web/vmware/downloads> に移動して、[VMware Site Recovery Manager] - [製品のダウンロード] の順に選択してから、[ドライバとツール] - [ストレージ レプリケーション アダプタ] - [ダウンロードする] の順に選択して、SRA をダウンロードします。
- SRA を別のベンダー サイトから取得する場合は、<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra> で Site Recovery Manager の『VMware 互換性ガイド』を参照して、使用している Site Recovery Manager リリースでその SRA が認定されていることを確認します。
- SRA 付属のドキュメントをお読みください。SRA は、ストレージ アレイに用意されている一部の機能をサポートしていません。SRA のサポート対象と要件の詳細については、SRA が提供するドキュメントに記載されています。たとえば、HP と EMC では、SRA が想定どおりに動作するために満たす必要がある物理要件が詳細に規定されています。
- SRA をインストールする前に、Site Recovery Manager Server をインストールします。
- ご使用の SRA には、他のベンダーが提供するコンポーネントをインストールする必要がある場合もあります。場合によっては、これらのコンポーネントの一部を Site Recovery Manager Server ホストにインストールする必要があります。他のコンポーネントでは Site Recovery Manager Server によるネットワーク アクセスのみが必要となる場合があります。そのような要件の最新情報については、インストールする SRA のリリース ノートおよび readme ファイルを参照してください。
- レプリケートされたデバイスのスナップショット コピーを作成するストレージ アレイの機能を有効にします。SRA のドキュメントを参照してください。

#### 手順

- 1 各 Site Recovery Manager Server ホストに SRA をインストールします。

インストーラで、SRA を C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra にインストールします。



- 2 vSphere Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックし、サイト ペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[構成] - [アレイ ベースのレプリケーション] - [ストレージ レプリケーション アダプタ] の順位選択し、[アダプタの再スキャン] ボタンをクリックします。

この操作により、SRA 情報が更新されて、Site Recovery Manager で SRA を検出できるようになります。

## アレイ マネージャの構成

保護サイトとリカバリ サイトのペアを決めたら、Site Recovery Manager によって、レプリケートされたデバイスの検出、データストア グループの計算、ストレージ操作の開始が実行されるように、両サイトで個別にアレイ マネージャを構成します。

通常、アレイ マネージャの構成は、サイトの接続後に 1 回のみ実行します。アレイ マネージャの接続情報または認証情報の変更や別のアレイ セットを使用する必要性がない限り、再構成する必要はありません。

### 前提条件

- Site Recovery Manager のインストールおよび構成 の [保護サイトとリカバリ サイトの接続の説明](#)にしたがって、サイトを接続します。
- [ストレージ レプリケーション アダプタのインストール](#) の説明にしたがって、両方のサイトに SRA をインストールします。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[構成] - [アレイ ベースのレプリケーション] - [アレイ ペア] の順にクリックします。
- 4 [追加] ボタンをクリックしてアレイ マネージャを追加します。
- 5 Site Recovery Manager で使用するストレージ レプリケーション アダプタを選択し、[次へ] をクリックします。

マネージャ タイプが表示されない場合、SRA を再スキャンします。または、Site Recovery Manager Server ホストに SRA がインストールされていることを確認します。

- 6 ローカル アレイ マネージャの名前を入力し、選択した SRA のタイプに必要な情報を入力し、[次へ] をクリックします。

このアレイ マネージャに関連するストレージを識別しやすいように説明的な名前を使用します。

これらのテキスト ボックスの入力方法の詳細については、SRA ベンダーが提供しているドキュメントを参照してください。テキスト ボックスには、SRA によって異なるものもあるが、IP アドレス、プロトコル情報、アレイ 名と IP アドレスの間のマッピング、およびユーザー名とパスワードなど、共通なものもあります。

- 7 (オプション) アレイ ペアを作成しない場合は、[現在は、リモート アレイ マネージャを作成しないでください] チェック ボックスを選択し、[終了] をクリックします。

- 8 リモート アレイ マネージャの名前を入力し、選択した SRA のタイプに必要な情報を入力し、[次へ] をクリックします。
- 9 [アレイ ペア] ページで、有効にするアレイ ペアを選択し、[次へ] をクリックします。
- 10 構成を確認して [終了] をクリックします。

## ストレージ レプリケーション アダプタの Site Recovery Manager Appliance への追加

アレイベースのレプリケーションに Site Recovery Manager を使用する場合は、ストレージ レプリケーション アダプタ (SRA) を Site Recovery Manager Server に追加する必要があります。SRA ファイルは、.tar.gz アーカイブとして配布されます。

保護サイトとリカバリ サイトの Site Recovery Manager Server ホストに適切な SRA をインストールする必要があります。複数のタイプのストレージ アレイを使用する場合は、両方の Site Recovery Manager Server ホスト上の各タイプのアレイに SRA をインストールする必要があります。

### 前提条件

- SRA をダウンロードします。<https://my.vmware.com/web/vmware/downloads> に移動して、[VMware Site Recovery Manager] - [製品のダウンロード] の順に選択してから、[ドライバとツール] - [ストレージ レプリケーション アダプタ] - [ダウンロードする] の順に選択します。
- 別のベンダー サイトから SRA を取得する場合は、使用している Site Recovery Manager リリースでこの SRA が認定されていることを確認します。<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra> にある VMware 互換性ガイドで Site Recovery Manager を確認してください。
- レプリケートされたデバイスのスナップショット コピーを作成するストレージ アレイの機能を有効にします。SRA のドキュメントを参照してください。

### 手順

- 1 管理者として Site Recovery Manager Appliance 管理インターフェイスにログインします。
- 2 Site Recovery Manager Appliance 管理インターフェイスで、[ストレージ レプリケーション アダプタ] をクリックしてから [新規アダプタ] をクリックします。
- 3 [アップロード] をクリックし、SRA ファイルを保存したディレクトリに移動して選択します。
- 4 処理が完了したら、[閉じる] をクリックします。  
ストレージ レプリケーション アダプタ カードが Site Recovery Manager Appliance 管理インターフェイスに表示されます。
- 5 vSphere Client または vSphere Web Client にログインします。
- 6 [Site Recovery] - [Site Recovery を開く] の順にクリックし、サイト ペアを選択して、[詳細表示] をクリックします。
- 7 [サイト ペア] タブで、[構成] - [アレイ ベースのレプリケーション] - [ストレージ レプリケーション アダプタ] の順位選択し、[アダプタの再スキャン] ボタンをクリックします。


## ストレージ レプリケーション アダプタの構成アーカイブのダウンロードとアップロード

アレイベース レプリケーションで Site Recovery Manager Appliance を使用していて、ストレージ レプリケーション アダプタ (SRA) を置き換える必要がある場合は、この SRA の構成アーカイブをダウンロードしてから、その構成を置き換え SRA にインポートできます。

### 前提条件

SRA 構成ファイルをダウンロードして別の SRA にインポートするには、同じベンダーから取得した SRA を使用する必要があります。

### 手順

- 1 管理者として Site Recovery Manager Appliance 管理インターフェイスにログインします。
- 2 [ストレージ レプリケーション アダプタ] タブをクリックします。
- 3 適切なストレージ レプリケーション アダプタ カードを選択し、ドロップダウン メニュー (  ) をクリックします。


オプション	説明
構成アーカイブのダウンロード	選択した SRA の構成アーカイブをダウンロードします。
構成アーカイブのアップロード	<p>選択した SRA の構成をインポートします。</p> <p>a SRA 構成アーカイブ ファイルを保存したディレクトリに移動して選択します。構成ファイルは、<code>.tar.gz</code> アーカイブとして配布されます。</p> <p>b [開く] をクリックします。</p>

## ストレージ レプリケーション アダプタの削除

Site Recovery Manager Appliance 管理インターフェイスを使用して、ストレージ レプリケーション アダプタ (SRA) を Site Recovery Manager Server から削除します。

**注：** SRA を削除すると、このアダプタによって制御されるストレージ アレイに関連する、現在実行中のすべての処理が中断されます。これには、リカバリ、テスト、クリーンアップ、再保護処理が含まれますが、これに限定されません。

### 手順

- 1 管理者として Site Recovery Manager Appliance 管理インターフェイスにログインします。
- 2 Site Recovery Manager Appliance 管理インターフェイスで、[ストレージ レプリケーション アダプタ] をクリックします。
- 3 適切なストレージ レプリケーション アダプタ カードを選択し、ドロップダウン メニュー (  ) から [削除] をクリックします。
- 4 アダプタの削除による影響を理解していることを確認し、[削除] をクリックします。

## 構成の変更を検出するためのアレイの再スキャン

デフォルトでは、Site Recovery Manager は 24 時間ごとにアレイを再スキャンしてデバイス構成の変更を確認します。ただし、アレイの再スキャンはいつでも実行できます。

[詳細設定] の `storage.minDsGroupComputationInterval` オプションを変更すると、Site Recovery Manager が定期的なアレイ スキャンを実行する頻度を再構成できます。「[ストレージ設定の変更](#)」を参照してください。

アレイ マネージャを構成すると、Site Recovery Manager は検出する一連のレプリケートされたストレージ デバイスに基づきデータストア グループを計算します。いずれかのサイトでアレイの構成を変更してデバイスを追加または削除する場合、Site Recovery Manager はアレイを再スキャンして、データストア グループを再計算する必要があります。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[構成] - [アレイ ベースのレプリケーション] - [アレイ ペア] の順にクリックします。
- 4 アレイ ペアを選択し、[アレイ マネージャのペア] - [アレイ ペアの検出] の順にクリックしてアレイを再スキャンするか、または [デバイスの検出] をクリックしてストレージ デバイスと整合性グループを再計算します。

アレイ ペアを選択すると、[アレイ ペア] タブには、ローカル デバイス名、ペアリングされているデバイス、レプリケーションの方向、デバイスが属する保護グループ、データストアがローカルとリモートのどちらなのか、各 SRA デバイスの整合性グループ ID など、すべてのストレージ デバイスに関する詳細な情報が示されます。

## アレイ マネージャの編集

ローカル アレイ マネージャの編集ウィザードまたはリモート アレイ マネージャの編集ウィザードを使用して、アレイ マネージャ名、または IP アドレスやユーザー名/パスワードなどその他の設定を変更します。

アダプタ フィールドの入力方法の詳細については、SRA ベンダーが提供しているドキュメントを参照してください。フィールドには、SRA によって異なるものもあるが、IP アドレス、プロトコル情報、アレイ名と IP アドレスの間のマッピング、およびユーザー名とパスワードなど、共通なものもあります。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[構成] - [アレイ ベースのレプリケーション] - [アレイ ペア] の順にクリックします。
- 4 アレイ ペアを選択し、[アレイ マネージャのペア] をクリックして、[ローカル アレイ マネージャの編集] または [リモート アレイ マネージャの編集] をクリックします。

## 5 アレイの名前を変更します。

このアレイ マネージャに関連するストレージを識別しやすいように説明的な名前を使用します。アレイ マネージャのタイプは変更できません。

## 6 アダプタ情報を変更します。

これらのフィールドは SRA によって作成されます。

## 7 [保存] をクリックして、アレイ マネージャの変更を完了します。

## スワップ ファイルにレプリケートされないデータストアを指定する

すべての仮想マシンにはスワップ ファイルが必要です。デフォルトで vCenter Server は、他の仮想マシンのファイルと同じデータストアにスワップ ファイルを作成します。Site Recovery Manager がスワップ ファイルをレプリケートしないようにするために、レプリケートされないデータストアでそれらのファイルを作成するように仮想マシンを構成できます。

通常の場合では、他の仮想マシンのファイルと同じデータストアにスワップ ファイルを保持する必要があります。ただし、ネットワーク帯域幅が余分に消費されないようにするため、スワップ ファイルがレプリケートされないようにすることが必要な場合があります。一部のストレージ ベンダーは、スワップ ファイルのレプリケートを推奨していません。絶対に必要な場合は、スワップ ファイルのレプリケーションのみを防止してください。

---

**注：** スワップ ファイル用にレプリケートされないデータストアを使用している場合は、保護サイトとリカバリ サイトの両方で、すべての保護ホストとクラスタにレプリケートされないデータストアを作成する必要があります。クラスタ内のすべてのホストは、レプリケートされていないデータストアにアクセスする必要があります。そうしないと、vMotion は動作しません。

---

### 手順

- 1 vSphere Client で、[ホストとクラスタ] を選択してホストを選択し、[構成] をクリックします。
- 2 [仮想マシン] から [スワップ ファイルの場所] を選択して [編集] をクリックします。
- 3 [特定のデータストアを使用する] を選択して、レプリケートされないデータストアを選択します。
- 4 [OK] をクリックします。
- 5 ホストのすべての仮想マシンをパワーオフしてからパワーオンします。  
ゲスト OS をリセットしただけでは不十分です。スワップファイルの場所の変更は、仮想マシンをパワーオフしてからパワーオンした後に有効になります。
- 6 スワップファイルに選択したデータストアを参照し、仮想マシン用の VSWP ファイルが存在することを確認します。

## ディザスタ リカバリ中に行う拡張されたストレージのデバイス隔離

拡張されたストレージのディザスタ リカバリでは、フェイルオーバー コマンドで、リカバリ サイトのデバイスを隔離する必要があります。

ディザスタ リカバリを開始するときに、保護サイトにある一部のホストがまだ稼動しており、仮想マシンの実行を継続していると、Site Recovery Manager は、ファイル ロックが原因で、対応するリカバリ サイトの仮想マシンをパワーオンできません。ストレージ アレイによってリカバリ サイトのデバイスが隔離されると、リカバリ サイトの ESX ホストは必要なロックを解除し、仮想マシンをパワーオンできます。

Site Recovery Manager は、保護サイトで非アクティブ化されなかった拡張されたデバイスに対するフェイルオーバー SRA コマンドで `isolation="true"` を使用する必要があります。

リカバリ サイトに同じデバイスから実行される複数の仮想マシンがあり、保護サイトからのストレージをリカバリ サイトの ESXi がマウントしている場合、隔離時に書き込み操作が失敗するリスクがあります。拡張されたストレージ上のすべての仮想マシンは、保護サイトで実行することが推奨されます。

拡張されたストレージの隔離がどのように実装されるかの詳細は、アレイ ベンダーに応じて異なります。一部のアレイ ベンダーは、隔離を使って、フェイルオーバー SRA コマンドの実行後に保護サイトのデバイスをアクセス不能にします。別のアレイ ベンダーは、特定のデバイスについて、ソースとターゲット サイトの間の通信を切断します。

## vSphere Replication と Site Recovery Manager の使用

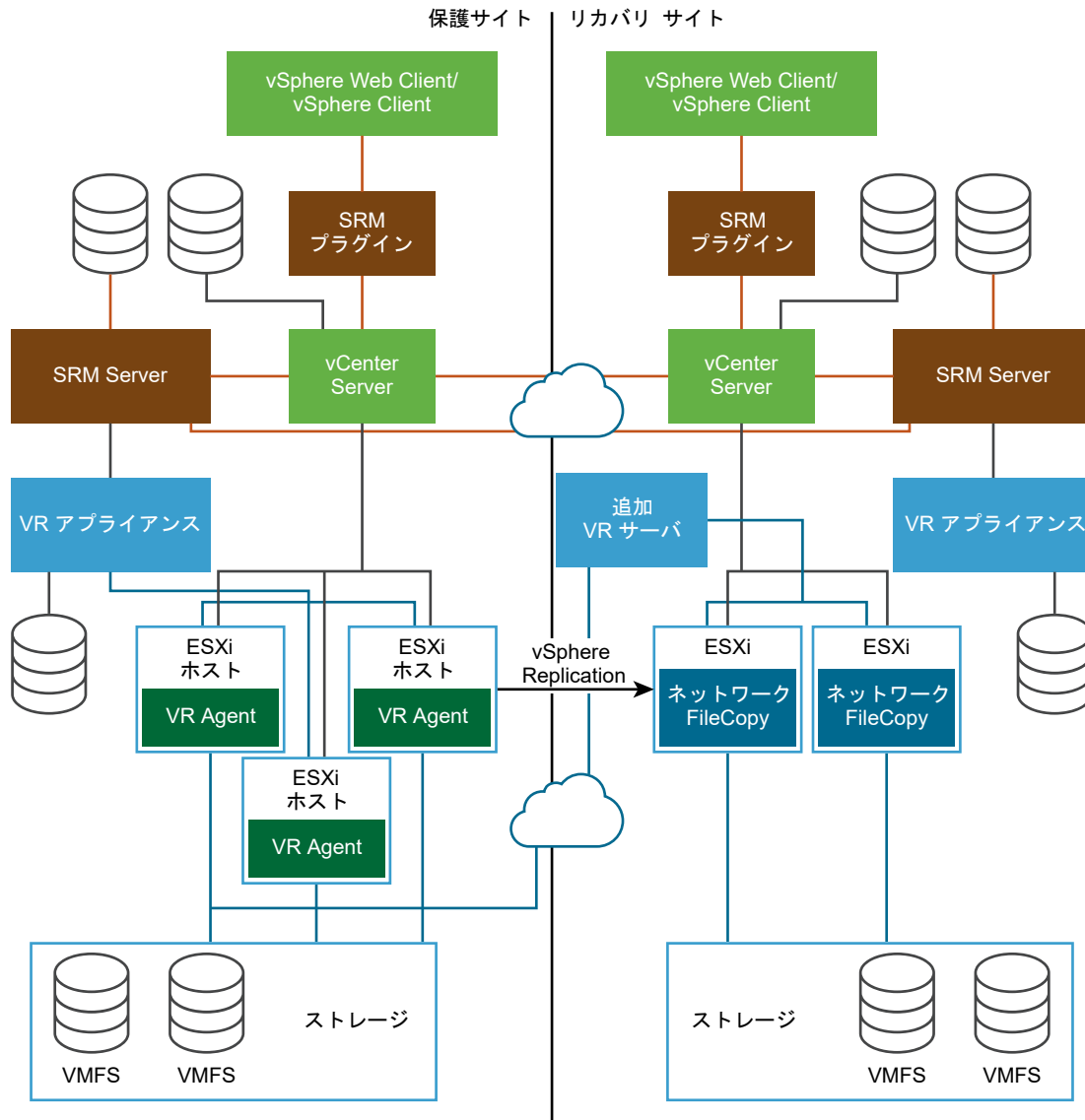
Site Recovery Manager は、vSphere Replication を使用してリカバリ サイトのサーバにデータをレプリケートできます。

vSphere Replication アプライアンスを展開し、Site Recovery Manager とは別に仮想マシンで vSphere Replication を構成します。vSphere Replication の展開と構成の詳細については、<https://www.vmware.com/support/pubs/vsphere-replication-pubs.html> の vSphere Replication のドキュメントを参照してください。

vSphere Replication にはストレージ アレイは必要ありません。vSphere Replication ストレージ レプリケーションのソースおよびターゲットには、任意のストレージ デバイス (ストレージ アレイに限定されない) を使用できます。

リカバリ サイトにある保護された仮想マシンのスナップショットを定期的に作成および保持するように vSphere Replication を構成できます。仮想マシンの複数の特定時点 (point-in-time, PIT) でのスナップショットを作成することにより、リカバリ サイトに仮想マシンの複数のレプリカを保持することができます。各スナップショットには、特定時点での仮想マシンの状態が反映されます。vSphere Replication を使用してリカバリを実行したときに、どのスナップショットをリカバリするかを選択できます。

図 2-2. Site Recovery Manager アーキテクチャと vSphere Replication の併用



## 仮想マシンのレプリケートと複数の特定の時点のインスタンスの有効化

最新の既知の整合性のある状態などの特定の時点 (PIT) で、仮想マシンをリカバリできます。

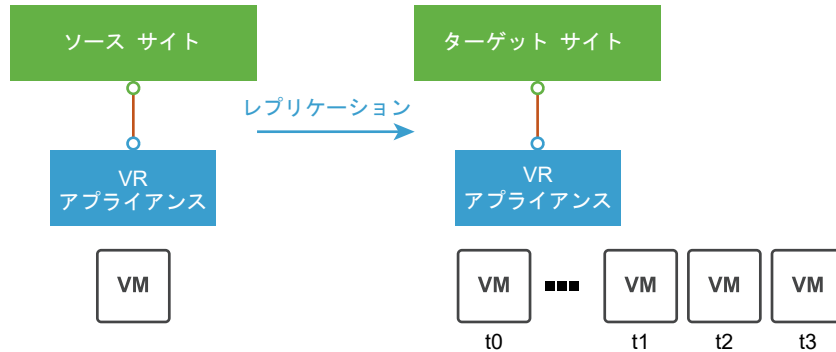
仮想マシンのレプリケーションを構成するときに、レプリケーションの構成ウィザードのリカバリ設定で複数の特定の時点 (MPIT) インスタンス を有効にできます。vSphere Replication は、指定されたリテンション ポリシーに基づいて、ターゲット サイトの仮想マシンのスナップショット インスタンスを一定数保持します。vSphere Replication は、最大 24 個のスナップショット インスタンスをサポートします。仮想マシンをリカバリ後、特定のスナップショットに復元できます。

レプリケーション中、vSphere Replication はターゲット サイトに、潜在的なウイルス、破損したアプリケーションを含む仮想マシンのあらゆる面をレプリケートします。仮想マシンにウイルスまたは破損が存在する状態で PIT スナップショットを保存するために vSphere Replication を構成した場合には、仮想マシンをリカバリしてから破損していない状態の仮想マシンのスナップショットに復元できます。

また、PIT インスタンスを使用して、データベースが正常であることがわかっている最後の状態にリカバリできます。

**注：** vSphere Replication が仮想マシンのスナップショットをレプリケートしません。

図 2-3. 仮想マシンの特定の時点 (PIT) へのリカバリ



## Site Recovery Manager でのアレイベース レプリケーションと vSphere Replication の使用

アレイベース レプリケーションと vSphere Replication の組み合わせを Site Recovery Manager デプロイで使用できます。

アレイベース アプリケーションと vSphere Replication を使用する混合 Site Recovery Manager デプロイを作成するには、両方のタイプのレプリケーションに対する保護サイトとリカバリ サイトを構成する必要があります。

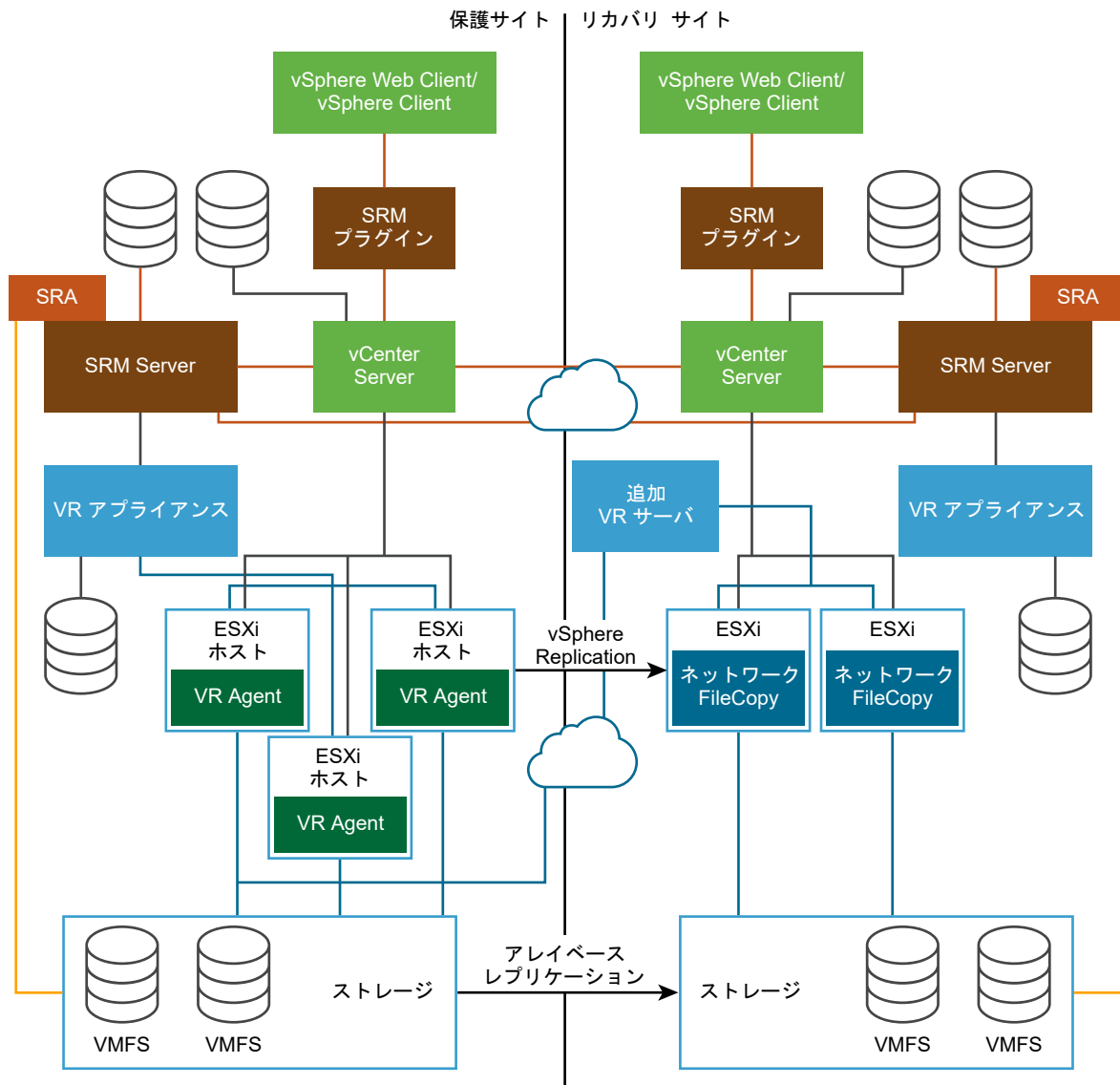
- ストレージ アレイをセットアップして接続し、両方のサイトに適切なストレージ レプリケーション アダプタ (SRA) をインストールします。
- 両方のサイトに vSphere Replication アプライアンスをデプロイし、アプライアンス間の接続を構成します。
- 必要に応じて、アレイベース レプリケーションまたは vSphere Replication を使用してレプリケーション用の仮想マシンを構成します。

**注：** アレイベース レプリケーションを使用してレプリケートするデータベースに存在する仮想マシンには、vSphere Replication を構成しないでください。

アレイベース レプリケーションで構成する仮想マシンにはアレイベースの保護グループを作成し、vSphere Replication で構成する仮想マシンには vSphere Replication 保護グループを作成します。保護グループにレプリケーション タイプを混在させることはできません。アレイ ベースの保護グループと vSphere Replication 保護グループを同じリカバリ プランに混在させることはできます。



図 2-4. アレイベース レプリケーションと vSphere Replication を使用する Site Recovery Manager アーキテクチャ



# マッピングの構成

## 3

マッピングにより、Site Recovery Manager が保護サイトにある仮想マシンのリソースをリカバリ サイトのリソースにどのようにマッピングするかを指定できます。

サイト全体のマッピングを構成して、保護サイトにある vCenter Server インベントリのオブジェクトを、リカバリ サイトにある vCenter Server インベントリの対応するオブジェクトにマッピングすることができます。

- ネットワーク（リカバリ プラン テストに使用する別のネットワークを指定するオプションを含む）
- データセンターまたは仮想マシンのフォルダ
- コンピューティング リソース（リソース プール、スタンドアロン ホスト、vApp、またはクラスタを含む）

リカバリ中にリカバリ サイトで仮想マシンが起動すると、その仮想マシンは、マッピングで指定したリカバリ サイトのリソースを使用します。双方向の保護と再保護を有効にするには、逆方向のマッピングを構成して、リカバリ サイトのオブジェクトを保護サイトの対応するオブジェクトに戻すことができます。また、逆方向に別のマッピングを構成することで、サイト上のリカバリ済み仮想マシンが、そのサイトにある保護された仮想マシンに対する別のリソースを使用するようにすることもできます。

Site Recovery Manager は、アレイベースの保護グループと vSphere Replication 保護グループ、またはストレージ ポリシー保護グループのどちらを使用するかに応じて異なる方法でインベントリ マッピングを適用します。保護グループのタイプに応じた Site Recovery Manager によるインベントリ マッピングの適用方法の違いについては、[アレイベース レプリケーション保護グループおよび vSphere Replication 保護グループ用のインベントリ マッピング](#)および[ストレージ ポリシー保護グループのインベントリ マッピング](#)を参照してください。

インベントリ オブジェクトのマッピングに加えてストレージ ポリシー保護グループを使用する場合は、保護サイトのストレージ ポリシーをリカバリ サイトのストレージ ポリシーにマッピングします。

この章には、次のトピックが含まれています。

- [アレイベース レプリケーション保護グループおよび vSphere Replication 保護グループ用のインベントリ マッピング](#)
- [ストレージ ポリシー保護グループのインベントリ マッピング](#)
- [インベントリ マッピングの構成](#)
- [ストレージ ポリシーのマッピングについて](#)
- [ストレージ ポリシーのマッピングの選択](#)

## アレイベース レプリケーション保護グループおよび vSphere Replication 保護グループ用のインベントリ マッピング

アレイベースの保護および vSphere Replication の保護の場合、Site Recovery Manager は、保護グループが作成されたときに、そのグループに含まれるすべての仮想マシンに対してインベントリ マッピングを適用します。

Site Recovery Manager は、アレイベースまたは vSphere Replication の保護グループが作成されたときに、ブレースホルダ仮想マシンを作成します。Site Recovery Manager は、ブレースホルダのリソース割り当てをサイト全体のインベントリ マッピングから導出します。

サイト全体のインベントリ マッピングを構成すると、必要に応じてインベントリ マッピングを保護グループに再適用することができます。たとえば、既存の保護グループに新しい仮想マシンを追加する場合などです。

サイトに対するサイト全体のインベントリ マッピングを変更しても、その変更は、Site Recovery Manager が既存の保護グループですでに保護している仮想マシンには影響しません。Site Recovery Manager が、以前保護されていた仮想マシンに新しいマッピングを適用するのは、それらの仮想マシンの保護が再構成された場合のみです。

Site Recovery Manager では、有効なインベントリ マッピングがない仮想マシンは保護できません。ただし、アレイベース レプリケーション保護グループと vSphere Replication 保護グループについては、サイト全体のインベントリ マッピングは必須ではありません。サイト全体の定義済みインベントリ マッピングなしで、アレイベース レプリケーション保護グループまたは vSphere Replication 保護グループを作成した場合は、グループ内の各仮想マシンを個別に構成できます。サイト全体のインベントリ マッピングは、保護グループ内の仮想マシンの保護を構成することで上書きできます。また、保護グループの作成後にサイト全体のインベントリ マッピングを作成し、それらのマッピングを保護グループに対して適用することもできます。

- サイト全体のインベントリ マッピングの構成方法については、[インベントリ マッピングの構成](#)を参照してください。
- 仮想マシンのマッピングを個別に構成する方法については、[アレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成](#)を参照してください。
- サイト全体のインベントリ マッピングを既存の保護グループに適用する方法については、[アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用](#)を参照してください。

ブレースホルダ仮想マシンでは NIC がサポートされていないため、ブレースホルダ仮想マシンのネットワーク構成を変更することはできません。ブレースホルダ仮想マシンのネットワークは、インベントリ マッピングでのみ変更できます。ネットワークのマッピングがない場合、個別の仮想マシンの保護を構成するときにネットワークを指定できます。ブレースホルダ仮想マシンに対する変更によって、仮想マシンの保護を構成するときに作成した設定が上書きされます。Site Recovery Manager は、テスト中やリカバリ中は、この変更をリカバリ サイトで保持します。

## ストレージ ポリシー保護グループのインベントリ マッピング

ストレージ ポリシー保護を使用する場合は、ストレージ ポリシー保護グループを含むリカバリ プランを実行すると、Site Recovery Manager によってインベントリ マッピングが仮想マシンに適用されます。

アレベースの保護グループと vSphere Replication 保護グループを使用する場合は、仮想マシンで保護を構成した時点で、Site Recovery Manager によってインベントリ マッピングが適用されます。ストレージ ポリシー保護グループを使用する場合は、ストレージ ポリシー保護が動的に行われるため、リカバリ プランを実行した時点で、Site Recovery Manager によってインベントリ マッピングが適用されます。仮想マシン配置の決定は、リカバリ プラン実行時のインベントリ マッピングに応じて行われます。そのため、Site Recovery Manager によってリカバリ サイトにプレースホルダ仮想マシンが作成されることはありません。

リカバリ プランを実行すると、Site Recovery Manager によってストレージ ポリシー保護グループのインベントリ マッピングが適用されるため、ストレージ ポリシー保護グループに含まれる仮想マシンに対して個別にマッピングを構成することはできません。ストレージ ポリシー保護を使用してリカバリを実行する場合、Site Recovery Manager は常にサイト全体のインベントリ マッピングを使用します。インベントリ マッピングがない場合、テスト リカバリ、計画移行、およびストレージ ポリシー保護グループを含むリカバリ プランのディザスタ リカバリは失敗します。ストレージ ポリシー保護グループ内の仮想マシンを定期的にポーリングしてマッピングが失われているかを確認し、マッピングの喪失が原因でストレージ ポリシー保護グループをリカバリできなくなる可能性がある場合は警告するように Site Recovery Manager を構成できます。マッピングが失われているか定期的にポーリングするよう構成する方法については、[レプリケーション設定の変更](#)を参照してください。

---

**注：** ネットワーク マッピングはなくても他のマッピングがある状態でテスト リカバリを実行すると、Site Recovery Manager は自動生成されたテスト ネットワークを使用します。テストは成功しますが警告が返されます。ネットワーク マッピングがないことを通知する警告付きでテスト リカバリが成功した場合は、ネットワーク マッピングを構成してテストをやり直してください。計画移行とディザスタ リカバリではテスト ネットワークは使用されないため、ネットワーク マッピングがないとこれらは失敗します。

---

マッピングがないことが原因でリカバリ プランに失敗したものの、保護サイトは使用可能な場合は、足りないマッピングを構成してリカバリ プランを再度実行してください。サイト全体のインベントリ マッピングの構成方法については、[インベントリ マッピングの構成](#)を参照してください。

## リソース インベントリ マッピングおよびストレージ ポリシー保護グループ

動的な仮想マシンの保護の結果として、ストレージ ポリシー保護グループには、リソース インベントリ マッピングの設定方法に関する特定の要件と制限があります。

- Site Recovery Manager では、ストレージ ポリシー保護グループによって保護されているデータストアをマウントした保護サイト上のすべての最上位レベルのコンピューティング リソース（クラスタまたは管理されていないホスト）に対して既存のリソース インベントリ マッピングが必要です。
- Site Recovery Manager は、最上位レベルのコンピューティング リソース マッピングに基づいて、リカバリされたデータストアを表示する必要があるかどうかを決定し、リソース プールのリソース マッピングは考慮しません。
  - 親の最上位レベルのコンピューティング リソースにリソース マッピングがない場合、Site Recovery Manager はリソース プールに既存のマッピングを適用することはできません。
  - 保護サイトのリソース プールの別のリカバリ コンピューティング リソース階層への既存のマッピングは、その親と比較して、そのリソース プールの下にある仮想マシンのストレージをマッピングされたコンピューティング リソースに公開しません。

ストレージ ポリシー保護グループのリカバリを正常に行うには、リソース マッピングを作成するときに次のルールを遵守する必要があります。

- ストレージ ポリシー保護グループによって保護されているデータストアをマウントした、保護されているすべての最上位レベルのコンピューティング リソース (クラスタまたは管理されていないホスト) に対してリソース マッピングを作成します。
- リソース プール用の追加マッピングを作成する必要がある場合は、それらを、その親の最上位レベルの保護されたコンピューティング リソースのマッピング先である、同じ最上位レベルのリカバリ コンピューティング リソースの下ターゲットにマッピングします。たとえば、保護されたホストまたはクラスタ P がリカバリ ホストまたはクラスタ R や R の下のリカバリ リソース プールにマッピングされている場合は、P の下の保護されたすべてのリソース プールも、R または R の下のリカバリ リソース プールにマッピングする必要があります。

## ストレージ ポリシー保護のための一時的なプレースホルダ マッピングについて

リカバリ プランを実行した時点で、Site Recovery Manager によってストレージ ポリシー保護用にインベントリ マッピングが適用されます。インベントリ マッピングを構成していない状態、またはマッピングしたオブジェクトが欠落している状態で、ストレージ ポリシー保護グループを含むリカバリ プランを実行すると、テスト リカバリ、計画移行、およびディザスタ リカバリは失敗します。

インベントリ マッピングは通常、保護サイトとリカバリ サイトを両方とも使用できる場合にのみ構成できます。マッピングがなく、保護サイトが使用できないことが原因で、ストレージ ポリシー保護グループを含むリカバリ プランが失敗した場合、足りないマッピングを通常の方法で構成することはできません。この状況を緩和するため、Site Recovery Manager は、マッピングがなく、保護サイトが使用できないことが原因でリカバリに失敗した場合に、一時的なプレースホルダ マッピングを作成します。一時的なプレースホルダ マッピングにより、足りないマッピングを構成できるため、保護サイトがオフラインのときに正常にリカバリを実行できます。一時的なプレースホルダ マッピングは、リカバリ プランに含まれる仮想マシンが配置された保護サイト上のインベントリ オブジェクトを識別するもので、完全なマッピングではありません。一時的なプレースホルダ マッピングには、リカバリ サイトのターゲット オブジェクトは含まれません。マッピングがなく、保護サイトが使用できないことが原因でリカバリが失敗し、Site Recovery Manager によって一時的なプレースホルダ マッピングが作成された場合は、一時的なプレースホルダ マッピングを完成させて、リカバリを正常に再実行できます。

一時的なプレースホルダ マッピングの構成方法については、[一時的なプレースホルダ マッピングの構成](#)を参照してください。

## 一時的なプレースホルダ マッピングの構成

マッピングがなく、保護サイトが使用できないことが原因で、ストレージ ポリシー保護グループを含むリカバリ プランが失敗すると、Site Recovery Manager によって一時的なプレースホルダ マッピングが作成されます。これらの一時的なプレースホルダ マッピングを完成させることでリカバリが成功します。

リカバリ プランの実行時に、Site Recovery Manager がストレージ ポリシー保護グループの仮想マシンに対してインベントリ マッピングを適用するため、ストレージ ポリシー保護グループにはサイト全体のインベントリ マッピングが必要です。サイト全体のインベントリ マッピングがない場合、リカバリ テスト、計画移行、およびストレージ ポリシー保護グループを含むリカバリ プランのディザスタ リカバリは失敗します。

マッピングがなく、保護サイトは使用できることが原因で、ストレージ ポリシー保護グループを含むリカバリ プランが失敗した場合は、足りないマッピングを通常の方法で構成し、リカバリを再度実行します。サイト全体のインベントリ マッピングの構成方法については、[インベントリ マッピングの構成](#)を参照してください。

マッピングがなく、保護サイトが使用できないことが原因で、ストレージ ポリシー保護グループを含むリカバリ プランが失敗した場合、足りないマッピングを通常の方法で構成することはできません。リカバリを成功させるには、マッピングがないことが原因でリカバリ プランが失敗したときに、Site Recovery Manager が作成する一時的なブレースホルダ マッピングを完成させる必要があります。

#### 前提条件

- 保護サイトは使用できません。
- ストレージ ポリシー保護グループを含むリカバリ プランでディザスタ リカバリを実行済みです。
- リカバリは、インベントリ マッピングがないため失敗しました。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、失敗したリカバリ プランを選択します。
- 4 [リカバリ手順] を選択し、エラー状態の手順を展開します。
- 5 エラー メッセージの上にマウス ポインタを置き、メッセージ全体を表示します。  
 インベントリ マッピングがない場合は、そのマッピングについてのエラーが表示されます。  
 たとえば、リソース マッピングがない場合は、「ブレースホルダ仮想マシンに関連付けられているホストを取得できません。リソース マッピング内にリソース プール「address」のマッピングがありません。」というメッセージが表示されます。
- 6 [サイト ペア] タブを選択し、リカバリ サイトのリモート SRM 接続を確認します。  
 保護サイトがオフラインになっており、Site Recovery Manager によって一時的なブレースホルダ マッピングが作成されたことを通知するメッセージが表示されます。
- 7 [ネットワークのマッピング]、[フォルダ マッピング]、[リソース マッピング]、および [ストレージ ポリシーのマッピング] の各タブをクリックします。  
 マッピングがない場合は、Site Recovery Manager によって保護サイト上のリソースが選択されています。リカバリ サイトでの対応するリソースには、「マッピングが見つかりません」と表示されます。
- 8 一時的なブレースホルダ マッピングを選択し、アイコンをクリックしてマッピングを編集します。
- 9 Site Recovery Manager が選択した保護サイト上のリソースからマッピングするリカバリ サイトのリソースを選択して、[OK] をクリックします。
- 10 [リカバリ プラン] タブをクリックし、失敗したリカバリ プランを選択し、リカバリ プランを再実行します。  
 足りないマッピングをすべて構成すると、リカバリは成功します。足りないマッピングがまだある場合、リカバリは失敗します。
- 11 リカバリが再び失敗した場合は、手順の **手順 4** から **手順 10** までをリカバリが成功するまで繰り返します。



## 次のステップ

保護サイトが再び使用できるようになったら、サイト全体のインベントリ マッピングを通常の方法で構成し、リカバリを再度実行します。これで、Site Recovery Manager は保護サイトでのリカバリ手順を完了できます。

**注：** Site Recovery Manager は一時的なブレースホルダ マッピングを保持しません。構成した一時的なブレースホルダ マッピングは、リカバリ サイトで Site Recovery Manager Server を再起動すると消失します。一時的なブレースホルダ マッピングを構成しなければならなかった場合は、リカバリの実行後に、必ず通常のインベントリ マッピングを構成する必要があります。

## 一時的なブレースホルダ マッピングの構成後に仮想マシンへのアクセス権をユーザーが取得

保護サイトが使用できないときに一時的なブレースホルダ マッピングを完了したユーザーが、本来アクセスできないはずの仮想マシンにアクセスできることがあります。

### 問題

保護サイトは、ディザスタ リカバリの間は使用できなくなり、Site Recovery Manager によって一時的なブレースホルダ マッピングが作成されます。リカバリ プランを実行するユーザーは、一時的なブレースホルダ マッピングを完了して、プランを再実行します。リカバリの完了後、ユーザーは、保護サイトでアクセス権がなかった仮想マシンに、リカバリ サイトでアクセスできるようになっています。

- ユーザーは、保護サイトが使用できないときにディザスタ リカバリを実行します。
- このユーザーには、保護サイトにあるすべてのインベントリ オブジェクトにアクセスする権限がありません。
- Site Recovery Manager は、マッピングの不足を検出し、ユーザーがアクセス権を持たない、保護サイト上のオブジェクトを含む一時的なブレースホルダ マッピングを作成します。
- ユーザーは、保護サイト上のオブジェクトから、自身がアクセスできるリカバリ サイト上のオブジェクトへのターゲット マッピングを構成します。
- リカバリ後、リカバリされた仮想マシンで、ユーザーがアクセス権を持つリカバリ サイトのリソースが使用されているため、それらの仮想マシンが保護サイト上にあったときにアクセス権がなかった仮想マシンにアクセスできるようになります。

### 原因

保護サイトが使用できない場合、Site Recovery Manager は、保護サイト上のインベントリ オブジェクトを使用して一時的なブレースホルダ マッピングを作成するまで、それらのオブジェクトの権限チェックを実行できません。

### 解決方法

リカバリ プランの実行権限を持つユーザーに、両方のサイトにあるすべてのオブジェクトへのアクセス権も付与されていることを確認します。

## インベントリ マッピングの構成

インベントリ マッピングは、リカバリ サイトのインベントリにデフォルト オブジェクトを提供し、リカバリの実行時に、リカバリされる仮想マシンによって使用されます。

アレイベースの保護および vSphere Replication 保護で、保護グループの作成前にサイト全体のインベントリ マッピングを構成する場合は、保護グループの作成時に各仮想マシンで個別に保護を構成する必要はありません。Site Recovery Manager は、保護グループの作成時に、アレイベース レプリケーション保護グループまたは vSphere Replication 保護グループ内のすべての仮想マシンにサイト全体のマッピングを適用します。

ストレージ ポリシー保護を使用する場合、Site Recovery Manager はリカバリ プランの実行時にインベントリ マッピングを適用します。ストレージ ポリシー保護グループに含まれる仮想マシンに、保護を個別に構成することはできません。結果として、ストレージ ポリシー保護を使用する場合は、サイト全体のインベントリ マッピングの構成が必要になります。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで [構成] を展開し、構成するリソースの種類を選択します。

オプション	操作
ネットワークのマッピング	保護サイトのネットワークをリカバリ サイトのネットワークにマッピングします。
フォルダ マッピング	保護サイトのデータセンターまたは仮想マシンのフォルダを、リカバリ サイトのデータセンターまたは仮想マシンのフォルダにマッピングします。
リソース マッピング	保護サイトのリソース プール、スタンドアロン ホスト、vApp、またはクラスタを、リカバリ サイトのリソース プール、スタンドアロン ホスト、vApp、またはクラスタにマッピングします。一方のサイトの任意のタイプのリソースを、他方のサイトの任意のタイプのリソースにマッピングできます。  <b>注：</b> クラスタの一部である個々のホストを他のリソース オブジェクトにマッピングすることはできません。

- 4 [新規] をクリックして新しいマッピングを作成します。
- 5 マッピングの作成を自動で行うか、手動で行うかを選択して、[次へ] をクリックします。

この手順は、ネットワーク マッピングとフォルダ マッピングにのみ当てはまります。自動マッピングはネットワークとフォルダ マッピングのみに使用できます。リソース マッピングの構成は手動で行う必要があります。

オプション	説明
自動	Site Recovery Manager により、自動的に保護サイトのネットワークとフォルダが同一の名前を持つリカバリ サイトのネットワークとフォルダにマッピングされます。
手動	保護サイトの特定のネットワークとフォルダをリカバリ サイトの特定のネットワーク、フォルダおよびリソースにマッピングします。

- 6 保護サイトの項目を選択し、リカバリ サイトの項目へマッピングします。
  - 自動マッピングを選択した場合は、左のインベントリ項目を展開してローカル サイトの親ノード（例：データセンターまたはフォルダ）を選択してから、右のインベントリ項目を展開してリモート サイトの親ノードを選択します。



- 手動マッピングを選択した場合、左のインベントリ項目を展開し、ローカル サイトの特定のオブジェクトを選択し、次に右のインベントリ項目を展開し、このオブジェクトをマッピングするリモート サイトのオブジェクトを選択します。

手動マッピングを選択する場合、ローカル サイトの複数項目をリモート サイトの単一項目へマッピングできます。リモート サイトでは一度に1つの項目のみを選択できます。

**注：** NSX ユニバーサル ワイヤへの自動マッピングは、ストレージ ポリシー保護グループでのみサポートされます。仮想マシン保護グループを使用している場合に、仮想マシンが同じユニバーサル ワイヤにリカバリされるようにするには、ユニバーサル ワイヤの両端の間のネットワーク マッピングを明示的に構成する必要があります。[Site Recovery Manager と NSX Data Center for vSphere の使用](#) を参照してください。

- 7 [マッピングの追加] をクリックします。

マッピングは、ページ下に表示されます。自動マッピングを選択した場合、Site Recovery Manager により、保護サイトで選択したノード下のすべての項目が、リカバリ サイトで選択したノード下の同一の名前を持つ項目に自動的にマッピングされます。

- 8 [次へ] をクリックします。

- 9 (オプション) ネットワーク マッピングを構成している場合は、[テスト ネットワークを選択します] ページの [テスト ネットワーク] 列のネットワークをクリックし、ドロップダウン メニューを使用して、リカバリ プランのテストに使用するネットワークを選択します。

Site Recovery Manager を構成して、リカバリ プランのテスト用に、分離されたネットワークをリカバリ サイト上に作成することができます。分離されたテスト ネットワークを作成することで、リカバリ サイト上の本番ネットワークにトラフィックを追加せずにテストを進めることが可能になります。

- [分離されたネットワーク (自動作成)] を選択して、リカバリ サイト上に、テストに使用するための分離されたネットワークを自動的に作成します。これはデフォルトのオプションです。
- リカバリ サイトの既存のネットワークを選択してテストに使用します。

- 10 (オプション) [逆方向のマッピングを準備] ページでマッピングのチェック ボックスを選択します。

このオプションを選択すると、リモート サイトの項目からローカル サイトの項目に、対応するマッピングが作成されます。双方向の保護を確立し、再保護操作を実行するには、逆方向のマッピングが必要です。複数のマッピングがリモート サイト上に同じターゲットを持つ場合、このオプションは選択できません。

- 11 [終了] をクリックして、マッピングを作成します。

- 12 手順 3 から 手順 11 を繰り返して、残りのリソース タイプのマッピングを確立します。

## ストレージ ポリシーのマッピングについて

ストレージ ポリシーに関連付けた仮想マシンは、ストレージ ポリシー保護グループに含めることで保護できます。

ストレージ ポリシーは、vCenter Server のインベントリやデータストアにある仮想マシンを、vCenter Server で定義したルールやタグに従って配置します。ストレージ ポリシーを使用することで、vCenter Server 環境の変更に合わせて、仮想マシンをインベントリ内で移動したり、別のデータストアに移動できます。

保護サイトにあるストレージ ポリシーをリカバリ サイトにあるストレージ ポリシーにマッピングすると、リカバリ プランの実行時に Site Recovery Manager は、リカバリ サイト上のマッピングしたストレージ ポリシーに従って、リカバリ サイトの vCenter Server インベントリやデータストアに、リカバリした仮想マシンを配置します。

## ストレージ ポリシーのマッピングの選択

保護サイトにあるストレージ ポリシーをリカバリ サイトにあるストレージ ポリシーにマッピングすると、リカバリ プランの実行時に Site Recovery Manager は、リカバリ サイト上のマッピングしたストレージ ポリシーに従って、リカバリ サイトの vCenter Server インベントリやデータストアに、リカバリした仮想マシンを配置できます。

### 前提条件

保護サイトとリカバリ サイトの両方にストレージ ポリシーが作成されています。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[構成] - [ストレージ ポリシーのマッピング] の順にクリックします。
- 4 サイトを選択し、[新規] をクリックしてマッピングを作成します。
- 5 マッピングの作成を自動で行うか、手動で行うかを選択して、[次へ] をクリックします。

オプション	説明
名前が一致するストレージ ポリシーのマッピングを自動的に準備する	Site Recovery Manager は、保護サイトのストレージ ポリシーを、リカバリ サイトにある同じ名前のストレージ ポリシーに自動的にマッピングします。
マッピングを手動で準備する	保護サイトの特定のストレージ ポリシーを、リカバリ サイトの特定のストレージ ポリシーにマッピングします。

- 6 保護サイトのストレージ ポリシーを選択し、リカバリ サイトのストレージ ポリシーにマッピングします。
  - 自動マッピングを選択した場合、Site Recovery Manager は、リカバリ サイトに同じ名前のストレージ ポリシーがある保護サイトで、任意のストレージ ポリシーを選択します。
  - 手動マッピングを選択した場合は、保護サイトの特定のストレージ ポリシーを選択し、次にこのストレージ ポリシーのマッピング対象となる、リカバリ サイト上のストレージ ポリシーを選択します。

手動マッピングを選択する場合、ローカル サイトの複数のストレージ ポリシーをリモート サイトの単一のストレージ ポリシーにマッピングできます。リモート サイトでは一度に 1 つの項目のみを選択できます。

- 7 [マッピングの追加] をクリックします。  
マッピングは、ページ下に表示されます。
- 8 [次へ] をクリックします。

- 9 (オプション) [逆方向のマッピング] ページでマッピングのチェック ボックスを選択し、[次へ] をクリックします。

このオプションを選択すると、リモート サイトのストレージ ポリシーからローカル サイトのストレージ ポリシーに、対応するマッピングが作成されます。双方向の保護を確立し、再保護操作を実行するには、逆方向のマッピングが必要です。複数のマッピングがリモート サイト上に同じターゲットを持つ場合、このオプションは選択できません。

- 10 [終了] をクリックして、マッピングを作成します。

# ブレースホルダ仮想マシンについて

# 4

データストア グループを含むアレイベース レプリケーション保護グループ、または個別の仮想マシンを含む vSphere Replication 保護グループを作成する場合、Site Recovery Manager は、保護グループ内の各仮想マシン用のブレースホルダ仮想マシンをリカバリ サイトで作成します。

ブレースホルダ仮想マシンは、仮想マシン ファイルのサブセットです。Site Recovery Manager は、このファイルのサブセットを使用して、リカバリ サイトの vCenter Server に仮想マシンを登録します。

ブレースホルダ仮想マシンのファイルはサイズがきわめて小さく、保護された仮想マシンの全コピーを表しているわけではありません。ブレースホルダ仮想マシンには、ディスクは接続されていません。ブレースホルダ仮想マシンは、リカバリ サイトにコンピューティング リソースを保持するほか、リカバリ実行時に、保護された仮想マシンがリカバリされる vCenter Server インベントリでの位置を指定します。

リカバリ サイトのインベントリにおけるブレースホルダ仮想マシンの有無は、vCenter Server 管理者にとって、仮想マシンが Site Recovery Manager によって保護されているかどうかの指標となります。また、ブレースホルダによって、vCenter Server 管理者は、Site Recovery Manager でのリカバリ プランのテストまたは実行時に、仮想マシンのパワーオンとローカル リソースの使用を開始できることがわかります。

保護された仮想マシンがリカバリ プランのテストまたは実行によりリカバリされると、Site Recovery Manager は、そのブレースホルダをリカバリした仮想マシンで置き換え、リカバリ プランの設定にしたがってパワーオンします。リカバリ プランのテストが完了すると、Site Recovery Manager は、クリーンアップ処理の一部として、ブレースホルダをリストアし、リカバリされた仮想マシンをパワーオフします。

---

**注：** Site Recovery Manager では、ストレージ ポリシー保護グループ用のブレースホルダ仮想マシンは作成されません。ストレージ ポリシー保護グループを使用している場合に、Site Recovery Manager が仮想マシンをリカバリ サイトにどのように配置するかについては、[ストレージ ポリシー保護グループのインベントリ マッピング](#) および [ストレージ ポリシーのマッピングについて](#) を参照してください。

---

## ブレースホルダ仮想マシン テンプレートについて

保護サイトのテンプレートを保護すると、Site Recovery Manager は、コンピューティング リソースのデフォルトのリソース プールに仮想マシンを作成し、その仮想マシンをテンプレートとしてマークして、ブレースホルダ テンプレートを作成します。Site Recovery Manager は、保護サイト上の仮想マシンのフォルダがマッピングされた、リカバリ サイト上のデータセンター内にある利用可能な一連のコンピューティング リソースからコンピューティング リソースを選択します。選択されたコンピューティング リソース内のすべてのホストは、1 つ以上のブレースホルダ データストアにアクセスする必要があります。コンピューティング リソース内の 1 台以上のホストで、保護される仮想マシン テンプレートのハードウェア バージョンがサポートされている必要があります。

## ブレースホルダ データストアについて

アレイベース レプリケーションを使用してデータストア グループを保護する場合、または vSphere Replication を使用して個別の仮想マシンを保護する場合は、Site Recovery Manager がブレースホルダ仮想マシン ファイルを保存する、リカバリ サイト上のデータストアを特定する必要があります。

**注：** Site Recovery Manager では、ストレージ ポリシー保護グループ用のブレースホルダ仮想マシンは作成されません。ストレージ ポリシー保護グループのみを使用している場合は、ブレースホルダ データストアを特定する必要はありません。

ブレースホルダ仮想マシン ファイルはサイズがきわめて小さいため、ブレースホルダ データストアは、すべての仮想マシンを収容できる大きさでなくてもかまいません。

計画された移行および再保護を有効にするには、両方のサイトでブレースホルダ データストアを選択する必要があります。

この章には、次のトピックが含まれています。

- [リカバリ中のブレースホルダ仮想マシンへの処理](#)
- [ブレースホルダ データストアの選択](#)

## リカバリ中のブレースホルダ仮想マシンへの処理

アレイベースの保護グループと vSphere Replication 保護グループを作成するときに、Site Recovery Manager はリカバリ サイト上にブレースホルダ仮想マシンを作成します。これらの保護グループが含まれるリカバリ プランを実行すると、Site Recovery Manager はこれらのブレースホルダを実際の仮想マシンに置き換えます。

**注：** Site Recovery Manager では、ストレージ ポリシー保護グループ用のブレースホルダ仮想マシンは作成されません。この例は、アレイベースの保護グループと vSphere Replication 保護グループに該当します。ストレージ ポリシー保護グループには当てはまりません。ストレージ ポリシー保護グループを使用する場合に、Site Recovery Manager が仮想マシンをリカバリする方法の詳細については、[ストレージ ポリシー保護グループについて](#)を参照してください。

この例では、アレイベースの保護グループと vSphere Replication 保護グループを含むリカバリ プランを実行するときに、Site Recovery Manager がリカバリ サイトのブレースホルダ仮想マシンを実際の仮想マシンに置き換えるプロセスを示しています。

- 1 仮想マシンは、使用されているレプリケーションのタイプに応じて、Site Recovery Manager から独立してリカバリ サイトにレプリケートされます。
  - データストアベースのレプリケーションの場合、ストレージ アレイは、仮想マシンのファイルを Raw ストレージとして格納しているデータストアを、ターゲットのストレージ アレイにレプリケートします。
  - vSphere Replication は、vSphere Replication ターゲットとして構成したデータストアに仮想マシンのコピーを作成することで、各仮想マシンをレプリケートします。これらの仮想マシンのコピーはパワーオンされません。
- 2 Site Recovery Manager がブレースホルダ仮想マシン ファイルの格納に使用する、リカバリ サイト上のデータストアを指定します。

- 3 データストア グループを追加するか、個別の仮想マシンを保護グループに追加して、Site Recovery Manager の保護を仮想マシンに構成する際に、Site Recovery Manager は、リカバリ サイトのブレースホルダ データストア内にその仮想マシンのブレースホルダを作成します。
- 4 リカバリ プランを実行するときに、Site Recovery Manager は保護サイトの仮想マシンをシャットダウンし、使用されているレプリケーションのタイプに応じてリカバリ サイトの仮想マシンをアクティブ化します。
  - データストアベースのレプリケーションの場合、Site Recovery Manager は、レプリケートされた仮想マシンを vCenter Server データストアとして格納するリカバリ サイトの Raw ストレージを検出します。Site Recovery Manager は、ブレースホルダ データストアが登録されている ESXi ホストまたはクラスタに、リカバリされたデータストアを登録します。
  - vSphere Replication は、リカバリ サイトの仮想マシンのコピーをパワーオンします。
- 5 Site Recovery Manager は、ブレースホルダ仮想マシンの ID を、リカバリ サイトで検出された、レプリケートされた仮想マシンとスワップするように vCenter Server に要求を送信します。

## ブレースホルダ データストアの選択

アレイベースの保護グループまたは vSphere Replication 保護グループを使用している場合は、ブレースホルダ仮想マシンを保存するために使用する Site Recovery Manager 用のブレースホルダ データストアをリカバリ サイトで指定する必要があります。

ペアの両方のサイトでブレースホルダ データストアを構成して、双方向の保護を確立し、再保護を実行する必要があります。

---

**注：** Site Recovery Manager では、ストレージ ポリシー保護グループ用のブレースホルダ仮想マシンは作成されません。ストレージ ポリシー保護グループのみを使用している場合は、ブレースホルダ データストアを選択する必要はありません。

---

### 前提条件

- 保護サイトと復旧サイトの接続およびペアリングが完了していることを確認します。
- ブレースホルダ データストアは一定の基準を満たしている必要があります。
  - クラスタの場合、クラスタ内のすべてのホストからブレースホルダ データストアを認識できる必要があります。
  - アレイベース レプリケーションを使用してレプリケートされたデータストアを、ブレースホルダ データストアとして選択することはできません。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[構成] - [ブレースホルダ データストア] を選択します。
- 4 サイトを選択し、[新規] をクリックして、ブレースホルダ データストアを構成します。

- 5 ローカル サイトでプレースホルダ仮想マシンの場所として指定するデータストアを選択し、[OK] をクリックします。

事前に構成されているデータストアが表示されますが、選択することはできません。データストアがレプリケートされ、Site Recovery Manager にそのデータストアのアレイ マネージャがない場合、レプリケートされるデータストアを選択するオプションが使用できる場合があります。Site Recovery Manager が管理していないレプリケートされたデータストアは選択しないでください。

---

**重要：** vSphere Replication を使用する場合は、レプリケーションのターゲット データストアとしてすでに使用しているプレースホルダ データストアを選択できます。同じデータストアを使用する場合、Site Recovery Manager はレプリケーション ターゲットの名前を使用し、サフィックス (1) を追加してプレースホルダ仮想マシンを作成します。vSphere Replication 保護グループについては、[vSphere Replication 保護グループ](#)を参照してください。同じデータストアを選択すると、レプリケーション ターゲットとプレースホルダ仮想マシンを区別する際に混乱することがあります。混乱を避けるためのベスト プラクティスは、個別のデータストアを使用することです。

プレースホルダ データストアが vSphere Replication のレプリカのターゲット データストアと同じストレージ DRS クラスタにないことを確認してください。

---

**注：** vSphere Replication を使用して、仮想マシンのレプリケーションを構成または再構成する場合は、プレースホルダ仮想マシン フォルダを仮想マシンのレプリケーション フォルダとして設定しないでください。

---

- 6 ペアのもう一方のサイトを選択します。
- 7 [手順 3](#) から[手順 5](#) までを繰り返し、もう一方のサイトのプレースホルダ データストアを構成します。



# 保護グループの作成および管理

## 5

レプリケーション ソリューションを構成した後、保護グループを作成できます。保護グループは、Site Recovery Manager によってまとめて保護される仮想マシンの集合です。

リカバリ 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。リカバリ プランでは、保護グループ内の仮想マシンを Site Recovery Manager がリカバリする方法を指定します。

仮想マシンの構成と保護グループの作成は、アレイベース レプリケーション、vSphere Replication、ストレージ ポリシー保護のどれを使用するかによって異なります。アレイベース レプリケーションを構成した仮想マシンと、vSphere Replication またはストレージ ポリシー保護を構成した仮想マシンを組み合わせた保護グループは作成できません。アレイベース レプリケーション保護グループと vSphere Replication 保護グループの組み合わせは同じリカバリ プランに含めることができます。アレイベース レプリケーション保護グループおよび vSphere Replication 保護グループと同じリカバリ プランに、ストレージ ポリシー保護グループを含めることはできません。

仮想マシンでレプリケーションを構成したら、リカバリ サイトの既存のリソース プール、フォルダ、ネットワークに各仮想マシンを割り当てる必要があります。インベントリ マッピングを選択して、サイト全体に適用されるデフォルト設定をこれらの割り当てに指定できます。アレイベース レプリケーション保護グループと vSphere Replication 保護グループに対し、インベントリ マッピングを指定しない場合は、保護グループ内の仮想マシンに個別にマッピングを構成します。ストレージ ポリシー保護グループ内の仮想マシンに個別にマッピングを構成することはできないため、ストレージ ポリシー保護グループを使用する場合は、サイト全体のインベントリ マッピングを構成します。

アレイベース レプリケーション保護グループまたは vSphere Replication 保護グループを作成すると、Site Recovery Manager によってプレースホルダ仮想マシンがリカバリ サイトに作成され、グループ内の各仮想マシンにインベントリ マッピングが適用されます。Site Recovery Manager によってリカバリ サイトのフォルダ、ネットワーク、またはリソース プールに仮想マシンをマッピングできない場合、Site Recovery Manager 仮想マシンは [マッピングがありません] ステータスに設定され、そのプレースホルダは作成されません。ストレージ ポリシー保護グループについては、リカバリ プランの実行時に、Site Recovery Manager によってインベントリ マッピングが適用されます。Site Recovery Manager では、ストレージ ポリシー保護グループ用のプレースホルダ仮想マシンは作成されません。

Site Recovery Manager は、レプリケーションが構成されていないか誤って構成されている仮想マシンを保護することはできません。アレイベースのレプリケーションの場合、仮想マシンが保護データベース上にあっても保護できません。

この章には、次のトピックが含まれています。

- [アレイベース レプリケーション保護グループとデータストア グループについて](#)
- [vSphere Replication 保護グループ](#)



- ストレージ ポリシー保護グループについて
- 暗号化された仮想マシンの保護
- 保護グループの状態の概要
- 仮想マシンの保護状態の概要
- 保護グループの作成
- フォルダ内の保護グループの整理
- データストア グループまたは仮想マシンの保護グループへの追加および保護グループからの削除
- アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用
- アレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成
- アレイベース保護グループまたは vSphere Replication 保護グループ内の仮想マシンの設定の変更
- 仮想マシンからの保護の削除

## アレイベース レプリケーション保護グループとデータストア グループについて

アレイベース レプリケーションの保護グループを作成するときに、アレイ情報を指定すると、Site Recovery Manager はデータストア グループへの仮想マシンのセットを計算します。データストア グループには、保護される仮想マシンのすべてのファイルが含まれます。

仮想マシンをアレイベース レプリケーション保護グループに追加します。それには、Site Recovery Manager が保護グループに関連付けるデータストア グループに所属するデータストアに仮想マシンを配置します。Site Recovery Manager は、保護仮想マシンの変更を検出すると、データストア グループを再計算します。たとえば、別の LUN 上にあるハード ディスクを保護仮想マシンに追加すると、Site Recovery Manager はその LUN を、その保護グループのデータストア グループに追加します。新しい LUN を保護するように保護を再構成する必要があります。Site Recovery Manager は、アレイ ペアを構成するとき、またはデバイスのリストを更新するときに整合性グループを計算します。

また、Storage vMotion を使用することで、データストア グループに属するいずれか 1 つのデータストアに仮想マシンのファイルを移動して、仮想マシンを保護グループに追加することもできます。仮想マシンのファイルを別のデータストアに移動することで、仮想マシンをアレイベース レプリケーション保護グループから削除することができます。

暗号化された仮想マシンは、アレイベース レプリケーション保護グループを使用することで保護およびリカバリができます。暗号化された仮想マシンの、アレイベース レプリケーションによる保護とリカバリには、VMware vSphere 6.7 以降が必要です。

ストレージ アレイで整合性グループがサポートされている場合、Site Recovery Manager は vSphere Storage DRS および vSphere Storage vMotion との互換性があります。Storage DRS と Storage vMotion を使用して、Site Recovery Manager によって保護されている整合性グループ内に仮想マシン ファイルを移動できます。ストレージ アレイで整合性グループがサポートされていない場合、Storage DRS と Storage vMotion を Site Recovery Manager と組み合わせて使用することはできません。

## Site Recovery Manager によるデータストア グループの計算方法

Site Recovery Manager は、グループ内のデータストアにファイルを持つ一連の仮想マシン、およびこれらのデータストアの保存先デバイスによって、データストア グループの構成を判別します。

アレイベース レプリケーションを使用する場合、各ストレージ アレイはレプリケートされる一連のデータストアをサポートします。ファイバ チャネルや iSCSI などの接続プロトコルを使用するストレージ エリア ネットワーク (SAN) では、これらのデータストアは LUN (Logical Storage Units) と呼ばれ、1 つ以上の物理データストアで構成されます。NFS (ネットワーク ファイル システム) アレイでは、レプリケートされたデータストアを一般にボリュームと呼びます。レプリケートされるストレージ デバイスの各ペアでは、1 つのデータストアがレプリケーション ソースで、もう 1 つのデータストアがレプリケーション ターゲットです。ソース データストアに書き込まれたデータは、アレイのレプリケーション ソフトウェアによって制御されるスケジュールでターゲット データストアにレプリケートされます。ストレージ レプリケーション アダプタ (SRA) と連携するように Site Recovery Manager を構成すると、レプリケーション ソースが保護サイトに、レプリケーション ターゲットがリカバリ サイトになります。

データストアには、仮想マシン ファイルのためのストレージがあります。物理ストレージ デバイスの詳細を隠すことで、データストアはストレージ容量の割り当てを簡素化し、仮想マシンのストレージ ニーズを満たすための同一のモデルを提供します。データストアは複数のデバイスにまたがる可能性があるため、Site Recovery Manager は、データストアをバックアップするすべてのデバイスがレプリケートされていることを確認してからでないと、そのデータストアを使用する仮想マシンを保護できません。Site Recovery Manager は、保護された仮想マシン ファイルを含むすべてのデータストアが確実にレプリケートされるようにする必要があります。リカバリまたはテスト中、Site Recovery Manager はそのようなデータストアをすべて同時に処理する必要があります。

これを実現するには、Site Recovery Manager は複数のデータストアにまたがる仮想マシンに対応するために、データストアをデータストア グループに統合します。Site Recovery Manager は、適切な仮想マシンを保護できるようにデータストア グループに必要なデータストアがすべて含まれているかを定期的にチェックし、確認します。必要な場合、Site Recovery Manager はデータストア グループを再計算します。たとえば、新しいデバイスを仮想マシンに追加し、以前はデータストア グループに含まれていなかったデータストアにそれらのデバイスを保存するような場合に再計算が行われます。

データストア グループは必要な数のデータストアで構成されています。仮想マシンの一部のファイルがグループ内の 1 データストアに保存されている場合、そのすべてのファイルが同じグループの一部であるデータストアに保存されるのを確保するためのデータストア数は、必要な数の最小数です。たとえば、ある仮想マシンのディスクが 2 つの異なるデータストアにある場合、Site Recovery Manager は両方のデータストアを 1 つのデータストア グループに結合します。Site Recovery Manager は、設定された基準に従って、デバイスをデータストア グループに結合します。

- 2 つの異なるデータストアに、同じ仮想マシンに属するファイルが含まれている。
- Microsoft Cluster Server (MSCS) クラスタの場合と同様に、2 つの仮想マシンに属するデータストアが、1 つの SAN アレイにある Raw ディスク マッピング (RDM) を共有している。

- 2つのデータストアが、同じデバイスの異なるパーティションに対応するエクステントにまたがっている。
- 1つのデータストアが、2つの異なるデバイスのパーティションに対応する2つのエクステントにまたがっている。2つのエクステントは、1つの整合性グループ内に存在する必要があります。また、SRAは、デバイス検出ストレージ内のアレイから整合性グループ情報を報告する必要があります。そうしなければ、SRAがこのデータストアを作成したエクステントがレプリケートされたことを報告しても、このデータストアに基づく保護グループを作成することができません。
- 複数のデータストアが整合性グループに属している。整合性グループは、データストアのターゲットセットのすべての状態がある時点でデータストアのソースセットの状態として存在した、レプリケートされたデータストアの集合です。非公式には、データストアを使用してリカバリが行われるとき、ターゲットにアクセスするソフトウェアが、そのソフトウェアで処理する準備ができていない状態のデータを見ることがないようにして、それらのデータストアがまとめてレプリケートされます。

## 複数の LUN またはエクステントにまたがる VMFS データストア上の仮想マシンの保護

すべてのストレージアレイが整合性グループをサポートしているわけではないため、すべてのSRAがストレージアレイから整合性グループ情報を報告するわけではありません。データストア検出コマンドの後にSRAがアレイからの整合性グループ情報を報告する場合、マルチエクステントVMFSデータストアを構成するLUNは、同じストレージアレイの整合性グループ内に存在しなければなりません。アレイが整合性グループをサポートしておらず、SRAが整合性グループ情報を報告しない場合は、Site Recovery Managerはマルチエクステントデータストア上にある仮想マシンを保護することができません。

## vSphere Replication 保護グループ

vSphere Replication 用に構成した仮想マシンを vSphere Replication 保護グループに含めることができます。

vSphere Replication 保護グループを作成または編集する際に、vSphere Replication 用に構成された、vCenter Server インベントリ内の仮想マシンを選択できます。

仮想マシンで vSphere Replication を構成する場合、リモートサイトのデータストア上のターゲット場所を選択します。vSphere Replication を構成した仮想マシンを保護グループに含めると、Site Recovery Manager によって、リカバリ用のブレースホルダ仮想マシンが作成されます。vSphere Replication のレプリケーションターゲットと Site Recovery Manager が両方に対して作成するブレースホルダ仮想マシンは、リカバリサイト上の同じデータストア上に配置できます。これは、これらが異なるデータストアフォルダに作成されるためです。レプリケーションターゲットとブレースホルダ仮想マシンが同じデータストア内にある場合、Site Recovery Manager は、サフィックス (1) の付いたレプリケーションターゲット名を使って、ブレースホルダ仮想マシンの名前を作成します。混乱を避けるため、vSphere Replication のレプリケーションターゲット用と Site Recovery Manager のブレースホルダ仮想マシン用にそれぞれ個別のデータストアを使用することをお勧めします。Site Recovery Manager は、リカバリサイトのブレースホルダ仮想マシンにインベントリマッピングを適用します。

---

**注：** vSphere Replication を使用して、仮想マシンのレプリケーションを構成または再構成する場合は、ブレースホルダ仮想マシンフォルダを仮想マシンのレプリケーションフォルダとして設定しないでください。

---

ユーザーが vSphere Replication を仮想マシンに構成したときに設定した目標リカバリ時点に従って、レプリケーション ターゲット仮想マシンのディスク ファイルは vSphere Replication によって同期されます。Site Recovery Manager でリカバリを実行すると、Site Recovery Manager によってレプリケーション ターゲット仮想マシンがパワーオンされて、プレースホルダ仮想マシンの代わりにリカバリ サイトの vCenter Server に登録されます。

vSphere Replication 保護グループを使用する場合、Site Recovery Manager は vSphere Replication に依存しますが、vSphere Replication は Site Recovery Manager に依存しません。vSphere Replication は、Site Recovery Manager とは個別に使用することができます。たとえば、vSphere Replication を使って vCenter Server インベントリ内のすべての仮想マシンをレプリケートできますが、これらの仮想マシンの一部だけを保護グループに含めることができます。vSphere Replication 構成を変更すると、保護グループに含めた仮想マシンの Site Recovery Manager の保護に影響が生じることがあります。

- Site Recovery Manager は、vSphere Replication 保護グループ内の仮想マシンの vSphere Replication ステータスを監視します。レプリケーションが保護グループ内の仮想マシンに対して機能していないと、Site Recovery Manager はその仮想マシンをリカバリすることはできません。
- 仮想マシンで vSphere Replication の構成を解除しても、ユーザーが追加した保護グループ内の仮想マシンは Site Recovery Manager 内にそのまま残ります。ただし、レプリケーションを再構成するまで、Site Recovery Manager はその仮想マシンをリカバリできません。仮想マシンで vSphere Replication の構成を解除する場合、その仮想マシンを保護グループから手動で削除できます。
- Site Recovery Manager によってアレイベースのレプリケーションですでに保護されたデータストア上の仮想マシンに対して、vSphere Replication を構成した場合、その仮想マシンを vSphere Replication 保護グループに含めようとすると、Site Recovery Manager によってエラーが報告されます。

vSphere Replication を構成した仮想マシンを保護グループから削除しても、vSphere Replication は引き続き、仮想マシンをリカバリ サイトにレプリケートします。関連リカバリ プランを実行する場合、その仮想マシンは保護グループ内の他の仮想マシンとともにリカバリされません。

## ストレージ ポリシー保護グループについて

ストレージ ポリシー保護グループにより、ストレージ ポリシーに関連付けられた仮想マシンを自動的に保護することができます。

データストアを保護サイトからリカバリ サイトにレプリケートするには、アレイベース レプリケーションを使用します。データストアにタグを付け、そのタグにマッピングしたストレージ ポリシーを作成すると、データストアは、そのストレージ ポリシーに自動的に関連付けられます。そのストレージ ポリシーを含むストレージ ポリシー保護グループは、データストアにある適切にタグ付けされたすべての仮想マシンを自動的に保護します。仮想マシンとストレージ ポリシーの関連付けを解除したり、仮想マシンをデータストアから削除すると、Site Recovery Manager はその仮想マシンの保護を自動的に解除します。

ストレージ ポリシー保護グループを作成する際、Site Recovery Manager は次の操作を実行します。

- ローカルの Site Recovery Manager Server インスタンスで、ストレージ ポリシー保護グループを表す管理対象オブジェクトを作成します。
- 選択したストレージ ポリシーをストレージ ポリシー保護グループに関連付けます。Site Recovery Manager は、ストレージ ポリシー保護グループに含めた、すべての準拠ストレージ ポリシーを保護します。

- ローカルのストレージ ポリシー保護グループは、ローカルの vCenter Server インスタンスにある適切な vSphere エンティティをアクティブに保護し、そのグループに含まれるストレージ ポリシーの準拠性を決定します。新規作成されたストレージ ポリシー保護グループによる初期の保護には、vSphere インベントリの既知の最新状態に基づいて、保護グループ内のストレージ ポリシーに関連付けられたすべての仮想マシンを保護することが含まれます。

**注：** 初期の保護には、関連する整合性グループについてのストレージ同期は含まれません。ストレージは、vSphere や Site Recovery Manager とは関係なく、ストレージの通常スケジュールに従ってレプリケートする必要があります。

- vSphere インベントリの監視を開始して、初期の保護以降にインベントリに追加された vSphere エンティティを検出します。Site Recovery Manager が vSphere エンティティの保護に失敗しても、ストレージ ポリシー保護グループの作成は失敗しませんが、保護グループのプロパティにエラーが表示されます。
- リカバリ サイトの Site Recovery Manager Server インスタンスで、ストレージ ポリシー保護グループを表すピア管理オブジェクトを作成します。このオブジェクトは、基盤となるストレージをリカバリする準備ができていなくても、作成直後からリカバリできます。

ストレージ ポリシー保護グループの作成後、保護されている vSphere のエンティティを確実にリカバリ可能にするため、基盤となるストレージを同期することが必要になる場合があります。保護グループを作成した直後に、最近行われた変更をレプリケートするオプションを指定して、テスト リカバリを実行してください。

## ストレージ ポリシー保護グループの前提条件

ストレージ ポリシー保護グループを作成する際は、まずストレージ ポリシーを作成し、使用中の環境が特定の前提条件を満たしていることを確認する必要があります。

### 前提条件

- データストア タグを作成してデータストアに割り当て、ストレージ ポリシーに関連付けます。
  - 環境で拡張リンク モードを使用しない場合は、保護サイトとリカバリ サイトの両方にタグ カテゴリとタグを作成して、保護サイトで保護対象とするデータストアに割り当てます。
  - 環境で拡張リンク モードを使用する場合は、保護サイトにのみタグ カテゴリとタグを作成します。これらのタグは、拡張リンク モード環境内の他の vCenter Server インスタンスにレプリケートされます。
- 両方のサイトの vCenter Server で仮想マシンのストレージ ポリシーを作成します。このポリシーには、保護対象のデータストアに割り当てたタグが含まれます。環境で拡張リンク モードが使用されている場合も、両方のサイトで仮想マシン ポリシーを作成します。各サイトのストレージ ポリシーには、異なる名前を付けることができます。
- 保護サイト上で保護対象の仮想マシンに適切なストレージ ポリシーを関連付けます。仮想マシンのすべてのディスクに同じストレージ ポリシーを関連付ける必要があります。
- アレイ ベンダーが提供するレプリケーション テクノロジーを使用して、保護サイトからリカバリ サイトへの、データストアのアレイベース レプリケーションを構成します。

- Site Recovery Manager でインベントリ マッピングを構成します。ストレージ ポリシー保護グループには、インベントリ マッピングの適用に関する特定の動作と、リソース インベントリ マッピングの設定方法に関する要件があります。たとえば、ストレージ ポリシー保護グループを使用していてマッピングを構成していない場合、計画移行またはディザスタ リカバリは失敗し、Site Recovery Manager は一時的なプレースホルダ マッピングにより操作を正常に終了します。
- Site Recovery Manager Server が起動すると、Site Recovery Manager は、vCenter Server のストレージ ポリシーベースの管理サービスとタグ マネージャ サービスに照会して、ストレージ ポリシーに関連付けられている仮想マシンを検索します。これらのサービスと vCenter Server は、Site Recovery Manager Server の起動または再起動時に実行中であることが必要です。これらが実行されていないと、Site Recovery Manager Server は起動しません。

ストレージ ポリシーの作成方法の詳細については、『VMware vSphere ESXi および vCenter Server 6.7』のドキュメントの[仮想マシン ストレージ ポリシー](#)を参照してください。

インベントリ マッピングの作成方法の詳細については、[インベントリ マッピングの構成](#)を参照してください。

ストレージ ポリシー保護グループおよびインベントリ マッピングの詳細については、[ストレージ ポリシー保護グループのインベントリ マッピング](#)を参照してください。

ストレージ ポリシー保護グループの既知の制限事項の詳細については、[ストレージ ポリシー保護グループの制限事項](#)を参照してください。

## ストレージ ポリシー保護グループの制限事項

ストレージ ポリシー保護グループには制限事項があります。

### 仮想マシン テンプレートの保護

保護されたストレージ ポリシーに準拠したデータストアには、仮想マシン テンプレートを含めないでください。

### RDM ディスクを使用する仮想マシンの保護

保護されたストレージ ポリシーに準拠したデータストアには、RDM ディスクを使用する仮想マシンを含めないでください。

### 仮想マシンの保護とライセンスの制限

- ライセンスの制限が原因で最初は保護されていなかった仮想マシンは、ライセンスの制限を満たすために整合性グループと仮想マシンを変更した後も保護されません。
- ライセンスの制限が原因で最初は保護されていなかった仮想マシンは、さらに多くの仮想マシン用のライセンスをインストールした後も保護されません。

### 拡張リンク モード環境での重複タグ

拡張リンク モードを使用する環境では、vCenter Server インスタンス間で一時的なネットワーク パーティションが発生すると、あるサイトで作成したタグと同名のタグを別のサイトでも作成することが可能になります。その結果、あるタグを使用してサイト上のデータストア セットをタグ付けした後、同じタグを使用して別のサイト上のデータストア セットをタグ付けしてしまう場合があります。Site Recovery Manager は ID ではなく名前を基準にしてタ

グを検索するため、ネットワーク パーティションの解消後は、どちらのサイトのデータストアも同じタグでタグ付けされているように見えます。重複するタグのどちらかを削除すると、そのタグが付いたデータストア内の整合性グループに対する保護が Site Recovery Manager によって解除される可能性があります。これらの整合性グループに含まれる仮想マシンは保護されなくなり、仮想マシンのリカバリ設定は削除されます。

この状況を回避するには、タグの競合を解決してから、ストレージ ポリシー保護グループを作成し、仮想マシンのリカバリ設定を構成します。ストレージ ポリシー保護グループの作成後にこの状況が発生した場合は、保護サイトを一時的にシャットダウンしてタグの競合を解決します。

## リカバリから再保護までの間のアレイ状態の変更

リカバリ プランの実行後、再保護を行うまでの間に、レプリケーションの反転に関する問題の修正などの目的でアレイ デバイスの状態を変更し、ストレージ デバイスの再スキャンを開始すると、Site Recovery Manager が予期せずに停止する場合があります。この状態になった場合は、対応する保護グループとリカバリ プランを再作成する必要があります。

## レプリケートされないデータストアとストレージ ポリシーの関連付け

レプリケートされないデータストアを、ストレージ ポリシー保護グループに含めたストレージ ポリシーに関連付けることができます。ただし、Site Recovery Manager は、レプリケートされないデータストアがストレージ ポリシー保護グループに含まれるストレージ ポリシーに関連付けられていたとしても、そのデータストア内の仮想マシンは保護しません。その保護グループを含むリカバリ プランを実行すると、レプリケートされていないデータストアにファイルがある仮想マシンは、保護グループ内にエラーがある状態が表示され、リカバリされません。

## 複数の整合性グループにまたがるデータストア

データストアは、複数の整合性グループにまたがるようには構成しないでください。Site Recovery Manager は、複数の整合性グループを使用するデータストアや仮想マシンを保護できず、処理は失敗する可能性があります。

- 整合性グループによってバックアップされている他のデータストアがストレージ ポリシーに含まれていない場合、保護グループは整合性グループをスキップする可能性があります。
- 保護グループは、データストアに関連する問題をレポートしないことがあります。
- 複数の整合性グループにまたがるデータストアを使用する仮想マシンは、仮想マシンで適切なストレージ ポリシーが使用されている場合でも、保護されない状態になります。
- 複数の整合性グループにまたがるデータストアは、レプリケートされず、ストレージ ポリシー保護グループによって保護されない状態として表示されます。これらのデータストアは、Site Recovery Manager が保護グループをリカバリ サイトに移行すると表示されなくなる場合があります。

## アレイベース レプリケーション保護グループとストレージ ポリシー保護グループでの同じ整合性グループの保護

レプリケートされたデータストアをタグ付けしてストレージ ポリシーに関連付ける場合は、ストレージ ポリシーとそれに関連する整合性グループをストレージ ポリシー保護グループに含めることができます。タグ付けされたデータストアを含むデータストア グループをアレイベース レプリケーション保護グループに含めることも可能です。その結果、整合性グループは、アレイベース レプリケーション保護グループとストレージ ポリシー保護グループの両方に含まれることになります。



ストレージ ポリシー保護グループとアレイベース レプリケーション保護グループの両方が同じ整合性グループを保護しようとした場合は、アレイベース レプリケーション保護グループが、整合性グループとそれに含まれる仮想マシンの所有権を得ます。ストレージ ポリシー保護グループは、整合性グループと仮想マシンをエラー状態としてマークします。この状態になった場合は、整合性グループをいずれかの保護グループから削除する必要があります。

- 整合性グループをアレイベース レプリケーション保護グループ内に残すには、影響を受ける仮想マシンをストレージ ポリシーとの関連付けから解除します。また、整合性グループをストレージ ポリシーとの関連付けから解除します。これで、整合性グループがストレージ ポリシー保護グループから削除されます。
- 整合性グループをストレージ ポリシー保護グループ内に残すには、アレイベース レプリケーション保護グループを編集してデータストアと仮想マシンを削除します。これで、ストレージ ポリシー保護グループのエラーが自動的に解消されます。

## リカバリ中およびリカバリ後の整合性グループと仮想マシンの保護ステータスの変更

データベースにタグを付けたリタグを解除したり、仮想マシンをストレージ ポリシーに関連付けたり関連付けを解除することによって、ストレージ ポリシー保護グループの一部である整合性グループと仮想マシンの保護ステータスを変更できます。仮想マシンと整合性グループの保護ステータスを変更して、計画移行またはディザスタ リカバリが実行されていない場合は、Site Recovery Manager が SPPG の仮想マシンと整合性グループの保護ステータスを更新します。

ストレージ ポリシー保護グループを使用した計画移行またはディザスタ リカバリ中に、仮想マシンと整合性グループの保護ステータスを変更した場合は、Site Recovery Manager のユーザー インターフェイスに保護サイトでの変更が表示される場合がありますが、リカバリ ワークフローは適切に更新できず、リカバリは失敗する可能性があります。

リカバリ プロセスを正常に実行するには、SPPG の計画移行またはディザスタ リカバリ中に、SPPG の仮想マシンと整合性グループの保護ステータスを変更してはなりません。具体的には、保護の変更がサポートされない期間は、SPPG を含むリカバリ プランが初めて「リカバリが進行中」状態に入ってから「リカバリ完了」状態に到達するまでです。

ストレージ ポリシー保護グループを含むリカバリ プランの実行に成功または失敗した場合、その保護グループに整合性グループや仮想マシンを追加することはできません。リカバリ済みまたは部分的にリカバリ済みの状態のストレージ ポリシー保護グループには、新しい整合性グループや仮想マシンを追加しないでください。新しい整合性グループまたは仮想マシンを追加できるのは、これまでリカバリ プランを実行したことがない、またはテスト リカバリのみを実行したことのある、既存のストレージ ポリシー保護グループです。

ストレージ ポリシー保護グループを含むリカバリ プランを実行したことがある場合は、新しいストレージ ポリシー保護グループに新しい整合性グループまたは仮想マシンを含める必要があります。新しい整合性グループや仮想マシンは、新しいストレージ ポリシー保護グループに追加する前に、リカバリ済みのストレージ ポリシー保護グループから削除してください。Site Recovery Manager では、1つの保護グループに含まれるオブジェクトの保護のみがサポートされます。

## リソース インベントリ マッピングの要件

ストレージ ポリシー保護グループには、リソース インベントリ マッピングの設定方法に関する特定の要件と制限があります。詳細については、[ストレージ ポリシー保護グループのインベントリ マッピング](#)を参照してください。



## ストレージ ポリシー保護グループと保護されていない仮想マシン

使用する環境、ストレージ ポリシーの実装、および保護対象のデータストアと仮想マシンの構成は、ストレージ ポリシー保護グループの前提条件を満たしている必要があります。前提条件を満たしていないと、Site Recovery Manager による、ストレージ ポリシー保護グループ内のすべての仮想マシンの保護が実行されない可能性があります。

ストレージ ポリシー保護を実現するために満たす必要のある前提条件については、[ストレージ ポリシー保護グループの前提条件](#)を参照してください。

たとえば、ストレージ ポリシーに関連付けられていない仮想マシンは、ストレージ ポリシーに関連付けられた仮想マシンと一緒に、タグ付けされたデータストアに配置できます。ストレージ ポリシー保護グループにストレージ ポリシーを含めると、これらの仮想マシンは、ストレージ ポリシーに関連付けられていないため Site Recovery Manager で保護されません。

保護されていない仮想マシンは、正しいストレージ ポリシーと関連付けられていないこと以外の理由で、ストレージ ポリシー保護グループに表示されることがあります。保護されていない仮想マシンがストレージ ポリシー保護グループに表示されるその他の状況に関する説明については、[ストレージ ポリシー保護グループの制限事項](#)を参照してください。

保護されていない仮想マシンがストレージ ポリシー保護グループに含まれる場合、これらの仮想マシンは、ストレージ ポリシー保護グループの [関連オブジェクト] - [仮想マシン] ビューに表示されます。保護グループはエラー状態で表示されます。

Site Recovery Manager が保護されていない仮想マシンをどのように扱うかは、実行するリカバリのタイプに応じて変わります。

---

**注：** 保護されていない仮想マシンは、これまでリカバリを実行したことのない、ストレージ ポリシー保護グループにある場合のみ保護できます。保護されていない仮想マシンを含むストレージ ポリシー保護グループに対してリカバリを実行したことがある場合は、リカバリの成否に関係なく、これらの仮想マシンをストレージ ポリシー保護グループから削除する必要があります。

---

- 保護されていない仮想マシンを含むストレージ ポリシー保護グループに対してテスト リカバリを実行すると、その操作は失敗し、エラーが返されます。レプリケートされていない仮想マシンが原因でテスト リカバリが失敗した場合は、クリーンアップを実行してから、保護されていない仮想マシンの保護または削除を試み、その後でテストを再び実行します。この保護グループに対してリカバリを実行したことがない場合は、クリーンアップの実行後、これらの仮想マシンを正しいストレージ ポリシーに関連付けたり、レプリケートされていないデータストアからレプリケートされたデータストアに仮想マシン ファイルを移動したりすることで、影響を受けた仮想マシンの修復を試みます。
- 保護されていない仮想マシンを含むストレージ ポリシー保護グループに対して計画移行を実行すると、その操作は失敗し、リカバリ プランは [不完全なリカバリ] 状態と表示されます。計画移行を無効化する手順の実行中、保護サイト上にある保護されていない仮想マシンは、Site Recovery Manager がストレージを読み取り専用にしにしないようにすることができます。そうしないと、仮想マシンがデータにアクセスできなくなる可能性があります。保護グループが [不完全なリカバリ] 状態の場合は、保護されていない仮想マシンを保護されたデータストアから削除し、ストレージ ポリシーとの関連付けを解除する必要があります。
- 保護されていない仮想マシンを含むストレージ ポリシー保護グループに対してディザスタ リカバリを実行すると、操作は成功しますが、Site Recovery Manager は保護されていない仮想マシンのリカバリを実行させ

ん。保護サイトが再びオンラインになった後で、計画移行を実行してリカバリを完了しようとしても、保護されていない仮想マシンが保護サイトにまだ存在する場合、計画移行は失敗します。保護グループが[不完全なリカバリ]状態の場合は、保護されていない仮想マシンを保護されたデータストアから削除し、ストレージ ポリシーとの関連付けを解除する必要があります。

## 暗号化された仮想マシンの保護

アレイ ベースのレプリケーション保護グループ、vSphere Replication 保護グループ、またはストレージ ポリシー保護グループ（SPPG）を使用して、暗号化された仮想マシンを保護およびリカバリできます。

ストレージ ポリシーを作成した後、次の手順を使用して、ストレージ ポリシーのルール セットを編集する必要があります。

### 前提条件

- SPPG を使用している場合は、[ストレージ ポリシー保護グループの前提条件](#)の前提条件を満たします
- リカバリ サイトと保護サイトで共通のキー マネージメント サーバ (KMS) が使用されていることや、両方のサイトのキー マネージメント サーバ クラスタで共通の暗号化キーが使用されていることを確認します。キー マネージメント サーバ クラスタの設定方法については、『VMware vSphere ESXi および vCenter Server 6.7』ドキュメントを参照してください。

### 手順

- 1 [仮想マシン ストレージ ポリシー] ウィザードの [ルール セット] ページで、[ストレージ ポリシーのルール セットを使用] を選択し、[ストレージの種類] に [タグ ベースの置換] オプションが選択されていることを確認します。
- 2 [ルールの追加] をクリックしてから、[カテゴリのタグ] をクリックします。
- 3 [カテゴリの選択] でカテゴリをクリックします。
- 4 [カテゴリのタグ] に [タグ付けしました...] が選択されていることを確認します。
- 5 [タグの追加...] をクリックしてから、タグを選択します。

### 次のステップ

- 1 ストレージ ポリシーのマッピングを作成し、リカバリ サイトのストレージ ポリシーが保護サイトのポリシーと同じであることを確認します。ストレージ ポリシーのマッピングの作成方法の詳細については、[ストレージ ポリシーのマッピングの選択](#)を参照してください。
- 2 アレイベースのレプリケーション保護グループ、vSphere Replication 保護グループ、またはストレージ ポリシー保護グループを作成します。アレイ ベースのレプリケーション保護グループの作成方法については、[アレイ ベース レプリケーション保護グループの作成](#)を参照してください。vSphere Replication 保護グループの作成方法については、[vSphere Replication 保護グループの作成](#)を参照してください。ストレージ ポリシー保護グループの作成方法の詳細については、[ストレージ ポリシー保護グループの作成](#)を参照してください。

## 保護グループの状態の概要

保護グループのステータスを監視して、それぞれの状態で許可されている操作を特定できます。

表 5-1. 保護グループの状態

状態	説明
Loading	インターフェイスが読み込んでいる間に、保護グループのステータスが表示されるまで短時間表示されます。
OK	グループはアイドルです。 すべての仮想マシンは OK 状態です。グループを編集できます。
Not Configured	グループはアイドルです。 一部の仮想マシンが OK 状態ではない場合があります。グループを編集できます。
Testing	グループは、テストを実行しているプランで使用されています。 グループは編集できません。
Test Complete	グループは、テストを実行しているプランで使用されています。 グループは編集できません。 クリーンアップが正常に実行されると、グループは OK または Not Configured 状態に戻ります。
Cleaning Up	グループは、テスト後にクリーンアップしているプランで使用されています。 グループは編集できません。 クリーンアップが正常に実行されると、グループは OK または Not Configured 状態に戻ります。 クリーンアップに失敗すると、グループは Testing 状態になります。
Recovering	グループは、リカバリを実行しているプランで使用されています。 グループは編集できません。 リカバリに成功すると、グループは Recovered 状態になります。 リカバリに失敗すると、グループ ステータスは Partially Recovered に変わります。
Partially Recovered	グループは、リカバリを完了したプランにありますが、いくつかの仮想マシンに対してリカバリは失敗しました。 仮想マシンは削除できますが、構成とリストアはできません。
Recovered	グループは、リカバリを正常に完了したプランにあります。 仮想マシンは削除できますが、構成とリストアはできません。
Reprotecting	グループは、再保護を実行しているプランで使用されています。 グループは編集できません。 再保護が正常に実行されると、グループは OK または Not Configured 状態に戻ります。 再保護に失敗すると、グループは Partially Reprotected 状態になります。
Partially Reprotected	グループは、再保護に失敗したプランにあります。 仮想マシンは削除できますが、構成とリストアはできません。
Configuring Protection	グループの仮想マシンに対して、保護の操作が処理中です。
Removing Protection	グループの仮想マシンからの保護の削除が処理中です。

表 5-1. 保護グループの状態（続き）

状態	説明
Restoring Placeholdersx	グループの仮想マシンのプレースホルダの作成が処理中です。
Restoring Placeholders	グループで少なくとも 1 つの [保護の構成] 処理と 1 つの [保護の削除] 処理の組み合わせが進行中です。

## 仮想マシンの保護状態の概要

保護グループの仮想マシンのステータスを監視して、それぞれの状態で許可されている操作を特定できます。

表 5-2. 仮想マシンの保護状態

状態	説明
Placeholder VM Not Found	プレースホルダ仮想マシンを削除しました。 [プレースホルダのリストア] アイコンが有効です。
Original protected VM not found	フェイルオーバーの後で再保護の前に元の本番仮想マシンを削除しました。 [プレースホルダのリストア] アイコンが有効です。
Datastore name used by VM is missing from group	仮想マシンには、保護グループに含まれないデータストアが必要です。 保護グループを編集してデータストアを含めます。
Datastore name used by VM is protected in a different group	仮想マシンには、別の保護グループにあるデータストアが必要です。 他の保護グループのデータストアを削除し、現在の保護グループを編集してデータストアを含めます。 2 つの保護グループにデータストアを含めることはできません。
Device not found: device name	保護された仮想マシンにレプリケートされていないディスクまたはデバイスが追加されました。 仮想マシンのレプリケーションを編集し、保護にデバイスを含めるか、または保護からデバイスを削除する必要があります。
Mapping missing: Folder name; Network name ; Resource pool name	この VM で、フォルダ、リソース プール、またはネットワークのマッピングが構成されていません。 サイトのインベントリ マッピングを修正するか、または仮想マシンを手動で構成します。
Placeholder VM creation error: error string from server	プレースホルダ仮想マシンの作成中のエラー。
OK	保護された仮想マシンは存在し、プロバイダ ステータスとプレースホルダ ステータスは両方ともクリーンです。
Invalid: error	仮想マシンは、ホーム データストアがレプリケートされていないか、または仮想マシンが削除されているために有効ではありません。 サーバからのエラー文字列に詳細情報が含まれます。 仮想マシンから保護を手動で削除します。
Not configured	保護グループを作成した後に、新しい仮想マシンを追加しました。 [すべて構成] を使用して、仮想マシンの保護を構成します。

表 5-2. 仮想マシンの保護状態（続き）

状態	説明
Error: error	エラーは次のいずれかです。 <ul style="list-style-type: none"> <li>■ リカバリ サイトのリソース プール、フォルダ、またはネットワークが同じデータセンターにありません。</li> <li>■ プレースホルダ データストアが見つかりません。</li> <li>■ 接続または権限の問題など、プレースホルダの作成時に発生した vCenter Server エラー。</li> </ul>
Configuring protection	仮想マシンの操作。
Removing protection	仮想マシンの操作。
Restoring placeholder	仮想マシンの操作。
Loading	インターフェイスが読み込んでいる間に、仮想マシンのステータスが表示されるまで短時間表示されます。
Mapping Conflict	Site Recovery Manager Server は、インベントリの競合を報告しました。 仮想マシンのリソース プールとフォルダが異なるデータセンターにあります。
Replication Error	vSphere Replication は、仮想マシンに関するエラーを報告します。
Replication Warning	vSphere Replication は、仮想マシンに関する警告を報告します。

## 保護グループの作成

Site Recovery Manager が仮想マシンを保護できるようにするには、保護グループを作成します。

保護グループを作成する場合は、処理が想定したとおりに完了するまで待機します。Site Recovery Manager が保護グループを作成し、グループ内の仮想マシンが正常に保護されていることを確認します。

フォルダの保護グループを整理することができます。

**注：** 保護グループの名前は、選択したフォルダの名前とは異なる必要があります。

## vSphere Replication 保護グループの作成

vSphere Replication を構成した仮想マシンを保護するには、vSphere Replication 保護グループを作成します。

### 前提条件

仮想マシンに vSphere Replication が構成されていることを確認します。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。

- 3 [保護グループ] タブをクリックし、[新規] をクリックして、保護グループを作成します。
- 4 [名前と方向] 画面で保護グループの名前と説明を入力し、方向を選択して、[次へ] をクリックします。
- 5 [保護グループ タイプ] ペインで [個々の仮想マシン (vSphere Replication)] を選択し、[次へ] をクリックします。
- 6 保護グループに追加する仮想マシンをリストから選択して、[次へ] をクリックします。

vSphere Replication 用に構成し、マシンと保護グループにまだ含まれていない仮想マシンのみがリストに表示されます。

- 7 必要に応じて、[リカバリ プラン] 画面で保護グループをリカバリ プランに追加できます。

オプション	説明
既存のリカバリ プランに追加	保護グループを既存のリカバリ プランに追加します。
新規のリカバリ プランに追加	保護グループを新規のリカバリ プランに追加します。 このオプションを選択する場合は、リカバリ プラン名を入力する必要があります。
今はリカバリ プランに追加しない	リカバリ プランに保護グループを追加しない場合は、このオプションを選択します。

- 8 設定を確認して、[終了] をクリックします。

## 結果

[保護グループ] タブで、保護グループの作成の進捗を監視できます。

- Site Recovery Manager が保護された仮想マシンにインベントリ マッピングを正常に適用すると、保護グループの保護ステータスは OK になります。
- インベントリ マッピングを構成しなかった場合、または Site Recovery Manager がインベントリ マッピングを適用できなかった場合、保護グループの保護ステータスは Not Configured になります。

## 次のステップ

保護グループの保護ステータスが [未構成] の場合は、仮想マシンにインベントリ マッピングを適用します。

- サイト全体にインベントリ マッピングを適用する場合、または設定済みのインベントリ マッピングが有効かどうかを確認する場合は、[インベントリ マッピングの構成](#)を参照してください。これらのマッピングをすべての仮想マシンに適用する場合は、[アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用](#)を参照してください。
- インベントリ マッピングを保護グループの各仮想マシンに個別に適用する場合は、[アレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成](#)を参照してください。

## ストレージ ポリシー保護グループの作成

ストレージ ポリシーに関連付けられている仮想マシンを保護するには、ストレージ ポリシー保護グループを作成します。

## 前提条件

[ストレージ ポリシー保護グループの前提条件](#) の要件を満たしていることを確認し、[ストレージ ポリシー保護グループの制限事項](#) を確認します。

## 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [保護グループ] タブをクリックし、[新規] をクリックして、保護グループを作成します。
- 4 [名前と方向] 画面で保護グループの名前と説明を入力し、方向を選択して、[次へ] をクリックします。
- 5 [保護グループ タイプ] 画面で [ストレージ ポリシー (アレイベース レプリケーション)] を選択して、[次へ] をクリックします。
- 6 保護グループに追加するデータストレージ ポリシーを選択して、[次へ] をクリックします。
- 7 必要に応じて、[リカバリ プラン] 画面で保護グループをリカバリ プランに追加できます。

オプション	説明
既存のリカバリ プランに追加	保護グループを既存のリカバリ プランに追加します。
新規のリカバリ プランに追加	保護グループを新規のリカバリ プランに追加します。 このオプションを選択する場合は、リカバリ プラン名を入力する必要があります。
今はリカバリ プランに追加しない	リカバリ プランに保護グループを追加しない場合は、このオプションを選択します。

- 8 設定を確認して、[終了] をクリックします。

[保護グループ] タブで、保護グループの作成の進捗を監視できます。

- Site Recovery Manager がストレージ ポリシーに関連付けられたすべての仮想マシンの保護に成功すると、保護グループの保護ステータスが OK になります。
- Site Recovery Manager がストレージ ポリシーに関連付けられたすべての仮想マシンを保護できない場合、保護グループの保護ステータスは Not Configured になります。

## 次のステップ

保護グループの保護ステータスが Not Configured の場合は、[ストレージ ポリシー保護グループの前提条件](#)の前提条件を満たしていることを確認し、[ストレージ ポリシー保護グループの制限事項](#)を確認し、ストレージ ポリシーの実装を適切に変更して、保護グループの再作成を試みてください。

## アレイベース レプリケーション保護グループの作成

アレイベース レプリケーションを構成した仮想マシンを保護するには、アレイベース レプリケーション保護グループを作成します。

## 前提条件

アレイベース レプリケーションを構成する仮想マシンがデータストアに含まれていることを確認します。



## 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [保護グループ] タブをクリックし、[新規] をクリックして、保護グループを作成します。
- 4 [名前と方向] 画面で保護グループの名前と説明を入力し、方向を選択して、[次へ] をクリックします。
- 5 [保護グループ タイプ] ペインで [データストア グループ (アレイベース レプリケーション)] を選択し、アレイペアを選択して、[次へ] をクリックします。
- 6 保護グループに追加するデータストア グループを選択して、[次へ] をクリックします。  
データストア グループを選択すると、そのグループに含まれる仮想マシンが [仮想マシン] テーブルに表示されます。
- 7 必要に応じて、[リカバリ プラン] 画面で保護グループをリカバリ プランに追加できます。

オプション	説明
既存のリカバリ プランに追加	保護グループを既存のリカバリ プランに追加します。
新規のリカバリ プランに追加	保護グループを新規のリカバリ プランに追加します。 このオプションを選択する場合は、リカバリ プラン名を入力する必要があります。
今はリカバリ プランに追加しない	リカバリ プランに保護グループを追加しない場合は、このオプションを選択します。

- 8 設定を確認して、[終了] をクリックします。

[保護グループ] タブで、保護グループの作成の進捗を監視できます。

- Site Recovery Manager が保護された仮想マシンにインベントリ マッピングを正常に適用すると、保護グループの保護ステータスは OK になります。
- インベントリ マッピングを構成しなかった場合、または Site Recovery Manager がインベントリ マッピングを適用できなかった場合、保護グループの保護ステータスは Not Configured になります。

## 次のステップ

保護グループの保護ステータスが [Not Configured] の場合は、仮想マシンにインベントリ マッピングを適用します。

- サイト全体にインベントリ マッピングを適用する場合、または設定済みのインベントリ マッピングが有効かどうかを確認する場合は、[インベントリ マッピングの構成](#)を参照してください。これらのマッピングをすべての仮想マシンに適用する場合は、[アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用](#)を参照してください。
- インベントリ マッピングを保護グループの各仮想マシンに個別に適用する場合は、[アレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成](#)を参照してください。



## フォルダ内の保護グループの整理

保護グループを整理するフォルダを作成できます。

保護グループの数が多い場合は、保護グループを複数のフォルダですると便利です。保護グループへのアクセスを制限するには、保護グループをフォルダ内に配置して、ユーザーまたはグループごとに異なる権限をそのフォルダに割り当てます。フォルダへの権限の割り当て方法の詳細については、[Site Recovery Manager のロールと権限の割り当て](#)を参照してください。

### 手順

- 1 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 2 [保護グループ] タブをクリックし、左側のペインで [保護グループ] を右クリックして、[新規フォルダ] をクリックします。
- 3 新規フォルダの名前を入力し、[追加] をクリックします。
- 4 フォルダに新しい保護グループまたは既存の保護グループを追加します。

オプション	説明
新規保護グループの作成	フォルダを右クリックして、[新規の保護グループ] を選択します。
既存の保護グループの追加	インベントリ ツリー内の保護グループを右クリックして、[移動] を選択します。ターゲットフォルダを選択し、[移動] をクリックします。

## データストア グループまたは仮想マシンの保護グループへの追加および保護グループからの削除

アレイベース レプリケーション保護グループではデータストア グループの追加と削除を、vSphere Replication 保護グループでは仮想マシンの追加と削除を実行できます。アレイベースのレプリケーション保護グループまたは vSphere Replication 保護グループの名前と説明も変更できます。

**注：** ストレージ ポリシー保護グループは、最初に作成したらそれ以降編集できません。既存のストレージ ポリシー保護グループに対する仮想マシンの追加や削除は、保護されているデータストア内の仮想マシンと関連付けられたストレージ ポリシーを変更することで行います。ストレージ ポリシー保護グループでの仮想マシンの追加や削除は、その保護グループでこれまでにリカバリが行われていない場合にのみ可能です。詳細については、[ストレージ ポリシー保護グループの制限事項](#)を参照してください。

### 前提条件

アレイベース レプリケーション保護グループまたは vSphere Replication 保護グループをすでに作成しています。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [保護グループ] タブをクリックし、保護グループを右クリックして、[編集] をクリックします。

4 (オプション) 保護グループの名前や説明を変更し、[次へ] をクリックします。

5 [次へ] をクリックします。

6 保護グループに含まれるデータストア グループまたは仮想マシンを変更します。

- アレイベースの保護グループでは、データストア グループを選択して保護グループに追加するか、または選択解除して保護グループから削除し、[次へ] をクリックします。
- vSphere Replication 保護グループでは、仮想マシンを選択して保護グループに追加するか、または選択解除して保護グループから削除し、[次へ] をクリックします。

7 設定を確認し、[次へ] をクリックして変更を適用します。

Site Recovery Manager が保護グループを更新している間に、変更内容を元に戻したり、キャンセルしたりすることはできません。

8 [終了] をクリックします。

## 結果

サイト全体にインベントリ マッピングを構成している場合、Site Recovery Manager は保護グループに追加した仮想マシンにマッピングを適用します。成功すると、仮想マシンのステータスは OK になります。

**注：** データストアまたは仮想マシンを保護グループに追加する場合、インベントリ マッピングは新しい仮想マシンにのみ適用されます。たとえば、インベントリ マッピングを変更してから OK 状態の保護グループにデータストアを追加すると、Site Recovery Manager は、新しいデータストアにある新たに保護された仮想マシンに新しいマッピングを適用します。以前に保護された仮想マシンは、以前のマッピングを引き続き使用します。

サイト全体にインベントリ マッピングを構成していない場合、保護グループのステータスは Not Configured になり、新しい仮想マシンのステータスは Mapping Missing になります。

## 次のステップ

保護グループのステータスが Not Configured で、新しい仮想マシンのステータスが Mapping Missing の場合は、仮想マシンにインベントリ マッピングを適用します。

- サイト全体にインベントリ マッピングを適用する場合、または設定済みのインベントリ マッピングが有効かどうかを確認する場合は、[インベントリ マッピングの構成](#)を参照してください。これらのマッピングをすべての仮想マシンに適用する場合は、[アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用](#)を参照してください。
- インベントリ マッピングを保護グループの各仮想マシンに個別に適用する場合は、[アレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成](#)を参照してください。

## アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用

アレイベースの保護グループまたは vSphere Replication 保護グループの保護ステータスが Not Configured の場合は、既存のサイト全体のインベントリ マッピングを使用して、未構成のすべての仮想マシンの保護を構成できます。

保護グループのステータスは、次のような理由で Not Configured になることがあります。

- 保護グループを作成する前にサイト全体のインベントリ マッピングを構成しませんでした。
- 保護グループを作成する前にブレースホルダ データストアのマッピングを構成しませんでした。
- 仮想マシンを作成した後に保護グループに追加しました。
- 仮想マシンの保護が解除されました。原因は、仮想マシンを保護グループに追加した後に再構成したためと考えられます。たとえば、仮想ディスクまたはデバイスを追加または削除した場合。

### 前提条件

- サイト全体のインベントリ マッピングを構成または再構成します。インベントリ マッピングを選択するには、[インベントリ マッピングの構成](#)を参照してください。
- ブレースホルダ データストアのマッピングを構成または再構成します。ブレースホルダ データストアを構成するには、[ブレースホルダ データストアの選択](#)を参照してください。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [保護グループ] タブをクリックし、保護グループをクリックして、右側のペインの [仮想マシン] タブをクリックします。
- 4 [すべての仮想マシンの構成] ボタンをクリックします。  
  
[すべての仮想マシンの構成] ボタンがアクティブになるには、保護グループの少なくとも 1 つの仮想マシンが [未構成] 状態になっている必要があります。
- 5 [はい] をクリックし、未構成のすべての仮想マシンにインベントリ マッピングを適用することを確認します。

- 6 仮想マシンのステータスを監視します。Site Recovery Manager で一部またはすべてのインベントリ マッピングを適用できなかった場合、または仮想マシンのプレースホルダを作成できなかった場合は、修正アクションを実行できます。

ステータス	操作
OK	操作は必要ありません。
未構成またはマッピングがありません	インベントリ マッピングを確認し、[すべての仮想マシンの構成] を再度クリックします。
プレースホルダ仮想マシン作成エラー	<p>プレースホルダ データストアのマッピングを確認して、プレースホルダ仮想マシンを再作成します。</p> <ul style="list-style-type: none"> <li>■ 個々の仮想マシンのプレースホルダを再作成するには、その仮想マシンを右クリックし、[プレースホルダの再作成] を選択します。</li> <li>■ いくつかの仮想マシンのプレースホルダを再作成するには、保護グループを右クリックし、[プレースホルダ仮想マシンのリストア] を選択します。</li> </ul>

## アレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成

アレイベースまたは vSphere Replication の保護グループに含まれる仮想マシンのマッピングは個々に構成できます。この機能により、リカバリ サイトのさまざまなリソースを異なる仮想マシンで使用できます。

サイト全体のインベントリ マッピングを構成している場合でも、アレイベースまたは vSphere Replication の保護グループに含まれる仮想マシンには、個々のインベントリ マッピングを構成できます。このような場合は、個々の仮想マシンから保護を削除し、フォルダとリソースのマッピングを構成してサイト全体のマッピングをオーバーライドできます。個々の仮想マシンのネットワークのマッピングは、保護を削除することなく変更できます。

個々の仮想マシンのプレースホルダ データストアを指定することはできません。保護サイトのデータストアは、サイト レベルでリカバリ サイトのプレースホルダ データストアにマッピングする必要があります。プレースホルダ データストアを構成するには、[プレースホルダ データストアの選択](#)を参照してください。

### 前提条件

アレイベースまたは vSphere Replication の保護グループが作成されています。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [保護グループ] タブをクリックし、構成する仮想マシンを含む保護グループをクリックします。
- 4 右側のペインで、[仮想マシン] タブをクリックします。
- 5 仮想マシンを右クリックし、[保護の構成] をクリックします。
- 6 リソースを展開し、[サイト マッピングのオーバーライド] チェックボックスを選択しリカバリ サイト上のリソースを選択して、インベントリ マッピングを構成します。[OK] をクリックします。

変更できるのは、フォルダ、リソース プール、およびネットワークのマッピングのみです。

- 7 仮想マシンのステータスを監視します。Site Recovery Manager で一部またはすべてのインベントリ マッピングを適用できなかった場合、または仮想マシンのプレースホルダを作成できなかった場合は、修正アクションを実行できます。

ステータス	操作
OK	操作は必要ありません。
未構成またはマッピングがありません	[保護の構成] を再度クリックして、インベントリのマッピングを確認します。
プレースホルダ仮想マシン作成エラー	サイト レベルでプレースホルダ データストアのマッピングを確認し、仮想マシンを右クリックして、[プレースホルダの再作成] をクリックします。

## アレイベース保護グループまたは vSphere Replication 保護グループ内の仮想マシンの設定の変更

保護されている仮想マシンの設定を変更したり、ハード ディスク、DVD ドライブなどのストレージ デバイスを追加または変更したりすると、対象となる仮想マシンの保護に影響することがあります。

**注：** ストレージ ポリシー保護グループ内で保護の対象となっている仮想マシンの設定を変更することはできません。

アレイベース レプリケーションを使用する場合、新しいデバイスの作成方法によっては、保護された仮想マシンへのデバイスの追加または変更が保護に影響します。

- 新しいデバイスが、保護グループに含まれないレプリケートされたデータストア上にある場合、仮想マシンを含む保護グループは Not Configured 状態になります。保護グループを再構成し、新しいデバイスを含むデータストアを保護グループに追加します。
- 新しいデバイスが別の保護グループが保護するレプリケートされたデータストアにある場合、仮想マシンの保護は無効になります。
- 新しいデバイスがレプリケートされていないデータストアにある場合は、データストアをレプリケートするか、またはデバイスから保護を削除する必要があります。
- Storage vMotion を使用してレプリケートされていないデータストアに仮想マシンを移動する場合、または Site Recovery Manager がストレージ レプリケーション アダプタ (SRA) を保持していないアレイ上のレプリケートされたデータストアに仮想マシンを移動する場合、仮想マシンの保護は無効になります。ただし、Storage vMotion を使用して、別の保護グループに含まれるデータストアに仮想マシンを移動できます。

vSphere Replication を使用して保護対象の仮想マシンにデバイスを追加する場合、仮想マシンの vSphere Replication を再構成して、新しいデバイスのレプリケーション オプションを選択する必要があります。vSphere Replication の設定の再構成については、<https://docs.vmware.com/jp/vSphere-Replication/index.html> の vSphere Replication のドキュメントを参照してください。

アレイベースの保護グループと vSphere Replication 保護グループの仮想マシンを変更した後に、ステータスが Not Configured、Device Not Found、Unresolved Devices、または Mapping Missing のすべての仮想マシンの保護を再構成する必要があります。アレイベースの保護グループまたは vSphere Replication 保護グループのすべてのメンバーにインベントリ マッピングを適用 およびアレイベース保護グループまたは vSphere Replication 保護グループの個別の仮想マシンのインベントリ マッピングを構成 を参照してください。

## 仮想マシンからの保護の削除

保護は、さまざまな理由で仮想マシンから削除されることがあります。仮想マシンから保護を削除すると、保護グループに別の影響が及びます。

保護を削除すると、リカバリ サイトのプレースホルダ仮想マシンが削除されます。アレイベース レプリケーション保護グループまたは vSphere Replication 保護グループの仮想マシンから保護を削除すると、仮想マシンと保護グループの状態は **未構成** になります。保護グループを含むリカバリ プランを保護対象の仮想マシンに対して実行すると成功しますが、Site Recovery Manager は **Not Configured** 状態の仮想マシンまたは保護グループをリカバリしません。計画移行を実行した場合、プランの状態は **Recovery Incomplete** になります。

---

**注：** ストレージ ポリシー保護グループの仮想マシンから一時的に保護を削除することはできません。

---

アレイベース レプリケーションでは、仮想マシンの Site Recovery Manager 保護とその仮想マシンの Site Recovery Manager ストレージ管理は区別されます。アレイベース レプリケーション保護グループの仮想マシンから保護を削除すると、Site Recovery Manager は仮想マシンをリカバリしなくなりますが、仮想マシンのファイルのストレージの監視と管理は継続されます。

保護は、次のような理由で仮想マシンから削除することがあります。

- vSphere Replication を使用していて、保護される仮想マシンを保護グループから除外したい場合。
- アレイベース レプリケーションを使用しているときに、保護しない仮想マシンが、他のユーザーによって、レプリケートされたデータストアに移動された場合。仮想マシンから保護を削除すると、保護グループの状態は **Not Configured** になります。そのグループ全体のテスト リカバリと計画移行は失敗します。ディザスタ リカバリはグループ内の保護された仮想マシンに対してのみ成功し、保護サイトに対する特定の処理はスキップされます。リカバリ プランの状態は **リカバリが必要** になります。この場合は、仮想マシンを保護されたデータストアに移動します。
- アレイベース レプリケーションを使用し、レプリケートされていないデータストアに格納されているデバイスが仮想マシンにある場合。仮想マシンから保護を削除すると、デバイス ファイルを再配置するときに、グループ内の他のすべての仮想マシンに対してディザスタ リカバリが正常に実行されるようになります。

仮想マシンから保護を削除すると、アレイベース レプリケーションと vSphere Replication のどちらを使用しているかに応じて、保護グループに異なる影響が出ます。

- アレイベース レプリケーション保護グループに含まれる仮想マシンから保護を削除する場合は、その仮想マシンのファイルを保護されていないデータストアに移動する必要があります。Site Recovery Manager がデータストア グループに含めたデータストアに、保護されていない仮想マシンのファイルを残すと、データストア グループ全体のテスト リカバリと計画移行は失敗します。ディザスタ リカバリは、データストア グループ内の保護された仮想マシンに対してのみ成功します。計画移行を実行してリカバリを終了するには、保護されていない仮想マシンを事前に移動しておく必要があります。
- 保護グループに含めた仮想マシンで vSphere Replication を無効にすると、この仮想マシンに対するリカバリは失敗しますが、その保護グループ内にある、正しく構成されているすべての仮想マシンのリカバリは成功します。保護グループを編集するか、[仮想マシンの削除] をクリックすることにより、仮想マシンの保護を削除し、保護グループから仮想マシンを削除する必要があります。[データストア グループまたは仮想マシンの保護グループへの追加および保護グループからの削除](#)を参照してください。

## 仮想マシンからの保護の削除

アレイベース レプリケーション保護グループまたは vSphere Replication 保護グループに含まれるレプリケートされた仮想マシンの保護は、保護グループから削除することなく、一時的に削除できます。

---

**注：** ストレージ ポリシー保護グループの仮想マシンから一時的に保護を削除することはできません。

---

### 手順

- 1 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 2 [保護グループ] タブをクリックし、保護グループを選択して、右側のペインの [仮想マシン] タブをクリックします。
- 3 仮想マシンを右クリックし、[保護の削除] をクリックします。
- 4 [はい] をクリックし、仮想マシンからの保護の削除を確認します。



# 復旧プランの作成、テスト、実行

## 6

保護サイトとリカバリ サイトで Site Recovery Manager を構成すると、リカバリ プランを作成、テスト、実行できます。

復旧プランは、自動化されたランブックに似ています。このリカバリ プランは、Site Recovery Manager が仮想マシンをパワーオンまたはパワーオフする順序や、リカバリした仮想マシンが使用するネットワーク アドレスなど、リカバリ プロセスのすべての手順を制御します。復旧プランは柔軟性があり、カスタマイズできます。

復旧プランには1つ以上の保護グループが含まれます。1つの保護グループを複数の復旧プランに含めることができます。たとえば、組織全体で保護サイトからリカバリ サイトへのサービスの計画移行を処理するために1つのリカバリ プランを作成し、個々の部門ごとに別のプランのセットを作成することができます。この例では、これらさまざまなリカバリ プランで1つの保護グループを参照しており、ユーザーはリカバリの実行方法を決定できます。

特定の保護グループを復旧する際、復旧プランは1度に1つだけ実行できます。別のリカバリ プランで共有されている保護グループを使用してリカバリ プランをテストまたは実行する場合、別のリカバリ プランが保護グループの状態を 保護グループ使用中 に変更するため実行できません。

### ■ 復旧プランのテスト

復旧プランを作成または変更する場合は、計画済みマイグレーションや障害復旧で使用する前にテストしてください。

### ■ リカバリ プランの実行による計画移行またはディザスタ リカバリの実行

計画された状況下で復旧プランを実行し、仮想マシンを保護サイトから復旧サイトに移行できます。保護サイトに、データ損失につながる可能性のある予期せぬイベントが発生した場合は、計画されていない環境でリカバリ プランを実行することもできます。

### ■ 復旧プランのテストと実行の相違点

復旧プランのテストによって、保護サイトまたは復旧サイトのいずれにも持続的な影響が及ぶことはありませんが、復旧プランを実行すると両方のサイトに重大な影響が及びます。

### ■ リカバリ サイトの複数のホストでの仮想マシンのテスト リカバリの実行

隔離されたテスト ネットワーク内にある複数のリカバリ サイトのホストで仮想マシンを復旧するリカバリ プランを作成できます。

### ■ 復旧プランの作成、テスト、実行

リカバリ プランを作成、テスト、実行して、リカバリ中に Site Recovery Manager のアクションをカスタマイズできます。



- **ストレージ ポリシー保護グループ内の仮想マシンのリカバリの無効化**

ストレージ ポリシー保護グループ内の仮想マシンのリカバリは、仮想マシンを保護グループから削除しなくても無効にできます。

- **ストレージ ポリシー保護グループ内の整合性グループのリカバリの無効化**

保護グループから削除しなくても、ストレージ ポリシー保護グループ内の整合性グループのリカバリを無効にすることができます。

- **リカバリ プランのステップのエクスポート**

今後の参照のために、またはリカバリ プランのハード コピーをバックアップとして保存するため、リカバリ プランのステップを様々なフォーマットでエクスポートできます。

- **リカバリ プランの履歴レポートの表示とエクスポート**

リカバリ プラン、リカバリ プランのテスト、またはテストのクリーンアップの各実行に関するレポートを表示およびエクスポートできます。

- **復旧プランの削除**

リカバリ プランが必要なくなった場合は、削除できます。

- **リカバリ プランの状態の概要**

リカバリ プランのステータスを監視して、それぞれの状態で許可されている操作を特定できます。プランの状態は、リカバリ プラン内の保護グループの状態によって決まります。

## 復旧プランのテスト

復旧プランを作成または変更する場合は、計画済みマイグレーションや障害復旧で使用する前にテストしてください。

復旧プランをテストすることにより、プランで保護する仮想マシンが復旧サイトに正しく復旧することを確認する必要があります。復旧プランをテストしないと、実際の障害復旧状況が発生したときに一部の仮想マシンは復旧できない可能性があり、これによってデータが損失する可能性があります。

リカバリ プランのテストでは、リカバリ プランがほぼ全面的に実行されます。ただし Site Recovery Manager は、保護サイトとリカバリ サイトで進行中の操作を中断しないようするため、いくつかの側面を除外します。ローカル仮想マシンをサスペンドするリカバリ プランは、テストでも実際のリカバリでも同じように実行されます。この例外により、テスト復旧を実行する場合、どちらのサイトであっても、レプリケーションや進行中のアクティビティが中断されることはありません。

vSphere Replication を使用する場合は、リカバリ プランをテストするときにも、保護サイトの仮想マシンはリカバリ サイトのレプリカ仮想マシン ディスク ファイルと同期されます。vSphere Replication サーバによって、リカバリ サイト上の仮想マシン ディスク ファイルの REDO ログが作成されるため、同期は正常に続行されます。テストの実行後にクリーンアップを実行すると、vSphere Replication サーバによってリカバリ サイト上のディスクから REDO ログが削除され、仮想マシンディスクのログに集積された変更が維持されます。

アレイベースのレプリケーションを使用して、リカバリ プランをテストする場合、保護サイトの仮想マシンは引き続き、リカバリ サイトのレプリカ仮想マシン ディスク ファイルにレプリケートされます。テスト リカバリ中に、リカバリ サイトに仮想マシンのディスク ファイルをホストしているボリュームのスナップショットがアレイによって作成されます。通常、テストの処理中にも、アレイ レプリケーションの処理は続行されます。テストの実行後にクリーンアップを行うと、テスト リカバリ ワークフローの一部として以前に作成されたスナップショットはアレイによって削除されます。

テスト復旧は必要なだけ実行できます。復旧プランのテストはいつでもキャンセルできます。

フェイルオーバーまたは別のテストを実行する前に、クリーンアップ操作を正常に実行する必要があります。[リカバリ プランをテストした後のクリーンアップ](#)を参照してください。

リカバリ プランをテストする権限にリカバリ プランを実行する権限は含まれません。また、リカバリ プランを実行する権限にリカバリ プランをテストする権限は含まれません。それぞれの権限は、個別に割り当てる必要があります。[Site Recovery Manager のロールと権限の割り当て](#)を参照してください。

## ネットワークとデータセンター ネットワークのテスト

リカバリ プランをテストするとき、Site Recovery Manager では、リカバリされた仮想マシンへの接続に使用するテスト ネットワークを作成できます。テスト ネットワークを作成することにより、本番環境の仮想マシンを妨害することを心配せずに、テストを実行することができます。

分離されたテスト ネットワークは固有の仮想スイッチによって管理され、ほとんどの場合、リカバリされた仮想マシンは、IP アドレスやゲートウェイなどのネットワーク プロパティを変更することなくそのネットワークを使用できます。分離されたテスト ネットワークは複数のホストに拡張できません。リカバリ プランでリカバリ中に使用するネットワークごとにテスト ネットワークを構成する必要があります。

相互に通信する必要がある仮想マシンを同じテスト ネットワークに復旧する必要があります。たとえば、Web サーバがデータベースの情報にアクセスする場合は、それらの Web サーバとデータベース仮想マシンを同じネットワークと一緒にリカバリする必要があります。

データセンター ネットワークは、リカバリ サイトの既存のネットワークです。テスト ネットワークとして使用するデータセンター ネットワークを選択できます。それを使用するため、復旧された仮想マシンはネットワーク アドレスの可用性規則に従う必要があります。これらの仮想マシンでは、ネットワークのスイッチがサービスを提供してルーティングすることが可能なネットワーク アドレスを使用する必要があり、正しいゲートウェイや DNS ホストなどを使用する必要があります。DHCP を使用するリカバリされた仮想マシンは、DHCP が適切に構成されていれば、追加のカスタマイズを行うことなくこのネットワークに接続できます。それ以外の仮想マシンでは、IP カスタマイズとそのカスタマイズに適用する追加のリカバリ プラン手順が必要になる場合があります。

## リカバリ プランの実行による計画移行またはディザスタ リカバリの実行

計画された状況下で復旧プランを実行し、仮想マシンを保護サイトから復旧サイトに移行できます。保護サイトに、データ損失につながる可能性のある予期せぬイベントが発生した場合は、計画されていない環境でリカバリ プランを実行することもできます。

**注：** リカバリ プランを実行して計画移行およびディザスタ リカバリを実行すると、Site Recovery Manager によって両方のサイトが変更されます。この変更を元に戻すには、膨大な時間と労力が必要になります。この時間と労力を考えると、復旧プランをテストする権限と復旧プランを実行する権限は、別々に割り当てる必要があります。

### 計画済みの移行

計画移行中に、Site Recovery Manager はリカバリ サイトの仮想マシンのデータを保護サイトの仮想マシンと同期します。

Site Recovery Manager は、保護された仮想マシンを正常にシャットダウンし、データ損失を防止するための最終同期を実行してから、リカバリ サイトの仮想マシンのパワーオンを試みます。

計画済みの移行中にエラーが発生した場合、プランは停止されるので、エラーを解決してプランを再実行できます。復旧後、仮想マシンを再保護できます。

### 災害復旧

ディザスタ リカバリでは、Site Recovery Manager は最初にストレージ同期を試みます。ストレージ同期が成功すると、Site Recovery Manager はレプリケーションを構成する際に設定する目標復旧ポイント (RPO) に基づいて、同期されたストレージ状態を使用してリカバリ サイトの仮想マシンを最新の使用可能な状態にリカバリします。

リカバリ プランを実行してディザスタ リカバリを行う場合、Site Recovery Manager は、保護サイトの仮想マシンのシャットダウンを試みます。Site Recovery Manager が仮想マシンをシャットダウンできない場合にも、Site Recovery Manager はリカバリ サイトでコピーをパワーオンします。

保護サイトがディザスタ リカバリ後にオンラインに復帰すると、リカバリ プランは矛盾した状態になり、本番環境の仮想マシンが両方のサイトで稼動するようになります。これは、スプリット ブレイン問題と呼ばれます。Site Recovery Manager はこの状態を検出し、プランを再度実行して、保護サイトの仮想マシンをパワーオフできるようにします。その後、リカバリ プランは整合性のある状態に戻り、ユーザーは再保護を実行できるようになります。

Site Recovery Manager が、保護サイトのデータストアが全バス ダウン (APD) の状態で、仮想マシンのシャットダウンを阻害していることを検出した場合、Site Recovery Manager は、仮想マシンのシャットダウンを再度試みるまでの間待機します。APD は通常一時的な状態なので、APD 状態にあるデータストアがオンラインに復帰するまで待機することにより、Site Recovery Manager は、そのデータストアの保護仮想マシンを正常にシャットダウンできます。

## VMware Tools の使用

Site Recovery Manager は VMware Tools のハートビートを使用して、リカバリ サイトで動作している仮想マシンを検出します。このようにして、Site Recovery Manager はすべての仮想マシンがリカバリ サイトで動作していることを確認できます。VMware Tools は、保護された仮想マシンのゲスト OS を正常にシャットダウンするためにも使用されます。このため、保護された仮想マシンに VMware Tools をインストールすることがベスト プラクティスです。保護された仮想マシンに VMware Tools をインストールしない、またはできない場合は、リカバリした仮想マシンで VMware Tools の起動を待たずにゲスト OS のシャットダウン手順をスキップするように Site Recovery Manager を構成する必要があります。[リカバリ設定の変更](#)を参照してください。

## 強制復旧による復旧の実行

保護サイトがオフラインになっていて、Site Recovery Manager がタスクを適時実行できない場合は、目標復旧時間 (RTO) が許容できないレベルまで上昇します。このような場合は、強制リカバリ オプションを使用してリカバリ プランを実行できます。強制リカバリ オプションでは、保護サイトでの操作を実行することなくリカバリ サイトで仮想マシンを起動します。

### 強制リカバリを使用するタイミング

強制リカバリは、保護サイトでインフラストラクチャが失敗し、その結果、保護された仮想マシンが管理不能になり、シャットダウン、パワーオフ、登録解除が実行できなくなった場合に使用します。こうした状態になると、長期間に渡ってシステムの状態が変更不能になります。

強制リカバリを実行しても、保護サイトの仮想マシンのシャットダウン処理は完了しません。このため、スプリットブレイン問題が発生しますが、リカバリはより迅速に完了します。

## vSphere Replication による強制リカバリ

vSphere Replication を使用してディザスタ リカバリを実行する場合、Site Recovery Manager は、再保護のために vSphere Replication ストレージを準備し、アレイベース レプリケーションで行うようなミラーリングの検証は行う必要がありません。

### アレイベース レプリケーションによる強制リカバリ

保護サイトのストレージ アレイがオフラインまたは使用不可になっている場合に、アレイベース レプリケーションを使用してディザスタ リカバリを実行すると、保護ストレージ アレイとリカバリ ストレージ アレイの間のミラーリングに影響することがあります。

強制リカバリの実行後、レプリケーション操作をさらに進めていく前に、保護アレイとリカバリ アレイ間のミラーリングが正しく設定されているかを確認する必要があります。ミラーリングが正しく設定されていない場合は、ストレージ アレイ ソフトウェアを使用してミラーリングを修正する必要があります。

保護サイトのストレージがまだ使用できる状態の場合に強制リカバリを有効にすると、シーケンスが開始されるまで、保護サイトでの大きな変更がリカバリ サイトにレプリケートされなくなります。ストレージ アレイの目標リカバリ時点 (RPO) の期間にしたがって、変更のレプリケーションが行われます。

新規の仮想マシンやテンプレートが保護サイトに追加され、リカバリがストレージ RPO の期間満了前に開始された場合、新しい仮想マシンまたはテンプレートは、レプリケートされたデータストアに表示されず、消失してしまいます。新しい仮想マシンまたはテンプレートの消失を避けるために、RPO 期間が終了するまで待機してから、強制リカバリでリカバリ プランを実行します。

強制リカバリが終了し、ストレージ アレイのミラーリングを確認したら、強制リカバリを必要としていた問題を解決できます。

根本的な問題を解決したら、リカバリ プランの計画移行を再度実行します。リカバリ プランが正常に完了するまで、何か問題が発生したら解決して、プランを再実行するという手順を繰り返します。リカバリ プランを再実行しても、リカバリ サイトのリカバリ済み仮想マシンには影響ありません。

## 強制リカバリの有効化

ディザスタ リカバリを実行する際に強制リカバリを選択するには、リカバリ サイトの Site Recovery Manager サーバの [詳細設定] で、`recovery.forceRecovery` オプションを有効にする必要があります。詳細については、[リカバリ設定の変更](#)を参照してください。

[リカバリ プランの実行] ウィザードで強制リカバリ オプションを選択できるのは、ディザスタ リカバリ モードの場合のみです。このオプションは、計画移行では使用できません。

## 強制リカバリ後の計画移行

強制リカバリの実行後に計画移行を実行すると、基盤となるデータストアが読み取り専用か、または使用できない場合に、保護サイトの仮想マシンが失敗してシャットダウンすることがあります。この場合、保護サイトの vCenter Server にログインして手動で仮想マシンをパワーオフします。仮想マシンをパワーオフした後、計画移行を再度実行します。

## 復旧プランのテストと実行の相違点

復旧プランのテストによって、保護サイトまたは復旧サイトのいずれにも持続的な影響が及ぶことはありませんが、復旧プランを実行すると両方のサイトに重大な影響が及びます。

復旧プランのテストおよび実行を行う場合は、異なる権限が必要です。

表 6-1. 復旧プランのテストと復旧プランの実行の違い

異なる領域	復旧プランのテスト	復旧プランの実行
必要な権限	Site Recovery Manager.リカバリ プラン.テスト 権限が必要。	Site Recovery Manager.リカバリ プラン.リカバリ 権限が必要。
保護サイトでの仮想マシンへの影響	なし	Site Recovery Manager は仮想マシンを優先順位の低い順にシャットダウンして、保護サイトでサスペンドされている仮想マシンをリストアします。
リカバリ サイトでの仮想マシンへの影響	リカバリ プランで必要な場合、Site Recovery Manager はローカル仮想マシンをサスペンドします。Site Recovery Manager は、テストのクリーンアップ後、サスペンドされた仮想マシンを再起動します。	リカバリ プランで必要な場合、Site Recovery Manager はローカル仮想マシンをサスペンドします。

表 6-1. 復旧プランのテストと復旧プランの実行の違い（続き）

異なる領域	復旧プランのテスト	復旧プランの実行
レプリケーションへの影響	Site Recovery Manager は、リカバリ サイトでレプリケートされたストレージの一時的なスナップショットを作成します。アレイ ベース レプリケーションの場合、Site Recovery Manager はアレイを再スキャンして検出します。	計画移行を行っている間、Site Recovery Manager はレプリケートされたデータストアを同期してから、レプリケーションを停止し、リカバリ サイトのターゲット デバイスを書き込み可能にします。ディザスタ リカバリ中、Site Recovery Manager によっては同じ手順が試行されますが、失敗した場合、Site Recovery Manager 保護サイトのエラーは無視されます。
ネットワーク	テスト ネットワークを明示的に割り当てる場合、Site Recovery Manager は、リカバリ した仮想マシンをテスト ネットワークに接続します。仮想マシンのネットワーク割り当てが [分離されたネットワーク (自動作成)] になっている、サイトレベルでマッピングされていない場合、Site Recovery Manager は仮想マシンを物理ネットワークに接続されていない一時的なネットワークに割り当てます。	Site Recovery Manager は、リカバリした仮想マシンをユーザー指定のデータセンター ネットワークに接続します。
復旧プランの中断	テストはいつでもキャンセルできます。	リカバリはいつでもキャンセルできます。

## リカバリ サイトの複数のホストでの仮想マシンのテスト リカバリの実行

隔離されたテスト ネットワーク内にある複数のリカバリ サイトのホストで仮想マシンを復旧するリカバリ プランを作成できます。

Site Recovery Manager では、vSwitch を DVS ベースにして、複数のホストに対応することができます。[サイトレベルのマッピングを使用] として構成されたデフォルトのテスト ネットワークを受け入れているにもかかわらず、サイトレベルでマッピングされていない場合、ホスト間でリカバリされる仮想マシンはリカバリ プランのテスト中に専用のテスト ネットワークに配置されます。各テスト スイッチはホスト間で隔離されています。その結果、同じリカバリ プランの仮想マシンはテスト リカバリの終了時に隔離されます。仮想マシンで通信できるようにするには、DVS スイッチまたは VLAN を確立および選択します。本番ネットワークに接続することなく、すべてのホストを互いに接続する隔離された VLAN により、より現実に近い形で復旧をテストすることができます。復旧ホスト間の接続を確立し、本番ネットワークからは隔離された状態を保つには、次の推奨事項にしたがってください。

- プライベートな隔離された VLAN に接続される DVS スイッチを作成します。このような VLAN はホストと仮想マシンを接続できるようにしますが、本番仮想マシンから隔離します。DVS がテスト用であることを明示的に指定する命名規則を使用し、リカバリ プラン エディタのリカバリ プランのテスト ネットワークの列でこの DVS を選択します。
- 保護サイトに戻るルートのないテスト VLAN を物理ネットワークに作成します。テスト VLAN をリカバリ サイトの vSphere クラスタにトランキングしてテスト VLAN ID の仮想スイッチを作成します。これらのスイッチをテスト用として識別するための明確な命名規則を使用します。リカバリ プラン エディタのテスト リカバリ ネットワークの列からこれらのスイッチを選択します。



## 復旧プランの作成、テスト、実行

リカバリ プランを作成、テスト、実行して、リカバリ中に Site Recovery Manager のアクションをカスタマイズできます。

### 手順

#### 1 復旧プランの作成

リカバリ プランを作成し、Site Recovery Manager が仮想マシンをリカバリする方法を確立します。

#### 2 フォルダによるリカバリ プランの整理

さまざまなユーザーまたはグループによるリカバリ プランへのアクセスを制御するには、リカバリ プランをフォルダ別に整理します。

#### 3 復旧プランの編集

復旧プランを編集して、その復旧プランの作成時に指定したプロパティを変更することができます。復旧プランは、保護サイトまたは復旧サイトから編集できます。

#### 4 復旧プランのテスト

リカバリ プランをテストする場合、Site Recovery Manager では、リカバリ サイトのテスト ネットワークとレプリケートされたデータの一時的なスナップショットでリカバリ プランの仮想マシンが実行されます。Site Recovery Manager では、保護サイトの操作が中断することはありません。

#### 5 リカバリ プランをテストした後のクリーンアップ

リカバリ プランをテストした後、クリーンアップ操作を実行することで、リカバリ プランを初期状態に戻すことができます。フェイルオーバーまたは別のテストを実行する前に、クリーンアップ操作を終了する必要があります。

#### 6 復旧プランの実行

リカバリ プランを実行するとき、Site Recovery Manager によってリカバリ プランの全仮想マシンがリカバリ サイトに移行されます。Site Recovery Manager は、保護サイトの対応する仮想マシンをシャットダウンしようとします。

#### 7 仮想マシンの特定の時点のスナップショットのリカバリ

vSphere Replication を使用すると、リカバリ プランの実行時に、仮想マシンに対する多数の特定時点の (PIT) スナップショットをリカバリするように Site Recovery Manager を構成できます。

#### 8 テストまたは復旧のキャンセル

ステータスが [テストの処理中] または [フェイルオーバー処理中] の場合は、いつでもリカバリ プランのテストをキャンセルできます。

## 復旧プランの作成

リカバリ プランを作成し、Site Recovery Manager が仮想マシンをリカバリする方法を確立します。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。

- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、[新規] をクリックして、リカバリ プランを作成します。
- 4 プランの名前、説明、方向を入力し、フォルダを選択して、[次へ] をクリックします。

**注：** リカバリ プランの名前は、選択したフォルダの名前とは異なる必要があります。

- 5 メニューからグループ タイプを選択します。

オプション	操作
個々の仮想マシンまたはデータストア グループの保護グループ	アレイベース レプリケーション保護グループと vSphere Replication 保護グループを含むリカバリ プランを作成するには、このオプションを選択します。
ストレージ ポリシー保護グループ	ストレージ ポリシー保護グループを含むリカバリ プランを作成するには、このオプションを選択します。 拡張されたストレージを使用している場合は、このオプションを選択します。

- 6 このプランで復旧する保護グループを 1 つ以上選択し、[次へ] をクリックします。
- 7 [テスト ネットワーク] ドロップダウン メニューから、テスト リカバリ中に使用するネットワークを選択して、[次へ] をクリックします。  
  
サイトレベルでマッピングされていない場合に、デフォルトの [サイトレベルのマッピングを使用] オプションを使用すると、分離されたテスト ネットワークが作成されます。
- 8 概要情報を確認し、[終了] をクリックして復旧プランを作成します。

## フォルダによるリカバリ プランの整理

さまざまなユーザーまたはグループによるリカバリ プランへのアクセスを制御するには、リカバリ プランをフォルダ別に整理します。

リカバリ プランの数が多い場合は、リカバリ プランを複数のフォルダで整理すると便利です。リカバリ プランへのアクセスを制限するには、リカバリ プランをフォルダ内に配置して、ユーザーまたはグループごとに異なる権限をそのフォルダに割り当てます。フォルダへの権限の割り当て方法の詳細については、[Site Recovery Manager のロールと権限の割り当て](#)を参照してください。

### 手順

- 1 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 2 [リカバリ プラン] タブをクリックし、左側のペインの [リカバリ プラン] を右クリックして、[新規フォルダ] をクリックします。
- 3 作成するフォルダの名前を入力し、[追加] をクリックします。



- 4 フォルダに新しいリカバリ プランまたは既存のリカバリ プランを追加します。

オプション	説明
新しいリカバリ プランの作成	フォルダを右クリックして、[新しいリカバリ プラン] を選択します。
既存のリカバリ プランの追加	インベントリ ツリー内のリカバリ プランを右クリックして、[移動] をクリックします。ターゲット フォルダを選択し、[移動] をクリックします。

## 復旧プランの編集

復旧プランを編集して、その復旧プランの作成時に指定したプロパティを変更することができます。復旧プランは、保護サイトまたは復旧サイトから編集できます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランを右クリックして、[編集] をクリックします。
- 4 (オプション) プランの名前や説明を変更し、[次へ] をクリックします。  
リカバリ プランの方向と場所は変更できません。
- 5 (オプション) 1 つ以上の保護グループを選択してプランに追加するか、または選択解除してプランから削除し、[次へ] をクリックします。
- 6 (オプション) ドロップダウン メニューから、リカバリ サイト上の別のテスト ネットワークを選択し、[次へ] をクリックします。
- 7 概要情報を確認して [終了] をクリックし、指定した変更を復旧プランに加えます。  
プランの更新は [最近のタスク] ビューで監視できます。

## 復旧プランのテスト

リカバリ プランをテストする場合、Site Recovery Manager では、リカバリ サイトのテスト ネットワークとレプリケートされたデータの一時的なスナップショットでリカバリ プランの仮想マシンが実行されます。Site Recovery Manager では、保護サイトの操作が中断することはありません。

リカバリ プランをテストすると、プランのすべての手順が実行されます。ただし、保護サイトの仮想マシンをパワーオフすることと、レプリケートされたデータをリカバリ サイトのデバイスで制御可能にすることはできません。プランにおいてリカバリ サイトのローカル仮想マシンをサスペンドする必要がある場合、Site Recovery Manager はテスト中にそれらの仮想マシンをサスペンドします。本番環境へのその他の変更は、どちらのサイトでもリカバリ プランのテストで実行されることはありません。

リカバリ プランをテストすると、リカバリ プラン内の仮想マシンの全ディスク ファイルのスナップショットがリカバリ サイトに作成されます。スナップショットの作成は、ストレージの I/O 待ち時間に追加されます。VMware Virtual SAN ストレージを使用してリカバリ プランをテストする際に応答時間の低下が検出される場合、Virtual SAN インターフェイスの監視ツールを使用して I/O 待ち時間を監視します。

## 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランを右クリックして、[テスト] をクリックします。  
リカバリ プランの [リカバリ手順] ビューで [テスト] アイコンをクリックして、テストを実行することもできます。
- 4 (オプション) [最近の変更をリカバリ サイトに複製する] を選択します。  
このチェック ボックスを選択すると、リカバリ サイトで保護された仮想マシンの最新コピーを得ることができますが、同期時間が長くなる場合があります。
- 5 [次へ] をクリックします。
- 6 テストの情報を確認し、[終了] をクリックします。
- 7 テストの進行状況を監視したり、メッセージに応答したりするには、[リカバリ] タブの [リカバリ手順] タブをクリックします。  
[復旧ステップ] タブには、個々のステップの進行状況が表示されます。[最近のタスク] のテスト タスクによって、全体的な進捗を追跡します。

## 次のステップ

リカバリ プランのテストが完了したらクリーンアップ操作を実行し、リカバリ プランをテスト前の元の状態に戻します。

## リカバリ プランをテストした後のクリーンアップ

リカバリ プランをテストした後、クリーンアップ操作を実行することで、リカバリ プランを初期状態に戻すことができます。フェイルオーバーまたは別のテストを実行する前に、クリーンアップ操作を終了する必要があります。

Site Recovery Manager は、テスト後にいくつかのクリーンアップ操作を実行します。

- 復旧した仮想マシンをパワーオフします。
- ID と構成情報を保持したまま、復旧した仮想マシンをブレースホルダに置き換えます。
- テスト中に復旧した仮想マシンによって使用されていた、レプリケートされたストレージのスナップショットをクリーンアップします。

## 前提条件

復旧プランのテストが完了したことを確認します。

## 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。

- 3 [リカバリ プラン] タブをクリックし、リカバリ プランを右クリックして、[クリーンアップ] を選択します。  
リカバリ プランの [リカバリ手順] ビューで [クリーンアップ] アイコンをクリックして、テストを実行することもできます。
- 4 クリーンアップ情報を確認し、[次へ] をクリックします。
- 5 [終了] をクリックします。
- 6 (オプション) エラーが発生してクリーンアップが終了する場合は、[強制クリーンアップ] チェック ボックスを選択して、クリーンアップ処理中のエラーを無視するように設定し、クリーンアップを再実行します。必要に応じて、クリーンアップがエラーなく終了するまで複数回実行します。

## 復旧プランの実行

リカバリ プランを実行するとき、Site Recovery Manager によってリカバリ プランの全仮想マシンがリカバリ サイトに移行されます。Site Recovery Manager は、保護サイトの対応する仮想マシンをシャットダウンしようとしています。

**注意：** リカバリ プランを実行すると、保護サイトとリカバリ サイトの構成が大幅に変更されて、レプリケーションが停止します。テストしていない復旧プランを実行しないでください。これらの変更を取り消すと大幅に時間と労力がかかる可能性があり、サービスのダウンタイムが長引く可能性があります。

### 前提条件

- 強制リカバリを使用するには、最初にこの機能を有効にしなければなりません。強制リカバリを有効にするには、[リカバリ設定の変更](#) に説明されている [recovery.forceRecovery] 設定を有効にします。
- インベントリ マッピングが完全に構成されていることを確認します。一時的なプレースホルダ インベントリ マッピングのみが構成された状態で、[使用可能な仮想マシンの vMotion を有効化] オプションを指定して計画移行を実行すると、両方のサイトが実行中であっても計画移行は失敗します。
- 計画移行で [使用可能な仮想マシンの vMotion を有効化] オプションを使用するには、仮想マシンで vMotion を有効にします。仮想マシンで vMotion を有効にする方法については、[計画移行用の vSphere vMotion の有効化](#) を参照してください。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランを右クリックして、[実行] をクリックします。
- 4 確認画面で情報を見直し、[この処理によって、保護データセンターとリカバリ データセンターの両方の仮想マシンとインフラストラクチャが永久的に変更されることを理解しています] を選択します。

## 5 実行する復旧のタイプを選択します。

オプション	説明
計画済みの移行	両方のサイトが実行されている場合、仮想マシンを復旧サイトに復旧します。計画移行中に保護サイトでエラーが発生した場合、計画移行操作は失敗します。拡張されたストレージがアレイでサポートされている場合は、[使用可能な仮想マシンの vMotion を有効化] チェック ボックスを選択します。
災害復旧	保護サイトに問題がある場合、仮想マシンを復旧サイトに復旧します。ディザスタ リカバリ中に保護サイトでエラーが発生した場合、ディザスタ リカバリは失敗せずに続行されます。

## 6 (オプション) [強制リカバリ - リカバリ サイトの操作のみ] チェック ボックスを選択します。

強制リカバリ機能を有効にし、[ディザスタ リカバリ] を選択した場合、このオプションを使用できます。

## 7 [次へ] をクリックします。

## 8 復旧情報を確認し、[終了] をクリックします。

## 9 個別の手順の進行状況を監視するには、リカバリ プランをクリックし、[リカバリ手順] タブをクリックします。

### 結果

[最近のタスク] パネルに、プラン全体の進行状況が表示されます。

## 仮想マシンの特定の時点のスナップショットのリカバリ

vSphere Replication を使用すると、リカバリ プランの実行時に、仮想マシンに対する多数の特定の時点の (PIT) スナップショットをリカバリするように Site Recovery Manager を構成できます。

### 前提条件

- 1 [詳細設定] の [vrReplication.preserveMpitImagesAsSnapshots] オプションの値を `true` に設定して、古い PIT スナップショットを維持するように Site Recovery Manager を構成します。詳細については、[vSphere Replication 設定の変更および仮想マシンのレプリケートと複数の特定の時点のインスタンスの有効化](#)を参照してください。
- 2 vSphere Replication を使用して仮想マシンのレプリケーションを構成します。
- 3 vSphere Replication 保護グループに仮想マシンを追加して、リカバリ プランに保護グループを含めます。

### 手順

#### 1 リカバリ プランを実行します。

リカバリ プランが完了したら、構成した数の PIT スナップショットで仮想マシンがリカバリ サイトにリカバリされます。

#### 2 [仮想マシンおよびテンプレート] ビューで、リカバリされた仮想マシンを右クリックし、[スナップショット] - [スナップショットの管理] の順に選択します。

#### 3 この仮想マシンの PIT スナップショットのいずれかを選択し、[復元] をクリックします。

リカバリされた仮想マシンは、選択した PIT スナップショットに戻ります。

- 4 (オプション) 仮想マシンに IP カスタマイズが設定されていて、古い PIT スナップショットを選択した場合は、リカバリした仮想マシンに IP アドレス設定を手動で行います。

## テストまたは復旧のキャンセル

ステータスが [テストの処理中] または [フェイルオーバー処理中] の場合は、いつでもリカバリ プランのテストをキャンセルできます。

テストまたはリカバリをキャンセルすると、Site Recovery Manager はプロセスを開始することなく、特定のルールを使用して処理中のプロセスを停止します。フェイルオーバーをキャンセルした場合は、再実行する必要があります。

- パワーオン、ハートビートの待機などの停止できないプロセスは、完了するまで実行してから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プロセスを元に戻すには、クリーンアップ操作を行います。

テストまたはリカバリをキャンセルするために必要な時間は、処理中のプロセスのタイプと数によって異なります。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブを選択し、リカバリ プランを右クリックして、[キャンセル] を選択します。プランは、[リカバリ手順] タブからキャンセルすることもできます。

### 次のステップ

テストをキャンセルした後にクリーンアップを実行します。

## ストレージ ポリシー保護グループ内の仮想マシンのリカバリの無効化

ストレージ ポリシー保護グループ内の仮想マシンのリカバリは、仮想マシンを保護グループから削除しなくても無効にできます。

終了時に必ずエラーとなるリカバリ プランを実行する場合は、エラーの原因となる仮想マシン（1 つまたは複数）のリカバリを無効にすることができます。個々の仮想マシンごとに手順を繰り返す必要があります。

### 前提条件

[リカバリを無効にする] 機能を使用するには、ストレージ ポリシー保護グループが部分的にリカバリされた状態になっている必要があります。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。

- 3 [保護グループ] タブをクリックし、ストレージ ポリシー保護グループをクリックして、[仮想マシン] タブをクリックします。
- 4 仮想マシンを選択して、[リカバリを無効にする] ボタンをクリックします。
- 5 [はい] をクリックして確認します。

#### 結果

次にリカバリ プランを実行するときに、仮想マシンのリカバリはスキップされます。

#### 次のステップ

リカバリ プランを再実行します。

## ストレージ ポリシー保護グループ内の整合性グループのリカバリの無効化

保護グループから削除しなくても、ストレージ ポリシー保護グループ内の整合性グループのリカバリを無効にすることができます。

SPPG のリカバリ プランを実行すると、整合性グループによってエラーが発生する場合には、整合性グループのリカバリを無効にすることができます。個々の整合性グループごとに手順を繰り返す必要があります。

#### 前提条件

[リカバリを無効にする] 機能を使用するには、ストレージ ポリシー保護グループを部分的にリカバリされた状態にして、次のいずれかの条件を満たす必要があります。

- 整合性グループがリカバリ サイトに表示されない。
- 整合性グループはリカバリ サイトに表示されるが、中身が空である。
- 整合性グループはリカバリ サイトに表示されるが、グループ内のすべての仮想マシンにエラーがある。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [保護グループ] タブを選択し、ストレージ ポリシー保護グループをクリックして、[整合性グループ] タブを選択します。
- 4 整合性グループを選択して、[リカバリを無効にする] ボタンをクリックします。
- 5 [はい] をクリックして確認します。

#### 結果

次にリカバリ プランを実行するときに、整合性グループのリカバリはスキップされます。

## 次のステップ

リカバリ プランを再実行します。[復旧プランの実行](#) を参照してください。

## リカバリ プランのステップのエクスポート

今後の参照のために、またはリカバリ プランのハード コピーをバックアップとして保存するため、リカバリ プランのステップを様々なフォーマットでエクスポートできます。

### 前提条件

テスト リカバリと実際のリカバリが進行中でないことを確認します。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランをクリックします。
- 4 (必須) [リカバリ手順] タブをクリックし、[表示] ドロップダウン メニューからリカバリ手順モードを選択します。

オプション	説明
テスト手順	テスト リカバリ手順をエクスポートします。
リカバリ手順	リカバリ手順をエクスポートします。
クリーンアップ手順	クリーンアップ手順をエクスポートします。
再保護手順	再保護手順をエクスポートします。

**注：** リカバリ プランの状態によっては、リカバリ手順のモードを選択するオプションを使用できない場合があります。

- 5 [手順のエクスポート] アイコンをクリックします。  
リカバリ プランの手順は、HTML、XML、CSV、MS Excel、Word ドキュメントの形式で保存できます。
- 6 [ダウンロード] をクリックしてウィンドウを閉じます。  
新しいタブでリカバリ プラン手順レポートを開くこともできます。

## リカバリ プランの履歴レポートの表示とエクスポート

リカバリ プラン、リカバリ プランのテスト、またはテストのクリーンアップの各実行に関するレポートを表示およびエクスポートできます。

リカバリ プランの履歴レポートによって、リカバリ プランの各実行、テスト、またはクリーンアップに関する情報を得ることができます。履歴には、プラン全体およびプランの各ステップの結果および開始時間と終了時間の情報が含まれます。履歴レポートはいつでもエクスポートできますが、履歴レポートには常に、完了した操作のエントリが含まれていません。操作が処理中の場合、履歴レポートは操作の完了後に表示されます。

Site Recovery Manager は、削除されたリカバリ プランの履歴を保持します。既存のプランと削除済みプランの履歴レポートをエクスポートできます。

既存のプランの履歴レポートをエクスポートするには、次の手順に従います。

#### 前提条件

リカバリ プランの実行やテスト、またはテスト後のクリーンアップが完了している必要があります。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[リカバリ プランの履歴] をクリックします。
- 4 (オプション) 特定の期間内のすべてのリカバリ プランの履歴リストをエクスポートするには、[すべてエクスポート] をクリックします。
- 5 (オプション) リカバリ プランの履歴リストからアイテムを選択し、特定の期間のリカバリ プランの履歴、リカバリ プランの実行、テスト、クリーンアップ、または再保護操作について [レポートのエクスポート] をクリックします。
- 6 生成されたファイルの形式を選択し、[ダウンロード] または [新しいタブで開く] をクリックします。

リカバリ プランの履歴は、HTML、XML、CSV、MS Excel、Word ドキュメントとして保存できます。

## 復旧プランの削除

リカバリ プランが必要なくなった場合は、削除できます。

#### 前提条件

リカバリ プランが整合性のある状態であることを確認します。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、削除するリカバリ プランを右クリックして、[削除] をクリックします。



## リカバリ プランの状態の概要

リカバリ プランのステータスを監視して、それぞれの状態で許可されている操作を特定できます。プランの状態は、リカバリ プラン内の保護グループの状態によって決まります。

表 6-2. リカバリの状態

状態	説明
Ready	<p>リカバリ ステップはクリアされます。</p> <p>ストレージ ポリシー保護グループの場合、リカバリ プランがこの状態になっていると、仮想マシンと整合性グループがリカバリ手順に表示されません。リカバリ プランに含まれる保護対象の仮想マシンは、[仮想マシン] タブで確認できます。</p>
Test in progress	<p>テストをキャンセルすると、プランは Cancel in progress 状態に移行します。</p>
Test complete	<p>テストは、エラーの有無に関わらず完了しました。テスト中に障害が発生した場合、プランは [テスト中断] の状態になります。</p>
Test interrupted	<p>テストの実行中にサーバが失敗しました。</p>
Cleanup in progress	<p>クリーンアップが正常に完了すると、プランの状態は Ready に移行します。</p> <p>クリーンアップが不完全な場合、状態は Cleanup Incomplete に移行します。</p> <p>[Force Cleanup] オプションを設定すると、エラー後に Ready に移行します。</p> <p>クリーンアップ中に失敗が発生すると、状態は Cleanup Incomplete に移行します。</p>
Cleanup Incomplete	<p>クリーンアップ中にエラーが発生しました。</p> <p>クリーンアップを再度実行できます。</p> <p>この状態からクリーンアップを実行する場合は、クリーンアップ ウィザードにエラーを無視するオプションがあります。</p>
Cleanup interrupted	<p>クリーンアップ中に Site Recovery Manager が失敗しました。</p> <p>リカバリのオプションは変更できません。</p>
Recovery in progress	<p>リカバリをキャンセルすると、状態は Cancel in progress に移行します。</p>
Disaster recovery complete	<p>保護サイトにおけるリカバリ中に、仮想マシンのシャットダウンでエラーが発生しました。サイトが接続されていなかったことが考えられます (スプリット ブレインの前の手順)。</p> <p>システムはスプリット ブレインを警告し、サイトが再接続されたときに再度リカバリを実行することを求めます。</p> <p>サイトが接続されている場合、状態は Recovery required (split brain) に移行します。</p>
Recovery started	<p>ピア サイトでリカバリが開始されましたが、サイトが接続されていない場合、正確な状態は不明です。</p> <p>リカバリ サイトにログインするか、またはサイトを再接続して、現在の状態を取得します。</p>

表 6-2. リカバリの状態（続き）

状態	説明
Recovery required (split brain)	<p>リカバリ中にサイトが切断されました。サイトの再接続時にスプリット ブレインのシナリオが検出されました。</p> <p>システムは、リカバリを再度実行してサイトを同期するように求めます。</p> <p>ストレージ ポリシー保護グループの場合、リカバリ プランがこの状態になっていると、仮想マシンと整合性グループがリカバリ手順に表示されません。リカバリ プランに含まれる保護対象の仮想マシンは、[仮想マシン] タブで確認できます。</p>
Recovery complete	<p>エラーが発生した場合、仮想マシンはエラーがある状態ですべてリカバリされます。リカバリの再実行により、エラーは修正されていません。</p> <p>プランは、スプリット ブレインのリカバリが解決した後にこの状態に移行します。</p> <p>前回のリカバリの実行のリカバリ ステップを確認できます。</p> <p>ストレージ ポリシー保護グループの場合、リカバリ プランがこの状態になっていると、仮想マシンと整合性グループがリカバリ手順に表示されません。リカバリ プランに含まれる保護対象の仮想マシンは、[仮想マシン] タブで確認できます。</p> <p>リカバリ中にサイトが切断されました。この状態は、接続ステータスによってのみトリガーされます。</p>
Incomplete recovery	<p>キャンセルされたリカバリまたはデータストアのエラー。リカバリを再実行します。</p> <p>エラーを解決してリカバリを再実行するか、またはエラーが発生している仮想マシンの保護を削除する必要があります。プランは、どちらかの方法によるエラーの解決を検出して、状態を <code>Recovery complete</code> に更新します。</p>
Partial recovery	<p>オーバーラップ プランによって、すべてではなく一部の保護グループがリカバリされました。</p>
Recovery interrupted	<p>リカバリ中の失敗により、リカバリが一時停止しています。[実行] をクリックして続行します。リカバリのオプションは変更できません。</p>
Cancel in progress	<p>テストをキャンセルすると、前回の結果がキャンセルされ、<code>Test complete</code> になります。</p> <p>リカバリをキャンセルすると、前回の結果がキャンセルされ、<code>Incomplete recovery</code> になります。</p> <p>処理を早期にキャンセルすると、<code>Ready</code> の状態になる場合があります。</p>
Reprotect in progress	<p>この状態でサーバが失敗すると、<code>Reprotect interrupted</code> に移行します。</p>
Partial reprotect	<p>オーバーラップ プランが再保護されました。</p> <p>すでに再保護されているグループは <code>Ready</code> 状態に移行しますが、他のグループが <code>Recovered</code> 状態であるため、これは有効です。</p>
Incomplete reprotect	<p>再保護は、ストレージ操作を完了しませんでした。新たな実行で再保護が成功するには、サイトが接続されている必要があります。</p> <p>再保護によってストレージ操作は完了しましたが、シャドウ仮想マシンの作成は完了しませんでした。仮想マシンを実行しているサイトが切断されていても再保護を再び実行し、その直後にリカバリに進むことができます。</p>

表 6-2. リカバリの状態（続き）

状態	説明
Reprotect interrupted	再保護中に Site Recovery Manager Server が失敗した場合は、再度再保護を実行して続行し、状態を適切にクリーンアップします。
Waiting for user input	テストは一時停止しています。プロンプトを閉じて、テストを再開します。 リカバリは一時停止しています。プロンプトを閉じて、リカバリを再開します。
Protection groups in use	プランには、別のプランのテストに使用されているグループが含まれます。 この状態は、他のプランがグループに対するテスト操作を完了し、まだクリーンアップを実行していないときにも発生します。  別のプランがテストまたはクリーンアップを完了するまで待機するか、またはプランを編集してグループを削除します。
Direction error	グループは、無効な状態である混合状態にあります。プランには、逆方向で Ready 状態の複数のグループが含まれています。どちらかの方向を正しい方向として選択し、反対の方向の保護グループを削除します。  このエラーは、オーバーラップ プランが実行され、すでにプラン内のいくつかのグループを再保護している場合に発生します。
Deleting	プランは、ピア プランの削除を待機している間にこの状態になります。他のプランが削除されると、プランは自動的に完了します。
Plan out of sync	この状態は、複数の状況で発生します。 <ul style="list-style-type: none"> <li>■ 成功したテスト リカバリとクリーンアップ操作の間。この状態のプランを編集できない場合は、クリーンアップを実行してプランを Ready 状態に戻します。クリーンアップを許可するには、場合によってはもう一方のサイトの VMware Site Recovery ユーザー インターフェイスでプランを開く必要があります。プランが Plan out of sync 状態のままの場合は、プランを編集します。</li> <li>■ 通常の操作中にプランを編集できます。</li> </ul> プランを編集用に関き、編集後に変更を保存すると、Site Recovery Manager は保護とリカバリの Site Recovery Manager サーバ間のプランに関する Site Recovery Manager の内部データを強制的に同期します。これにより、Plan out of sync ステータスがクリアされます。
No protection groups	プランに保護グループが含まれていないので、プランを実行できません。 リカバリ サイトを含めて、プランを編集できます。  空のプランは、API またはユーザー インターフェイスを使用するか、または保護グループを削除することによって作成できます。
Internal error	プランに不明な状態の保護グループがあるか、またはその他の予期しないエラーが発生しました。  プランを実行することはできませんが、削除はできます。

# リカバリ プランの構成

# 7

リカバリ プランを構成すると、Site Recovery Manager Server または仮想マシンでのコマンドの実行、Site Recovery Manager Server またはゲスト OS でプランを実行するときに応答が必要となるメッセージの表示、リカバリ時の不必要な仮想マシンのサスペンド、仮想マシン間の依存関係の構成、仮想マシン ネットワーク設定のカスタマイズ、保護された仮想マシンのリカバリ優先順位の変更が可能です。

簡単なリカバリ プラン（リカバリした仮想マシンの接続先となるテスト ネットワークと、パワーオンし、カスタマイズされるまで仮想マシンを待機するタイムアウト値のみを指定するプラン）でも Site Recovery Manager 構成を効果的にテストできます。

ほとんどの復旧プランには、本番環境で使用する構成が必要です。たとえば、保護サイトでの緊急時の復旧プランは、サイトから別のサイトへのサービスの計画済み移行の場合の復旧プランと異なる可能性があります。

復旧プランは、常に、復旧の対象となる保護グループの現在の状態を反映します。保護グループのメンバーが OK 以外のステータスを示す場合は、復旧プランに変更を加える前に、その問題を修正する必要があります。

リカバリ プランの実行時、このプランの状態は、プランに含まれる保護グループの状態ではなく、プランの実行状態を反映します。

## リカバリ プランの手順

リカバリ プランは、計画移行や再保護などの所定のワークフローを特定の順序で実行する必要があります。それらのステップの順序または目的を変更することはできませんが、メッセージの表示やコマンドの実行を行う独自のステップを挿入できます。

Site Recovery Manager は、異なるリカバリ プランの手順を異なる方法で実行します。

- 一部の手順はすべてのリカバリ時に実行されます。
- 一部の手順はテスト リカバリ時にのみ実行されます。
- ステップの中にはテスト復旧中に常にスキップされるものがあります。
- 一部のステップは拡張されたストレージでのみ実行されます。

リカバリ プランをカスタマイズする場合は、リカバリの手順、手順の順序、手順を実行する状況を理解していることが重要です。

## リカバリ順序

リカバリ プランを実行する際に、Site Recovery Manager は次の処理を実行します。

- 1 Site Recovery Manager は設定した優先順位に従って仮想マシンをパワーオフし、優先順位の高いマシンを最後にパワーオフします。リカバリ プランのテスト時に、Site Recovery Manager はこの手順を省略します。
- 2 Site Recovery Manager は、設定した優先順位に従ってリカバリ サイトの仮想マシンのグループをパワーオンします。ある優先順位のグループのリカバリを開始するには、そのグループよりも1つ上の優先順位に位置するグループのすべての仮想マシンのリカバリが成功または失敗している必要があります。

リカバリ中は、優先順位が異なるグループの仮想マシン間にある依存関係は無視されます。同じ優先グループの仮想マシン間に依存関係が存在する場合、Site Recovery Manager は最初にほかの仮想マシンが依存している仮想マシンをパワーオンします。

Site Recovery Manager が仮想マシンの依存関係を満たす場合、Site Recovery Manager は vCenter Server でサポートされている数の仮想マシンを同時にパワーオンしようとします。

## リカバリ プランのタイムアウトと一時停止

リカバリ プランの手順の実行時に発生するタイムアウトには、いくつかの種類があります。タイムアウトによって、ステップを完了するための時間として許容された指定間隔でプランが一時停止します。

メッセージ ステップは、ユーザーがメッセージを確認するまでプランを一時停止します。メッセージ手順をリカバリ プランに追加する前に、その手順が必要かどうかを確認します。メッセージ手順を含むリカバリ プランをテストまたは実行する前に、ユーザーがプランの進行状況を監視し、必要に応じてメッセージに応答できるようになっていることを確認します。

## 拡張されたストレージのリカバリ ステップ

リカバリ プランのウィザードを使用すると、クロス vSphere vMotion を実行し、保護サイトの拡張されたストレージ上にある、保護対象のパワーオンされたすべての仮想マシンにフェイルオーバーを実行できるようになります。このオプションを選択すると、リカバリ手順のうち、保護サイトの仮想マシンをパワーオフする直前に、2つの手順が追加されます。

- [仮想マシンの移行用にストレージを準備]: Site Recovery Manager は、整合性グループごとにリカバリ サイトのプリファレンスを変更します。
- [仮想マシンの移行]: 本番環境の仮想マシンがパワーオンされていないと、このステップは失敗します。本番環境の仮想マシンがパワーオンされている場合、Site Recovery Manager は vSphere vMotion を開始して、仮想マシンをリカバリ サイトに移行します。

---

**注意：** 移行に適した仮想マシンが、これに適していない仮想マシンよりも優先順位が低い場合、または移行に適していない仮想マシンに対して依存関係がある場合は、移行されません。

---

## カスタム リカバリ手順の作成

復旧中にコマンドを実行したりユーザーに対してメッセージを表示したりするカスタム復旧ステップを作成できます。

Site Recovery Manager は、Site Recovery Manager Server またはリカバリ プランの一部になっている仮想マシンでカスタム手順を実行できます。

カスタム リカバリ手順を追加すると、追加した手順はテスト ワークフローと実行ワークフローで共有されます。サスペンドされる仮想マシンでカスタム手順を実行することはできません。

再保護中に、Site Recovery Manager は、リカバリ プランのすべてのカスタム リカバリ手順を保持します。再保護後にリカバリまたはテストを実行した場合、カスタム リカバリ手順は新しいリカバリ サイト、つまり元の保護サイトで実行されます。

再保護後、通常は変更せずにメッセージを表示するカスタム復旧ステップを直接使用します。

ネットワーク構成など、サイト固有の情報を含むコマンドを実行するカスタムの手順がある場合は、再保護の後にこれらの手順を変更しなければならないことがあります。

リカバリ プラン手順内で、特定の操作の完了を示すコマンドやプロンプトを構成できます。ただし、[テスト ネットワークの構成] 手順の前にコマンドやプロンプトを追加することはできません。

ストレージ ポリシー保護グループに関する次のトップレベルのステップにコマンドやプロンプトを追加することはできません。

- ストレージ整合性グループのテスト リカバリを完了
- 仮想マシンのテスト リカバリを完了
- 保護グループのテスト リカバリを完了
- 保護グループのライブ移行を完了
- 保護サイトで保護グループの操作を完了
- ストレージ整合性グループのリカバリを完了
- 仮想マシンのリカバリを完了
- 保護グループのリカバリを完了

## カスタム リカバリ ステップの種類

いろいろな種類のカスタム リカバリ ステップを作成してリカバリ プランに含めることができます。

カスタム リカバリ ステップは、コマンド リカバリ ステップかメッセージ プロンプト ステップのどちらかです。

### コマンド リカバリ手順

コマンド リカバリ ステップには、トップレベル コマンドか仮想マシンあたりのコマンドが含まれています。

#### トップレベルのコマンド

Site Recovery Manager Server で実行されるトップレベルのコマンドです。これらのコマンドを使用して、物理デバイスをパワーオンしたり、ネットワーク トラフィックをリダイレクトしたりできます。

#### 仮想マシンごとのコマンド

Site Recovery Manager は、リカバリ プロセス中に仮想マシンごとのコマンドを新規にリカバリされた仮想マシンに関連付けます。これらのコマンドを使用して、仮想マシンをパワーオンした後で構成タスクを実行でき

ます。コマンドは、仮想マシンのパワーオンの前後どちらでも実行できます。仮想マシンがパワーオンされた後に実行するように構成するコマンドは、Site Recovery Manager Server または新規にリカバリされた仮想マシンのどちらでも実行できます。新たにリカバリされた仮想マシン上で実行するコマンドは、VMware Tools がリカバリされた仮想マシン上で使用するユーザー アカウントのコンテキストで実行されます。書き込むコマンドの機能によっては、VMware Tools がリカバリされた仮想マシン上で使用するユーザー アカウントを変更する必要がある場合があります。

## メッセージ プロンプト リカバリ手順

リカバリ中に Site Recovery Manager ユーザー インターフェイスにメッセージを表示します。このメッセージを使用してリカバリを一時停止し、リカバリ プランを実行するユーザーに情報を提示できます。たとえば、メッセージによって、手動リカバリ タスクを実行するかステップを検証するよう、ユーザーに指示できます。ユーザーがプロンプトに直接応答できる唯一のアクションは、メッセージを閉じてリカバリを続行することです。

## コマンドおよびプロンプト ステップの実行

ストレージ ポリシー保護グループで、最優先の仮想マシンの前にコマンドまたはプロンプトを追加すると、Site Recovery Manager は、すべての仮想マシンに対する [仮想マシンのポリシーの適用] 手順の完了後に、そのコマンドまたはプロンプトを実行します。

アレイベース レプリケーション保護グループと vSphere Replication 保護グループでは、[書き込み可能なストレージのスナップショットを作成] と空でない最初の仮想マシンの優先グループの間に追加された最初のコマンドまたはプロンプト（カスタム手順）は、再起動が失敗する場合に備えて、[書き込み可能なストレージのスナップショットを作成] 手順と並行して開始されます。

## Site Recovery Manager がカスタム リカバリ手順のエラーを処理する方法

Site Recovery Manager は、リカバリ手順の種類に基づいて、異なる方法でカスタム リカバリ手順の障害を処理します。

Site Recovery Manager は、すべてのカスタム リカバリ手順を実行しようとしませんが、一部のコマンド リカバリ手順を終了できない場合があります。

## コマンド リカバリ手順

デフォルトでは、Site Recovery Manager はコマンド リカバリ手順が終了するまで 5 分間待機します。タイムアウトは、コマンドごとに構成することができます。コマンドがこのタイムアウト期間内に終了した場合は、復旧プラン内の次の復旧ステップが実行されます。カスタム コマンドに失敗した場合の Site Recovery Manager の処理方法は、コマンドの種類に応じて異なります。

コマンドの種類	説明
トップレベルのコマンド	リカバリ手順に失敗すると、Site Recovery Manager はその失敗をログに記録し、[リカバリ手順] タブに警告を表示します。後続のカスタム復旧ステップが続けて実行されます。
仮想マシンごとのコマンド	仮想マシンのパワーオンの前または後に、バッチで実行します。1 つのコマンドが失敗すると、バッチ内の残りの仮想マシンごとのコマンドは実行されません。たとえば、パワーオン前に実行するコマンドを 5 つ追加し、パワーオン後に実行するコマンドを 5 つ追加した場合、パワーオン前にそのバッチの 3 番目のコマンドが失敗すると、パワーオン前に実行する残りの 2 つのコマンドは実行されません。Site Recovery Manager は仮想マシンをパワーオンしないため、パワーオン後のコマンドを実行できません。

## メッセージ プロンプト リカバリ手順

メッセージ プロンプトを発行するカスタム復旧ステップが失敗することはありません。代わりに、プロンプトが閉じるまで、リカバリ プランは一時停止します。

## コマンド 手順を記述するためのガイドライン

リカバリ プランに追加するカスタム リカバリ手順のすべてのバッチ ファイル、スクリプト、またはコマンドは、一定の要件を満たす必要があります。

リカバリ プランに追加するコマンド ステップを作成する場合は、コマンド ステップの実行環境を必ず考慮してください。コマンド ステップでのエラーは、リカバリ プランの整合性に影響します。コマンドをプランに追加する前に、リカバリ サイトの Site Recovery Manager Server でテストします。

## Site Recovery Manager for Windows

- ローカル ホストでフル パスを使用して Windows コマンド シェルを起動する必要があります。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 ラインを使用します。

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

- バッチ ファイルとコマンドは、リカバリ サイトの Site Recovery Manager Server にインストールする必要があります。
- バッチ ファイルとコマンドは、300 秒以内に終了する必要があります。そうしないと、エラーが発生してリカバリ プランが終了します。この制限を変更するには、[リカバリ設定の変更](#)を参照してください。
- 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 エンコードを使用する必要があります。Site Recovery Manager は、スクリプト出力の最後の 4 KB のみをログ ファイルとリカバリ履歴に記録します。さらに多くの出力を生成するスクリプトでは、その出力を標準出力に送信してログに記録するのではなく、ファイルにリダイレクトされるようにします。

## Site Recovery Manager Appliance

- スクリプトは、管理者ユーザーのホーム ディレクトリ `/home/admin` にコピーする必要があります。
- SRM ユーザーが実行できるように、スクリプトのアクセス権限を変更する必要があります。たとえば、bash スクリプトの場合は、次のコマンド ラインを使用します。

```
chmod 755 Myscript.sh
```

- スクリプトを実行する場合は、ローカル ホストのフル パスを使用する必要があります。たとえば、bash スクリプトを実行するには、次のコマンドを使用します。

```
/bin/sh /home/admin/Myscript.sh
```

## コマンド ステップの環境変数

Site Recovery Manager は、カスタム復旧ステップのコマンドで使用できる環境変数を使用可能にします。



Site Recovery Manager Server でのコマンド ステップは、Site Recovery Manager サービス アカウントの ID を使用して実行されます。デフォルトの構成では、リカバリした仮想マシンでのコマンド手順は、VMware Tools サービス アカウントの ID を使用して実行されます。[recovery.autoDeployGuestAlias] 設定と互換性のある仮想マシンのデフォルトの構成は変更できます。[recovery.autoDeployGuestAlias] 設定については、[リカバリ設定の変更](#)を参照してください。

Site Recovery Manager は、コマンド手順を実行している間だけ環境変数を設定します。コマンドが完了すると、特定の環境変数は Site Recovery Manager Server およびリカバリした仮想マシンのゲスト OS には存在しません。

表 7-1. すべてのコマンド ステップで使用可能な環境変数

名前	値	例
<i>VMware_RecoveryName</i>	実行中の復旧プランの名前。	プラン A
<i>VMware_RecoveryMode</i>	復旧モード。	テストまたは復旧
<i>VMware_VC_Host</i>	復旧サイトでの vCenter Server のホスト名。	vc_hostname.example.com
<i>VMware_VC_Port</i>	vCenter Server への接続に使用するネットワーク ポート。	443

Site Recovery Manager は、Site Recovery Manager Server またはリカバリされた仮想マシンのいずれかで実行される仮想マシンごとのコマンド ステップで追加の環境変数を利用できるようにします。

表 7-2. 仮想マシンごとのコマンド ステップで使用可能な環境変数

名前	値	例
<i>VMware_VM_Uuid</i>	この仮想マシンを一意に識別するために vCenter Server により使用される UUID。	4212145a-eeae-a02c-e525-ebba70b0d4f3
<i>VMware_VM_Name</i>	この仮想マシンの名前。保護サイトで設定されます。	新規仮想マシン
<i>VMware_VM_Ref</i>	仮想マシンの管理対象オブジェクト ID。	vm-1199
<i>VMware_VM_Guest</i> 名前	VIM API により定義されたゲスト OS の名前。	otherGuest
<i>VMware_VM_GuestIp</i>	仮想マシンの IP アドレス（判明している場合）。	192.168.0.103
<i>VMware_VM_Path</i>	仮想マシンの VMX ファイルへのパス。	[datastore-123] jquser-vm2/jquser-vm2.vmx

表 7-3. リカバリした仮想マシンで実行される仮想マシンごとのコマンド手順で使用可能な環境変数

名前	値および説明	例
<code>VMware_GuestOp_OutputFile</code>	<p>値はコマンド出力ファイルへのパスです。</p> <p>コマンドによりファイルが作成されると、Site Recovery Manager はファイルのコンテンツをダウンロードし、結果としてそれをリカバリプランの履歴およびサーバ ログに追加します。</p> <p>Site Recovery Manager は、コマンド出力ファイルの最後の 4 KB 分をリカバリプランの履歴およびサーバ ログに追加します。スクリプトにより 4 KB を超える出力が生成された場合は、出力はカスタム場所に記録する必要があります。</p> <p>コマンドが終了すると、Site Recovery Manager はコマンド出力ファイルを削除します。</p>	<code>C:\Windows\TEMP\vmware0\srmStdOut.log</code>

### 例：Site Recovery Manager で実行できるコマンド

Site Recovery Manager for Windows の場合は、次のコンテンツを含む `myServerScript.bat` ファイルを作成できます。

```
@echo off
echo %DATE% %TIME% : Recovery Plan %VMware_RecoveryName% ran in %VMware_RecoveryMode% mode"
:: some more custom actions
```

`myServerScript.bat` ファイルを実行するには、次のコマンドを使用します。

```
C:\Windows\System32\cmd.exe /c C:\myScripts\myServerScript.bat > %VMware_GuestOp_OutputFile%
2>&1
```

Site Recovery Manager Appliance の場合は、次のコンテンツを含む `myServerScript.sh` スクリプトを作成できます。

```
clear
echo "$(date "+%Y-%m-%d %H:%M:%S") : Recovery Plan $VMware_RecoveryName ran in
$VMware_RecoveryMode mode"
# some more custom actions
```

**注：** スクリプトにコマンドを記述するときは、縦棒 (|) と単一引用符 (') 記号を使用しないでください。

`myServerScript.bat` スクリプトを実行するには、次のコマンド コンテンツを使用します。

```
/bin/sh /home/admin/myServerScript.sh
```

### 例：リカバリした仮想マシンで実行するコマンドのコンテンツ

Windows のゲスト OS の場合、次のコンテンツを含む `myGuestScript.bat` ファイルを作成できます。

```
@echo off
echo %DATE% %TIME% : VM %VMware_VM_Name% recovered by RP %VMware_RecoveryName% ran in
%VMware_RecoveryMode% mode
echo %DATE% %TIME% : Configured with the following FQDN: %VMware_VM_GuestName% and IP:
```

```
%VMware_VM_GuestIp%
:: some more custom actions
```

myGuestScript.bat ファイルを実行するには、次のコマンドを使用します。

```
C:\Windows\System32\cmd.exe /c C:\myScripts\myGuestScript.bat > %VMware_GuestOp_OutputFile%
2>&1
```

Linux または UNIX のゲスト OS の場合、次のコンテンツを含む myGuestScript.sh ファイルを作成できます。

```
echo $(date) : VM $VMware_VM_Name recovered by $VMware_RecoveryName ran
echo $(date) : Configured with the following FQDN: $VMware_VM_GuestName and IP:
$VMware_VM_GuestIp
# some more custom actions
```

myGuestScript.sh ファイルを実行するには、次のコマンドを使用します。

```
/bin/sh myGuestScript.sh &>$VMware_GuestOp_OutputFile
```

## トップレベルのメッセージ プロンプトまたはコマンド手順の作成

リカバリ プランのどこにでもトップレベルのリカバリ手順を追加できます。トップレベルのコマンド手順は、リカバリ時に Site Recovery Manager Server で実行するコマンドやスクリプトです。リカバリ時に、ユーザーの了承が必要なメッセージ プロンプトを表示する手順も追加できます。

### 前提条件

カスタム ステップを追加するリカバリ プランがあります。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブでリカバリ プランを選択し、[リカバリ手順] をクリックします。
- 4 [表示] ドロップダウン メニューで、追加する手順のタイプを選択します。

オプション	説明
[テスト手順]	リカバリ プランを手順するときに実行する手順を追加します。
[リカバリ手順]	計画移行やディザスタ リカバリを行う際に実行する手順を追加します。

クリーンアップや再保護の操作には手順を追加できません。

- 5 ステップを追加する場所を選択します。
  - 手順の前に手順を追加するには、目的の手順を右クリックして [先行する手順を追加] を選択します。
  - 最後の手順の後に手順を追加するには、最後の手順を右クリックして [後続の手順を追加] を選択します。

- 6 [SRM Server でのコマンド] または [プロンプト] を選択します。
- 7 [名前] テキスト ボックスに、手順の名前を入力します。  
[リカバリ手順] ビューの手順のリストに手順名が表示されます。
- 8 [内容] テキスト ボックスにコマンド、スクリプト、またはメッセージ プロンプトを入力します。
  - [SRM Server でのコマンド] を選択した場合は、実行するコマンドまたはスクリプトを入力します。
  - [プロンプト] を選択した場合は、リカバリ プランの実行時に表示するメッセージの内容を入力します。
- 9 (オプション) コマンドの [タイムアウト] 設定を変更して Site Recovery Manager Server で実行します。  
このオプションは、プロンプト手順を作成する場合は使用できません。
- 10 [追加] をクリックしてリカバリ プランにステップを追加します。

#### 次のステップ

新規作成した手順を右クリックして、この手順を編集または削除するオプションや、この手順の前後に手順を追加するオプションを選択できます。

## 個別の仮想マシンのメッセージ プロンプトまたはコマンド ステップの作成

Site Recovery Manager による仮想マシンのパワーオンの前後に、ユーザーにタスクの実行を求めるプロンプトを表示したり、Site Recovery Manager が仮想マシンにタスクを実行したりするためのカスタム リカバリ手順を構成できます。

Site Recovery Manager は、カスタマイズ情報と同じ方法で、保護された仮想マシンまたはリカバリされた仮想マシンにコマンド手順を関連付けます。複数のリカバリ プランに同じ仮想マシンが含まれる場合、Site Recovery Manager はすべてのリカバリ プランにコマンドとプロンプトを含めます。

#### 前提条件

カスタム ステップを追加するリカバリ プランがあります。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブでリカバリ プランを選択し、[リカバリ手順] をクリックします。
- 4 仮想マシンを右クリックして、[リカバリの構成] をクリックします。
- 5 [リカバリ プロパティ] タブで、[パワーオン前の手順] または [パワーオン後の手順] をクリックします。
- 6 プラス アイコンをクリックして、ステップを追加します。

## 7 作成する手順の種類を選択します。

オプション	説明
[プロンプト]	プランが次の手順に進む前に、ユーザーにタスクを実行するように求めるか、またはユーザーによる確認が必要な情報を提供するように求めます。このオプションは、パワーオン前の手順とパワーオン後の手順の両方で使用できます。
[SRM Server でのコマンド]	Site Recovery Manager Server でコマンドを実行します。このオプションは、パワーオン前の手順とパワーオン後の手順の両方で使用できます。
[リカバリした仮想マシンでのコマンド]	リカバリした仮想マシンでコマンドを実行します。このオプションは、パワーオン後の手順でのみ使用できます。

## 8 [名前] テキスト ボックスに、手順の名前を入力します。

[リカバリ手順] ビューの手順のリストに手順名が表示されます。

## 9 [内容] テキスト ボックスにコマンド、スクリプト、またはメッセージ プロンプトを入力します。

- [SRM Server でのコマンド] または [リカバリした仮想マシンでのコマンド] を選択した場合は、実行するコマンドまたはスクリプトを入力します。
- [プロンプト] を選択した場合は、リカバリ プランの実行時に表示するメッセージの内容を入力します。

## 10 (オプション) コマンドの [タイムアウト] 設定を変更して Site Recovery Manager Server で実行します。

このオプションは、プロンプト手順を作成する場合は使用できません。

## 11 リカバリ プランに手順を追加するには、[追加] をクリックします。

## 12 パワーオン前またはパワーオン後にコマンドを実行するように仮想マシンを再構成するには、[OK] をクリックします。

# リカバリ プラン実行時の仮想マシンのサスペンド

Site Recovery Manager では、リカバリおよびテスト リカバリ中にリカバリ サイトの仮想マシンをサスペンドできます。

リカバリ サイトの仮想マシンのサスペンドは、アクティブ/アクティブ データセンター環境を使用していて、リカバリ サイトで重要度の低いワークロードが実行されている場合に有効です。リカバリ サイトで重要度の低いワークロードをホストしている仮想マシンをサスペンドすると、Site Recovery Manager はリカバリされた仮想マシンのために容量を解放できます。Site Recovery Manager は、フェイルオーバーが逆方向に実行されるときに、フェイルオーバー処理中にサスペンドされた仮想マシンを再開します。

サスペンドする仮想マシンを追加できるのは復旧サイトだけです。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランをクリックして、[リカバリ手順] をクリックします。

- 4 [リカバリ サイトの重要度の低い仮想マシンをサスペンド] を右クリックし、[重要度の低い仮想マシンの追加または削除] をクリックします。
- 5 リカバリ サイトでリカバリ中にサスペンドする仮想マシンを選択します。
- 6 [保存] をクリックします。

#### 結果

Site Recovery Manager は、リカバリ プランの実行中にリカバリ サイトの仮想マシンをサスペンドします。

## 仮想マシンの復旧優先順位の指定

デフォルトで Site Recovery Manager は、新しいリカバリ プランに含まれるすべての仮想マシンをリカバリ優先順位レベル 3 に設定します。仮想マシンのリカバリ優先順位は、上下させることができます。リカバリ優先順位は、仮想マシンのシャットダウンとパワーオンの順序を決定します。

仮想マシンの優先順位を変更すると、Site Recovery Manager は、この仮想マシンが含まれるすべてのリカバリプランに新しい優先順位を適用します。

Site Recovery Manager は、設定した優先順位に従ってリカバリ サイトの仮想マシンを起動します。Site Recovery Manager は最初に優先順位 1 の仮想マシン、次に優先順位 2 の仮想マシン、という順番で仮想マシンを起動します。Site Recovery Manager は VMware Tools のハートビートを使用して、リカバリ サイトで動作している仮想マシンを検出します。この方法により、Site Recovery Manager は、優先順位を与えられたすべての仮想マシンが次の優先順位を持つ仮想マシンが起動する前に実行していることを確認できます。したがって、保護対象の仮想マシンに VMware Tools をインストールする必要があります。

---

**注意：** 拡張されたストレージの移行に適した仮想マシンの優先順位が、移行に適していない仮想マシンの優先順位よりも低い場合、移行に適した仮想マシンは移行されません。

---

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランをクリックして、[仮想マシン] をクリックします。
- 4 仮想マシンを右クリックし、[優先グループ] をクリックします。
- 5 仮想マシンの新しい優先順位を選択します。  
最高の優先順位は 1、最低の優先順位は 5 です。
- 6 優先順位の変更を確認するには、[はい] をクリックします。

## 仮想マシンの依存関係の構成

仮想マシンが、同じ保護グループの別の仮想マシンで実行するサービスに依存する場合は、これらの仮想マシン間の依存関係を構成できます。依存関係を構成すると、リカバリ サイトで仮想マシンを正しい順序で開始できます。依存関係は、同じ優先順位の仮想マシンでのみ有効です。

**注意：** 拡張されたストレージの移行に適した仮想マシンが、拡張されたストレージの移行に適していない仮想マシンに依存している場合、移行に適した仮想マシンは移行されません。

リカバリ プランを実行すると、Site Recovery Manager は、まず他の仮想マシンが依存する仮想マシンを開始してから、依存関係のある仮想マシンを開始します。Site Recovery Manager が、別の仮想マシンが依存する仮想マシンを開始できない場合、リカバリ プランは続行されますが警告が表示されます。同じリカバリ優先グループに属している仮想マシン間の依存関係のみを構成できます。優先順位の低いグループに属している仮想マシンに依存するように仮想マシンを設定すると、Site Recovery Manager は依存関係をオーバーライドし、優先順位の高いグループに属している仮想マシンを最初に開始します。

依存仮想マシンを含む保護グループをリカバリ プランから削除すると、依存関係がある仮想マシンの依存関係で、保護グループのステータスがこのプランにない に設定されます。構成した仮想マシンに、その仮想マシンが依存する仮想マシンとは異なる優先順位が設定されている場合、依存仮想マシンのステータスは [低優先度] または [高優先度] に設定されます。

### 前提条件

依存関係のある仮想マシンとその仮想マシンが依存する仮想マシンが同じリカバリ プラン、および同じリカバリ優先グループに属していることを確認します。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランをクリックして、[仮想マシン] をクリックします。
- 4 1 台以上の他の仮想マシンに依存する仮想マシンを右クリックして [リカバリの設定] をクリックします。
- 5 [仮想マシンの依存関係] を展開します。
- 6 ドロップダウン メニューから [すべてを表示] を選択します。
- 7 選択したリカバリ プランのすべての仮想マシンのリストから、1 台以上の仮想マシンを選択します。  
選択した仮想マシンが、依存関係のリストに追加されます。
- 8 [仮想マシンの依存関係] リストにある仮想マシンがオンになっていること、および依存関係のステータスが [OK] であることを確認します。
- 9 (オプション) 依存関係を削除するには、ドロップダウン メニューから [仮想マシンの依存関係を表示] を選択し、この仮想マシンが依存する仮想マシンのリストから仮想マシンを選択し、[削除] をクリックします。
- 10 [OK] をクリックします。

## 計画移行用の vSphere vMotion の有効化

vSphere vMotion による仮想マシンの移行は、計画移行でのみ可能です。vSphere vMotion は [リカバリ プロパティ] ダイアログ ボックスで有効または無効にすることができます。

### 前提条件

- vSphere vMotion による移行を実行する前に、仮想マシンがストレージ ポリシー保護グループに属していること、拡張されたストレージに配置されていること、およびパワーオンされていることを確認します。
- インベントリ マッピングが完全に構成されていることを確認します。一時的なプレースホルダ インベントリ マッピングのみが構成された状態で、[使用可能な仮想マシンの vMotion を有効化] オプションを指定して計画移行を実行すると、両方のサイトが実行中であっても計画移行は失敗します。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランをクリックして、[仮想マシン] タブをクリックします。
- 4 仮想マシンを右クリックして、[リカバリの構成] をクリックします。  
[計画移行に vMotion を使用します (仮想マシンをパワーオンする必要があります)] を選択します。
- 5 [OK] をクリックします。

### 結果

計画移行中に電源の入れ直しは行われません。構成済みのシャットダウンや起動、またはパワーオン前に構成されたステップは無視されます。パワーオン後に構成された手順は実行されます。

## 仮想マシンの起動およびシャットダウン オプションの構成

リカバリ サイトでのリカバリ中に仮想マシンを起動およびシャットダウンする方法を構成できます。

仮想マシンのゲスト OS を保護サイトでパワーオフする前にシャットダウンするかどうかを構成できます。リカバリ サイトで仮想マシンをパワーオンするかどうかを構成できます。リカバリ プランを続行する前に VMware Tools またはその他のアプリケーションをリカバリした仮想マシンで起動できるように、仮想マシンのパワーオン後の遅延を構成することもできます。

### 前提条件

リカバリ プランを作成しました。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。



- 3 [リカバリ プラン] タブをクリックし、リカバリ プランをクリックして、[仮想マシン] をクリックします。
- 4 仮想マシンを右クリックして、[リカバリの構成] をクリックします。
- 5 [シャットダウン アクション] を展開し、この仮想マシンに対するシャットダウン メソッドを選択します。

オプション	説明
[パワーオフ前にゲスト OS をシャットダウン]	仮想マシンをパワーオフする前に正常にシャットダウンします。シャットダウン操作のタイムアウト期間を設定できます。タイムアウト期間を 0 に設定することは、パワーオフ オプションと同じです。このオプションを使用するには、VMware Tools が仮想マシンで実行されている必要があります。  <b>注：</b> タイムアウトになると、仮想マシンがパワーオフします。タイムアウトになったことによって仮想マシンの OS がシャットダウン タスクを完了しなかった場合には、データの損失が発生することがあります。シャットダウンに長い時間を要する大規模な仮想マシンには、それに応じてパワーオフのタイムアウトを長く設定します。
[パワーオフ]	ゲスト OS をシャットダウンすることなく仮想マシンをパワーオフします。

- 6 [起動アクション] を展開し、リカバリ後に仮想マシンをパワーオンするかどうかを選択します。

オプション	説明
[パワーオンする]	リカバリ サイトで仮想マシンをパワーオンします。
[パワーオンしない]	仮想マシンをリカバリしますが、パワーオンはしません。

- 7 (オプション) [VMware Tools の待機] チェック ボックスをオンまたはオフにします。

このオプションは、[手順 6](#) で [パワーオン] を選択した場合のみ使用できます。

[VMware Tools の待機] を選択すると、Site Recovery Manager は仮想マシンのパワーオン後に VMware Tools が起動するまで待機してから、リカバリ プランの次の手順に進みます。VMware Tools が起動するタイムアウト期間を設定できます。

- 8 (オプション) [パワーオン後の手順の実行および従属仮想マシンの起動前の追加遅延時間] チェック ボックスを選択または選択解除し、追加の遅延時間を指定します。

このオプションは、[手順 6](#) で [パワーオン] を選択した場合のみ使用できます。

たとえば、仮想マシンをパワーオンした後に、別の仮想マシンが依存するアプリケーションが起動できるように、追加の遅延を指定することもできます。

## 仮想マシンの保護とリカバリに関する制限事項

仮想マシンの Site Recovery Manager による保護とリカバリは制限の対象になります。

### サスペンドされた仮想マシンの保護と復旧

仮想マシンをサスペンドすると、vSphere によってそのメモリ状態が作成および保護されます。仮想マシンを再開すると、保存されたメモリ状態が vSphere によって復元されるため、仮想マシンは実行しているアプリケーションとゲスト OS の処理を中断なく操作を継続することができます。

## スナップショットのある仮想マシンの保護と復旧

アレイベース レプリケーションは、スナップショットのある仮想マシンの保護と復旧をサポートしますが、制限があります。

スナップショットの差分ファイルを保存するためのカスタム ロケーションを指定するには、workingDir パラメータを VMX ファイルで設定します。Site Recovery Manager では、workingDir パラメータの使用はサポートされていません。

vSphere Replication では、スナップショットを含む仮想マシンの保護がサポートされていますが、リカバリできるのは最新のスナップショットのみです。vSphere Replication では、リカバリされた仮想マシンのスナップショット情報が削除されます。その結果、複数のポイント イン タイムのスナップショットを維持するように vSphere Replication を構成しない限り、スナップショットはリカバリ後に使用できなくなります。vSphere Replication で複数のポイント イン タイム スナップショットを使用して古いスナップショットをリカバリすることについては、「[仮想マシンのレプリケートと複数の特定の時点のインスタンスの有効化](#)」を参照してください。

## メモリ状態スナップショットのある仮想マシンの保護と復旧

メモリ状態スナップショットのある仮想マシンを保護する場合、保護サイトとリカバリ サイトの ESXi ホストは、VMware ナレッジベースの記事 [vMotion CPU Compatibility Requirements for Intel Processors](#) および [vMotion CPU Compatibility Requirements for AMD Processors](#) に記載されているとおり、互換性のある CPU を搭載している必要があります。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二つの機能は、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。

## リンク クローン仮想マシンの保護と復旧

vSphere Replication では、リンク クローンである仮想マシンの保護と復旧はサポートされていません。

アレイベース レプリケーションでは、スナップショット ツリーのすべてのノードがレプリケートされた場合に、リンク クローンである仮想マシンの保護と復旧がサポートされます。

## 予約、アフィニティ ルール、制限による仮想マシンの保護と復旧

Site Recovery Manager は、仮想マシンを復旧サイトに復旧するとき、仮想マシンに配置した予約、アフィニティ ルール、または制限を保存しません。Site Recovery Manager がリカバリ サイトの予約、アフィニティ ルール、および制限を保持しないのは、リカバリ サイトに保護サイトとは異なるリソース要件が存在する場合があるためです。唯一の例外は、[Reserve all guest memory (All locked)] 設定です (保護された仮想マシンで有効になっている場合)。

復旧された仮想マシンに予約、アフィニティ ルール、および制限を設定するには、復旧サイトのリソース プールで予約と制限を構成し、リソース プールのマッピングをそれぞれ設定します。また、復旧サイトのプレースホルダ仮想マシンで予約、アフィニティ ルール、制限を手動で設定することもできます。

## 複数のアレイ上にコンポーネントがある仮想マシンの保護と復旧

Site Recovery Manager でのアレイベース レプリケーションは、アレイ ペア概念に依存します。Site Recovery Manager は、復旧するデータストアのグループを 1 つのユニットとして定義します。その結果、アレイベース レプリケーションを使用して保護する仮想マシンのコンポーネントを格納する方法が制限されます。

- Site Recovery Manager は、リカバリ サイトの単一アレイにレプリケートされる仮想マシン コンポーネントを保護サイトの複数アレイに格納することはサポートしていません。
- Site Recovery Manager は、仮想マシン コンポーネントが保護サイトのアレイとリカバリ サイトのアレイの両方にまたがっている場合、リカバリ サイトの複数アレイにレプリケートされる仮想マシン コンポーネントを保護サイトの複数アレイに格納することはサポートしていません。

複数アレイの仮想マシン コンポーネントを復旧サイトの単一アレイまたはアレイの範囲内にレプリケートする場合、保護サイトにあるデータストアの UUID の VMX 構成は復旧サイトの構成に一致しません。

仮想マシンの VMX ファイルの場所によって、仮想マシンが属するアレイ ペアが決定されます。仮想マシンは 2 つのアレイ ペアに属することはできません。そのため、仮想マシンに複数のディスクがあり、そのうち 1 つが、仮想マシンが属するアレイ ペアに含まれていないアレイに存在する場合は、Site Recovery Manager は仮想マシン全体を保護できません。Site Recovery Manager は、仮想マシンと同じアレイ ペアにないディスクをレプリケートされないデバイスとして処理します。

したがって、Site Recovery Manager が仮想マシンのすべてのコンポーネントを保護できるように、LUN の仮想マシンのすべての仮想ディスク、スワップ ファイル、RDM デバイス、および作業ディレクトリを同じアレイに格納します。

# 仮想マシンの IP プロパティのカスタマイズ

## 8

仮想マシンの IP 設定は、保護サイトとリカバリ サイトでカスタマイズできます。仮想マシンの IP プロパティをカスタマイズすると、リカバリされた仮想マシンがターゲット サイトで起動するとき、既定の IP 設定がオーバーライドされます。

仮想マシンの IP プロパティをカスタマイズしない場合、Site Recovery Manager は、保護サイトからリカバリ サイトへのリカバリまたはそのテストを実行する際に、リカバリ サイトの IP 設定を使用します。Site Recovery Manager は、元のリカバリ サイトから元の保護サイトへのリカバリまたはそのテストを実行する際に、再保護後の保護サイトの IP 設定を使用します。

Site Recovery Manager は、さまざまなタイプの IP カスタマイズをサポートします。

- IPv4 および IPv6 アドレスの使用。
- サイトごとに異なる IP カスタマイズの構成。
- DHCP、固定 IPv4、または固定 IPv6 アドレスの使用。
- Windows 仮想マシンと Linux 仮想マシンのアドレスのカスタマイズ。
- 仮想マシンごとに複数の NIC のカスタマイズ。

---

**注：** 1 つの NIC に構成するのは 1 つの IP アドレスのみです。

---

Site Recovery Manager が IP カスタマイズをサポートしているゲスト OS のリストについては、<https://docs.vmware.com/jp/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.html> に掲載されている「Site Recovery Manager 8.2 の互換性マトリックス」を参照してください。

カスタマイズ設定は、保護された仮想マシンに関連付けます。そのため、同じ保護仮想マシンが複数のリカバリ プランに含まれている場合、すべてのリカバリ プランで 1 つのカスタマイズ設定のコピーが使用されます。IP のカスタマイズは、仮想マシンのリカバリ プロパティを構成するプロセスの一部として構成します。

リカバリ サイトで NIC をカスタマイズしない場合には、NIC は引き続き保護サイトの IP 設定を使用し、サイトが逆の場合も同様です。Site Recovery Manager はリカバリ中に仮想マシンに IP カスタマイズを適用しません。

IP のカスタマイズは、個々の仮想マシンか複数の仮想マシンに適用できます。

仮想マシンで IP カスタマイズを構成する場合、Site Recovery Manager はこれらの仮想マシンにリカバリ手順を追加します。

### ゲスト OS の起動

ゲストの起動プロセスは、IP カスタマイズを構成するすべての仮想マシンで並列して実行されます。

## IP のカスタマイズ

Site Recovery Manager は、IP カスタマイズを仮想マシンにプッシュします。

### ゲスト OS のシャットダウン

Site Recovery Manager は、変更を反映し、仮想マシンの再起動時にゲスト OS のサービスによってその変更が適用されるように、仮想マシンをシャットダウンしてから再起動します。

IP のカスタマイズ プロセスが終了した後、仮想マシンは、優先グループ、およびユーザーが設定した依存関係にしたがってオンになります。

---

**注：** 仮想マシンの IP のプロパティをカスタマイズするには、仮想マシンに VMware Tools または VMware OSP (Operating System Specific Packages) をインストールする必要があります。<http://www.vmware.com/download/packages.html> を参照してください。

---

#### ■ 個々の仮想マシンの IP プロパティの手動カスタマイズ

個々の仮想マシンの IP 設定は、保護サイトとリカバリ サイトの両方で手動でカスタマイズできます。

#### ■ 複数の仮想マシンの IP プロパティのカスタマイズ

DR IP Customizer ツールを使用し、サブネット レベルの IP マッピング ルールを定義することにより、保護サイトとリカバリ サイトの複数の仮想マシンの IP プロパティをカスタマイズできます。

## 個々の仮想マシンの IP プロパティの手動カスタマイズ

個々の仮想マシンの IP 設定は、保護サイトとリカバリ サイトの両方で手動でカスタマイズできます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランをクリックして、[仮想マシン] をクリックします。
- 4 仮想マシンを右クリックして、[リカバリの構成] をクリックします。
- 5 [IP カスタマイズ] タブをクリックして、ドロップダウン メニューから [手動の IP カスタマイズ] を選択します。
- 6 IP 設定を変更する NIC を選択します。
- 7 設定する IP アドレスのセットに応じて、保護サイトまたはリカバリ サイトに対して [構成] をクリックします。
- 8 IPv4 設定を行うには、[IPv4] タブをクリックします。
  - DHCP を選択するか、固定アドレスの場合、IP アドレス、サブネット情報、およびゲートウェイ サーバのアドレスを入力します。
  - 仮想マシンがパワーオンされていて、VMware Tools がインストールされている場合は、[取得] をクリックして、仮想マシンに構成されている現在の設定をインポートできます。

## 9 IPv6 設定を行うには、[IPv6] タブをクリックします。

- DHCP を選択するか、固定アドレスの場合、IP アドレス、サブネット情報、およびゲートウェイ サーバのアドレスを入力します。
- 仮想マシンがパワーオンされていて、VMware Tools がインストールされている場合は、[取得] をクリックして、仮想マシンに構成されている現在の設定をインポートできます。

## 10 DNS 設定を行うには、[DNS] タブをクリックします。

### ■ 表 8-1. DNS 設定

設定	オプション
DNS サーバ	DNS サーバの検出方法を選択します。 <ul style="list-style-type: none"> <li>■ DHCP を使用して DNS アドレスを自動的に取得します。</li> <li>■ 優先 DNS サーバおよび代替 DNS サーバを指定します。</li> </ul>
DNS サフィックス	DNS サフィックスを入力して [追加] をクリックするか、既存の DNS サフィックスを選択して [削除]、[上へ移動]、または [下へ移動] をクリックします。

- 仮想マシンがパワーオンされていて、VMware Tools がインストールされている場合は、[取得] をクリックして、仮想マシンに構成されている現在の設定をインポートできます。

## 11 (必須) [WINS] タブをクリックして、プライマリ WINS アドレスとセカンダリ WINS アドレスを入力します。

WINS タブは、Windows 仮想マシンの DHCP または IPv4 アドレスを構成する場合にのみ使用できます。

## 12 手順 7 から手順 10 を繰り返し、必要に応じてリカバリ サイトまたは保護サイトの設定を行います。

## 13 必要に応じて、他の NIC に対する構成プロセスを繰り返します。

### 結果

リカバリ サイトの設定はリカバリ中に適用されます。保護サイトの設定はフェイルバック中に適用されます。

**注：** 手動で IP カスタマイズを定義した仮想マシンは、リカバリ中の IP マッピング ルールの評価の対象ではありません。手動で指定した IP アドレス設定は IP アドレス マッピング ルールよりも優先されます。

## 仮想マシンへの IP カスタマイズ ルールの適用

保護された仮想マシンのリカバリ設定に IP カスタマイズ ルールを適用できます。

IP カスタマイズ ルールを適用する場合は、各ネットワーク マッピングにサブネット IP マッピング ルールを指定します。

詳細設定オプション `recovery.useIpMapperAutomatically` を `True` に設定し、仮想ネットワークの IP マッピング ルールを構成した場合、Site Recovery Manager はリカバリ時に仮想マシンをカスタマイズするサブネット IP マッピング ルールを評価します。このオプションを `False` に設定すると、Site Recovery Manager はリカバリ時に IP マッピング ルールを評価しません。[IP カスタマイズ] オプションを使用すると、各仮想マシンのこのオプションの効果をオーバーライドすることができます。

`recovery.useIpMapperAutomatically` のデフォルト オプションは True です。Auto に設定すると、Site Recovery Manager は IP カスタマイズ ルールを使用して仮想マシンをカスタマイズします。

#### 前提条件

Site Recovery Manager が IP カスタマイズをサポートしているゲスト OS のリストについては、<https://docs.vmware.com/jp/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.html> に掲載されている「Site Recovery Manager 8.2 の互換性マトリックス」を参照してください。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブを選択し、リカバリ プランをクリックして、[仮想マシン] を選択します。
- 4 仮想マシンを右クリックして、[リカバリの構成] をクリックします。
- 5 [IP カスタマイズ] モード リストから [該当する場合、IP カスタマイズ ルールを使用する] を選択して [OK] をクリックします。

## 複数の仮想マシンの IP プロパティのカスタマイズ

DR IP Customizer ツールを使用し、サブネット レベルの IP マッピング ルールを定義することにより、保護サイトとリカバリ サイトの複数の仮想マシンの IP プロパティをカスタマイズできます。

Site Recovery Manager の前のリリースでは、DR IP Customizer ツールを使用して複数の仮想マシンの IP プロパティをカスタマイズしていました。DR IP Customizer に加えて、サブネットレベルの IP カスタマイズ ルールを定義して複数の仮想マシンの IP プロパティをカスタマイズできます。

サブネット レベルの IP カスタマイズ ルールは、DR IP Customizer と組み合わせて使用できます。

- CSV ファイルを使用して複数の仮想マシンの IP カスタマイズ設定を明示的に定義する場合は、DR IP Customizer を使用するのが最も早い方法です。
- vSphere Web Client を使用して、仮想マシンにサブネット レベルの IP カスタマイズ ルールを適用します。

DR IP Customizer を使用して構成する仮想マシンは、サブネット レベルの IP カスタマイズ ルールの対象になりません。DR IP Customizer または IP サブネット ルールを使用して、同じ IP カスタマイズ結果を得ることができます。

## DR IP Customizer ツールを使用した複数の仮想マシンの IP プロパティのカスタマイズ

DR IP Customizer ツールを使用すると、保護サイトとリカバリ サイトで保護された複数の仮想マシンのための明示的な IP カスタマイズ設定を定義できます。

サブネット IP マッピング ルールの定義に加えて、DR IP Customizer ツールを使用して、仮想マシンをリカバリ サイトで起動する際にカスタマイズされたネットワーク設定を適用できます。カスタマイズされた IP 設定は、コマンドで区切られた値 (CSV) ファイルで DR IP Customizer ツールに提供します。



CSV ファイルを手動で作成するのではなく、DR IP Customizer ツールを使用して、保護された仮想マシンのネットワーク構成情報を含む CSV ファイルをエクスポートできます。このファイルを CSV ファイルのテンプレートとして利用し、ファイル内の値をカスタマイズして復旧サイトに適用できます。

- 1 DR IP Customizer を実行し、保護された仮想マシンのネットワーク情報を含む CSV ファイルを生成します。
- 2 復旧サイトに関連するネットワーク情報で、生成された CSV ファイルを変更します。
- 3 保護されたマシン上で DR IP Customizer を再度実行し、仮想マシンがリカバリ サイト上で起動するときに、ネットワーク構成情報を変更した CSV を適用します。

DR IP Customizer ツールを保護サイトからリカバリ サイトのいずれかで実行できます。保護された仮想マシンの仮想マシン ID は、サイトごとに異なるため、DR IP Customizer ツールを実行して CSV ファイルを生成するときにどのサイトを使用したとしても、設定の適用時に再度 DR IP Customizer を実行するときには、生成時と同じサイトを使用する必要があります。

保護サイトとリカバリ サイトの IP 設定をカスタマイズすると、再保護操作中に Site Recovery Manager が正しい構成を使用できます。

Site Recovery Manager が IP カスタマイズをサポートしているゲスト OS のリストについては、<https://docs.vmware.com/jp/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.html> に掲載されている「Site Recovery Manager 8.2 の互換性マトリックス」を参照してください。

#### ■ リカバリ プランの IP アドレス マッピングのレポート

IP アドレス マップ レポートは、サイトと復旧プランでグループ分けされた、保護仮想マシンとそのブレースホルダの IP プロパティを説明する XML ドキュメントを生成します。この情報は、復旧プランのネットワーク要件の理解に役立ちます。

#### ■ DR IP Customizer ツールの構文

DR IP Customizer ツールには、Site Recovery Manager が保護する仮想マシンのネットワーク情報の収集に使用できるオプションが含まれます。仮想マシンを復旧サイト上で起動するときに、これらのオプションを使用してカスタマイズを適用することもできます。

#### ■ DR IP Customizer CSV ファイルの構造

DR IP Customizer コンマで区切られた値 (CSV) ファイルには、ファイル内の各列の意味を定義するヘッダー行および復旧プランの各ブレースホルダ仮想マシンの 1 つまたは複数の行が含まれています。

#### ■ DR IP Customizer CSV ファイルの変更

DR IP Customizer のコンマで区切られた値 (CSV) ファイルを変更し、カスタマイズされたネットワーク設定を復旧サイト上での起動時に仮想マシンに適用します。

#### ■ DR IP Customizer の実行による複数の仮想マシンの IP プロパティのカスタマイズ

DR IP Customizer ツールを使用して、Site Recovery Manager が保護する複数の仮想マシンの IP プロパティをカスタマイズできます。

### リカバリ プランの IP アドレス マッピングのレポート

IP アドレス マップ レポートは、サイトと復旧プランでグループ分けされた、保護仮想マシンとそのブレースホルダの IP プロパティを説明する XML ドキュメントを生成します。この情報は、復旧プランのネットワーク要件の理解に役立ちます。



IP アドレス マップ レポートは両方のサイトに接続する必要があるため、ユーザーはいずれかのサイトでコマンドを実行できます。コマンドの実行時に、各サイトの vCenter Server ログイン認証情報を入力するよう求めるプロンプトが表示されます。

#### 手順

- 1 保護サイトまたはリカバリ サイトのいずれかの Site Recovery Manager Server ホストにログインし、コマンド プロンプトを開きます。
- 2 作業ディレクトリを次のディレクトリに変更します。

- Windows の場合 : C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin
- Linux の場合 : /opt/vmware/srm/bin/

- 3 dr-ip-reporter コマンドを実行します。

- Platform Services Controller に単一の vCenter Server インスタンスがある場合には、以下のコマンドを実行します。

- Windows の場合 :

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

- Linux の場合 :

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out path_to_report_file.xml
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

この例では、dr-ip-reporter で Site Recovery Manager Server の vmware-dr.xml ファイルを指定し、https://Platform\_Services\_Controller\_address で Platform Services Controller に関連付けられた vCenter Server インスタンスにレポート ファイルを生成しています。

- 複数の vCenter Server インスタンスがある Platform Services Controller を使用している場合は、--vcid パラメータに vCenter Server ID を指定する必要があります。

- Windows の場合 :

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

- Linux の場合 :

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

この例では、dr-ip-reporter で Site Recovery Manager Server の vmware-dr.xml ファイルを指定し、ID が `vCenter_Server_ID` の vCenter Server インスタンスにレポート ファイルを生成しています。

**注：** vCenter Server ID は vCenter Server の名前とは同じではありません。

- ネットワークのリストを特定のリカバリ プランが必要とするものだけに制限するには、コマンド ラインに `--plan` オプションを含めます。

- Windows の場合：

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--plan recovery_plan_name
```

- Linux の場合：

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--plan recovery_plan_name
```

## DR IP Customizer ツールの構文

DR IP Customizer ツールには、Site Recovery Manager が保護する仮想マシンのネットワーク情報の収集に使用できるオプションが含まれます。仮想マシンを復旧サイト上で起動するときに、これらのオプションを使用してカスタマイズを適用することもできます。

**注：** Site Recovery Manager では、DR IP Customizer ツールを使用して、サブネットレベル IP マッピング ルールを定義して、仮想マシンの IP アドレス設定をカスタマイズすることができます。サブネットレベル IP マッピング ルールを DR IP Customizer と組み合わせて使用できます。サブネットレベル IP マッピング ルールと DR IP Customizer を一緒に使用する方法については、[複数の仮想マシンの IP プロパティのカスタマイズ](#)を参照してください。

- Windows 版の Site Recovery Manager を使用している場合は、Site Recovery Manager Server ホスト マシンの `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` フォルダで `dr-ip-customizer.exe` 実行可能ファイルを検索します。
- Site Recovery Manager Virtual Appliance を使用している場合は、アプライアンスの `/opt/vmware/srm/bin/` ディレクトリに `dr-ip-customizer` が配置されています。

`dr-ip-customizer.exe` または `dr-ip-customizer` を実行するときは、カンマ区切り値 (CSV) ファイルを生成するのか、それとも適用するのかによって異なるオプションを指定します。

```
dr-ip-customizer.exe
--cfg SRM サーバ構成 XML
--cmd apply/drop/generate
[--csv 既存の CSV ファイル名]
[--out 生成する新規 CSV ファイル名]
--uri https://host[:port]/lookupservice/sdk
```

```
--vcid UUID
[--ignore-thumbprint]
[--extra-dns-columns]
[--verbose]
```

DR IP Customizer ツールを保護サイトからリカバリ サイトのいずれかで実行できます。保護された仮想マシンの仮想マシン ID は、サイトごとに異なるため、DR IP Customizer ツールを実行して CSV ファイルを生成するときには、どのサイトを使用したとしても、設定の適用時に再度 DR IP Customizer を実行するときには、生成時と同じサイトを使用する必要があります。

DR IP Customizer ツールが提供するオプションの中には、必須のものと任意のものがあります。

**表 8-2. DR IP Customizer のオプション**

オプション	説明	必須
-h [ --help ]	dr-ip-customizer.exe または dr-ip-customizer の使用に関する情報が表示されます。	いいえ
--cfg arg	アプリケーション XML 構成ファイル vmware-dr.xml へのパス。	はい
--cmd arg	別のコマンドを指定して、DR IP Customizer を別のモードで実行します。 <ul style="list-style-type: none"> <li>■ apply コマンドは、既存の CSV ファイルから Site Recovery Manager Server インスタンスのリカバリ プランにネットワーク カスタマイズ設定を適用します。</li> <li>■ generate コマンドは、Site Recovery Manager が vCenter Server インスタンスのために保護するすべての仮想マシンの基本 CSV ファイルを生成します。</li> <li>■ drop コマンドは、入力 CSV ファイルで指定された仮想マシンから復旧設定を削除します。</li> </ul> CSV を生成するために使用したのと同じ vCenter Server インスタンスを、常に apply および drop コマンドに指定します。	はい
--csv arg	CSV ファイルへのパス。	apply と drop コマンドを実行する場合は、はい。
-o [ --out ] arg	generate コマンドが作成する新しい CSV 出力ファイルの名前。既存の CSV ファイルの名前を指定する場合は、generate コマンドで現在の内容が上書きされます。	generate コマンドを実行する場合は、はい。

表 8-2. DR IP Customizer のオプション（続き）

オプション	説明	必須
--uri arg	https://host[:port]/ lookupservice/sdk 形式の Platform Service Controller の Lookup Service URL。ポート番号が 443 でない場合、指定し ます。Site Recovery Manager インスタ ンスにより、このアドレスはプライマリ サイト のインフラノードと関連づけられます。  CSV を生成するために使用したものと 同じ vCenter Server インスタンスを、 apply および drop コマンドに使用します。	はい
--vcid arg	プライマリ サイトの vCenter Server イン スタンス UUID。	オプション。プライマリ サイトのインフラ ストラクチャが複数の vCenter Server イン スタンスを含んでいない場合。
-i [ --ignore-thumbprint ]	vCenter Server サムプリント確認プロンプ トを無視します。	いいえ
-e [ --extra-dns-columns ]	入力 CSV ファイルに DNS 情報の追加列が 含まれる場合に指定する必要があります。	いいえ
-v [ --verbose ]	詳細出力を有効にします。任意の dr-ip- customizer.exe または dr-ip- customizer コマンドラインに -- verbose オプションを含めて、追加の診断メ ッセージをログに記録できます。	いいえ

次の例のように、--vcid 値が指定されていない場合はいつでも、ツールで UUID を Lookup Service に出力で  
きます。

■ Windows の場合：

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\config\vmware-dr.xml" -i --cmd generate -o "c:\tmp\output.csv" --uri
https://service.company.com:443/lookupservice/sdk --vcid ?
```

■ Linux の場合：

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml" -i --cmd
generate -o "/home/admin/output.csv" --uri
https://service.company.com:443/lookupservice/sdk --vcid ?
```

生成されたエラー メッセージには、vCenter Server インスタンスの UUID の後に Lookup Service で登録され  
た各 vCenter Server の vCenter Server DNS ホスト名が表示されます。

```
ERROR: Failed to locate VC instance. Use one of the following known VC
instances: e07c907e-cd41-4fe7-b38a-f4c0e677a18c vc.company.com
```

## DR IP Customizer CSV ファイルの構造

DR IP Customizer コンマで区切られた値（CSV）ファイルには、ファイル内の各列の意味を定義するヘッダー行および復旧プランの各ブレースホルダ仮想マシンの 1 つまたは複数の行が含まれています。

**注：** Site Recovery Manager では、DR IP Customizer ツールを使用して、サブネットレベル IP マッピングルールを定義して、仮想マシンの IP アドレス設定をカスタマイズすることができます。サブネットレベル IP マッピングルールを DR IP Customizer と組み合わせて使用できます。サブネットレベル IP マッピングルールと DR IP Customizer を一緒に使用する方法については、[複数の仮想マシンの IP プロパティのカスタマイズ](#)を参照してください。

保護サイトのみを設定、または復旧サイトのみを設定を行うことも、両サイトの設定を行うこともできます。異なるネットワークアダプタのセットをまったく異なる方法で使用するよう、それぞれのサイトを設定できます。

CSV ファイルの一部のフィールドは、それぞれの行で入力する必要があります。カスタマイズ設定が必要ない場合は、その他のフィールドは空白のままにしておくことができます。

**表 8-3. DR IP Customizer CSV ファイルの列**

列	説明	カスタマイズのルール
仮想マシン ID	1 つの仮想マシンに対して複数の行からアプリケーションの情報を収集するために DR IP Customizer が使用する固有の識別子。これは、vCenter Server が使用する仮想マシン ID がある場合はその ID と同じになります。ない場合は BIOS ID と同じになります。	カスタマイズ不可。空白不可。
仮想マシン名	人が読める仮想マシンの名前であり、vCenter Server インベントリに表示されます。	カスタマイズ不可。空白不可。
vCenter Server	保護サイトまたは復旧サイトいずれかの vCenter Server インスタンスのアドレス。vCenter Server 列の各サイトの仮想マシンの IP 設定を設定することができます。	カスタマイズ不可。空白不可。 この列には両方の vCenter Server インスタンスを含めることができます。各 vCenter Server インスタンスには個別の行が必要です。あるサイトで使用する IP 設定のセットを設定し、別のサイトで使用する別の IP 設定のセットを設定できます。また、再保護操作のために、両方のサイトで使用する IP 設定を指定することができます。

表 8-3. DR IP Customizer CSV ファイルの列（続き）

列	説明	カスタマイズのルール
アダプタ ID	カスタマイズするアダプタの ID。アダプタ ID 0 は、仮想マシンのすべてのアダプタのグローバル設定を設定します。アダプタ ID 1、2、3 などの設定値は、仮想マシン上の特定の NIC の設定を行います。	<p>カスタマイズ可能。空白不可。</p> <p>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 が使用する他のすべてのアダプタに継承されます。</p> <p>CSV ファイルの複数の行に複数の DNS サーバを含めることができます。たとえば、グローバル DNS ホストが 2 つ必要な場合は、アダプタ ID 0 の 2 つの行を含めます。</p> <ul style="list-style-type: none"> <li>■ 1 つの行には、すべての仮想マシンの情報と 1 つの DNS ホストが含まれます。</li> <li>■ もう 1 つの行には、2 番目の DNS ホストのみが含まれます。</li> </ul> <p>別の DNS サーバを特定のアダプタに追加するには、DNS サーバを適切なアダプタの行に追加します。たとえば、DNS サーバを アダプタ ID 1 に追加します。</p>
DNS ドメイン	このアダプタの DNS ドメイン。	<p>カスタマイズ可能。空白可。</p> <p>値を入力する場合は、<b>example.company.com</b> の形式とする必要があります。</p>
Net BIOS	このアダプタ上の NetBIOS を有効にするかどうかを選択します。	<p>カスタマイズ可能。空白可。</p> <p>空白以外の場合は、この列は <code>disableNetBIOS</code>、<code>enableNetBIOS</code>、<code>enableNetBIOSViaDhcp</code> のいずれかの文字列が含まれている必要があります。</p>
プライマリ WINS	DR IP Customizer は WINS 設定が Windows 仮想マシンにのみ適用されるのを検証しますが、NetBIOS 設定を検証しません。	カスタマイズ可能。空白可。
セカンダリ WINS	DR IP Customizer は WINS 設定が Windows 仮想マシンにのみ適用されるのを検証しますが、NetBIOS 設定を検証しません。	カスタマイズ可能。空白可。
IP アドレス	この仮想マシンの IPv4 アドレス。	<p>カスタマイズ可能。空白不可。</p> <p>仮想マシンには複数の仮想ネットワーク アダプタを設定することができます。1 つの 静的 IPv4 アドレスで各仮想ネットワーク アダプタを構成できます。特定の静的アドレスにフィールドが設定されていない場合、DHCP に設定する必要があります。</p>
サブネット マスク	仮想マシンのサブネット マスク。	カスタマイズ可能。空白可。
ゲートウェイ	IPv4 ゲートウェイまたは、この仮想マシンのゲートウェイ。	カスタマイズ可能。空白可。

表 8-3. DR IP Customizer CSV ファイルの列（続き）

列	説明	カスタマイズのルール
IPv6 アドレス	この仮想マシンの IPv6 アドレス。	<p>カスタマイズ可能。IPv6 を使用しない場合は、空白可。</p> <p>仮想マシンには、複数の仮想ネットワーク アダプタを持つことができます。1 つの 静的 IPv6 アドレスで各仮想ネットワーク アダプタを構成できます。特定の静的アドレスにフィールドが設定されていない場合、DHCP に設定する必要があります。</p> <p>Windows Server 2003 で Site Recovery Manager Server を実行し、仮想マシンの IPv6 アドレスをカスタマイズする場合、Site Recovery Manager Server インスタンスで IPv6 を有効にする必要があります。Site Recovery Manager はカスタマイズ中に IP アドレスを検証するので、IPv6 アドレスをカスタマイズしている場合は、Site Recovery Manager Server で IPv6 アドレスを有効にする必要があります。Windows Server のそれより新しいバージョンでは、デフォルトで IPv6 が有効になっています。</p>
IPv6 サブネット プリフィックス長	使用する IPv6 サブネット プリフィックス長。	カスタマイズ可能。空白可。
IPv6 ゲートウェイ	IPv6 ゲートウェイまたは、このアダプタのゲートウェイ。	カスタマイズ可能。空白可。
DNS サーバ	DNS サーバ（複数可）のアドレス。	<p>カスタマイズ可能。空白可。</p> <p>アダプタ ID 0 行にこの設定を入力する場合は、グローバル設定として扱われます。Windows 仮想マシンでは、アダプタ ID 0 以外のアダプタ ID 行でこれを設定している場合、各アダプタにこの設定が適用されます。Linux 仮想マシンでは、すべてのアダプタでこの設定がグローバル設定となります。</p> <p>この列には、各 NIC の 1 つまたは複数の IPv4 または IPv6 DNS サーバを含めることができます。</p>
DNS サフィックス	DNS サーバのサフィックス（複数可）。	<p>カスタマイズ可能。空白可。</p> <p>これらの設定は、Windows および Linux 仮想マシンの両方のすべてのアダプタのグローバル設定です。</p>

## DR IP Customizer CSV ファイルの変更

DR IP Customizer のコンマで区切られた値 (CSV) ファイルを変更し、カスタマイズされたネットワーク設定を復旧サイト上での起動時に仮想マシンに適用します。

**注：** Site Recovery Manager では、DR IP Customizer ツールを使用して、サブネットレベル IP マッピングルールを定義して、仮想マシンの IP アドレス設定をカスタマイズすることができます。サブネットレベル IP マッピングルールを DR IP Customizer と組み合わせて使用できます。サブネットレベル IP マッピングルールと DR IP Customizer を一緒に使用する方法については、[複数の仮想マシンの IP プロパティのカスタマイズ](#)を参照してください。

CSV ファイルで仮想マシンのネットワーク構成を表す際には、仮想マシン構成に階層情報を含むことが課題です。たとえば、単一の仮想マシンに複数のアダプタがあったり、各アダプタにゲートウェイなどの要素のリストが複数存在したりする場合があります。CSV 形式は、階層表記のシステムを提供しません。結果として、DR IP Customizer が生成する CSV ファイルの各行が特定の仮想マシンの一部またはすべての情報を提供します。

シンプルなネットワーク構成の仮想マシンの場合、すべての情報を 1 行にまとめることができます。より複雑な仮想マシンの場合、複数の行が必要です。複数のネットワーク カードや複数のゲートウェイが構成されている仮想マシンには、行が複数必要です。CSV ファイルの各行には、適用される仮想マシンやアダプタについて記述した識別情報が含まれます。情報は、適切な仮想マシンに適用されるように集計されます。

DR IP Customizer CSV ファイルを変更する場合は、これらのガイドラインにしたがってください。

- 設定が不要な場合は値を省略します。
- 各アダプタに指定できる最小行数を使用します。
- どのフィールドにもコンマを使用しないでください。
- 必要に応じてアダプタ ID 設定を指定します。DR IP Customizer は、アダプタ ID 0 で指定した設定をすべての NIC に適用します。設定を個別の NIC に適用するには、アダプタ ID 1、2、...、 $n$  フィールドの値を指定します。
- 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。追加行を対象の仮想マシンと関連付けるには、VM ID、仮想マシン名、vCenter Server、アダプタ ID 列の値をコピーします。
- それぞれの保護サイトとリカバリ サイトのネットワーク アダプタに IP アドレスを指定するか、複数の DNS サーバ アドレスを指定するには、各アドレスに新しい行を追加します。VM ID、仮想マシン名 およびアダプタ ID の値を各行にコピーします。



## DR IP Customizer CSV ファイルの例

--cmd generate コマンドで dr-ip-customizer.exe または dr-ip-customizer を実行することで、vCenter Server 上で保護された仮想マシンのネットワーク情報を含む CSV ファイルを取得します。CSV ファイルを編集し、保護された仮想マシンの IP アドレス設定をカスタマイズします。

**注：** Site Recovery Manager では、DR IP Customizer ツールを使用して、サブネットレベル IP マッピングルールを定義して、仮想マシンの IP アドレス設定をカスタマイズすることができます。サブネットレベル IP マッピングルールを DR IP Customizer と組み合わせて使用できます。サブネットレベル IP マッピングルールと DR IP Customizer を一緒に使用する方法については、[複数の仮想マシンの IP プロパティのカスタマイズ](#)を参照してください。

### 例：生成された DR IP Customizer CSV ファイル

保護された仮想マシンが 2 台のみの簡易セットアップの場合、生成された CSV ファイルには、仮想マシン ID、仮想マシン名、両サイト上の vCenter Server インスタンスの名前、および 1 つのアダプタのみが含まれることになります。

```
VM ID,VM Name,vCenter Server,Adapter ID,DNS Domain,Net BIOS,
Primary WINS,Secondary WINS,IP Address,Subnet Mask,Gateway(s),
IPv6 Address,IPv6 Subnet Prefix length,IPv6 Gateway(s),
DNS Server(s),DNS Suffix(es)
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-B,0,,,,,,,,,
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-A,0,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,vm-1-linux,vcenter-server-site-A,0,,,,,,,,,
```

ここで生成された CSV ファイルには、vm-3-win と vm-1-linux という 2 台の仮想マシンが示されています。仮想マシンは、保護サイトおよびリカバリ サイト、vcenter-server-site-B、および vcenter-server-site-A にあります。DR IP Customizer は、アダプタ ID 0 で各仮想マシンおよび各サイトのエントリを生成します。各仮想マシン上の NIC の数を把握したら、行を追加してそれぞれの NIC をカスタマイズすることができます。

### 例：固定 IPv4 アドレスの設定

生成された CSV ファイルを変更し、固定 IPv4 アドレスの 2 つのネットワーク アダプタを、保護サイトおよびリカバリ サイト上の仮想マシンの 1 つ vm-3-win に割り当てることができます。

読みやすさを考慮し、次の表内の CSV ファイルの例では、空の列を省略しています。DNS ドメイン、NetBIOS、IPv6 アドレス、IPv6 サブネット プリフィックス長、および IPv6 ゲートウェイ（複数可）の列はすべて省略されています。

表 8-4. 変更された CSV ファイル内での固定 IPv4 アドレスの設定

仮想マシン ID	仮想マシン名	vCenter Server	アダプタ ID	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 サフィックス
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	1.1.1.1	
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com

表 8-4. 変更された CSV ファイル内での固定 IPv4 アドレスの設定（続き）

仮想マシン ID	仮想マシン名	vCenter Server	アダプタ ID	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 サフィックス
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

この CSV ファイル内の情報では、保護サイトとリカバリ サイトの vm-3-win に異なる固定 IPv4 設定が適用されています。

■ vcenter-server-site-B サイト上：

- この仮想マシンのすべての NIC に DNS サフィックス example.com および eng.example.com を設定します。
- プライマリおよびセカンダリ WINS サーバ 2.2.3.4 および 2.2.3.5、固定 IPv4 アドレス 192.168.1.21、DNS サーバ 1.1.1.1 で、NIC、アダプタ ID 1 を追加します。
- プライマリおよびセカンダリ WINS サーバ 2.2.3.4 および 2.2.3.5、固定 IPv4 アドレス 192.168.1.22、DNS サーバ 1.1.1.2 で、NIC、アダプタ ID 2 を追加します。

■ vcenter-server-site-A サイト上：

- この仮想マシンのすべての NIC に DNS サフィックス example.com および eng.example.com を設定します。
- この仮想マシンのすべての NIC に DNS サーバ 1.1.0.1 および 1.1.0.2 を設定します。
- 固定 IPv4 アドレス 192.168.0.21 で、NIC、アダプタ ID 1 を追加します。
- プライマリおよびセカンダリ WINS サーバ 1.2.3.4 および 1.2.3.5、固定 IPv4 アドレス 192.168.0.22 で、NIC、アダプタ ID 2 を追加します。

#### 例：固定および DHCP IPv4 アドレスの設定

生成された CSV ファイルを変更し、固定 IPv4 アドレスと DHCP IPv4 アドレスを組み合わせる複数の NIC を仮想マシンの 1 つ vm-3-win に割り当てることができます。設定は、保護サイトとリカバリ サイトで異なっても構いません。

読みやすさを考慮し、次の表内の CSV ファイルの例では、空の列を省略しています。DNS ドメイン、NetBIOS、IPv6 アドレス、IPv6 サブネット プリフィックス長、および IPv6 ゲートウェイ（複数可）の列はすべて省略されています。

表 8-5. 変更された CSV ファイル内での固定および DHCP IPv4 アドレスの設定

仮想マシン ID	仮想マシン名	vCenter Server	アダプタ ID	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 サフィックス
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com

表 8-5. 変更された CSV ファイル内での固定および DHCP IPv4 アドレスの設定（続き）

仮想マシン ID	仮想マシン名	vCenter Server	アダプタ ID	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 サフィックス
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			dhcp				
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

この CSV ファイル内の情報では、保護サイトとリカバリ サイトの vm-3-win に異なる固定および動的 IPv4 設定が適用されています。

■ vcenter-server-site-B サイト上：

- この仮想マシンのすべての NIC に DNS サフィックス example.com および eng.example.com を設定します。
- DHCP を使用して IP アドレスを取得する プライマリおよびセカンダリ WINS サーバ 2.2.3.4 および 2.2.3.5 で NIC、アダプタ ID 1 を追加し、固定 DNS サーバ 1.1.1.1 を設定します。
- プライマリおよびセカンダリ WINS サーバ 2.2.3.4 および 2.2.3.5、固定 IPv4 アドレス 192.168.1.22、DNS サーバ 1.1.1.2 で、NIC、アダプタ ID 2 を追加します。

■ vcenter-server-site-A サイト上：

- この仮想マシンのすべての NIC に DNS サフィックス example.com および eng.example.com を設定します。
- この仮想マシンのすべての NIC に DNS サーバ 1.1.0.1 および 1.1.0.2 を設定します。
- DHCP を使用して IPv4 アドレスおよびグローバルに割り当てられた DNS サーバ情報を取得する NIC、アダプタ ID 1 を追加します。
- プライマリおよびセカンダリ WINS サーバ 1.2.3.4 および 1.2.3.5、固定 IPv4 アドレス 192.168.0.22 で、NIC、アダプタ ID 2 を追加します。

#### 例：固定および DHCP IPv4 および IPv6 アドレスの設定

生成された CSV ファイルを変更して、複数の NIC を仮想マシンの 1 つ vm-3-win に割り当てることができます。NIC は、固定および DHCP IPv4 および IPv6 アドレスを組み合わせ使用できます。設定は、保護サイトとリカバリ サイトの両方で異なっても構いません。

読みやすさを考慮し、次の表内の CSV ファイルの例では、空の列を省略しています。DNS ドメインおよび NetBIOS の列は省略されています。

表 8-6. 変更された CSV ファイル内での固定および DHCP IPv4 および IPv6 アドレスの設定

仮想 マシン ID	仮想 マシン 名	vCenter Server	アダ プタ ID	プライ マリ WIN S	セカ ンダ リ WIN S	IP アド レス	サブネ ットマ スク	ゲート ウェイ	IPv6 アドレ ス	IPv6 サブネ ットブ リフィ ックス 長	IPv6 ゲート ウェイ	DNS サーバ	DNS サフィ ックス
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e	vm-3 -win	vcen ter- serv er- site- B	0										exam ple.com
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e	vm-3 -win	vcen ter- serv er- site- B	0										eng.e xampl e.com
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e		vcen ter- serv er- site- B	1	2.2.3 .4	2.2.3 .5	192.16 8.1.21	255.2 55.25 5.0	192.16 8.1.1	dhcp			1.1.1.1	
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e		vcen ter- serv er- site- B	2	2.2.3 .4	2.2.3 .5	dhcp			::ffff:19 2.168.1 .22	32	::ffff:19 2.168.1 .1	1.1.1.2	
prot ecte d- vm-1 0301	vm-3 -win	vcen ter- serv er- site- A	0										exam ple.com

表 8-6. 変更された CSV ファイル内での固定および DHCP IPv4 および IPv6 アドレスの設定 (続き)

仮想 マシン ID	仮想 マシン名	vCenter Server	アダ プタ ID	プライ マリ WIN S	セカ ンダ リ WIN S	IP アド レス	サブネ ットマ スク	ゲート ウェイ	IPv6 アドレ ス	IPv6 サブネ ットブ リフィ ックス 長	IPv6 ゲート ウェイ	DNS サーバ	DNS サフィ ックス
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e	vm-3 -win	vcen ter- serv er- site- A	0										eng.e xampl e.com
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e		vcen ter- serv er- site- A	1			dhcp			::ffff:19 2.168. 0.22	32	::ffff:19 2.168. 0.1	::ffff:19 2.168. 0.250	
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e		vcen ter- serv er- site- A	1									::ffff:19 2.168. 0.251	
103b 9e8b -1f90 -faca -802 8-13 820b 8f23 6e		vcen ter- serv er- site- A	2	1.2.3. 4	1.2.3. 5	192.16 8.0.22	255.2 55.25 5.0	192.16 8.0.1				1.1.1.1	

この CSV ファイル内の情報では、保護サイトとリカバリ サイトの vm-3-win に異なる IP アドレス設定が適用されています。

■ vcenter-server-site-B サイト上 :

- この仮想マシンのすべての NIC に DNS サフィックス example.com および eng.example.com を設定します。

- 固定 IPv4 アドレス 192.168.1.21 を設定し、DHCP を使用して IPv6 アドレスを取得し、DNS サーバ 1.1.1.1 を使用するプライマリおよびセカンダリ WINS サーバ 2.2.3.4 および 2.2.3.5 で NIC、アダプタ ID 1 を追加します。
- DHCP を使用して IPv4 アドレスを取得し、固定 IPv6 アドレス ::ffff:192.168.1.22 を設定し、DNS サーバ 1.1.1.2 を使用するプライマリおよびセカンダリ WINS サーバ 2.2.3.4 および 2.2.3.5 で NIC、アダプタ ID 2 を追加します。
- vcenter-server-site-A サイト上 :
  - この仮想マシンのすべての NIC に DNS サフィックス example.com および eng.example.com を設定します。
  - DHCP を使用して IPv4 アドレスを取得し、固定 IPv6 アドレス ::ffff:192.168.1.22 を設定する NIC、アダプタ ID 1 を追加します。アダプタ ID 1 は、固定 IPv6 DNS サーバ ::ffff:192.168.0.250 および ::ffff:192.168.0.251 を使用します。
  - プライマリおよびセカンダリ WINS サーバ 1.2.3.4 および 1.2.3.5、固定 IPv4 アドレス 192.168.0.22、DNS サーバ 1.1.1.1 を使用して、NIC、アダプタ ID 2 を追加します。IPv6 列を空白のままにすることで、アダプタ ID 2 は IPv6 アドレスに DHCP を使用します。

## DR IP Customizer の実行による複数の仮想マシンの IP プロパティのカスタマイズ

DR IP Customizer ツールを使用して、Site Recovery Manager が保護する複数の仮想マシンの IP プロパティをカスタマイズできます。

**注：** Site Recovery Manager では、DR IP Customizer ツールを使用して、サブネットレベル IP マッピングルールを定義して、仮想マシンの IP アドレス設定をカスタマイズすることができます。サブネットレベル IP マッピングルールを DR IP Customizer と組み合わせて使用できます。サブネットレベル IP マッピングルールと DR IP Customizer を一緒に使用する方法については、[複数の仮想マシンの IP プロパティのカスタマイズ](#)を参照してください。

### 前提条件

- 環境内の vCenter Server インスタンスにアクセスできるコンピュータ上で DR IP Customizer ツールを使用します。
- Windows 版 Site Recovery Manager を使用している場合、DR IP Customizer ツールを実行するのに使用しているユーザー アカウントには、少なくとも Site Recovery Manager リカバリ プラン管理者ロールが必要です。
- Site Recovery Manager Virtual Appliance を使用している場合は、管理者ユーザーで SSH に接続する必要があります。

### 手順

- 1 Site Recovery Manager Server ホストにログインして、コマンド シェルを開きます。
- 2 作業ディレクトリを次のディレクトリに変更します。
  - Windows の場合 : C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin



- Linux の場合 : /opt/vmware/srm/bin/

### 3 dr-ip-customizer コマンドを実行し、保護された仮想マシンの情報を含むコンマで区切られた値 (CSV) ファイルを生成します。

- 単一の vCenter Server インスタンスが配置された Platform Services Controller を使用している場合  
Windows の場合は、次のコマンドを実行します。

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\config\vmware-dr.xml"
--cmd generate --out "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

Linux の場合は、次のコマンドを実行します。

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd generate --out "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

この例では、dr-ip-customizer で Site Recovery Manager Server の vmware-dr.xml ファイルを指定し、https://Platform\_Services\_Controller\_address で Platform Services Controller に関連付けられた vCenter Server インスタンスに CSV ファイルを生成しています。

- 複数の vCenter Server インスタンスがある Platform Services Controller の場合には、--vcid パラメータに vCenter Server ID を指定する必要があります。--vcid を指定しない場合、または不正な ID を提供した場合には、ツールにはすべての使用可能な vCenter Server インスタンスがリストされます。

Windows の場合は、次のコマンドを実行します。

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\config\vmware-dr.xml"
--cmd generate --out "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

Linux の場合は、次のコマンドを実行します。

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd generate --out "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

この例では、dr-ip-customizer で Site Recovery Manager Server の vmware-dr.xml ファイルを指定し、ID が vCenter\_Server\_ID の vCenter Server インスタンスに CSV ファイルを生成しています。

---

**注：** vCenter Server ID は vCenter Server の名前とは同じではありません。

---

- 4 (必須) vCenter Server サムプリントを確認し、**y** と入力してこの vCenter Server インスタンスが信頼できるものであると確定します。

--ignore-thumbprint オプションを指定している場合は、サムプリントを確認するプロンプトは表示されません。

- 5 vCenter Server インスタンスのログイン認証情報を入力します。

再度、vCenter Server インスタンスが信頼できるかどうか確認するよう求めるプロンプトが表示される場合があります。

- 6 生成された CSV ファイルを編集して、復旧プランの仮想マシンの IP プロパティをカスタマイズします。

スプレッドシート アプリケーションを使用して CSV ファイルを編集することができます。変更した CSV ファイルを新しい名前で保存します。

- 7 dr-ip-customizer を実行して、変更した CSV ファイルからカスタマイズした IP プロパティを適用します。

DR IP Customizer ツールを保護サイトカリカバリ サイトのいずれかで実行できます。保護された仮想マシンの仮想マシン ID は、サイトごとに異なるため、DR IP Customizer ツールを実行して CSV ファイルを生成するときにはどのサイトを使用したとしても、設定の適用時に再度 DR IP Customizer を実行するときには、生成時と同じサイトを使用する必要があります。

- 単一の vCenter Server インスタンスが配置された Platform Services Controller を使用している場合 Windows の場合は、次のコマンドを実行します。

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml"
--cmd apply --csv "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

Linux の場合は、次のコマンドを実行します。

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd apply --csv "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

この例では、dr-ip-customizer で Site Recovery Manager Server の vmware-dr.xml ファイルを指定し、https://Platform\_Services\_Controller\_address で Platform Services Controller に関連付けられた vCenter Server に CSV ファイルでカスタマイズを適用しています。

- 複数の vCenter Server インスタンスがある Platform Services Controller の場合には、--vcid パラメータに vCenter Server ID を指定する必要があります。

Windows の場合は、次のコマンドを実行します。

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml"
--cmd apply --csv "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

Linux の場合は、次のコマンドを実行します。

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd apply --csv "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

この例では、dr-ip-customizer で Site Recovery Manager Server の vmware-dr.xml ファイルを指定し、ID が vCenter\_Server\_ID の vCenter Server インスタンスに CSV ファイルでカスタマイズを適用しています。

## 結果

指定したカスタマイズは、復旧時に CSV ファイルに指定してあるすべての仮想マシンに適用されます復旧プランのプロパティを編集するときに、それらのマシンの IP 設定を個別に構成する必要はありません。

## IP カスタマイズ ルールの定義による複数仮想マシンの IP プロパティのカスタマイズ

保護サイトやリカバリ サイトで選択した構成済み仮想ネットワーク マッピングに、単一のサブネットレベルの IP マッピング ルールを指定できます。

サブネットレベルのマッピングを設定すると、アダプタレベルの IP マッピングを正確に定義する必要がなくなります。あるいは、Site Recovery Manager が関連アダプタに適用する IP カスタマイズ ルールを指定します。IP カスタマイズ ルールは、テスト ワークフローやリカバリ ワークフローに使用されます。異なるネットワーク マッピング間で IP カスタマイズ ルールを再使用することはできません。

### 重要：

- IP サブネット マッピング ルールは IPv4 のみをサポートします。
- ルールに基づいた IPv6 のカスタマイズは、Site Recovery Manager ではサポートされません。
- IP サブネット マッピング ルールを IPv6 を有効にした Windows 仮想マシンに適用する場合、リカバリ後の IPv6 設定には、DHCP でも静的アドレスでも、影響はありません。Linux 仮想マシンの場合、IPv6 設定は DHCP にリセットされます。
- Site Recovery Manager は、手動の IP カスタマイズを使用するように構成した仮想マシンの IP マッピング ルールを評価しません。

保護サイトの IPv4 サブネットからリカバリ サイトの IPv4 サブネット（たとえば、10.17.23.0/24 から 10.18.22.0/24）にフェイルオーバーする仮想マシンに IP カスタマイズ ルールを適用します。IP カスタマイズ ルールは、リカバリ時に Site Recovery Manager がリカバリ済み仮想マシンの NIC に設定された既存の IP 構成を評価し、10.18.22.0/24 サブネットに 10.17.23.0/24 サブネットで見つかった固定 NIC を再構成します。

ルールを満たす場合、Site Recovery Manager は、元の IPv4 アドレスのホスト ビットを維持し、ターゲットのサブネットに割り当ててすることで、以前の固定 IPv4 アドレスから新しい固定 IPv4 アドレスを取得します。たとえば、元の保護サイトのアドレスが 10.17.23.55/24 の場合、新しいアドレスは 10.18.22.55/24 です。

デフォルト ゲートウェイのテキスト ボックスが空の場合、Site Recovery Manager は、元の IPv4 アドレスのホスト ビットを維持し、ターゲットのサブネットに割り当てることで、元のゲートウェイ パラメータから新しいゲートウェイ パラメータを取得します。たとえば、元の保護されたサイト ゲートウェイが 10.17.23.1 の場合、新しいゲートウェイは 10.18.22.1 になります。明示的なゲートウェイ パラメータを指定する場合、Site Recovery Manager では、IPv4 アドレスの構文が正しく、正確に適用されているかチェックが行われます。

Site Recovery Manager は、DNS とその他のパラメータを指定どおりに適用します。DHCP 対応 NIC のネットワーク構成はリカバリ時に変更されないのでカスタマイズの対象にはなりません。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで [構成] - [ネットワーク マッピング] の順にクリックします。
- 4 カスタマイズ ルールを定義するネットワーク マッピングを選択します。
- 5 ルールを定義するには、[IP カスタマイズ ルールの追加] をクリックします。
- 6 保護サイトとリカバリ サイトにマップするサブネット IP 範囲を指定します。
- 7 リカバリ サイト ネットワークのネットワーク設定を指定します。
- 8 [追加] をクリックして、変更内容を保存します。

# 復旧後の仮想マシンの再保護

## 9

リカバリが完了すると、リカバリ サイトはプライマリ サイトになりますが、仮想マシンはまだ保護された状態にはなりません。元の保護サイトがまだ稼働している場合、保護の方向を反転させることで、元の保護サイトを新しいリカバリ サイトとして使用できます。

すべての保護グループとリカバリ プランを再作成して、逆方向の保護を手動で再確立する作業は時間がかかり、エラーが生じる傾向にあります。Site Recovery Manager には再保護機能があり、これによって保護を自動的に反転させることができます。

Site Recovery Manager がリカバリを実行した後、仮想マシンはリカバリ サイトで起動します。再保護を実行することによって、保護サイトがオンラインになったときに、レプリケーションの方向反転を行い、復旧サイト上で復旧された仮想マシンを保護して元の保護サイトに戻します。

再保護では、復旧の前に確立された保護情報を使用して保護の方向反転を行います。再保護プロセスは、リカバリがエラーなしで終了した後でのみ開始できます。復旧がエラーで完了した場合、すべてのエラーを修正して復旧を再実行する必要があります。エラーが発生しなくなるまでこのプロセスを繰り返します。

再保護操作の完了後にテストを実行することによって、保護サイトと復旧サイトの新しい構成が有効であることを確認できます。

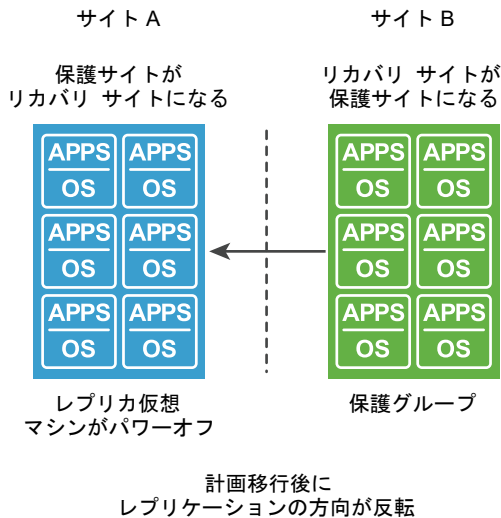
アレイベース レプリケーション保護グループ、vSphere Replication 保護グループ、およびストレージ ポリシー保護グループを含むリカバリ プランで再保護を実行できます。

## 再保護操作の実行

サイト A が保護サイトで サイト B が復旧サイトだとします。サイト A がオフラインになると、リカバリ プランのディザスタ リカバリ ワークフローを実行して、仮想マシンをサイト B でオンラインにします。リカバリの後に、サイト A で保護された仮想マシンはサイト B で保護なしで起動します。

サイト A がオンラインに戻ると、保護を反転する前にサイト A の仮想マシンとデータストアをパワーオフしてアンマウントする必要があるため、計画移行を実行してリカバリを完了します。次に再保護操作を開始し、サイト B でリカバリした仮想マシンを保護します。サイト B が保護サイトになり、サイト A がリカバリ サイトになります。Site Recovery Manager は、サイト B からサイト A にレプリケーションの方向を反転します。

図 9-1. Site Recovery Manager 再保護プロセス



- **Site Recovery Manager がアレイベース レプリケーションを使用して仮想マシンを再保護する方法**  
アレイベース レプリケーションを使用する再保護プロセスでは、Site Recovery Manager は保護の方向を反転させ、新しい保護サイトから新しいリカバリ サイトへのストレージの同期を強制的に実行します。
- **Site Recovery Manager が vSphere Replication を使用して仮想マシンを再保護する方法**  
vSphere Replication を使用する再保護プロセスで、Site Recovery Manager は保護の方向を反転させ、新しい保護サイトから新しいリカバリ サイトへのストレージの同期を強制的に実行します。
- **Site Recovery Manager がストレージ ポリシー保護を使用して仮想マシンを再保護する方法**  
ストレージ ポリシー保護を使用する再保護プロセスでは、Site Recovery Manager はレプリケーション方向を反転させ、かつてのリカバリ サイト上にある関連するストレージ ポリシーに関連付けられた仮想マシンを保護します。Site Recovery Manager は、vSphere エンティティの保護と、新しい保護サイトの監視を再確立します。
- **再保護を実行するための前提条件**  
再保護を実行できるのは、特定の前提条件を満たす場合のみです。
- **仮想マシンの再保護**  
再保護を行うと、Site Recovery Manager の保護グループとリカバリ プランが逆方向に再構成されます。再保護操作の後に、計画移行ワークフローを使用して仮想マシンを元のサイトに戻すことができます。
- **再保護の状態の概要**  
再保護プロセスではいくつかの状態が発生します。これらの状態は、Site Recovery ユーザー インターフェイスのリカバリ プランで確認できます。

## Site Recovery Manager がアレイベース レプリケーションを使用して仮想マシンを再保護する方法

アレイベース レプリケーションを使用する再保護プロセスでは、Site Recovery Manager は保護の方向を反転させ、新しい保護サイトから新しいリカバリ サイトへのストレージの同期を強制的に実行します。

再保護プロセスを開始すると、Site Recovery Manager は基になるストレージ アレイにレプリケーションの方向を反転するように指示します。レプリケーションが反転されると、Site Recovery Manager は、新しいリカバリ サイト（再保護処理前の元の保護サイト）にプレースホルダ仮想マシンを作成します。

Site Recovery Manager は、プレースホルダ仮想マシンを新しい保護サイトに作成する際に、元の保護された仮想マシンの場所を使用してプレースホルダ仮想マシンを作成する場所を決定します。Site Recovery Manager は、元の保護された仮想マシンの ID を使用してプレースホルダを作成します。元の保護された仮想マシンが使用できなくなっている場合、Site Recovery Manager は元のリカバリ サイトから元の保護サイトへのインベントリ マッピングを使用して、プレースホルダ仮想マシンのリソース プールとフォルダを特定します。再保護プロセスを実行する前に、両方のサイトでインベントリ マッピングを構成しておく必要があります。そうしなければ、再保護プロセスが失敗することがあります。

アレイベース レプリケーションを使用して仮想マシンを再保護する場合、Site Recovery Manager は、元の保護された仮想マシンが保持されているデータストアではなく、元の保護サイト用のプレースホルダ データストアにプレースホルダ仮想マシンのファイルを配置します。

新しい保護サイトから新しい復旧サイトへのデータの同期を強制的に実行すると、保護サイトで実行されている保護される仮想マシンの現在のコピーを復旧サイトで得られます。同期を強制的に実行することにより、再保護プロセスが完了した直後にリカバリを実行できます。

## Site Recovery Manager が vSphere Replication を使用して仮想マシンを再保護する方法

vSphere Replication を使用する再保護プロセスで、Site Recovery Manager は保護の方向を反転させ、新しい保護サイトから新しいリカバリ サイトへのストレージの同期を強制的に実行します。

vSphere Replication で再保護を実行する場合、Site Recovery Manager は同期中の最初のコピーとして元の VMDK ファイルを使用します。復旧ステップ中の完全同期は主にチェックサムを実行するもので、ネットワークを介して転送されるデータは少量のみです。

新しい保護サイトから新しい復旧サイトへのデータの同期を強制的に実行すると、保護サイトで実行されている保護される仮想マシンの現在のコピーを復旧サイトで得られます。同期を強制的に実行することにより、再保護プロセスが完了した直後にリカバリを実行できます。

vSphere Replication によって保護された仮想マシンで逆方向レプリケーションを手動で設定するには、Site Recovery ユーザー インターフェイスを使用して、古いリカバリ サイト（つまり新たな保護サイト）でのレプリケーション グループの受け入れを強制的に停止します。元の保護サイトにある仮想マシンだけを削除しても、反転は失敗します。

## Site Recovery Manager がストレージ ポリシー保護を使用して仮想マシンを再保護する方法

ストレージ ポリシー保護を使用する再保護プロセスでは、Site Recovery Manager はレプリケーション方向を反転させ、かつてのリカバリ サイト上にある関連するストレージ ポリシーに関連付けられた仮想マシンを保護します。Site Recovery Manager は、vSphere エンティティの保護と、新しい保護サイトの監視を再確立します。

ストレージ ポリシー保護グループのレプリケーション反転は、基盤となるストレージにのみ影響するので、アレイベース レプリケーション保護グループのレプリケーション反転と同じです。ストレージ ポリシー保護グループを含むリカバリ プランで再保護を実行すると、ストレージ アレイのレプリケーション テクノロジーにより、保護グループに含まれるストレージ ポリシーに関連付けられたすべての整合性グループのレプリケーションが反転します。

ストレージ アレイが、保護グループに含まれる整合性グループのレプリケーション反転に失敗すると、リカバリ プランが [不完全な再保護] 状態になります。この状態になった場合は、ストレージの問題を解決して再保護を再度実行する必要があります。ストレージ ポリシー保護グループに対する再保護の再実行が影響するのは、前回の再保護操作が正常に完了しなかった整合性グループのレプリケーション方向のみです。

ストレージ アレイによってレプリケーション方向が反転されると、Site Recovery Manager が vSphere エンティティの保護と監視を再確立します。再保護中に行われる vSphere エンティティの保護と監視の再確立の条件は、ストレージ ポリシー保護グループの作成中に行われる vSphere エンティティの保護と監視の再確立の条件より緩やかです。

- Site Recovery Manager は、準拠性を確かめるため、新しい保護サイトのストレージ ポリシーを確認します。新しい保護サイトのストレージ ポリシーが非準拠でも、再保護は失敗しませんが、Site Recovery Manager がそのストレージ ポリシーに関連付けられた仮想マシンを保護することはできません。準拠性については、[ストレージ ポリシー保護グループの前提条件](#)と[ストレージ ポリシー保護グループの制限事項](#)を参照してください。
- Site Recovery Manager は、新しい保護サイトで vSphere エンティティの監視を再び開始します。
- Site Recovery Manager は、準拠しているすべての仮想マシンの保護を開始します。ここで言う仮想マシンは、最初にリカバリ プランを実行したときにリカバリされた一連の仮想マシンではない場合があります。自分または他のユーザーが、新しい保護サイトでさらに別の仮想マシンをこのストレージ ポリシーと関連付けている可能性があるためです。Site Recovery Manager が新しい保護サイトにある仮想マシンの保護に失敗しても、再保護は失敗しません。
- ストレージ ポリシー保護グループは、新しい保護サイトから新しいリカバリ サイトにリカバリできます。

## 再保護を実行するための前提条件

再保護を実行できるのは、特定の前提条件を満たす場合のみです。

アレイベース レプリケーション保護グループ、vSphere Replication 保護グループ、およびストレージ ポリシー保護グループを含むリカバリ プランで再保護を実行できます。

再保護を実行する前に、前提条件を満たす必要があります。

- 1 計画移行を実行し、リカバリ プランのすべての手順が正常に完了していることを確認します。リカバリ中にエラーが起こった場合、エラーの原因となった問題を解決して、リカバリを再実行する必要があります。リカバリを再実行する際、それまでに成功していた操作は省略されます。たとえば、正常にリカバリされた仮想マシンは、再びリカバリされることはなく、中断なしで処理が続行されます。
- 2 元の保護サイトが使用できる必要があります。vCenter Server インスタンス、ESXi Server、Site Recovery Manager Server インスタンス、および対応するデータベースがすべてリカバリする必要があります。
- 3 ディザスタ リカバリ操作を実行した場合、両方のサイトが再び実行されたら計画移行を実行する必要があります。計画移行中にエラーが発生した場合、エラーを解決して成功するまで計画移行を再実行する必要があります。



特定の状況では、再保護は実行できません。

- リカバリ プランを完了しようとするとき必ずエラーが発生する。再保護を行うには、リカバリ プランのすべての手順が正常に完了している必要があります。
- 元のサイトをリストアできない。たとえば、物理的な大災害により元のサイトが完全に使用できなくなっている場合など。保護サイトとリカバリ サイトのペアを解除して、ペアリングを再作成するには、両方のサイトが使用可能である必要があります。元の保護サイトをリストアできない場合、保護サイトとリカバリ サイトで Site Recovery Manager を再インストールする必要があります。

## 仮想マシンの再保護

再保護を行うと、Site Recovery Manager の保護グループとリカバリ プランが逆方向に再構成されます。再保護操作の後に、計画移行ワークフローを使用して仮想マシンを元のサイトに戻すことができます。

### 前提条件

再保護を実行するための前提条件を参照してください。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブをクリックし、リカバリ プランを右クリックして、[再保護] をクリックします。
- 4 チェック ボックスを選択して、再保護操作の取り消しができないことを理解していることを確認します。
- 5 (オプション) リカバリ サイトにクリーンアップ処理を行っているときにエラーを無視するには、[強制クリーンアップ] チェック ボックスを選択して、[次へ] をクリックします。  
[強制クリーンアップ] オプションは、初期再保護操作でエラーが発生した後にのみ使用できます。
- 6 再保護情報を確認し、[終了] をクリックします。
- 7 再保護処理の進行状況を監視するには、リカバリ プランを選択し、[リカバリ手順] タブをクリックします。
- 8 再保護操作が完了したら、リカバリ プランを選択し、[履歴] をクリックして、[選択した履歴項目のレポートをエクスポートします] ボタンをクリックします。

リカバリ プランは、再保護操作中にエラーが発生した場合でも「準備完了」状態に戻ることがあります。履歴レポートで再保護操作をチェックし、エラーが発生していないことを確認してください。再保護中にエラーが発生している場合は、エラーの解決を試みてからテスト リカバリを実行し、エラーが解決されていることを確認する必要があります。再保護中に発生したエラーを解決しないまま計画移行またはディザスタ リカバリを試行すると、仮想マシンの一部がリカバリに失敗することがあります。

### 結果

Site Recovery Manager は、リカバリ サイトと保護サイトを反転します。Site Recovery Manager は、保護サイトから仮想マシンのプレースホルダ コピーを新しいリカバリ サイトに作成します。

## 再保護の状態の概要

再保護プロセスではいくつかの状態が発生します。これらの状態は、Site Recovery ユーザー インターフェイスのリカバリ プランで確認できます。

再保護に失敗した場合、または一部しか成功しなかった場合、再保護を完了するための修正アクションを実行できます。

表 9-1. 再保護の状態

状態	説明	修正アクション
Reprotect In Progress	Site Recovery Manager は再保護を実行しています。	なし
Partial Reprotect	複数のリカバリ プランが同じ保護グループを共有し、その一部の保護グループが別のプランで正常に再保護された場合に発生します。	部分的にしか再保護されていないプランで再保護を再度実行します。
Incomplete Reprotect	再保護中に障害があるために、発生します。たとえば、逆方向レプリケーションに失敗した場合や、ブレースホルダ仮想マシンの作成に失敗した場合は、この状態になることがあります。	<ul style="list-style-type: none"> <li>■ 再保護操作で逆方向レプリケーションに失敗した場合は、サイトが接続されていることを確認します。次に、Site Recovery ユーザー インターフェイスで再保護の進行状況を確認し、再保護タスクを再度開始します。それでも再保護に成功しない場合は、[強制クリーンアップ] オプションを使用して再保護タスクを実行します。</li> <li>■ Site Recovery Manager がブレースホルダ仮想マシンの作成に失敗した場合でも、リカバリは可能です。Site Recovery ユーザー インターフェイスで再保護手順を確認して問題を解決し、再保護を再び実行します。</li> </ul>
Reprotect Interrupted	再保護プロセスでいずれかの Site Recovery Manager サーバが不意に停止した場合、この状態になります。	両方の Site Recovery Manager サーバが実行されていることを確認して、再保護タスクを再度開始します。
Ready	再保護が正常に完了すると発生します。	なし。

# フェイルバックの実行による事前リカバリ サイト構成のリストア

# 10

復旧後に、保護サイトと復旧サイトの元の構成をリストアするために、フェイルバックとして知られる一連のオプションの手順を実行できます。

計画移行または災害復旧の後で、前の復旧サイトが保護サイトになります。復旧の直後、新しい保護サイトには復旧する復旧サイトがありません。再保護を実行すると、新しい保護サイトは元の保護サイトによって保護され、元の保護の方向が反転されます。再保護の詳細については、[9 章 復旧後の仮想マシンの再保護](#) を参照してください。

保護サイトとリカバリ サイトの構成をリカバリ前の初期構成にリストアするには、フェイルバックを実行します。

フェイルバックを実行するには、再保護と計画移行の一連の操作を実行します。

- 1 再保護を実行します。復旧サイトが保護サイトとなります。前の保護サイトが復旧サイトとなります。
- 2 保護サイトの仮想マシンをシャットダウンし、リカバリ サイトの仮想マシンを起動するには、計画移行を実行します。仮想マシンの可用性を維持するために、計画移行を開始する前にテストを実行できます。テストでエラーが特定されれば、計画移行の実施前に問題を解決できます。
- 3 2 回目の再保護を実施し、保護サイトおよび復旧サイトを復旧前の元の構成に戻します。

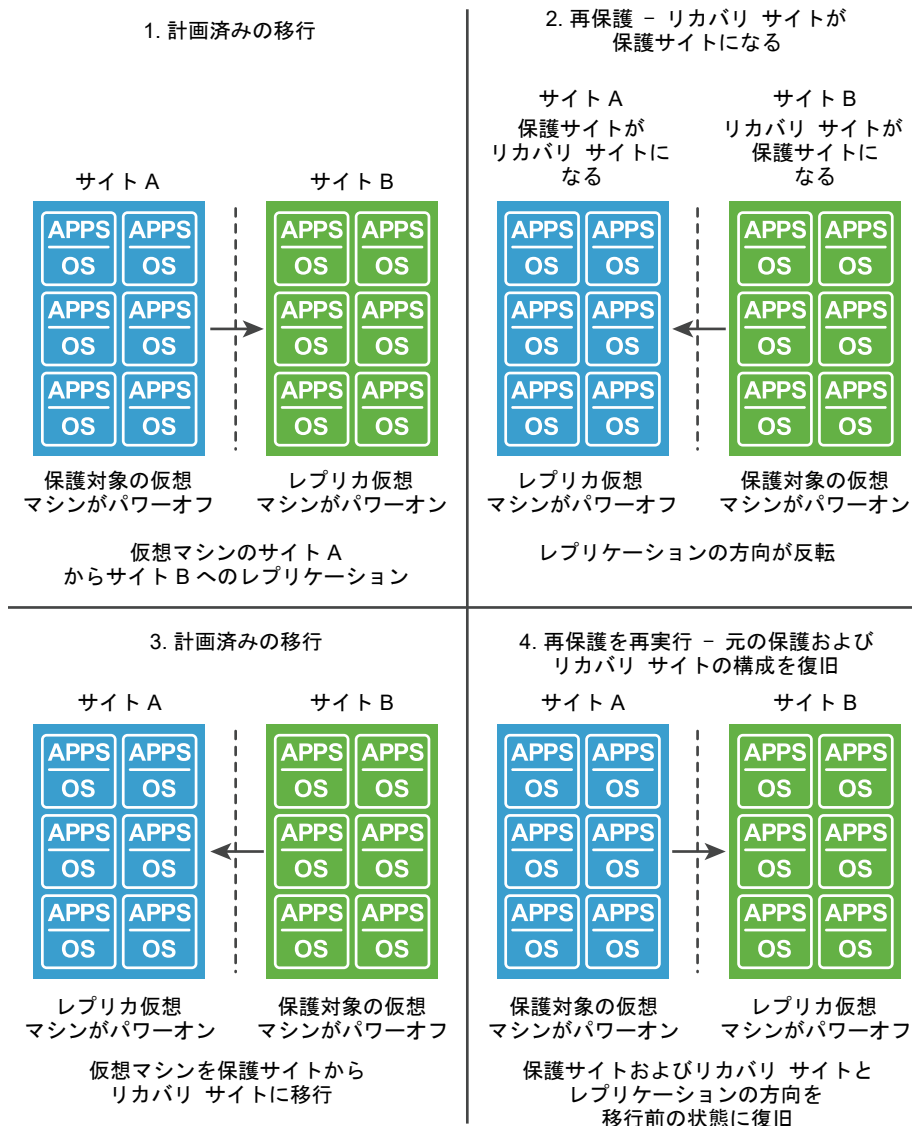
フェイルバックを構成して実行できるのは、インシデント後にオンラインに戻した後元の保護サイトにサービスをリストアする準備ができたときです。

## フェイルバック操作の実行

最初は A が保護サイトで B が復旧サイトだとします。復旧が実行されると、サイト A がサイト B に移行されます。サイト A を保護サイトとしてリストアするには、フェイルバックを実行します。

- 1 仮想マシンをサイト A からサイト B に複製します。
- 2 再保護を実行します。前の復旧サイトである サイト B が保護サイトとなります。Site Recovery Manager は、保護情報を使用してサイト B の保護を確立します。サイト A がリカバリ サイトとなります。
- 3 サイト B で保護された仮想マシンをサイト A にリカバリするには、計画移行を実行します。
- 4 2 度目の再保護を実行します。サイト A が保護サイトとなりサイト B が復旧サイトとなります。

図 10-1. Site Recovery Manager フェイルバック プロセス



この章には、次のトピックが含まれています。

#### ■ フェイルバックの実行

## フェイルバックの実行

Site Recovery Manager がリカバリを実行したら、フェイルバックを実行して、保護サイトと復旧サイトの元の設定をリストアできます。

サイト A からサイト B へのリカバリ後、リカバリされた仮想マシンはサイト B で保護されることなく実行されています。

#### 前提条件

- 計画移行またはディザスタ リカバリの一環としてリカバリを実行していること。

- 元の保護サイト（サイト A）は実行中であること。
- 復旧後は再保護を実行していないこと。
- ディザスタ リカバリを実行している場合は、元の保護サイトにあるホストとデータストアが再び動作しているときに、計画移行を実行する必要があります。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [リカバリ プラン] タブでリカバリ プランを右クリックして、[再保護] をクリックします。
- 4 チェック ボックスを選択して、再保護操作の取り消しができないことを理解していることを確認します。
- 5 [強制クリーンアップ] を有効にするかどうかを決定し、[次へ] をクリックします。  
[強制クリーンアップ] は、再保護を一度実行してエラーが発生した場合にのみ使用可能です。このオプションを有効にすると、エラーを無視して仮想マシンが強制的に削除され、リカバリ プランが Ready 状態に戻ります。
- 6 再保護情報を確認し、[終了] をクリックします。
- 7 リカバリ プランを選択し、[リカバリ手順] をクリックして、再保護操作を完了するまで監視します。
- 8 （必須） 必要に応じて、エラーが発生しない状態で終了するまで再保護を再実行します。  
再保護操作の終了時に Site Recovery Manager によってレプリケーションが反転されるため、元のリカバリサイト（サイト B）が保護サイトになっています。
- 9 リカバリ プランを計画移行として実行するには、リカバリ プランを右クリックして、[リカバリ] をクリックします。
- 10 リカバリ プランを選択し、[リカバリ手順] をクリックして、計画移行を完了するまで監視します。  
計画移行では、新しい保護サイト（サイト B）で仮想マシンをシャットダウンし、新しい復旧サイト（サイト A）で仮想マシンを起動します。必要に応じて、エラーのない状態で終了するまで計画移行を再実行します。  
計画移行が完了すると、仮想マシンは元の保護サイト（サイト A）で実行されますが、仮想マシンは保護されません。元の復旧サイト（サイト B）の仮想マシンはパワー オフされます。
- 11 リカバリ プランを右クリックして [再保護] をクリックし、ウィザードの手順に沿って、2 回目の再保護操作を実行します。

#### 結果

保護サイトおよび復旧サイトが復旧前の元の構成に戻りました。保護サイトはサイト A、復旧サイトはサイト B になっています。

# 他のソフトウェアとの Site Recovery Manager の相互運用性

# 11

Site Recovery Manager Server は、サイトで vCenter Server の拡張機能として動作します。Site Recovery Manager は、他の VMware ソリューションやサードパーティ製ソフトウェアと互換性があります。

Site Recovery Manager を使用して保護しているデプロイメントで、vCenter Update Manager、vCenter Server Heartbeat、VMware Fault Tolerance、vSphere Storage vMotion、vSphere Storage DRS などの他の VMware ソリューションを使用できます。Site Recovery Manager Server が接続されている vCenter Server インスタンスに他の VMware ソリューションを接続するには注意が必要です。Site Recovery Manager と同じ vCenter Server インスタンスに他の VMware ソリューションを接続すると、Site Recovery Manager または vSphere をアップグレードするときに問題が生じる可能性があります。『VMware 製品の相互運用性マトリックス』（英語版）で、使用している Site Recovery Manager のバージョンとこれらのソリューションのバージョンとの互換性と相互運用性を確認します。

この章には、次のトピックが含まれています。

- Site Recovery Manager と vCenter Server
- Site Recovery Manager と VMware vSAN ストレージおよび vSphere Replication の併用
- リカバリ時の Site Recovery Manager と DPM および DRS の連携方法
- 復旧時の Site Recovery Manager と Storage DRS および Storage vMotion の連携方法
- Site Recovery Manager と vSphere High Availability の連携方法
- Site Recovery Manager が拡張されたストレージと相互作用する方法
- Site Recovery Manager と NSX Data Center for vSphere の使用
- Site Recovery Manager と vSphere PowerCLI
- Site Recovery Manager および仮想マシンの暗号化
- Site Recovery Manager と vRealize Orchestrator
- Microsoft Cluster Server およびフォールトトレラント仮想マシンの保護
- Site Recovery Manager を SIOC データストアと併用
- Site Recovery Manager をアドミッションコントロール クラスタと併用
- Site Recovery Manager と RDM ディスク デバイスに接続された仮想マシン
- Site Recovery Manager と Active Directory ドメイン コントローラ

## Site Recovery Manager と vCenter Server

Site Recovery Manager は vCenter Server のサービス（ストレージ管理、認証、権限、ゲストのカスタマイズなど）を利用します。Site Recovery Manager は、vSphere 管理ツールの標準セットを使用してこれらのサービスを管理します。

Site Recovery Manager Server は一部のサービスを vCenter Server に依存しているので、Site Recovery Manager をインストールする前に、サイトに vCenter Server をインストールして構成しておく必要があります。

Site Recovery Manager と vSphere Replication は、vCenter Server Appliance または標準的な vCenter Server と併用できます。片方のサイトで vCenter Server Appliance を実行し、もう片方のサイトで標準的な vCenter Server を実行できます。

### vCenter Server インベントリへの変更が Site Recovery Manager に及ぼす影響

Site Recovery Manager 保護グループは vCenter Server インベントリのサブセットに適用されるので、vCenter Server の管理者とユーザーによる保護インベントリへの変更は、Site Recovery Manager の保護とリカバリの整合性に影響することがあります。Site Recovery Manager は、保護サイトとリカバリ サイトの vCenter Server インベントリ内の仮想マシン、フォルダ、リソース プール、ネットワークなどの特定のオブジェクトの可用性に依存します。リカバリ プランによって参照されるフォルダやネットワークなどのリソースを削除すると、プランが無効になることがあります。vCenter Server インベントリでのオブジェクトの名前の変更や再配置は、テスト中またはリカバリ中にリソースがアクセス不能にならない限り Site Recovery Manager への影響はありません。

アレイベース レプリケーションおよび vSphere Replication の場合、Site Recovery Manager は処理を中断することなく保護サイトで特定の変更を実行できます。

- 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。

Site Recovery Manager では、処理を中断することなくリカバリ サイトで特定の変更を実行できます。

- 別のフォルダやリソース プールへのブレースホルダ仮想マシンの移動。
- 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。

---

**注：** ストレージ ポリシー保護グループでは、変更の処理方法が異なります。[ストレージ ポリシー保護グループのインベントリ マッピング](#) を参照してください。

---

### Site Recovery Manager と vCenter Server データベース

Site Recovery Manager が拡張する vCenter Server インストールの更新を行う場合は、更新中に vCenter Server データベースを再初期化しないでください。Site Recovery Manager では、すべての vCenter Server オブジェクトに関する ID 情報が Site Recovery Manager データベース内に保存されます。vCenter Server データベースを再初期化すると、Site Recovery Manager で保存されている ID データと新しい vCenter Server インスタンスの ID 情報が一致なくなり、オブジェクトが見つからなくなります。



## Site Recovery Manager と VMware vSAN ストレージおよび vSphere Replication の併用

VMware vSAN ストレージと Site Recovery Manager および vSphere Replication を併用できます。

Site Recovery Manager は vSphere Replication と vSAN をサポートしています。vSAN ストレージとアレイベース レプリケーションを併用することはできません。

vSphere Replication と vSAN の互換性のあるバージョンについては、[https://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php) にある『VMware 製品の相互運用性マトリックス』を参照してください。

vSphere Replication と vSAN の併用の詳細については、『vSphere Replication の管理』の [vSphere Replication と VMware vSAN ストレージの併用](#) を参照してください。

## リカバリ時の Site Recovery Manager と DPM および DRS の連携方法

DPM (Distributed Power Management) と DRS (Distributed Resource Scheduler) は必須ではありませんが、Site Recovery Manager は両方のサービスをサポートするため、Site Recovery Manager を使用する場合にこれらのサービスから一定の利点を得ることができます。

DPM は、ESX ホストの電力使用状況を管理する機能です。DRS は ESX ホストへの仮想マシンの割り当てを管理する機能です。

Site Recovery Manager はリカバリ サイトでクラスタの DPM を一時的に無効化し、リカバリやテスト リカバリを開始するときにクラスタのすべてのホストをパワーオンします。これにより、仮想マシンのリカバリ中に十分なホスト容量を確保できます。リカバリやテストが完了すると、Site Recovery Manager は、リカバリ サイトのクラスタの DPM 設定を元の値に戻します。

計画移行および再保護の操作では、Site Recovery Manager は保護サイトで影響のあるクラスタの DPM も無効にしてクラスタのすべてのホストをパワーオンします。これにより、Site Recovery Manager はホスト レベルの操作（たとえば、再保護操作後のデータストアのアンマウントやストレージのクリーンアップ）を完了できます。計画移行や再保護の操作が完了すると、Site Recovery Manager は保護サイトのクラスタの DPM 設定を元の値に戻します。

クラスタ内のホストは実行状態のままなので、DPM は必要に応じてホストをパワーダウンできます。Site Recovery Manager は、使用可能な ESX ホスト全体で仮想マシンをラウンドロビン順に登録して、潜在的な負荷をできるだけ均一に分散します。DRS がクラスタで無効になっている場合でも、Site Recovery Manager は常に DRS 配置を使用して、リカバリ サイトでリカバリした仮想マシンをパワーオンする前にホスト全体にわたってインテリジェントに負荷を分散します。

DRS が有効で完全自動モードの場合は、Site Recovery Manager がリカバリした仮想マシンをパワーオンしている間、DRS は他の仮想マシンを移行してクラスタ全体に負荷をさらに分散します。Site Recovery Manager がリカバリした仮想マシンのパワーオンを終了した後も、DRS はクラスタ全体のすべての仮想マシンの負荷分散を継続します。



## 復旧時の Site Recovery Manager と Storage DRS および Storage vMotion の連携方法

特定のガイドラインに従う場合、Storage DRS または Storage vMotion を使用するように構成されているサイトで仮想マシンを保護するときに Site Recovery Manager を使用できます。

Storage DRS または Storage vMotion の動作は、Site Recovery Manager をアレイ ベースのレプリケーションまたは vSphere Replication のどちらかと併用しているかによって異なります。

Site Recovery Manager が Storage DRS にタグ付けをするデータストアをどのように処理するかについての詳細は、<http://kb.vmware.com/kb/2108196> を参照してください。

### Storage DRS または Storage vMotion を使用するサイトでの Site Recovery Manager とアレイベース レプリケーションの併用

Storage DRS または Storage vMotion を使用するサイトでの仮想マシンの保護にアレイベース レプリケーションを使用する場合は、次のガイドラインに従う必要があります。

- Storage DRS では、自動または手動で移行を実行するために、配置の推奨を計算してデータストアの保護およびレプリケーションのステータスが検討されます。Storage DRS は、データストアがレプリケートされているかどうか、整合性グループか保護グループのどちらに属しているかを確認し、それに応じてデータストアにタグ付けをします。Site Recovery Manager によるデータストアのタグ付け処理の詳細については、「<http://kb.vmware.com/kb/2108196>」を参照してください。
- Site Recovery Manager は、異なる整合性グループからのデータストアを含む Storage DRS クラスタをサポートします。仮想マシンを保護グループに属さないデータストアに移行する場合は、そのデータストアを含めるように保護グループを再構成します。
- Site Recovery Manager は、同じ整合性グループ内のレプリケートされていないデータストア間およびレプリケートされたデータストア間では制限なしに Storage vMotion をサポートします。この場合、Storage DRS は自動モードでクラスタの Storage vMotion を自動実行したり、手動モードでクラスタの Storage vMotion に推奨を発行したりできます。
- レプリケートされたデータストアとレプリケートされていないデータストア間、または異なる整合性グループ内のレプリケートされたデータストア間の Storage vMotion には、特別な考慮事項が適用されます。この場合、Storage DRS は自動で Storage vMotion を初期化したり推奨したりできません。Storage vMotion を手動で初期化すると、考えられる影響について説明する警告が表示されます。
- Storage DRS または Storage vMotion を使用して定期的に仮想マシンを移動しないでください。手動で定期的に仮想マシンを移動する推奨は受け入れないでください。時々仮想マシンを移動することはできますが、仮想マシンを過度に移動すると問題が発生する可能性があります。仮想マシンの移動には、ネットワーク上で仮想マシンをレプリケートするアレイが必要です。これには時間がかかり、帯域幅が消費されます。Storage DRS または Storage vMotion によって仮想マシンが移動された場合、リカバリ中に問題が発生する可能性があります。
- Storage DRS または Storage vMotion によって仮想マシンが同じ保護グループ内の異なる整合性グループに移動された場合、Site Recovery Manager による仮想マシンの新しい場所のリカバリ サイトへの

伝播と、アレイによるリカバリ サイトへの変更のレプリケーションの間に短い間隔が発生します。さらに、アレイによってソースおよびターゲットの整合性グループがリカバリ サイトで整合性のある状態にレプリケートされている間に別の間隔も発生します。アレイによってすべての変更がリカバリ サイトに伝播されている間に、この仮想マシンのディザスタ リカバリは失敗する可能性があります。

- Storage DRS または Storage vMotion によって仮想マシンが異なる保護グループに移動された場合、Site Recovery Manager でこの仮想マシンの保護エラーが発生します。以前の保護グループで仮想マシンの保護を構成解除してから、新しい保護グループで仮想マシンの保護を構成する必要があります。新しい保護グループで保護を構成するまで、この仮想マシンの計画移行またはディザスタ リカバリは失敗します。
- 保護されている仮想マシンにディスクを追加すると、仮想マシン全体を移動した場合と同じ問題が発生します。Site Recovery Manager ではこの操作は禁止されていませんが、仮想マシンにレプリケートされていないディスクが含まれていて、このディスクを保護対象から除外していない場合は、移動後に仮想マシンをパワーオンできなくなります。

## Storage DRS または Storage vMotion を使用するサイトでの Site Recovery Manager と vSphere Replication の併用

Storage DRS または Storage vMotion を使用するサイトでの仮想マシンの保護に vSphere Replication を使用する場合は、ガイドラインに従います。

- vSphere Replication は、保護サイトおよびリカバリ サイトの vSphere Storage DRS と互換性があります。保護サイトでは、Storage DRS を使用して進行中のレプリケーションに影響を与えずに vSphere Replication が保護する仮想マシンのディスク ファイルを移動できます。リカバリサイトでは、Storage DRS が Storage DRS クラスタ上のレプリカ ディスク ファイルを識別し、移行推奨を生成できるように、vCenter Single Sign-On サービスを使用して vSphere Replication アプライアンスを登録する必要があります。Storage DRS を使用して、以降のリカバリに影響を与えずにレプリカ ディスク ファイルを移行できます。詳細については、vSphere Replication のドキュメントの「vCenter Single Sign-On を使用した vSphere Replication の登録」を参照してください。
- vSphere Replication は保護サイトの Storage vMotion と互換性があります。Storage vMotion を使用して進行中のレプリケーションに影響を与えずに、保護サイトの仮想マシンのディスク ファイルを移動できます。
- Site Recovery Manager は変更を検出し、仮想マシンを正常にフェイルオーバーします。
- Site Recovery Manager は、vSphere Replication のレプリカ ディスクを含むデータストアのあるリカバリ サイトの Storage DRS クラスタをサポートします。
- vSphere Replication は Storage vMotion と互換性があり、ディスクまたは仮想マシンのホーム ディレクトリが移動されたときにディスクまたは仮想マシンの状態を保存します。ディスクまたは仮想マシンのレプリケーションは、移動後も正常に続行されます。
- 完全同期は、Storage DRS が移行推奨を生成する原因、あるいは Storage DRS が完全自動モードで実行中の場合は Storage vMotion をトリガする原因となります。これは、DRS ルールが非常にアグレッシブな場合、または仮想マシンの多数が同時に完全同期を実行する場合に発生します。Storage DRS のデフォルトの I/O 待ち時間のしきい値は、15 ミリ秒です。デフォルトでは、Storage DRS はロード バランシングを 8 時間ごと

に実行します。また、Storage DRS は、I/O 負荷に関する十分な統計情報が収集されるまで、Storage vMotion 推奨の生成を待機します。そのため、完全同期が長時間続き、その間にその完全同期で生成される追加 I/O によって待ち時間が I/O 待ち時間のしきい値を超える場合にのみ、完全同期が Storage DRS 推奨に影響します。

- Storage DRS を保護された仮想マシンのデータストアで手動で使用する場合、フェイルオーバー後も古い推奨が存在している可能性があります。元のサイトにフェイルオーバーした仮想マシンを再保護した後にこれらの古い Storage DRS 推奨を適用すると、Site Recovery Manager のブレースホルダ仮想マシンは破損し、以降の元のサイトへのリカバリが、Storage DRS 推奨が適用された仮想マシンで失敗する原因になります。古い更新を適用する場合には、ブレースホルダ仮想マシンを登録解除し、Site Recovery Manager の修復操作を使用して有効なブレースホルダを再作成します。この問題を回避するには、再保護が正常に完了した後に、該当する Storage DRS のストレージ クラスタに Storage DRS 推奨を再生成して、そのサイトからの前のフェイルオーバーによる古い推奨を消去します。

## Site Recovery Manager と vSphere High Availability の連携方法

Site Recovery Manager を使用して vSphere High Availability (HA) が有効化されている仮想マシンを保護できます。

HA は、不具合のあるホスト上の仮想マシンを同じサイト内の新しいホスト上で再起動することで ESXi ホストの不具合から仮想マシンを保護します。Site Recovery Manager は、仮想マシンをリカバリ サイトで再起動することでサイト全体の不具合から仮想マシンを保護します。HA と Site Recovery Manager との主要な違いは、HA は個々の仮想マシンで動作し、仮想マシンを自動的に再起動するという点です。Site Recovery Manager はリカバリ プラン レベルで機能し、ユーザーが手動でリカバリを開始する必要があります。

仮想マシンの HA 設定をリカバリ サイトに転送するには、仮想マシンの保護を構成した後の任意の時点で、リカバリ前にブレースホルダ仮想マシン上で HA 設定を設定しなければなりません。

アレイベースのレプリケーションまたは vSphere Replication を使用して、HA 仮想マシンをレプリケートできます。HA が保護サイトの別のホスト上で保護された仮想マシンを再起動した場合、vSphere Replication は、仮想マシンの再起動後に完全同期を実行します。

Site Recovery Manager で仮想マシンを保護する際に、HA は必須ではありません。同様に、HA にも Site Recovery Manager は必須ではありません。

## Site Recovery Manager が拡張されたストレージと相互作用する方法

拡張されたストレージのサポートは、アレイベース レプリケーションで利用できます。

Site Recovery Manager は、Cross vCenter Server vMotion を使用して計画移行を実行することで、保護されているサイトとリカバリ サイトとの間におけるアクティブ-アクティブな拡張されたストレージをサポートし、サービスのダウンタイムを排除します。ディザスタ リカバリとテスト リカバリでは、既存の LUN ベースのリカバリ機能が引き続き使用されます。

**重要：** 拡張されたストレージは、vCenter Single Sign-On 拡張リンク モード環境でのみサポートされます。サイトが拡張リンク モードでない場合、Cross vCenter Server vMotion を使用した計画移行は失敗します。拡張されたストレージは、計画移行でクロス vCenter Server vMotion を使用する場合に必要です。

## 保護グループ

**重要：** 拡張されたストレージの保護グループを、ストレージ ポリシー保護グループとして作成する必要があります。ストレージのプロファイルは、拡張されたストレージのデバイスを保護およびリカバリするために作成して使用することが必要です。

- 拡張されたデバイスを伴う保護グループには、保護されているサイトからリカバリ サイトに向かう、優先方向が指定されていなければなりません。優先方向は、サイトの環境設定（対応するデバイスについてアレイで管理されている設定）と一致する必要があります。アレイがサイトの環境設定をサポートしている場合、保護されているサイトにはサイトの環境設定がなければなりません。
- 拡張された仮想マシン、拡張されていない仮想マシン、および整合性グループは、同じ保護グループや同じリカバリ プランに含めることができます。
- 拡張された仮想マシンは、拡張されたデータストア上になければならないほか、保護サイトでパワーオン状態になっていることが必要です。
- 同一の拡張されたデバイスのペアを使用して、2 つの保護グループを反対方向に作成することはできません。保護サイトにある保護対象のデバイスに対応する、リカバリ サイトの拡張されたデバイスに仮想マシンを配置することはできますが、保護サイトのストレージをリカバリ サイトの ESXi がマウントしている場合は、データが破損するリスクがあります。これらの仮想マシンは、保護することはできませんが、再保護のプロセスで自動的に保護されます。

## 計画済みの移行

- [リカバリ プランの実行] ウィザードには、Cross vCenter Server vMotion を使用して計画移行を実行するためのオプションがあります。このオプションが選択されている場合は、保護サイト上の拡張されたストレージにある、保護されているすべてのパワーオン状態の仮想マシンに対して Cross vCenter Server vMotion が使用されます。このオプションが選択されていない場合は、レプリケートされた LUN（拡張されたストレージを含む）に対して通常のリカバリ ワークフローが使用されます。
- 何らかの理由で Cross vCenter Server vMotion が失敗すると、リカバリ プランは「仮想マシンの移行」ステップで停止し、続行しません。Site Recovery Manager による Cross vCenter Server vMotion の使用を妨げている問題を解決できない場合は、vSphere vMotion のオプションをオフにしてリカバリ プランを再実行してください。こうすることで、移行では、レプリケートされた LUN に対して通常のリカバリ ワークフローが使用されます。

- 無効化のステップでは、拡張されたデバイスは、vMotion が使用されていなくても保護サイトにマウントされたままです。Site Recovery Manager は、保護サイト上の拡張されたデバイスにある、保護されていないレプリカ仮想マシンを無視し、それらを登録解除することもしません。

## テスト リカバリ

- テスト リカバリは、レプリケートされたデバイス（拡張されたデバイスを含む）を対象とした通常のテスト ワークフローを使用して実行されます。拡張されたデバイスにある各仮想マシンに対しては、vMotion の互換性チェックが実行されます。
- 拡張されたデバイスの読み書き可能なスナップショットを作成することがアレイでサポートされていない場合は、Site Recovery Manager でこれらのデバイスに対してテスト リカバリを実行することはできません。

## クロス vCenter Server vMotion

Cross vCenter Server vMotion は、vSphere Distributed Switch のポート グループから標準のスイッチ ネットワークへの移行ではサポートされません。このインスタンスで、仮想マシンに対して Cross vCenter Server vMotion を実行しようとすると、次のようなエラー メッセージが発生します。

- 保護グループ「<PG-name>」内の仮想マシン「<vm-name>」の Cross vCenter Server vMotion と互換性のあるクラスター「<cluster-name>」内にホストが見つかりません。
- このソース ネットワーク タイプに基づく vMotion に対してこのターゲット ネットワーク タイプがサポートされていないため、現在接続しているネットワーク インターフェイス「<network-adapter-name>」はネットワーク「<network-name>」を使用できません。

Cross vCenter Server vMotion は、以下の状況では機能しません。

- クラスターに対して Distributed Resource Scheduler が無効な場合
- 仮想マシンにスナップショットがある場合
- 仮想マシンがリンク クローンの場合

vSphere でのクロス vCenter Server vMotion の要件については、ESXi および vCenter Server 6.7 のドキュメントで説明されています。

## Site Recovery Manager と NSX Data Center for vSphere の使用

Site Recovery Manager は、インベントリ マッピングを構成しなくても、保護サイトとリカバリ サイト上に存在する NSX ネットワークに接続された仮想マシンを保護できます。

NSX Data Center for vSphere は、vCenter Server の境界をまたぐレイヤー 2 ネットワークの作成を可能にする、ユニバーサル論理スイッチをサポートします。NSX でユニバーサル論理スイッチを使用する場合、同じレイヤー 2 ネットワークに接続された保護サイトとリカバリ サイトの両方に、仮想ポート グループが作成されます。これは、ストレージ ポリシー保護グループとユニバーサル論理スイッチを使用するときに、ネットワーク マッピングを指定する必要がないことを意味します。Site Recovery Manager は NSX Data Center for vSphere と連携して、仮想マシンをリカバリ サイトの適切なネットワークに自動的にマッピングします。

この自動マッピングは、拡張ネットワークのネットワーク マッピングを手動で構成することで、オーバーライドできます。拡張リンク モードと非拡張リンク モードのトポロジがサポートされます。

#### [制限事項]

- NSX ユニバーサル ワイヤの自動マッピングは、ストレージ ポリシー保護グループおよびユニバーサル論理スイッチでのみサポートされます。[]
- ストレージ ポリシー保護グループのネットワーク自動マッピングは、VMware NSX-T™ Data Center ではサポートされません。
- 仮想マシン保護グループの場合は、仮想マシンが同じユニバーサル ワイヤにリカバリされるようにするために、ユニバーサル ワイヤの両端の間のネットワーク マッピングを明示的に構成する必要があります。
- この機能は、フル リカバリの場合にのみサポートされます。テスト フェイルオーバーは手動で行う必要があります。

詳細については、[インベントリ マッピングの構成](#)を参照してください。

## Site Recovery Manager と vSphere PowerCLI

VMware vSphere PowerCLI では、Site Recovery Manager タスクにコマンドラインでアクセスする場合に Windows PowerShell インターフェイスを使用できます。

vSphere PowerCLI から Site Recovery Manager API を利用できます。vSphere PowerCLI を使用して Site Recovery Manager を管理したり、Site Recovery Manager タスクを自動化するスクリプトを作成できます。

vSphere PowerCLI を使用して Site Recovery Manager を管理する方法については、<https://www.vmware.com/support/developer/PowerCLI/> で vSphere PowerCLI のドキュメントを参照してください。

## Site Recovery Manager および仮想マシンの暗号化

Site Recovery Manager を使用すると、アレイベースの保護グループ、ストレージ ポリシー保護グループ、および vSphere Replication 保護グループを使用して、暗号化された仮想マシンを保護およびリカバリできます。

暗号化を行うと、仮想マシンだけでなく、仮想マシンのディスクや他のファイルも保護されます。vCenter Server とキー管理サーバ (KMS) の間に信頼できる接続を設定します。これにより、vCenter Server は必要に応じて KMS からキーを取得できるようになります。保護サイトとリカバリ サイトには同じ名前で登録された KMS クラスタを使用する必要があります。詳細については、『VMware vSAN 管理ガイド』の「KMS クラスタのセットアップ」を参照してください。

暗号化された仮想マシンのゲスト カスタマイズを実行するには、Site Recovery Manager に ESXi 6.5 以降が必要です。

仮想マシンの暗号化の詳細については、『vSphere セキュリティ』ドキュメントの[仮想マシンの暗号化](#)を参照してください。

ストレージ ポリシー保護グループおよび暗号化された仮想マシンの詳細については、[暗号化された仮想マシンの保護](#)を参照してください。

vSphere Replication および暗号化された仮想マシンの詳細については、『vSphere Replication の管理』ドキュメントの[暗号化された仮想マシンのレプリケーション](#)を参照してください。

## Site Recovery Manager と vRealize Orchestrator

vRealize Orchestrator Plug-in for Site Recovery Manager を使用すると、特定の Site Recovery Manager の操作を vRealize Orchestrator ワークフローに含めることで、これらの操作を自動化できます。

vRealize Orchestrator Plug-in for Site Recovery Manager には、Site Recovery Manager の操作を実行するアクションとワークフローが含まれています。vRealize Orchestrator 管理者の場合、Site Recovery Manager プラグインのアクションとワークフローを含むワークフローを作成できます。Site Recovery Manager のアクションとワークフローを vRealize Orchestrator ワークフローに含めることで、Site Recovery Manager の操作を、他の vRealize Orchestrator プラグインが提供する自動操作と組み合わせることができます。

たとえば、vCenter Server 用の vRealize Orchestrator プラグインのアクションとワークフローを使用するワークフローを作成することで、仮想マシンを作成、構成して vCenter Server に登録することができます。Site Recovery Manager プラグインのアクションとワークフローを同じワークフロー内で使用することで、保護グループを作成して、仮想マシンを作成時点から保護できます。また、Site Recovery Manager のアクションとワークフローを使用して、保護された仮想マシンのリカバリ設定の一部を構成することもできます。vCenter Server および Site Recovery Manager のアクションとワークフローを vRealize Orchestrator ワークフロー内で組み合わせると、仮想マシンの作成と保護のプロセスを自動化できます。

複数の vRealize Orchestrator Plug-in for Site Recovery Manager インスタンスを単一の Site Recovery Manager インスタンスに接続する共有リカバリ サイト構成で、vCenter Server を使用できます。また、同じ vCenter Single Sign-On サーバに接続されている複数の vRealize Orchestrator Plug-in for Site Recovery Manager インスタンス上の複数の Site Recovery Manager インスタンスで、vCenter Server を使用することもできます。

vRealize Orchestrator を使用してワークフローを作成する方法については、[vRealize Orchestrator のドキュメント](#)を参照してください。

## Microsoft Cluster Server およびフォールトトレラント仮想マシンの保護

Site Recovery Manager を使用して Microsoft Cluster Server (MSCS) とフォールトトレラント仮想マシンを保護することができますが、いくつかの制約があります。

Site Recovery Manager を使用して MSCS とフォールトトレラント仮想マシンを保護するには、環境の変更が必要な場合があります。

### MSCS およびフォールトトレラント仮想マシンの保護についての一般的な制限

MSCS およびフォールトトレラント仮想マシンの保護には、次の制限があります。

- アレイ ベース レプリケーションは、MSCS 仮想マシンの保護にのみ使用できます。vSphere Replication での MSCS 仮想マシンの保護はサポートされていません。



- MSCS またはフォールト トレランス対応の仮想マシンの保護と再保護には、保護サイトおよびリカバリ サイトの両方に VMware High Availability (HA) と VMware Distributed Resource Scheduler (DRS) が必要です。再保護中に MSCS またはフォールト トレランス仮想マシンをそのプライマリ サイトとセカンダリ サイト間で移動する際は、HA と DRS を有効にして、アフィニティ ルールとアンチアフィニティ ルールを適切に設定する必要があります。詳細については、[MSCS 仮想マシンの保護のための DRS 要件](#)を参照してください。
- アレイベース レプリケーションを使用すると、複数の vCPU フォールト トレランス (SMP-FT) 仮想マシンを保護できます。プライマリおよびセカンダリの両方のフォールト トレランス仮想マシンのディスク ファイルが、レプリケートされた LUN 上に配置されていて、すべての LUN が同じ整合性グループに属している必要があります。
- Site Recovery Manager がフェイルオーバーを試行するのは、プライマリ SMP-FT 仮想マシンのみです。プライマリ SMP-FT 仮想マシンのファイルに問題があっても、セカンダリ SMP-FT 仮想マシンへのフェイルバックを試行しません。
- SMP-FT 仮想マシンが保護されていて、そのストレージがレプリケーションの要件を満たさない場合、Site Recovery Manager は警告を生成しません。
- 1 つの保護グループで保護できるのは、1 台の SMP-FT 仮想マシンのみです。
- Site Recovery Manager は、vSphere Replication でレプリケートされた SMP-FT 仮想マシンをサポートしません。
- Site Recovery Manager は、ストレージ ポリシー保護グループ内の SMP-FT 仮想マシンをサポートしません。SMP-FT はストレージ プロファイルをサポートしません。
- 再保護の実行中に、Site Recovery Manager は元の保護サイト上の SMP-FT 構成を保持しません。
- フェイルオーバーの実行中に、ターゲット仮想マシンは非 FT 仮想マシンとしてパワーオンされます。フェイルオーバー後にターゲット仮想マシンを SMP-FT 仮想マシンとして構成するには、Site Recovery Manager の外部ツールを使用します。

## MSCS 仮想マシンの保護のための ESXi ホスト要件

MSCS またはフォールト トレランス仮想マシンを保護するには、仮想マシンが実行されている ESXi ホスト マシンが特定の基準を満たしている必要があります。

- フォールト トレランス仮想マシンおよびそのシャドウを 2 つの別々の ESXi Server インスタンスで実行する必要があります。
- MSCS 仮想マシンのクラスタを、次の構成で実行することができます。

### 筐体内クラスタ

クラスタ内の MSCS 仮想マシンが単一の ESXi ホスト上で実行されています。1 台の ESXi ホスト上に最大で 5 個の MSCS ノードを使用できます。

### 筐体間クラスタ



最大で 5 つの ESXi ホスト インスタンスに MSCS クラスタを分散することができます。単一の ESXi ホスト インスタンス上にある任意の MSCS クラスタの仮想マシン ノードを 1 つのみ保護できます。複数の MSCS ノード 仮想マシンが同じ MSCS クラスタに参加していない場合、1 つの ESXi ホスト上でそれらの仮想マシンを実行することができます。この構成には、クォーラム ディスクとしてファイバ チャネル SAN 上に共有ストレージが必要です。

## MSCS 仮想マシンの保護のための DRS 要件

MSCS 仮想マシンを含むサイトで DRS を使用するには、DRS ルールを構成して Site Recovery Manager が仮想マシンを保護できるようにする必要があります。ガイドラインを使用することにより、プレースホルダ仮想マシンが筐体間クラスタ MSCS デプロイまたは筐体内クラスタ MSCS デプロイのいずれかにある場合、DRS を実行するサイトで MSCS 仮想マシンを保護できます。

- ゲスト OS で MSCS を構成する前に、保護サイトの仮想マシンに DRS ルールを設定します。仮想マシンをデプロイ、構成、パワーオンした直後に DRS ルールを設定します。
- MSCS ノードの保護グループを作成した直後、プレースホルダ仮想マシンがリカバリ サイトに表示されたらすぐに、DRS ルールをリカバリ サイトの仮想マシンに設定します。
- 保護サイトで設定した DRS ルールはリカバリ後のリカバリ サイトに転送されません。したがって、リカバリサイトのプレースホルダ仮想マシンには DRS ルールを設定する必要があります。
- リカバリ サイトに DRS ルールを設定する前に、テスト リカバリまたは実際のリカバリを実行しないでください。

保護サイトまたはリカバリ サイトのいずれかでガイドラインを守らない場合、vSphere vMotion は MSCS 仮想マシンを Site Recovery Manager がサポートしていない構成に移動することがあります。

- 保護サイトまたはリカバリ サイトのいずれかの筐体内クラスタ デプロイの場合、vSphere vMotion は MSCS 仮想マシンを別の ESXi ホストに移動することがあります。
- 保護サイトまたはリカバリ サイトのいずれかの筐体間クラスタ デプロイの場合、vSphere vMotion は一部またはすべての MSCS 仮想マシンを 1 つの ESXi ホストに移動することがあります。

## Site Recovery Manager を SIOC データストアと併用

Site Recovery Manager はストレージ I/O コントロール (SIOC) を完全にサポートします。

### SIOC を使用するデータストアでの仮想マシンの計画移行

Site Recovery Manager の前のリリースでは、計画移行を実行する前にリカバリ プランに含まれているデータストアでストレージ I/O コントロール (SIOC) を無効にする必要がありました。Site Recovery Manager のこのリリースは SIOC を完全にサポートしているので、計画移行を実行する前に SIOC を無効にする必要はありません。

## SIOC を使用するデータストアでの仮想マシンの災害復旧および再保護

Site Recovery Manager の前のリリースでは、SIOC を有効にしてディザスタ リカバリを実行すると、リカバリは成功しますがエラーが発生しました。リカバリ後に保護サイトで SIOC を手動で無効にし、計画移行のリカバリを再度実行する必要があります。計画移行が正常に実行されるまで、再保護を実行することはできませんでした。Site Recovery Manager のこのリリースは SIOC を完全にサポートしているので、リカバリはエラーなしで成功し、ディザスタ リカバリの後に SIOC を無効にせずに計画移行と再保護を実行できます。

## Site Recovery Manager をアドミッション コントロール クラスタと併用

クラスタでアドミッション コントロールを使用してリカバリ サイトのリソースを予約できます。

ただし、アドミッション コントロールを使用することで、リカバリ プランの実行時に Site Recovery Manager が仮想マシンをパワーオンできなくなり、ディザスタ リカバリに影響を与えることがあります。仮想マシンがパワーオンになることで関連したアドミッション コントロールの制約が違反される場合、アドミッション コントロールは仮想マシンがパワーオンするのを防止する可能性があります。

リカバリ プランにコマンド ステップを追加して、リカバリ中にアドミッション コントロールを無効にする PowerCLI スクリプトを実行できます。コマンド ステップの作成については、[カスタム リカバリ手順の作成](#) を参照してください。

- 1 リカバリ プランに、PowerCLI スクリプトを実行してアドミッション コントロールを無効にするパワーオン前のコマンド ステップを作成します。

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$false
```

- 2 リカバリプランに、仮想マシンのパワーオン後にアドミッション コントロールを再度有効にするパワーオン後のコマンド ステップを作成します。

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$true
```

リカバリ中にアドミッション コントロールを無効にした場合は、テスト リカバリに続いてクリーンアップを実行した後に、手動でアドミッション コントロールを再度有効にする必要があります。アドミッション コントロールを無効にすると、HA (High Availability) がリカバリ サイトで仮想マシンを再起動する機能に影響を与えることがあります。アドミッション コントロールは長時間無効にしないでください。

## Site Recovery Manager と RDM ディスク デバイスに接続された仮想マシン

Raw ディスク マッピング (RDM) ディスク デバイスに接続されている仮想マシンの保護とリカバリは、アレイベース レプリケーションを使用するか vSphere Replication を使用するかに応じて、異なる方法でサポートされます。

**注：** ストレージ ポリシー保護グループでは、Site Recovery Manager は、RDM デバイスに接続された仮想マシンの保護をサポートしません。

- アレイベース レプリケーションは、物理互換モードと仮想互換モードの RDM デバイスをサポートします。Site Recovery Manager をアレイベース レプリケーションとともに使用する場合、RDM を使用する仮想マシンは、物理互換モードまたは仮想互換モードのいずれかで保護してリカバリできます。
- vSphere Replication では、ソース デバイスとターゲット デバイス両方の RDM デバイスを仮想モードでのみサポートします。vSphere Replication を使用する場合、物理互換モードで RDM を使用する仮想マシンを保護してリカバリすることはできません。
- アレイベース レプリケーションと vSphere Replication の両方を使用する場合は、アレイベース レプリケーションを使用して物理互換モードでのみ RDM を使用する仮想マシンを保護してリカバリできます。アレイベース レプリケーションまたは vSphere Replication を使用すると、仮想互換モードで RDM を使用する仮想マシンを保護してリカバリできます。

## Site Recovery Manager と Active Directory ドメイン コントローラ

Site Recovery Manager は、Site Recovery Manager でサポートされている他のアプリケーションと同様に、Active Directory ドメイン コントローラとして機能する仮想マシンの保護をサポートします。

Active Directory のネイティブのレプリケーション テクノロジーとリストア モードの代わりに、ディザスタ シナリオで Site Recovery Manager を使用して Active Directory インフラストラクチャを保護できます。問題が発生した場合は、特定のネットワーク構成とドメイン コントローラの相互依存関係に関連している可能性があります。

# Site Recovery Manager の高度な構成

# 12

Site Recovery Manager のデフォルト構成では、いくつかの簡単なリカバリ シナリオを実行できます。上級ユーザーは、Site Recovery Manager をカスタマイズして、より広範なサイト リカバリ要件をサポートできます。

この章には、次のトピックが含まれています。

- Site Recovery Manager の設定の再構成
- 大規模な Site Recovery Manager 環境を実行するように設定を変更する

## Site Recovery Manager の設定の再構成

[詳細設定] を使用すると、Site Recovery Manager サービスの多くのカスタム設定を表示または変更できます。[詳細設定] では、適切な権限を保有するユーザーが Site Recovery Manager のさまざまな機能の操作に影響するデフォルト値を変更できます。

---

**重要：** アップグレード中、Site Recovery Manager は以前のインストールで構成した詳細設定を保持しません。これは仕様です。デフォルト値の変更またはパフォーマンスの向上により、Site Recovery Manager の旧バージョンで設定した詳細設定が新しいバージョンで必要なくなる、または互換性がなくなることがあります。同様に、同じバージョンの Site Recovery Manager をアンインストールして再インストールする場合、以前のインストールからデータベースを再利用しても、詳細設定は保持されません。

---

## 接続設定の変更

Site Recovery Manager は、他のサービスと通信します。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [接続] をクリックします。

- 4 サイトを選択し、[編集] をクリックして、設定を変更します。

オプション	操作
「サイト ダウン」 イベントを発生する前の ping の失敗回数を変更する。デフォルト値は 5 です。	[connections.hmsPanicDelay] テキスト ボックスに新しい値を入力します。
チェック エラーを宣言するまでに試行するステータス チェック (ping) の回数を変更する。デフォルト値は 2 です。	[connections.hmsPingFailedDelay] テキスト ボックスに新しい値を入力します。
サーバからの更新待機時間のタイムアウト値を変更する。デフォルト値は 900 秒です。	[connections.waitForUpdatesTimeout] テキスト ボックスに新しい値を入力します。

- 5 変更内容を保存するには、[OK] をクリックします。

## Site Recovery Manager 履歴レポート収集の設定の変更

Site Recovery Manager 履歴レポートは、失敗の前後の Site Recovery Manager Server の動作を診断する際に役立ちます。エクスポートする履歴レポートの数は変更できます。

保護サイトとしてサイト A、リカバリ サイトとしてサイト B を使用して、フェイルオーバー、テスト、クリーンアップ、および再保護の各操作を実行する場合、リカバリ サイトのサイト B のサポート バンドルを収集する際にこれらの操作の履歴レポートをエクスポートできます。最新の履歴は、Site Recovery Manager データベースから直接取得されます。

再保護が実行されると、サイト A が新しいリカバリ サイトになり、サイト B が保護サイトになります。フェイルオーバー、テスト、クリーンアップ、および再保護の各操作を実行する場合は、リカバリ サイトのサイト A のサポート バンドルを収集する際に履歴レポートをエクスポートできます。

### 前提条件

- 管理者の認証情報があることを確認します。
- Site Recovery Manager は、有効なデータベース認証情報を使用してアクセスできる Site Recovery Manager データベースに接続されている必要があります。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [履歴のエクスポート] をクリックします。
- 4 サイトを選択し、[編集] をクリックして、設定を変更します。
- 5 必要に応じて [exportHistory.numReports] の値を変更します。  
0 ~ 50 の値を入力できます。デフォルト値は 5 です。
- 6 レポートをエクスポートしない場合は、この値をゼロ (0) にします。
- 7 変更内容を保存するには、[OK] をクリックします。

## ローカル サイトの設定の変更

Site Recovery Manager は Site Recovery Manager Server ホストのリソース消費を監視し、リソースのしきい値に達するとアラームを発生します。Site Recovery Manager がアラームを発生するしきい値およびその方法は変更できます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [ローカル サイト ステータス] をクリックします。
- 4 サイトを選択し、[編集] をクリックして、設定を変更します。

オプション	操作
Site Recovery Manager がローカル サイトの CPU 使用率、ディスク容量、空きメモリをチェックする時間間隔を変更します。デフォルト値は 60 秒です。	[localSiteStatus.checkInterval] テキスト ボックスに新しい値を入力します。
ローカル サイトの CPU 使用率、ディスク容量、空きメモリに関するアラームを Site Recovery Manager が通知してから次に通知するまでの待機間隔を変更します。デフォルト値は 600 秒です。	[localSiteStatus.eventFrequency] テキスト ボックスに新しい値を入力します。
サーバ クロック間の最大許容時差を変更します。デフォルトは 20 秒です。	[localSiteStatus.maxClockSkew] テキスト ボックスに新しい値を入力します。検出されたサーバ クロック時間が Site Recovery Manager Server のクロックと設定秒数を超えてずれている場合、Site Recovery Manager はイベントを発生させます。
Site Recovery Manager が CPU の高使用率のイベントを通知する CPU 使用率の上限を変更します。デフォルト値は 70 です。	[localSiteStatus.maxCpuUsage] テキスト ボックスに新しい値を入力します。
証明書の有効期限切れイベントを通知する前に Site Recovery Manager 証明書の有効期限が切れるまでの日数を変更します。デフォルト値は 30 日です。	[localSiteStatus.minCertRemainingTime] テキスト ボックスに新しい値を入力します。
Site Recovery Manager がディスク容量の不足イベントを通知するディスクの空き容量率を変更します。デフォルト値は 100 Mb です。	[localSiteStatus.minDiskSpace] テキスト ボックスに新しい値を入力します。
Site Recovery Manager がメモリ不足のイベントを通知する空きメモリ量の下限を変更します。デフォルト値は 32 MB です。	[localSiteStatus.minMemory] テキスト ボックスに新しい値を入力します。

- 5 変更内容を保存するには、[OK] をクリックします。

## ログ設定の変更

Site Recovery Manager が記録する Site Recovery Manager Server コンポーネントのログ レベルは変更することができます。

Site Recovery Manager Server はログ ローテーションを実行します。Site Recovery Manager Server を再起動する場合、またはログ ファイルが大きくなった場合、Site Recovery Manager Server は新しいログ ファイルを作成し、後続のログ メッセージをその新しいログ ファイルに書き込みます。Site Recovery Manager Server は、新しいログ ファイルを作成するときに、古いログ ファイルを圧縮してスペースを確保します。

一部の Site Recovery Manager Server コンポーネントの場合、ログ ファイルが急激に大きくなり過ぎるようであれば、ログ レベルを下げるすることができます。またコンポーネントによっては、ログ レベルを上げて問題の診断に役立てることができます。指定可能なログ レベルの一覧は、すべての Site Recovery Manager Server コンポーネントで同じです。

### [なし]

ログをオフにします。

### [静的]

最小限のログ エントリを記録します。

### [パニック]

パニック ログ エントリのみを記録します。パニック メッセージは完全な障害の場合に生成されます。

### [エラー]

パニックおよびエラーのログ エントリを記録します。障害となる問題でも、そうでない問題でも、発生する可能性があります。

### [警告]

パニック、エラー、および警告のログ エントリを記録します。警告メッセージは、不適切であっても、予期される一連の動作の一部となっている動作の場合に生成されます。

### [情報]

パニック、エラー、警告、および情報のログ エントリを記録します。情報メッセージは、通常動作に関する情報です。

### [詳細]

パニック、エラー、警告、情報、および詳細のログ エントリを記録します。詳細メッセージは、情報メッセージよりも詳しい情報です。

### [最詳細]

パニック、エラー、警告、情報、詳細、および最詳細のログ エントリを記録します。最詳細メッセージは、記録可能なすべての情報です。このログ レベルはデバッグで役立ちますが、処理速度に影響しかねないほどのデータが生成されます。

**注：** この問題を解決するために、VMware サポートによって指示された場合にのみ、このログ レベルを設定します。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [ログ マネージャ] をクリックします。
- 4 サイトを選択し、[編集] をクリックして、ログ設定を変更します。

デフォルトでは、ログ レベルの説明で特に指定がない限り、すべてのコンポーネントが最詳細レベルのログを記録します。

オプション	説明
logManager にエントリが存在しないすべてのコンポーネントのログ レベルを設定します。デフォルトは詳細です。	[logManager.Default] ドロップダウン メニューからログ レベルを選択します。
外部 API モジュールのログ レベルの設定。デフォルトは詳細です。	[logManager.ExternalAPI] ドロップダウン メニューからログ レベルを選択します。
vSphere Replication のログ レベルの設定。デフォルトは詳細です。	[logManager.HbrProvider] ドロップダウン メニューからログ レベルを選択します。
IP Customizer ツールのログ レベルの設定。デフォルトは詳細です。	[logManager.IPCustomizer] ドロップダウン メニューからログ レベルを選択します。
インベントリ マッピングのログ レベルの設定。デフォルトは詳細です。	[logManager.InventoryMapper] ドロップダウン メニューからログ レベルを選択します。
ライセンスの問題のログ レベルの設定。デフォルトは詳細です。	[logManager.Licensing] ドロップダウン メニューからログ レベルを選択します。
データ保全問題のログ レベルの設定。デフォルトは詳細です。	[logManager.Persistence] ドロップダウン メニューからログ レベルを選択します。
リカバリ処理のログ レベルの設定。デフォルトは最詳細です。	[logManager.Recovery] ドロップダウン メニューからログ レベルを選択します。デフォルトの場合、リカバリ ログは [最詳細] に設定されます。
リカバリ構成処理のログ レベルの設定。デフォルトは詳細です。	[logManager.RecoveryConfig] ドロップダウン メニューからログ レベルを選択します。
アレイベース レプリケーション処理のログ レベルの設定。デフォルトは詳細です。	[logManager.Replication] ドロップダウン メニューからログ レベルを選択します。
Site Recovery Manager Server と vCenter Server の間の権限問題のログ レベルの設定。デフォルトは詳細です。	[logManager.ServerAuthorization] ドロップダウン メニューからログ レベルを選択します。
セッション管理のログ レベルの設定。デフォルトは詳細です。	[logManager.SessionManager] ドロップダウン メニューからログ レベルを選択します。



オプション	説明
SOAP Web サービス アダプタのログ レベルの設定。デフォルトは情報です。	[logManager.SoapAdapter] ドロップダウン メニューからログ レベルを選択します。SOAP アダプタが生成するトラフィックのレベルが原因で、ログ レベルを [最詳細] に設定すると処理速度に影響することがあります。デフォルトの場合、SOAP アダプタ ログは [情報] に設定されます。
ストレージ問題のログ レベルの設定。デフォルトは詳細です。	[logManager.Storage] ドロップダウン メニューからログ レベルを選択します。
アレイベースのストレージ プロバイダからのメッセージのログ レベルの設定。デフォルトは詳細です。	[logManager.StorageProvider] ドロップダウン メニューからログ レベルを選択します。

## 5 変更内容を保存するには、[OK] をクリックします。

新しいログ レベルは、[OK] をクリックするとすぐに適用されます。Site Recovery Manager サービスを再起動する必要はありません。Site Recovery Manager Server を再起動する場合、ログは選択したレベルに設定されたままになります。

## リカバリ設定の変更

リカバリ プランをテストまたは実行する場合に発生するタイムアウトのデフォルト値を調整できます。タイムアウトが原因でタスクが失敗した場合は、デフォルト値を調整できます。

リカバリ プランのステップの実行中に発生するタイムアウトには、いくつかの種類があります。これらのタイムアウトによって、ステップを完了するための時間として与えられた指定間隔でプランが一時停止します。

仮想マシンの保護を構成する際に Site Recovery Manager は仮想マシンにいくつかの詳細設定を適用します。

- `recovery.autoDeployGuestAlias`
- `recovery.defaultPriority`
- `recovery.powerOnTimeout`
- `recovery.powerOnDelay`
- `recovery.customizationShutdownTimeout`
- `recovery.customizationTimeout`
- `recovery.skipGuestShutdown`
- `recovery.powerOffTimeout`

Site Recovery Manager は、各 Site Recovery Manager サイトで仮想マシンのリカバリ設定のコピーを保存します。リカバリの詳細設定が保護サイトやリカバリ サイトによって異なる場合、Site Recovery Manager は仮想マシンのリカバリ設定を各サイトで異なる値に初期化します。Site Recovery Manager はサイト A からサイト B に仮想マシンをリカバリするときに、サイト B にローカル リカバリ設定を適用します。サイト B からサイト A にリカバリするときに、Site Recovery Manager はサイト A のローカル リカバリ設定を適用します。リカバリプランの [仮想マシン] タブで個々の仮想マシンのリカバリ設定を明示的に編集し、保存しない限り、このように適用されます。影響のある仮想マシンのリカバリ設定を同期し、両方の Site Recovery Manager サイトで同じになるようにします。

## 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [リカバリ] の順にクリックします。
- 4 サイトを選択し、[編集] をクリックして、リカバリ サイトの設定を変更します。

オプション	操作
<p>ゲスト ユーザー マッピングの自動構成を有効または無効にします。このオプションは、VMware Tools の互換性のあるバージョンを使用する仮想マシンでのみ利用可能です。デフォルト値は true です。</p> <p>VMware Tools の互換性のあるバージョンについては、Site Recovery Manager 8.2 の互換性マトリックスを参照してください。</p>	<p>[recovery.autoDeployGuestAlias] の値を選択して、ゲスト ユーザー マッピングの自動構成を有効または無効にします。</p> <p>この値が true の場合、Site Recovery Manager はリカバリ中にすべての仮想マシンのゲスト OS にゲスト ユーザー マッピングを作成し、リカバリが終了するとそれらを削除します。このオプションを使用するには、VMware Tools の互換性のあるバージョンをインストールし、リカバリする仮想マシンで IP カスタマイズまたはゲスト内の呼び出し操作を構成する必要があります。リカバリ プロセスを実行する前に、リカバリ サイトの ESXi ホストと vCenter Single Sign-On サーバ間で時刻を同期する必要があります。</p> <p>この値が false の場合、リカバリ サイトのローカルの Site Recovery Manager ソリューション ユーザーを保護されている仮想マシンのゲスト ユーザー アカウントに手動でマッピングする必要があります。ゲスト OS ユーザーは、コマンドを実行する権限およびゲスト OS のファイルにアクセスする権限を保有している必要があります。IP カスタマイズまたはゲスト内の呼び出し操作を構成する場合は、保護されている仮想マシンのゲスト OS とリカバリ サイトの vCenter Single Sign-On サーバ間で時刻を同期する必要があります。</p> <p>Site Recovery Manager サイトが拡張リンク モードになっている場合は、vSphere Web Client を使用してゲスト ユーザー マッピングを構成できます。</p> <p>ゲスト ユーザー マッピングを構成する方法については、『VMware vSphere ESXi および vCenter Server』ドキュメントの「ゲスト OS でのユーザー マッピングの構成」の章を参照してください。</p> <p>Site Recovery Manager サイトが拡張リンク モードになっていない場合は、vSphere API を使用してゲスト ユーザー マッピングを構成し、必ずエイリアス証明書をマッピングしておく必要があります。ベスト プラクティスは、vCenter Single Sign-On サーバの署名証明書を使用することです。vSphere API については、『VMware vSphere API リファレンス』ドキュメントを参照してください。</p>
<p>IP カスタマイズで仮想マシンのパワーオフ タイムアウトを変更します。デフォルト値は 300 秒です。</p>	<p>[recovery.customizationShutdownTimeout] テキスト ボックスに新しい値を入力します。この値は、IP カスタマイズ ワークフローのみで使用される最小の仮想マシンのパワーオフ タイムアウト（秒）です。仮想マシン リカバリ設定でパワーオフ タイムアウトを指定する場合は、2 つの設定のうち大きい方の値が優先されます。</p>
<p>IP カスタマイズ タイムアウトを変更する。デフォルト値は 600 秒です。</p>	<p>[recovery.customizationTimeout] テキスト ボックスに別の値を入力します。この値は、Site Recovery Manager Server の IP カスタマイズ スクリプトの準備で使用されるタイムアウトです。ほとんどの場合、この値を変更する必要はありません。</p>
<p>仮想マシンのリカバリのデフォルトの優先順位を変更する。デフォルト値は 3 です。</p>	<p>[recovery.defaultPriority] テキスト ボックスに別の値を入力します。</p>
<p>強制リカバリを有効または無効にする。デフォルト値は false です。</p>	<p>[recovery.forceRecovery] チェック ボックスを選択または選択解除します。保護サイトに接続できないことで RTO に深刻な影響を与えている場合、強制リカバリを有効化します。この設定では、リカバリ ブランの実行時に強制リカバリの選択を禁じる制限のみが排除されます。実際に強制リカバリを有効にするには、ブランを実行するときにこの設定を選択します。</p>

オプション	操作
クラスタ内のホストをパワーオンするときのタイムアウトを変更する。デフォルト値は 1200 秒です。	[recovery.hostPowerOnTimeout] テキスト ボックスに別の値を入力します。
ゲストのシャットダウンが完了し仮想マシンがパワーオフするのを待機する場合のデフォルトのタイムアウト値を変更する。デフォルト値は 300 秒です。	<p>[recovery.powerOffTimeout] テキスト ボックスに別の値を入力します。この値は、仮想マシンをシャットダウンするための最終手段としてパワーオフを試みるまでのゲスト OS のタイムアウト値を定義します。</p> <p><b>注：</b> タイムアウトになると、仮想マシンがパワーオフします。タイムアウトになったことによって仮想マシンの OS がシャットダウン タスクを完了しなかった場合には、データの損失が発生することがあります。シャットダウンに長い時間を要する大規模な仮想マシンには、<a href="#">仮想マシンの起動およびシャットダウン オプションの構成</a>で説明するとおり、ゲスト OS によるパワーオフのタイムアウトを仮想マシンに個別に設定します。</p>
仮想マシンをパワーオンしてから依存タスクを開始するまでの遅延を変更する。デフォルト値は 0 です。	[recovery.powerOnDelay] テキスト ボックスに別の値を入力します。新しい値は、復旧サイトでの仮想マシンに対するパワーオン操作に適用されます。
仮想マシンのパワーオン時に VMware Tools を待機するタイムアウトを変更する。デフォルト値は 300 秒です。	[recovery.powerOnTimeout] テキスト ボックスに別の値を入力します。新しいパワーオン値は、復旧サイトでの仮想マシンに対するパワーオン操作に適用されます。保護されている仮想マシンに VMware Tools がインストールされていない場合は、この値を 0 に設定して、これらの仮想マシンをパワーオフするときに VMware Tools を待機しないようにし、SRM でのタイムアウト エラーを回避します。
ゲスト OS のシャットダウンのスキップを有効または無効にする。デフォルト値は false です。	<p>[recovery.skipGuestShutdown] チェック ボックスを選択または選択解除します。</p> <p>skipGuestShutdown=true の場合、Site Recovery Manager は、保護サイトの仮想マシンでゲスト OS のシャットダウンを試みることはしませんが、代わりにそれらを直接パワーオフします。この場合、recovery.powerOffTimeout に設定された値は、この設定とともに何の影響も及ぼしません。VMware Tools が仮想マシンにインストールされていない場合は、この設定を有効にして、Site Recovery Manager でのゲスト OS のシャットダウン エラーを回避してください。</p> <p>シャットダウン タイムアウトなしで、ゲスト OS をバイパスして仮想マシンを直接パワーオフするオプションを有効にすることもできます。<a href="#">仮想マシンの起動およびシャットダウン オプションの構成</a> を参照してください。</p>
リカバリ中に自動 VM IP のカスタマイズを有効または無効にする。デフォルト値は true です。	[recovery.uselpMapperAutomatically] チェック ボックスを選択または選択解除します。IP マッピング ルールが仮想ネットワークで構成されている場合にこのオプションを選択すると、リカバリ中、Site Recovery Manager によってこれらのルールが評価されて、VM のカスタマイズが決まります。このオプションを選択解除すると、リカバリ中、IP マッピング ルールは評価されません。[仮想マシン リカバリ設定/IP カスタマイズ モード] で VM ごとにこのオプションをオーバーライドすることができます。

## 5 変更内容を保存するには、[OK] をクリックします。

### 次のステップ

以前に保護対象とした仮想マシンに変更を適用するには、これらの仮想マシンを再構成する必要があります。たとえば、defaultPriority 設定を再構成する場合は、すでに保護している仮想マシンの優先順位を、新しい defaultPriority 設定に合わせて手動で再構成できます。変更の適用は、リカバリ プランまたは保護グループから行えます。

[リカバリ プランの仮想マシンへのリカバリ設定の適用](#) および [保護グループの仮想マシンへのリカバリ設定の適用](#) を参照してください。

## リカバリ プランの仮想マシンへのリカバリ設定の適用

保護されている仮想マシンでリカバリ詳細設定を変更した場合にその設定を有効にするには、仮想マシンを再構成する必要があります。

リカバリ プランのリカバリ設定は、単一の設定または単一の仮想マシンを対象にすると、より効率的に構成できます。ディザスタ リカバリや不完全なリカバリの状況で設定を変更する場合など、この方法でしか設定を適用できない場合もあります。

### 手順

- 1 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 2 [リカバリ プラン] タブを選択し、仮想マシンが属するリカバリ プランをクリックします。
- 3 [仮想マシン] タブで、仮想マシンを右クリックして [リカバリの設定] をクリックします。
- 4 リカバリ プロパティ設定に必要な変更を加えます。
- 5 [OK] をクリックします。

### 次のステップ

保護グループの仮想マシンにリカバリ設定を適用するには、[保護グループの仮想マシンへのリカバリ設定の適用](#)を参照してください。

## 保護グループの仮想マシンへのリカバリ設定の適用

保護されている仮想マシンのリカバリ詳細設定を変更した場合、仮想マシンが再構成されるまで新しい設定は有効になりません。

複数の仮想マシンに設定を適用するときは、保護グループの機能を使用することで、リカバリ設定をより簡単に更新できます（保護グループは単一の仮想マシンにも使用できます）。これにより、保護グループ内のすべての仮想マシンを選択して、一度に設定を更新できます。

### 手順

- 1 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 2 [保護グループ] タブを選択し、仮想マシンが属する保護グループをクリックします。
- 3 [仮想マシン] タブで、仮想マシンを右クリックして [保護の削除] をクリックします。  
仮想マシンのステータスが [未構成] に変更されます。
- 4 [すべての仮想マシンの構成] をクリックして保護グループのすべての仮想マシンを再構成するか、または仮想マシンを選択して [保護の構成] をクリックし、その仮想マシンのみを再構成します。

### 次のステップ

リカバリ プランの仮想マシンにリカバリ設定を適用するには、[リカバリ プランの仮想マシンへのリカバリ設定の適用](#)を参照してください。

## リモート マネージャ設定の変更

完了するまでに長時間かかるタスクを実行する場合、タスクの完了前にリモート サイトのデフォルト タイムアウト 期間が経過する可能性があります。時間のかかるタスクが完了できるように、追加のタイムアウトを構成できます。

時間のかかるタスクは、大きな仮想マシンのテスト リカバリまたはクリーンアップなどが考えられます。仮想マシンに大容量ディスクがある場合は、テスト リカバリまたはフル リカバリの実行に長時間かかることがあります。デフォルトのタイムアウト期間中は、サイト間の接続が監視されます。タスクが完了するまでの時間がデフォルトのタイムアウト期間より長く、タスクの実行中に他のサイトに通知が送信されない場合は、タイムアウトになることがあります。この場合、リモート マネージャ設定を変更して時間のかかるタスクが完了するまでに Site Recovery Manager がタイムアウトしないようにできます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [リモート マネージャ] の順にクリックします。
- 4 サイトを選択し、[編集] をクリックして、リモート マネージャの設定を変更します。

オプション	操作
リモート処理が完了するまで待機する最長時間を構成します。デフォルト値は 900 秒です。	[remoteManager.defaultTimeout] テキスト ボックスに別の値を入力します。
仮想マシンを Site Recovery Manager で保護されているとマークします。デフォルト値は true です。	[remoteManager.enableCustomFields] チェック ボックスを選択します。
リモート サイトでリクエストを集計するまで待機する期間を設定します。デフォルト値は 2,000 ミリ秒です。	[remoteManager.powerOnAggregationInterval] テキスト ボックスに別の値を入力します。
キャンセルされたタスクが停止するまで待機する最長時間を設定します。デフォルト値は 300 秒です。	[remoteManager.taskCancelDefaultTimeout] テキスト ボックスに別の値を入力します。
リモート サイトでタスクが完了する追加タイムアウト期間を構成します。デフォルト値は 900 秒です。	[remoteManager.taskDefaultTimeout] テキスト ボックスに別の値を入力します。
リモート タスクが進行状況を報告するまで待機する秒数を設定します。この時間に進行状況を受信した場合、タスクが完了するまでの許容時間が延長されます。デフォルト値は 180 秒です。	[remoteManager.taskProgressDefaultTimeout] テキスト ボックスに別の値を入力します。
失敗した場合に仮想マシンのパワーオンを試行する回数を設定します。デフォルト値は 5 回です。	[remoteManager.vmPowerOnRetryCount] テキスト ボックスに別の値を入力します。
失敗した場合に仮想マシンのゲスト OS のシャットダウンを試行する回数を設定します。デフォルト値は 5 回です。	[remoteManager.vmGuestShutDownRetryCount] テキスト ボックスに別の値を入力します。

オプション	操作
失敗した場合に仮想マシンの設定の再構成を試行する回数を構成します。デフォルト値は 5 回です。	[remoteManager.vmReconfigureRetryCount] テキスト ボックスに別の値を入力します
xVC-vMotion のタイムアウトを待機する秒数を構成します。デフォルト値は 3,600 秒です。	[remoteManager.xVcVMotionTimeout] テキスト ボックスに別の値を入力します。

- 5 変更内容を保存するには、[OK] をクリックします。

## リモート サイトの設定の変更

リモート サイトの Site Recovery Manager Server が使用可能かどうかを判断するために保護サイトの Site Recovery Manager Server が使用するデフォルト値を変更できます。

Site Recovery Manager は、保護サイトとリカバリ サイト間の接続を監視し、接続が切断されるとアラームを出します。Site Recovery Manager が接続イベントを発生する条件や Site Recovery Manager がアラームを発生する方法を変更できます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [リモート サイト ステータス] の順にクリックします。
- 4 サイトを選択し、[編集] をクリックして、設定を変更します。

オプション	操作
「サイト ダウン」イベントを発生する前の ping の失敗回数を変更する。デフォルト値は 5 です。	[remoteSiteStatus.drPanicDelay] テキスト ボックスに別の値を入力します。
チェック エラーを宣言するまでに試行するリモート サイト ステータス チェック (ping) の回数を変更する。デフォルト値は 2 です。	[remoteSiteStatus.drPingFailedDelay] テキスト ボックスに別の値を入力します。

- 5 変更内容を保存するには、[OK] をクリックします。

## レプリケーション設定の変更

レプリケーション設定を編集して、仮想マシン プレースホルダの作成が完了するまでの Site Recovery Manager の待ち時間を変更できます。ストレージ ポリシー保護グループ内の仮想マシンの保護ポーリング間隔を変更できます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。

- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [レプリケーション] の順にクリックします。
- 4 サイトを選択し、[編集] をクリックして、設定を変更します。

オプション	操作
計画移行中に保護サイトを無効にしている間、保護されていないレプリカ仮想マシンのチェックをスキップする。デフォルト値は false です。	チェックボックスを選択して値 [replication.disablePiggybackVmsCheckDuringDeactivate] を有効にします。
ブレースホルダ仮想マシンを作成するときの待機時間のタイムアウト値（秒単位）を変更する。デフォルト値は 300 秒です。	[replication.placeholderVmCreationTimeout] テキスト ボックスに別の値を入力します。
ストレージ ポリシー保護グループ内の仮想マシンを定期的にポーリングしてマッピングが失われているかを確認し、マッピングの喪失が原因でストレージ ポリシー保護グループをリカバリできなくなる可能性がある場合は、警告する。デフォルト値は false です。	チェックボックスをオンにして、値 [replication.pollForMissingInventoryMappings] を true に変更します。
整合性グループ情報がリモート サイトにレプリケートされ、そのサイトでオンライン同期が開始するまでの待機時間のタイムアウト値（秒単位）を変更する。デフォルトは 900 秒です。	[replication.protectionInfoSyncTimeout] テキスト ボックスに別の値を入力します。
ストレージ ポリシー保護グループおよび失われているインベントリ マッピングをポーリングする間隔（秒）を変更する。デフォルト値は 120 秒です。	[replication.protectionPollInterval] テキストボックスに新しい値を入力します。 <b>注：</b> ポーリング間隔を更新する前に、環境の変化、環境が変化する頻度、および環境のパフォーマンスを予測します。

- 5 変更内容を保存するには、[OK] をクリックします。

## SSO 設定の変更

Site Recovery Manager が SSO トークンを更新するためのシングル サインオン設定を変更できます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [SSO] の順にクリックします。
- 4 サイトを選択し、[編集] をクリックして [sso.sts.tokenLifetime] 設定を変更し、更新するまでに SSO トークンを使用する秒数を指定します。  
  
デフォルト値は 28800 秒です（8 時間）。
- 5 変更内容を保存するには、[OK] をクリックします。



## ストレージ設定の変更

ストレージ設定を調整して、Site Recovery Manager と vCenter Server がストレージ レプリケーション アダプタ (SRA) との間で通信する方法を変更できます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [ストレージ] の順にクリックします。
- 4 サイトを選択し、[編集] をクリックして、ストレージの設定を変更します。

オプション	操作
リカバリしたデータストアにタグを添付するまでの待機時間 (秒単位) を変更します。デフォルト値は 30 秒です。	[storage.attachTagsDelaySec] テキスト ボックスに新しい値を入力します。
SRA コマンドを実行するまでのタイムアウト (秒単位) を変更します。デフォルト値は 300 秒です。	[storage.commandTimeout] テキスト ボックスに別の値を入力します。
データストアの監視に関連する操作間のタイムアウト (秒単位) を変更する。デフォルト値は 30 秒です。	[storage.datastoreMonitoringPollingInterval] テキスト ボックスに別の値を入力します。
Site Recovery Manager がタグ カテゴリと、Storage DRS の互換性に必要な「レプリケート済み」のタグを作成できるようにします。デフォルト値は true です。	[storage.enableSdrsStandardTagCategoryCreation] チェック ボックスを選択します。
Storage DRS との互換性のため、Site Recovery Manager がレプリケートおよび保護されたデータストアにタグを作成、適用できるようにします。デフォルト値は true です。	[storage.enableSdrsTagging] チェック ボックスを選択します。チェック ボックスをクリアすると、Site Recovery Manager はすべてのタグとタグ カテゴリを削除し、Storage DRS との互換性は失われます。
Storage DRS との互換性のため、Site Recovery Manager が、レプリケートまたは保護されたデータストア上の失われたタグまたは不正なタグを修復できるようにします。デフォルト値は true です。	[storage.enableSdrsTaggingRepair] チェック ボックスを選択します。
同時実行 SRA 操作の最大数を変更する。デフォルト値は 5 です。	[storage.maxConcurrentCommandCnt] テキスト ボックスに別の値を入力します。
ログに記録する SRA コマンドのコンソール出力の最大長 (バイト単位) を変更します。デフォルト値は 1,048,576 バイト (1 MB) です。	[storage.maxSraCommandOutputLength] テキスト ボックスに別の値を入力します。 <ul style="list-style-type: none"> <li>■ 0 の値を指定すると、SRA 出力はログに記録されません。</li> <li>■ -1 の値を指定すると、出力の長さは無制限になります。</li> <li>■ 512 バイトから 10 MB までの範囲に収まらない、0 や -1 以外の値を入力すると、値は自動的にデフォルトの 1 MB に設定されます。</li> </ul>
データストア グループの計算間隔の最小値 (秒) を変更する。デフォルト値は 0 です。	[storage.minDsGroupComputationInterval] テキスト ボックスに別の値を入力します。



オプション	操作
進行中のデータ同期操作のステータス更新間隔を変更する。デフォルト値は 30 秒です。	[storage.querySyncStatusPollingInterval] テキスト ボックスに別の値を入力します。
Storage DRS のタグ付けに関連した操作の間隔を変更します。デフォルト値は 50 秒です。	[storage.sdrsTaggingPollInterval] テキスト ボックスに別の値を入力します。
ストレージ アレイの検出チェック間隔を変更する。デフォルト値は 86400 秒です (24 時間)。	[storage.storagePingInterval] テキスト ボックスに別の値を入力します。
データ同期操作が完了するまでの最大許容時間を変更する。デフォルト値は 86400 秒です (24 時間)。	[storage.syncTimeout] テキスト ボックスに別の値を入力します。

- 変更内容を保存するには、[OK] をクリックします。

## ABR ストレージ ポリシー設定の変更

仮想マシン ストレージ ポリシーと一致するデータストアの自動検出を実行するため、ABR ストレージ ポリシー設定を変更して、間隔（秒単位）を指定することができます。

### 手順

- vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 左側のペインで [構成] - [詳細設定] - [ABR ストレージ ポリシー] の順にクリックします。
- サイトを選択し、[編集] をクリックします。
- 必要に応じて [storagePolicyAbrReplication.policyDatastorePollInterval] の値を変更します。デフォルト値は 20 秒です。
- 変更内容を保存するには、[OK] をクリックします。

## ストレージ プロバイダ設定の変更

アレイ ベース レプリケーションの場合、SAN プロバイダは、Site Recovery Manager とストレージ レプリケーション アダプタ (SRA) 間のインターフェイスです。SRA によっては、デフォルトの SAN プロバイダの値を変更する必要があります。Site Recovery Manager の SAN プロバイダに関するデフォルトのタイムアウト値などの動作を変更できます。

再署名、データストア名の修正、ホストの再スキャン カウント、および秒単位のタイムアウトの設定を変更することができます。これらの値の詳細については、アレイ ベンダーの SRA のドキュメントを参照してください。

### 手順

- vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。

- 3 左側のペインで [構成] - [詳細設定] - [ストレージ プロバイダ] の順にクリックします。
- 4 サイトを選択し、[編集] をクリックして、ストレージ プロバイダの設定を変更します。

オプション	操作
重複するボリュームのある LUN を分離および再接続するように Site Recovery Manager を設定する。デフォルト値は true です。	[storageProvider.autoDetachLUNsWithDuplicateVolume] チェック ボックスを選択します。
テストおよびリカバリ中に ESXi ホストの LVM.EnableResignature フラグを設定する。デフォルト値は 0 です。	[storageProvider.autoResignatureMode] テキスト ボックスに、フラグを無効にするには 0、有効にするには 1、無視するには 2 と入力します。デフォルト設定は 0 です。このフラグを 1 に設定すると、Site Recovery Manager は、Site Recovery Manager が管理しないボリュームを含む既知のすべての VMFS スナップショット ボリュームに再署名します。フラグ設定を 0 のままにすると、Site Recovery Manager は、管理対象の VMFS スナップショット ボリュームにのみ再署名します。
LUN の一括接続操作が各 ESXi ホストで完了するまで待機するタイムアウトを秒単位で変更する。デフォルト値は 3,600 秒です。	[storageProvider.batchAttachTimeoutSec] テキスト ボックスに値を入力します。
LUN の一括接続解除操作が各 ESXi ホストで完了するまで待機するタイムアウトを秒単位で変更する。デフォルト値は 3,600 秒です。	[storageProvider.batchDetachTimeoutSec] テキスト ボックスに値を入力します。
VMFS ボリュームがマウントされるまでの Site Recovery Manager の待機間隔を変更する。デフォルト値は 3,600 秒です。	[storageProvider.batchMountTimeoutSec] テキスト ボックスに別の値を入力します。この値は、マウントするのに長時間かかる VMFS ボリュームを Site Recovery Manager がチェックすることによりタイムアウトが発生した場合に変更します。この設定は、Site Recovery Manager 5.5.1 以降で使用可能です。
VMFS ボリュームがマウント解除されるまでの Site Recovery Manager の待機間隔を変更する。デフォルト値は 3,600 秒です。	[storageProvider.batchUnmountTimeoutSec] テキスト ボックスに別の値を入力します。この値は、マウント解除するのに長時間かかる VMFS ボリュームを Site Recovery Manager がチェックすることによりタイムアウトが発生した場合に変更します。この設定は、Site Recovery Manager 5.5.1 以降で使用可能です。
VMFS/NFS ボリュームの一括マウント解除の再試行回数を設定する。デフォルトは 3 回です。	[storageProvider.datastoreUnmountRetryCount] テキスト ボックスに別の値を入力します。
Site Recovery Manager がデータストアのアンマウントを試行する前に待機する間隔を変更します。デフォルトは 1 秒です。	[storageProvider.datastoreUnmountRetryDelaySec] テキスト ボックスに別の値を入力します。
テストおよびリカバリ中に、SRA の応答を受信してから、ESXi ホスト上でデータストアを取得するまでに待機する時間を秒単位で変更します。この設定は、SCSI デバイスがない場合のみ適用されます。デフォルト値は 0 です。	[storageProvider.fetchDatastoreDelaySec] テキスト ボックスに別の値を入力します。
リカバリの正常完了時に、リカバリ データストア名につけたプリフィックス snap-xx を強制的に削除する。デフォルト値は false です。	[storageProvider.fixRecoveredDatastoreNames] チェック ボックスを選択します。

オプション	操作
Site Recovery Manager がリカバリされたデータストアの名前に <code>snap-xx</code> プリフィックスを適用する前に待機する時間を変更します。デフォルト値は 0 秒です。	[storageProvider.fixRecoveredDatastoreNamesDelaySec] テキスト ボックスに別の値を入力します。
テストおよびリカバリ中にホスト スキャンを遅らせる。デフォルト値は 0 秒です。	<p>SRA は、ESXi ホストでリカバリ サイトの昇格ストレージ デバイスが利用可能になる前に、応答を Site Recovery Manager に送信できます。Site Recovery Manager は、SRA から応答を受信すると、ストレージ デバイスを再スキャンします。ストレージ デバイスの準備がまだ完了していないと、ESXi ではそれらが検出されず、Site Recovery Manager では、再スキャンするときにレプリケートされたデバイスが見つかりません。データストアは作成されず、復旧された仮想マシンは見つかりません。</p> <p>ESXi ホストで使用可能になるまでストレージ再スキャンの開始を遅らせるには、[storageProvider.hostRescanDelaySec] テキスト ボックスに別の値を入力します。データストアが使用できない問題が発生した場合は、この値のみを変更します。</p>
テストおよびリカバリ中にホスト スキャンを繰り返す。デフォルト値は 1 です。	<p>[storageProvider.hostRescanRepeatCnt] テキスト ボックスに別の値を入力します。一部のストレージ アレイでは、たとえば、フェイルオーバーされた LUN のスナップショットを検出するため、複数回の再スキャンが必要です。前のリリースでは、[storageProvider.hostRescanRepeatCnt] パラメータを使用してリカバリの遅延を設定していた可能性があります。その代わりに、[storageProvider.hostRescanDelaySec] パラメータを使用してください。</p>
各 HBA 再スキャンが完了するまでの Site Recovery Manager の待機間隔を変更する。デフォルト値は 300 秒です。	[storageProvider.hostRescanTimeoutSec] テキスト ボックスに別の値を入力します。
Site Recovery Manager が VMFS ボリュームの再署名を試行する回数を設定する。デフォルト値は 1 です。	[storageProvider.resignatureFailureRetryCount] テキスト ボックスに別の値を入力します。
VMFS ボリュームに再署名する場合のタイムアウトを設定する。デフォルト値は 900 秒です。	<p>[storageProvider.resignatureTimeoutSec] テキスト ボックスに別の値を入力します。</p> <p>[storageProvider.hostRescanTimeoutSec] 設定を変更する場合は、[storageProvider.resignatureTimeoutSec] 設定の値を [storageProvider.hostRescanTimeoutSec] で使用するのと同じタイムアウト値まで増加します。</p>
Storage vMotion の完了後に Site Recovery Manager での VMX ファイル候補から除外する VMX ファイル パスを指定する。デフォルト値は .snapshot です。	<p>一部のアレイでは、storageProvider.storageVmotionVmxSearch 検索アルゴリズムで無視する必要がある VMX ファイル パスが作成されます。</p> <p>[storageProvider.storageVmotionVmxFilePathsToSkip] テキスト ボックスでコンマ区切りの文字列のリストを入力して、Storage vMotion の完了後に無視する VMX ファイル パスを指定します。Site Recovery Manager は、Storage vMotion の完了後に、これらの文字列を 1 つ以上含む VMX ファイル パスを VMX ファイルの候補として見なしません。</p>
Storage vMotion がテストまたはリカバリの前またはその期間に移動した仮想マシンを識別する、リカバリしたデータストアの VMX ファイルを検索する。デフォルト値は true です。	<p>このオプションはデフォルトで選択されています。</p> <p>[storageProvider.storageVmotionVmxSearch] チェック ボックスを選択解除してこのオプションを無効にします。</p>
対応するリモート拡張デバイスと一致するようにローカル拡張デバイスのタイムアウトを秒単位で設定する。デフォルトは 300 秒です。	[storageProvider.stretchedDevicesMatchTimeout] テキスト ボックスに別の値を入力します。

オプション	操作
ホスト当たりの並列 xVC-vMotion リクエストの数を設定する。この制限は、ソース ホストとターゲット ホストの両方に適用されます。デフォルト値は 2 です。	[storageProvider.vmMigrationLimitPerHost] テキスト ボックスに別の値を入力します。
新たに検出されたデータストアがアクセス可能になるまで待機するタイムアウトを秒単位で設定する。デフォルト値は 60 秒です。	[storageProvider.waitForAccessibleDatastoreTimeoutSec] テキスト ボックスに別の値を入力します。
Site Recovery Manager がリカバリ後にデータストアの検出を待機できるようにします。	[storageProvider.waitForDeviceRediscovery] チェック ボックスを選択します。
Site Recovery Manager がフェイルオーバー後にデータストアの検出を待機できるようにします。	[storageProvider.waitForDeviceRediscoveryAfterPrepareFailover] チェック ボックスを選択します。
Virtual Center が新たに検出されたデータストアを報告するまで待機するタイムアウトを秒単位で設定する。デフォルト値は 30 秒です。	[storageProvider.waitForRecoveredDatastoreTimeoutSec] テキスト ボックスに別の値を入力します。
VMFS ボリュームがマウントされるまで Site Recovery Manager が待機する時間間隔を秒単位で設定する。デフォルト値は 30 秒です。	[storageProvider.waitForVmfsVolumesMountedStateTimeoutSec] テキスト ボックスに別の値を入力します。

- 5 変更内容を保存するには、[OK] をクリックします。

## vSphere Replication 設定の変更

グローバル設定を調整して、Site Recovery Manager と vSphere Replication の関係方法を変更できます。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [vSphere Replication] の順にクリックします。

#### 4 サイトを選択し、[編集] をクリックして、vSphere Replication の設定を変更します。

オプション	説明
Site Recovery Manager に、他のソリューションで管理されている仮想マシンのリカバリを許可する。デフォルト値は false です。	vSphere Replication により、ソリューションで仮想マシンのレプリケーションを管理できるようになります。デフォルトでは、Site Recovery Manager は自身が管理する仮想マシンのみをリカバリします。他のソリューションでレプリケーションが管理されている仮想マシンを Site Recovery Manager がリカバリできるようにするには、[vrReplication.allowOtherSolutionTagInRecovery] チェックボックスをオンにします。
リカバリ時に複数の古い特定の時点 (PIT) のスナップショットを維持する。デフォルト値は true です。	保護された仮想マシンの PIT スナップショットを作成するように vSphere Replication を構成する場合、Site Recovery Manager は、リカバリが実行されるときに最新のスナップショットのみをリカバリします。リカバリ時に古い PIT スナップショットをリカバリするには、[vrReplication.preserveMpitImagesAsSnapshots] チェックボックスを選択します。
再保護操作時にリバース レプリケーションのタイムアウト期間を変更する	[vrReplication.reverseReplicationTimeout] テキスト ボックスに別の値を入力します。入力する値は、設定するタイムアウトの時間の半分にする必要があります。デフォルト値は 7200 で、使用している同期タイムアウトの間の (14400 秒) に対応します。再保護操作の間に vSphere Replication がレプリケーション方向を反転させるときにタイムアウト エラーが発生する場合は、この値を変更してください。
vSphere Replication 同期操作のタイムアウト期間を変更します。デフォルト値は 7200 です。	[vrReplication.synchronizationTimeout] テキスト ボックスに新しい値を入力します。入力する値は、設定するタイムアウトの時間の半分にする必要があります。デフォルト値は 7200 で、使用している同期タイムアウトの間の (14400 秒) に対応します。リカバリ サイトで vSphere Replication が仮想マシンを同期させるときにタイムアウト エラーが発生する場合は、この値を変更してください。
レプリケーションのデフォルトの RPO 設定を変更します。デフォルト値は 240 です。	[vrReplication.timeDefault] テキスト ボックスに別の値を入力します。デフォルト値は 240 分 (4 時間) です。この値はレプリケーションの構成時に選択しますが、個々の仮想マシンまたは仮想マシン グループのレプリケーションを構成するときに [レプリケーションの構成] ウィザードで別の RPO を指定することができます。

#### 5 変更内容を保存するには、[OK] をクリックします。

## テレメトリ設定の変更

Site Recovery Manager のテレメトリ設定を編集して、テレメトリ レポートを送信するときに使用するプロキシホストを指定できます。

#### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 左側のペインで [構成] - [詳細設定] - [テレメトリ] の順にクリックします。

- 4 サイトを選択し、[編集] をクリックして、設定を変更します。

オプション	説明
テレメトリ レポートを送信する際に使用する HTTP プロキシのホスト名を指定します。	[telemetry.proxyHost] テキスト ボックスに HTTP プロキシ名前を入力します。
テレメトリ レポートを送信する際に使用する HTTP プロキシのポートを指定します。	[telemetry.proxyPort] ボックスにポート番号を入力します。
テレメトリ レポートを送信するときに HTTP プロキシへの接続に SSL を使用するかどうかを指定します。デフォルト値は false です。	スライダを移動して、値 [telemetry.proxyUseSsl] を true に変更します。

- 5 [OK] をクリックして、変更内容を保存します。

## 大規模な Site Recovery Manager 環境を実行するように設定を変更する

Site Recovery Manager を使用して多数の仮想マシンのテストまたはリカバリを行う場合は、使用中の環境で最良のリカバリ時間を達成するため、またはタイムアウトを回避するために、デフォルトの Site Recovery Manager 設定を変更しなければならない場合があります。

大規模環境では、Site Recovery Manager は多数の仮想マシンを同時にパワーオンまたはパワーオフする場合があります。多数の仮想マシンを同時にパワー オンまたはパワー オフすると、仮想インフラストラクチャで負荷が重くなり、タイムアウトが発生する可能性があります。特定の Site Recovery Manager 設定を変更してタイムアウトを回避するには、Site Recovery Manager が同時に実行するパワーオン操作またはパワーオフ操作の数を制限するか、タイムアウト値を増やします。

パワー オン操作またはパワー オフ操作に設定する制限は、インフラストラクチャで処理できるパワー オンまたはパワー オフの同時操作の数に応じて異なります。

vSphere Web Client または Site Recovery Manager クライアント プラグインの [詳細設定] メニューで特定のオプションを変更します。その他の設定を変更するには、Site Recovery Manager Server または Site Recovery Manager Virtual Appliance の `vmware-dr.xml` 構成ファイルを編集します。該当するオプションがある場合は、必ずクライアント メニューを使用して設定を変更してください。設定を変更する場合は、保護サイトとリカバリ サイトの両方の Site Recovery Manager インスタンスと vCenter Server インスタンスで同じ変更を行う必要があります。

変更可能な設定については、「[大規模な Site Recovery Manager 環境の設定](#)」を参照してください。

### 手順

- 1 vSphere Web Client または vSphere Client で、クラスタを選択します。
- 2 [構成] タブで、[サービス] - [vSphere DRS] を選択します。

vCenter Server 6.0 Update 3 を使用している場合は、[管理] タブで、[サービス] - [vSphere DRS] を選択します。

- 3 [編集] をクリックします。

- 4 [詳細オプション] で、srmMaxBootShutdownOps を設定します。

オプション	説明
[オプション] テキスト ボックス	srmMaxBootShutdownOps と入力します。
[値] テキスト ボックス	起動処理とシャット ダウン処理の同時実行数の最大値を入力します。たとえば、値を 32 に設定すると、仮想マシン 1 ～ 32 が同時に起動またはシャットダウンし、仮想マシン 33 は最初のバッチの仮想マシンのいずれかが終了した後すぐに、起動またはシャットダウンします。仮想マシン 34 は、最初のバッチの 2 番目の仮想マシンが終了した後に起動します（以下同様）。

- 5 変更内容を保存するには、[OK] をクリックします。
- 6 Site Recovery Manager Server ホストにログインします。
- 7 テキスト エディタで vmware-dr.xml ファイルを開きます。
- Windows 版の Site Recovery Manager を使用している場合は、Site Recovery Manager Server ホスト マシンの C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config フォルダで vmware-dr.xml ファイルを検索します。
  - Site Recovery Manager Virtual Appliance を使用している場合は、アプライアンスの /opt/vmware/srm/conf/ ディレクトリで vmware-dr.xml ファイルを検索します。
- 8 vmware-dr.xml ファイルの defaultMaxBootAndShutdownOpsPerCluster 設定と defaultMaxBootAndShutdownOpsPerHost 設定を変更します。

```
<config>
...
  <defaultMaxBootAndShutdownOpsPerCluster>24</defaultMaxBootAndShutdownOpsPerCluster>
  <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
...
</config>
```

これらの要素が vmware-dr.xml ファイルにまだない場合は、<config> セクションの任意の場所に追加できます。

<defaultMaxBootAndShutdownOpsPerCluster> 値を 24 に設定すると、最初のバッチ（24 台）内のいずれかの仮想マシンが終了した後すぐに、次のゲストが起動またはシャットダウンします。つまり、仮想マシン 1 ～ 24 はすべて同時に起動し、仮想マシン 25 は最初のバッチの仮想マシンのいずれかが終了した後に起動します。仮想マシン 26 は、最初のバッチ内の 2 番目の仮想マシンが終了した後に起動します（以下同様）。

- 9 新しい設定を適用するには、Site Recovery Manager Server を再起動します。
- 10 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
- 11 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。



- 12 左側のペインで [構成] - [詳細設定] - [vSphere Replication] の順にクリックし、  
`vrReplication.synchronizationTimeout` と  
`vrReplication.reverseReplicationTimeout` の設定値を増やします。

デフォルト値は 7200 で、使用している同期タイムアウトの間隔 (14400 秒) に対応します。

- 13 [詳細設定] - [ストレージ] の順に選択し、サイトを選択して、`storage.commandTimeout` の設定値を増やします。

デフォルト値は 300 秒です。

- 14 変更内容を保存するには、[OK] をクリックします。

## 大規模な Site Recovery Manager 環境の設定

大量の仮想マシンを保護するには、デフォルトの Site Recovery Manager 設定に変更を加えて使用環境に最適なリカバリ時間を設定するか、またはタイムアウトを回避します。

vSphere Web Client または Site Recovery Manager クライアント プラグインの [詳細設定] メニューで特定のオプションを変更します。その他の設定を変更するには、Site Recovery Manager Server または Site Recovery Manager Virtual Appliance の `vmware-dr.xml` 構成ファイルを編集します。該当するオプションがある場合は、必ずクライアント メニューを使用して設定を変更してください。設定を変更する場合は、保護サイトとリカバリ サイトの両方の Site Recovery Manager インスタンスと vCenter Server インスタンスで同じ変更を行う必要があります。

設定を変更するには、[大規模な Site Recovery Manager 環境を実行するように設定を変更する](#) を参照してください。



表 12-1. パワーオンまたはパワーオフの同時操作の数を変更する設定

オプション	説明
[srmMaxBootShutdownOps]	任意のクラスタでの同時パワーオン処理の最大数を指定します。ゲスト シャットダウン（強制パワーオフではありません）はこの値にしたがって調整されます。ゲスト シャットダウンは、プライマリ サイト シャットダウン（計画済みフェイルオーバー）と IP カスタマイズ ワークフローの実行中に発生します。vSphere Web Client または vSphere Client のクラスタごとにこのオプションを変更するには、クラスタを右クリックして [設定] を選択します。[vSphere DRS] をクリックしてから [編集] - [詳細オプション] をクリックします。オプションを入力して、vmware-dr.xml ファイルに設定可能な [defaultMaxBootAndShutdownOpsPerCluster] 値をオーバーライドします。vmware-dr.xml ファイルでグローバル値 [defaultMaxBootAndShutdownOpsPerCluster] を設定してから、vSphere Web Client または vSphere Client の個々のクラスタに異なる [srmMaxBootShutdownOps] 値を設定できます。デフォルトでは、調整がオフになっています。
[defaultMaxBootAndShutdownOpsPerCluster]	Site Recovery Manager が保護するすべてのクラスタに、同時パワーオン処理の最大数を指定します。ゲスト シャットダウン（強制パワーオフではありません）はこの値にしたがって調整されます。ゲスト シャットダウンは、プライマリ サイト シャットダウン（計画済みフェイルオーバー）と IP カスタマイズ ワークフローの実行中に発生します。この設定は、vmware-dr.xml ファイルで変更します。vSphere Web Client で設定可能な [srmMaxBootShutdownOps] 値は、[defaultMaxBootAndShutdownOpsPerCluster] 値をオーバーライドします。vmware-dr.xml ファイルでグローバル値 [defaultMaxBootAndShutdownOpsPerCluster] を設定してから、vSphere Web Client の個々のクラスタに異なる [srmMaxBootShutdownOps] 値を設定できます。デフォルトでは、調整がオフになっています。
[defaultMaxBootAndShutdownOpsPerHost]	任意のスタンドアロン ホストでの同時パワーオン処理の最大数を指定します。このオプションは、vmware-dr.xml ファイルでのみ設定できます。デフォルトでは、調整がオフになっています。

表 12-2. タイムアウト期間を変更する設定値

オプション	説明
[vrReplication.synchronizationTimeout]	Site Recovery Manager はタイムアウトを強制して、テストまたはフェイルオーバー時に vSphere Replication によってレプリケートされた仮想マシンのオンラインまたはオフライン同期を完了します。同期処理が所定時間内に終了しないと（たとえば、ネットワーク速度が遅かったり、大きな仮想マシンであったりするため）、Site Recovery Manager はテストまたはフェイルオーバー時に障害を報告します。Site Recovery ユーザー インターフェイスでこのオプションを変更します。Site Recovery の [ホーム] タブで、サイト ペアを選択し、[詳細表示] をクリックします。左側のペインで [構成] - [詳細設定] - [vSphere Replication] の順に選択します。デフォルト値は 7200 で、使用している同期タイムアウトの間隔 (14400 秒) に対応します。
[vrReplication.reverseReplicationTimeout]	再保護操作時のリバース レプリケーションのタイムアウト期間。Site Recovery ユーザー インターフェイスでこのオプションを変更します。Site Recovery の [ホーム] タブで、サイト ペアを選択し、[詳細表示] をクリックします。左側のペインで [構成] - [詳細設定] - [vSphere Replication] の順に選択します。デフォルト値は 7200 で、使用している同期タイムアウトの間隔 (14400 秒) に対応します。
[storage.commandTimeout]	ABR 関連のワークフローで SRA コマンドを実行するときのタイムアウトです。LUN やスナップショットを取得する場合など、場合によっては、一部のアレイドでの応答にデフォルト時間より長くかかることがあります。Site Recovery ユーザー インターフェイスでこのオプションを変更します。Site Recovery の [ホーム] タブで、サイト ペアを選択し、[詳細表示] をクリックします。左側のペインで [構成] - [詳細設定] - [ストレージ] の順に選択します。デフォルト値は 300 秒です。

# Site Recovery Manager のイベントとアラーム

# 13

Site Recovery Manager はイベントのログをサポートしています。各イベントには、イベントが発生する場合に Site Recovery Manager が起動することができる対応するアラームが含まれます。この方法により、システムの健全性を追跡し、Site Recovery Manager が提供する保護に影響が出る前に潜在的な問題を解決します。

この章には、次のトピックが含まれています。

- Site Recovery Manager がサイト間の接続を監視する方法
- Site Recovery Manager アラームの作成

## Site Recovery Manager がサイト間の接続を監視する方法

Site Recovery Manager は、保護サイトとリカバリ サイト間の接続を監視し、リモート サイトの応答が停止するとイベントを記録します。

Site Recovery Manager が、ペアになっている 2 台の Site Recovery Manager Server インスタンスの間に接続を確立すると、接続を開始した Site Recovery Manager Server は `RemoteSiteUpEvent` イベントを送信します。

Site Recovery Manager は、監視された接続がダウンしていることを検出したとき、ping 要求をリモート サイトに送信して定期的な接続確認を開始します。Site Recovery Manager は、接続確認を監視しイベントを記録します。

- 接続監視は、いくつかの失敗した ping をスキップします。この数を設定するには、`remoteSiteStatus.drPingFailedDelay` 値を設定します。デフォルトは 2 です。
- 失敗してスキップされた ping の数が `remoteSiteStatus.drPingFailedDelay` 設定の値を超過すると、Site Recovery Manager は `RemoteSitePingFailedEvent` イベントを送信します。
- 失敗してスキップされた ping の数が上限を超過すると、Site Recovery Manager は、ping が失敗するたびに `RemoteSiteDownEvent` イベントを送信し、`RemoteSitePingFailedEvent` イベントの送信を停止します。失敗した ping の上限値を設定するには、`remoteSiteStatus.drPanicDelay` 値を設定します。デフォルトは 5 です。
- Site Recovery Manager は接続が再確立されるまで、`RemoteSiteDownEvent` イベントの送信を継続します。
- リモート サイトの Site Recovery Manager サーバへの接続が再確立されると、Site Recovery Manager は `RemoteSiteUpEvent` イベントを送信します。

## Site Recovery Manager アラームの作成

Site Recovery Manager はアラームを vCenter Server でサポートされているアラームに追加します。Site Recovery Manager アラームは、E メール通知を送信し、SNMP トラップを送信し、vCenter Server ホストでスクリプトを実行するように構成できます。

[アラーム定義] タブには、すべての Site Recovery Manager アラームが一覧表示されます。各アラームの設定を編集して、イベントでアラームがトリガーされたときに Site Recovery Manager が実行するアクションを指定できます。デフォルトでは、Site Recovery Manager のどのアラームもアラームを構成するまで動作しません。

**注：** 複数の vCenter Server がある環境では、Site Recovery Manager は、特定の vCenter Server のイベントを選択した場合にも、拡張として登録されている Site Recovery Manager サーバからのすべてのイベントを表示します。

### 前提条件

アラームで E メール通知を送信するには、[vCenter Server 設定] メニューで [E メール] 設定を構成します。『ESXi および vCenter Server のドキュメント』を参照してください。

### 手順

- 1 vSphere Client で、vCenter Server をクリックします。
- 2 [構成] タブで [詳細] を展開してから [アラーム定義] をクリックすると、vCenter Server アラームのリストが表示されます。
- 3 新しいアラームを追加するには、[追加] をクリックします。
- 4 [名前] ページで、アラーム名、説明を入力し、[次へ] をクリックします。
- 5 [ターゲット] ページで、ドロップダウン メニューからターゲットを選択し、[次へ] をクリックします。
- 6 [アラーム ルール] ページで、ドロップダウン メニューと対応するステータスからイベントを選択します。  
リストで繰り返されるイベントがある場合、各イベントは単一の Site Recovery Manager インスタンスを表し、それが登録されている拡張に対するアラームをトリガーします。たとえば、複数の Site Recovery Manager インスタンスがあるシナリオでは、両方の拡張の同じイベントに対して `RecoveryPlanCreated` (SRM 1) と `RecoveryPlanCreated` (SRM 2) を使用できます。
- 7 アラームをトリガーする条件を追加するには、[引数を追加] をクリックし、ドロップダウン メニューから引数を選択し、演算子および警告から重大な条件までの遷移を選択します。
- 8 (オプション) E メール通知の送信、SNMP トラップの送信、またはスクリプトの実行を選択します。
- 9 [次へ] をクリックします。
- 10 [確認] ページで、アラームを有効にするかどうかを選択し、[作成] をクリックします。

## Site Recovery Manager のイベント参照

Site Recovery Manager はさまざまな種類のイベントを監視します。

## サイト ステータス イベント

サイト ステータス イベントは、保護サイトと復旧サイトのステータス、およびその間の接続に関する情報を提供します。

表 13-1. サイト ステータス イベント

イベント名	イベント タイプ	イベントの説明	カテゴリ
不明な状態	UnknownStatusEvent	Site Recovery Manager Server のステータスは不明です	情報
リモート サイトが停止しました	RemoteSiteDownEvent	Site Recovery Manager Server はリモートの Site Recovery Manager Server との接続を失いました。	エラー
リモート サイトの ping に失敗しました	RemoteSitePingFailedEvent	リモート サイトでの障害か、ネットワーク接続の問題です。	警告
リモート サイトが作成されました	RemoteSiteCreatedEvent	ローカル サイトはリモート サイトと正常にペアリングされました。	情報
リモート サイトが起動しました	RemoteSiteUpEvent	Site Recovery Manager Server はリモートの Site Recovery Manager Server との接続を再確立します。	情報
リモート サイトが削除されました	RemoteSiteDeletedEvent	リモートの Site Recovery Manager サイトが削除されました。	情報
vSphere Replication で複製された仮想マシンが保護グループに追加されました	HbrGroupVmAssociatedEvent	vSphere Replication で複製された仮想マシンが保護グループに追加されました。	情報
vSphere Replication で複製された仮想マシンが保護グループから削除されました	HbrGroupVmDisassociatedEvent	vSphere Replication で複製された仮想マシンが保護グループから削除されました。	情報
ローカルの vSphere Replication サーバが停止しています	LocalHmsConnectionDownEvent	vSphere Replication への接続の試行を繰り返しましたが失敗しました。	エラー
ローカルの vSphere Replication サーバへの接続がリストアされました	LocalHmsConnectionUpEvent	vSphere Replication への接続に成功しました。	情報
ローカルの vSphere Replication サーバが応答しません	LocalHmsPingFailedEvent	ローカルの vSphere Replication サーバへの接続を確立できませんでした	警告
ディスク容量が不足しています	LowDiskSpaceEvent	ローカル サイトの空きディスク領域が少なくなっています。	警告
メモリが不足しています	LowMemoryEvent	ローカル サイトの使用可能なメモリが少なくなっています。	警告
SRM Server 証明書はまだ有効ではありません	SrmCertificateNotValidEvent	指定された SRM Server の SSL/TLS 証明書には未来の日付が指定されています。	エラー
SRM Server 証明書の有効期限が切れます	SrmCertificateExpiringEvent	指定された SRM Server の SSL/TLS 証明書は指定された日数で期限が切れます。	情報
SRM Server 証明書の有効期限が切れました	SrmCertificateExpiredEvent	指定された SRM Server の SSL/TLS 証明書は有効期限が切れています。	エラー

## 保護グループ イベント

保護グループ イベントは保護グループに関連するアクションとステータスに関する情報を示します。

表 13-2. 保護グループ レプリケーション イベント

イベント	説明	原因	カテゴリ
CreatedEvent	保護グループを作成しました。	保護グループの作成のコミット段階の完了時に、両方の vCenter Server に投稿します。	情報
RemovedEvent	保護グループを削除しました。	保護グループの削除のコミット段階の完了時に、両方の vCenter Server に投稿します。	情報
ReconfiguredEvent	保護グループを再構成しました。	保護グループの再構成のコミット段階の完了時に、両方の vCenter Server に投稿します。	情報
ProtectedVmCreatedEvent	グループの仮想マシンが保護のために構成されました。	仮想マシンの保護のコミット段階の完了時に、両方の vCenter Server に投稿します。	情報
ProtectedVmRemovedEvent	グループの仮想マシンが保護のために構成されなくなりました。	仮想マシンの保護解除のコミット段階の完了時に、両方の vCenter Server に投稿します。	情報
ProtectedVmReconfiguredProtectionSettingsEvent	仮想マシンの保護設定を再構成しました。	仮想マシン保護設定の再構成のコミット段階の完了時に、両方の vCenter Server に投稿します。	情報
ProtectedVmReconfiguredRecoveryLocationSettingsEvent	仮想マシンの復旧ロケーション設定を再構成しました。	保護された仮想マシンのリカバリ場所の設定の再構成を正常に完了したときにのみ、保護サイト vCenter Server に投稿します。	情報
PlaceholderVmCreatedEvent	vCenter Server インベントリにプレースホルダ仮想マシンが作成されました。	保護、修理操作の結果として、プレースホルダ仮想マシンを作成したときに、リカバリ サイト vCenter Server に投稿します。	情報
PlaceholderVmCreatedFromOldProductionVmEvent	古い保護された仮想マシンの識別情報を使用して、vCenter Server インベントリにプレースホルダ仮想マシンが作成されました。	保護操作の間または後で、古い保護仮想マシンとプレースホルダ仮想マシンのスワッピングの結果として、プレースホルダ仮想マシンを作成したときに、リカバリ サイト vCenter Server に投稿します。	情報
VmFullyProtectedEvent	グループの仮想マシン：未解決のデバイスはすべて解決されています。	保護仮想マシンの未解決だったデバイスはすべて解決されました。	警告
VmNotFullyProtectedEvent	グループの仮想マシン：保護のために 1 つまたは複数のデバイスを構成する必要があります。	空でない unresolvedDevices セットでリカバリ場所の設定を更新してデバイスを処理するときのみ、保護サイト vCenter Server に投稿します。これは、保護された仮想マシンに変更を行ったり、仮想マシンの再保護中にトリガーできます。	警告
PlaceholderVmUnexpectedlyDeletedEvent	グループの仮想マシン：プレースホルダ仮想マシンは vCenter Server インベントリから削除されました。	プレースホルダ仮想マシンが予期せずに削除されたか、vCenter Server インベントリから除去されたことが Site Recovery Manager で検出されたときにのみ、リカバリ サイト vCenter Server に投稿します。	警告

表 13-2. 保護グループ レプリケーション イベント（続き）

イベント	説明	原因	カテゴリ
ProductionVmDeletedEvent	グループの仮想マシン：保護された仮想マシンは仮想マシン vCenter Server インベントリ から削除されました。	保護された仮想マシンが削除されたか、vCenter Server インベントリから削除されたときに投稿します。	エラー
ProductionVmInvalidEvent	グループの仮想マシン：レプリケーションする保護された仮想マシンのファイルのロケーションを解決できません。	レプリケートするために保護された仮想マシン ファイルをレプリケーション プロバイダが検出できないときに投稿します。	エラー

## 復旧イベント

リカバリ イベントは Site Recovery Manager のリカバリ プロセスに関連するアクションとステータスに関する情報を示します。

表 13-3. 復旧イベント

イベント名	イベントタイプ	イベントの説明	カテゴリ
リカバリ プランは、指定した仮想マシンのリカバリを開始しました。	RecoveryVmBegin	復旧仮想マシンが正常に作成された時に通知します。仮想マシン ID がわかる前に一部のエラーが発生すると、イベントは発行されません。	情報
リカバリ プランは、仮想マシンのリカバリを完了しました。	RecoveryVmEnd	最後のパワーオン後のスクリプトが完了した後、または仮想マシンの recovery-stopping エラーが発生した後で通知します。	情報
リカバリ プラン [[data.Plan]] で仮想マシン [[data.Vm]] の登録に失敗しました。	RecoveryVmRegisterFailed	リカバリされた仮想マシンがリカバリ サイトの VC への登録に失敗した後の SPPG の場合に通知します。そのプランがローカル VC に対して実行された場合、[data.local] は true になります。	情報
リカバリ プラン <i>hostname</i> が作成されました。	PlanCreated	新しいプランが作成されたときに通知します。プランがホストされる各 vCenter Server インスタンスに送信されます。	情報
リカバリ プランが破棄されました。	PlanDestroy	プランがサイトから削除されたときに、通知します。プランの削除が要求されたサイトでは、他のサイトでプランが削除されるのを待つ間、大幅な遅延が発生する場合があります。プランがホストされる各 vCenter Server インスタンスに送信されます。	情報
リカバリ プランが変更されました。	PlanEdit	既存のプランが編集されたときに通知します。	情報
リカバリ プランでテストが開始されました。	PlanExecTestBegin	復旧テストが開始されたときに、復旧サイトで通知します。	情報
リカバリ プランでテストが開始されました。	PlanExecTestEnd	復旧テストが完了したときに、復旧サイトで通知します。	情報
リカバリ プランでテスト クリーンアップが開始されました。	PlanExecCleanupBegin	クリーンアップが開始されたときに、復旧サイトで通知します。	情報

表 13-3. 復旧イベント（続き）

イベント名	イベントタイプ	イベントの説明	カテゴリ
リカバリ プランの中でテスト クリーンアップが完了しました。	PlanExecCleanupEnd	復旧テストクリーンアップが完了したときに、復旧サイトで通知します。	情報
リカバリ プランでリカバリが開始されました。	PlanExecBegin	復旧が開始されたときに、復旧サイトで通知します。	情報
リカバリ プランがリカバリを完了しました。	PlanExecEnd	復旧が完了したときに、復旧サイトで通知します。	情報
リカバリ プランの再保護操作が開始されました。	PlanExecReprotectBegin	再保護が開始されたときに、復旧サイトで通知します。	情報
リカバリ プランの再保護操作が完了しました。	PlanExecReprotectEnd	再保護が完了したときに、復旧サイトで通知します。	情報
リカバリ プランは、プロンプトを表示してユーザー入力を待っています。	PlanPromptDisplay	プロンプト ステップが見つかったときに復旧サイトで通知します。キーは、プロンプトの固有な識別子です。	情報
リカバリ プランでプロンプトに対する応答を受け取りました。	PlanPromptResponse	プロンプト ステップが閉じたとき復旧サイトで通知します。	情報
リカバリ プランで、Site Recovery Manager Server マシンでのコマンドの実行が開始されました。	PlanServerCommandBegin	Site Recovery Manager が Site Recovery Manager Server マシンでコールアウト コマンドの実行を開始したときに、リカバリ サイトで通知します。	情報
リカバリ プランで、Site Recovery Manager Server マシンでのコマンドの実行が完了しました。	PlanServerCommandEnd	Site Recovery Manager が Site Recovery Manager Server マシンでコールアウト コマンドの実行を終了したときに、リカバリ サイトで通知します。	情報
リカバリ プランで、リカバリされた仮想マシンでのコマンドの実行が開始されました。	PlanVmCommandBegin	Site Recovery Manager がリカバリされた仮想マシンでコールアウト コマンドの実行を開始したときに、リカバリ サイトで通知します。	情報
リカバリ プランで、リカバリされた仮想マシンでのコマンドの実行が完了しました。	PlanVmCommandEnd	Site Recovery Manager がリカバリされた仮想マシンでコールアウト コマンドの実行を終了したときに、リカバリ サイトで通知します。	情報

## ストレージとストレージ プロバイダ イベント

ストレージやストレージ プロバイダ イベントは、アクションやステータス関連のストレージまたはストレージ プロバイダに関する情報を提供します。



表 13-4. SRA イベント

イベント	説明	原因	カテゴリ
StorageAdaptLoadEvent	指定された SRA をロードしました。	Site Recovery Manager は起動時またはユーザーが開始した SRA の再ロード中に、新しい SRA を検出しました。	情報
StorageAdaptReloadFailEvent	指定したバスからの SRA のロードに失敗しました。	Site Recovery Manager は、起動時またはユーザーが開始した SRA の再ロード中に、既知の SRA を再ロードできませんでした。	エラー
StorageAdaptChangeEvent	指定した SRA の新しいバージョンをロードしました。	Site Recovery Manager は既知の SRA がアップグレードされたことを検出しました。	情報

表 13-5. アレイ マネージャ イベント

イベント	説明	原因	カテゴリ
SAManagerAddedEvent	指定した SRA を使用して、特定のアレイ マネージャを作成しました。	ユーザーがアレイ マネージャを追加しました。	情報
SAManagerRemovedEvent	指定したアレイ マネージャを削除しました。	ユーザーがアレイ マネージャを削除しました。	情報
SAManagerReconfigEvent	指定したアレイ マネージャを再構成しました。	ユーザーがアレイ マネージャのプロパティを編集しました。	情報
SAManagerPingOkEvent	指定したアレイ マネージャの ping が成功しました。	Site Recovery Manager Server はアレイ マネージャを正常に ping しました。	情報
SAManagerPingFailEvent	指定したアレイ マネージャの ping に失敗しました。	アレイ マネージャの ping 中にエラーが発生しました。	エラー

表 13-6. アレイ ペア イベント

イベント	説明	原因	カテゴリ
SAPairDiscoveredEvent	アレイ マネージャを使用してレプリケートされたアレイ ペアを検出しました。	ユーザーがレプリケートされたアレイ ペアを検出したアレイ マネージャを作成しました。	情報
SAPairEnabledEvent	アレイ マネージャを使用してレプリケートされたアレイ ペアを有効にしました。	ユーザーはアレイ ペアを有効にしました。	情報
SAPairDisabledEvent	アレイ マネージャを使用してレプリケートされたアレイ ペアを無効にしました。	ユーザーがアレイ ペアを無効にしました。	情報

表 13-6. アレイ ペア イベント（続き）

イベント	説明	原因	カテゴリ
SAPairPingOkEvent	レプリケートされたアレイ ペアの ping が成功しました。	Site Recovery Manager Server はアレイ ペアを正常に ping しました。	情報
SAPairPingFailEvent	レプリケートされたアレイ ペアの ping に失敗しました。	アレイ ペアの ping 中にエラーが発生しました。	エラー

表 13-7. データストア イベント

イベント	説明	原因	カテゴリ
StorageDsDiscoveredEvent	レプリケートされたデータストアを検出しました。	Site Recovery Manager Server は、レプリケートされたデータストアを検出しました。	情報
StorageDsLostEvent	指定されたデータストアは、もはやレプリケートされていません。	データストアをバックアップするストレージ デバイスのレプリケーションをユーザーがオフにしました。	情報
StorageRdmDiscoveredEvent	指定された仮想マシンに接続されたレプリケートされた RDM が検出されました。	Site Recovery Manager Server は、レプリケートされた RDM を検出しました。これは、RDM ディスクを保護された仮想マシンに追加するときに表示されます。	情報
StorageRdmLostEvent	指定した仮想マシンに接続されている RDM はもはやレプリケートされません。	ユーザーは RDM をバックアップする LUN のレプリケーションをオフにしました。	情報

表 13-8. 保護イベント

イベント	説明	原因	カテゴリ	イベント ターゲット
SPDsProtEvent	指定された保護グループでデータストアを保護しました。	ユーザーは新しい保護グループまたは既存の保護グループにデータストアを含めました。	情報	データストア
SPDsUnprotEvent	指定されたデータストアの保護を解除しました。	ユーザーは保護グループからデータストアを削除するか、このデータストアが含まれている保護グループを削除しました。これは、保護グループから削除するか保護グループを削除することによってデータストアの保護を解除するときに表示されます。	情報	データストア
SPVmDiscoveredEvent	レプリケートされた仮想マシンを検出しました。	ユーザーはレプリケートされたデータストアの仮想マシンを作成しました。	情報	仮想マシン
SPVmLostEvent	指定した仮想マシンが、もはやレプリケートされません。	ユーザーはレプリケートされたデータストアから仮想マシンを移行しました。	情報	仮想マシン

表 13-8. 保護イベント（続き）

イベント	説明	原因	カテゴリ	イベント ターゲット
SPDsProtMissingEvent	レプリケートされたデータストアは指定された保護グループに含まれる必要がありますが、代替の保護グループに含まれています。	これは、マージが必要なデータストアがあり、まだ保護されていない場合に表示されます。競合イベントでは、データストアはすでに保護されています。	警告	データストア
SPDsProtConflictEvent	レプリケートされたデータストアは、指定された保護グループに含める必要があります。	これは、マージが必要なデータストアがあり、まだ保護されていない場合に表示されます。競合イベントでは、データストアはすでに保護されています。	エラー	データストア
SPDsReplicationLostEvent	指定された保護グループに含まれるデータストアが、もはやレプリケートされません。	ユーザーがデータストアをバックアップするデバイスのレプリケーションをオフにしました。	エラー	データストア
SPGroupProtRestoredEvent	保護は指定された保護グループに対してリストアされました。	保護グループの以前の（空でない）問題が解決しました。	情報	保護グループ
SPVmdsProtMissingEvent	仮想マシンで使用するデータストアは、指定された保護グループに含める必要があります。	保護グループによってすでに保護されている仮想マシンにデータストアを追加し、このデータストアがこの保護グループの一部ではない場合は、追加する必要があります。	警告	データストア
SPVmdsProtConflictEvent	指定された仮想マシンにより使用されるデータストアは指定された保護グループに追加される必要がありますが、現在は代替保護グループで使用中です。	保護グループによってすでに保護されている仮想マシンにデータストアを追加し、このデータストアがこの保護グループの一部ではない場合は、追加する必要があります。	エラー	データストア
SPVmdsReplicationLostEvent	指定された仮想マシンで使用され、指定された保護グループに含まれているデータストアは、もはやレプリケートされません。	説明を参照してください。	エラー	データストア
SPVmProtRestoredEvent	指定された保護グループの指定された仮想マシンの保護がリストアされました。	保護された仮想マシンの以前の（空でない）問題が解決しました。保護されていない仮想マシンに関連した問題が解決されたときに、このイベントは投稿されません。	情報	仮想マシン
SPCgSpansProtGroupsEvent	指定された整合性グループは、指定された保護グループにまたがっています。	これは、別々の保護グループで保護される 2 つのデータストアがあり、それらを後でアレイの 1 つの整合性グループにマージするときに表示されます。	エラー	データストア
SPCgDsMissingProtEvent	指定された整合性グループのデータストアは、指定された保護グループに含める必要があります。	説明を参照してください。	エラー	データストア

表 13-8. 保護イベント（続き）

イベント	説明	原因	カテゴリ	イベント ターゲット
SPDspansConsistGroupsEvent	データストアは別の整合性グループのデバイスにまたがっています。	これは、複数の LUN の先頭にデータストアがあっても、それらの LUN が同じ整合性グループに属していない場合に表示されます。	エラー	データストア
SPNfsDsUrlConflictEvent	指定されたボリュームからマウントされた NFS データストアは、リモートホストからマウントされた異なる URL をもっています。リモートパスは指定された URL があります。一方で、他のホストからマウントされたデータストアには、指定された URL があります。	同じ NFS ボリュームは 2 つの異なるデータストアの同じ NFS サーバの異なる IP アドレスを使用してマウントされています。	エラー	データストア

## ライセンス イベント

ライセンシング イベントは、Site Recovery Manager ライセンシング ステータスの変更に関する情報を提供します。

表 13-9. ライセンス イベント

イベント	説明	原因
LicenseExpiringEvent	指定したサイトの Site Recovery Manager ライセンスは、指定した日数で有効期限が切れます。	24 時間ごとに、評価版ではない有効期限のあるライセンスが残り日数に対してチェックされます。このイベントは、結果を投稿します。
EvaluationLicenseExpiringEvent	指定したサイトの Site Recovery Manager 評価ライセンスは、指定した日数で有効期限が切れます。	24 時間ごとに、評価ライセンスは残り日数に対してチェックされます。このイベントは、結果を投稿します。
LicenseExpiredEvent	指定したサイト ライセンスの Site Recovery Manager ライセンスの有効期限が切れました。	30 分ごとに、有効期限の切れた（評価版ではない）ライセンスはこのイベントを投稿します。
EvaluationLicenseExpiredEvent	指定したサイト ライセンスの Site Recovery Manager 評価ライセンスの有効期限が切れました。	30 分ごとに、評価版ライセンスはこのイベントを投稿します。
UnlicensedFeatureEvent	指定したサイトの Site Recovery Manager ライセンスは、ライセンスの指定数を超えて割り振られています。	24 時間ごとに、仮想マシンの保護または保護解除の時点で、このイベントはライセンスの合計数がライセンスの容量を超える場合に投稿されます。
LicenseUsageChangedEvent	指定したサイトの Site Recovery Manager ライセンスは、合計ライセンス数のうち指定した数を使用しています。	24 時間ごとに、仮想マシンの保護または保護解除の時点で、このイベントはライセンスの合計数がライセンスの容量を超えない場合に投稿されます。

## 権限イベント

権限イベントは、Site Recovery Manager 権限への変更についての情報を提供します。

表 13-10. 権限イベント

イベント	説明	原因
PermissionsAddedEvent	Site Recovery Manager 上のエンティティ用に作成された権限。	エンティティ用の権限は、指定されたロールを使用して作成されました。IsPropagate フラグは、権限がエンティティ階層の下へ伝達されているかどうかを示します。
PermissionsDeletedEvent	Site Recovery Manager 上のエンティティ用に削除された権限ルール。	エンティティに対する権限が削除されました。
PermissionsUpdatedEvent	Site Recovery Manager 上のエンティティ用に変更された権限。	示されているエンティティに対する権限が変更されました。

## SNMP トラップ

Site Recovery Manager は、vCenter Server で定義されるコミュニティ ターゲットに SNMP トラップを送信します。SNMP トラップは、vSphere Web Client を使用して構成できます。localhost または 127.0.0.1 を SNMP トラップのターゲット ホストとして入力すると、Site Recovery Manager は Site Recovery Manager インストーラによって構成される vSphere Server の IP アドレスまたはホスト名を使用します。

表 13-11. SNMP トラップ

イベント	説明	原因
RecoveryPlanExecuteTestBeginTrap	このトラップは、リカバリ プランがテストを開始するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態。
RecoveryPlanExecuteTestEndTrap	このトラップは、リカバリ プランがテストを終了するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、結果ステータス。
RecoveryPlanExecuteCleanupBeginTrap	このトラップは、リカバリ プランがテストのクリーンアップを開始するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態。
RecoveryPlanExecuteCleanupEndTrap	このトラップは、リカバリ プランがテストのクリーンアップを終了するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、結果ステータス。
RecoveryPlanExecuteBeginTrap	このトラップは、リカバリ プランがリカバリを開始するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態。
RecoveryPlanExecuteEndTrap	このトラップは、リカバリ プランがリカバリを終了するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、結果ステータス。
RecoveryPlanExecuteReprotectBeginTrap	このトラップは、Site Recovery Manager がリカバリ プランの再保護ワークフローを開始するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態。
RecoveryPlanExecuteReprotectEndTrap	このトラップは、Site Recovery Manager がリカバリ プランの再保護ワークフローを終了したときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、結果ステータス。

表 13-11. SNMP トラップ（続き）

イベント	説明	原因
RecoveryVmBeginTrap	このトラップは、リカバリ プランが仮想マシンのリカバリを開始するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、仮想マシン名、仮想マシン UUID。
RecoveryVmEndTrap	このトラップは、リカバリ プランが仮想マシンのリカバリを終了したときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、仮想マシン名、仮想マシン UUID、結果ステータス。
RecoveryPlanServerCommandBeginTrap	このトラップは、リカバリ プランが Site Recovery Manager Server マシンでコマンド コールアウトの実行を開始するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、コマンド名。
RecoveryPlanServerCommandEndTrap	このトラップは、リカバリ プランが Site Recovery Manager Server マシンでコマンド コールアウトの実行を終了したときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、コマンド名、結果ステータス。
RecoveryPlanVmCommandBeginTrap	このトラップは、リカバリされる仮想マシンでリカバリ プランがコマンド コールアウトの実行を開始するときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、コマンド名、仮想マシン名、仮想マシン UUID。
RecoveryPlanVmCommandEndTrap	このトラップは、リカバリされる仮想マシンでリカバリ プランがコマンド コールアウトの実行を終了したときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、コマンド名、仮想マシン名、仮想マシン UUID、結果ステータス。
RecoveryPlanPromptDisplayTrap	このトラップは、続行前にリカバリ プランがユーザー入力を必要とするときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態、プロンプト文字列。
RecoveryPlanPromptResponseTrap	このトラップは、続行前にリカバリ プランがユーザー入力を必要としなくなったときに送信されます。	Site Recovery Manager のサイト名、リカバリ プラン名、リカバリ タイプ、実行状態。

# Site Recovery Manager ログ ファイルの収集

# 14

Site Recovery Manager の日常の実行中に発生する問題の原因を特定するには、内容を確認するか、または VMware サポートに送信するために Site Recovery Manager ログ ファイルを収集する必要があります。

Site Recovery Manager は、VMware サポートによる問題の診断に役立つ情報を含むいくつかのログ ファイルを作成します。Site Recovery Manager ログ コレクタを使用して、ログ ファイルの収集を簡素化できます。

Site Recovery Manager Server とクライアントは、異なるログ ファイルを使用します。

Site Recovery Manager Server ログ ファイルには、サーバ構成に関する情報とサーバの動作に関連するメッセージが含まれます。Site Recovery Manager Server ログ バンドルには、最新のリカバリ プランの実行のシステム情報と履歴レポートも含まれます。

Site Recovery Manager クライアント ログ ファイルには、クライアント構成に関する情報とクライアント プラグインの動作に関連するメッセージが含まれます。Site Recovery Manager のバンドルには、ログ ディレクトリのストレージ レプリケーション アダプタ (SRA) サブディレクトリのコンテンツとインストーラのログ ファイルも含まれます。

Site Recovery Manager システムの一部である vCenter Server インスタンスと ESXi Server インスタンスのログ ファイルには、Site Recovery Manager の問題を診断するときに役立つ情報が含まれていることもあります。

Site Recovery Manager ログ ファイルは、ファイルを収集または取得し、選択した場所に配置される Zip ファイルに圧縮します。

Site Recovery Manager の操作中に発生したエラーは、エラー ダイアログ ボックスまたは [最近のタスク] ウィンドウに表示されます。ほとんどのエラーでは、Site Recovery Manager ログ ファイルにもエントリが生成されます。リカバリ サイトと保護サイトで最近のタスクとログ ファイルを確認してください。

## Site Recovery Manager インターフェイスを使用する Site Recovery Manager ログ ファイルの収集

Site Recovery Manager ログは、ユーザーが指定した場所にダウンロードできます。

この情報を使用して、問題を理解し、解決してください。最善の結果を得るには、各サイトからログを収集してください。

### 手順

- 1 vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。

- 2 [Site Recovery] ホーム タブでサイトのペアを選択して、[詳細表示] をクリックします。
- 3 [サイト ペア] タブで、[サマリ] をクリックし、Site Recovery Manager ボックスの [名前] をクリックします。
- 4 サーバを選択し、[ログのエクスポート] をクリックします。
- 5 [ダウンロード] をクリックし、ログをダウンロードします。

## 手動での Site Recovery Manager ログ ファイルの収集

Site Recovery Manager Server ログ ファイルを手動で生成したログ バンドルにダウンロードできます。ログ ファイルを手動で収集するのは、vSphere Client にアクセスできない場合に便利です。

これらの手順で生成されるログのバンドルは、vSphere Client を使用して生成するログとまったく同じものです。

### 手順

- ◆ Site Recovery Manager ログ ファイルを収集するには、次のいずれかの方法を使用します。

タスク	操作
コマンド プロンプトを使用して、Site Recovery Manager Server Windows ホストマシンからログ バンドルを生成する	<ol style="list-style-type: none"> <li>a Site Recovery Manager Server ホストにログインし、コマンド プロンプトを開きます。</li> <li>b 作業ディレクトリを C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin に変更します。</li> <li>c 次のコマンドを実行します。cscript srm-support.wsf 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 ファイルが作成された月、日、年、時間、および分を示します。ログ バンドルはデフォルトでデスクトップに保存されます。</li> </ol>
[スタート] メニューを使用して、Site Recovery Manager Server Windows ホストマシンからログ バンドルを生成する	<ol style="list-style-type: none"> <li>a Site Recovery Manager Server ホストにログインします。</li> <li>b [スタート] - [プログラム] - [VMware] - [VMware Site Recovery Manager] - [VMware vCenter Site Recovery Manager ログ バンドルの生成] の順に選択します。</li> </ol>
Site Recovery Manager Appliance からログ バンドルを生成する	<ol style="list-style-type: none"> <li>a Site Recovery Manager Appliance ホスト マシンにログインして、コマンド プロンプトを開きます。</li> <li>b 作業ディレクトリを /opt/vmware/srm/bin/ に変更します。</li> <li>c 次のコマンドを実行します。 <ul style="list-style-type: none"> <li>■ 管理者ユーザーとしてログインしている場合：sudo ./srm-support-linux.sh</li> <li>■ root ユーザーとしてログインしている場合：./srm-support-linux.sh</li> </ul> </li> </ol>

## Site Recovery Manager Server ログ ファイルのサイズと数の変更

Site Recovery Manager Server ログ ファイルのサイズ、数、場所を変更できます。

Site Recovery Manager Server の vmware-dr.xml 構成ファイルで、Site Recovery Manager ログの設定を変更できます。



## 手順

1 Site Recovery Manager Server ホストにログインします。

2 テキスト エディタで vmware-dr.xml ファイルを開きます。

- Windows 版の Site Recovery Manager を使用している場合は、Site Recovery Manager Server ホスト マシンの C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config フォルダで vmware-dr.xml ファイルを検索します。
- Site Recovery Manager Virtual Appliance を使用している場合は、アプライアンスの /opt/vmware/srm/conf/ ディレクトリで vmware-dr.xml ファイルを検索します。

3 vmware-dr.xml ファイルの <log> セクションを探します。

4 保持するログの最大サイズをバイト単位で設定します。

ログの最大サイズを設定するには、<maxFileSize> セクションを <log> セクションに追加します。デフォルトは 10,485,760 バイトです。

```
<log>
  <maxFileSize>10485760</maxFileSize>
</log>
```

5 保持するログ ファイルの最大数を設定します。

ログの最大数を設定するには、<maxFileNum> セクションを <log> セクションに追加します。デフォルトのログ ファイル数は 20 個です。

```
<log>
  <maxFileNum>20</maxFileNum>
</log>
```

6 (オプション) <log> セクションの <directory> セクションを変更して、ログ ファイルを格納する Site Recovery Manager Server 上の場所を変更します。

**注：** ログ ファイルの場所を変更する場合は、新しいディレクトリに書き込むために必要な権限が Site Recovery Manager ユーザー アカウントにあることを確認する必要があります。

- Windows 版 Site Recovery Manager を使用している場合、ログのデフォルト パスは C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs です。
- Site Recovery Manager Appliance を使用している場合、ログ ファイルのデフォルトの場所は /var/log/vmware/srm です。

7 ログ ファイルのデフォルトのプリフィックスを変更します。

デフォルト プリフィックスを変更するには、<log> セクションの <name> セクションを変更します。

```
<log>
  <name>vmware-dr</name>
</log>
```

## 8 ログ レベルを変更します。

ログ レベルを変更するには、<log> セクションの <level> セクションを変更します。可能なログ レベルは、エラー、警告、情報、詳細、および最詳細です。レベルを最詳細に設定すると、パフォーマンスが大幅に低下します。

```
<log>
  <level>info</level>
</log>
```

## 9 (オプション) Site Recovery Manager Server コンポーネントのログ レベルを設定します。

該当する <level> セクションを変更すると、コンポーネントに特定のログ レベルを設定できます。たとえば、リカバリ コンポーネントのログ レベルを最詳細に設定できます。

```
<level id="Recovery">
  <logName>Recovery</logName>
  <logLevel>trivia</logLevel>
</level>
```

## 10 (オプション) ストレージ レプリケーション アダプタのログ レベルを設定します。

Site Recovery Manager ログ レベルを設定しても、SRA のログ レベルは設定されません。SRA ログ レベルを変更するには、<level id="SraCommand"> セクションを vmware-dr.xml に追加して SRA ログ レベルを設定します。

```
<level id="SraCommand">
  <logName>SraCommand</logName>
  <logLevel>trivia</logLevel>
</level>
```

## 11 Site Recovery Manager Server サービスを再開して変更を有効にします。

# Site Recovery Manager コア ダンプの構成

Site Recovery Manager のコア ダンプ設定を構成してコア ダンプ ファイルの場所を変更し、ファイルを圧縮することができます。

Site Recovery Manager コア ダンプの設定は Site Recovery Manager Server の vmware-dr.xml 構成ファイルで変更できます。

### 手順

#### 1 Site Recovery Manager Server ホストにログインします。

#### 2 テキスト エディタで vmware-dr.xml ファイルを開きます。

- Windows 版の Site Recovery Manager を使用している場合は、Site Recovery Manager Server ホスト マシンの C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config フォルダで vmware-dr.xml ファイルを検索します。

- Site Recovery Manager Virtual Appliance を使用している場合は、アプライアンスの `/opt/vmware/srm/conf/` ディレクトリで `vmware-dr.xml` ファイルを検索します。
- 3 `vmware-dr.xml` ファイルの `<coreDump>` セクションを変更してコア ダンプを格納する Site Recovery Manager Server 上の場所を変更します。

**注：** コア ダンプ ファイルの場所を変更する場合は、新しいディレクトリに書き込むために必要な権限が Site Recovery Manager ユーザー アカウントにあることを確認する必要があります。

- Windows 版の Site Recovery Manager を使用している場合、コア ダンプのデフォルト パスは `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles` です。ただし、この場所がないか、または書き込み可能でない場合は除きます。デフォルトのパスが使用できない場合、Site Recovery Manager Server では `C:\ProgramData\VMware` が使用されます。
  - Site Recovery Manager Appliance を使用している場合、コア ダンプのデフォルトの場所は `/var/log/vmware/srm/DumpFiles` です。
- 4 コアダンプのシステム パラメータを使用して作成および圧縮されるダンプ ファイルの数を制限します。

```
<debug>
  <dumpCoreCompression>true,false</dumpCoreCompression>
  <dumpFullCore>true,false</dumpFullCore>
</debug>
```

パラメータ	説明
<code>dumpCoreCompression</code>	指定しない場合、デフォルトの値は <code>false</code> になります。Site Recovery Manager Server は、コア ダンプ ファイルの作成中に前のコア ダンプ ファイルを圧縮しません。 <code>true</code> を指定すると、Site Recovery Manager Server は新しいコア ダンプの作成時にすべての古いコア ダンプを圧縮します。
<code>dumpFullCore</code>	指定しない場合、デフォルトの値は <code>false</code> になります。Site Recovery Manager Server が数 MB のコア ダンプ ファイルを生成します。これは、問題が発生したときのサポートのヒントになります。この値を <code>true</code> に設定すると、Site Recovery Manager Server は、コア ダンプ発生時のワークロードに応じてサイズが数 GB になることがある、完全なコア ダンプ ファイルを生成します。この大きいファイルは、問題が発生したときのサポートに役立ちます。ディスク容量に余裕がある場合は、この値を <code>true</code> に設定します。

- 5 コア ダンプ ファイルの最大数を変更するには、`<debug>` セクションに行を追加します。

```
<maxCoreDumpFiles>max_files</maxCoreDumpFiles>
```

指定しない場合、デフォルトの値は 4 です。この値で、コア ダンプ ディレクトリ内に保持するコア ダンプ ファイルの最大数を指定します。Site Recovery Manager Server がコア ダンプを作成すると、`dumpFullCore` が `true` の場合は特に、Site Recovery Manager Server は必要に応じて古いファイルを削除し、ファイルが最大数を超過してディスク領域を消費しすぎないようにします。

# Site Recovery Manager のトラブルシューティング

# 15

保護グループやリカバリ プランの作成、リカバリ、またはゲストのカスタマイズで問題がある場合は、その問題のトラブルシューティングが可能です。

問題の原因をお探しの場合は、VMware ナレッジベース (<http://kb.vmware.com/>) もぜひご確認ください。

## リカバリ サイトで多数の仮想マシンを同時にパワーオンするとエラーが起こる場合がある

多数の仮想マシンで同時に起動操作を実行すると、アレイ ベースのリカバリまたは vSphere Replication のリカバリ時にエラーが起こる場合があります。

### 問題

リカバリ サイトで多数の仮想マシンを同時にパワーオンすると、リカバリの履歴レポートに次のエラーが表示される場合があります。

- コマンド 'echo "Starting IP customization on Windows ..." > > %VMware\_GuestOp\_OutputFile%。
- カスタマイズを完了できません。スクリプト作成のランタイム エラーまたは無効なスクリプト パラメータが原因の可能性があります。
- ゲスト仮想マシンへのファイルのアップロード時にエラーが発生しました。
- VMware Tools を 600 秒間待機した後にタイムアウトになりました。

### 原因

デフォルトでは、Site Recovery Manager では同時にパワーオン操作を実行できる数が制限されていません。リカバリ サイトで仮想マシンをパワーオンするときにエラーが発生する場合、vmware-dr.xml ファイルを変更して、同時にパワーオンする仮想マシンの数に制限を設けることができます。

これらのエラーが発生する場合は、スタンドアローン ホストまたはクラスタの使用環境の容量に合わせてリカバリ サイトでのパワーオン操作の数を制限します。

### 解決方法

- 1 Site Recovery Manager Server ホストにログインします。

## 2 テキスト エディタで vmware-dr.xml ファイルを開きます。

- Windows 版の Site Recovery Manager を使用している場合は、Site Recovery Manager Server ホスト マシンの C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config フォルダで vmware-dr.xml ファイルを検索します。
- Site Recovery Manager Virtual Appliance を使用している場合は、アプライアンスの /opt/vmware/srm/conf/ ディレクトリで vmware-dr.xml ファイルを検索します。

## 3 defaultMaxBootAndShutdownOpsPerCluster と defaultMaxBootAndShutdownOpsPerHost の値を更新して、リカバリ サイトでのパワーオン操作の数を制限します。

次の例は、パワーオン操作の数をクラスタごとに最大 32、スタンドアローン ホストごとに最大 4 に制限する方法を示しています。

```
<config>
  <defaultMaxBootAndShutdownOpsPerCluster>32</defaultMaxBootAndShutdownOpsPerCluster>
  <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
</config>
```

## 4 Site Recovery Manager サーバ サービスを再起動します。

# 仮想マシンの保護グループへの追加が未解決のデバイス エラーにより失敗する

仮想マシンのデバイスをマップしていない場合に、仮想マシンの保護グループへの追加がエラーで失敗します。

### 問題

仮想マシンを保護グループに追加するときに、「未解決のデバイスが原因で仮想マシン「*virtual machine name*」を保護できません」というエラーが表示されます。

### 原因

保護サイトにある仮想マシンのデバイスをリカバリ サイトの対応するデバイスにマップしませんでした。

### 解決方法

仮想マシンの保護設定を[アレイベース保護グループ](#)または [vSphere Replication 保護グループ](#)内の仮想マシンの[設定の変更](#)の説明に従って構成してください。

# 保護の構成がプレースホルダの作成エラーにより失敗する

複数の仮想マシンの保護を構成した場合、プレースホルダの作成エラーにより構成が失敗します。

### 問題

同時に多数の仮想マシンの保護を構成すると、次のプレースホルダ作成タイムアウト エラーまたはプレースホルダ作成命名エラーにより失敗します。

- プレースホルダ仮想マシン作成エラー: 操作がタイムアウトしました: 300 秒

- プレースホルダ仮想マシン作成エラー:「`placeholder_name`」という名前はすでに存在しています

この問題は、次のようないくつかの方法で保護を構成したときに発生します。

- 多数の仮想マシンが含まれる 1 つ以上のデータストアを含む保護グループを作成する。
- 多数の仮想マシンの Site Recovery Manager インターフェイスで [保護グループ] - [仮想マシン] - [すべてリストア] オプションを使用する。
- Site Recovery Manager API を使用して多数の仮想マシンを手動で保護する。

#### 原因

リカバリ サイトのインフラストラクチャが、プレースホルダ仮想マシンの同時作成量を処理できません。

#### 解決方法

`replication.placeholderVmCreationTimeout` 設定をデフォルトの 300 秒より大きい値に変更します。[レプリケーション設定の変更](#)を参照してください。

この設定の変更に Site Recovery Manager Server を再起動する必要はありません。Site Recovery Manager によって、仮想マシンの保護を次回構成したときに設定が適用されます。

## プレースホルダを短い時間内に削除し、再作成を行うと失敗する

データストアからすべてのプレースホルダ仮想マシンを削除し、データストアをアンマウントしてから、データストアの再マウントを行うと、プレースホルダ仮想マシン再作成に失敗する場合があります。

#### 問題

データストアのアンマウント後にすぐプレースホルダを再作成すると、エラー `NoCompatibleHostFound` で失敗する可能性があります。

#### 原因

ESXi ホストとデータストア間の関連付けは、10 分間隔で更新されます。データストアをアンマウントしてから再マウントして、次の更新の前にプレースホルダを再作成すると、ホストが見つかりません。

#### 解決方法

プレースホルダ仮想マシンを再作成するには、データストアをアンマウントして再マウントしてから 10 分以上待機します。

## ホストが不正な状態にあるため計画移行が失敗する

計画移行中にリカバリ サイトの ESXi ホストをメンテナンス モードにすると、計画移行が失敗します。

#### 問題

計画移行がエラー「エラー: その操作は、ホストの現在の状態では実行できません。」により失敗する。

## 原因

リカバリ サイトの ESXi ホストがメンテナンス モードの場合、Site Recovery Manager はリカバリ サイトの仮想マシンをパワーオンできません。

## 解決方法

リカバリ サイトの ESXi ホストのメンテナンス モードを終了し、計画移行を再実行します。

# ストレージ ポリシー保護グループを同期できなかったために、計画移行に失敗する

ストレージ ポリシー保護グループを含むリカバリ プランの計画移行を実行すると、保護グループに対する変更の同期が完了していないために、リカバリ プランが失敗します。

## 問題

ストレージ ポリシー保護グループを含むリカバリ プランの計画移行を実行すると、「ピア サイトは保護グループへの変更の同期を完了していません」というエラー メッセージが表示されます。

## 原因

ストレージ ポリシー保護グループを含むリカバリ プランの計画移行を実行する際、Site Recovery Manager は、リカバリ プランを実行する前に、保護サイトとリカバリ サイトの両方で保護グループが同期されているかどうかを確認します。

保護グループが両方のサイトで同期されている場合は、計画移行が開始されます。保護グループが両方のサイトで同期されていない場合は、エラー メッセージが表示されます。

## 解決方法

- 1 エラー メッセージを閉じて、再度、[終了] をクリックします。
- 2 (オプション) エラーが解消されない場合は、計画移行をキャンセルし、しばらく待ってから計画移行を改めて実行します。

# 一部の仮想マシンでネットワークのカスタマイズ時にタイムアウトエラーによりリカバリが失敗する

復旧時に、一部の仮想マシンが復旧せず、ネットワークのカスタマイズ時にタイムアウト エラーが発生します。

## 問題

リカバリ時に、一部の仮想マシンがデフォルトのタイムアウト期間である 120 秒以内にリカバリしません。

## 原因

この問題は、次のいずれかの理由で発生する場合があります。

- VMware Tools パッケージが復旧する仮想マシンにインストールされていない。

- 複数の仮想マシンを同時にリカバリしようとする、リカバリ サイトのクラスタのリソース使用量が多くなる。この場合、特定のタイムアウト設定の値を増やしてタスクの完了までの時間を延長できます。[リカバリ設定の変更](#) を参照してください。

#### 解決方法

- 1 VMware Tools パッケージが復旧する仮想マシンにインストールされていることを確認します。
- 2 リカバリ サイトで利用できる容量を確認します。

リカバリ サイトのリソース使用量が多くなっている場合は、ゲスト カスタマイズのタイムアウト期間を延長するとこの問題を解決できます。

  - a vSphere Client または vSphere Web Client で、[Site Recovery] - [Site Recovery を開く] の順にクリックします。
  - b Site Recovery の [ホーム] タブで、サイト ペアを選択し、[詳細表示] をクリックします。
  - c 左側のペインで [構成] - [詳細設定] - [リカバリ] の順にクリックします。
  - d サイトを選択し、[編集] をクリックして、リカバリ サイトの設定を変更します。
  - e `recovery.customizationTimeout` パラメータをデフォルトの 600 秒から増やします。
  - f `recovery.powerOnTimeout` パラメータをデフォルトの 300 秒から増やします。
- 3 復旧を再度実行します。

## リカバリが利用できないホストまたはデータストアのエラーで失敗する

vCenter Server インベントリに変更が加えられた直後にリカバリまたはテスト リカバリを実行すると、ホスト ハードウェアとデータストアが使用できないエラーによりリカバリまたはテスト リカバリが失敗します。

#### 問題

「ハードウェア バージョンが「7」、データストアが「ds\_id」で、パワーオンされていてメンテナンス モードではないホストは利用できません...」というエラーでリカバリまたはテスト リカバリが失敗します。

#### 原因

Site Recovery Manager Server はホスト インベントリ状態のキャッシュを保持します。インベントリに最新の変更が加えられた場合、たとえばホストがアクセス不能になった場合、切断された場合、または一部のデータストアへの接続が途切れた場合、Site Recovery Manager Server はキャッシュを更新するのに最大 15 分を必要とする可能性があります。Site Recovery Manager Server のキャッシュに誤ったホスト インベントリ状態がある場合は、リカバリまたはテスト リカバリが失敗することがあります。

#### 解決方法

ホストのインベントリに変更を加えた場合は、15 分待ってから、リカバリを実行します。このエラーが再度表示される場合は、15 分待ってから、リカバリを再実行します。



## 再保護が vSphere Replication のタイムアウト エラーで失敗する

vSphere Replication 保護グループを含むリカバリ プランに再保護を実行すると、操作がエラーでタイムアウトになります。

### 問題

vSphere Replication 保護グループを含むリカバリ プランの再保護操作は、エラー「Operation timed out: 7200 seconds VR synchronization failed for VRM group <Unavailable>. Operation timed out: 7200 seconds.」で失敗する。

### 原因

再保護を実行すると、Site Recovery Manager は vSphere Replication の保護グループへのオンライン同期を実行します。これによって操作のタイムアウトが発生する可能性があります。デフォルト タイムアウト値は 2 時間で、使用している同期タイムアウトの間隔（4 時間）に対応します。

### 解決方法

[詳細設定] で `vrReplication.synchronizationTimeout` と `vrReplication.reverseReplicationTimeout` のタイムアウト値を増やします。 [vSphere Replication 設定の変更](#) を参照してください。

## VMware Tools の待機中にリカバリ プランがタイムアウトする

リカバリ プランの実行が、VMware Tools の起動待機中にタイムアウト エラーにより失敗します。

### 問題

リカバリ プランの仮想マシンのシャットダウン ステップまたは VMware Tools の待機ステップでリカバリ操作が失敗します。

### 原因

Site Recovery Manager では、リカバリされた仮想マシンがリカバリ サイトで実行中の場合は検出に VMware Tools ハートビートが使用されます。リカバリ操作には、保護された仮想マシンに VMware Tools がインストールされている必要があります。保護された仮想マシンに VMware Tools がインストールされていない場合、または VMware Tools の起動を待ってから Site Recovery Manager を起動するように構成している場合、リカバリが失敗します。

### 解決方法

保護された仮想マシンに VMware Tools をインストールします。保護対象の仮想マシンに VMware Tools をインストールしない、またはできない場合には、リカバリした仮想マシンで VMware Tools が起動するのを待機せずにゲスト OS のシャットダウンのステップをスキップするように Site Recovery Manager を構成する必要があります。 [リカバリ設定の変更](#) を参照してください。

## vSphere Replication 保護グループの同期の失敗

vSphere Replication 保護グループを含むテスト リカバリ、計画移行、およびリカバリ プランの再保護中に、仮想マシンの同期手順がエラーにより失敗します。

### 問題

vSphere Replication 保護グループの仮想マシンの同期が、「エラー - VRM グループ <使用不可> の VR 同期が失敗しました。オブジェクトがすでに削除されているか、オブジェクトの作成が完了していません」というエラー メッセージが表示されて失敗します。

### 原因

保護グループ内の 1 つ以上の仮想マシンの過剰な I/O トラフィックにより、同期が終了する前にタイムアウトすることがあります。これはトラフィックが過剰なために発生することがあります。たとえば、ログ レベルを最詳細モードに設定すると、過剰な I/O トラフィックが発生することがあります。

### 解決方法

- 1 Site Recovery Manager Server ホストにログインします。
- 2 テキスト エディタで vmware-dr.xml ファイルを開きます。
  - Windows 版の Site Recovery Manager を使用している場合は、Site Recovery Manager Server ホスト マシンの C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config フォルダで vmware-dr.xml ファイルを検索します。
  - Site Recovery Manager Virtual Appliance を使用している場合は、アプライアンスの /opt/vmware/srm/conf/ ディレクトリで vmware-dr.xml ファイルを検索します。
- 3 <topology><drTaskCleanupTime> 要素を vmware-dr.xml ファイルに追加します。  
 <topology> 要素は、<Config> タグの最上位レベルの任意の場所に追加できます。<drTaskCleanupTime> 値を少なくとも 300 秒に設定します。ログ レベルを最詳細に設定する場合は、<drTaskCleanupTime> を 1000 秒に設定します。
 

```
<topology>
  <drTaskCleanupTime>1000</drTaskCleanupTime>
</topology>
```
- 4 vmware-dr.xml ファイルを保存して閉じます。
- 5 Site Recovery Manager Server サービスを再起動して新しい設定を適用します。

## データストアの再スキャンがストレージ デバイスの準備ができていないため失敗する

テスト リカバリまたはリカバリを開始するときに、一部の SRA は ESXi ホストでリカバリ サイトの昇格ストレージ デバイスが使用可能になる前に、応答を Site Recovery Manager に送信します。Site Recovery Manager はストレージ デバイスを再スキャンし、再スキャンが失敗します。

## 問題

ストレージ デバイスの準備がまだ完了していないと、ESXi Server ではこれらのデバイスが検出されず、Site Recovery Manager では、再スキャンするときにレプリケートされたデバイスが検出されません。これによりいくつかの問題が発生する可能性があります。

- データストアは作成されず、リカバリされた仮想マシンは見つかりません。
- ESXi ホストが vCenter Server ハートビートに応答なくなり、vCenter Server から切断されます。この場合、vCenter Server から Site Recovery Manager にエラーが送信され、テスト リカバリまたは実際のリカバリが失敗します。
- ESXi ホストは使用できますが、再スキャンとディスク再署名が Site Recovery Manager または vCenter Server のタイムアウトを超えるため、Site Recovery Manager エラーになります。

## 原因

Site Recovery Manager が再スキャンを開始するときにストレージ デバイスが準備できていません。

## 解決方法

ストレージ デバイスが ESXi ホストで使用可能になるまでストレージ再スキャンの開始を遅らせるには、`storageProvider.hostRescanDelaySec` 設定の値を 20 ～ 180 秒に増やします。[ストレージ プロバイダ設定の変更](#)を参照してください。

---

**注：** Site Recovery Manager 5.1 以前では、`storageProvider.hostRescanRepeatCnt` パラメータを使用してリカバリの遅延を設定している可能性があります。その代わりに、`storageProvider.hostRescanDelaySec` パラメータを使用してください。

---

# 計画移行中にリカバリが 36% で停止する

計画移行中に保護サイト上の Site Recovery Manager サービスを停止すると、処理が 36% の位置で停止します。

## 問題

計画移行中に保護サイトの Site Recovery Manager サービスを停止すると、ステップ 15 [保護サイトのストレージのアンマウント] に進んだ時点で、ワークフローが（正常に終了するのではなく）36% の位置に留まったままになることがあります。

## 解決方法

[キャンセル] をクリックしてワークフローをキャンセルし、ワークフローをもう一度実行します。

# レプリケートされていない構成ファイルに関するエラーが発生して処理が失敗する

リカバリ操作または再保護操作を双方向で同時に実行している場合に、レプリケートされていない仮想マシンの構成ファイルに関するエラーが発生して処理が失敗します。

## 問題

アレイベース レプリケーション保護グループまたはストレージ ポリシー保護グループを含む複数のリカバリ プランを同時に実行する場合を考えます。このとき、一部の処理がサイト A からサイト B に対して実行され、他のいくつかの処理がサイト B からサイト A に対して実行されると、「仮想マシン「`virtual_machine_name`」は、構成ファイル「`virtual_machine_config_file.vmx`」が複製されていないデータストアか保護されていないデータストア上にあるため保護できません。」というエラーが表示されて、プランの一部またはすべてが失敗します。

## 原因

この問題は、あるサイト上で行われるデータストアの計算が、逆の方向で実行中のリカバリ処理によって遅延することが原因で発生することが考えられます。

## 解決方法

いくつかの処理が完了するのを待ってから、失敗したリカバリ プランの処理を再実行します。または、同じ方向の計画移行をすべて一緒に実行します。片方向の処理が終了したら、逆方向の計画移行を実行します。

# 制限されたユーザー権限によってリカバリが失敗する

Site Recovery Manager ソリューション ユーザーに IP カスタマイズまたはゲスト OS 内の呼び出し操作を実行する権限がない場合、リカバリ プロセス中にエラーが発生することがあります。

## 問題

Site Recovery Manager ソリューション ユーザーにリカバリする仮想マシンのゲスト OS に対する適切な権限がない場合、リカバリ プロセス中に次のいずれかのエラー メッセージが表示されることがあります。

```
GuestPermissionDenied
```

```
CannotAccessFile
```

## 原因

この問題は、Site Recovery Manager ソリューション ユーザーがゲスト OS のファイルにアクセスする権限またはコマンドを実行する権限を持たないゲスト OS ユーザーにマッピングされている場合に発生します。

## 解決方法

- 1 Site Recovery Manager を使用してゲスト ユーザー マッピングを構成する場合は、VMware Tools サービスを実行するゲスト OS ユーザーにファイルにアクセスする権限またはコマンドを実行する権限があることを確認します。  
  
ゲスト ユーザー マッピングの自動構成を有効または無効にする方法については、[リカバリ設定の変更](#)を参照してください。
- 2 (オプション) ゲスト ユーザー マッピングを手動で構成する場合は、リカバリ サイトにローカルな Site Recovery Manager ソリューション ユーザーを適切な権限を保有するゲスト OS ユーザーにマッピングします。
- 3 リカバリ プランを再実行します。

## サポートされていない VMware Tools と ESXi の組み合わせによってリカバリが失敗する

仮想マシンにインストールされている VMware Tools のバージョンとリカバリ サイトの ESXi ホストのバージョンが Site Recovery Manager と互換性がない場合、リカバリ プロセスが失敗することがあります。

### 問題

リカバリ プロセス中に次のエラーが表示されることがあります。

```
OperationNotSupportedByGuest
```

### 原因

この問題は、VMware Tools と ESXi の互換性のないバージョンを使用すると発生することがあります。Site Recovery Manager、VMware Tools、および ESXi の間の互換性については、Site Recovery Manager 8.2 の互換性マトリックスを参照してください。

### 解決方法

- ◆ VMware Tools と ESXi のバージョンが Site Recovery Manager と互換性があることを確認します。