IBM Spectrum Protect for Virtual Environments
バージョン 8.1.10

Data Protection for VMware インストール・ガイド

お願い

本書および本書で紹介する製品をご使用になる前に、121 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM Spectrum Protect for Virtual Environments バージョン 8、リリース 1、モディフィケーション 10 (製品番号 5725-X00)、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに 適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典：
IBM Spectrum Protect for Virtual Environments
Version 8.1.10
Data Protection for VMware Installation Guide

発行：
日本アイ・ビー・エム株式会社

担当：
トランスレーション・サービス・センター

目次

本書について v
本書の対象読者 v
資料 v

新機能 vii

第 1 章 Data Protection for VMware のインストールおよびアップグレード 1
インストール可能コンポーネント 1
Data Protection for VMware vSphere GUI 3
IBM Spectrum Protect Recovery Agent 5
IBM Spectrum Protect vSphere Client プラグイン 6
Data Protection for VMware コマンド・ライン・インターフェース 6
IBM Spectrum Protect ファイル・リストア・インターフェース 7
データ・ムーバー機能 7
Data Protection for VMware のインストール計画 9
インストール・ロードマップ 9
インストールのシナリオ 10
システム要件 11
Data Protection for VMware コンポーネントのインストール 20
Data Protection for VMware インストール・パッケージの入手 20
インストール・ウィザードを使用した Data Protection for VMware コンポーネントのインストール 21
サイレント・モードでの Data Protection for VMware コンポーネントのインストール 24
インストール後の最初のステップの実行 26
Data Protection for VMware のアップグレード 28
Data Protection for VMware のアップグレード 28
サイレント・モードの Windows 64 ビット・システムでの Data Protection for VMware のアップグレード 29
サイレント・モードの Linux システムでの Data Protection for VMware のアップグレード 30
vCenter サーバーの Linked Mode 環境での Data Protection for VMware のアップグレード 31
Data Protection for VMware のアンインストール 31
Windows への Data Protection for VMware のアンインストール 31
Windows 用 Data Protection for VMware のサイレント・モードでのアンインストール 33
Linux システムの Data Protection for VMware のアンインストール 34
既存の Data Protection for VMware インストール環境の変更 36
既存の Data Protection for VMware インストール環境のパッケージの変更 36
既存の Data Protection for VMware インストール環境の機能の変更 37

第 2 章 Data Protection for VMware の構成 39
Windows でのウィザードを使用した新規インストールの構成 39
Linux でのウィザードを使用した新規インストールの構成 40
マルチサーバー環境の構成 41
デフォルトのバックアップ・サーバーの構成 41
追加のバックアップ・サーバーの構成 42
追加のバックアップ・サーバーでのスケジュールの 作成 43
随時バックアップの実行 43
随時リストア操作の実行 44
ノートブックを使用した、既存のインストール済み環境の編集 44
環境でファイル・リストア操作を使用可能にする 45
Linux でのファイル・リストア操作のセットアップ 46

ファイル・リストア操作のオプションの変更 47
ファイル・リストア・オプション 47
ファイル・リストア操作のログ・アクティビティーの 構成 48
ファイル・リストア・ログ・アクティビティー ・オプション 49
タグ付けサポートのためのデータ・ムーバー・ノードの構成 50
仮想マシン全体のインスタント・リストア操作のための環境の構成 53
1. iSCSI ソフトウェアを ESXi ホストで構成する 53
2. データ・ムーバーへのアプリケーションのインストールと構成 53
3. Recovery Agent 接続の設定 54
4. ESXi ホストおよびデータ・ムーバーの専用の iSCSI ネットワークの構成 54
Data Protection for VMware のセキュリティー設定の構成 56
データ・ムーバーと VMCLI のノードを IBM Spectrum Protect サーバー に接続するためのセキュリティー設定の構成 56
Transport Layer Security を使用した Data Protection for VMware vSphere GUI 通信の構成 60
VMware vCenter Server ユーザー特権の要件 66
Data Protection for VMware vSphere GUI のユーザーの役割 68
Data Protection for VMware GUI 登録キー 70
recovery agent GUI の構成 71
recovery agent から IBM Spectrum Protect サーバーへのセキュア通信の使用可能化 75
ロケール設定 78
ログ・ファイル関連のアクティビティー 79
Data Protection for VMware のサービスの開始と実行 81

付録 A 拡張構成タスク 83
vSphere 環境での IBM Spectrum Protect ノードのセットアップ 83
vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ 85
vSphere 環境でのデータ・ムーバー・ノードの手動でのセットアップ 86
Windows データ・ムーバー・ノードのセットアップ 87
Linux データ・ムーバー・ノードのセットアップ 89
vSphere 環境での Data Protection for VMware コマンド・ライン・インターフェースの構成 93
vSphere 環境のコマンド・ライン・インターフェース 構成のチェックリスト 95
テープ構成のガイドライン 98
Linux システム上の iSCSI 装置の手動構成 100
Windows システム上の iSCSI 装置の手動構成 103
Linux システム上のマウント・プロキシー・ノードの手動構成 104
リモート Windows システム上のマウント・プロキシー・ノードの手動構成 106
リモート Windows システムの 2 次サーバーでのファイル・リストア機能の手動構成 108
Linux システムでの複数のクライアント・アクセプター・サービスの手動構成 110
VMCLI 構成ファイルの変更 112

付録 B 増分永久増分バックアップ戦略へのマイグレーション 115

付録 C アクセシビリティー 119

特記事項 121
用語集 125

索引 127

本書について

IBM Spectrum Protect for Virtual Environments は、オフホストのブロック・レベルの増分バックアップと、Windows および Linux のゲスト・マシン用のフル VM バックアップからのファイル・リカバリーと Instant Restore を提供します。ブロック・レベルの増分バックアップが使用可能になるのは、IBM Spectrum Protect for Virtual Environments を IBM Spectrum® Protect データ・ムーバーと一緒に使用する場合です。

本書の対象読者

本書は、IBM Spectrum Protect for Virtual Environments をインストールおよび構成するユーザーおよび管理者を対象としています。

「*IBM Spectrum Protect for Virtual Environments: Data Protection for VMware* ユーザーズ・ガイド」には、概要情報、ユーザー・タスク、バックアップおよびリストアのシナリオ、コマンド解説書、およびエラー・メッセージが記載されています。

資料

IBM Spectrum Protect 製品ファミリーには、IBM Spectrum Protect Plus、IBM Spectrum Protect for Virtual Environments、IBM Spectrum Protect for Databases、および IBM® のその他のいくつかのストレージ管理製品が含まれます。

IBM 製品資料を確認するには、IBM Knowledge Center を参照してください。

バージョン 8.1.10 の新機能

IBM Spectrum Protect for Virtual Environments バージョン 8.1.10 では、問題と APAR に対応する更新が導入されました。

このリリースおよび直前のバージョン 8 リリースでの新機能と更新のリストについては、Data Protection for VMware の更新を参照してください。

資料に変更が加えられた場合、余白に垂直バー (|) を付けて表示しています。

第 1 章 Data Protection for VMware のインストールおよびアップグレード

IBM Spectrum Protect for Virtual Environments のインストールには、計画立案、インストール、および初期構成が含まれます。

インストール可能コンポーネント

Data Protection for VMware には、仮想環境を保護するためにインストールできるいくつかのコンポーネントが含まれています。

コンポーネントの可用性は、オペレーティング・システム環境によって異なります。ご使用の環境で使用可能なコンポーネントを判別するには、以下の表を確認してください。

Windows および Linux では、すべてのインストール場所が固定の場所になります。Windows での場所は以下の表に示します。Linux の場合: Spectrum Protect for VE コンポーネントは `/opt/tivoli/tsm/tdpvmware` にインストールされます。Linux Spectrum Protect バックアップ/アーカイブ API およびクライアントは、VE インストーラーによって固定の場所 (`/opt/tivoli/tsm/client/api` および `/opt/tivoli/tsm/client/ba`) にインストールされます。

各インストール・パッケージでは、エンド・ユーザーのご使用条件が提示されます。このご使用条件に同意しない場合、インストール・プロセスは停止します。

表 *1.* オペレーティング・システム別に使用可能な *Data Protection for VMware* コンポーネント

コンポーネント	Linux®	Windows
IBM Spectrum Protect Recovery Agent このコンポーネントは、仮想マウント機能とインスタント・リストア機能を提供します。 Windows の固定インストール場所: `C:\Program Files\Tivoli\TSM\RecoveryAgent`		√
Recovery Agent コマンド・ライン・インターフェース コマンド・ライン・インターフェースは、マウント操作に使用されます。 Windows の固定インストール場所: `C:\Program Files\IBM\SpectrumProtect\Framework`		√
資料 README ファイルおよび NOTICES ファイルを含む資料。	√	√
Data Protection for VMware 使用可能化ファイル このコンポーネントにより、IBM Spectrum Protect Data Protection for VMware は以下のバックアップ・タイプを実行することができます。 • 永久増分の増分バックアップ • 永久増分フルバックアップ このコンポーネントは、アプリケーション保護のために必要です。バックアップ作業負荷をオフロードする場合は、このファイルを vStorage バックアップ・サーバーにインストールする必要があります。	√	√

表 1. オペレーティング・システム別に使用可能な *Data Protection for VMware* コンポーネント (続き)

コンポーネント	Linux®	Windows
Data Protection for VMware vSphere GUI このコンポーネントは、VMware vCenter Server 上の VM データにアクセスするグラフィカル・ユーザー・インターフェース (GUI) です。GUI のコンテンツはこれらのビューで参照可能です。 • Web ブラウザー・ビュー。 このビューには、GUI Web サーバー・ホストの URL を使用してサポート対象の Web ブラウザーでアクセスします。 例えば、次のようにします。 `https://guihost.mycompany.com:9081/TsmVMwareUI/` • IBM Spectrum Protect vSphere Client プラグイン ビュー。このビューは VMware vSphere Web Client からアクセスできます。このビューのパネルは、vSphere Web クライアント内に組み込むために独自の設計になっていますが、このビューのデータおよびコマンドは、他のビューと同じ GUI Web サーバーから取得されます。IBM Spectrum Protect vSphere Client プラグインは、Web ブラウザーのビューで使用可能な機能のサブセット、およびいくつかの追加機能を提供します。	√	√
ファイル・リストア GUI このコンポーネントは Web ベースの GUI です。ユーザーは、これを使用することで、管理者の支援を受けずに VMware 仮想マシンのバックアップからファイルをリストアすることができます。この GUI は、 Data Protection for VMware GUI がインストールされると自動的にインストールされます。 これは、構成ウィザードによって使用可能に設定できます。	√	√
データ・ムーバー IBM Spectrum Protect Data Protection for VMware データ・ムーバーは、Data Protection for VMware のデータを移動するコンポーネントです。データ・ムーバーは、仮想環境から IBM Spectrum Protect バックアップ・サーバーにデータを移動します。サーバーにデータ・ムーバーをインストールすると、 そのサーバーを vStorage バックアップ・サーバーとして使用できるようになります。データ・ムーバーは、Data Protection for VMware と同じシステムにも、別のサーバーにもインストールできます。 Windows の固定インストール場所: `C:\Program Files\Tivoli\TSM\baclient`	√	√

Windows では、JVM は `C:\Program Files\Common Files\Tivoli\TSM\jvmNNNNNN` にインストールされます。ここで、`NNNNNN` は JVM バージョン番号 (例: `JVM80516`) です。Web サーバーは `C:\IBM\SpectrumProtect\webserver` にインストールされます。

Data Protection for VMware V8.1.8 以降では、TSM4VE パッケージの Framework コンポーネントおよび DP for VMware コンポーネントの場所を変更することはできなくなりました。 デフォルトの場所は `C:\Program Files\IBM\SpectrumProtect` です。

- Framework - `C:\Program Files\IBM\SpectrumProtect\Framework`: FLR、Derby、vmcli、 および tsmcli の各ファイル。
- DP for VMware - `C:\Program Files\IBM\SpectrumProtect\DPVMware`: vmgui ファイル。

1. ファイル・リストア・インターフェース・コンポーネントは、Windows システムにインストールされて使用可能にされている必要がありますが、このインターフェースを 使用して、Windows および Linux 両方のゲスト仮想マシン上のファイルをリストアすることができます。
2. Data Protection for VMware をインストールした場合、データ・ムーバーはインストールに組み込まれています。

Data Protection for VMware は、バックアップ作業負荷を VM から vStorage バックアップ・サーバーにオフロードします。このタスクを完了するには、データ・ムーバーが vStorage バックアップ・サーバーにインストールされている必要があります。

Data Protection for VMware vSphere GUI

Data Protection for VMware vSphere GUI (vSphere GUI) コンポーネントは、 VMware vCenter Server 上の VM データにアクセスするグラフィカル・ユーザー・インターフェースです。

概要

Data Protection for VMware vSphere GUI は、以下のタスクを実行するための基本インターフェースです。

- VM の IBM Spectrum Protect サーバーへのバックアップを開始またはスケジュールします。
- IBM Spectrum Protect サーバーから VM のフルリカバリーを開始します。
- タスクの進行状況、完了した最新のイベント、バックアップ状況、およびスペース使用量に関するレポートを発行します。この情報は、バックアップ処理で発生したエラーのトラブルシューティングに 役立つ場合があります。

ヒント: vSphere GUI を使用してタスクを実行する方法に関する情報は、GUI と一緒にインストールされるオンライン・ヘルプで提供されています。各 GUI ウィンドウの「**詳細情報**」をクリックすると、タスク・アシスタンスのオンライン ・ヘルプが開きます。

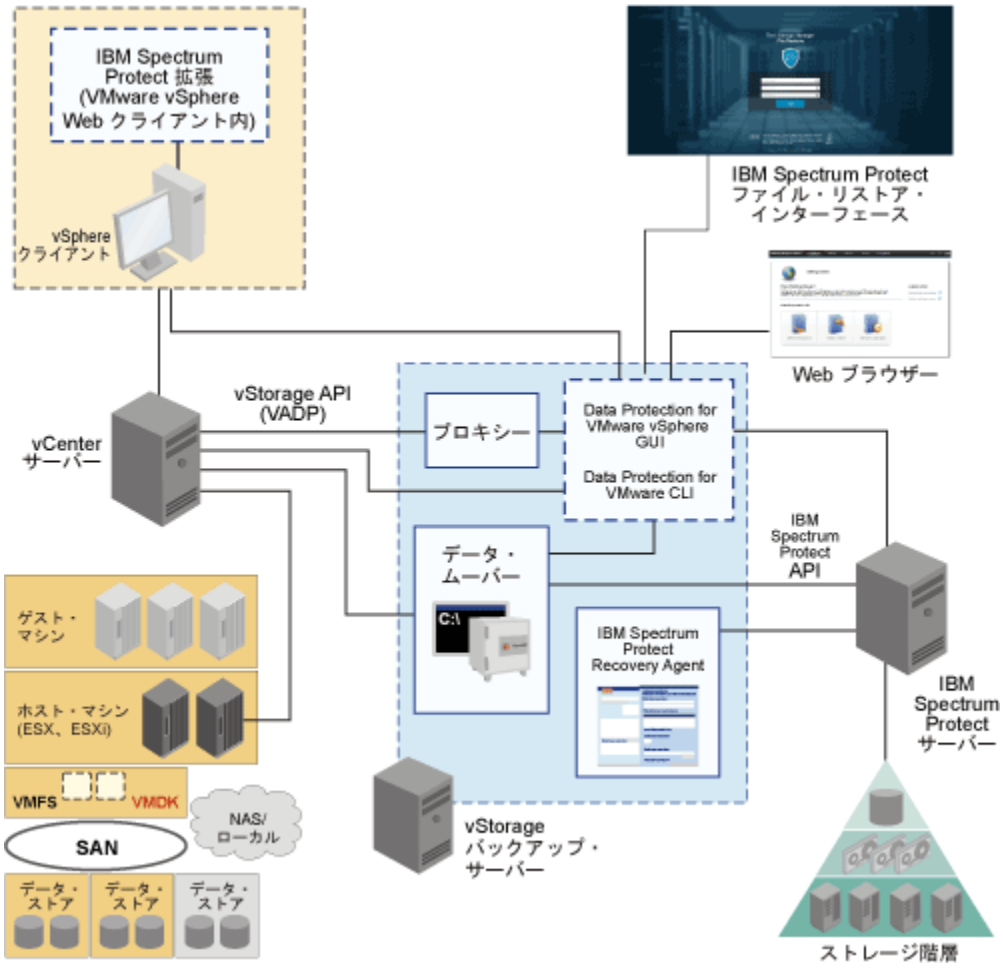

図 *1. VMware vSphere* ユーザー環境の *Data Protection for VMware* システム・コンポーネント

要件

Data Protection for VMware vSphere GUI は、オペレーティング・システムの前提条件を満たすどのシステムにもインストールできます。vSphere GUI は入出力データ転送を処理しないため、リソース要件は最小です。

ヒント: vSphere GUI を vStorage バックアップ・サーバーにインストールすることが、最も一般的な構成です。

vSphere GUI は、以下のシステムへのネットワーク接続を持っている必要があります。

- vStorage バックアップ・サーバー
- IBM Spectrum Protect サーバー
- vCenter Server

また、Derby データベースのポート (デフォルト 1527) および GUI Web サーバーのポート (デフォルト 9081) を使用可能にする必要があります。

構成

複数の vSphere GUI を単一の vCenter Server に登録することができます。このシナリオでは、単一の VMware vSphere GUI が管理するデータ・センター (およびその VM ゲスト・バックアップ) の数を削減します。これにより、vCenter Server は、vCenter Server に定義されているデータ・センターの総数のうち、サブセットを管理することができます。

管理対象のデータ・センターを更新するには、「**構成**」 > 「**構成の編集**」に進んでください。

複数の vSphere GUI を単一の vCenter Server に登録する際には、次のガイドラインが適用されます。

- 各データ・センターは、インストールされている vSphere GUI 1 つのみで管理することができます。
- インストール済みの vSphere GUI ごとに固有の VMCLI ノード名が必要です。
- インストールされた vSphere GUI ごとに固有のデータ・ムーバー・ノード名を使用することにより、ノードの管理が単純化されます。

vSphere GUI へのアクセス

vSphere GUI には、次の方法でアクセスします。

- スタンドアロンの Web ブラウザー GUI。 この GUI にアクセスするには、GUI Web サーバーへの URL ブックマークを使用します。例えば、次のようになります。

  ```
  https://hostname:port/TsmVMwareUI/
  ```

  ここで、

  – *hostname* は、Data Protection for VMware vSphere GUI がインストールされているシステムの 名前です。
  – *port* は、vSphere GUI にアクセス可能なポート番号です。デフォルトのポート番号は 9080 です。セキュア・ポートのデフォルトは 9081 です。
- GUI Web サーバーに接続して IBM ストレージ内の仮想マシンにアクセスする vSphere Web Client 拡張 (Data Protection 拡張と呼ばれる)。このコンテンツは、Web ブラウザー GUI で提供されるもののサブセットです。

インストール時に、1 つ以上のアクセス方式を指定できます。

Windows デフォルトのインストール・ディレクトリーは、`C:¥IBM¥SpectrumProtect¥webserver` です。

Linux デフォルトのインストール・ディレクトリーは `/opt/tivoli/tsm/tdpvmware/common/webserver` です。

IBM Spectrum Protect Recovery Agent

Recovery Agent サービスを使用して、IBM Spectrum Protect サーバーから任意のスナップショット・ボリュームをマウントします。

概要

iSCSI プロトコルを使用してリモート・システムからスナップショットにアクセスすることができます 。

クライアント・システム上で、読み取り専用アクセス権限を使用して、ローカル側でスナップショットを表示する必要がある場合は、Data Protection for VMware V8.1.4 以前のバージョンを使用してください。

さらに、Recovery Agent は、インスタント・リストア機能とゲスト内アプリケーション保護の両方を提供します。インスタント・リストアを使用すると、リストア操作がバックグラウンドで進行中の間に、使用中のボリュームを使用可能なままにしておくことができます。アプリケーション保護により、Microsoft Exchange Server および Microsoft SQL Server など、ゲスト仮想マシンにインストールされているアプリケーションをバックアップおよびリストア 保護に使用できるようになります。

Recovery Agent は、リモート・システムから以下のタスクを実行することができます。

- リストア可能なデータに関する以下のような情報を収集します。
  – バックアップされた VM。
  – バックアップされた仮想マシンで使用可能なスナップショット。
  – 特定のスナップショットで使用可能な区画。

コマンド、パラメーター、および戻りコードについて詳しくは、「*IBM Spectrum Protect for Virtual Environments: Data Protection for VMware* ユーザーズ・ガイド」のコマンド解説セクションを参照してください。

要件

Windows Windows システムでは、Recovery Agent GUI およびコマンド・ライン・インターフェースが、Data Protection for VMware のフルインストール、またはデータ・ムーバーの拡張インストールの一部としてインストールされます。

Recovery Agent へのアクセス

Windows Recovery Agent には、次のように「**スタート**」メニューからアクセスできます。「**スタート**」 > 「**IBM Spectrum Protect**」 > 「**IBM Spectrum Protect for Virtual Environments**」 > 「**IBM Spectrum Protect Recovery Agent**」

IBM Spectrum Protect vSphere Client プラグイン

IBM Spectrum Protect vSphere Client プラグインは、Data Protection for VMware vSphere GUI のビューを提供する VMware vSphere Web Client 拡張です。

概要

IBM Spectrum Protect vSphere Client プラグインは、Data Protection for VMware vSphere GUI のブラウザーのビューで使用可能な機能のサブセット、およびいくつかの追加機能を提供します。

要件

IBM Spectrum Protect vSphere Client プラグインをインストールするには、IBM Spectrum Protect for Virtual Environments 構成ウィザードの実行時に以下のオプションを選択する必要があります。

- 構成ウィザードの「**vCenter 設定**」ページで、「**登録の更新**」を選択し、関連する vCenter にプラグインを登録します。
- GUI ホスト・アドレス、vCenter ユーザーおよびパスワードを入力します。

  注: デフォルトのドメインは、ローカル・ドメイン・アドレスに基づいており、外部からアクセスことはできません。外部アクセスが必要な場合は、DNS によって解決できる GUI ホスト・アドレスまたは IP アドレスを指定してください。

ウィザードが完了すると、プラグインが vCenter に登録されます。

Data Protection プラグインへのアクセス

このプラグインには、vSphere Web Client からアクセスできます。

1. vCenter 資格情報を使用して vSphere Web Client にログインします。Data Protection プラグインは、メインメニューの「**IBM Spectrum Protect**」の下にあります。
2. このメニュー項目を選択すると、IBM Spectrum Protect 拡張の主な作業域に移動します。 vCenter インベントリー内の特定項目に関連付けられている「**モニター**」セクションと「**構成**」セクションでも IBM Spectrum Protect for Virtual Environments 機能を使用できます。

Data Protection for VMware コマンド・ライン・インターフェース

この Data Protection for VMware CLI は、Data Protection for VMware vSphere GUI と一緒にインストールされる、全機能を持つコマンド・ライン・インターフェースです。

概要

Data Protection for VMware CLI を使用して、以下のタスクを実行できます。

- VM の IBM Spectrum Protect サーバーへのバックアップを開始またはスケジュールします。
- IBM Spectrum Protect サーバーから VM、VM ファイル、または VM ディスク (VMDK) のフルリカバリーを開始します。
- バックアップ・データベースと環境についての構成情報を表示します。

Data Protection for VMware vSphere GUI は 1 次タスク・インターフェースですが、Data Protection for VMware CLI は実用的な 2 次インターフェースを 提供します。

例えば、Data Protection for VMware CLI を使用して、Data Protection for VMware vSphere GUI によって実装されるスケジューリング・メカニズムとは異なるスケジューリング・メカニズムを実装することができます。また、Data Protection for VMware CLI は、スクリプトによる自動化の結果を評価する場合に役立ちます。

Data Protection for VMware コマンド・ライン・インターフェースへのアクセス

Data Protection for VMware CLI は、コマンド・ラインからアクセスできます。

使用可能なコマンドについて詳しくは、「*IBM Spectrum Protect for Virtual Environments: Data Protection for VMware* ユーザーズ・ガイド」のコマンド解説セクションを参照してください。

IBM Spectrum Protect ファイル・リストア・インターフェース

VMware 仮想マシンのバックアップから個々のファイルをリストアできます。

概要

ファイル・リストア・インターフェースは、 VM バックアップから個々のファイルをリストアできる Web ベースのインターフェースです。 このインターフェースの 利点は、ファイル、ソフトウェア、およびプラットフォームの所有者が、 IBM Spectrum Protect のバックアップおよびリストア 操作の予備知識を持っていなくても、 所有しているファイルをリストアできるという点です。

ファイル・リストア・インターフェース 機能は、vSphere 環境内のデータを保護するためのオプションを選択すると、インストールされます。Data Protection for VMware 構成ウィザードで、使用可能にするインターフェースのファイル・リストア機能を有効にする必要があります。

IBM Spectrum Protect ファイル・リストア・インターフェースへのアクセス

ファイル・リストア・インターフェースにアクセスするには 、Web ブラウザーを開き、管理者から提供された URL を入力します。 例えば、次のようにします。

```
https://hostname:9081/FileRestoreUI
```

ここで、*hostname* は、Data Protection for VMware vSphere GUI がインストールされているシステムのホスト名です。

データ・ムーバー機能

データ・ムーバーは、Data Protection for VMware のソフトウェア・コンポーネントであり、IBM Spectrum Protect サーバー との間でデータを移動します。

概要

典型的な VMware 環境では、仮想マシンのバックアップをデータ・センター・ノードに保存するために、データ・ムーバーを使用します。

Data Protection for VMware をインストールした場合、データ・ムーバーはインストールに組み込まれています。データ・ムーバーは、Data Protection for VMware vSphere GUI、および他の Data Protection for VMware コンポーネントと同じシステムにインストールされています。

データ・ムーバーを他の Data Protection for VMware コンポーネントのリモート・システムに別にインストールして、複数システム間でバックアップ・ワークロードを再配布することも可能です。

スナップショット差分バックアップ操作は、VMware 環境ではサポートされません。Data Protection for VMware データ・ムーバーもインストールされているホスト 上の NetApp ファイラーにあるファイル・システムのスナップショット 差分バックアップ操作を実行することはできません。

データ・ムーバーのセットアップ

データ・ムーバーの計画、インストール、構成について詳しくは、以下のリストを参照してください。

アクション	説明
ご使用の vSphere 環境を保護するために必要なデータ・ムーバーの数を判別	ご使用の vSphere 環境を保護するために、複数のデータ・ムーバー・ノードが必要になる可能性があります。 必要なデータ・ムーバー・ノードの数を判別するには、技術情報 2007197 を参照します。 この技術情報には、データ・ムーバー・ノードのために仮想マシンまたは物理マシンを使用する際の考慮事項やデータ・ムーバーの局所性の考慮事項も含まれています。
Data Protection for VMware をインストール	Data Protection for VMware をインストールするには、Data Protection for VMware インストーラーを実行し、Windows オペレーティング・システムの場合は「**標準インストール**」、Linux オペレーティング・システムの場合は「**完了**」を選択します。このインストール・オプションにより、データ・ムーバーを含むすべての Data Protection for VMware コンポーネントがインストールされます・ Data Protection for VMware インストーラーを実行する方法について詳しくは、20 ページの『Data Protection for VMware コンポーネントのインストール』を参照してください。
ご使用の環境に合うデータ・ムーバーを定義	Data Protection for VMware インストール・ウィザードが完了すると、Data Protection for VMware vSphere GUI 構成ウィザードが開き、IBM Spectrum Protect サーバー との通信をセットアップできます。 構成ウィザードの「**データ・ムーバー・ノード**」ページで、ローカル・データ・ムーバー、および別個のシステムにインストールする任意のリモート・データ・ムーバーの情報を定義します。 Windows オペレーティング・システムにインストールし、データ・ムーバーの定義時に「**サービスの作成**」を選択した場合、データ・ムーバーの構成情報は以下の場所のオプション・ファイルに保管されます。 `C:\Program Files\Tivoli\TSM\baclient\` さらに、データ・ムーバーに必要なサービスが構成されます。 Linux オペレーティング・システムまたは Windows オペレーティング・システムにデータ・ムーバーをインストールするものの、構成中に「**サービスの作成**」を選択しない場合、オプション・ファイルを作成して、必要なサービスを構成するために85 ページの『vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ』のステップを実行する必要があります。

アクション	説明
必要に応じて、リモート・システムに追加のデータ・ムーバーをインストールして構成	リモート・システムにデータ・ムーバーをインストールするには、Data Protection for VMware インストーラーを実行し、以下のアクションのいずれかを実行します。 Windows オペレーティング・システムの場合は、構成ウィザードで「**拡張インストール**」 > 「**データ・ムーバー機能のみのインストール**」を選択します。 Linux オペレーティング・システムの場合は、構成ウィザードの「**インストール・セット**」リストから「**カスタム**」を選択します。「**Data Protection for VMware データ・ムーバー**」が選択されていることを確認します。 このオプションは、デフォルトで選択されています。 インストールが完了したら、リモート・システムにデータ・ムーバーをセットアップするために、85 ページの『vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ』の指示に従います。

Data Protection for VMware のインストール計画

Data Protection for VMware は、VMware ESXi ベースのホストから vStorage バックアップ・サーバーにバックアップの作業負荷をオフロードすることにより、VM でバックアップを実行した場合の影響を取り除きます。

Data Protection for VMware は、統合されたデータ・ムーバーと連携して、VM の永久増分フルバックアップおよび永久増分の増分バックアップを実行します。 このデータ・ムーバー・ノードは、保管のため、および後に VM イメージ・レベルのリストアを実行するために、データを IBM Spectrum Protect サーバーに「移動」します。ディスク・ボリューム・レベルおよびフル VM レベルでのインスタント・リストアが有効です。

ヒント: データ・ムーバーは、独自のユーザー・インターフェースと 文書を含む、別個にライセンス交付されるコンポーネントです。VM を保護するための包括的な計画を Data Protection for VMware に適切に統合するためには、この製品とその資料を熟知している必要があります。Data Protection for VMware for Windows 64 ビットには、データ・ムーバー機能が含まれます。

インストール・ロードマップ

以下の表に、インストール・プロセスを正常に完了するための手順を示します。

表 *2. Data Protection for VMware* の新規または既存のお客様用のインストール・タスク

ステップ	タスク	参照箇所
1	システム要件の確認	Data Protection for VMware をインストールするシステムが、システム要件を満たしていることを確認します。
2	ユーザー権限要件の確認。	必要なユーザー権限レベルを使用することで、潜在的なインストール・エラーや遅延を回避します。
3	必要な通信ポートの可用性の確認。	Data Protection for VMware のインストールを試行する前に、必要な通信ポートを開くことで、インストールの失敗や遅延を回避します。

表 2. *Data Protection for VMware* の新規または既存のお客様用のインストール・タスク (続き)		
ステップ	**タスク**	**参照箇所**
4	Data Protection for VMware のインストール: • インストール・ウィザードを使用した Data Protection for VMware のインストール • 24 ページの『サイレント・モードでの Data Protection for VMware コンポーネントのインストール』 Data Protection for VMware のアップグレード: Data Protection for VMware のアップグレード	各インストール・パッケージには、ユーザーのライセンス・ファイル (EULA) が提供されます。このファイルを受け入れないと、インストールは終了します。
5	39 ページの『Windows でのウィザードを使用した新規インストールの構成』 Data Protection for VMware をアップグレードする予定である場合、インストールされているコンポーネントに応じて、追加の構成タスクが必要になる場合があります。 詳しくは、「*IBM Spectrum Protect for Virtual Environments: Data Protection for VMware* ユーザーズ・ガイド」の構成に関するトピックを参照してください。	構成ウィザードを使用して初期構成を行います。 インストールする機能によって、このセクションで記載されているように、追加の構成タスクが必要になる場合があります。

ヒント: 特定の Data Protection for VMware バックアップ環境に必要なプロキシー・ホストの数を計画する際には、IBM Spectrum Protect Wiki で入手可能な以下の資料が役立ちます。
Step by Step Guide To vStorage Backup Server (Proxy) Sizing
この資料は、IBM Spectrum Protect for Virtual Environments 製品セクションで入手可能です。

インストールのシナリオ

Data Protection for VMware をインストールする前に、ビジネス・ニーズに最も適したシナリオを選択します。

GUI を使用して、またはサイレント・モードで、Data Protection for VMware およびデータ・ムーバーをインストールできます。

- 21 ページの『インストール・ウィザードを使用した Data Protection for VMware コンポーネントのインストール』
- 24 ページの『サイレント・モードでの Data Protection for VMware コンポーネントのインストール』

プラットフォームごとに使用可能な機能およびコンポーネントのリストについては、 1 ページの『インストール可能コンポーネント』を参照してください。

表 3. インストールのシナリオ		
シナリオ番号	**説明**	**完了しなければならないタスク**
1	Data Protection for VMware とデータ・ムーバーを同じシステムにインストールする新規インストールには、このシナリオを使用します。	Windows Suite インストーラーは、GUI モードまたはサイレント・モードで使用することができます。 Linux InstallAnywhere は、GUI モードまたはサイレント・モードで使用することができます。

表 3. インストールのシナリオ (続き)		
シナリオ番号	**説明**	**完了しなければならないタスク**
2	データ・ムーバー (マウント・プロキシー)、Recovery Agent および必要なサポート・パッケージをこのシステムにインストールする場合は、このシナリオを使用します。	Windows Suite インストーラーを使用して拡張インストールを行うことができます。 Linux データ・ムーバー機能は、Data Protection for VMware と一緒にインストールされます。

システム要件

Data Protection for VMware コンポーネントを実装するには、ご使用のシステムが該当するシステム要件を満たしていることが必要です。

ソフトウェア要件

ソフトウェアおよびオペレーティング・システムの要件の詳細は、時間の経過とともに変わる可能性があります。現在のソフトウェア要件については、技術情報 1505139 を参照してください。

ハードウェア要件

ハードウェア要件は、次の項目に応じて異なります。

- 保護対象サーバーの数
- 保護対象ボリュームの数
- データ・セットのサイズ
- LAN および SAN 接続

注 : recovery agent コンポーネントは、LAN フリー環境での操作をサポートしていません。

次の表は、 Data Protection for VMware のインストールに必要なハードウェア要件を示しています。

表 4. *Data Protection for VMware* のハードウェア要件		
コンポーネント	**最小要件**	**推奨**
システム	IntelPentium D デュアルコア・プロセッサーまたは同等製品	適用外
メモリー	4 GB の RAM、4 GB の仮想アドレス・スペース	適用外
利用可能なハード・ディスク	4.4 GB	9.0 GB
ネットワーク	1 GbE	10 GbE

注 : 仮想マシンのバックアップは、並列処理の数によっては大量のメモリーを使用します。

dsmc backup vm コマンドに関するメモリー所要量は拡張可能であり、以下の数式で計算できます。

必要メモリー = (DiskSize / MBLKSize) * ReadBufferSize * VMMAXPARALLEL

ここで、

- **DiskSize** は、現在処理中のゲスト・ディスクのサイズです
- **MBLKSize** は、メガブロックのサイズです。 2 TB 未満のディスクの場合は 128 MB、2 TB 以上のディスクの場合は 1 GB になります。
- **ReadBufferSize** は、MBLK 情報に使用される IBM Spectrum Protect 内部バッファーのサイズです。このバッファー・サイズは 256 KB になります。

- **VMMAXPARALLEL** は、単一のバックアップ操作処理で、ある一時点でバックアップできる仮想マシンの最大数を指定します。

例えば、それぞれ 40 GB ディスクを使用する 10 のゲストをバックアップし、単一のバックアップ操作処理において VMMAXPARALLEL 2 で実行するには以下が必要になります。

- **DiskSize** = 40 GB = 41943040 KB;
- **MBLKSize** = 128 MB = 131072 KB;
- **ReadBufferSize** = 256 KB;
- **VMMAXPARALLEL** = 2。

必要メモリー = (41943040 / 131072) * 256kB * 2 = 163840KB = 160MB。

注 : 5 つの並列バックアップ操作処理で、'VMMAXPARALLEL 2' で同じ数のゲストをバックアップする場合、(最大で) 前述の例の 5 倍のメモリー、つまり 800 MB が必要になります。

制約事項 : 以下の制限事項は、バックアップ操作に含まれる VMware VMDK に適用されます。

- 永久増分の増分バックアップ・モードの場合、バックアップ操作に含まれる個々の VMDK が 8 TB を超えてはなりません。VMDK が 8 TB を超えると、バックアップ操作は失敗します。デフォルトの 2 TB より大きいサイズに VMDK のサイズを増やすには、vmmaxvirtualdisks オプションを使用して最大サイズを指定します。 詳しくは、IBM Knowledge Center の vmmaxvirtualdisks を検索してください。

いずれのバックアップ・モードの場合も、実行中の失敗を回避するには、データ・ムーバーのオプション・ファイルで vmskipmaxvirtualdisks yes を指定して、VMDK の処理をスキップします。 詳細については、Vmskipmaxvirtualdisks を参照してください。

ファイル・リストアの前提条件

IBM Spectrum Protect Data Protection for VMware ファイル・リストア・インターフェースを 使用してファイルをリストアする前に、ご使用の環境が最小限の前提条件を満たしていることを確認してください。

ファイル・リストア機能を有効にするには、Windows システム上に Data Protection for VMware がインストールされている必要があります。

VMware 仮想マシンの前提条件

以下の前提条件が、リストアするファイルが含まれている VMware 仮想マシンに適用されます。

- Linux Windows VMware ツールが仮想マシンにインストールされている必要があります。
- Linux Windows ファイル・リストア操作中、仮想マシンが実行されている必要があります。
- Windows データ・ムーバー・システムは、リストアするファイルが含まれている仮想マシンと同じ Windows ドメインに属しているか、仮想マシンと信頼関係があるドメイン内にある必要があります。
- Windows 仮想マシンが Windows ドメインから削除され、後にリストアされる場合、ドメイン信頼関係を確保するために、仮想マシンはそのドメインに再加入する必要があります。ドメイン信頼関係がリストアされるまで、 仮想マシンからファイルをリストアしないようにしてください。
- Windows リストアするファイルをユーザーが所有していない場合は、その仮想マシンに対する Microsoft Windows の 「ファイルおよびディレクトリーのリストア」特権をユーザーに割り当てる必要があります。
- Data Protection for VMware ファイル・リストア・インターフェースを 使用するために必要な Microsoft Windows ドメインのアカウントの前提条件について詳しくは、技術情報 1998066 を参照してください。
- Linux 仮想マシンではローカル・ユーザー認証が必要です。 認証は、Windows ドメイン、Lightweight Directory Access Protocol (LDAP)、Kerberos、またはその他のネットワーク認証方式を介して使用することはできません。
- Linux Red Hat Enterprise Linux 6 オペレーティング・システムでは、 sshd デーモン構成ファイル内の ChallengeResponseAuthentication オプション (/etc/ssh/sshd_config) が YES に指定されているか、コメント化されている必要があります。例えば、 以下のステートメントはどちらも有効です。

```
ChallengeResponseAuthentication yes
```

```
#ChallengeResponseAuthentication no
```

このオプションの変更後、 sshd デーモンを再始動してください。

データ・ムーバーの前提条件

データ・ムーバー・システムは、1 つのシステムから別のシステムに「データを移動する」特定のデータ・ムーバーを表します。

Windows データ・ムーバー・システムは、リストアするファイルが含まれている仮想マシンと同じ Windows ドメインに属している必要があります。

マウント・プロキシーの前提条件

マウント・プロキシー・システムは、マウントされた仮想マシン・ディスクに iSCSI 接続を介してアクセスする Linux または Windows プロキシー・システムを表します。このシステムにより、マウントされた仮想マシン・ディスク上のファイル・システムが、ファイル・リストア・インターフェースへのリストア・ポイントとしてアクセス可能になります。

Linux Linux オペレーティング・システムでは、論理ボリューム・マネージャー (LVM) ボリューム・グループがシステムで 使用可能になると、それらのグループを活動化するデーモンが提供されています。LVM ボリューム・グループがシステムで 使用可能になったときに活動化されないように、このデーモンを Linux マウント・プロキシー・システムで設定してください。このデーモンの設定方法について詳しくは、該当する Linux 資料を参照してください。

Linux Windows Windows マウント・プロキシー・システムと Linux マウント・プロキシー・システムは、同じサブネット上になければなりません。

Microsoft Windows ドメイン・アカウントの前提条件

Windows ドメイン・アカウントには、以下の前提条件が適用されます。最初の要件は、すべての VM に対するローカル管理権限を持つ Windows ドメイン・ユーザー・アカウントを設定することです。

- 仮想マシン・ゲストへのファイル・リカバリーを有効にするために必要なタスクを実行するには、Windows ドメインに属していて、マウント・プロキシー・システムのローカル管理者であるユーザー・アカウントが必要です。このアカウントを持つ管理者は、Data Protection for VMware vSphere GUI 構成ウィザードまたはノートブックにアカウント 資格情報を入力して、環境をファイル・リストア操作に使用可能にします。
- ファイル・リストア・インターフェースを 使用するための十分な特権を持つユーザー・アカウントを作成するために、Windows のグループ・ポリシー・オブジェクトを 使用して、単一のドメイン・ユーザーを一元管理し、ローカル管理者の資格情報を使用して複数のマシンにアクセスできるようにして、オプションで望ましくないアクションを制限することができます。

以下のステップで、このユーザー・アカウントを作成する方法を説明します。Active Directory ユーザーとコンピューター MMC スナップインを 使用して、ドメイン・コントローラーで以下のステップを実行してください。

1. 「**操作**」->「**新規作成**」->「**グループ**」を選択して、「**FR Admins**」という名前の新規セキュリティー・グループを作成します。グループのスコープは「グローバル」に設定する必要があります。
2. ユーザー名 `fradmin1` を持つ新規ドメイン・ユーザー・アカウントを作成して、「**FR Admins**」セキュリティー・グループに追加します。その他のドメイン・ユーザー・アカウントもグループに追加できます。
3. `fradmin1` がアクセスできる一連のコンピューターに対する制御を強化するには、新規組織単位を作成します。
4. ドメイン・オブジェクトから、「**新規作成**」->「**組織単位**」を選択して、「`FR Computers`」という名前を指定します。
5. 「`FR Computers`」組織単位に数台のマシンのデータを取り込みます。

グループ・ポリシー MMC スナップインからドメイン ・コントローラーで以下のステップを実行します。

1. 「FR Admin GPO」という新規グループ・ポリシー・オブジェクトを作成します。これにより、「**FR Admins**」グループ内の管理者が、グループ・ポリシー・オブジェクトが適用される組織単位に関連付けられているコンピューターのローカル管理者グループに追加されます。
2. グループ・ポリシー・オブジェクトで、アカウントをローカル管理者とオプションでリモート・デスクトップ・ユーザーに追加します。
3. 「FR Computers」組織単位を選択して、新しく作成されたグループ・ポリシー・オブジェクトを追加します。

   注: グループ・ポリシー・オブジェクトはドメイン自体に関連付けられている可能性がありますが、その場合、fradmin1 は、そのドメイン内のすべてのコンピューターのローカル管理者グループに属します。明示的な組織単位を使用すると、制御を強化できます。
4. オプションで、グループ・ポリシー管理を使用して、「Deny log on locally」や「Deny log on through Terminal Services」など、ローカル・マシンに対する望ましくないアクションを制限します。
5. VMware vSphere GUI 構成ウィザードまたはノートブックの 「ファイル・リストア」ページで、上記のステップで作成された domain¥fradmin1 アカウントを使用するために設定を更新します。
6. マウント・プロキシー・クライアント・アクセス・デーモン (CAD) サービスを再開します。

適切な特権を持つアカウントをセットアップした後、以下を実行します。

- Windows 資格情報を Data Protection for VMware vSphere GUI 構成ウィザードまたはノートブックに 入力して、環境をファイル・リストア操作に使用可能にします。
- Windows ファイル所有者は、Windows ドメイン・ユーザー資格情報を使用して、 (リストアするファイルが入っている) リモート仮想マシンにアクセスします。これらの資格情報は、ログイン時にファイル・リストア・インターフェースで 入力されます。ドメイン・ユーザー資格情報は、ファイル所有者がリモート仮想マシンにログインしてファイルをリモート 仮想マシンにリストアする権限を持っていることを検証します。これらの資格情報には、特別な権限は必要ありません。
- Windows ファイル所有者は、(ドメイン内のすべてのコンピューターにアクセスするのではなく) 特定のコンピューターのみにアクセスを制限する Windows ドメイン・ユーザー・アカウントを使用する場合、このドメイン・ユーザー・アカウントからアクセス可能なコンピューターのリストにマウント・プロキシー・システムが含まれていることを確認してください。含まれていない場合、ファイル所有者はファイル・リストア・インターフェースにログインできません 。

磁気テープ・メディアの前提条件

磁気テープ・メディアからのファイル・リストアはサポートされません。そのため、ディスク・ストレージからファイル・リストアを行う方法をお勧めします。

必要なインストール権限

インストールを開始する前に、ご使用のユーザー ID に必要な権限レベルが含まれていることを確認します。

このタスクについて

表 *5. Data Protection for VMware* のインストールおよび構成に必要なユーザー権限

システム	必要な権限
Windows	管理者
Linux	root

表 5. *Data Protection for VMware* のインストールおよび構成に必要なユーザー権限 *(続き)*	
システム	**必要な権限**
vCenter Server	管理者特権 vCenter Server 役割には、「**拡張**」 > 「**拡張の登録 (Register extension)** 」、「**拡張の登録解除 (Unregister extension)**」、「**拡張の更新 (Update extension)**」の特権が必要です。この新しい役割は、インストール時に指定されたユーザー ID に対応する VMware vCenter Server 階層内の vCenter オブジェクトに適用する必要があります。
IBM Spectrum Protect サーバー **制約事項 :** サーバーを再始動する必要があります。	管理アクセス権 (**System** または **Unrestricted Policy Domain** 特権)

必要な通信ポート
Data Protection for VMware のインストール時にファイアウォール内で開く必要がある通信ポートのリストを表示します。

表に示されたポートは、標準的なインストール済み環境を表しています。標準的なインストール済み環境は、同じ Windows システム上の以下のコンポーネントから構成されます。

- Data Protection for VMware GUI サーバー
- vStorage バックアップ・サーバー (データ・ムーバー)
- Windows マウント・プロキシー
- IBM Spectrum Protect ファイル・リストア・インターフェース

標準的ではないインストール済み環境を使用する場合、多くのポートが必要になる可能性があります。

制約事項 : Windows マウント・プロキシーと Linux マウント・プロキシーは、同じサブネット上になければなりません。

表 6. 必要な通信ポート. この表は、Data Protection for VMware がアクセスするポートを示しています。		
TCP ポート	**イニシエーター: アウトバウンド (ホストから)**	**ターゲット: インバウンド (ホストへ)**
443	vStorage バックアップ・サーバー	vCenter Server (セキュア HTTP)
443	Data Protection for VMware vSphere GUI サーバー	vCenter Server
443 この設定は、データ・ムーバーが Linux システムである場合にのみ必要です。	Windows マウント・プロキシー	vCenter Server
443	vStorage バックアップ・サーバー	Platform Services Controller
443	Data Protection for VMware vSphere GUI サーバー	Platform Services Controller
443	Windows マウント・プロキシー	Platform Services Controller
902 443	vCenter Server	ESXi ホスト

表 6. 必要な通信ポート. この表は、Data Protection for VMware がアクセスするポートを示しています。 (続き)

TCP ポート	イニシエーター: アウトバウンド (ホストから)	ターゲット: インバウンド (ホストへ)
902 443	vStorage バックアップ・サーバー (プロキシー)	ESXi ホスト (保護されたすべてのホスト)
1500 (**tcpport**)	vStorage バックアップ・サーバー (プロキシー)	IBM Spectrum Protect サーバー
1500 (**tcpadminport**)	Data Protection for VMware vSphere GUI サーバー • 1500 (**tcpadminport**) は、非 SSL 通信です • SSL 通信では、**tcpadminport** が、IBM Spectrum Protect サーバーとの SSL 通信をサポートする唯一のポートです。 通常、SSL プロトコルに使用する正しいポート番号は、IBM Spectrum Protect サーバーの dsmserv.opt ファイルの **ssltcpadminport** オプションで指定された値です。ただし、dsmserv.opt ファイルで **adminonclient no** が指定されている場合、SSL プロトコルに使用する正しいポート番号は、**ssltcpadminport** オプションで指定された値です。 **ssltcpadminport** オプションには、デフォルト値はありません。 したがって、ユーザーが値を指定する必要があります。	IBM Spectrum Protect サーバー
1527 内部 Derby データベース		
1501 1581 (**httpport**)	IBM Spectrum Protect サーバー	vStorage バックアップ・サーバー • データ・ムーバー・スケジューラー • Web クライアント • クライアント・アクセプター・デーモン
1581 (**httpport**) 1582, 1583 (**webports**)	Data Protection for VMware vSphere GUI サーバー	vStorage バックアップ・サーバー
9081 GUI Web サーバー (HTTPS プロトコル)	vSphere Client	Data Protection for VMware vSphere GUI サーバー (Web ブラウザーから vCenter にアクセスするためのセキュア HTTPS ポート)

表 6. 必要な通信ポート. この表は、Data Protection for VMware がアクセスするポートを示しています。 (続き)

TCP ポート	イニシエーター: アウトバウンド (ホストから)	ターゲット: インバウンド (ホストへ)
22 Recovery Agent の SSH デフォルト・ポート	Recovery Agent	Data Protection for VMware Windows「マウント」ホスト • Linux Recovery Agent の SSH
3260	Linux Data Protection for VMware ファイル・リストア	Data Protection for VMware Windows「マウント」ホスト • iSCSI
3260 Recovery Agent の iSCSI デフォルト・ポート	ファイル・リストア用の動的ディスクを備えた Windows ターゲット	Data Protection for VMware Windows「マウント」ホスト • iSCSI
5985	ファイル・リストア GUI 操作	Windows リモート管理
135	Windows マウント・プロキシー	IBM Spectrum Protect ファイル・リストア・インターフェースを 使用してリストアするファイルが含まれている VMware 仮想マシン

VMware vCenter Server ユーザー特権の要件
Data Protection for VMware 操作を実行するには 特定の VMware vCenter Server 特権が必要です。

Data Protection for VMware vSphere GUI の Web ブラウザーのビューを使用して VMware データ・センターを保護するために必要な vCenter Server 特権

Data Protection for VMware vSphere GUI のブラウザー・ビューにサインインする vCenter Server のユーザー ID には、

GUI が管理するデータ・センターのコンテンツを表示するための十分な VMware 特権が必要です。

例えば、VMware vSphere 環境に 5 つのデータ・センターが含まれているとします。ユーザー「jenn」が十分な特権を持っているのは、これらのデータ・センターのうち 2 つに対してのみです。この結果、十分な特権が存在するこれら 2 つのデータ・センターのみがビューで「jenn」に対して表示されます。 他の 3 つのデータ・センター (「jenn」が特権を持っていない) は、ユーザー「jenn」に表示されません。

VMware vCenter Server は、一連の特権をまとめて、1 つの役割として定義します。 特権を作成するため、指定されたユーザーまたはグループのオブジェクトに 役割を適用します。 VMware vSphere Web Client から、一連の特権を持つ役割を作成する必要があります。 バックアップ操作およびリストア操作用の vCenter Server 役割を作成するには、VMware vSphere Client の「**役割の追加 (Add a Role)**」機能を使用します。

vCenter 内のすべてのデータ・センターに特権を伝搬したい場合は、vCenter Server を指定して、「子に伝達 (propagate to children)」チェック・ボックスを選択します。 あるいは、必要なデータ・センターのみに役割を割り当てて、「子に伝達 (propagate to children)」チェック・ボックスを選択すると、権限を制限することができます。 ブラウザーの制約はデータ・センター・レベルです。

次の例では、2 つの VMware ユーザー・グループに対してデータ・センターへのアクセスを制御する方法を示します。 最初に、技術情報 7047438 に定義されている特権をすべて含む役割を作成します。この例の特権セットは、「TDPVMwareManage」という名前の役割で識別されています。グループ 1 は、Primary1_DC データ・センターと Primary2_DC データ・センター用の仮想マシンを管理するためのアクセスを必要としています。グループ 2 は、Secondary1_DC データ・センターおよび Secondary2_DC データ・センターの仮想マシンを管理するためのアクセスが必要です。

グループ 1 では、Primary1_DC データ・センターと Primary2_DC データ・センターに「TDPVMwareManage」役割を割り当てます。グループ 2 では、Secondary1_DC データ・センターと Secondary2_DC データ・センターに「TDPVMwareManage」役割を割り当てます。

各 VMware ユーザー・グループ内のユーザーは、Data Protection for VMware GUI を使用して、それぞれのデータ・センター内の仮想マシンのみを管理できます。

ヒント: 役割を作成する際には、オブジェクトに対して他のタスクを実行するために後で必要になる可能性がある余分な特権を役割に追加することを考慮してください。

データ・ムーバーを使用するために必要な vCenter Server の特権

vStorage バックアップ・サーバー (データ・ムーバー・ノード) にインストールされている IBM Spectrum Protect データ・ムーバーには、VMCUser オプションおよび VMCPw オプションが必要です。 VMCUser オプションでは、バックアップ、リストア、または照会する vCenter Server または ESX サーバーのユーザー ID を指定します。このユーザー ID (VMCUser) に割り当てられる必要な特権により、クライアントは仮想マシン環境および VMware 環境で操作を確実に実行することができます。このユーザー ID には、上記技術情報で説明されている VMware 特権が必要です。

バックアップ操作およびリストア操作用の vCenter Server 役割を作成するには、VMware vSphere Client の「**役割の追加 (Add a Role)**」機能を使用します。 このユーザー ID (VMCUser) の特権を追加する場合は、「子に伝達 (propagate to children)」オプションを選択する必要があります。 また、バックアップおよびリストア以外のタスクのために、その他の特権をこの役割に追加することを検討してください。 VMCUser オプションでは、制約は最上位オブジェクトに適用されます。

Data Protection for VMware vSphere GUI の IBM Spectrum Protect vSphere Client プラグインのビューを使用して VMware データ・センターを保護するために必要な vCenter Server 特権

IBM Spectrum Protect vSphere Client プラグインでは、GUI へのサインインに必要な特権とは別の一連の特権が必要です。

インストール時には、IBM Spectrum Protect vSphere Client プラグインのために次のカスタム特権が作成されます。

- 「**データ・センター**」 > 「**IBM Data Protection**」
- 「**グローバル**」 > 「**IBM Data Protection の構成**」

IBM Spectrum Protect vSphere Client プラグインに必要なカスタム特権は、個別の拡張として登録されます。 特権拡張キーは com.ibm.tsm.tdpvmware.IBMDataProtection.privileges です。

これらの特権によって、VMware 管理者は、IBM Spectrum Protect vSphere Client プラグインのコンテンツへのアクセスを有効または無効にすることができます。 必要な VMware オブジェクトに対してこれらのカスタム特権を持つユーザーのみが IBM Spectrum Protect vSphere Client プラグインのコンテンツにアクセスできます。 vCenter Server ごとに IBM Spectrum Protect vSphere Client プラグインが 1 つ登録され、vCenter Server をサポートするように構成されているすべての GUI ホストで共有されます。

VMware vSphere Web Client から、IBM Spectrum Protect vSphere Client プラグインを使用して、仮想マシンに対してデータ保護機能を実行できるユーザーの役割を作成する必要があります。この役割では、Web クライアントが必要とする標準の仮想マシン管理者役割の特権に加えて、「**データ・センター**」 > 「**IBM Data Protection**」特権を指定する必要があります。 それぞれのデータ・センターで、ユーザーによる仮想マシンの管理を許可する対象のユーザーまたはユーザー・グループごとに、この役割を割り当てます。

vCenter レベルのユーザーには、「**グローバル**」 > 「**IBM Data Protection**」特権が必要です。この特権により、ユーザーは vCenter Server と Data Protection for VMware vSphere GUI Web サーバー間の接続を管理、編集、またはクリアすることが可能になります。この特権は、それぞれの vCenter Server を保護する Data Protection for VMware vSphere GUI について熟知する管理者に割り当ててください。IBM Spectrum Protect vSphere Client プラグインの接続は、拡張の「**接続**」ページで管理します。

次の例では、2 つのユーザー・グループに対してデータ・センターへのアクセスを制御する方法を示します。グループ 1 は、NewYork _DC データ・センターおよび Boston_DC データ・センターの仮想マシンを管理するためのアクセスが必要です。グループ 2 は、LosAngeles_DC データ・センターおよび SanFranciso_DC データ・センターの仮想マシンを管理するためのアクセスが必要です。

VMware vSphere client から、例えば「IBMDataProtectManage」役割を作成し、標準の仮想マシンの管理者役割の特権を割り当て、さらに「**データ・センター**」 > 「**IBM Data Protection**」特権を割り当てます。

グループ 1 では、NewYork _DC データ・センターと Boston_DC データ・センターに「IBMDataProtectManage」役割を割り当てます。グループ 2 では、LosAngeles_DC データ・センターと SanFranciso_DC データ・センターに「IBMDataProtectManage」役割を割り当てます。

各グループのユーザーは、vSphere Web Client の IBM Spectrum Protect vSphere Client プラグインを使用して、それぞれのデータ・センターの仮想マシンのみを管理できます。

不十分な権限に関連した問題

Web ブラウザーのユーザーにデータ・センターに対する十分な権限がない場合、ビューへのアクセスがブロックされます。 代わりに、ユーザーの権限が不十分であるために管理対象データ・センターへのアクセスを許可されていないことを通知する、エラー・メッセージ GVM2013E が発行されます。 不十分な権限から生じる問題について、ユーザーに通知するその他の新規メッセージも参照可能です。権限に関連した問題を解決するには、ユーザー役割が前のセクションの説明どおりにセットアップされていることを確認してください。 ユーザー役割は、「vCenter Server のユーザー ID およびデータ・ムーバーに必要な特権」表に示されるすべての特権を持っている必要があります。また、これらの特権は「子に伝達 (propagate to children)」チェック・ボックスを使用してデータ・センター・レベルで適用されている必要があります。

IBM Spectrum Protect vSphere Client プラグインのユーザーにデータ・センターに対する十分な権限がない場合、当該データ・センターとそのコンテンツのデータ保護機能は拡張では使用不可になります。

IBM Spectrum Protect ユーザー ID (VMCUser オプションによって指定される) に含まれる権限が、バックアップおよびリストア操作に不十分である場合は、次のメッセージが表示されます。

```
ANS9365E VMware vStorage API エラー。
「この操作を実行する許可が拒否されました。」
```

IBM Spectrum Protect ユーザー ID に含まれる権限がマシンの表示には不十分である場合は、次のメッセージが表示されます。

```
VM コマンドのバックアップが開始されました。処理する仮想マシンの合計数: 1
ANS4155E 仮想マシン「tango」が VMware サーバー上に見つかりませんでした。
ANS4148E 仮想マシン「foxtrot」のフル VM バックアップが失敗しました。RC 4390
```

特権の使用について詳しくは、**Data Protection for VMware vSphere GUI およびデータ・ムーバーに必要な vCenter Server の特権**を参照してください。

VMware Virtual Center Server を介して、権限の問題についてのログ情報を取得するには、以下のステップを実行します。

1. 「**vCenter Server 設定**」で、「**ロギング オプション**」を選択し、「**vCenter ロギング**」を「**最詳細 (Trivia)**」に設定します。
2. 権限エラーを再現します。
3. 余分なログ情報が記録されないように、「**vCenter ロギング**」を前の値にリセットします。
4. 「**システム ログ**」で、最新の vCenter Server ログ (vpxd-*wxyz*.log) を検索し、ストリング NoPermission を検索します。 例えば、次のようにします。

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   このログ・メッセージは、ユーザー ID に含まれる権限が、スナップショットの作成 (createSnapshot) には不十分であることを示しています。

Data Protection for VMware コンポーネントのインストール

ご使用のオペレーティング・システム用の Data Protection for VMware パッケージで使用可能なすべてまたは一部のコンポーネントをインストールできます。

このタスクについて

Data Protection for VMware インストーラーを使用して、 以下のコンポーネントをインストールできます。

- IBM Spectrum Protect Recovery Agent
- Windows Recovery Agent コマンド・ライン・インターフェース
- Windows 資料 (README ファイルおよび NOTICES ファイル)
- Data Protection for VMware の使用可能化ファイル
- Data Protection for VMware vSphere GUI
- データ・ムーバー機能。これには、以下の項目が含まれます。
  - データ・ムーバー GUI
  - データ・ムーバー Web クライアント
  - クライアント API (64 ビット) ランタイム・ファイル
  - 管理クライアント・コマンド・ライン
  - VMware vStorage API ランタイム・ファイル

フルインストールを選択することも、拡張インストールのオプションを使用してデータ・ムーバー (マウント・プロキシー)、Recovery Agent、および必須のサポート・パッケージをインストールすることも可能です。

ヒント: Data Protection for VMware ソフトウェアと同じシステム上に複数のデータ・ムーバーを作成したり、リモート・システム上にデータ・ムーバーを作成したりすることができます。このような構成により、Data Protection for VMware が使用することができるリソースを増やすことができます。データ・ムーバーがインストールされているシステムは、vStorage バックアップ・サーバーと呼ばれます。

Data Protection for VMware インストール・パッケージの入手

Data Protection for VMware インストール・パッケージは、IBM ダウンロード・サイト (IBM パスポート・アドバンテージなど) から入手できます。

始める前に

Linux

ファイルのダウンロードを予定している場合、ファイルを正しくダウンロードできるように、最大ファイル・サイズに関するシステム・ユーザー制限を無制限に設定してください。

1. 最大ファイル・サイズ値を照会するには、次のコマンドを発行します。

   ```
   ulimit -Hf
   ```

2. 最大ファイル・サイズのシステム ・ユーザー制限が無制限に設定されていない場合、ご使用のオペレーティング・システムの資料の指示に従って、無制限に変更してください。

手順

1. 以下のいずれかの Web サイトから、適切なパッケージ・ファイルをダウンロードします。
   - 初めてインストールする場合または新規リリースの場合は、パスポート・アドバンテージ (http://www.ibm.com/software/lotus/passportadvantage/) にアクセスします。パスポート・アドバンテージは、ライセンス交付を受けたパッケージ・ファイルをダウンロードできる唯一のサイトです。
   - 最新の情報、更新、および保守フィックスについては、 IBM Spectrum Protect のサポート・サイト (http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager) にアクセスします。

2. IBM ダウンロード・サイトからパッケージをダウンロードした場合は、以下のステップを実行します。
   a. パッケージ・ファイルを、選択したディレクトリーにダウンロードします。パスに含める文字数は 40 文字以下でなければなりません。インストール・ファイルは、必ず、空のディレクトリーに解凍してください。インストール・ファイルは、前に解凍したファイルやその他のファイルが含まれるディレクトリーには解凍しないでください。
   b. Linux パッケージに対する実行権限が設定されていることを確認します。必要な場合、次のコマンドを発行してファイル許可を変更します。

      ```
      chmod a+x package_name.bin
      ```

   c. Linux 次のコマンドを発行して、パッケージを解凍します。

      ```
      ./package_name.bin
      ```

      ここで、*package_name* はダウンロードしたファイルの名前です。
   d. Windows *package_name* をダブルクリックして、 パッケージを解凍します。ここで、*package_name* はダウンロードしたファイルの名前です。

インストール・ウィザードを使用した Data Protection for VMware コンポーネントのインストール

インストール・ウィザードを使用して、Data Protection for VMware コンポーネントをインストールできます。

このタスクについて

Windows Suite インストーラーを使用して、Data Protection for VMware とデータ・ムーバーの両方をインストールできます。

Linux スタンドアロン・インストーラーを使用して、Data Protection for VMware とデータ・ムーバーの両方をインストールできます。

Windows システムへの Data Protection for VMware コンポーネントのインストール

Data Protection for VMware のコンポーネントおよび機能をインストール・ウィザードを使用してインストールします。

始める前に

Data Protection for VMware コンポーネントをインストールする前に、以下の要件を満たしていることを確認してください。

- 管理者特権のアクセス権を持つユーザー ID。
- 管理者特権のアクセス権を使用した、VMware vCenter Server 6.x 以降へのネットワーク接続。
- 管理者アクセス権 (**System** または **Unrestricted Policy Domain** 特権) を使用した、IBM Spectrum Protect サーバーへのネットワーク接続。このサーバーが使用可能で稼働している必要があります。
- 必ず、以下の要件を検討してください。
  - 11 ページの『システム要件』
  - 14 ページの『必要なインストール権限』
  - 15 ページの『必要な通信ポート』

Data Protection for VMware をインストールする前に、以下のオプションについて理解しておく必要があります。

インストール・タイプ

標準インストール
標準インストールでは、Data Protection for VMware のすべてのコンポーネントおよび機能がインストールされます。

拡張インストール
「拡張インストール」パネルは、個々のデータ・ムーバーをインストールするためのオプションを提供します。このプロセスでは、データ・ムーバー (マウント・プロキシー)、Recovery Agent および必要なサポート・パッケージをシステムにインストールします。データ・ムーバーを個別に追加する場合は、このインストール・オプションを使用します。このオプションによりアプリケーション保護エージェントもインストールされるため、個々のデータベースのリカバリーが可能になります。インストール後、IBM Spectrum Protect GUI を使用すると VMware vSphere プラグインを介してデータ・ムーバーとサービスを構成できます。

このタスクについて

Suite インストーラーを使用して、Data Protection for VMware をインストールすることができます。Suite インストーラー用の `spinstall.exe` ファイルは、インストール・パッケージのルートにあります。

インストール可能なコンポーネントおよび機能のリストについては、1 ページの『インストール可能コンポーネント』を参照してください。

手順

Data Protection for VMware をインストールするには、インストールすることを選択したコンポーネントの `spinstall.exe` ファイルのロケーションから以下の手順を実行します。

1. `spinstall.exe` ファイルをダブルクリックします。
2. ウィザードの指示に従って、選択したコンポーネントをインストールします。

次のタスク

Data Protection for VMware vSphere GUI にアクセスするには、以下を参照してください。

- 27 ページの『Data Protection for VMware vSphere GUI へのアクセス』

GUI を初めて開始したときに、構成ウィザードが自動的に表示されます。

Linux システムへの Data Protection for VMware のインストール

InstallAnywhere モードを使用して、Data Protection for VMware を Linux システムにインストールします。

始める前に

Data Protection for VMware をインストールする前に、 以下の要件を満たしていることを確認してください。

- 作業を進める前に、ユーザー ID が必要な権限レベルを持っていること、および必要な通信ポートが開いていることを確認します。
- インストール・プロセスにより、ユーザー `tdpvmware` が作成されます。すべての **`vmcli`** コマンドは、ユーザー `tdpvmware` として、root ユーザー ID を使用して発行する必要があります。
- コンソール・モードでインストールを行う場合は、X Window サーバーが必要です。
- 必ず、以下の要件を検討してください。
  - 11 ページの『システム要件』
  - 14 ページの『必要なインストール権限』
  - 15 ページの『必要な通信ポート』

手順

Data Protection for VMware をインストールするには、以下の手順を実行します。

1. インストール・フォルダーのルートから、`CD/Linux/DataProtectionForVMware` ディレクトリーに変更します。
2. コマンド・ラインから、以下のコマンドを入力します。

```
./install-Linux.bin
```

タスクの結果

警告またはエラーを受信した場合は、ログ・ファイルで詳細を確認してください。79 ページの『ログ・ファイル関連のアクティビティー』を 参照してください。

障害が発生したために Data Protection for VMware をインストールできない場合は、34 ページの『Linux システムの Data Protection for VMware のアンインストール』の『Data Protection for VMware の手動による削除』の手順を参照してください。

Linux での Data Protection for VMware のクリーン・インストールの実行

Linux のインストールが中断されても、通常は再開できます。しかし、インストールが再開できない場合、クリーン・インストールが必要です。

このタスクについて

クリーン・インストールを開始する前に、製品が削除されていることを確実にしてください。クリーン環境を確実にするには、以下の手順を実行します。

手順

1. Data Protection for VMware vSphere GUI がインストールされている場合は、以下のタスクを実行します。
   a) 次のを発行して、Data Protection for VMware コマンド・ライン・インターフェース を停止します。
   `/etc/init.d/vmcli stop`
   b) 次のコマンドを発行して、Data Protection for VMware GUI Web サーバーを停止します。
   `/etc/init.d/webserver stop`
   c) 次のを発行して、`.rpm` パッケージを除去します。
   `rpm -e TIVsm-TDPVMwarePlugin`
2. デプロイメント・エンジン製品の項目を除去します。
   a) 次のを発行して、デプロイメント・エンジンのすべての項目をリストします。
   `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b) 次のを発行して、デプロイメント・エンジンのすべての項目を除去します。
   `/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>`
   c) `/var/ibm/common` ディレクトリーを除去します。
   d) `/usr/ibm/common` ディレクトリーを除去します。
   e) `acu_de.log` ファイルが存在する場合は、それを削除して、`/tmp` ディレクトリーをクリーンアップします。
   f) デプロイメント・エンジンをインストールしたユーザーの ID を含む `/tmp` ディレクトリーを除去します。
   g) `/etc/inittab` システム・ファイルから デプロイメント・エンジンの項目をすべて除去します。これらの項目は `#Begin AC Solution Install block` と `#End AC Solution Install block` で区切られています。それらの区切り文字間のすべてのテキストを除去し、区切りテキスト自体を除去します。
   h) `/etc/services` システム・ファイルから デプロイメント・エンジンの参照をすべて除去します。
3. 失敗したインストールからすべての Data Protection for VMware ファイルを除去します。
   a) <*USER_INSTALL_DIR*> 内のファイルを除去します。これは、失敗したインストールが試行されたパスです。例えば、`/opt/tivoli/tsm/TDPVMware/` です。
   b) デスクトップ・ショートカットを除去します。
4. グローバル・レジストリー・ファイル (`/var/.com.zerog.registry.xml`) をバックアップします。このファイルをバックアップした後、Data Protection for VMware を参照するすべてのタグを除去します。

5. TDPVMware ストリングを含む、root の下のログ・ファイルを除去します。
   例えば、次のようにします。
   IA-TDPVMware-00.log または IA-TDPVMware_Uninstall-00.log。
6. Data Protection for VMware コマンド・ライン・インターフェースを実行したユーザーを除去します。
   a) 次のコマンドを発行します。

```
userdel -r tdpvmware
```

   b) 次のコマンドを発行します。

```
groupdel tdpvmware
```

   ヒント : 一部のバージョンの Linux では、関連付けられているユーザーが他に誰もいないグループも **userdel** コマンドで除去されます。そのため、コマンド関連の失敗メッセージは無視してください。

タスクの結果
これらのステップを完了した後、クリーン・インストールを開始します。

サイレント・モードでの Data Protection for VMware コンポーネントのインストール

Data Protection for VMware は、バックグラウンドでインストールできます。 サイレント・インストール中は、メッセージは表示されません。

このタスクについて

Windows Suite インストーラーを使用して、Data Protection for VMware とデータ・ムーバーの両方をインストールできます。

Linux スタンドアロン・インストーラーを使用して、Data Protection for VMware とデータ・ムーバーの両方をインストールできます。

サイレント・モードでの Windows システムへの Data Protection for VMware のインストール

Suite インストーラーをサイレント・モードで使用して、すべての Data Protection for VMware コンポーネントおよびデータ・ムーバー機能をインストールします。

始める前に
Data Protection for VMware およびデータ・ムーバー機能をインストールする前に、ご使用のシステムが、以下のセクションに記載されている要件を満たしていることを確認してください。

- 11 ページの『システム要件』
- 14 ページの『必要なインストール権限』
- 15 ページの『必要な通信ポート』

このタスクについて

制約事項 : Windows では、一部のデフォルトのインストール場所が固定されています。コンポーネントのインストール・ディレクトリーを見つけるには、セクション 1 ページの『インストール可能コンポーネント』 を参照してください。

手順

Data Protection for VMware をインストールするには、以下の手順を実行します。

1. コマンド・プロンプトから次のコマンドを実行します。

```
cd extract_folder\TSMVMWARE_WIN
```

2. 次のを入力します。

```
spinstall.exe /silent
```

初めてボリュームをマウントすると、次のメッセージが表示されます。

```
仮想ボリューム・ドライバーがまだ登録されていません。Recovery Agent can register
the driver now. 登録中に Microsoft Windows ロゴの警告が表示される
場合があります。
この登録を受け入れると登録を完了することができます。
仮想ボリューム・ドライバーを今すぐ登録しますか?
```

続行するには、「**はい**」をクリックして仮想ボリューム・ドライバーを登録します。

関連タスク

33 ページの『Windows 用 Data Protection for VMware のサイレント・モードでのアンインストール』
Windows オペレーティング・システム上の Data Protection for VMware をサイレント・アンインストールすることができます。

サイレント・モードでの Linux システムへの Data Protection for VMware のインストール

Linux オペレーティング・システムにサイレント ・インストールする Data Protection for VMware 機能をカスタマイズすることができます。

始める前に

Data Protection for VMware をインストールする前に、 以下の要件を満たしていることを確認してください。

- 作業を進める前に、ユーザー ID が必要な権限レベルを持っていること、および必要な通信ポートが開いていることを確認します。
- インストール・プロセスにより、ユーザー `tdpvmware` が作成されます。すべての **`vmcli`** コマンドは、ユーザー `tdpvmware` として、root ユーザー ID を使用して発行する必要があります。
- コンソール・モードでインストールを行う場合は、X Window サーバーが必要です。
- 必ず、以下の要件を検討してください。
  - 11 ページの『システム要件』
  - 14 ページの『必要なインストール権限』
  - 15 ページの『必要な通信ポート』

このタスクについて

制約事項 : Linux では、すべてのインストール場所が固定されています。コンポーネントのインストール・ディレクトリーを見つけるには、セクション 1 ページの『インストール可能コンポーネント』 を参照してください。

Data Protection for VMware は、Linux オペレーティング・システムに対して、以下のサイレント・インストール機能を提供します。

表 *7. Data Protection for VMware* のサイレント・インストール機能

機能	説明	デフォルトでインストール
Docs	README ファイル	可

表 7. *Data Protection for VMware* のサイレント・インストール機能 (続き)		
機能	**説明**	**デフォルトでインストール**
TDPVMwareDM	この機能のインストールには、使用可能化ファイルが含まれます。 IBM Spectrum Protect が、以下のバックアップ・タイプを実行することを可能にします。 • 定期的増分 VM バックアップ • フル VM 永久増分バックアップ • 増分永久増分 VM バックアップ バックアップ作業負荷をオフロードする場合は、このファイルを vStorage バックアップ・サーバーにインストールする必要があります。	可
TDPVMwareGUI	Data Protection for VMware vSphere GUI. **注 :** また、使用可能化ファイルのインストールも含まれます。	不可

手順

Data Protection for VMware をインストールするには、インストール・パッケージを解凍したディレクトリーから、以下のステップを実行します。

1. *path*`../Linux/DataProtectionForVMware/installer.properties` ファイルを開き、以下の項目のコメントを外し、ライセンスに同意します (*path* はインストール・フォルダー)。

   ```
   LICENSE_ACCEPTED=TRUE
   ```

2. 以下のいずれかの方法を選択して、Data Protection for VMware コンポーネントをインストールします。
   - デフォルト・インストールの場合は、`CD/Linux/DataProtectionForVMware` フォルダーを開き、以下のコマンドを入力します。

     ```
     ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
     ```

   - カスタム・インストールの場合は、以下の手順を実行します。
     a. 以下の手順に従い、適切な値を使用して `installer.properties` ファイルを編集します。
        1) **`INSTALL_MODE=Custom`** を指定します。必ず、このステートメントから番号記号 (#) を削除してください。
        2) **`CHOSEN_INSTALL_FEATURE_LIST`** オプションを使用して、インストールする機能を指定します。例えば、すべての機能をインストールする場合は、以下の値を使用します。

           ```
           CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
           ```

     b. `CD/Linux/DataProtectionForVMware` フォルダーから以下のコマンドを発行します。

        ```
        ./install-Linux.bin -i silent -f installer.properties
        ```

Data Protection for VMware のインストール後の最初のステップの実行

Data Protection for VMware をインストールした後は、構成の準備をします。Data Protection for VMware を構成する場合は、構成ウィザードを使用する方法をお勧めします。

構成ワークシート

Data Protection for VMware の構成と管理を行うときに必要な情報を記録するのに、このワークシートを使用します。 このワークシートは、構成後に、指定した値を覚えておくために役立ちます。

表 *8. Data Protection for VMware* の構成ワークシート

項目	値	注
IBM Spectrum Protect サーバー情報		
IBM Spectrum Protect サーバー・アドレス		
IBM Spectrum Protect サーバー・ポート		
IBM Spectrum Protect サーバー管理者 ID/パスワード		
IBM Spectrum Protect サーバー管理ポート		
ノード定義オプション		
ノードに追加する接頭部		
新規ノードの登録時に使用するポリシー・ドメイン		
vCenter ノードの名前/パスワード		
VMCLI ノードの名前/パスワード		
データ・センター・ノードの名前/パスワード **要確認 :** 複数のデータ・センター・ノードを作成できます。		データ・センター・ノード名は、指定された接頭部、下線文字、データ・センター名の順に構成された名前になります。 例えば、 *nodePrefix_datacenterName* のようになります。
vStorage バックアップ・サーバー上のデータ・ムーバー・ノードの名前/パスワード **要確認 :** 複数のデータ・ムーバー・ノードを作成できます。		データ・ムーバー・ノードは、データ・センター・ノード名、下線文字、DM の順に構成された名前になります。 例えば、 *datacenterNodename*_DM のようになります。
リモート・サーバー上のデータ・ムーバー・ノードの名前/パスワード **要確認 :** vStorage バックアップ・サーバー上にない複数のデータ・ムーバー・ノードを作成できます。		
マウント・プロキシー・ノード マウント・プロキシー・ノードは、データをリストアする際に使用されます。	Windows: Linux:	

Data Protection for VMware vSphere GUI へのアクセス

Data Protection for VMware vSphere GUI を使用して、VMware vCenter 環境内の仮想マシンのバックアップ、リストア、および管理を行います。

始める前に

Data Protection for VMware vSphere GUI にアクセスできるようにするには、インストール時に、vSphere 環境内のデータを保護するためのオプションを選択しておく必要があります。

手順

- インストール時に「**Web ブラウザーによる GUI へのアクセスを可能にする**」オプションを選択した場合は、ブラウザーから Data Protection for VMware vSphere GUI にアクセスできます。

  1. Web ブラウザーを開いて、以下の URL を入力します。

```
https://hostname:port/TsmVMwareUI
```

ここで、

- *hostname* は、Data Protection for VMware vSphere GUI がインストールされているシステムの名前です。
- *port* は、vSphere GUI にアクセス可能なポート番号です。デフォルトのポート番号は 9080 です。セキュア・ポートのデフォルトは 9081 です。

2. vCenter のユーザー ID およびパスワードを使用してログインします。

- インストール時に「**Web ブラウザーによる GUI へのアクセスを可能にする**」オプションを選択しなかった場合は、以下の手順を実行して Data Protection for VMware vSphere GUI を開始できます。

1. VMware vSphere Client を開き、vCenter のユーザー ID とパスワードを使用してログオンします。
2. vSphere Client の「**ソリューションとアプリケーション**」パネルで、Data Protection for VMware vSphere GUI アイコンをクリックします。

Data Protection for VMware のアップグレード

Data Protection for VMware を、このソフトウェアの旧バージョンからアップグレードすることができます。

以前のバージョンとの互換性については、技術情報 1993819 を参照してください。

バージョン 7.1.8 からのアップグレード : アップグレード・プロセス時に、既存の `jextract` ファイルを上書きするかどうかを尋ねるメッセージが表示された場合、「**すべてはい**」を選択します。

Data Protection for VMware のアップグレード

この手順は、Data Protection for VMware V8.1.10 にアップグレードする 方法について記載しています。

始める前に

重要 : このアップグレード手順は、IBM Spectrum Protect Snapshot for VMware がインストールされていないシステムに適用されます。

Data Protection for VMware をアップグレードするには、管理者特権が必要です。

既存の Data Protection for VMware vSphere GUI への更新は、以下のように処理されます。

- Data Protection for VMware vSphere GUI のアップグレード・プロセスが開始される前に、パラメーター・ファイルがバックアップされます。
- 同じ Derby データベースのポート番号と WebSphere® Application Server のデフォルトの基本ポート番号が使用されます。
- Linux プロファイル (`vmcliprofile`) の値が、Data Protection for VMware コマンド・ライン・インターフェース に使用されます。

制約事項 :

- Windows IBM Spectrum Protect for Virtual Environments がデフォルト以外の場所にインストールされている場合、アップグレード・プロセスでは、IBM Spectrum Protect for Virtual Environments V8.1.10 機能をデフォルトのインストール・ディレクトリーにインストールします。デフォルト以外の場所にアップグレードすることはできません。 各機能のデフォルトのインストール・ディレクトリーについては、1 ページの『インストール可能コンポーネント』のサブトピックを参照してください。
- Linux Windows アップグレード・プロセスでは、新規コンポーネントはインストールされません。

  例えば、前のバージョンで recovery agent GUI のみがインストールされている場合、アップグレード手順では、recovery agent コマンド・ライン・インターフェースはインストールされません 。このようなシナリオでは、インストール・プログラムを再実行してから、欠落しているコンポーネントのインストールを選択する必要があります。
- Linux Windows vCenter では、GUI ホストのドメイン名へのアクセス権限が必要です。

Data Protection vSphere プラグインをアップグレードするには、アップグレードに使用される GUI ホストのドメイン名が vCenter からアクセス可能でなければなりません。ドメイン名にアクセスできない場合、アップグレード後にプラグインの再登録が必要になります。

- Linux Linux 上の recovery agent のバージョンは、Windows プロキシー上の recovery agent と同じバージョンでなければなりません。したがって、Linux 上の recovery agent をアップグレードする場合は、Windows プロキシー上の recovery agent のバージョンもアップグレードする必要があります。

手順

Data Protection for VMware をアップグレードするには、以下の手順を実行します。

1. 実行中の Data Protection for VMware コンポーネントおよびサービスをすべて停止します。
2. すべてのマウント済み仮想ボリュームをアンマウントします。

   recovery agent GUI またはコマンド・ライン・インターフェース (**mount del** コマンド) を使用して、ボリュームをアンマウントできます。
3. 21 ページの『Windows システムへの Data Protection for VMware コンポーネントのインストール』の指示に従ってください。

   注 : Linux データ・ムーバー V6.x がインストールされている場合は、 V8.1.10 をインストールする前に、それをアンインストールする必要があります。 トピック「IBM Spectrum Protect Linux x86_64 クライアントのアンインストール」の指示に従ってください。
4. コード・パッケージをダウンロードします。
5. コード・パッケージを保存したフォルダーから、以下のようにアップグレード・プロセスを開始します。

   a) Windows

   `spinstall.exe` ファイルを実行します。

   b) Linux

   `install-Linux.bin` ファイルを実行します。

   1 つのマシンに 1 つの Data Protection for VMware vSphere GUI のみをインストールできます。 そのため、同一のマシンで複数の Data Protection for VMware vSphere GUI は許可されません。

サイレント・モードの Windows 64 ビット・システムでの Data Protection for VMware のアップグレード

サポートされている 64 ビット・オペレーティング・システムの Data Protection for VMware を、サイレント・アップグレードすることができます。

始める前に

Data Protection for VMware V6.x がデフォルト以外の場所にインストールされている場合、サイレント・アップグレード・プロセスでは、Data Protection for VMware V8.1.10 機能をデフォルトのインストール・ディレクトリーにインストールします。デフォルト以外の場所にサイレント・アップグレードすることはできません。 各機能のデフォルトのインストール・ディレクトリーについては、1 ページの『インストール可能コンポーネント』セクションのサブトピックを参照してください。

手順

Data Protection for VMware をアップグレードするには、以下の手順を実行します。

1. 稼働している Data Protection for VMware コンポーネントをすべて停止します。
2. すべてのマウント済み仮想ボリュームをアンマウントします。

   recovery agent GUI またはコマンド・ライン・インターフェース (**mount del** コマンド) を使用して、ボリュームをアンマウントできます。
3. すべてのマウント済み仮想ボリュームをアンマウントします。

   recovery agent GUI またはコマンド・ライン・インターフェース (**mount del** コマンド) を使用して、ボリュームをアンマウントできます。

4. コード・パッケージをダウンロードします。
5. Data Protection for VMware のフォルダーにナビゲートします。
6. コマンド・プロンプト・ウィンドウから以下のコマンドを入力します。
   ```
   spinstall.exe /silent REGISTER_EXTENSION=1 VCENTER_HOSTNAME=<hostname>
   VCENTER_USERNAME=<username> VCENTER_PASSWORD=<pass> /debuglog<file_path>
   ```

サイレント・モードの Linux システムでの Data Protection for VMware のアップグレード

サポートされている Linux オペレーティング・システムの Data Protection for VMware を、サイレント・アップグレードすることができます。

このタスクについて

サイレント・インストール機能では、以下の Data Protection for VMware パラメーターを使用します。

表 *9. Data Protection for VMware* サイレント・インストールのアップグレード・パラメーター

パラメーター	説明	デフォルト値
VCENTER_HOSTNAME	vCenter Server の完全修飾ドメイン名または IP アドレス	None
VCENTER_USERNAME	vCenter のユーザー ID。このユーザー ID は、拡張機能の登録および登録解除を行う権限を持った VMware 管理者でなければなりません。	None
VCENTER_PASSWORD	vCenter のパスワード。	None
DIRECT_START	Web ブラウザーで Data Protection for VMware vSphere GUI にアクセスするには、**DIRECT_START=YES** を指定します。Data Protection for VMware vSphere GUI には、GUI Web サーバーへの URL ブックマークを介してアクセスします。 Web ブラウザーで Data Protection for VMware vSphere GUI にアクセスしない場合は、**DIRECT_START=NO** を指定します。	YES **重要 :** アップグレードが完了した後は、製品を再インストールしない限り、**DIRECT_START** 値を変更することはできません。

手順

Data Protection for VMware をアップグレードするには、以下の手順を実行します。

1. アクティブなバックアップ・セッション、リストア・セッション、またはマウント・セッションがないことを確認します。
2. 既存の Data Protection for VMware vSphere GUI または recovery agent GUI がすべて閉じられていることを確認します。
3. コード・パッケージをダウンロードします。
4. Data Protection for VMware のフォルダーから、Linux フォルダーに移動します。
5. コマンド・プロンプト・ウィンドウから、適切なパラメーターを指定して `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` コマンドを入力します。
   例: `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true -DVCENTER_HOSTNAME=9.11.90.86 -DVCENTER_USERNAME=administrator@vsphere.local -DVCENTER_PASSWORD=**** -DREGISTER_EXTENSION=yes -DDIRECT_START=yes`

vCenter サーバーの Linked Mode 環境での Data Protection for VMware のアップグレード

Data Protection for VMware コンポーネントが現行の VMware Linked Mode 機能をサポートできるようにするには、すべての Data Protection for VMware GUI ホストがタイムリーに更新される必要があります。

このタスクについて

注 : この情報は、VMware vCenter で実行されている vSphere アプリケーションのバージョン 6.0、6.5、および 6.7 に固有のものです。

VMware vCenter Server Linked Mode は、サーバーが多数の仮想マシンをサポートできるように管理ゾーンの概要を表示するツールです。IBM Spectrum Protect Data Protection for VMware プラグインは、Linked Mode で実行される VMware と互換性があります。VMware のこの機能について詳しくは、vCenter Enhanced Linked Mode の VMware 資料を参照してください。

vCenter が Linked Mode である場合、vSphere UI にすべての vCenter の単一のビューが表示されます。 相互にリンクされている任意の vCenter にログインすることで、同じ UI を表示できます。そのため、IBM Spectrum Protect Data Protection プラグインは、単一の vCenter のみでインストールおよび構成されている場合でも、すべての vCenter で表示されます。

このプラグインはすべての vCenter で表示できますが、プラグインの機能を使用できるのは、IBM Spectrum Protect Data Protection for VMware GUI ホストに関連付けられている各 vCenter のみです。

vCenter Server Linked Mode 環境をアップグレードする 際、以下の問題を考慮してください。

- Linked Mode で vCenter を使用する場合、最初にアップグレードされる vCenter は、リンクされているすべての vCenter に表示される新しいレベルのプラグインになります。IBM Spectrum Protect Data Protection for VMware プラグインは、下位レベルのリリースの単一の GUI ホストと互換性があるように開発されています。例えば、Data Protection for VMware V8.1.6 プラグインは引き続き Data Protection for VMware V8.1.4 GUI ホストと互換性があります。
- 下位レベルの GUI ホストは引き続き新しいプラグインと連動しますが、新しいリリースに導入された機能は使用できません。新しいプラグインの全機能を使用できるようにするには、すべての GUI ホストをタイムリーに更新する必要があります。

例

バージョン 8.1.6 にアップグレードする 前は、vCenter1 および vCenter2 は Linked Mode です。それぞれに IBM Data Protection for VMware GUI ホストがあります。vSphere および GUI ホスト内のプラグインはバージョン 8.1.4 です。

vCenter1 は V8.1.6 にアップグレードされます。プラグインおよび GUI host1 は V8.1.6 になります。vCenter2 の vSphere にログインするユーザーには、V8.1.4 プラグインではなく、V8.1.6 プラグインが表示されます。 このユーザーは、「**IBM Spectrum Protect**」**->**「**構成**」**->**「**接続**」にナビゲートして、vCenter1 の GUI ホストは V8.1.6 であり、vCenter2 の GUI ホストはまだ V8.1.4 であることを確認できます。

Spectrum Protect プラグインは、vCenter2 で V8.1.4 であったときと同様に機能します。相違点は、vCenter2 の GUI ホストが V8.1.6 にアップグレードされるまでは、V8.1.6 の新機能を vCenter2 では使用できず、vCenter1 でのみ使用できることです。

Data Protection for VMware のアンインストール

Data Protection for VMware をアンインストールするプロセスは、新規インストールとアップグレード・バージョンで同じです。

Windows への Data Protection for VMware のアンインストール

Windows システムから Data Protection for VMware コンポーネントをアンインストールし、ファイルおよびディレクトリーを削除します。

始める前に

正常にアンインストールするために、以下のガイドラインに従ってください。

- 他の Data Protection for VMware Web GUI ホストが IBM Spectrum Protect vSphere Client プラグインを使用している場合は、Web クライアント拡張機能の登録を抹消しないでください。

このタスクについて

アンインストールの完了後、構成ファイルおよびプロパティー・ファイルは、C:¥Program Files¥IBM¥SpectrumProtect¥Framework¥VEGUI¥config ディレクトリーに配置されています。

手順

1. 稼働している Data Protection for VMware コンポーネントをすべて停止します。
2. すべてのマウント済み仮想ボリュームをアンマウントします。
3. データ・ムーバーの delete backup コマンドを使用して、既存の仮想マシンのバックアップをすべて削除します。
4. dsmcutil remove コマンドを使用して、インストール済みのデータ・ムーバー・サービスをすべて削除します。

   サービス・リストを確認するには、C:¥Program Files¥Tivoli¥TSM¥baclient¥ にアクセスして、コマンド dsmcutil list を実行してください。

   リスト・サービスには引用符付き名前を採用し、以下のようなコマンドを使用してサービスを削除します。

   ```
    dsmcutil remove /name:"TSM Remote Client Agent"
   dsmcutil remove /name:"TSM Client Acceptor"
   ```

5. 「**スタート**」 > 「**コントロール パネル**」 > 「**プログラムと機能**」 > 「**プログラムのアンインストール**」をクリックします。以下のプログラムをアンインストールします。
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware Suite
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware ライセンス
   - IBM Spectrum Protect JVM
6. ファイル・システムから以下の Data Protection for VMware ファイルおよびディレクトリー (存在する場合) を削除します。

   IBM Spectrum Protect for Virtual Environments V8.1.6 以上の場合、以下を削除します。

   ```
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   ```

   残りログ・ファイルおよび構成ファイルが必要なくなった場合、

   ```
   C:\Program Files\Tivoli\TSM
   ```

   も削除できます。これらのファイルを保持したい場合は、ファイルは C:\Program Files\Tivoli\TSM\baclient に配置されています。

   IBM Spectrum Protect for Virtual Environments V8.1.4 以前の場合、以下を削除します。

   ```
   C:\IBM\tivoli
   C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
   C:\Program Files\Common Files\Tivoli
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   ```

   残りログ・ファイルおよび構成ファイルが必要なくなった場合、

   ```
   C:\Program Files\Tivoli\TSM
   ```

も削除できます。これらのファイルを保持したい場合は、ファイルは C:\Program Files\Tivoli\TSM\baclient に配置されています。

次のタスク

すべてのコンポーネントがシステムから 削除されたことを確認します。

Windows 用 Data Protection for VMware のサイレント・モードでのアンインストール

Windows オペレーティング・システム 上の Data Protection for VMware をサイレント・アンインストールすることができます。

このタスクについて

アンインストールの完了後、構成ファイルおよびプロパティー・ファイルは、C:¥Program Files¥IBM¥SpectrumProtect¥Framework¥VEGUI¥config ディレクトリーに配置されています。

手順

Data Protection for VMware をアンインストールするには、以下の手順を実行します。

1. 稼働している Data Protection for VMware コンポーネントをすべて停止します。
2. すべてのマウント済み仮想ボリュームをアンマウントします。

   recovery agent GUI またはコマンド・ライン・インターフェース (**mount del** コマンド) を使用して、ボリュームをアンマウントできます。
3. コマンド・プロンプト・ウィンドウで以下を行います。
   - Data Protection for VMware vSphere GUI プラグインを登録解除して、Data Protection for VMware コンポーネントをアンインストールします。
     a. インストーラーの以下のディレクトリーに移動します。

     ```
     TSMVMWARE_WIN\DPVMware
     ```

     b. 次のを入力します。

     ```
     spinstall.exe /s /v"/qn REBOOT=ReallySuppress
     ```

     ```
     REMOVE=ALL UNREGISTER_EXTENSION=1
     ```

     ```
     VCENTER_HOSTNAME=<vCenter hostname or IP>
     ```

     ```
     VCENTER_USERNAME=<vCenter user name>
     ```

     ```
     VCENTER_PASSWORD=<vCenter password>"
     ```

   - Suite インストーラーを使用してすべての機能をアンインストールします。
     a. インストーラーの以下のディレクトリーに移動します。

     ```
     TSMVMWARE_WIN
     ```

     b. 次のを入力します。

     ```
     spinstall.exe /silent /remove
     ```

   注 : 完全アンインストールでは、上記に示したように Data Protection for VMware vSphere GUI を登録解除する必要があります。
4. アンインストールが完了したら、システムを再始動します。

Linux システムの Data Protection for VMware のアンインストール

Data Protection for VMware をアンインストールして、サポートされている Linux オペレーティング・システム上のファイルとディレクトリーを削除します。

始める前に

正常にアンインストールするために、以下のガイドラインに従ってください。

- IBM Spectrum Protect サーバーからノードを削除します。これは、Data Protection for VMware 製品のアンインストール前に行う必要があります。
  1. dsmadmc を /opt/tivoli/tsm/client/ba/bin/dsmadmc から実行します。
  2. ノードのファイル・スペースを削除するために、以下の del コマンドを使用することが必要な場合があります: `del file` *`nodename`* `*`
  3. ノードを照会する場合は、q コマンドを使用します: `q filespace` *`nodename`* `*`
  4. ノードを削除する場合は、rem コマンドを使用します: `rem node` *`nodename`*
- データ・ムーバー用に作成された dsmcad サービスを停止します。技術情報 http://www-01.ibm.com/support/docview.wss?uid=swg21358414 の指示に従います。
  1. dsmcad サービスが稼働中かどうかを確認する場合は、ps コマンドを使用します。`ps -ef|grep dsmcad`
  2. dsmcad サービスを停止する場合は、kill コマンドを使用します。`kill -9` *`dsmcad-processID`*
- データ・ムーバー・サービスの作成に関連するファイルをクリーンアップする必要があります。インストール・ディレクトリーに移り、以下のコマンドを発行します。

  ```
  /opt/tivoli/tsm/client/ba/bin/dsmutillnx cleanupDmFiles 1
  ```

  Enter を押してノード名を選択し、Enter を押して削除します。

  ノード名は dsm.sys で見つけることができます。
- VMware vSphere 5.5 環境から IBM Spectrum Protect vSphere Client プラグインをアンインストールすると、関連した特権ラベルと説明のみが削除されます。実際の特権はインストールされたままになります。この問題は、VMware の既知の制限です。詳しくは、次の VMware Knowledge Base の記事を参照してください。http://kb.vmware.com/kb/2004601。
- 製品がアンインストールされた後、Data Protection for VMware 使用可能化ファイルは除去されません。

このタスクについて

Linux システム上の Data Protection for VMware をアンインストールする場合、デフォルトで、アンインストールのタイプは元のインストールのタイプと同じプロセスです。別のアンインストール・プロセスを使用するには、正しいパラメーターを指定してください。例えば、サイレント・インストール・プロセスを使用した場合は、`–i swing` パラメーターを指定すると、インストール・ウィザードを使用してアンインストールできます。アンインストール・プロセスは、root ユーザーとして実行してください。root ユーザーのプロファイルを参照する必要があります。su コマンドを使用して root に切り替える場合は、`su -` コマンドで root プロファイルを参照します。

アンインストール・プロセスでプログラム・ファイルの除去が開始すると、アンインストール・プロセスを取り消しても、システムはクリーンな状態に戻りません。この状態により、再インストールしようとしても失敗する可能性があります。 そのため、35 ページの『Linux システムからの Data Protection for VMware の手動による除去』で説明されているタスクを実行してシステムをクリーンにしてください。

Data Protection for VMware をアンインストールするには、以下の手順を実行します。

手順

1. アンインストール・プログラムのディレクトリーに移動します。 以下のパスは、アンインストール・プログラムへのデフォルト・ロケーションです。/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/

2. インストールのタイプに応じて、以下のいずれかの方式で Data Protection for VMware をアンインストールします。

   注 : この手順のコマンドは 1 行で入力する必要があります。 以下の例では、ページのフォーマットに対応するために 2 行で表示されています。

   - インストール・ウィザードを使用して Data Protection for VMware をアンインストールするには、次のコマンドを入力します。

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
     ```

   - Data Protection for VMware のアンインストールにコンソールを 使用する場合、次のコマンドを入力します。

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
     ```

   - Data Protection for VMware をサイレントにアンインストールする 場合、次のコマンドを入力します。

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
     -f uninstall.properties
     ```

     `uninstall.properties` ファイルには、vCenter の接続情報が入っています。この情報は、Data Protection for VMware vSphere GUI をアンインストールする 場合に必要です。

Linux システムからの Data Protection for VMware の手動による除去

このタスクについて

標準のアンインストール手順を使用して Data Protection for VMware をアンインストールできない 場合は、以下のステップの説明に従って、システムから Data Protection for VMware を手動で除去する必要があります。 このプロセスを root ユーザーとして実行してください。

手順

1. Data Protection for VMware vSphere GUI をインストールした場合は、次のコマンドを使用して Package Manager データベースからそのパッケージを除去します。

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. 次のコマンドを使用して IBM Spectrum Protect API を除去します。

   ```
   rpm -e TIVsm-API64
   gskssl64.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. デプロイメント・エンジンから製品項目を除去します。

   a) 次のコマンドを発行して、すべての項目のリストを表示します。

   ```
   /usr/ibm/common/acsi/bin/de_lsrootiu.sh
   ```

   b) 次のコマンドを発行して、Data Protection for VMware に関連したインストール済み装置項目を除去します。

   ```
   /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>
   ```

   以下の装置項目が除去されていることを確認します。

   ```
   FBJRE
   TDPVMwareGUI
   JavaHelp
   TDPVMwareDM
   ```

   アンインストーラーが完了したら、(存在する場合) 以下のディレクトリーを削除します。

- /opt/tivoli/tsm/client
- /opt/tivoli/tsm/tdpvmware

ユーザー tdpvmware および関連付けられているディレクトリーを削除します。

- userdel tdpvmware
- /home/tdpvmware
- /etc/adsm

4. グローバル・レジストリー・ファイル (/var/.com.zerog.registry.xml) をバックアップします。

   ファイルがバックアップされた後、Data Protection for VMware に関連するすべてのタグを除去します。
5. インストール・ディレクトリー (/opt/tivoli/tsm/tdpvmware) にあるすべてのファイルを除去します。また、デスクトップ上のすべてのショートカットも除去します。
6. ファイル名に TDPVMware が含まれる、/root ディレクトリーにあるログ・ファイルをバックアップします。
   例えば、IA-TDPVMware-00.log または IA-TDPVMware_Uninstall-00.log です。

   これらのログ・ファイルをバックアップした後、除去します。ログ・ファイルを除去すると、インストール・プロセスが再度失敗する場合に発行されるエラーを表示することができます。
7. これで、22 ページの『Linux システムへの Data Protection for VMware のインストール』 の説明に従い製品を再度インストールできるようになりました。

既存の Data Protection for VMware インストール環境の変更

このセクションでは、既存の Data Protection for VMware インストール環境のパッケージと機能の変更方法について説明します。

Suite インストーラーを使用すると、基礎となるパッケージがシステムにインストールされている 間に変更を行うことが可能です。 個別のパッケージ機能のいずれかを変更するには、Windows の「**プログラムと機能**」コントロール パネルを使用できます。

既存の Data Protection for VMware インストール環境のパッケージの変更

Suite インストーラーを使用して、既存の Data Protection for VMware インストール環境のパッケージを変更することができます。

始める前に

Suite インストーラーを使用する前に、ソース・メディアをお手元にご用意ください。 Suite インストーラー用の spinstall.exe 実行可能ファイルは、インストール・パッケージのルートにあります。

このタスクについて

Suite インストーラーを使用して、既存の Data Protection for VMware インストール環境にインストールされているパッケージを変更します。 以下を追加または削除するように選択できます。

- データ・ムーバー
- Data Protection for VMware

以下のステップを実行してください。

手順

1. spinstall.exe ファイルをダブルクリックして、Suite インストーラー・パッケージを実行します。
2. 「**カスタム・セットアップ**」パネルで、パッケージのチェック・ボックスを使用して、インストールする必要があるパッケージを決定します。
3. このインストール環境に必要なパッケージを選択します。

既存の Data Protection for VMware インストール環境の機能の変更

Windows の「プログラムと機能」コントロール パネルを使用して、既存の Data Protection for VMware インストール環境の機能を変更することができます。

始める前に

インストール・パッケージを変更する前に、ソース・メディアをお手元にご用意ください。

このタスクについて

Windows を使用して、Data Protection for VMware の既存のインストール環境で、どの個別パッケージ機能を使用可能にするかを変更します。 以下の機能を変更するように選択できます。

- データ・ムーバー
- Data Protection for VMware

以下のステップを実行してください。

手順

1. Windows 「**コントロール パネル**」の「**プログラムと機能**」セクションで、IBM Spectrum Protect for Virtual Environments: Data Protection for VMware アプリケーションを右クリックします。
2. 「**変更**」をクリックし、現在インストールされているパッケージの機能を更新します。
3. このインストール環境に必要な機能を選択します。

第 2 章 Data Protection for VMware の構成

このセクションでは、Data Protection for VMware の構成と関連サービスの開始について説明します。

ヒント : Data Protection for VMware のインストール後、IBM License Metric Tool がデータ・ムーバーをカウントするのは、そのムーバーが IBM Spectrum Protect サーバーに接続されており、データ操作に使用されている場合のみです。 以降、そのデータ・ムーバーは常にライセンスの計算に含まれます。サーバーに接続されておらず、データ操作に使用されていないデータ・ムーバーは、ライセンスの計算から除外されます。

Windows でのウィザードを使用した新規インストールの構成

Windows で初期構成を行ったり、少量の変更を行うには、構成ウィザードを使用します。

始める前に

Linux のみの環境を使用するシステムの場合は、Linux でのウィザードを使用した新規インストールの構成を参照してください。

Data Protection for VMware がインストールされているシステムは、以下のサーバーへのネットワーク接続が必要です。

- リモート・データ・ムーバー
- IBM Spectrum Protect サーバー
- vCenter Server

このタスクについて

Data Protection for VMware 環境を構成するには、以下の手順を実行してください。

手順

1. Web ブラウザーを開き、GUI Web サーバーのアドレスを入力します。
   例えば、次のようにします。

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

2. vCenter のユーザー名およびパスワードを使用してログインします。
3. 「**始めに**」ウィンドウで、「**構成**」ウィンドウに移動し、「**構成ウィザードの実行**」をクリックします。
4. 「**要約**」ウィンドウが表示されるまで、ウィザードの各ページの指示に従います。 設定を確認して、「**完了**」をクリックし、構成を完了してウィザードを終了します。

   ヒント : それぞれの構成ページに関する情報は、GUI とともにインストールされるオンライン・ヘルプに記載されています。各 GUI ウィンドウの「**詳細情報**」をクリックすると、タスク・アシスタンスのオンライン・ヘルプが開きます。 「構成ウィザードの実行」トピックを参照してください。
5. 以下の手順に従って、データ・ムーバー・ノードが正しく構成されていることを確認します。
   a) 「**構成**」タブをクリックして「**構成状況**」ページを表示します。
   b) 「**構成状況**」ページでデータ・ムーバー・ノードを選択し、「**状況の詳細**」ペインでその状況を表示します。

      ノードに警告またはエラーが表示されている場合は、そのノードをクリックし、「**状況詳細 (Status Details)**」ペインの情報を使用して問題を解決します。 次に、ノードを選択してから「**選択したノードの検証 (Validate Selected Node)**」をクリックして、問題が解決したかどうか確認します。「**最新表示**」をクリックし、すべてのノードを再テストします。

タスクの結果

ファースト・パス : このウィザード・タスクを正常に完了した後は、VM データをバックアップするための追加の構成タスクは必要ありません。

Linux でのウィザードを使用した新規インストールの構成

Linux で初期構成を行ったり、少量の変更を行うには、構成ウィザードを使用します。

始める前に

Data Protection for VMware がインストールされているシステムは、以下のサーバーへのネットワーク接続が必要です。

- リモート・データ・ムーバー
- IBM Spectrum Protect サーバー
- vCenter Server

このタスクについて

Linux で Data Protection for VMware 環境を構成するには、以下の手順を実行します。

手順

1. Linux ホストでインストーラーを実行します。
2. オプション 2 および 3 (**データ・ムーバー** および **GUI**) を選択します。
3. インストールが完了したら、次の場所で構成ウィザードを実行します。

   ```
   https://localhost:9081/TsmVMwareUI
   ```

   セットアップを容易にするために、GUI ホスト上に定義するのはデータ・ムーバー 1 つのみにしてください。Web クライアント・プラグイン GUI を使用してさらに多くのデータ・ムーバーを追加または構成できるようにするには、事前にこのデータ・ムーバーを手動で構成する必要があります。

   注 : アップグレードを実行中であり、アップグレード前に作業中のデータ・ムーバー・インスタンスがあった場合には、サービスを再始動するだけです。これで Web クライアント・プラグインを今後の操作に使用できます。
4. ウィザードのパネルに入力中に、以下の情報を収集します。
   - 登録されたデータ・ムーバーおよびマウント・プロキシー・ペアのノード名およびパスワード。
   - 作成された各データ・ムーバーおよびマウント・プロキシーの `dsm.sys` のコンテンツ。
5. 構成ウィザードが完了したら、GUI ホストで実行されるデータ・ムーバーを手動でセットアップします。

   このステップ、およびステップ 6 および 7 については、 Linux 上の手動セットアップに関する情報を参照してください。トピック vSphere 環境でのデータ・ムーバー・ノードの手動設定を参照してください。
6. データ・ムーバー・インスタンスが実行されている場合は、GUI ホスト上で実行される Linux マウント・プロキシー・インスタンスを手動でセットアップします。
7. Linux マウント・プロキシー・インスタンスが実行されている場合は、Windows ホスト上に Windows マウント・プロキシー・インスタンスを手動でセットアップします。
8. これで Web クライアント・プラグインを今後の操作に使用できます。レガシー GUI インターフェースは、デフォルトの Spectrum Protect サーバー情報を変更または更新する場合に使用できます。

タスクの結果

ファースト・パス : このウィザード・タスクを正常に完了した後は、VM データをバックアップするための追加の構成タスクは必要ありません。

マルチサーバー環境の構成

単一の vSphere プラグインから、複数のバックアップ・サーバー全体のバックアップ、スケジュール、およびリストアの操作をすべて確認できるようになりました。

単一のビューからの複数のバックアップ・サーバーにわたるデータ保護環境全体のモニター

IBM Spectrum Protect のインストール後、セットアップ・ウィザードを使用して初期バックアップ・サーバーを構成することができます。このサーバーは、GUI ホスト上で Web アプリケーションとして実行されるため、デフォルトのバックアップ・サーバーとして指定されます。続いて、プラグインを使用して追加のバックアップ・サーバーを追加または削除することができます。デフォルトのバックアップ・サーバーは、プラグインから削除してはなりません。その後、vCenter にデータ・センターをサポートする複数の IBM Spectrum Protect バックアップ・サーバーを割り当てることができます。各データ・センターは、さまざまな Spectrum Protect サーバーのうちの 1 つのバックアップ・サーバーに関連付けられます。すべてのバックアップ・サーバーを、単一の vSphere プラグインまたは Data Protection for VMware GUI ホストから管理することができます。

デフォルトのバックアップ・サーバーの構成

IBM Spectrum Protect Data Protection for VMware のインストール後、構成ウィザードを使用して初期のデフォルト・バックアップ・サーバーをセットアップすることができます。

手順

1. インストール・ウィザードでプロセスを完了したら、「**Data Protection for VMware 構成の起動ウィザード**」チェック・ボックスを選択して、「**終了**」をクリックします。

   ウィザードは `https://localhost:9081/TsmVMwareUI/` という URL を使用して Web ブラウザーで起動されます。
2. vCenter 管理者資格情報を指定して Data Protection for VMware に対する認証を行います。
3. 「VMware vSphere vCenter」タブで、プラグインの登録の詳細を更新します。GUI ホスト・アドレスが、vCenter から ping できる有効なアドレスであることを確認します。
4. 「**サーバー資格情報**」タブに、デフォルトのバックアップ・サーバーの詳細を入力します。デフォルトのバックアップ・サーバーは、構成ウィザードが配置されている Web GUI (`https://localhost:9081/TsmVMwareUI/`) で使用されます。
5. 接頭語およびポリシー・ドメインを選択します。ベスト・プラクティスは、バックアップ・サーバーごとに異なる接頭部を選択することです。
6. デフォルト値を受け入れるか、または「**vCenter ノード**」タブおよび「**VMCLI ノード**」タブで名前を変更します。
7. 「**GUI ドメイン**」ペインで、「**管理対象データ・センター**」列に、デフォルト・サーバーがバックアップするデータ・センターのみを追加します。追加のバックアップ・サーバーが管理するデータ・センターがあればそれを省略します。
8. デフォルトを受け入れるか、または「**データ・ムーバー・ノード**」タブおよび「**マウント・プロキシー・ノード**」タブで名前を変更します。今後の手動による構成手順のために、データ・ムーバー・ノードとマウント・プロキシー・ノードのパスワードを適宜メモしておいてください。
9. オプションで、ファイル・リストアをこの段階でセットアップすることを選択できます。
10. 「**要約**」ページを確認し、「**終了**」をクリックして、構成プロセスを完了します。
11. オプションで、vSphere Client にログオンして構成を確認します。Client に直接ナビゲートすることも、構成画面で「**vSphere Web クライアントを開く (Open vSphere Web Client)**」ボタンをクリックすることもできます。

追加のバックアップ・サーバーの構成

IBM Spectrum Protect vSphere プラグインを使用して、追加のバックアップ・サーバーを構成することができます。

始める前に

注 : vSphere プラグインを使用して追加のバックアップ・サーバーを構成する場合は、SSL プロトコルをサポートするサーバーを使用する必要があります。

手順

1. Web GUI ホストの初期構成が完了したら、プラグインにログインし、IBM Spectrum Protect 構成にナビゲートします。
2. 「**構成**」 **->** 「**接続**」 をクリックして、プラグインと GUI ホストとの間の接続をセットアップします。
3. GUI ホストをポイントするように接続を編集します。

   接続が正常に完了したら、「**バックアップ・サーバー**」タブをクリックします。バックアップ・サーバーの情報を表示するには、表を更新することが必要な必要があります。更新後、 Web GUI ホストで構成されたデフォルト・サーバーが表示されます。
4. 追加のバックアップ・サーバーを作成するには、「**+**」(サーバーの追加) ボタンをクリックします。 2 番目のサーバーの情報を入力してください。
5. API およびサーバーに初めてアクセスする場合は、デジタル証明書を受け入れるようにプロンプトが出される場合があります。最初の証明書は、Web GUI ホストの REST API への接続を証明します。2 番目の証明書は、新規のバックアップ・サーバー自体を証明します。続行するためには両方の証明書を受け入れる必要があります。
6. ドロップダウン・リストからポリシー・ドメインを選択し、接頭部を選択します。ベスト・プラクティスは、バックアップ・サーバーごとに異なる接頭部を選択することです。
7. 要約画面で、選択内容を確認し、「**終了**」をクリックしてバックアップ・サーバーを追加します。
8. 「**結果**」ペインの「**データ・センターの関連の追加**」をクリックして、データ・センターを追加します。
9. 「**データ・センターの管理**」で、特定の vCenter 内のすべてのデータ・センターのリストを確認します。バックアップ・サーバーに関連付けるデータ・センターを選択します。「**関連の形成**」をクリックして、バックアップ・サーバーをデータ・センターに関連付けます。
10. 「**関連の形成**」をクリックし、そのデータ・センターに関連付ける必要があるサーバーの詳細を入力します。
11. データ・センター用のデータ・ムーバーを追加します。各データ・センターには独自のデータ・ムーバーが必要です。ただし、同じ 1 つのデータ・ムーバーのインストール済み環境を複数のデータ・センターに使用できます。「**データ・ムーバーの追加**」を選択して、データ・ムーバー・ペインに直接移動します。
12. 「**データ・ムーバー**」タブの「**データ・ムーバーの追加**」をクリックします。データ・ムーバー・ホストは、GUI ホスト・マシンにあっても構いません。別の選択肢としてデータ・ムーバーを別個にインストールすることもできます。
13. 最初のデータ・ムーバーがデータ・センターに追加されると、スケジュールが自動的に作成されます。
14. 「**構成**」 **->** 「**スケジュール**」をクリックします。 スケジュール表を更新して、新規スケジュールを確認します。

    追加のバックアップ・サーバーが構成され、Data Protection for VMware で使用できるようになりました。

追加のバックアップ・サーバーでのスケジュールの 作成

デフォルトのバックアップ・サーバーのセットアップ後、IBM Spectrum Protect vSphere プラグインを使用して、追加のバックアップ・サーバーを構成します。

始める前に

初期のデフォルト・スケジュールにはオブジェクトがありません。スケジュールには、バックアップを開始するためのタグ付きオブジェクトが必要です。

このタスクについて

1 つ以上のバックアップ・サーバーを構成したら、デフォルトのスケジュールを作成できます。このスケジュールを使用して、追加のバックアップ・サーバーを定義できます。追加スケジュールが必要な場合は、タグ付けと互換性があるスケジュールの作成の指示に従ってください。

各スケジュールは特定の 1 つのデータ・センターに関連付けられます。また各スケジュールには、1 つまたは複数のデータ・ムーバーを設定することができます。

手順

1. バックアップする、スケジュールのオブジェクトを 追加するには、そのスケジュールに関連付けられているデータ・センターに移動します。データ・センター・レベル以下でオブジェクトを選択するか、オブジェクトを右クリックし、「**IBM Spectrum Protect**」 **->** 「**データ保護の構成**」をクリックします。
2. 「**バックアップ・ポリシーの構成**」ペインで、そのオブジェクトのバックアップを 開始する新規スケジュールを選択します。
3. オブジェクトの関連付けが済んだら、以下の項目を確認します。
   - 「**構成**」 **->** 「**IBM Spectrum Protect**」表示画面をクリックした場合に、オブジェクトに正しい情報が表示されることを確認します。
   - 「**メニュー**」 **->** 「**IBM Spectrum Protect**」 **->** 「**構成**」 **->** 「**スケジュール**」をクリックして、選択したオブジェクトがスケジュールにリストされていることを 確認します。
   - スケジュールの実行後、オブジェクトに移動して「**モニター**」 **->** 「**IBM Spectrum Protect**」をクリックします。

   ヒント: オプションで、コマンド・ラインからスケジュールの開始時刻を更新するには、以下のアクションを実行します。

   a. dsmadmc ロケーションに移動します。`C:/Program Files/Tivoli/TSM/baclient`

   b. プロンプトが出された場合、そのサーバーに関連付けられているデータ・ムーバーの `dsm*opt` ファイルを見つけます。(`dir * opt`)

   c. コマンド `dsmadmc - optfile=dsm.datamovername.opt` を発行します。

   d. スケジュールを 10 分後に開始する場合は、以下のコマンドを入力します。

   ```
   update schedule policyDomain scheduleName StartTIME=NOW+00:10
   ```

随時バックアップの実行

複数の IBM Spectrum Protect バックアップ・サーバーの構成が完了したら、随時バックアップを実行することができます。

手順

1. バックアップをテストする 特定サーバーに関連付けられたデータ・センターを選択します。 そのデータ・センター内のオブジェクトに移動し、オブジェクトを右クリックして「**バックアップ**」をクリックします。
2. 必要なオプションを選択し、「**開始**」をクリックしてバックアップを開始します。
3. オプションで、vSphere の「**最近のタスク**」表で進行状況をモニターします。

4. オプションで、バックアップの完了後に、オブジェクト・バックアップを選択して「**モニター**」**->**「**IBM Spectrum Protect**」をクリックすると、状況を確認することができます。

随時リストア操作の実行

仮想マシン (VM) の IBM Spectrum Protect サーバーへのバックアップ後で、随時リストア操作を実行することができます。

手順

1. データ・センターを選択し、「**モニター**」 **->** 「**IBM Spectrum Protect**」を選択して、バックアップを持つ VM を判別します。

   VM すべてのリストおよびそのバックアップ状況を示すリストを含む表が示されます。
2. インベントリー内にバックアップを持つ VM を選択し、「**IBM Spectrum Protect**」 **->** 「**リストア**」を右クリックします。
3. リストア・ポイントを選択し、追加のオプションがあればそれを指定します。
4. リストア・ウィザードが完了したら、「**終了**」をクリックします。
5. オプションで、vSphere の「**最近のタスク**」ビューを使用してリストアの進行状況をモニターします。
6. オプションで、インベントリー内のリストア操作の状況を確認します。

ノートブックを使用した、既存のインストール済み環境の編集

「構成の編集」ノートブックを 使用して、既存の構成設定を編集します。

始める前に

「構成の編集」ノートブックには、以下の既存構成用タスクが提供されています。

- IBM Spectrum Protect 管理者 ID の設定または変更
- VMCLI ノードのパスワードのリセットおよびアンロック
- (vSphere 環境) Data Protection for VMware vSphere GUI ドメインに対する VMware データ・センターの追加または除去。
- マウント・プロキシー・ノードの追加または除去。既存のマウント・プロキシー・ノードのパスワードの変更。
- データ・ムーバー・ノードの追加または除去。既存のデータ・ムーバー・ノードのパスワードの変更。
- ファイル・リストアの有効化。
- データ・ムーバー・ノード用のタグ付けサポートの有効化。

このタスクについて

既存の構成を編集するには、以下のステップを実行します。

手順

1. Web ブラウザーを開き、GUI Web サーバーのアドレスを入力します。
   例えば、次のようにします。

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   vCenter のユーザー名およびパスワードを使用してログインします。
2. 「**始めに**」ウィンドウで、「**構成**」ウィンドウに移動し、「**構成の編集**」をクリックします。
3. 実行する編集タスクに関連したページに進み、指示に従います。別の「**構成設定**」ページに進む前に、「**OK**」をクリックして変更を保存する必要があります。 そうしないと、変更が有効になりません。

   重要 : 各構成ページに関する情報は、GUI と一緒にインストールされるオンライン・ヘルプで提供されています。 各 GUI ウィンドウの「**詳細情報**」をクリックすると、タスク・アシスタンスのオンライン・ヘルプが開きます。 「既存の構成の編集」トピックを参照してください。

タスクの結果
更新された設定が「**構成**」ウィンドウに表示されます。

Windows 環境でファイル・リストア操作を使用可能にする

管理者がファイル・リストア機能を有効にしている場合、ファイル所有者は支援を受けずにファイルをリストアできます。

始める前に

すべての前提条件が満たされていることを確認していない場合は、「*IBM Spectrum Protect for Virtual Environments: Data Protection for VMware* ユーザーズ・ガイド」のファイル・リストアの前提条件に関するトピックを確認してください。

このタスクについて

Data Protection for VMware vSphere GUI がインストールされているシステムで、以下の手順を実行します。

手順

1. Web ブラウザーを開いて GUI Web サーバー・アドレスを入力することにより、Data Protection for VMware vSphere GUI を開始します。
   例えば、次のようにします。

   ```
   https://<GUI web server address>:9081/TsmVMwareUI/
   ```

   vCenter のユーザー ID およびパスワードを使用してログインします。
2. 「**始めに**」ウィンドウで、 「**構成**」をクリックし、「**タスク**」リストからいずれかのタスクを選択します。
   - 新しい環境を構成する場合は、以下の手順を実行します。
     a. 「**クライアント構成ウィザードの実行**」を選択します。
     b. ウィザードの各ページの指示に従います。以下のガイドに従って、 「**ファイル・リストア**」ページに入力します。
        1) 「**ファイル・リストアを有効にする**」オプションを選択します。
        2) ファイル・リストア・インターフェースに 表示される管理者の連絡先情報を入力します。連絡先情報を提示したくない場合は、チェック・ボックスをクリアしてください。
        3) 環境に Windows 仮想マシンのバックアップが含まれている場合は、Windows ドメイン・ユーザーの資格情報を入力します。それ以外の場合は、チェック・ボックスをクリアして、資格情報を入力しないでください。

           ヒント : ファイル・リストア操作では、リモート仮想マシン上のネットワーク共有にアクセスするために、Windows ドメイン・ユーザーの資格情報を使用します。環境に Windows 仮想マシンのバックアップが含まれており、資格情報が入力されていないか、誤った資格情報が入力されている場合、操作は失敗します。そのため、このチェック・ボックスは、Windows 仮想マシンのバックアップが存在しない場合にのみクリアしてください。
        4) ファイル・リストア・インターフェースの URL をクリックして、インターフェースがアクセス可能であることを確認します。

           要確認 : ファイル・リストア・インターフェースの URL を記録して保持してください。ゲスト仮想マシンの所有者は、この URL を介してファイル・リストア・インターフェースにアクセスします。
        5) 「**OK**」をクリックして変更を保存します。
   - 既存の環境を更新する場合は、以下の手順を実行します。
     a. 「**TSM 構成の編集**」を選択します。
     b. 「**ファイル・リストア**」ページで、以下のガイドに従って操作します。

1)「**ファイル・リストアを有効にする**」オプションを選択します。

2) ファイル・リストア・インターフェースに 表示される管理者の連絡先情報を入力します。連絡先情報を提示したくない場合は、チェック・ボックスをクリアしてください。

3) 環境に Windows 仮想マシンのバックアップが含まれている場合は、Windows ドメイン・ユーザーの資格情報を入力します。それ以外の場合は、チェック・ボックスをクリアして、資格情報を入力しないでください。

   ヒント : ファイル・リストア操作では、リモート仮想マシン上のネットワーク共有にアクセスするために、Windows ドメイン・ユーザーの資格情報を使用します。環境に Windows 仮想マシンのバックアップが含まれており、資格情報が入力されていないか、誤った資格情報が入力されている場合、操作は失敗します。そのため、このチェック・ボックスは、Windows 仮想マシンのバックアップが存在しない場合にのみクリアしてください。

4) ファイル・リストア・インターフェースの URL をクリックして、インターフェースがアクセス可能であることを確認します。

   要確認 : ファイル・リストア・インターフェースの URL を記録して保持してください。ゲスト仮想マシンの所有者は、この URL を介してファイル・リストア・インターフェースにアクセスします。

5)「**OK**」をクリックして変更を保存します。

タスクの結果

この環境でファイル・リストア操作が可能になります。ファイル所有者は、この URL を使用して IBM Spectrum Protect ファイル・リストア・インターフェースへアクセスし 、これらのファイルをリストアできます。

Linux Linux でのファイル・リストア操作のセットアップ

Linux システム上に Data Protection for VMware をインストールするときにファイル・リストア機能を有効にするには、Data Protection for VMware 環境を Windows システム上に追加でセットアップする必要があります。

このタスクについて

Data Protection for VMware を Linux 環境内で実行する場合、ファイル・リストア機能を有効にするために Windows システム上にファイル・リストア機能をインストールする必要があります。

手順

1. ファイル・リストア機能に使用される別個の Windows サーバーをセットアップします。
2. Data Protection for VMware を Windows システムにインストールします。 インストール中はデフォルト値をそのまま受け入れます。
3. Data Protection for VMware を Windows システムで構成する場合、以下のノード名を使用します。
   a) VCENTER_FR という名前の vCenter ノードを作成します。
   b) VMCLI_FR という名前の VMCLI ノードを作成します。
   c) Linux 環境のデータ・センター・ノード名を再利用します。
   例えば、DATACENTER です。
   d) データ・ムーバー・ノードを作成しないでください。 このシナリオでは、ファイル・リストア機能にデータ・ムーバー・ノードは必要ありません。
   e) REMOTE_FR_MP_WIN および REMOTE_FR_MP_LNX という名前のマウント・プロキシー・ノードのペアを新たに作成します。
4. 構成ウィザードの「**ファイル・リストア**」ページで、「ファイル・リストアを有効にする（Enable File Restore）」 オプションを選択します。
5. ファイル・リストア・インターフェースにアクセスするには、Web ブラウザーを開き、管理者から提供された URL を入力します。
   例えば、次のようにします。

```
https:¥¥hostname:9081¥FileRestoreUI
```

ここで、hostname は、Data Protection for VMware がインストールされている Windows システムのホスト名です。

タスクの結果

以下の例は、IBM Spectrum Protect サーバーのプロキシー・ノードの関係を示します。

```
tsm: SERVER>q proxy

Target Node         Agent Node
---------------     ---------------------------------------------
VCENTER             VMCLI DATACENTER
VCENTER_FR          VMCLI_FR DATACENTER
DATACENTER          VMCLI VMCLI_FR
                     DATAMOVER1
                     REMOTE_MP_WIN REMOTE_MP_LNX
                     REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

ファイル・リストア機能を有効にするために作成された追加ノードには、_FR サフィックスが付きます。

Windows ファイル・リストア操作のオプションの変更

ファイル・リストア操作のリストア処理を管理者が構成および制御できるようにするには、frConfig.props ファイル内のオプションを変更します。

このタスクについて

Data Protection for VMware vSphere GUI がインストールされているシステムで、以下の手順を実行します。

手順

1. frConfig.props ファイルがあるディレクトリーに移動します。
   例えば、コマンド・プロンプトを開いて、 以下のコマンドを実行します。

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
   ```

2. テキスト・エディターを使用して管理者モードで frConfig.props ファイルを開き、必要に応じてオプションを変更します。
   47 ページの『ファイル・リストア・オプション』に記載されている情報を使用して、 変更するオプションを決定してください。
3. 変更を保存して、frConfig.props ファイルを閉じます。

タスクの結果

変更したオプションが、IBM Spectrum Protect ファイル・リストア・インターフェースに 適用されます。

ファイル・リストア・オプション

frConfig.props オプションは、ファイル・リストア操作の構成、サポート、リストア処理を制御します。

enable_contact_info=false | true
管理者の連絡先情報を提供するかどうかを指定します。この連絡先情報は、ファイル所有者がサポートを受ける際に使用できます。

false
ファイル所有者は、管理者の連絡先情報を受け取りません。この値がデフォルトです。

true
ファイル所有者は、管理者の連絡先情報を受け取ります。

enable_contact_info=true と指定する場合は、 **contact_info** オプションで情報を指定する必要があります。

enable_filerestore=false | true
ファイル所有者が IBM Spectrum Protect ファイル・リストア・インターフェースを 使用して、 仮想マシンにある自身のファイルをリストアできるかどうかを指定します。

false
ファイル所有者は、IBM Spectrum Protect ファイル・リストア・インターフェースを 使用して自身のファイルをリストアできません。この値がデフォルトです。

true
ファイル所有者は、IBM Spectrum Protect ファイル・リストア・インターフェースを 使用して自身のファイルをリストアできます。

maximum_mount_points=*num_mount_points*
ユーザー・アカウントが使用可能な同時リカバリー・ポイントの最大数を指定します。 最小値は 1 リカバリー・ポイントです。最大値は 256 マウント・ポイントです。デフォルト値は 2 マウント・ポイントです。

ヒント: 同時リストア操作で仮想マシンが複数回マウントされないようにするには、このオプション値を小さい値に設定します。

mount_session_timeout_minutes=*num_mins*
リストアおよびマウントされたリカバリー・ポイントがアイドル状態であることが可能な期間 (分) を指定します。この期間を超えると、セッションが取り消されます。 取り消されると、リカバリー・ポイントはアンマウントされます。最大値は、8 時間 (480 分) です。デフォルト値は 30 分です。

ヒント: セッションが予期せず取り消されることがないようにするには、この期間 (分数) を長くしてください。

restore_info_duration_hours=*num_hrs*
最新のリストア・アクティビティーに 関する情報を IBM Spectrum Protect ファイル・リストア・インターフェースで 保存する期間 (時間) を指定します。リストア・アクティビティー・ウィンドウを使用して、 エラー情報および最近完了したタスクを表示します。この情報は、 最近リストアされたファイルを検索する手段を提供します。最大値は 14 日間 (336 時間) です。デフォルト値は、1 週間 (168 時間) です。

contact_info=*administrator information*
ファイル所有者がサポートを受けるために使用できる管理者の連絡先情報を指定します。連絡先情報は、 IBM Spectrum Protect ファイル・リストア・インターフェースの 以下の場所に表示されます。

- ログイン・ウィンドウ
- ヘルプ・メニューの「**バージョン情報**」ペイン
- インターフェース ・メッセージ内のサポート情報リンク

以下のオプションは、Data Protection for VMware vSphere GUI 構成ウィザードまたはノートブックを 使用して上書きできます。

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

ファイル・リストア操作のログ・アクティビティーの 構成

ファイル・リストア操作のログの形式および記録方法を管理者が構成および制御できるようにするには、FRLog.config ファイル内のオプションを変更します。

始める前に

FRLog.config ファイルは、IBM Spectrum Protect ファイル・リストア・インターフェースに 初めてアクセスしたときに生成されます。

このタスクについて
Data Protection for VMware vSphere GUI がインストールされているシステムで、以下の手順を実行します。

手順

1. FRLog.config ファイルがあるディレクトリーに移動します。
   コマンド・プロンプトを開き、次のコマンドを発行します。

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
   ```

2. テキスト・エディターを使用して管理者モードで FRLog.config ファイルを開き、必要に応じてオプションを変更します。
   49 ページの『ファイル・リストア・ログ・アクティビティー ・オプション』に記載されている情報を使用して、 変更するオプションを決定してください。
3. 変更を保存して、FRLog.config ファイルを閉じます。
4. GUI Web サーバーを再始動する。
   a)「**スタート**」 > 「**コントロール パネル**」 > 「**管理ツール**」 > 「**サービス**」をクリックします。
   b)「**Data Protection for VMware Web サーバー・サービス**」を右クリックして、「**再始動**」をクリックする。

タスクの結果
ファイル・リストア操作に関するロギング情報の内容および形式に、設定が適用されます。

ファイル・リストア・ログ・アクティビティー ・オプション

FRLog.config オプションは、ファイル・リストア操作のロギング情報の内容および形式を制御します。

以下のオプションにより、ファイル・リストア・タスクに関する情報を fr_gui.log ログ・ファイルに記録します。

MAX_LOG_FILES=*number*
保存する fr_gui.log ファイルの最大数を指定します。デフォルト値は 8 です。

MAX_LOG_FILE_SIZE=*number*
fr_gui.log ファイルの最大サイズを KB で指定します。デフォルト値は 8192 KB です。

以下のオプションにより、ファイル・リストア・サービスに関する情報を fr_api.log ログ・ファイルに記録します。 これらのサービスは、ファイル・リストア・アクティビティーに 関連する内部 API サービスです。

API_MAX_LOG_FILES=*number*
保存する fr_api.log ファイルの最大数を指定します。デフォルト値は 8 です。

API_MAX_LOG_FILE_SIZE=*number*
fr_api.log ファイルの最大サイズを KB で指定します。デフォルト値は 8192 KB です。

API_LOG_FILE_NAME=*API_log_file_name*
API ログ・ファイルの名前を指定します。デフォルト値は fr_api.log です。

API_LOG_FILE_LOCATION=*API_log_file_name*
API ログ・ファイルのロケーションを指定します。ロケーションは、スラッシュ (/) を使用して指定する必要があります。 デフォルトのロケーションは C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs です。

FR.API.LOG=ON | OFF
ファイル・リストア・サービスのロギングを有効にするかどうかを指定します。

- ファイル・リストア・サービスのロギングを有効にする場合は、ON を指定します。デフォルト値は ON です。
- ファイル・リストア・サービスのロギングを無効にする場合は、OFF を指定します。

ファイル・リストア操作時に発生する可能性がある問題のトラブルシューティングについては、ファイル・リストアのトレース・オプション を参照してください。 FRLog.config ファイルにはトレース・オプションも指定されます。

タグ付けサポートのためのデータ・ムーバー・ノードの構成

データ・ムーバー・ノードでタグ付けサポートが有効にされている場合、管理者は、データ保護タグを VMware vCenter 内のインベントリー・オブジェクトに適用することができます。

始める前に

次の要件を満たしていることを確認してください。

- VMware vCenter Server は、バージョン 6.0 Update 1 以上でなければなりません。
- Data Protection for VMware vSphere GUI をタグ付けサポートを使用して正しく機能させるには、GUI のインストール時に以下の要件が満たされていることを確認してください。
  - 少なくとも 1 つのデータ・ムーバーと Data Protection for VMware vSphere GUI は、同じサーバー上にインストールされている必要があります。 vCenter Server の資格情報を保存するように、このデータ・ムーバー・ノードを構成する必要があります。 資格情報を保存するには、構成ウィザードを実行してデータ・ムーバー・ノードのパスワードを保存するか、データ・ムーバーのコマンド・ラインで **dsmc set password** コマンドを使用します。

    仮想マシンまたは物理マシンで追加のデータ・ムーバーとして実行する他のデータ・ムーバーを使用する場合、それらを他のサーバーにインストールできます。 タグ付けサポートを使用する場合、これらのデータ・ムーバーすべてを VMTAGDATAMOVER YES オプションを使用して構成することも必要です。 これらの追加データ・ムーバーをタグ・ベースのデータ・ムーバーとして正しく機能させるために、追加データ・ムーバーと同じサーバー上に Data Protection for VMware vSphere GUI をインストールする必要はありません。
  - Linux

    Linux データ・ムーバーの場合は、LD_LIBRARY_PATH 環境変数でデータ・ムーバー・インストール・ディレクトリーおよび Java™ 共有ライブラリー libjvm.so を指定する必要があります。データ・ムーバーで vmtagdatamover オプションを使用可能にする場合は、タグ付けサポートに libjvm.so へのパスが使用されます。 8.1.8 以降、新規スクリプト (spve.sh) が /etc/profile.d に追加されました。これにより、dsmc、 dsmcad、および dsmj の各アプリケーションに対する LD_LIBRARY パスが正しく設定されます。これは libjvm.so も対象となります。LD_LIBRARY_PATH に関するエラーが表示された場合は、以下の手動の手順に従ってください。

    1. IBM Java の場合:

       ```
       export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic
       ```

       Oracle Java の場合:

       ```
       export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server
       ```

    2. クライアント・アクセプター・サービスとデータ・ムーバー・スケジューラー・サービスを、vStorage バックアップ・サーバーとして機能するように構成するには、/etc/init.d/dsmcad ファイルに次の環境変数を設定します。

       ```
       export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
       ```

    注 : Linux オペレーティング・システムでは、デフォルトのユーザー名 (tdpvmware) を使用して Data Protection for VMware vSphere GUI をインストールする必要があります。
  - UNIX および Linux クライアントでは、TSM.PWD ファイル内の既存のパスワードは、同じロケーションの新規のパスワード・ストアにマイグレーションされます。 root ユーザーの場合、パスワード・ストアのデフォルト・ロケーションは /etc/adsm です。非 root ユーザーの場合、パスワード・ストアのロケーションは、passworddir オプションで指定されます。

TSM.PWD ファイルは、マイグレーション後に削除されます。

注 : タグ付けの処理に必要な特権の使用について詳しくは、Data Protection for VMware コンポーネントのインストールを参照してください。

このタスクについて

データ保護タグを使用して、VMware インベントリー・オブジェクト内の仮想マシンのバックアップ・ポリシーを構成することができます。 これらのデータ保護タグは、変更可能な設定として IBM Spectrum Protect vSphere Client プラグインに提示されます。

手順

- 以下のいずれかの方式を使用します。

オプション	説明
vSphere プラグイン GUI を使用してデータ・ムーバー・ノードを構成するには、以下のようにします	1. vSphere プラグインから、IBM Spectrum Protect を選択します。 2.「**構成**」タブで、「**データ・ムーバー**」を選択します。 3.「**データ・ムーバーの追加**」パネルで、ドロップダウン・メニューからデータ・センターを選択します。 4.「**データ・ムーバー名**」、「**データ・ムーバーのホスト名**」、「**vCenter ユーザー**」および「**vCenter のパスワード**」でデフォルトを受け入れるか、設定を編集します。 5. 設定が完了したら、「**追加**」をクリックします。 詳細は、「Data Protection for VMware vSphere GUI インストール・ガイド」のトピック『vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ』を参照してください。
Data Protection for VMware vSphere GUI を使用して、Windows または Linux のタグ付けサポートのために新規データ・ムーバーを構成する場合	1. Data Protection for VMware vSphere GUI がインストールされているシステムで、Web ブラウザーを開き、GUI Web サーバーのアドレスを入力して GUI を開始します。例えば次のとおりです。 `https://<GUI web server address>:9081/TsmVMwareUI/` 2. vCenter のユーザー ID およびパスワードを使用してログインします。 3.「**構成**」タブに進み、「**IBM Spectrum Protect 構成の編集**」アクションを選択します。 4. 構成ノートブックの「**データ・ムーバー・ノード**」ページに進みます。 5. 以下のステップを実行して、データ・ムーバー・ノードを追加します。 a. タグ付けサポートをセットアップしたいデータ・ムーバー・ノードに対して、「**サービスの作成**」を選択します。デフォルトでは、「**タグ・ベース・ノード**」が選択され、データ・ムーバー・ノードでタグ付けサポートが有効になっています。 b. タグ・ベースのノードをデフォルトのデータ・ムーバー・ノードとして指定するには、「**デフォルトのデータ・ムーバー**」を選択します。 デフォルトのデータ・ムーバー・ノードは、コンテナーが既に保護セットに属している場合、データ・センター内のコンテナーに追加されたすべての新規 VM をバックアップします。 デフォルトのデータ・ムーバーは、Data Mover タグが割り当てられていない保護セット内の VM もバックアップします。

オプション	説明
	ヒント: Linux システムで、新規データ・ムーバー・ノードをデフォルトのタグ付けノードとして選択した場合、そのデータ・センターに関連付けられている他のデータ・ムーバー・オプション・ファイルから vmtagdefaultdatamover 行を削除してください。 c.「**OK**」をクリックして変更を保存します。 vmtagdatamover オプションおよび vmtagdefaultdatamover (設定されている場合) オプションが、データ・ムーバー・オプション・ファイル (dsm.opt) に追加されます。
既存の Windows データ・ムーバー・ノードが Data Protection for VMware vSphere GUI と同じサーバー上にあるときに、ノードをタグ付けサポートのために構成する場合	1. 前述の手順のステップ 1 から 3 を完了し、タグ付けサポートのために新規データ・ムーバー・ノードを構成します。 2.「**データ・ムーバー・ノード**」ページで、タグ付けサポートを有効にしたいノードに対して「**タグ・ベース・ノード**」を選択します。 3. **オプション:** タグ・ベースのノードをデフォルトのデータ・ムーバー・ノードとして指定するには、「**デフォルトのデータ・ムーバー**」を選択します。
既存の Linux データ・ムーバー・ノードをタグ付サポートのために構成する場合、または Data Protection for VMware vSphere GUI と異なるサーバーにある既存の Windows データ・ムーバー・ノードを構成する場合	1. vmtagdatamover yes オプションをデータ・ムーバー・オプション・ファイル (Linux の場合は dsm.sys、Windows の場合は dsm.opt) に追加します。 2. **オプション:** タグ・ベースのノードをデフォルトのデータ・ムーバー・ノードとして指定するには、vmtagdefaultdatamover yes または vmtagdefaultdatamover *dm_name* オプションをデータ・ムーバー・オプション・ファイルに追加します。 **ヒント:** Linux システムで、新規データ・ムーバー・ノードをデフォルトのタグ付けノードとして選択した場合、そのデータ・センターに関連付けられている他のデータ・ムーバー・オプション・ファイルから vmtagdefaultdatamover 行を削除してください。

タスクの結果

データ・ムーバー・ノードがタグ付けサポートに対して有効になっている場合、データ・ムーバーはバックアップの実行時にタグ付け情報について VMware インベントリーを照会します。 その後、データ・ムーバーは、設定されているデータ保護タグに応じて仮想マシンをバックアップします。 データ・ムーバー・ノードがタグ付けサポート用に構成されていない場合、バックアップ操作時にすべてのデータ保護タグは無視されます。

関連情報

Vmtagdatamover
Vmtagdefaultdatamover
バックアップ・ポリシーの構成

仮想マシン全体のインスタント・リストア操作のための環境の構成

仮想マシン全体のインスタント・リストア操作およびインスタント・アクセス操作のために専用の iSCSI ネットワークをセットアップします。

始める前に

iSCSI 仮想スイッチおよび仮想マシン・ネットワークを構成する際に実行する特定のステップを確認するには、該当する VMware 資料 (ESXi または vSphere) を使用してください。 一般ガイドラインは提供されますが、仮想ネットワークおよび仮想スイッチの追加方法に関する固有の資料と説明は、製品資料に掲載されていません。 この資料の公開時点は、VMware vSphere ESXi および vCenter 5.5 の資料は、「VMware ESXi および vCenter Server 5 のドキュメント」で参照可能です。「ネットワーク構成」のトピックには、仮想スイッチと仮想ネットワークを追加および構成するための情報が記載されています。

重要 : これらの構成設定は、仮想マシンのフル・インスタント・リストアとインスタント・アクセスの操作が効率的に行われるように、VMware 環境のセットアップを支援するために提供されています。 ただし、これらの設定は VMware 構成タスクと VMware ユーザー・インターフェースに 適用されるので、詳細なステップバイステップの手順については、該当する VMware の資料を参照する必要があります。

このタスクについて

この手順では、インスタント・リストア操作に使用される各 ESXi ホスト上に iSCSI アダプターが必要です。 アダプターをセットアップするには 、該当する VMware 資料を使用してください。資料の公開時点では、以下の手順をこの VMware vSphere リソースで参照可能です。

- ソフトウェア iSCSI アダプターをセットアップするには 、VMware の説明「ソフトウェア iSCSI アダプタの構成」手順の指示に従ってください。
- ハードウェア iSCSI アダプターをセットアップするには 、VMware の説明「独立型ハードウェア iSCSI アダプタの設定」手順の指示に従ってください。

1. iSCSI ソフトウェアを ESXi ホストで構成する

手順

このタスクでは iSCSI ソフトウェアを基本的な構成でセットアップします。

1. インスタント・リストア操作に使用される ESXi ホストにログインします。
2. iSCSI アダプターが 使用可能になるまで、以下の VMware の Knowledge Base の記事の指示に従ってください。

   http://kb.vmware.com/kb/1008083
   IBM Spectrum Protect は、iSCSI ターゲット・サーバーを自動的にディスカバーします。
3. iSCSI アダプター (ESXi ホスト上) の IP アドレスは、データ・ムーバーに使用されるサブネット・アドレスと同じであることを確認します。
4. ESXi ホストで Storage vMotion ライセンスが有効であることを確認します。

次のタスク

iSCSI ソフトウェアを ESXi ホスト上をセットアップした後、データ・ムーバー・システム 上にアプリケーションをインストールして構成します。

2. データ・ムーバーへのアプリケーションのインストールと構成

始める前に

Recovery Agent および IBM Spectrum Protect データ・ムーバーがデータ・ムーバー・システムに既にインストールおよび構成されている場合は、ステップ 3 から開始してください。

手順

このタスクでは、インスタント・リストア操作のために、これらのアプリケーションと設定を使用して、データ・ムーバー・システムをセットアップします。

1. Recovery Agent および IBM Spectrum Protect データ・ムーバーを、データ・ムーバー・システムにインストールします。

   Data Protection for VMware のインストール手順のステップ 4 で、「**ゲスト内アプリケーション保護用の完全なデータ・ムーバーのインストール (Install a complete data mover for in-guest application protection)**」インストール・タイプを選択します。
2. データ・ムーバーを構成します。

   クライアントの資料のトピック「データ・ムーバーの構成」の指示に従います。
3. iSCSI サーバー IP アドレスを設定します。

   a) `C:¥Program Files¥Tivoli¥TSM¥baclient¥dsm.opt` ファイルに移動して、次のパラメーターを指定します。

   ```
   VMISCSIServeraddress=<IP address of the network card on the data mover
   system that exposes the iSCSI targets.>
   ```

   データ・ムーバー・システムに複数のネットワーク・カードがある場合、iSCSI ネットワークに正しいネットワーク・カードを指定するようにしてください。

次のタスク
データ・ムーバー・システムがセットアップされたら 、Recovery Agent CLI と Recovery Agent GUI 間の接続を設定してください。

3. Recovery Agent 接続の設定

始める前に
Recovery Agent コマンド・ライン・インターフェース (CLI) V7.1.x は、Recovery Agent GUI へのコマンド・ライン API と見なすことができます。Recovery Agent CLI を使用して、Recovery Agent GUI と通信できます。

手順

このタスクでは、Recovery Agent CLI と Recovery Agent GUI 間の接続を設定します。

1. データ・ムーバー・システムで Recovery Agent CLI を開始します。

   Windows の「**スタート**」メニューで、「**プログラム**」 > 「**IBM Spectrum Protect**」 > 「**IBM Spectrum Protect for Virtual Environments**」 > 「**IBM Spectrum Protect Recovery Agent**」をクリックします。
2. コマンド・プロンプト・ウィンドウに以下のコマンドを入力します。

   ```
   RecoveryAgentShell.exe -c set_connection mount_computer <IP address
   of the network card on the data mover system that exposes the iSCSI targets.>
   ```

   このコマンドは、Recovery Agent CLI と Recovery Agent GUI の間の接続を設定します。

次のタスク
接続の設定後、専用の iSCSI ネットワークを構成します。

4. ESXi ホストおよびデータ・ムーバーの専用の iSCSI ネットワークの構成

始める前に
このタスクを実行する前に、以下のガイドラインを確認してください。

- インスタント・リストア操作のために専用の iSCSI ネットワークを使用します。
- インスタント・リストア操作に使用される各 ESXi ホストには、使用可能な第 2 の物理ネットワーク・カードが必要です。 この第 2 のネットワーク・カードは、各 ESXi ホストのソフトウェア iSCSI アダプターにバインドされます。
- 仮想マシンで実行されているデータ・ムーバー・システムには、使用可能な第 2 のネットワーク・カードが必要です。 この第 2 のネットワーク・カードは、ESXi ホストのソフトウェア iSCSI アダプターにバインドされます。

- インスタント・リストア操作に使用される各 ESXi ホストには、使用可能な第 2 の VMware データ・ストアが必要です。 この一時データ・ストアは、操作時に作成された仮想マシンの構成情報とデータを保管しています。

手順

このタスクは、ESXi ホスト、および仮想マシンで実行されているデータ・ムーバーのための専用 iSCSI ネットワークをセットアップします。

1. インスタント・リストア操作に使用される ESXi ホストにログインします。
2. iSCSI ネットワークの仮想スイッチをセットアップします。
   以下のステップでは、仮想スイッチに *vSwitch1* を使用します。
   a) **「接続タイプ」** に「**VMkernel ネットワーク アダプタ**」を選択します。
   iSCSI ネットワークには、この接続タイプが必要です。
   b) **「VMkernel ネットワーク アクセス」** に「**vSphere 標準スイッチの作成**」を選択します。
   c) **「VMkernel 接続設定」** に「**ネットワーク ラベル**」を選択します。
   vSwitch1、およびこのネットワークが iSCSI トラフィック用であることを示すラベルを指定します。
   例: *VMkernel iSCSI*。
   d) **「VMkernel IP 接続設定」** に、*vSwitch1* の IP アドレスとサブネット・マスクを指定します。
   サブネット・マスクまたは **VMkernel デフォルト・ゲートウェイ**の値は変更しないでください。
   e) 運用する iSCSI ネットワークのカーネル・ポートを指定します。
3. 仮想マシン・ネットワークの仮想スイッチをセットアップします。
   以下のステップでは、仮想スイッチに *vSwitch0* を使用します。
   a) **「接続タイプ」** に「**仮想マシン**」を選択します。
   b) **「VMkernel ネットワーク アクセス」** に「**vSphere 標準スイッチの作成**」を選択します。
   c)「**ポート グループのプロパティ**」タブに移動して、「**ネットワーク ラベル**」を選択します。
   vSwitch1 仮想マシン・ネットワークに指定した同じラベルを指定します。
   例: *VMkernel iSCSI*。
4. 新しく作成した iSCSI アダプターを **「VMkernel ネットワーク アダプタ」** にバインドします。
   VMware の「iSCSI アダプタと VMkernel アダプタのバインド」手順の指示に従ってください。 この資料の公開時点では、この手順は「VMware ESXi および vCenter Server 5 のドキュメント」で参照可能です。

   ヒント: iSCSI デバイスのスキャン時にタイムアウトが発生した場合は、ESXi ホストに接続される iSCSI デバイスの数を減らします。 その後、iSCSI デバイスを再スキャンしてください。
5. iSCSI アダプターのバインディングのプロパティーが 正しいことを確認してください。
   a) VMware vSphere Client の「**ハードウェア**」 > 「**ストレージ アダプタ**」に移動します。
   b) iSCSI アダプターを右クリックして、「**iSCSI イニシエーターのプロパティ**」を選択します。 以下のバインディング・プロパティーが存在することを確認します。

表 *10. iSCSI* ネットワーク設定	
仮想マシン・ネットワーク	**iSCSI ネットワーク**
標準スイッチ: *vSwitch0*	**標準スイッチ**: *vSwitch1*
仮想マシンのポート グループ: *VM Network*	**VMkernel ポート**: *VMkernel iSCSI* **ヒント:** *VMkernel iSCSI* は、**VMkernel Adapter**: *vmk1* にバインドされます。これは **Physical Network Adapter**: *vmnic1* にあります。

表 *10. iSCSI* ネットワーク設定 *(*続き*)*	
仮想マシン・ネットワーク	**iSCSI ネットワーク**
物理アダプタ: *vmnic0*	**VMkernel ネットワーク アダプタ**: *vmk1*
	物理ネットワーク アダプタ: *vmnic1*
	仮想ネットワーク アダプタ **IP address**: 192.168.42.x (iSCSI ネットワークのサブネット)

タスクの結果
専用の iSCSI ネットワークが VM 全体のインスタント・リストアおよびインスタント・アクセス操作のために使用できるようになりました。

Data Protection for VMware のセキュリティー設定の構成

Data Protection for VMware データ・ムーバー、vmcli コマンド・ライン・インターフェース、および Data Protection for VMware vSphere GUI コンポーネントを使用するには、IBM Spectrum Protect サーバー とのセキュア接続を有効にするための構成が必要です。

データ・ムーバーと VMCLI のノードを IBM Spectrum Protect サーバー に接続するためのセキュリティー設定の構成

IBM Spectrum Protect サーバー V7.1.8 または V8.1.2 以降に接続する際に、データ・ムーバーと VMCLI のノードの Data Protection for VMware セキュリティー設定に関連して、いくつかの構成オプションがあります。これらのオプションのデフォルト値を受け入れると、拡張セキュリティー用にコンポーネントを容易に構成できます。これは、ほとんどのユース・ケースで推奨されます。

デフォルト・セキュリティー設定を使用した構成 (ファスト・パス)

ファスト・パスは、デフォルト値が受け入れられた際に、サーバーに対するデータ・ムーバー・ノードと VMCLI ノードの接続のセキュリティーに影響を与える構成オプション、および各種ユース・ケースの振る舞いを詳細に示します。 このファスト・パスのシナリオでは、エンドポイントにおける構成プロセスの手順が最低限になるように抑えています。

このシナリオでは、IBM Spectrum Protect サーバー **SESSIONSECURITY** パラメーターが **TRANSITIONAL** (初回接続時のデフォルト値) に設定されていると想定して、ノードの初回接続時にサーバーから証明書を自動的に取得します。このシナリオに従って、最初に IBM Spectrum Protect サーバー を V7.1.8 以降の V7 レベル、あるいは V8.1.2 以降の V8 レベルにアップグレードした後、Data Protection for VMware をこれらのレベルにアップグレードする (またはその逆) ことができます。

重要 : IBM Spectrum Protect サーバーが LDAP 認証用に構成されている場合、このシナリオは使用できません。LDAP が使用されている場合、dsmcert ユーティリティーを 使用して必要な証明書を手動でインポートできます。 詳細については、58 ページの『自動証明書配布を使用しない構成』を参照してください。

セッション・セキュリティーに影響するデータ・ムーバー・ノード・オプション

以下の dsmc オプションは、データ・ムーバー・ノードのセキュリティー設定を指定します。 これらのオプションについて詳しくは、クライアント・オプションのリファレンスを参照してください。

- SSLREQUIRED。 デフォルト値 Default を使用すると、V7.1.8 または V8.1.2 より前のバージョンのサーバーへの既存のセッション・セキュリティー接続が有効になり、認証に TLS を使用して V7.1.8 または V8.1.2 以降のサーバーに安全に接続するように Data Protection for VMware データ・ムーバーが自動的に構成されます。
- SSLACCEPTCERTFROMSERV。 デフォルト値 Yes を使用すると、データ・ムーバーがサーバーからの自己署名パブリック証明書を自動的に受け入れ、V7.1.8 または V8.1.2 以降のサーバーに接続する際に、その証明書を使用するようにデータ・ムーバーを自動的に構成できます。

- SSL。 デフォルト値 No を使用すると、データ・ムーバーと V7.1.8 または V8.1.2 より前のサーバー間でデータが転送される場合に、暗号化が使用されないことを指定します。データ・ムーバーが V7.1.8 または V8.1.2 以降のサーバーに接続する場合、デフォルト値 No を使用すると、オブジェクト・データが暗号化されないことを指定します。データ・ムーバーがサーバーと 通信する際に、他のすべての情報は暗号化されます。 値 Yes は、データ・ムーバーがサーバーと 通信する際に、オブジェクト・データなどのすべての情報を暗号化するために TLS が使用されることを指定します。
- SSLFIPSMODE。 デフォルト値 No を使用すると、連邦情報処理標準 (FIPS) 認定 TLS ライブラリーが不要であることを指定します。

また、以下のオプションはデータ・ムーバーが V7.1.8 または V8.1.2 より前のサーバーに対して TLS 接続を使用する場合のみ適用されます。これらのオプションは、データ・ムーバーが以降のサーバーに接続する場合は無視されます。

- SSLDISABLELEGACYTLS。 値 No は、SSL セッションで TLS 1.2 を必要としないデータ・ムーバーを示します。 これは、TLS 1.1 以下の SSL プロトコルでの接続を許可します。 データ・ムーバーが、V7.1.7 または V8.1.1 以下の IBM Spectrum Protect サーバー と通信する際は No がデフォルトです。
- LANFREESSL。 デフォルト値 No は、LAN フリー・データ転送が構成されている場合には、データ・ムーバーがストレージ・エージェントとの通信に TLS を使用しないことを示します。
- REPLSSLPORT。 データ・ムーバーが複製ターゲット・サーバーと通信する場合、TLS に対応した TCP/IP ポート・アドレスを指定します。

セッション・セキュリティーに影響する VMCLI ノード・オプション

以下のパラメーターは、VMCLI ノードのセキュリティー設定を指定します。 これらのオプションについて詳しくは、プロファイル・パラメーターを参照してください。

- VE_TSM_SSL。 デフォルト値 NO を使用すると、データ・ムーバーと V7.1.8 または V8.1.2 より前のサーバー間でデータが転送される場合に、暗号化が使用されないことを指定します。V7.1.8 より前のサーバーに接続する際にすべての情報を暗号化するため TLS を使用する場合は、この値を YES に設定してください。
- VE_TSM_SSLACCEPTCERTFROMSERV。 デフォルト値 YES を使用すると、インターフェースでサーバーからの自己署名パブリック証明書を自動的に受け入れ、V7.1.8 または V8.1.2 以降のサーバーにデータ・ムーバーが接続する際に、その証明書を使用するように自動的にインターフェースを 構成できます。
- VE_TSM_SSLREQUIRED。 デフォルト値 DEFAULT を使用すると、V7.1.8 または V8.1.2 より前のバージョンのサーバーへの既存のセッション・セキュリティー接続が有効になり、認証に TLS を使用して V7.1.8 または V8.1.2 以降のサーバーに安全に接続するようにインターフェースが 自動的に構成されます。

デフォルトのセキュリティー設定のユース・ケース

- 最初に、サーバーが V7.1.8 または V8.1.2 以降にアップグレードされます。その後、Data Protection for VMware がアップグレードされます。 その際、既存のデータ・ムーバーと VMCLI のノードが、SSL 通信を使用していない 場合は、以下のようになります。
  - データ・ムーバーと VMCLI のノードのセキュリティー・オプションに対しては変更が不要です。
  - ノードがサーバーで認証される際に、TLS を使用するように構成は自動的に更新されます。
- 最初に、サーバーが V7.1.8 または V8.1.2 以降にアップグレードされます。その後、Data Protection for VMware がアップグレードされます。 その際、既存のデータ・ムーバーと VMCLI ノードが SSL 通信を使用している 場合は、以下のようになります。
  - データ・ムーバーと VMCLI のノードのセキュリティー・オプションに対しては変更が不要です。
  - 既存のサーバーのパブリック 証明書との SSL 通信は引き続き使用されます。
  - SSL 通信は、サーバーで必要とされる TLS レベルを使用するように自動的に拡張されます。
- 最初に、Data Protection for VMware が V7.1.8 または V8.1.2 以降にアップグレードされます。次に、サーバーがアップグレードされます。 その際、既存のデータ・ムーバーと VMCLI のノードが、SSL 通信を使用していない 場合は、以下のようになります。
  - データ・ムーバーと VMCLI のノードのセキュリティー・オプションに対しては変更が不要です。

  - V7.1.8 または V8.1.2 より前のレベルのサーバーに対して既存の認証プロトコルが引き続き使用されます。
  - サーバーが V7.1.8 または V8.1.2 以降に更新された後、ノードがサーバーで認証される際に、TLS を使用するように構成は自動的に更新されます。
- 最初に、Data Protection for VMware が V7.1.8 または V8.1.2 以降にアップグレードされます。次に、サーバーがアップグレードされます。 その際、既存のデータ・ムーバーと VMCLI ノードが SSL 通信を使用している 場合は、以下のようになります。
  - データ・ムーバーと VMCLI のノードのセキュリティー・オプションに対しては変更が不要です。
  - V7.1.8 または V8.1.2 より前のレベルのサーバーに対して、既存のサーバーのパブリック 証明書との SSL 通信が引き続き使用されます。
  - サーバーが V7.1.8 または V8.1.2 以降に更新された後、SSL 通信は、サーバーで必要とされる TLS レベルを使用するように自動的に拡張されます。
- 最初に、Data Protection for VMware が V7.1.8 または V8.1.2 以降にアップグレードされます。その後、データ・ムーバーと VMCLI のノードが複数サーバーに接続されます。 その際、サーバーがそれぞれ異なる時点でアップグレードされる 場合、以下のようになります。
  - データ・ムーバーと VMCLI のノードのセキュリティー・オプションに対しては変更が不要です。
  - データ・ムーバーと VMCLI のノードは、V7.1.8 または V8.1.2 より前のバージョンのサーバーに対して既存の認証とセッション・セキュリティーのプロトコルを 使用します。そして、最初に V7.1.8 または V8.1.2 以降のサーバーに接続したときに TLS 認証を使用するように自動的にアップグレードされます。セッション・セキュリティーはサーバーごとに 管理されます。
- 新規クライアント・インストールでは (サーバーが V7.1.8 または V8.1.2 以降の場合)、以下のようになります。
  - 新規インストールに応じて Data Protection for VMware を構成します。
  - セキュリティー・オプションのデフォルト 値によって、TLS 暗号化セッション認証用に自動的にデータ・ムーバーと VMCLI のノードが構成されます。
  - クライアントとサーバー 間のすべてのデータ転送を暗号化する必要がある場合、SSL パラメーターを Yes 値に設定します。
- 新規クライアント・インストールでは (サーバーが V7.1.8 または V8.1.2 より前のバージョンの場合)、以下のようになります。
  - 新規クライアント・インストールに応じてクライアントを構成します。
  - データ転送すべての SSL 暗号化が必要とは限らない場合、クライアントのセッション・セキュリティー・パラメーターのデフォルト値を受け入れます。
    - サーバーが V7.1.8 または V8.1.2 以降にアップグレードされるまで 非 SSL 認証プロトコルが使用されます。
  - データ・ムーバーとサーバー 間のすべてのデータ転送を暗号化する必要がある場合、SSL パラメーターの値を Yes に設定し、引き続き手動によって SSL 用のデータ・ムーバーを構成します。
    - 構成の手順は、Secure Sockets Layer を使用した Tivoli Storage Manager クライアント/サーバー通信の構成 を参照してください。
    - サーバーが V7.1.8 または V8.1.2 以降に更新された後、SSL 通信は、サーバーで必要とされる TLS レベルを使用するように自動的に拡張されます。

自動証明書配布を使用しない構成

このシナリオでは、サーバーからの証明書の自動配布が受け入れられない場合に、データ・ムーバー および VMCLI のノードのセキュリティーに影響する構成オプションについて詳しく示します。例えば、サーバーが LDAP 認証を使用するように構成されている場合、または認証局 (CA) による署名が証明書に必要な場合には、サーバーからの証明書の自動配布が受け入れられません。

セッション・セキュリティーに影響するオプション

セキュリティー設定のオプションは、データ・ムーバー・ノードが初めて V7.1.8 または V8.1.3 以降のサーバーに接続する際にサーバーからの自己署名パブリック証明書を自動的に受け入れないようにするために、SSLACCEPTCERTFROMSERV オプションを No に設定する必要があるという点を除き、56 ページの『デフォルト・セキュリティー設定を使用した構成 (ファスト・パス)』で説明されているものと同じです。

自動証明書配布を使用しないデータ・ムーバー・ノードを構成するためのユース・ケース

自動証明書配布を行うことができない、あるいは必要ない場合は、dsmcert ユーティリティーを 使用して証明書をインポートします。 IBM Spectrum Protect サーバー または CA から必要な証明書を入手します。 CA には、VeriSign や Thawte などの企業から得られる証明書、またはお客様の社内で保守される内部 CA があります。

データ・ムーバーと VMCLI のノードが同じマシン上にある場合に必要な証明書は 1 つのみです。ノードがそれぞれ別のマシンにある場合、証明書はマシンごとに 1 つずつ必要です。

- 最初に、サーバーが V7.1.8 または V8.1.2 にアップグレードされます。その後、Data Protection for VMware がアップグレードされます。 その際、既存のデータ・ムーバーのノードが、SSL 通信を使用していない 場合は、以下のようになります。
  - 値 No を指定して SSLACCEPTCERTFROMSERV オプションを設定します。
  - IBM Spectrum Protect サーバー または CA から必要な証明書を入手し、dsmcert ユーティリティーを使用して証明書をインポートします。 構成の手順は、Secure Sockets Layer を使用した Tivoli Storage Manager クライアント/サーバー通信の構成 を参照してください。
- 最初に、サーバーが V7.1.8 または V8.1.2 にアップグレードされます。その後、Data Protection for VMware がアップグレードされます。 その際、既存のデータ・ムーバーのノードが SSL 通信を使用している 場合は、以下のようになります。
  - データ・ムーバーのノードのセキュリティー ・オプションに対しては変更が不要です。ノードに SSL 通信のためのサーバー証明書が既にある場合、SSLACCEPTCERTFROMSERV オプションは適用されません。
  - 既存のサーバーのパブリック 証明書との SSL 通信は引き続き使用されます。
  - SSL 通信は、サーバーで必要とされる TLS レベルを使用するように自動的に拡張されます。
- 最初に、Data Protection for VMware が V7.1.8 または V8.1.2 にアップグレードされます。次に、サーバーがアップグレードされます。 その際、既存のデータ・ムーバーのノードが、SSL 通信を使用していない 場合は、以下のようになります。
  - 値 No を指定して SSLACCEPTCERTFROMSERV オプションを設定します。
  - V7.1.8 または V8.1.2 より前のレベルのサーバーに対して既存の認証プロトコルが引き続き使用されます。
  - データ・ムーバーのノードを V7.1.8 または V8.1.2 以降のサーバーに接続する前に、以下を行います。
    - IBM Spectrum Protect サーバー または CA から必要な証明書を入手し、dsmcert ユーティリティーを使用して証明書をインポートします。 構成の手順は、Secure Sockets Layer を使用した Tivoli Storage Manager クライアント/サーバー通信の構成 を参照してください。
- 最初に、Data Protection for VMware が V7.1.8 または V8.1.2 にアップグレードされます。次に、サーバーがアップグレードされます。 その際、既存のデータ・ムーバーのノードが SSL 通信を使用している 場合は、以下のようになります。
  - データ・ムーバーのノードのセキュリティー ・オプションに対しては変更が不要です。ノードに SSL 通信のためのサーバー証明書が既にある場合、SSLACCEPTCERTFROMSERV オプションは適用されません。
  - V7.1.8 または V8.1.2 より前のレベルのサーバーに対して、既存のサーバーのパブリック 証明書との SSL 通信が引き続き使用されます。
  - サーバーが V7.1.8 または V8.1.2 以降に更新された後、SSL 通信は、サーバーで必要とされる TLS レベルを使用するように自動的に拡張されます。

- 最初に、Data Protection for VMware が V7.1.8 または V8.1.2 にアップグレードされます。その後、データ・ムーバーのノードが 複数サーバーに接続されます。その際、サーバーがそれぞれ異なる時点でアップグレードされる場合、以下のようになります。
  - 値 No を指定して SSLACCEPTCERTFROMSERV オプションを設定します。
  - V7.1.8 または V8.1.2 より前のレベルのサーバーに対して既存の認証プロトコルが引き続き使用されます。
  - データ・ムーバーのノードを V7.1.8 または V8.1.2 以降のサーバーに接続する前、または SSL 通信が任意のサーバー・レベルで必要な場合に、以下を行います。
    - IBM Spectrum Protect サーバー または CA から必要な証明書を入手し、dsmcert ユーティリティーを使用して証明書をインポートします。 構成の手順は、Secure Sockets Layer を使用した Tivoli Storage Manager クライアント/サーバー通信の構成 を参照してください。
  - データ・ムーバーのノードは、V7.1.8 または V8.1.2 より前のバージョンのサーバーに対して既存の認証とセッション・セキュリティーのプロトコルを使用します。そして、最初に V7.1.8 または V8.1.2 以降のサーバーに接続したときに TLS 認証を使用するように自動的にアップグレードされます。セッション・セキュリティーはサーバーごとに 管理されます。
- 新規 Data Protection for VMware インストールでは (サーバーが V7.1.8 または V8.1.2 以降の場合)、以下のようになります。
  - 新規インストールに応じて Data Protection for VMware を構成します。
  - 値 No を指定して SSLACCEPTCERTFROMSERV オプションを設定します。
  - IBM Spectrum Protect サーバー または CA から必要な証明書を入手し、dsmcert ユーティリティーを使用して証明書をインポートします。 構成の手順は、Secure Sockets Layer を使用した Tivoli Storage Manager クライアント/サーバー通信の構成 を参照してください。
  - データ・ムーバーとサーバー間のすべてのデータ転送を暗号化する必要がある場合、SSL パラメーターを Yes 値に設定します。
- 新規 Data Protection for VMware インストールでは (サーバーが V7.1.8 または V8.1.2 より前のバージョンで、SSL 暗号化セッションが必要 な場合)、以下のようになります。
  - 新規インストールに応じて Data Protection for VMware を構成します。
  - SSL パラメーターを Yes 値に設定します。
  - IBM Spectrum Protect サーバー または CA から必要な証明書を入手し、dsmcert ユーティリティーを使用して証明書をインポートします。 構成の手順は、Secure Sockets Layer を使用した Tivoli Storage Manager クライアント/サーバー通信の構成 を参照してください。
- 新規 Data Protection for VMware インストールでは (サーバーが V7.1.8 または V8.1.2 より前のバージョンで、SSL 暗号化セッションが必要ない 場合)。以下のようになります。
  - 新規インストールに応じて Data Protection for VMware を構成します。
  - 値 No を指定して SSLACCEPTCERTFROMSERV オプションを設定します。
    - サーバーが V7.1.8 または V8.1.2 以降にアップグレードされるまで 非 SSL 認証プロトコルが使用されます。
  - データ・ムーバーのノードを V7.1.8 または V8.1.2 以降のサーバーに接続する前に、以下を行います。
    - IBM Spectrum Protect サーバー または CA から必要な証明書を入手し、dsmcert ユーティリティーを使用して証明書をインポートします。 構成の手順は、Secure Sockets Layer を使用した Tivoli Storage Manager クライアント/サーバー通信の構成 を参照してください。

Transport Layer Security を使用した Data Protection for VMware vSphere GUI 通信の構成

Data Protection for VMware vSphere GUI は、 Transport Layer Security (TLS) プロトコルを使用して、Web ブラウザー、VMware vCenter Server、およびオプションで IBM Spectrum Protect サーバー とのセキュア通信を提供します。

このタスクについて

Web ブラウザーと VMware VCenter Server との通信の場合、常に TLS プロトコルが有効になります。Data Protection for VMware のインストール時、自己署名 TLS デジタル証明書が生成され、接続に使用されます。

また、認証局 (CA) によって署名された証明書を使用して Web ブラウザーと通信することも可能です。Data Protection for VMware CA の証明書を使用するには、Web ブラウザー・セッション用のサード・パーティー証明書の使用を参照してください。

IBM Spectrum Protect サーバー との通信の場合、TLS プロトコルを使用するかどうは、サーバーのバージョンによって異なります。

IBM Spectrum Protect サーバー V7.1.7 または V8.1.1 以前を使用している場合
サーバーとの通信の際の TLS プロトコルの使用はオプションです。 61 ページの『IBM Spectrum Protect サーバーとのセキュア通信の使用可能化』 の説明に従って、トラストストアを作成して更新し、証明書をインポートすることで、TLS プロトコルを介してサーバーと通信するために Data Protection for VMware vSphere GUI を手動で有効にできます。

IBM Spectrum Protect サーバー V7.1.8 または V8.1.2 以降を使用している場合
TLS プロトコルは必須です。 多くの場合、56 ページの『デフォルト・セキュリティー設定を使用した構成 (ファスト・パス)』 に示すデフォルトのセキュリティー設定を使用することで、トラストストアは初回使用時に自動的に作成されます。ただし、シナリオによっては、トラストストアを手動で作成することが必要な場合があります。

重要 : ファスト・パスのシナリオでは、IBM Spectrum Protect サーバー **SESSIONSECURITY** パラメーターが **TRANSITIONAL** (初回接続時のデフォルト値) に設定されていると想定して、Data Protection for VMware vSphere GUI のサーバーとの初回接続時に自動的に証明書を取得します。GUI がサーバーに接続されると、**SESSIONSECURITY** パラメーターは **STRICT** に設定されます。 GUI ではサーバーに接続する際にサーバー管理者 ID を使用するので、別のエンティティーが 接続用にその ID を使用していた場合、サーバーへの接続の試行時に GUI にエラー・メッセージが表示されます。この問題を解決するには、**SESSIONSECURITY** パラメーターを **TRANSITIONAL** に戻します。

IBM Spectrum Protect サーバーとのセキュア通信の使用可能化
IBM Spectrum Protect サーバー V7.1.7 以前、または V8.1.2 以前を使用している場合、TLS プロトコルを使用したサーバーへの接続はオプションであり、このプロトコルを使用したサーバーとの Data Protection for VMware vSphere GUI 通信を有効にする場合は、通信を手動で有効にしなければなりません。

始める前に
サーバー管理者から証明書のコピーを入手します。

このタスクについて

V7.1.8 または V8.1.2 以降のサーバーを使用する場合、TLS プロトコルは必須であり、証明書を使用するトラストストアは、56 ページの『デフォルト・セキュリティー設定を使用した構成 (ファスト・パス)』 で説明したデフォルトのセキュリティー設定を使用することで、最初の使用時に自動的に作成されます。ただし、シナリオによっては、このトピックの説明に従ってトラストストアを手動で作成し、Data Protection for VMware vSphere GUI を構成することが必要な場合があります。

以下の手順では、Java™ キーと証明書管理ツール **keytool** を使用します。

Linux オペレーティング・システムの場合、ツールは `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/` ディレクトリーにあります。

Microsoft Windows オペレーティング・システムの場合、ツールは、`C:¥Program Files¥Common Files¥tsm¥Tivoli¥TSM¥jvm80516¥jre¥bin` ディレクトリーにあります。

keytool コマンドを実行するときに、絶対パスの指定が必要になる場合があります。

手順

1. コマンド・ラインで、トラストストアのロケーションのディレクトリーに 移動します。
   - Linux の場合: `/opt/tivoli/tsm/tdpvmware/common/scripts/`

- Windows の場合: `C:¥Program Files¥IBM¥SpectrumProtect¥Framework¥VEGUI¥scripts¥`

2. トラストストアを作成し、以下のコマンドを指定して証明書をインポートします。

```
keytool -importcert -alias my-cert -file cert.pem -keystore
tsm-ve-truststore.jks -storepass password
```

各構成要素について説明します。

-alias *my-cert*
トラストストア内の証明書を識別する固有の別名。

-file *cert.pem*
サーバー自己署名証明書または CA ルート証明書が含まれているファイル。

-storepass *password*
鍵ストアのパスワード。後で使用できるように、必ずこのパスワードを覚えておいてください。

3. Data Protection for VMware vSphere GUI を開始して、「**構成**」ウィンドウに進みます。
   - 初期構成を作成している場合は、「**タスク**」 > 「**IBM Spectrum Protect 構成ウィザードの実行**」をクリックして、「**サーバー資格情報**」ページに進みます。
   - 既存の構成を変更している場合は、「**タスク**」 > 「**IBM Spectrum Protect 構成の編集**」をクリックして、「**サーバー資格情報**」ページに進みます。
4. 「**IBM Spectrum Protect 管理ポート**」フィールドにポート番号を入力します。これは、SSL または TLS を使用した管理接続を許可するサーバー・ポートです。
5. 「**管理ポートで暗号化通信を使用する**」を選択します。
6. この設定を後の GUI セッションで使用する場合は、「**管理者 ID、パスワード、ポート設定の保存 (Save the administrator ID, password, and port settings)**」を選択します。
7. 「**OK**」をクリックして変更を適用します。

認証局からの証明書の使用
認証局 (CA) によって署名された証明書を使用するには、複数の手順を実行する必要があります。

このタスクについて

以下の手順では、標準鍵と、**keytool** と呼ばれる証明書管理ツールを使用します。

Linux オペレーティング・システムの場合、これは `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/` ディレクトリーにあります。

Microsoft Windows オペレーティング・システムの場合、これは `C:¥Program Files¥Common Files¥tsm¥Tivoli¥TSM¥jvm80516¥jre` ディレクトリーにあります。

コマンド・ラインから **keytool** を実行するときに、絶対パスの指定が必要になる場合があります。

手順

1. 鍵ストアへのアクセス権限を取得します。
2. 証明書署名要求 (CSR) を作成します。
3. 署名を得るために証明書署名要求を認証局に送信します。
4. 署名付き証明書を Data Protection for VMware vSphere GUI に受信します。

鍵ストアへのアクセス権限の取得

証明書は Java 鍵ストアに保管されます。鍵ストア・コンテンツはパスワードで保護されています。鍵ストア内の証明書を取り扱うには、鍵ストアへのアクセス権限を取得する必要があります。

このタスクについて

デフォルトの自己署名証明書および鍵ストア・パスワードは、インストール時に自動的に生成されるため、ユーザーが初期パスワードを知ることはほとんどありません。

元の鍵ストアを新規鍵ストアおよび新規自己署名証明書で置き換えるには、以下の手順を実行します。新規鍵ストアは、ユーザーが選択したパスワードで保護されています。

すでに鍵ストア・パスワードがわかっている場合は、この手順をスキップしてください。

手順

1. Data Protection for VMware vSphere GUI サービスを停止します。
2. コマンド・ラインで、鍵ストアのロケーションのディレクトリーに移動します。
   - Linux の場合: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Windows の場合: `C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥resources¥security¥`
3. 鍵ストア・ファイル (`key.jks`) のバックアップ・コピーを作成して、そのコピーを名前変更するか、別のロケーションに移動します。
4. 次のコマンドを発行して、新規鍵ストアおよび新規自己署名証明書を作成します。

   ```
   keytool -genkeypair -alias vekey -dname
   CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
   -sigalg SHA256withRSA -keysize 2048 -validity days -keystore
   key.jks -storepass password -keypass password
   ```

   各構成要素について説明します。

   -dname CN=*fqdn*,OU=Tivoli_Storage_Manager_for_VMware,O=IBM
   fqdn は、Data Protection for VMware vSphere GUI がインストールされているコンピューターの DNS 名または完全修飾ドメイン名です。

   -validity *days*
   証明書の有効期間。

   -storepass *password*
   鍵ストアのパスワード。後で使用できるように、必ずこのパスワードを覚えておいてください。

   -keypass *password*
   証明書の秘密鍵パスワード。このパスワードは鍵ストア・パスワードと一致しなければなりません。
5. **securityUtility** ツールを使用して、鍵ストア・パスワードをエンコードします。次のコマンドを発行します。
   - Linux の場合: `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
   - Windows の場合: `C:¥IBM¥SpectrumProtect¥webserver¥bin¥securityUtility.bat encode`

   プロンプトが出されたら鍵ストア・パスワードを入力し、出力を (クリップボードにコピーするなどして) 保存します。
6. エディターで `bootstrap.properties` ファイルを開いて、`veProfile.keystore.pswd` プロパティーを前のステップでエンコードした値に設定します。

   `bootstrap.properties` ファイルは、以下の場所にあります。
   - Linux の場合: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`
   - Windows の場合: `C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥`
7. Data Protection for VMware vSphere GUI サービスを開始します。

関連資料

81 ページの『Data Protection for VMware のサービスの開始と実行』

デフォルトでは、Windows オペレーティング・システムを始動すると、ローカル・システム・アカウントで recovery agent が開始されます。

証明書署名要求の作成

鍵ストアへのアクセス権限を取得した後で、証明書署名要求 (CSR) を作成する必要があります。

手順

CSR を作成するには、以下の手順を実行します。

1. コマンド・ラインで、鍵ストアのロケーションのディレクトリーに移動します。
   - Linux の場合: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Windows の場合: `C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥resources¥security¥`
2. 次のコマンドを発行して、新規証明書を作成します。

   ```
   keytool -genkeypair -alias mykey -dname
   CN=fqdn,OU=unit,O=organization -keyalg RSA -sigalg SHA256withRSA
   -keysize 2048 -validity days -keystore key.jks -storepass
   password -keypass password
   ```

   各構成要素について説明します。

   -alias *mykey*
   mykey は、鍵ストア内の証明書を識別する固有の別名です。これは、署名付き証明書の受信時に名前変更されます。

   -dname CN=*fqdn*,OU=*unit*,O=*organization*
   fqdn は、Data Protection for VMware vSphere GUI がインストールされているコンピューターの DNS 名または完全修飾ドメイン名です。

   unit および *organization* は、ポリシーまたは認証局によって要求される組織情報です。

   -validity *days*
   証明書の有効期間。

   -storepass *password*
   鍵ストアのパスワード。鍵ストア・パスワードが不明な場合、または忘れた場合は、62 ページの『鍵ストアへのアクセス権限の取得』を参照してください。

   -keypass *password*
   証明書の秘密鍵パスワード。このパスワードは鍵ストア・パスワードと一致しなければなりません。
3. 次のコマンドを発行して、CSR を作成します。

   ```
   keytool -certreq -alias mykey -file certreq.pem -keystore key.jks
   ```

   各構成要素について説明します。

   -alias *mykey*
   前のステップで使用した証明書別名。

   -file *certreq.pem*
   証明書署名要求を保管するファイル。

認証局への証明書署名要求の送信

証明書要求(`certreq.pem`) の作成後に、その要求を署名対象の認証局に送信する必要があります。その認証局固有の手順に従ってください。

署名付き証明書の受信

認証局 (CA) から署名付き証明書を取得した後に、鍵ストアに証明書を受信する必要があります。

手順

署名付き証明書を受信するには、以下の手順を実行します。

1. コマンド・ラインで、鍵ストアのロケーションのディレクトリーに移動します。
   - Linux の場合: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Windows の場合: `C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥resources¥security¥`
2. CA から受信したファイルを、このロケーションにコピーします。これらのファイルには、Data Protection for VMware vSphere GUI の CA ルート証明書、中間 CA 証明書 (ある場合)、および署名付き証明書が含まれています。
3. Data Protection for VMware vSphere GUI サービスを停止します。
4. 鍵ストア・ファイル (`key.jks`) を別の名前でコピーするか、別のロケーションにコピーして、鍵ストア・ファイルのバックアップ・コピーを作成します。
5. 中間 CA 証明書がある場合は、以下のコマンドを使用してインポートします。証明書の承認を求めるプロンプトが出された場合は、*yes* と応答します。必要に応じて、複数の中間 CA に対してこのステップを繰り返します。

   ```
   keytool -importcert -alias ca-intermediate -file intermediate.pem
   -keystore key.jks -storepass password
   ```

   各構成要素について説明します。

   -alias *ca-intermediate*
   鍵ストア内の証明書を識別する固有の別名。各中間証明書に固有の別名を指定する必要があります。

   -file *intermediate.pem*
   CA から取得した中間証明書ファイル。

   -storepass *password*
   鍵ストアのパスワード。
6. 次のコマンドを発行して、CA ルート証明書をインポートします。証明書の承認を求めるプロンプトが出された場合は、*yes* と応答します。

   ```
   keytool -importcert -alias ca-root -file root.pem -keystore
   key.jks -storepass password
   ```

   各構成要素について説明します。

   -alias *ca-root*
   鍵ストア内の証明書を識別する固有の別名。

   -file *root.pem*
   CA から取得したルート証明書ファイル。

   -storepass *password*
   鍵ストアのパスワード。
7. 次のコマンドを発行して、署名付き証明書をインポートします。

   ```
   keytool -importcert -alias mykey -file signedcert.pem -keystore
   key.jks -storepass password
   ```

   各構成要素について説明します。

   -alias *mykey*
   署名付き証明書の別名。別名は、鍵ストアの作成時に使用したものと同じでなければなりません。新規鍵ストアおよび新規自己署名証明書の作成について詳しくは、鍵ストアへのアクセス権限の取得を参照してください。

   -file *signedcert.pem*
   CA から受信した署名付き証明書ファイル。

   -storepass *password*
   鍵ストアのパスワード。
8. Data Protection for VMware vSphere GUI サービスを開始します。

関連資料

81 ページの『Data Protection for VMware のサービスの開始と実行』
デフォルトでは、Windows オペレーティング・システムを始動すると、ローカル・システム・アカウントで recovery agent が開始されます。

VMware vCenter Server ユーザー特権の要件

Data Protection for VMware 操作を実行するには 特定の VMware vCenter Server 特権が必要です。

Data Protection for VMware vSphere GUI の Web ブラウザーのビューを使用して VMware データ・センターを保護するために必要な vCenter Server 特権

Data Protection for VMware vSphere GUI のブラウザー・ビューにサインインする vCenter Server のユーザー ID には、

GUI が管理するデータ・センターのコンテンツを表示するための十分な VMware 特権が必要です。

例えば、VMware vSphere 環境に 5 つのデータ・センターが含まれているとします。ユーザー「jenn」が十分な特権を持っているのは、これらのデータ・センターのうち 2 つに対してのみです。この結果、十分な特権が存在するこれら 2 つのデータ・センターのみがビューで「jenn」に対して表示されます。 他の 3 つのデータ・センター (「jenn」が特権を持っていない) は、ユーザー「jenn」に表示されません。

VMware vCenter Server は、一連の特権をまとめて、1 つの役割として定義します。 特権を作成するため、指定されたユーザーまたはグループのオブジェクトに 役割を適用します。 VMware vSphere Web Client から、一連の特権を持つ役割を作成する必要があります。 バックアップ操作およびリストア操作用の vCenter Server 役割を作成するには、VMware vSphere Client の「**役割の追加 (Add a Role)**」機能を使用します。

vCenter 内のすべてのデータ・センターに特権を伝搬したい場合は、vCenter Server を指定して、「子に伝達 (propagate to children)」チェック・ボックスを選択します。 あるいは、必要なデータ・センターのみに役割を割り当てて、「子に伝達 (propagate to children)」チェック・ボックスを選択すると、権限を制限することができます。 ブラウザーの制約はデータ・センター・レベルです。

次の例では、2 つの VMware ユーザー・グループに対してデータ・センターへのアクセスを制御する方法を示します。 最初に、技術情報 7047438 に定義されている特権をすべて含む役割を作成します。この例の特権セットは、「TDPVMwareManage」という名前の役割で識別されています。グループ 1 は、Primary1_DC データ・センターと Primary2_DC データ・センター用の仮想マシンを管理するためのアクセスを必要としています。グループ 2 は、Secondary1_DC データ・センターおよび Secondary2_DC データ・センターの仮想マシンを管理するためのアクセスが必要です。

グループ 1 では、Primary1_DC データ・センターと Primary2_DC データ・センターに「TDPVMwareManage」役割を割り当てます。グループ 2 では、Secondary1_DC データ・センターと Secondary2_DC データ・センターに「TDPVMwareManage」役割を割り当てます。

各 VMware ユーザー・グループ内のユーザーは、Data Protection for VMware GUI を使用して、それぞれのデータ・センター内の仮想マシンのみを管理できます。

ヒント: 役割を作成する際には、オブジェクトに対して他のタスクを実行するために後で必要になる可能性がある余分な特権を役割に追加することを考慮してください。

データ・ムーバーを使用するために必要な vCenter Server の特権

vStorage バックアップ・サーバー (データ・ムーバー・ノード) にインストールされている IBM Spectrum Protect データ・ムーバーには、VMCUser オプションおよび VMCPw オプションが必要です。 VMCUser オプションでは、バックアップ、リストア、または照会する vCenter Server または ESX サーバーのユーザー ID を指定します。このユーザー ID (VMCUser) に割り当てられる必要な特権により、クライアントは仮想マシン環境および VMware 環境で操作を確実に実行することができます。このユーザー ID には、上記技術情報で説明されている VMware 特権が必要です。

バックアップ操作およびリストア操作用の vCenter Server 役割を作成するには、VMware vSphere Client の「**役割の追加 (Add a Role)**」機能を使用します。 このユーザー ID (VMCUser) の特権を追加する場合は、「子に伝達 (propagate to children)」オプションを選択する必要があります。 また、バックアップおよ

びリストア以外のタスクのために、その他の特権をこの役割に追加することを検討してください。 VMCUser オプションでは、制約は最上位オブジェクトに適用されます。

Data Protection for VMware vSphere GUI の IBM Spectrum Protect vSphere Client プラグインのビューを使用して VMware データ・センターを保護するために必要な vCenter Server 特権

IBM Spectrum Protect vSphere Client プラグインでは、GUI へのサインインに必要な特権とは別の一連の特権が必要です。

インストール時には、IBM Spectrum Protect vSphere Client プラグインのために次のカスタム特権が作成されます。

- 「**データ・センター**」 > 「**IBM Data Protection**」
- 「**グローバル**」 > 「**IBM Data Protection の構成**」

IBM Spectrum Protect vSphere Client プラグインに必要なカスタム特権は、個別の拡張として登録されます。 特権拡張キーは com.ibm.tsm.tdpvmware.IBMDataProtection.privileges です。

これらの特権によって、VMware 管理者は、IBM Spectrum Protect vSphere Client プラグインのコンテンツへのアクセスを有効または無効にすることができます。 必要な VMware オブジェクトに対してこれらのカスタム特権を持つユーザーのみが IBM Spectrum Protect vSphere Client プラグインのコンテンツにアクセスできます。 vCenter Server ごとに IBM Spectrum Protect vSphere Client プラグインが 1 つ登録され、vCenter Server をサポートするように構成されているすべての GUI ホストで共有されます。

VMware vSphere Web Client から、IBM Spectrum Protect vSphere Client プラグインを使用して、仮想マシンに対してデータ保護機能を実行できるユーザーの役割を作成する必要があります。この役割では、Web クライアントが必要とする標準の仮想マシン管理者役割の特権に加えて、「**データ・センター**」 > 「**IBM Data Protection**」特権を指定する必要があります。 それぞれのデータ・センターで、ユーザーによる仮想マシンの管理を許可する対象のユーザーまたはユーザー・グループごとに、この役割を割り当てます。

vCenter レベルのユーザーには、「**グローバル**」 > 「**IBM Data Protection**」特権が必要です。この特権により、ユーザーは vCenter Server と Data Protection for VMware vSphere GUI Web サーバー間の接続を管理、編集、またはクリアすることが可能になります。この特権は、それぞれの vCenter Server を保護する Data Protection for VMware vSphere GUI について熟知する管理者に割り当ててください。IBM Spectrum Protect vSphere Client プラグインの接続は、拡張の「**接続**」ページで管理します。

次の例では、2 つのユーザー・グループに対してデータ・センターへのアクセスを制御する方法を示します。グループ 1 は、NewYork _DC データ・センターおよび Boston_DC データ・センターの仮想マシンを管理するためのアクセスが必要です。グループ 2 は、LosAngeles_DC データ・センターおよび SanFranciso_DC データ・センターの仮想マシンを管理するためのアクセスが必要です。

VMware vSphere client から、例えば「IBMDataProtectManage」役割を作成し、標準の仮想マシンの管理者役割の特権を割り当て、さらに「**データ・センター**」 > 「**IBM Data Protection**」特権を割り当てます。

グループ 1 では、NewYork _DC データ・センターと Boston_DC データ・センターに「IBMDataProtectManage」役割を割り当てます。グループ 2 では、LosAngeles_DC データ・センターと SanFranciso_DC データ・センターに「IBMDataProtectManage」役割を割り当てます。

各グループのユーザーは、vSphere Web Client の IBM Spectrum Protect vSphere Client プラグインを使用して、それぞれのデータ・センターの仮想マシンのみを管理できます。

不十分な権限に関連した問題

Web ブラウザーのユーザーにデータ・センターに対する十分な権限がない場合、ビューへのアクセスがブロックされます。 代わりに、ユーザーの権限が不十分であるために管理対象データ・センターへのアクセスを許可されていないことを通知する、エラー・メッセージ GVM2013E が発行されます。 不十分な権限から生じる問題について、ユーザーに通知するその他の新規メッセージも参照可能です。権限に関連した問題を解決するには、ユーザー役割が前のセクションの説明どおりにセットアップされていることを確認してください。 ユーザー役割は、「vCenter Server のユーザー ID およびデータ・ムーバーに必要な特権」表に示されるすべての特権を持っている必要があります。また、これらの特権は「子に伝達 (propagate to children)」チェック・ボックスを使用してデータ・センター・レベルで適用されている必要があります。

IBM Spectrum Protect vSphere Client プラグインのユーザーにデータ・センターに対する十分な権限がない場合、当該データ・センターとそのコンテンツのデータ保護機能は拡張では使用不可になります。

IBM Spectrum Protect ユーザー ID (VMCUser オプションによって指定される) に含まれる権限が、バックアップおよびリストア操作に不十分である場合は、次のメッセージが表示されます。

```
ANS9365E VMware vStorage API エラー。
「この操作を実行する許可が拒否されました。」
```

IBM Spectrum Protect ユーザー ID に含まれる権限がマシンの表示には不十分である場合は、次のメッセージが表示されます。

```
VM コマンドのバックアップが開始されました。処理する仮想マシンの合計数: 1
ANS4155E 仮想マシン「tango」が VMware サーバー上に見つかりませんでした。
ANS4148E 仮想マシン「foxtrot」のフル VM バックアップが失敗しました。RC 4390
```

特権の使用について詳しくは、**Data Protection for VMware vSphere GUI およびデータ・ムーバーに必要な vCenter Server の特権**を参照してください。

VMware Virtual Center Server を介して、権限の問題についてのログ情報を取得するには、以下のステップを実行します。

1. 「**vCenter Server 設定**」で、「**ロギング オプション**」を選択し、「**vCenter ロギング**」を「**最詳細 (Trivia)**」に設定します。
2. 権限エラーを再現します。
3. 余分なログ情報が記録されないように、「**vCenter ロギング**」を前の値にリセットします。
4. 「**システム ログ**」で、最新の vCenter Server ログ (vpxd-*wxyz*.log) を検索し、ストリング NoPermission を検索します。 例えば、次のようにします。

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   このログ・メッセージは、ユーザー ID に含まれる権限が、スナップショットの作成 (createSnapshot) には不十分であることを示しています。

Data Protection for VMware vSphere GUI のユーザーの役割

Data Protection for VMware vSphere GUI の機能の可用性は、IBM Spectrum Protect 管理者 ID に割り当てられている権限のレベルに基づいています。

管理者 ID はノード名と一致している必要があります。以前の製品リリースでは、**REGISTER NODE** コマンドは、ノード名と一致する管理ユーザー ID を自動的に作成していました。 IBM Spectrum Protect V8.1 以降では、**REGISTER NODE** コマンドは、ノード名と一致する管理ユーザー ID を自動的に作成しません。

新規ノードを登録する場合、IBM Spectrum Protect サーバー管理者は、**REGISTER NODE** サーバー・コマンドで userid パラメーターを指定する必要があります。

```
REGISTER NODE node_name password userid=user_id
```

ここで、ノード名と管理ユーザー ID は同じでなければなりません。例えば次のとおりです。

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

デフォルトでは、ノードにはクライアント所有者権限があります。

Data Protection for VMware vSphere GUI で実行できるタスクは、管理者 ID に割り当てられている特権クラスに基づきます。

管理者 ID に無制限のポリシー・ドメイン特権がない場合は、IBM Spectrum Protect サーバーにノードを新規に登録したり、ノードのプロキシー関係を設定したりすることはできません。管理者 ID を入力しない場合、IBM Spectrum Protect サーバー上で実行できるマクロ・スクリプトが作成されます。

IBM Spectrum Protect 管理者 ID は、Data Protection for VMware vSphere GUI の構成時に要求されます。次の表に、その ID に割り当てられている特権クラスに基づいて使用できる機能をリストします。

- 「可」の値は、そのユーザー役割に使用可能な機能を示しています。
- 「不可」の値は、そのユーザー役割に使用不可の機能を示しています。

現行の Data Protection for VMware vSphere GUI の役割を表示するには、ナビゲーション・バーでユーザー ID の上にカーソルを移動します。

表 *11. IBM Spectrum Protect* 管理者 *ID* の特権要件に基づいて使用できる機能

	オペレーター	**レポート作成担当オペレーター**	**制限付き管理者**	**管理者**
要約	バックアップとリストアをすぐに実行	オペレーターに加えて、レポート作成	オペレーターに加えて、レポート作成およびリストされているポリシー・ドメインに対するスケジュール操作	初期構成を含むすべての役割
IBM Spectrum Protect 管理者 ID の権限クラス	なし	以下のいずれかの特権クラス • ストレージ • オペレーター • 分析者	ポリシー (制限付き) または以下のいずれかの特権クラス • ストレージ • オペレーター • 分析者	ポリシー (制限なし) またはシステム
「バックアップ」タブ				
「**すぐに実行**」バックアップ・タスクの管理	可	可	可	可
「**スケジュール済み**」バックアップ・タスクの管理	不可 [1]	不可 [1]	ポリシー・ドメイン内で可	可
「**すぐに実行**」バックアップ・タスクの表示	可	可	可	可
「**スケジュール済み**」バックアップ・タスクの表示	不可	可	可	可
「**スケジュール済み**」バックアップ・タスクの削除	不可	不可	ポリシー・ドメイン内で可	可
「リストア」タブ				
「**リストア**」タスクの実行	可	可	可	可
「レポート」タブ				
イベント	不可	可	可	可
最近のタスク	可	可	可	可
バックアップ状況	不可	可	可	可
アプリケーション保護	不可	可	可	可
データ・センター占有情報	不可	可	可	可
「構成」タブ				

表 *11. IBM Spectrum Protect* 管理者 *ID* の特権要件に基づいて使用できる機能 *(*続き*)*

	オペレーター	レポート作成担当オペレーター	制限付き管理者	管理者
ノード登録 (「**構成状況**」->「**構成ウィザードの実行**」)	不可	不可	不可 [2]	可
IBM Spectrum Protect 管理者 ID 資格情報の変更 (「**構成状況**」->「**構成の編集**」)	可	可	可	可
VMCLI ノード・パスワードの変更 (「**構成状況**」->「**構成の編集**」)	不可	不可	可	可
GUI ドメインの変更 (「**構成状況**」->「**構成の編集**」)	可 [3]	可 [3]	可 [3]	可
データ・ムーバー・ノードの変更 (「**構成状況**」->「**構成の編集**」)	不可	不可	不可 [2]	可
マウント・プロキシー・ノードの変更 (「**構成状況**」->「**構成の編集**」)	不可	不可	不可 [2]	可

1. 無制限ドメイン・ポリシーが必要であるため、ノードを登録できません。
2. VMware データ・センターの追加または削除、データ・センター・ノードの登録を行うことができます。

IBM Spectrum Protect 管理者 ID の権限レベルおよび対応する Data Protection for VMware vSphere GUI の役割を表示するには、次のようにします。

1. 「**構成**」ウィンドウに進みます。
2. 「**構成の編集**」をクリックします。
3. 関連情報が「**Spectrum Protect サーバー資格情報**」ページに表示されます。

重要 :

- IBM Spectrum Protect の管理者 ID の権限レベルが IBM Spectrum Protect サーバーで変更された場合は、この変更を反映するために、Data Protection for VMware vSphere GUI を再始動する必要があります。
- 「**ユーザーの役割**」を変更する場合は、別の「**構成設定**」ページに移動したり、別の構成変更を試行したりする前に、「**OK**」をクリックして変更を保存する必要があります。さもないと、「**ユーザーの役割**」の変更は有効になりません。

Data Protection for VMware GUI 登録キー

インストール時に選択したオプションに応じて、さまざまな方法を使用して Data Protection for VMware GUI にアクセスすることができます。 Data Protection for VMware GUI の登録キーが作成されます。

「Data Protection for VMware GUI」という語句は、次の GUI に適用されます。

- Web ブラウザーでアクセスした Data Protection for VMware vSphere GUI
- vSphere Web Client GUI 内の IBM Spectrum Protect vSphere Client プラグイン

IBM Spectrum Protect vSphere Client プラグイン 登録キーは、`com.ibm.tsm.tdpvmware.IBMDataProtection` です。このキーは、インストール時に「**vSphere Web**

Client 拡張を登録」チェック・ボックスを選択すると登録されます。 vCenter Server ごとに、IBM Spectrum Protect vSphere Client プラグインの単一インスタンスが登録されます。

Web ブラウザーでアクセスした Data Protection for VMware vSphere GUI に対しては、登録キーは作成されません。

登録キーを表示するには、VMware 管理対象オブジェクト ブラウザ (MOB) にログインします。 MOB にログインした後、「**コンテンツ (Content)**→「**拡張マネージャー (Extension Manager)**」に進み、登録キーを表示します。

recovery agent GUI の構成

マウント、ファイルのリストア、またはインスタント・リストア操作のための、recovery agent GUI をセットアップする方法の手順を説明します。

始める前に

これらの構成タスクを完了してから、recovery agent GUI 内の操作を試行する必要があります。

重要 : recovery agent GUI を使用してタスクを実行する方法については、GUI と一緒にインストールされるオンライン・ヘルプに記載されています。いずれかの GUI ウィンドウで「**ヘルプ**」をクリックすると、タスクを支援するためのオンライン・ヘルプが開きます。

手順

1. ファイルをリストアするシステムにログオンします。 recovery agent がシステムにインストールされている必要があります。
2. recovery agent GUI 内の「**TSM サーバーの選択**」をクリックして、IBM Spectrum Protect サーバーに接続します。

   recovery agent が、Data Protection for VMware vSphere GUI と同じシステムにインストールされており、アプリケーションが Data Protection for VMware vSphere GUI 構成ウィザードを使用して正常に構成されている場合、以下のような条件が存在します。

   - データ・ムーバー・ノードおよび IBM Spectrum Protect サーバーが、recovery agent の「**TSM サーバー**」フィールドに取り込まれます。
   - 「**TSM サーバーの情報**」パネルの以下のフィールドにはデータが取り込まれます。
     - 「**認証ノード**」には、使用可能なデータ・ムーバー・ノードのリストが含まれます。
     - 「**ターゲット・ノード**」には、選択されたデータ・ムーバー・ノードに使用可能なデータ・センター・ノードのリストが含まれます。

   データ・ムーバー・ノード 1 つだけが、構成ウィザードを使用してローカルに定義されていた場合、recovery agent では開始時にそのノードを使用して認証を行います。

   recovery agent は、IBM Spectrum Protect サーバーに接続した最後のノード名を記憶します。 このノード (接続する最後のノード名) に対して「**パスワード・アクセス Generate を使用 (Use Password access generate)**」が選択される場合、recovery agent では始動時に以下の資格情報を使用して IBM Spectrum Protect サーバーに接続します。以前に IBM Spectrum Protect サーバーに接続されておらず、ウィザードではデータ・ムーバー・ノードが 1 つとデータ・センター・ノードが 1 つのみが構成されている場合、recovery agent では始動時に以下の資格情報を使用して、IBM Spectrum Protect サーバーに接続します。

   次のオプションを指定します。

   サーバー・アドレス
   IBM Spectrum Protect の IP アドレスまたはホスト名を入力します。

   サーバー・ポート
   サーバーとの TCP/IP 通信に使用するポート番号を入力します。デフォルトのポート番号は 1500 です。

   ノード・アクセス方式:

Asnodename

このオプションは、プロキシー・ノードを使用して、ターゲット・ノードにある VM バックアップにアクセスする場合に選択します。 プロキシー・ノードとは、ターゲット・ノードに代わって操作を実行するための「プロキシー」権限を付与されているノードです。

一般に、IBM Spectrum Protect 管理者は、`grant proxynode` コマンドを使用して、2 つの既存ノード間のプロキシー関係を作成します。

このオプションを選択する場合は、以下の手順を実行します。

a. 「**ターゲット・ノード**」フィールドに、ターゲット・ノード (VM バックアップが置かれているノード) の名前を入力します。
b. 「**認証ノード**」フィールドにプロキシー・ノードの名前を入力します。
c. 「**パスワード**」フィールドにプロキシー・ノードのパスワードを入力します。
d. 「**OK**」をクリックして、上記設定を保存し、IBM Spectrum Protect 情報ダイアログを終了します。

この方法を使用する場合、recovery agent ユーザーはプロキシー・ノード・パスワードのみを知っており、ターゲット・ノード・パスワードは保護されます。

Fromnode

このオプションは、ターゲット・ノード内の特定の VM のスナップショット・データにのみ限定されているアクセス権限を持つノードを使用する場合に選択します。

一般的に、`set access` コマンドを使用することにより、VM バックアップを所有するターゲット・ノードからのアクセス権限がこのノードに与えられます。

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

例えば、次のコマンドは、`myMountNode` という名前のノードに、`myTestVM` という名前の VM からファイルをリストアするための権限を付与します。

```
set access backup -TYPE=VM myTestVM myMountNode
```

このオプションを選択する場合は、以下の手順を実行します。

a. 「**ターゲット・ノード**」フィールドに、ターゲット・ノード (VM バックアップが置かれているノード) の名前を入力します。
b. 制限付きアクセスが与えられるノードの名前を「**認証ノード**」フィールドに入力します。
c. 制限付きアクセスが与えられるノードのパスワードを「**パスワード**」フィールドに入力します。
d. 「**OK**」をクリックして、上記設定を保存し、IBM Spectrum Protect 情報ダイアログを終了します。

この方法を使用する場合、バックアップされた VM の完全リストが表示されます。 ただし、リストアできるのは、ノードがアクセス権限を付与されている VM バックアップのみです。 また、サーバー上でのスナップショット・データの有効期限切れは保護されません。 そのため、この方法ではインスタント・リストアはサポートされません。

Direct

このオプションは、ターゲット・ノード (VM バックアップが置かれているノード) に対する認証を直接受ける場合に使用します。

このオプションを選択する場合は、以下の手順を実行します。

a. 「**認証ノード**」フィールドに、ターゲット・ノード (VM バックアップが置かれているノード) の名前を入力します。
b. 「**パスワード**」フィールドにターゲット・ノードのパスワードを入力します。
c. 「**OK**」をクリックして、上記設定を保存し、IBM Spectrum Protect 情報ダイアログを終了します。

パスワード・アクセス生成を使用 (Use Password access generate)
このオプションを選択したときにパスワード・フィールドが空の場合、recovery agent では、レジストリーに保管されている既存のパスワードを使用して認証を行います。オプションを選択しない場合は、パスワードを手動で入力する必要があります。

このオプションを使用するには、オプションが適用されるノードに対して、最初に手動で初期パスワードを設定する必要があります。最初に IBM Spectrum Protect ノードに接続する際に、「**パスワード**」フィールドにパスワードを入力し、「**パスワード・アクセス生成を使用**」チェック・ボックスを選択して、初期パスワードを指定する必要があります。

ただし、「**認証ノード**」としてローカル・データ・ムーバー・ノードを使用する場合、パスワードがすでにレジストリーに保管されている場合があります。その場合、「**パスワード・アクセス生成を使用**」チェック・ボックスを選択して、パスワードを入力しないでください。

recovery agent は、保護対象の VM のリストに対して指定されたサーバーを照会し、そのリストを表示します。

3. 「**設定**」をクリックして、以下のマウント・オプション、バックアップ・オプション、およびリストア・オプションを設定してください。

仮想ボリューム書き込みキャッシュ
Windows バックアップ・プロキシー・ホスト上で実行している recovery agent は、インスタント・リストアとマウント中に作成された、データの変更を保存します。 これらの変更は、仮想ボリューム上の書き込みキャッシュに保存されます。 デフォルトで、書き込みキャッシュが使用可能になっており、パスは `C:¥ProgramData¥Tivoli¥TSM¥TDPVMware¥mount¥`、最大キャッシュ・サイズは選択されたフォルダーの使用可能なスペースの 90% に指定されています。 システム・ボリュームが満杯にならないように、書き込みキャッシュをシステム・ボリューム以外のボリューム上のパスに変更してください。

一時ファイル用のフォルダー
データの変更内容が保存される場所のパスを指定します。 書き込みキャッシュはローカル・ドライブ上になければなりません。共有フォルダー上のパスには設定できません。 書き込みキャッシュが使用不可またはフルになっている場合は、インスタント・リストア・セッションまたはマウント・セッションを開始しようとしても失敗します。

キャッシュ・サイズ
書き込みキャッシュのサイズを指定します。 使用可能な最大キャッシュ・サイズは、選択されたフォルダーの使用可能なスペースの 90% です。

制約事項 : 復元処理の間の中断を防ぐために、アンチウィルス・ソフトウェアのすべての保護設定から書き込みキャッシュのパスを削除してください。

データ・アクセス
アクセスするデータのタイプを指定します。 オフライン・デバイス (テープや仮想テープ・ライブラリーなど) を使用する場合は、該当するデータ・タイプを指定する必要があります。

ストレージ・タイプ
スナップショットのマウント元となる以下のストレージ・デバイスのいずれかを指定してください。

ディスク/ファイル
スナップショットは、ディスクまたはファイルからマウントされます。 このデバイスがデフォルトです。

テープ
スナップショットは、テープ・ストレージ・プールからマウントされます。 このオプションが選択されている場合は、複数のスナップショットをマウントしたり、Instant Restore 操作を実行したりすることはできません。

VTL
スナップショットは、オフラインの仮想テープ・ライブラリーからマウントされます。 同じ仮想テープ・ライブラリー上での同時マウント・セッションがサポートされています。

注 : ストレージ・タイプが変更されたときには、その変更を有効にするために、このサービスを再始動する必要があります。

有効期限切れ保護を無効にする
マウント操作時は、IBM Spectrum Protect サーバーのスナップショットは操作中に失効しないようにロックされています。有効期限切れは、さらなる別のスナップショットがマウント済みのスナップショット・シーケンスに追加されるために発生する場合があります。 この値は、マウント操作中に有効期限切れ保護を無効にするかどうかを指定します。

- スナップショットを有効期限切れから保護する場合は、このオプションを選択しないでください。 IBM Spectrum Protect サーバー上のスナップショットはロックされ、スナップショットはマウント操作中に有効期限切れから保護されます。
- 有効期限切れ保護を無効にする場合は、このオプションを選択してください。このオプションは、デフォルトで選択されています。IBM Spectrum Protect サーバーのスナップショットはロックされず、スナップショットはマウント操作中に有効期限切れから保護されません。そのため、スナップショットはマウント操作中に失効する場合があります。有効期限が切れると、予期しない結果を招きマウント・ポイントに悪影響を及ぼすおそれがあります。 例えば、マウント・ポイントが使用不可になったり、エラーが発生したりする可能性があります。 ただし、有効期限は、現在のアクティブ・コピーには影響しません。アクティブ・コピーは操作中に失効することはありません。

  スナップショットがターゲット複製サーバー上にある場合、そのスナップショットは読み取り専用モードなのでロックすることはできません。サーバーによるロック試みが原因で、マウント操作が失敗することがあります。 ロック試みが行われないようにし、そのような失敗を防ぐためには、このオプションを選択して有効期限切れ保護を無効にします。

先読みサイズ (16 KB ブロック単位)
読み取り要求が 1 つのブロックに対して送信された後に、ストレージ・デバイスから取得される追加データ・ブロックの数を指定します。 デフォルト値は次のとおりです。

- ディスクまたはファイル: 64
- テープ: 1024
- VTL: 64

すべてのデバイスの最大値は 1024 です。

先読みキャッシュ・サイズ (ブロック)
追加データ・ブロックが保管されるキャッシュのサイズを指定します。 デフォルト値は次のとおりです。

- ディスクまたはファイル: 10000
- テープ: 75000
- VTL: 10000

各スナップショットには独自のキャッシュがあるため、同時にマウントまたはリストアされるスナップショット数を必ず計画してください。 累積キャッシュ・サイズは 75000 ブロックを超えることはできません。

ドライバー・タイムアウト (秒)
この値は、ファイル・システム・ドライバーからのデータ要求を処理するための時間の長さを指定します。 この時間内に処理が完了しない場合、要求は取り消され、ファイル・システム・ドライバーにエラーが返されます。 タイムアウトが発生する場合は、この値を増やすことを検討してください。 例えば、ネットワークが低速の場合、ストレージ・デバイスがビジーの場合、あるいは複数のマウント・セッションまたはインスタント・リストア・セッションの処理が行われている場合にタイムアウトが発生することがあります。デフォルト値は次のとおりです。

- ディスクまたはファイル: 60
- テープ: 180
- VTL: 60

「**OK**」をクリックして変更を保存し、「**設定**」を終了してください。

4. 各 IBM Spectrum Protect サーバー・ノード (Asnodename オプションおよび Fromnode オプションで指定されたもの) でバックアップを削除できることを確認してください。

recovery agent では、操作時に、未使用の一時オブジェクトが作成されます。BACKDELete=Yes サーバー・オプションを指定することにより、これらのオブジェクトを、ノード内に累積されないように削除することができます。

a) IBM Spectrum Protect サーバーにログオンし、以下のように、コマンド・ライン・モードで管理クライアント・セッションを開始します。

```
dsmadmc -id=admin -password=admin -dataonly=yes
```

b) 次のコマンドを入力します。

```
Query Node <nodename> Format=Detailed
```

各ノードのコマンド出力に次のステートメントが含まれていることを確認してください。

```
Backup Delete Allowed?: Yes
```

このステートメントが含まれていない場合は、次のコマンドを使用して各ノードを更新してください。

```
UPDate Node <nodename> BACKDELete=Yes
```

各ノードについて Query Node コマンドを再度実行し、各ノードでバックアップを削除できることを確認してください。

5. iSCSI ネットワークで Recover Agent を使用し、その Recovery Agent がデータ・ムーバーを使用しない場合は、C:¥ProgramData¥Tivoli¥TSM¥RecoveryAgent¥mount¥RecoveryAgent.conf ファイルにアクセスして、[IMOUNT] タグおよび **Target IP** パラメーターを指定します。

```
[IMOUNT config]
Target IP=<IP address of the network card on the system
that exposes the iSCSI targets.>
```

例えば、次のようにします。

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

「Target IP」パラメーターを追加または変更した後に、Recovery Agent GUI または Recovery Agent CLI を再始動してください。

recovery agent から IBM Spectrum Protect サーバーへのセキュア通信の使用可能化

IBM Spectrum Protect サーバーが Secure Sockets Layer (SSL) または Transport Layer Security (TLS) プロトコルを使用するように構成されている場合は、recovery agent が プロトコルを使用してサーバーと通信できるようにすることが可能です。

始める前に

サーバーへのセキュア通信の構成を開始する前に、以下の要件を検討してください。

- SSL を有効にした各サーバーには、それぞれ固有の証明書が必要です。証明書のタイプは、以下のいずれかのタイプです。
  - サーバーによって自己署名された証明書。
  - サード・パーティー認証局 (CA) によって発行された証明書。CA 証明書には、Symantec や Thawte などの企業から得られる証明書、またはお客様の社内で保守される内部証明書があります。
- パフォーマンス上の理由で、セキュリティーが必要なセッションには SSL または TLS のみを使用してください。増加した要件を管理するには、サーバー・システムにプロセッサー・リソースを追加します。

- TLS バージョン 1.2 を使用してサーバーに接続するクライアントの場合、証明書の署名アルゴリズムが Secure Hash Algorithm 1 (SHA-1) 以降でなければなりません。 TSL V1.2 を使用するサーバーに対して自己署名証明書を使用する場合、cert256.arm 証明書を使用する必要があります。 IBM Spectrum Protect 管理者は、サーバー上のデフォルト証明書を変更する必要がある場合があります。
- TLS 1.2 より安全度の低いセキュリティー・プロトコルを無効にするには、**SSLDISABLELEGACYtls yes** オプションを C:¥windows¥system32¥fb.opt ファイルまたは C:¥Windows¥SysWOW64¥fb.opt ファイルに追加します。 TLS 1.2 以降を使用することで、悪意のあるプログラムによる攻撃を防止するのに役立ちます。

IBM Spectrum Protect サーバー自己署名証明書を使用したセキュア通信の使用可能化
IBM Spectrum Protect サーバーで自己署名証明書を使用している場合は、サーバー管理者から証明書のコピーを取得し、SSL または TLS プロトコルを使用してサーバーと通信するように recovery agent を構成する必要があります。

このタスクについて

各サーバーが独自の証明書を生成します。 バージョン 6.3 以降のサーバーは、cert256.arm という名前のファイル (TLS 1.2 以降を使用している場合) または cert.arm という名前のファイル (旧バージョンの SSL または TLS を使用している場合) を生成します。V6.3 より前のサーバー・バージョンでは、プロトコルに関係なく cert.arm という名前のファイルを生成します。 サーバー上でデフォルトとして設定されている証明書を選択する必要があります。

証明書ファイルは、サーバー・ワークステーション上のサーバー・インスタンス・ディレクトリーに保管されます。例えば、C:¥IBM¥tivoli¥tsm¥server¥bin¥cert256.arm です。証明書ファイルが存在しない場合は、これらのオプション・セットを使用してサーバーを再始動したときに証明書ファイルが作成されます。

手順

自己署名証明書を使用した、リカバリー・エージェントからサーバーへの SSL または TLS 通信を有効にするには、以下のようにします。

1. GSKit バイナリー・パスとライブラリー・パスをクライアント上の PATH 環境変数に追加します。
   例えば次のとおりです。

   ```
   set PATH=C:¥Program Files¥Common Files¥Tivoli¥TSM¥api64¥gsk8¥bin¥;
       C:¥Program Files¥Common Files¥Tivoli¥TSM¥api64¥gsk8¥lib64;%PATH%
   ```

2. クライアント上で初めて SSL または TLS を構成する場合、クライアントのローカル鍵データベース dsmcert.kdb を作成する必要があります。
   C:¥Windows¥SysWOW64 ディレクトリーから、次の例に示されているように **gsk8capicmd_64** コマンドを実行します。

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   指定したパスワードは、鍵データベースの暗号化に使用されます。パスワードは暗号化されて自動的に stash ファイル (dsmcert.sth) に保管されます。クライアントは、stash ファイルを使用して鍵データベース・パスワードを取得します。
3. サーバー自己署名証明書を入手します。
4. dsmcert.kdb データベースに証明書をインポートします。各クライアントの証明書を dsmcert.kdb にインポートする必要があります。
   C:¥Windows¥SysWOW64 ディレクトリーから、次の例に示されているように **gsk8capicmd_64** コマンドを実行します。

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server server_name self-signed
   key"
   -file path_to_certificate -format ascii -trust enable
   ```

dsmcert.kdb データベースには複数のサーバー証明書を追加することができるため、クライアントはさまざまなサーバーに接続することができます。 異なる証明書には、異なるラベルが必要です。ラベルには、わかりやすいラベルを使用してください。

重要 : サーバーの災害復旧の場合、証明書が失われると、サーバーは自動的に新規証明書を生成します。その後、各クライアントが新規証明書をインポートする必要があります。

5. サーバー証明書を dsmcert.kdb データベースに追加した後、`ssl yes` オプションを `C:¥Windows¥SysWOW64¥fb.opt` ファイルに追加し、`tcpport` オプションの値を更新します。

   重要 :

   通常、サーバーでは、SSL 接続および TLS 接続は、SSL および TLS 以外の接続とは別のポートでセットアップされます。 `tcpport` 値には、SSL および TLS 以外で使用するポート番号を指定しないでください。 `tcpport` の値が誤っている場合、リカバリー・エージェントはサーバーに接続できません。

   SSL または TLS が有効にされているリカバリー・エージェントを使用して SSL および TLS 以外のポートに接続することはできません。また、SSL または TLS が有効にされていないリカバリー・エージェントに SSL または TLS のポートを接続することもできません。

6. 以下のリカバリー・エージェント構成ファイルで、正しい SSL または TLS のポートを設定します。
   - `C:¥ProgramData¥Tivoli¥TSM¥RecoveryAgent¥mount¥RecoveryAgent.conf`
   - `C:¥ProgramData¥Tivoli¥TSM¥RecoveryAgent¥mount¥RecoveryAgentDMNodes.conf`

サード・パーティーの証明書を使用したセキュア通信の使用可能化

IBM Spectrum Protect サーバーがサード・パーティー認証局 (CA) を使用している場合、CA ルート証明書を取得する必要があります。

このタスクについて

証明書が Symantec や Thawte などの CA によって発行されている場合、クライアントでは SSL あるいは TLS を使用する準備ができているため、以下の構成ステップをスキップすることができます。 プリインストール済み CA ルート証明書のリストについては、IBM Knowledge Center で「**認証局ルート証明書**」を検索してください。

証明書が、プリインストールされたルート証明書によって発行されていない場合、あるいはお客様の社内で保守されている内部 CA 証明書である場合は、SSL または TLS プロトコルを使用してサーバーと通信するように recovery agent を構成する必要があります。

手順

CA 証明書を使用した、リカバリー・エージェントからサーバーへの SSL または TLS 通信を有効にするには、以下のようにします。

1. GSKit バイナリー・パスとライブラリー・パスを PATH 環境変数に追加します。
   例えば次のとおりです。

   ```
   set PATH=C:¥Program Files¥Common Files¥Tivoli¥TSM¥api64¥gsk8¥bin¥;
       C:¥Program Files¥Common Files¥Tivoli¥TSM¥api64¥gsk8¥lib64;%PATH%
   ```

2. クライアント上で初めて SSL または TLS を構成する場合、クライアントのローカル鍵データベース dsmcert.kdb を作成する必要があります。
   クライアントの場合、`C:¥Windows¥SysWOW64` ディレクトリーから、次の例に示されているように **gsk8capicmd_64** コマンドを実行します。

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   指定したパスワードは、鍵データベースの暗号化に使用されます。パスワードは暗号化されて自動的に stash ファイル (dsmcert.sth) に保管されます。 クライアントは、stash ファイルを使用して鍵データベース・パスワードを取得します。

3. CA 証明書を入手します。

4. dsmcert.kdb データベースに証明書をインポートします。各クライアントの証明書を dsmcert.kdb にインポートする必要があります。

   クライアントの場合、C:¥Windows¥SysWOW64 ディレクトリーから、次の例に示されているように **gsk8capicmd_64** コマンドを実行します。

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"
   -file path_to_CA_root_certificate -format ascii -trust enable
   ```

   dsmcert.kdb データベースには複数のサーバー証明書を追加することができるため、クライアントはさまざまなサーバーに接続することができます。 異なる証明書には、異なるラベルが必要です。ラベルには、わかりやすいラベルを使用してください。

   重要 : サーバーの災害復旧の場合、証明書が失われると、サーバーは自動的に新規証明書を生成します。各クライアントが新規証明書をインポートする必要があります。
5. サーバー証明書を dsmcert.kdb データベースに追加した後、ssl yes オプションを C:¥Windows¥SysWOW64¥fb.opt ファイルに追加し、tcpport オプションの値を更新します。

   重要 :

   通常、サーバーでは、SSL 接続および TLS 接続は、SSL および TLS 以外の接続とは別のポートでセットアップされます。 tcpport 値には、SSL および TLS 以外で使用するポート番号を指定しないでください。 tcpport の値が誤っている場合、リカバリー・エージェントはサーバーに接続できません。

   SSL または TLS が有効にされているリカバリー・エージェントを使用して SSL および TLS 以外のポートに接続することはできません。また、SSL または TLS が有効にされていないリカバリー・エージェントに SSL または TLS のポートを接続することもできません。
6. 以下のリカバリー・エージェント構成ファイルで、正しい SSL または TLS のポートを設定します。
   - C:¥ProgramData¥Tivoli¥TSM¥RecoveryAgent¥mount¥RecoveryAgent.conf
   - C:¥ProgramData¥Tivoli¥TSM¥RecoveryAgent¥mount¥RecoveryAgentDMNodes.conf

ロケール設定

ロケール設定は、インターフェース、メッセージ、およびオンライン・ヘルプに使用される言語を識別します。

Data Protection for VMware GUI

「Data Protection for VMware GUI」という語句は、次の GUI に適用されます。

- Web ブラウザーでアクセスした Data Protection for VMware vSphere GUI
- vSphere Web Client GUI 内の IBM Spectrum Protect vSphere Client プラグイン

Data Protection for VMware GUI を実行するプロセッサー、VMware vSphere クライアント、および IBM Spectrum Protect サーバーの間でロケール設定が不整合である環境では、Data Protection for VMware GUI の実行はサポートされません。

Data Protection for VMware GUI を実行するプロセッサー、VMware vSphere クライアント、および IBM Spectrum Protect サーバーの間で同じロケール設定を指定してください。

「詳細情報」リンクから Data Protection for VMware GUI のヘルプ・ページに初めてアクセスすると、 ヘルプは、Data Protection for VMware GUI を実行しているシステムのロケール設定で指定されている言語で表示されます。ヘルプに初めてアクセスしたときに、ヘルプは、VMware vSphere Client のロケールで指定されている言語では表示されません。 この状態では、Data Protection for VMware GUI のヘルプ・ページが表示された後、ヘルプ内で少なくとも 2 つのリンクをクリックしてからヘルプを閉じます。 次に「詳細情報」リンクからヘルプが開始されたときには、VMware vSphere Client のロケール設定で指定された言語で表示されます。

IBM Spectrum Protect ファイル・リストア・インターフェース

インターフェースのコンテンツおよびメッセージ ・プロンプトの言語は、 IBM Spectrum Protect ファイル・リストア・インターフェースにアクセスする Web ブラウザーの言語設定によって決まります。

fr_api.log ログ・ファイルに記録されるエラー・メッセージについては、IBM Spectrum Protect ファイル・リストア・インターフェースは、 Data Protection for VMware vSphere GUI を実行しているシステムのロケール設定で指定されている言語を使用します。

ログ・ファイル関連のアクティビティー

Data Protection for VMware は、インストール操作、バックアップ操作、マウント操作、およびリストア操作中に、いくつかのログ・ファイルを作成および変更します。

Data Protection for VMware ログ・ファイルは、.sf ファイル拡張子を使用するプレーン・テキスト・ファイルです。

Windows ログは、以下のディレクトリーにあります。
%ALLUSERSPROFILE%¥Tivoli¥TSM¥TDPVMware
これらのディレクトリーには、Data Protection for VMware の各コンポーネントのサブディレクトリーが含まれています。例えば、recovery agent サブディレクトリーは ¥mount で、Recovery Agent コマンド・ライン・インターフェースのサブディレクトリーは ¥shell です。
ログ・ファイルを検索するには、 「**Windows**」 >「**スタート**」メニューから、 「**コントロール パネル**」 >「**検索**」を選択し、 *.log と入力します。

Linux ログは、以下の両方のパスにあります。
<user.home>/tivoli/tsm/ve/mount/log
/opt/tivoli/tsm/TDPVMware/mount/engine/var
次のコマンドを入力することにより、ログ・ファイルを検索することができます。

```
find /opt/tivoli/ -name "*.log"
```

重要 : 既存のログ・ファイルは、インストールが開始されるたびに毎回上書きされます。インストールで問題が発生し、製品の再インストールが必要な場合は、 インストールを再試行する前に、既存の TDPVMwareInstallation.log ファイルを %allusersprofile% ディレクトリーから取得してください。

注 : Data Protection for VMware サービスの実行中、いくつかのログ・ファイルはオープン状態のまま保持されます。そのため、一部のファイル・マネージャーはこれらのファイルの現行状態を示さずに、ファイル・サイズがゼロであると報告することがあります。これらのファイルのいずれかを選択するかまたは開くと、ファイル・マネージャーはファイルの詳細を更新します。

recovery agent ログ・ファイル

recovery agent ログ・ファイルは TDP_FOR_VMWARE_MOUNT*nnn*.sf です。最新データを含むログ・ファイルは、*040* の番号の付いたログ・ファイル (TDP_FOR_VMWARE_MOUNT040.sf) に保管されます。ログ・ファイルが最大サイズの限度に達すると、新しいログ・ファイルが作成されます。 ログ・ファイルの名前は、ログ・ファイル番号が 1 つずつ減ることを除き、同一です。 具体的に説明すると、番号が *040* のログ・ファイル内のデータは、番号が *039* のログ・ファイルにコピーされます。 番号が *040* のログ・ファイルには、最新のログ・ファイル・データが含まれます。 *040* が再び最大ファイル・サイズに達すると、*039* ファイルの内容が *038* に移動し、再び *040* の情報が *039* に移動します。

Data Protection for VMware GUI のログ・ファイル

Data Protection for VMware vSphere GUI は、次のディレクトリーにログ・ファイルを配置します。
Windows C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥logs
Linux /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs
ログ・ファイルを収集する場合は、圧縮ファイルにすべてのサブディレクトリーを含めるようにしてください。

Data Protection for VMware コマンド・ライン・インターフェース ログ・ファイル

Data Protection for VMware コマンド・ライン・インターフェース は、次のディレクトリーにログ・ファイルを配置します。

Windows C:¥Program Files¥IBM¥SpectrumProtect¥Framework¥VEGUI¥logs

Linux /opt/tivoli/tsm/tdpvmware/common/logs

ログ・ファイルを収集する場合は、圧縮ファイルにすべてのサブディレクトリーを 含めるようにしてください。

IBM Spectrum Protect ファイル・リストア・インターフェースのログ・ファイル

IBM Spectrum Protect ファイル・リストア・インターフェースは、 エラー・メッセージのログを fr_api.log、fr_gui.log、および messages.log ファイルに記録します。これらのファイルは、デフォルトで以下のディレクトリーにあります。

Windows C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥logs

Linux /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

ファイル・リストア・ログ ・アクティビティー ・ファイル (FRLog.config) 内の API_LOG_FILE_NAME オプションおよび API_LOG_FILE_LOCATION オプションを設定することにより、fr_api.log ファイルの名前とロケーションを変更することができます。

ファイル・リストア操作のログも IBM Spectrum Protect サーバーによって記録されます。サーバー管理コマンド・ライン・クライアントでこれらのメッセージを 検索できます。

- コマンド・ライン・モードで管理クライアント・セッションを開始するには、次のコマンドをワークステーションに入力します。

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  示されているように **-ID** オプションおよび **-PASSWORD** オプションを指定して **DSMADMC** コマンドを入力することで、ユーザー ID とパスワードの入力を求めるプロンプトが表示されなくなります。
- SQL 要約拡張テーブルを検索してファイル・リストア操作に関する結果を表示するには、管理コマンド・ライン・クライアントから **select** コマンドを実行します。

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  ```

  select 文に以下の 1 つ以上の基準を含めることによって、検索を絞り込むことができます。

  - * ENTITY='*DATA_MOVER_NODE_NAME*'
  - * AS_ENTITY='*DATA_CENTER_NODE_NAME*'
  - * SUB_ENTITY='*VM_HOST_NAME*'
  - * START_TIME='*yyyy-MM-dd HH:mm:ss*'

  例えば、次のようにします。

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
  and START_TIME>'2017-03-11 17:30:00'
  ```

  START_TIME 基準は、等号 (=)、より小 (<)、またはより大 (>) の記号を使用した照会をサポートします。
- ファイル・リストア操作に関するイベントを SQL アクティビティー ・ログ・テーブルで検索して表示するには、 管理コマンド・ライン・クライアントから **select** コマンドを実行します。

  ```
  select * from ACTLOG
  ```

  select 文に以下の 1 つ以上の基準を含めることによって、検索を絞り込むことができます。

  - * NODENAME='*DATA_CENTER_NODE_NAME*'
  - * DATE_TIME='*yyyy-MM-dd HH:mm:ss*'

例えば、次のようにします。

```
select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
```

DATA_MOVER_NODE_NAME および *DATA_CENTER_NODE_NAME* を大文字で指定します。

DATE_TIME 基準は、等号 (=)、より小 (<)、またはより大 (>) の記号を使用した照会をサポートします。

Data Protection for VMware のサービスの開始と実行

デフォルトでは、Windows オペレーティング・システムを始動すると、ローカル・システム・アカウントで recovery agent が開始されます。

Microsoft Windows 上の recovery agent サービスの実行

Windows の「スタート」メニューから recovery agent を開始すると、サービスは自動的に停止します。「スタート」メニューから開始した recovery agent アプリケーションが終了すると、サービスは自動的に開始します。 さらに、これらのオペレーティング・システムの場合、サービスは GUI を提供しません。GUI を使用するには、Windows の「スタート」メニューに進み、「**すべてのプログラム**」 > 「**IBM Spectrum Protect**」 > 「**Data Protection for VMware**」 > 「**recovery agent**」を選択します。

Data Protection for VMware コマンド・ライン・インターフェース

以下のタスクを実行して、Data Protection for VMware コマンド・ライン・インターフェース が実行中であることを確認できます。

Windows 「**スタート**」 > 「**コントロール パネル**」 > 「**管理ツール**」 > 「**サービス**」に進み、Data Protection for VMware コマンド・ライン・インターフェースの状況が「開始」であることを確認します。

Linux スクリプト・ディレクトリー (/opt/tivoli/tsm/tdpvmware/common/scripts/) に進み、次のコマンドを発行します。

```
./vmclid status
```

- デーモンが実行中でない場合は、次のコマンドを発行してデーモンを手動で開始します。

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  また、以下の init スクリプトを、デーモンの停止と開始に使用できます。

  ```
  ./vmclid stop
  ./vmclid start
  ```

付録 A 拡張構成タスク

使用可能なアプリケーション・インターフェースを 使用して各コンポーネントを手動で構成し、検査する必要があります。

始める前に
このタスクに進む前に、以下の条件が存在することを確認してください。

- ノードの登録に、IBM Spectrum Protect サーバーが使用可能でなければならない。
- Data Protection for VMware vSphere GUI が、オペレーティング・システムの前提条件を満たすシステムにインストールされている。以下のシステムへのネットワーク接続を持っている必要があります。
  - vStorage バックアップ・サーバー
  - IBM Spectrum Protect サーバー
  - vCenter Server

手順

1. IBM Spectrum Protect サーバーにログオンし、t_ve_cfg_regtsmnodes.dita で説明されているタスクを実行します。
2. vStorage バックアップ・サーバーにログオンし、85 ページの『vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ』で説明されているタスクを実行します。
3. Data Protection for VMware vSphere GUI がインストールされているシステムにログオンし、93 ページの『vSphere 環境での Data Protection for VMware コマンド・ライン・インターフェースの 構成 』で説明されているタスクを実行します。
4. Data Protection for VMware vSphere GUI がインストールされているシステムで vSphere Client を開始し、vCenter にログオンします。

   vSphere Client がすでに実行中である場合は、いったん停止して再開する必要があります。
5. vSphere Client のホーム・ディレクトリーに進みます。「ソリューションとアプリケーション (Solutions and Applications)」パネルで Data Protection for VMware vSphere GUI のアイコンをクリックします。

   ヒント : このアイコンが 表示されない場合、Data Protection for VMware vSphere GUI が登録されていないか、接続エラーが発生しました。

   a. vSphere クライアント・メニューで、「**プラグイン**」 > 「**プラグインの管理 (Manage Plug-ins)**」に進んで、プラグイン・マネージャーを開始します。

   b. Data Protection for VMware vSphere GUI を見つけることができ、接続エラーが発生した場合は、`ping` コマンドを発行して、Data Protection for VMware vSphere GUI がインストールされているマシンへの接続を確認します。

タスクの結果
Data Protection for VMware vSphere GUI は、バックアップ操作とリストア操作の準備ができました。

vSphere 環境での IBM Spectrum Protect ノードのセットアップ

この手順では、ノードを手動で IBM Spectrum Protect サーバーに登録し、vSphere 環境でそれらのノードにプロキシー権限を付与する方法を説明しています。

始める前に

重要 :

このタスクについて
この手順のすべてのステップは、IBM Spectrum Protect サーバーで実行されます。

ヒント: このタスクは、Data Protection for VMware vSphere GUI 構成ウィザードまたは「構成の編集」ノートブックを使用しても完了できます。Web ブラウザーを開いて GUI Web サーバーにアクセスすることにより、Data Protection for VMware vSphere GUI を開始します。例えば、次のようにします。

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

vCenter ユーザー名とパスワードを使用してログインします。

- 初期構成の場合は、「**構成**」 > 「**構成ウィザードの実行**」に進んでください。
- 既存構成の場合は、「**構成**」 > 「**構成の編集**」に進んでください。

手順

1. IBM Spectrum Protect サーバーにログオンし、以下のように、コマンド・ライン・モードで管理クライアント・セッションを開始します。

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. REGister Node コマンドを発行して、以下のノードを IBM Spectrum Protect サーバーに登録します。

   a) VMware vCenter を表すノード (vCenter ノード):

   ```
   REGister Node MY_VCNODE <password for MY_VCNODE>
   ```

   b) IBM Spectrum Protect と Data Protection for VMware vSphere GUI の間の通信を行うノード (VMCLI ノード):

   ```
   REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
   ```

   c) データ・センターを表し、VM データが保管されるノード (データ・センター・ノード):

   ```
   REGister Node MY_DCNODE <password for MY_DCNODE>
   ```

   d) 1 つのシステムから別のシステムに「データを移動する」ノード (データ・ムーバー・ノード):

   ```
   REGister Node MY_DMNODE <password for MY_DMNODE>
   ```

   重要: ノードを IBM Spectrum Protect サーバーに登録する時に userid パラメーターを使用しないでください。

3. GRant PROXynode コマンドを発行して、これらのノードのプロキシー関係を定義します。

   要確認: ターゲット・ノードがデータを所有し、エージェント・ノードはそれらのターゲット・ノードの代わりに機能します。ターゲット・ノードへのプロキシー権限が付与されると、エージェント・ノードは、そのターゲット・ノードのバックアップ操作とリストア操作を実行することができます。

   a) 次のコマンドを発行して、vCenter ノードにプロキシー権限を付与します。

   ```
   GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
   ```

   このコマンドは、MY_DCNODE および MY_VMCLINODE に、MY_VCNODE の代わりに VM をバックアップおよびリストアする権限を付与します。

   b) 次のコマンドを発行して、データ・センター・ノードにプロキシー権限を付与します。

   ```
   GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
   ```

   このコマンドは、MY_VMCLINODE および MY_DMNODE に、MY_DCNODE の代わりに VM をバックアップおよびリストアする権限を付与します。

   c) (オプション) ご使用環境内の追加のデータ・センター・ノードまたはデータ・ムーバー・ノードにプロキシー権限を付与します。

   d) IBM Spectrum Protect サーバーの Query PROXynode コマンドを発行して、プロキシー関係を検査します。予期されるコマンド出力を以下に示します。

予期されるコマンド出力は次のとおりです。

```
Target Node       Agent Node
--------------    ----------------------------
MY_VCNODE           MY_DCNODE  MY_VMCLINODE
MY_DCNODE           MY_VMCLINODE  MY_DMNODE
```

次のタスク

IBM Spectrum Protect ノードを正常にセットアップした後、次の手動構成タスクは、85 ページの『vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ』の説明に従ってデータ・ムーバー・ノードをセットアップすることです。

vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ

vSphere 環境でバックアップの作業負荷を vStorage バックアップ・サーバーにオフロードする 場合、「データ・ムーバー」ウィザードを使用して、一連のデータ・ムーバー・ノードをセットアップして 操作を実行し、データを IBM Spectrum Protect サーバーに移動することができます。

始める前に

データ・ムーバー・ノードをセットアップする 場合は、構成の変更、必要なサービスの開始、およびセットアップの 検証が必要です。

これらのタスクは、一連のデータ・ムーバー・ノードの作成を簡素化および高速化するプラグイン GUI を使用して実行できます。あるいは、手動で作業を実行できます。詳しくは、86 ページの『vSphere 環境でのデータ・ムーバー・ノードの手動でのセットアップ』 を参照してください。

標準の Data Protection for VMware 環境では、データ・ムーバー・ノードごとに別個の `dsm.opt` ファイル (Windows) または `dsm.sys` ファイル・スタンザ (Linux) が使用されます。vStorage バックアップ・サーバー上の複数のデータ・ムーバー・ノードがデータ重複排除に使用されており、これらのノードが、同じデータ・センター・ノードのデータを移動する権限を持っている場合、それぞれの `dsm.opt` ファイルまたは `dsm.sys` ファイル・スタンザの `dedupcachepath` オプションに異なる値が指定されている必要があります。

物理データ・ムーバー・ノードは、通常は SAN を使用してデータをバックアップおよびリストアします。ストレージ・ボリュームに直接アクセスするようにデータ・ムーバー・ノードを構成する場合は、自動ドライブ名割り当てをオフにしてください。名前の割り当てをオフにしないと、データ・ムーバー・ノード上のクライアントが仮想ディスクの Raw Data Mapping (RDM) を破壊する可能性があります。仮想ディスクの RDM が破損していると、バックアップが失敗します。

制約事項 : Data Protection for VMware は、(データ・ムーバーとして使用される) vStorage バックアップ・サーバー がそれ自体をバックアップするためのスケジューリングをサポートしていません。vStorage バックアップ・サーバーは、必ずその独自のスケジュールから除外するようにしてください。vStorage バックアップ・サーバーを含む VM のバックアップを実行するには、別の vStorage バックアップ・サーバーを使用してください。

上記調整のいずれかを実行する必要がある場合、トピック「vSphere 環境でのデータ・ムーバー・ノードの手動設定」を参照してください。

このタスクについて

vSphere プラグインを使用して、データ・ムーバー・ノードを構成します。

手順

1. vSphere プラグインから、IBM Spectrum Protect を選択します。
2. 「**構成**」タブで、「**データ・ムーバー**」を選択します。
3. 「**データ・ムーバーの追加**」パネルで、ドロップダウン・メニューからデータ・センターを選択します。
4. 必要に応じて、以下のフィールドを編集します。

- **データ・ムーバー名**: ノード名 (ノード接頭部に基づいた推奨名が入力済み)、データ・センター・ノード名、データ・ムーバー名、そして増分番号。
- **データ・ムーバー・ホスト名**
- **vCenter ユーザー**、プラグインを登録したユーザーの名前で既に入力済みです。
- **vCenter のパスワード**

設定が完了したら、「**追加**」をクリックします。

5. 「**結果**」画面が表示されます。
   - 構成済みデータ・ムーバーの名前。
   - オプション・ファイルの場所。このファイルを編集して、データ・ムーバーを構成できます。
   - ログ・ファイルの場所。
   - 使用されたデフォルト・オプション。
6. 「**IBM Spectrum Protect**」>「**データ・ムーバーの構成**」タブを使用して、データ・ムーバーをテストできるようになりました。また、データ・ムーバーを選択し、「**検証**」をクリックするか、データ・ムーバーの次回追加時に状況を確認することで、インストールを確認することもできます。
7. 「**IBM Spectrum Protect**」>「**スケジュール**」タブを使用することで、データ・ムーバーをスケジュールに追加できます。

vSphere 環境でのデータ・ムーバー・ノードの手動でのセットアップ

vSphere 環境でバックアップの作業負荷を vStorage バックアップ・サーバーにオフロードする 場合、データ・ムーバー・ノードを手動でセットアップして操作を実行することで、データを IBM Spectrum Protect サーバーに移動できます。

物理データ・ムーバー・ノードは、通常は SAN を使用してデータをバックアップおよびリストアします。ストレージ・ボリュームに直接アクセスするようにデータ・ムーバー・ノードを構成する場合は、自動ドライブ名割り当てをオフにしてください。 名前の割り当てをオフにしないと、データ・ムーバー・ノード上のクライアントが仮想ディスクの Raw Data Mapping (RDM) を破壊する可能性があります。仮想ディスクの RDM が破損していると、バックアップが失敗します。

必須サービス : 以下の手順に示すように、データ・ムーバーには、クライアント・アクセプター・サービス、リモート・クライアント・エージェント・サービス、およびデータ・ムーバー・スケジューラーが必要です。データ・センターからデータ・ムーバーを削除する場合、これらのサービスをデータ・ムーバーからアンインストールして削除してください。

重要 : データ・ムーバーが Data Protection for VMware vSphere GUI と同じ Windows システムにインストールされており、データ・ムーバー構成中に「**サービスの作成**」が選択されている場合、以下のステップは不要です。

標準の Data Protection for VMware 環境では、データ・ムーバー・ノードごとに別個の `dsm.opt` ファイル (Windows) または `dsm.sys` ファイル・スタンザ (Linux) が使用されます。vStorage バックアップ・サーバー上の複数のデータ・ムーバー・ノードがデータ重複排除に使用されており、これらのノードが、同じデータ・センター・ノードのデータを移動する権限を持っている場合、それぞれの `dsm.opt` ファイルまたは `dsm.sys` ファイル・スタンザの `dedupcachepath` オプションに異なる値が指定されている必要があります。最良の結果を得るには、それぞれの `dsm.opt` ファイルまたは `dsm.sys` ファイル・スタンザに、異なる `schedlogname` および `errorlogname` オプションを指定します。

注 : これらの手順のすべてのステップは、vStorage バックアップ・サーバーで実行されます。

物理データ・ムーバー・ノードは、通常は SAN を使用してデータをバックアップおよびリストアします。ストレージ・ボリュームに直接アクセスするようにデータ・ムーバー・ノードを構成する場合は、自動ドライブ名割り当てをオフにしてください。名前の割り当てをオフにしないと、データ・ムーバー・ノード上のクライアントが仮想ディスクの Raw Data Mapping (RDM) を破壊する可能性があります。仮想ディスクの RDM が破損していると、バックアップが失敗します。

制約事項 : Data Protection for VMware は、データ・ムーバーとして使用される vStorage バックアップ・サーバーについて (それ自体をバックアップする) スケジューリングをサポートしていません。vStorage バックアップ・サーバーは、必ずその独自のスケジュールから除外するようにしてください。データ・ムーバ

ーとして使用される vStorage バックアップ・サーバーをバックアップするには、別の vStorage バックアップ・サーバーを使用してください。

必要な情報の収集

ウィザードでデータ・ムーバー・ノードを作成するときに、GUI ホスト構成ウィザードからデータ・ムーバー情報を収集する必要があります。必要な情報について詳しくは、トピック 27 ページの『構成ワークシート』を参照してください。データ・ムーバーを手動で構成する前に、以下の情報を収集して記録します。

- vCenter のユーザー名とパスワード
- データ・ムーバー・ノード名
- データ・ムーバー・パスワード
- データ・ムーバー・サンプル・オプション

データ・ムーバー名およびサンプル・オプション・ファイルは、以下のプロセスによって後の段階で収集できます。

1. Web ブラウザーを開き、GUI Web サーバーのアドレスを以下のように入力します。 `https://guihost.mycompany.com:9081/TsmVMwareUI/`
2. vCenter のユーザー名およびパスワードを使用してログインし。「構成モード」が選択されていることを確認します。
3. 構成ウィザードで、「**データ・ムーバー・ノード**」ページに進みます。
4. 目的のデータ・ムーバーを見つけ、「**表示**」をクリックします。
5. 「**表示**」タブからサンプル・オプションをオプション ・ファイルにコピーします。
6. ご使用の環境に合わせて、必要に応じてこれらのオプションを更新します。

各プラットフォームに必要なオプションの最小セットは、以下のトピックで示されています。

- 87 ページの『Windows データ・ムーバー・ノードのセットアップ』
- 89 ページの『Linux データ・ムーバー・ノードのセットアップ』

Windows データ・ムーバー・ノードのセットアップ

vStorage バックアップ・サーバーを使用して、Windows データ・ムーバー・ノードをセットアップできます。

始める前に

概念を説明するトピック 86 ページの『vSphere 環境でのデータ・ムーバー・ノードの手動でのセットアップ』 に記載されている情報を収集します。

手順

1. データ・ムーバーのサンプル `dsm.opt` オプション・ファイルのオプションを、`C:\Program Files\Tivoli\TSM\baclient` にあるオプション・ファイルにコピーします。 データ・ムーバーの後にオプション・ファイルを指定します。例えば、`dsm.PREFIX_DATACENTER_DM.opt` のようにします。
2. ご使用の環境に合わせて必要な場合にこれらのオプションを更新できます。 オプションの説明については、クライアント・オプションの解説を参照してください。

   インスタント・アクセス、インスタント・リストア、またはマウント (ファイル・リストア) の操作の場合は、必ず、データ・ムーバーのオプション ・ファイルに VMISCSISERVERADDRESS を追加してください。インスタント操作中に iSCSI データの転送に使用される、vStorage バックアップ・サーバー上のネットワーク・カードの iSCSI サーバー IP アドレスを指定します。ESX ホスト上の iSCSI デバイスにバインドされている物理ネットワーク・インターフェース ・カード (NIC) は、iSCSI の転送に使用される vStorage バックアップ・サーバー上の NIC と同じサブネット上になければなりません。
3. 次のコマンドを発行して、データ・ムーバー・ノードの VMware vCenter ユーザーとパスワードを設定します `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`

必要な管理者権限については、技術情報 7047438 を参照してください。

4. この手順では、IBM Spectrum Protect クライアント GUI 構成ウィザードを使用して、クライアント・アクセプター・サービスおよびスケジューラー・サービスをセットアップします。デフォルトでは、リモート・クライアント・エージェント・サービスもウィザードを使用してセットアップされます。このタスクに IBM Spectrum Protect クライアント・サービス構成ユーティリティー (dsmcutil) を使用する場合は、リモート・クライアント・エージェント・サービスも必ずインストールする必要があります。以下のタスクを実行して、クライアント・アクセプター・サービスおよびデータ・ムーバー・スケジューラー・サービスをセットアップします。
5. 以下のタスクを実行して、クライアント・アクセプター・サービスおよびデータ・ムーバー・スケジューラー・サービスをセットアップします。

   - この手順では、IBM Spectrum Protect クライアント GUI 構成ウィザードを使用して、クライアント・アクセプター・サービスおよびスケジューラー・サービスをセットアップします。デフォルトでは、リモート・クライアント・エージェント・サービスもウィザードを使用してセットアップされます。このタスクに IBM Spectrum Protect クライアント・サービス構成ユーティリティー (**dsmcutil**) を使用する場合は、リモート・クライアント・エージェント・サービスも必ずインストールしてください。

     「**ユーティリティー**」>「**セットアップ・ウィザード**」に進み、ファイル・メニューから IBM Spectrum Protect クライアント構成ウィザードを開始します。

     –「**TSM Web クライアントの構成**」を選択します。 プロンプトに従って情報を入力します。

       a.「いつサービスを開始しますか?」オプションで、「**Windows のブート時に自動で行う**」を選択します。

       b.「このウィザードの完了時にサービスを開始しますか?」オプションで「**はい**」を選択します。

     操作が正常に完了したら、ウィザードのウェルカム・ページに戻ります。

     ヒント: 同じマシン上で複数のデータ・ムーバー・ノードを構成する場合は、各クライアント・アクセプター・インスタンスに別々のポート値を指定する必要があります。

     –「TSM クライアント・スケジューラーの構成」を選択します。 プロンプトに従って情報を入力します。

       a. スケジューラー名を入力する場合は、必ず「**スケジューラーを管理するためのクライアント・アクセプター・デーモン (CAD) の使用**」オプションを選択してください。

       b.「いつサービスを開始しますか?」オプションで、「**Windows のブート時に自動で行う**」を選択します。

       c.「このウィザードの完了時にサービスを開始しますか?」オプションで「**はい**」を選択します。

タスクの結果

構成設定を確認するには、以下のようにします。

1. -asnodename および -optfile のコマンド・ライン・パラメーターを指定して、dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt でデータ・ムーバーのコマンド・ライン・セッションを開始します。

   初回サインオンの後に、パスワードを求めるプロンプトが出されないことを確認してください。

   

   重要: IBM Spectrum Protect スケジューラーの失敗を防止するために、asnodename オプションが dsm.opt ファイル (Windows) または dsm.sys ファイル・スタンザ (Linux) で設定されていないことを確認してください。 スケジューラーは、IBM Spectrum Protect サーバーに asnodename (データ・センター・ノード) ではなく nodename (データ・ムーバー・ノード) に関連付けられているスケジュールを照会します。 asnodename が dsm.opt または dsm.sys で設定されていると、(nodename ではなく) asnodename に関連付けられているスケジュールが照会されます。その結果、スケジューリング操作は失敗します。

以下のタスクを実行します。

1. 次のコマンドを発行して、IBM Spectrum Protect サーバーとの接続を確認します。

```
dsmc query session
```

このコマンドは、セッションに関する情報 (現行ノード名、セッションが確立された時刻、サーバー情報、およびサーバー接続情報を含む) を表示します。

2. 以下のコマンドを発行して、VM をバックアップできることを確認します。

```
dsmc backup vm vm1
```

ここで、 vm1 は VM の名前です。

3. 次のコマンドを発行して、バックアップが正常に完了したことを確認します。

```
dsmc query vm "*"
```

4. 次のコマンドを発行して、VM をリストアできることを確認します。

```
dsmc restore vm vm1 -vmname=vm1-restore
```

5. クライアント・アクセプターとエージェントが正しくセットアップされていることを確認します。
   a. Web ブラウザーに IBM Spectrum Protect vSphere Client プラグイン・アドレスを入力します。例えば、次のようにします。

```
https://guihost.mycompany.com/vsphere-client/
```

   b. vCenter のユーザー名およびパスワードを使用してログインします。
   c. vSphere Web Client で、「**IBM Spectrum Protect**」 > 「**構成**」 > 「**データ・ムーバー**」をクリックします。
   d. データ・ムーバーの「**ステータス**」列に「**検証済み**」が表示されていることを確認します。「**失敗**」が表示された場合、ステータス上にマウスを移動して、障害のメッセージを表示します。

      ヒント : Data Protection for VMware vSphere GUI がインストールされているシステムで IP アドレスが変更された場合は、以下を実行する必要があります。

   e. トラブルシューティング で説明されているタスクを完了してください。
   f. Data Protection for VMware vSphere GUI で操作が使用可能になるように、クライアント・アクセプターを再度セットアップします。そうしないと、プラグイン・マネージャーにより、Data Protection for VMware vSphere GUI の状況が使用不可と表示されます。

関連タスク

83 ページの『拡張構成タスク』
使用可能なアプリケーション・インターフェースを 使用して各コンポーネントを手動で構成し、検査する必要があります。

Linux データ・ムーバー・ノードのセットアップ

vStorage バックアップ・サーバーを使用して、Linux データ・ムーバー・ノードをセットアップできます。

始める前に

概念を説明するトピック 86 ページの『vSphere 環境でのデータ・ムーバー・ノードの手動でのセットアップ』 に記載されている情報を収集します。

このタスクについて

手順

1. Java の Linux インストール場所 `export JAVA_HOME=/opt/tivoli/tsm/tdpvmware/common/jre/jre` にある IBM のインストール済み Java バージョンを使用します。
2. 関連する環境変数を設定します。

a. JAVA_HOME 環境変数が正しくエクスポートされていることを確認します。

```
JAVA_HOME=<jre-or-jdk-install-dir>
```

b. PATH 環境変数が正しくエクスポートされていることを確認します。

```
export PATH=$PATH:$JAVA_HOME/jre/bin
```

3. 以下のタスクを実行して、クライアント・アクセプター・サービスおよびデータ・ムーバー・スケジューラー・サービスをセットアップします。

- **Linux でデータ・ムーバーを構成します。**

  Linux のデータ・ムーバーの場合は、ご使用の Linux OS とバージョン (**systemd** または **SysV**) に応じて、適切な構成方法を使用します。これらについて、以下のセクションで説明します。

  systemd を使用して Linux でデータ・ムーバーを構成するには、以下のステップを実行します。

  この手順の例では、PREFIX_DATACENTER_DM がノード名として使用されています。

  a. 以下のスクリプトを /etc/systemd/system をコピーして、それに dsmcad@PREFIX_DATACENTER_DM.service と名前を付けます。

```
#!/bin/bash
#
# (C) Copyright IBM Corporation 2018
#
# chkconfig: 35 95 5
# description: IBM Spectrum Protect Client Acceptor Daemon
#
### BEGIN INIT INFO
# Provides: dsmcad
# Required-Start: $local_fs $remote_fs $network $syslog
# Required-Stop:
# Default-Start: 3 5
# Default-Stop: 0 1 2 6
# Short-Description: IBM Spectrum Protect Client Acceptor Daemon
# Description: Start dsmcad to enable scheduler and Web GUI.
### END INIT INFO
# SERVERNAME referenced in dsm.$SERVERNAME.opt and dsm.sys
SERVERNAME=LNX11L_DATACENTER_DM1
DSMCAD_DIR=/opt/tivoli/tsm/client/ba/bin
DSMCAD_BIN=$DSMCAD_DIR/dsmcad
OPTION_FILE=$DSMCAD_DIR/dsm.$SERVERNAME.opt
PID_FILE=/var/run/dsmcad-$SERVERNAME.pid
export JAVA_HOME=/opt/tivoli/tsm/tdpvmware/common/jre/jre
export LD_LIBRARY_PATH=$DSMCAD_DIR:$JAVA_HOME/lib/amd64/classic
export PATH=$JAVA_HOME/bin:$PATH
createPidFile()
{
  pid=`pgrep -f $OPTION_FILE`
  pidarr=($pid)
    if [ -n "${pidarr[1]}" ]
    then
       echo ${pidarr[1]} > $PID_FILE
    else
      echo ${pidarr[0]} > $PID_FILE
    fi
}
removePidFile()
{
  if [ -f $PID_FILE ]
  then
    rm -f $PID_FILE
  fi}
```

  SERVERNAME がノード名に設定されるようにスクリプトを更新します。

  b. このスクリプトにさらなる変更を加える必要はありません。スクリプトに 664 許可があることを確認するには、コマンド chmod 664 dsmcad@.service を発行します。

  c. /opt/tivoli/tsm/client/ba/ba/ba/bin に dsm.PREFIX_DATACENTER_DM.opt という名前のテキスト・ファイルを作成して、設定 servername PREFIX_DATACENTER_DM を追加します。

d. /opt/tivoli/tsm/client/ba/ba/bin に dsm.sys を作成し、データ・ムーバーのサンプル・オプションを追加します。

   オプションの説明については、オプションの解説を参照してください。

   インスタント・アクセス、インスタント・リストア、またはマウント (ファイル・リストア) の操作の場合は、必ず、データ・ムーバーのオプション・ファイルに VMISCSISERVERADDRESS を追加する必要があります。インスタント操作中に iSCSI データの転送に使用される、vStorage バックアップ・サーバー上のネットワーク・カードの iSCSI サーバー IP アドレスを指定します。ESX ホスト上の iSCSI デバイスにバインドされている物理ネットワーク・インターフェース ・カード (NIC) は、iSCSI の転送に使用される vStorage バックアップ・サーバー上の NIC と同じサブネット上になければなりません。

e. 構成ファイルを作成した後、vCenter 資格情報を保管して、データ・ムーバーやマウント・プロキシーが vCenter インベントリーにアクセスできるようにします。/opt/tivoli/tsm/client/ba/bin に移動して、コマンド `./dsmc set password -type=VM fullyqualifieddomainnameofvcenter vcenteruserid vcenterpassword` を実行します。

   必要な管理者権限については、技術情報 7047438 を参照してください。

f. サービスの使用を開始するには、次の 3 つのコマンドを発行します。

   - `systemctl daemon-reload`
   - `systemctl enable dsmcad@PREFIX_DATACENTER_DM.service`
   - `systemctl start dsmcad@PREFIX_DATACENTER_DM.service`

g. 1 つのデータ・ムーバーを構成したら、Web クライアント・プラグイン GUI を使用して、追加のデータ・ムーバーまたはマウント・プロキシーを追加できます。

注 : PREFIX_DATACENTER_DM に関連付けられたサービスを、確実にシステムのリブート時に自動再始動するには、コマンド `systemctl enable dsmcad@PREFIX_DATACENTER_DM.service` を実行します。

サービスを停止するには、コマンド `systemctl stop dsmcad@PREFIX_DATACENTER_DM.service` を実行します。

注 : IBM Spectrum Protect をアンインストールする 場合は、関連するサービスを停止して削除する必要があります。

- 上記の stop コマンドを使用して dsmcad サービスを停止します。
- コマンド `systemctl disable dsmcad@PREFIX_DATACENTER_DM.service` を使用してサービスを無効にします。
- dsmcad@.service を /etc/systemd/system ディレクトリーから削除します。

SysV を使用してデータ・ムーバーを Linux に構成するには、以下のステップを実行します。

この手順の例では、PREFIX_DATACENTER_DM がノード名として使用されています。

a. 提供された rc.dsmcad スクリプトをコピーし、SERVERNAME がノード名 SERVERNAME=PREFIX_DATACENTER_DM に設定されるようにスクリプトを更新します。

b. ファイルを /etc/init.d/dsmcad.PREFIX_DATACENTER_DM という名前で保存します。

c. `chmod 755 dsmcad.PREFIX_DATACENTER_DM` を使用してファイルに 755 許可があることを確認します。

d. /opt/tivoli/tsm/client/ba/ba/ba/bin に dsm.PREFIX_DATACENTER_DM.opt という名前のテキスト・ファイルを作成して、設定 `servername PREFIX_DATACENTER_DM` を追加します。

e. /opt/tivoli/tsm/client/ba/ba/bin に dsm.sys を作成し、データ・ムーバーのサンプル・オプションを追加します。

   オプションの説明については、オプションの解説を参照してください。

インスタント・アクセス、インスタント・リストア、またはマウント (ファイル・リストア) の操作の場合は、必ず、データ・ムーバーのオプション・ファイルに VMISCSISERVERADDRESS を追加する必要があります。インスタント操作中に iSCSI データの転送に使用される、vStorage バックアップ・サーバー上のネットワーク・カードの iSCSI サーバー IP アドレスを指定します。ESX ホスト上の iSCSI デバイスにバインドされている物理ネットワーク・インターフェース・カード (NIC) は、iSCSI の転送に使用される vStorage バックアップ・サーバー上の NIC と同じサブネット上になければなりません。

f. 構成ファイルを作成した後、vCenter 資格情報を保管して、データ・ムーバーやマウント・プロキシーが vCenter インベントリーにアクセスできるようにします。/opt/tivoli/tsm/client/ba/bin に移動して、コマンド ./dsmc set password –type=VM fullyqualifieddomainnameofvcenter vcenteruserid vcenterpassword を実行します。

必要な管理者権限については、技術情報 7047438 を参照してください。

g. /opt/tivoli/tsm/client/ba/bin に移動して、コマンド ./dsmc set password type=VM fullyqualifieddomainname vcenteruserid vcenterpassword を実行します。

h. 使用している OS に応じて、以下のコマンドのいずれかを実行します。

- Red Hat: chkconfig - - add dsmcad.PREFIX_DATACENTER_DM
- SUSE: chkconfig - - add dsmcad.PREFIX_DATACENTER_DM
- Ubuntu: update-rc.d dsmcad.PREFIX_DATACENTER_DM defaults

i. 次のコマンドを実行します。service dsmcad.PREFIX_DATACENTER_DM start

j. 1 つのデータ・ムーバーを構成したら、Web クライアント・プラグイン GUI を使用して、追加のデータ・ムーバーまたはマウント・プロキシーを追加できます。

注: chkconfig コマンドを実行すると、dsmcad.PREFIX_DATACENTER_DM はシステムのリブート時に再始動します。

サービスを開始するには次のコマンドを実行します。service dsmcad.PREFIX_DATACENTER_DM start

サービスを停止するには次のコマンドを実行します。service dsmcad.PREFIX_DATACENTER_DM stop

注: IBM Spectrum Protect をアンインストールする場合は、関連するサービスを停止する必要があります。

- 上記の stop コマンドを使用して dsmcad サービスを停止します。
- 補助ファイル (/var/run/dsmcad.PREFIX_DATACENTER_DM.pid など) が削除されるように、コマンド systemctl disable dsmcad@PREFIX_DATACENTER_DM.service を使用してサービスを無効にします。
- RHEL または SLES では、コマンド chkconfig --del dsmcad.PREFIX_DATACENTER_DM を使用します。
- Ubuntu では、コマンド update-rc.d dsmcad.PREFIX_DATACENTER_DM remove を使用します。
- dsmcad.* ファイルを /etc/init.d ディレクトリーから削除します。

タスクの結果

1. -asnodename および -optfile のコマンド・ライン・パラメーターを指定して、dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt でデータ・ムーバーのコマンド・ライン・セッションを開始します。

   初回サインオンの後に、パスワードを求めるプロンプトが出されないことを確認してください。

重要 : IBM Spectrum Protect スケジューラーの失敗を防止するために、asnodename オプションが dsm.opt ファイル (Windows) または dsm.sys ファイル・スタンザ (Linux) で設定されていないことを確認してください。 スケジューラーは、IBM Spectrum Protect サーバーに asnodename (データ・センター・ノード) ではなく nodename (データ・ムーバー・ノード) に関連付けられているスケジュールを照会します。 asnodename が dsm.opt または dsm.sys で設定されていると、(nodename ではなく) asnodename に関連付けられているスケジュールが照会されます。その結果、スケジューリング操作は失敗します。

以下のタスクを実行します。

1. 次のコマンドを発行して、IBM Spectrum Protect サーバーとの接続を確認します。

   ```
   dsmc query session
   ```

   このコマンドは、セッションに関する情報 (現行ノード名、セッションが確立された時刻、サーバー情報、およびサーバー接続情報を含む) を表示します。
2. 以下のコマンドを発行して、VM をバックアップできることを確認します。

   ```
   dsmc backup vm vm1
   ```

   ここで、 vm1 は VM の名前です。
3. 次のコマンドを発行して、バックアップが正常に完了したことを確認します。

   ```
   dsmc query vm "*"
   ```
4. 次のコマンドを発行して、VM をリストアできることを確認します。

   ```
   dsmc restore vm vm1 -vmname=vm1-restore
   ```
5. クライアント・アクセプターとエージェントが正しくセットアップされていることを確認します。
   a. Web ブラウザーに IBM Spectrum Protect vSphere Client プラグイン・アドレスを入力します。例えば、次のようにします。

      ```
      https://guihost.mycompany.com/vsphere-client/
      ```

   b. vCenter のユーザー名およびパスワードを使用してログインします。
   c. vSphere Web Client で、「**IBM Spectrum Protect**」 > 「**構成**」 > 「**データ・ムーバー**」をクリックします。
   d. データ・ムーバーの「**ステータス**」列に「**検証済み**」が表示されていることを確認します。「**失敗**」が表示された場合、ステータス上にマウスを移動して、障害のメッセージを表示します。

      ヒント : Data Protection for VMware vSphere GUI がインストールされているシステムで IP アドレスが変更された場合は、以下を実行する必要があります。
   e. トラブルシューティング で説明されているタスクを完了してください。
   f. Data Protection for VMware vSphere GUI で操作が使用可能になるように、クライアント・アクセプターを再度セットアップします。そうしないと、プラグイン・マネージャーにより、Data Protection for VMware vSphere GUI の状況が使用不可と表示されます。

vSphere 環境での Data Protection for VMware コマンド・ライン・インターフェースの構成

Data Protection for VMware vSphere GUI がインストールされているシステムで、Data Protection for VMware コマンド・ライン・インターフェース のプロファイルを更新します。

始める前に

プロファイル (vmcliprofile) は、Data Protection for VMware vSphere GUI がインストールされているシステムの次のディレクトリーに置かれています。

Linux /opt/tivoli/tsm/tdpvmware/common/scripts

Windows 64 ビット: C:¥Program Files¥IBM¥SpectrumProtect¥Framework¥VEGUI¥scripts

このタスクについて

この手順のすべてのステップは、Data Protection for VMware vSphere GUI がインストールされているシステムで実行されます。

ヒント: このタスクは、Data Protection for VMware vSphere GUI 構成ウィザードまたは構成ノートブックを使用して完了することもできます。Data Protection for VMware vSphere GUI の「**構成**」ウィンドウに進み、「**構成ウィザードの実行**」または「**構成の編集**」をクリックします。

手順

1. 以下の設定を使用してプロファイルを更新します。

   VE_TSMCLI_NODE_NAME
   Data Protection for VMware コマンド・ライン・インターフェース を IBM Spectrum Protect サーバーおよびエージェント・ノード (MY_VMCLINODE) に接続するノードを指定します。

   制約事項: VMCLI ノードは、IBM Spectrum Protect サーバーと通信する時に SSL プロトコルまたは LDAP 認証をサポートしません。

   VE_VCENTER_NODE_NAME
   vCenter を表す仮想ノード (MY_VCNODE) を指定します。

   VE_DATACENTER_NAME
   データ・センターへマップされる仮想ノードを指定します。正しい構文は次のとおりです。
   `datacenter_name::datacenter_node_name`

   - `datacenter_name` 値には、大/小文字の区別があります。
   - ご使用の環境内のデータ・センターごとに、必ずこのパラメーター (MY_DCNODE) を設定してください。
   - Data Protection for VMware vSphere GUI は、vCenter 内で同じ名前を持つ複数のデータ・センターをサポートしません。

   VE_TSM_SERVER_NAME
   IBM Spectrum Protect サーバーのホスト名または IP を指定します。

   VE_TSM_SERVER_PORT
   IBM Spectrum Protect サーバーに使用するポート名を指定します。デフォルト値は 1500 です。

   これらの設定を使用したプロファイルの例は次のとおりです。

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

2. pwd.txt ファイルで VMCLI ノードのパスワードを設定します。

   このパスワードは、Data Protection for VMware コマンド・ライン・インターフェース を IBM Spectrum Protect サーバーおよび データ・ムーバー・ノードに接続するノード用です。 これは、VE_TSMCLI_NODE_NAME プロファイル・パラメーターによって指定されます。

   a) echo コマンドを発行して、パスワードを含むテキスト・ファイルを作成します。

   Linux
   ```
   echo password1 > pwd.txt
   ```
   Windows
   ```
   echo password1> pwd.txt
   ```

   Windows パスワード (password1) と右不等号 (>) の間にスペースが存在してはなりません。

   b) 以下の vmcli コマンドを発行して、VMCLI ノードのパスワードを設定します。
   ```
   vmcli -f set_password -I pwd.txt
   ```

重要：

- Linux `vmcli -f set_password` コマンドは、root としてではなく、tdpvmware ユーザーとして発行する必要があります。
- Linux Windows アプリケーション保護レポートを生成する計画の場合は、**-type VMGuest** パラメーターを指定して、パスワードが VM に適用されるように指定する必要があります。 例えば、次のようにします。

```
vmcli -f set_password -type VMGuest -I password.txt
```

3. Data Protection for VMware コマンド・ライン・インターフェースが実行中であることを確認します。

   Windows 「**スタート**」 > 「**コントロール パネル**」 > 「**管理ツール**」 > 「**サービス**」をクリックし、Data Protection for VMware コマンド・ライン・インターフェースの状況が「開始」であることを確認します。

   Linux スクリプト・ディレクトリー (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) に進み、次のコマンドを発行します。

```
./vmclid status
```

   - デーモンが実行中である場合、ステップ 4 に進みます。
   - デーモンが実行中でない場合は、次のコマンドを発行してデーモンを手動で開始します。

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

     また、以下の init スクリプトを、デーモンの停止と開始に使用できます。

```
./vmclid stop
./vmclid start
```

4. 次の vmcli コマンドを発行して、Data Protection for VMware コマンド・ライン・インターフェースが IBM Spectrum Protect ノード構成を認識することを確認します。

```
vmcli -f inquire_config -t TSM
```

5. ノードを検証して、構成エラーが発生していないことを確認します。
   a) vSphere Client の「ソリューションとアプリケーション」ウィンドウのアイコンをクリックして、Data Protection for VMware vSphere GUI を開始します。
   b)「**構成**」ウィンドウに進みます。
   c) 表からノードを選択し、「**選択されたノードの検証**」を選択します。「**状況の詳細**」ペインに状況情報が表示されます。

次のタスク

Linux Windows 以下のセクションで説明されている 3 つの手動構成タスクを正常に完了した後は、

1. 83 ページの『vSphere 環境での IBM Spectrum Protect ノードのセットアップ』
2. 85 ページの『vSphere プラグイン GUI を使用したデータ・ムーバー・ノードのセットアップ』

VM データをバックアップするために必要な追加タスクはありません。

vSphere 環境のコマンド・ライン・インターフェース構成のチェックリスト

この手順は、コマンド・ライン・インターフェースを 使用して、vSphere 環境の Data Protection for VMware を構成する場合にのみ使用してください。

手順

IBM Spectrum Protect サーバーのステップ 1 とステップ 2 を完了します。

1. 以下のノードを IBM Spectrum Protect サーバーに登録します。

a) VMware vCenter を表すノード (vCenter ノード):

```
REGister Node MY_VCNODE <password for MY_VCNODE>
```

b) IBM Spectrum Protect と Data Protection for VMware vSphere GUI の間の通信を行うノード (VMCLI ノード):

```
REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
```

c) データ・センターを表し、VM データが保管されるノード (データ・センター・ノード):

```
REGister Node MY_DCNODE <password for MY_DCNODE>
```

d) 1 つのシステムから別のシステムに「データを移動する」ノード (データ・ムーバー・ノード):

```
REGister Node MY_DMNODE <password for MY_DMNODE>
```

2. これらのノードのプロキシー関係を定義します。

a) 次のコマンドを発行して、vCenter ノードにプロキシー権限を付与します。

```
GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

このコマンドは、MY_DCNODE と MY_VMCLINODE に、MY_VCNODE の代わりに VM をバックアップおよびリストアする権限を付与します。

b) 次のコマンドを発行して、データ・センター・ノードにプロキシー権限を付与します。

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

このコマンドは、MY_VMCLINODE と MY_DMNODE に、MY_DCNODE の代わりに VM をバックアップおよびリストアする権限を付与します。

c) (オプション) ご使用環境内の追加のデータ・センター・ノードまたはデータ・ムーバー・ノードにプロキシー権限を付与します。

d) IBM Spectrum Protect サーバーの Query PROXynode コマンドを発行して、プロキシー関係を検査します。予期されるコマンド出力を以下に示します。

```
Target Node       Agent Node
--------------    ------------------------------
MY_VCNODE               MY_DCNODE  MY_VMCLINODE
MY_DCNODE             MY_VMCLINODE  MY_DMNODE
```

vStorage バックアップ・サーバーでステップ 3 から 9 までを完了します。

3. 以下のデータ・ムーバー・オプションに適切な値を設定します。

- Windows dsm.opt オプション・ファイルで以下のオプションを指定します。
- Linux dsm.sys ファイルのデータ・ムーバー・ノードに関するスタンザで、以下のオプションを指定します。

```
NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPORT
COMMMETHOD
HTTPPORT
```

注: HTTPPORT は、複数のクライアント・アクセプター・サービス (CAD) が使用されている場合にのみ必要です。例えば、2 つのデータ・ムーバー・ノード (および 2 つの CAD サービス) がある場合、各データ・ムーバー・ノードのオプション・ファイルは、異なる HTTPPORT 値を指定している必要があります。

以下に、これらのオプションが指定されたサンプル dsm.dm.opt ファイルを提供します。

```
NODename MY_DMNODE
PASSWORDAccess generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort 1500
COMMMethod tcpip
HTTPPORT    1583
```

4. 次のコマンドを発行して、IBM Spectrum Protect サーバーとの接続を確認します。
   `dsmc query session`
5. 次のコマンドを発行して、データ・ムーバー・ノードの VMware vCenter ユーザーとパスワードを設定します。
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
6. 以下の IBM Spectrum Protect サービスをセットアップします。
   - Windows
     a. スケジューラー・サービスをインストールします。
     ```
     dsmcutil install scheduler /name:"TSM Central Scheduler Service"
     /node:MY_DMNODE   /password:MY_DMNODEPWD /startnow:no /autostart:no
     ```
     b. CAD をインストールします。
     ```
     dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
     /password:MY_DMNODEPWD /optfile:c:¥tsm¥baclient¥dsm.dm.opt
     /cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
     ```
     c. リモート・クライアント・エージェント・サービスをインストールします。
     ```
     dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
     /password:MY_DMNODEPWD /optfile:c:¥tsm¥baclient¥dsm.dm.opt
     /partnername:"TSM CAD - MY_DMNODE" /startnow:no
     ```
   - Linux `dsm.sys` ファイルで、データ・ムーバー・ノードのスタンザに、`managedservices` オプションを指定します。
     `schedule` パラメーターと `webclient` パラメーターを必ず指定します。
     ```
     managedservices schedule webclient
     ```
     この設定は、クライアント・アクセプターが Web クライアントとスケジューラーの 両方を管理することを指示します。
7. Linux
   クライアント・アクセプター・サービスを開始します。
   インストール・プログラムは、クライアント・アクセプター・デーモン (`dsmcad`) の始動スクリプトを `/etc/init.d` に作成します。クライアント・アクセプター・デーモンは、スケジューラー・タスクまたは Web クライアントを管理する前に開始する必要があります。次のコマンドを root として使用して、デーモンを開始します。
   ```
   service dsmcad start
   ```
   システムの再始動後にクライアント・アクセプター・デーモンが自動的に開始されるようにするには、シェル・プロンプトで以下のようにサービスを追加します。
   ```
   # chkconfig --add dsmcad
   ```
8. IBM Spectrum Protect サービスが正しくセットアップされていることを確認します。
   a) リモート・システムにログオンします。
   b) Web ブラウザーを使用して、次のアドレスとポートを使用し、HOST1 システムに接続します。

```
http://HOST1.xyz.yourcompany.com:1581
```

Data Protection for VMware vSphere GUI がインストールされているシステムでステップ 10 を完了します。

9. Data Protection for VMware コマンド・ライン・インターフェース プロファイル (vmcliprofile) 内の以下のオプションに適切な値を設定します。

```
VE_TSMCLI_NODE_NAME
VE_VCENTER_NODE_NAME
VE_DATACENTER_NAME
VE_TSM_SERVER_NAME
VE_TSM_SERVER_PORT
```

これらのオプションを使用したプロファイルの例は次のとおりです。

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

このプロファイルは以下のディレクトリーにあります。

Linux /opt/tivoli/tsm/tdpvmware/common/scripts

Windows 64 ビット: C:¥Program Files¥IBM¥SpectrumProtect¥Framework¥VEGUI¥scripts

a) VMCLI ノードのパスワードを設定します。

1) echo コマンドを発行して、パスワードを含むテキスト・ファイルを作成します。

Linux
```
echo password1 > pwd.txt
```

Windows
```
echo password1> pwd.txt
```

2) 以下の vmcli コマンドを発行して、VMCLI ノードのパスワードを設定します。

重要 : Linux このコマンドは、root としてではなく、tdpvmware ユーザーとして発行する必要があります。

```
vmcli -f set_password -I pwd.txt
```

b) Data Protection for VMware コマンド・ライン・インターフェース が実行中であることを確認します。

Windows Windows コマンド・プロンプトから次のを発行します。

```
net start
```

Linux 次のコマンドを出します。

```
./vmclid status
```

c) 次の vmcli コマンドを発行して、Data Protection for VMware コマンド・ライン・インターフェースが IBM Spectrum Protect ノード構成を認識することを確認します。

```
vmcli -f inquire_config -t TSM
```

テープ構成のガイドライン

テープ・ストレージに対してバックアップ操作を試行する前に、以下のガイドラインを確認してください。

テープへのバックアップの準備

Linux Windows テープへのバックアップを試行する前に、以下のパラメーターがテープ・バックアップ用に IBM Spectrum Protect サーバーで設定されなければなりません。

1. 管理クラスの定義:

```
define mgmtclass <domain name> <policy set name> <mgmtclass name>
```

例えば、次のようにします。

```
define mgmtclass tape tape DISK
```

2. コピー・グループを定義します。

```
define copygroup <domain name> <policy set name> <mgmtclass name>
destination=<stgpool name>
```

例えば、次のようにします。

```
define copygroup tape tape DISK destination=Diskpool
```

3. ポリシー・セットを活動化します。

```
activate policyset <domain name> <policy set name>
```

例えば、次のようにします。

```
activate policyset tape tape
```

物理的なテープに対するバックアップを構成する場合は、追加の構成要件があります。 常にディスク上に IBM Spectrum Protect メタデータ (制御ファイル)、テープ上に VM の実際のバックアップ・データを保持しておく必要があります。

- デフォルト管理クラス以外の管理クラスで、VMMC オプションを使用して VMware バックアップ (および VMware 制御ファイル) を保管します。
- VMCTLMC オプションを使用して、特に VMware 制御ファイル用に VMware バックアップ時に使用する管理クラスを指定します。 ユーザーが指定した管理クラスは、デフォルト管理クラスを指定変更します。 さらに、VMMC オプションによって指定された管理クラスを指定変更します。 VMCTLMC 管理クラスは、テープにマイグレーションされないディスク ・ストレージ・プールを指定しなければなりません。
- VM バックアップでの保存を制御するには、常に VMMC オプションを使用します。 このオプションは、ディスク構成とテープ構成の両方に適用されます。 VMCTLMC は制御ファイルの保存には使用されません。 制御ファイルとデータ・ファイルは同じグループに含まれており、VMMC オプションの保存ポリシーに基づいて同時に有効期限が切れます。 両方のオプションが設定されていると、VMMC はデータ・ファイルに使用され、VMCTLMC は制御ファイルに使用されます。

制約事項 : LAN フリー構成のストレージ・エージェントを使用するリストア操作では、データが 1 次ストレージ・プールから取得可能であっても、コピー・ストレージ・プールからファイルをリストアする場合があります。これは、リストア要求が特定のファイルを対象とする場合、またはリストア要求が no-query メソッドを使用しない場合、および LAN フリー・パスを経由してアクセスできないストレージ・プールにファイルの 1 次コピーが保管されている場合に起こることがあります。これは、Data Protection for VMware バックアップ操作など、リストア以外の状況にも影響を与える可能性があります。Data Protection for VMware 環境の VM 制御ファイルの推奨ストレージ・メソッドはディスクです。したがって、増分バックアップ処理時にはファイルをリストアするためのマウントが必要なくなります。これらの VM 制御ファイルは、ディスク上に配置する必要があるだけではなく、LAN フリー・パスを介して使用できるコピー・ストレージ・プールへのバックアップが禁止されています。バックアップする場合は、Data Protection for VMware クライアントからの LAN フリーの増分バックアップ時にファイルをリストアするために、テープ・マウントが使用されます。

IBM Spectrum Protect サーバー環境でディスクからテープへのマイグレーションを 使用する場合、マイグレーションの前に、以下のガイドラインを考慮してください。

- ディスク・ストレージ・プールの MIGDELAY を、ディスクからのマウント要求を最も満たす値に設定します。 標準的な使用パターンは、高い割合で個々のファイル・リカバリーが数日以内に発生していることを示します。 例えば、ファイルの最終変更日時から、通常 3 日ないし 5 日です。 このため、リカバリー操作を最適化するために、この短い期間、データをディスクに保持することを考慮してください。

さらに、ディスク・ストレージ・プールでクライアント・サイド重複排除が使用されている場合は、頻度の高い VM バックアップに対応した MIGDELAY オプションを設定してください。 VM で少なくとも 2 回のフルバックアップが実行されるまで、重複排除されたストレージ・プールからテープにデータをマイグレーションしないでください。 データがテープに移動すると、そのデータは重複排除されなくなります。例えば、フルバックアップを 週次で実行する場合は、MIGDELAY を 10 日以上の値に設定することを検討してください。この設定により、それぞれのフルバックアップで、テープへの移動前に前回のバックアップからの重複データが認識されて使用されます。

- DISK デバイス・クラスのストレージ・プールではなく、デバイス・クラス・ファイルのストレージ・プールを使用します。 デバイス・クラス MAXCAPACITY パラメーターで指定される、ボリューム・サイズの標準的な値は 8 GB から 16 GB です。 関連ストレージ・プールに対して、ファイル・スペースごとにコロケーションを適用することを検討してください。 バックアップされる各 VM は、IBM Spectrum Protect サーバーで個別のファイル・スペースとして表されます。 ファイル・スペースごとのコロケーションにより、特定の VM に対する複数の増分バックアップのデータが同じボリューム (ディスク・ファイル) に保存されます。 テープへのマイグレーションが行われると、ファイル・スペースごとのコロケーションにより、特定の VM に対する複数の増分バックアップが物理的なテープ上に一緒に置かれます。

「**設定**」ダイアログを使用して、テープ・モード値を設定してください。

マウントまたはインスタント・リストア操作で、バックアップ操作によって同じテープ・ストレージが同時に使用中であることが必要な場合、そのバックアップ操作は中断されます。

Linux Linux システム上の iSCSI 装置の手動構成

この手順では、iSCSI マウント操作時に使用される Linux システムの構成方法について説明します。 VM スナップショットは、IBM Spectrum Protect サーバー・ストレージからマウントされます。

始める前に

iSCSI マウント中に、iSCSI ターゲットが Recovery Agent システム上に作成されます。Recovery Agent システムに、Microsoft iSCSI イニシエーターは必要ありません。

ヒント: Red Hat Enterprise Linux および SUSE Linux Enterprise Server では、Open-iSCSI イニシエーターが提供されています。

このタスクを実行する前に、以下の iSCSI 要件を確認してください。

- 任意のシステムから iSCSI ターゲットに接続し、バックアップ・データを含めるボリュームを作成することができます。 このボリュームを他のシステムからマウントすることができます。
- iSCSI ターゲットに接続する必要があるシステムでは、iSCSI イニシエーターが必要です。
- データをリストアするシステム上に、iSCSI イニシエーターがインストールされている必要があります。
- 1 つのボリュームが複数のディスクにわたる場合、必要なすべてのディスクをマウントする必要があります。 ミラーリングされたボリュームが使用される場合は、ミラーリングされたディスクの 1 つのみをマウントしてください。 1 つのディスクをマウントすると、時間のかかる同期操作がなくなります。

このタスクについて

iSCSI マウント操作時に使用される Linux システムを構成するには、以下のステップを実行します。

手順

1. データをリストアするシステム上の iSCSI イニシエーター名を記録します。
   iSCSI イニシエーター名は、`/etc/iscsi/initiatorname.iscsi` ファイルに入っています。
   `InitiatorName=` 値が空の場合は、次のコマンドを使用してイニシエーター名を作成します。

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   以下は、イニシエーター名の例です。

   ```
   iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

2. イニシエーター名を `/etc/iscsi/initiatorname.iscsi` ファイルに追加します。

a) **vi** コマンドを使用して、/etc/iscsi/initiatorname.iscsi ファイルを編集します。 例えば、次のようにします。

```
twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
```

b) イニシエーター名を指定して、**InitiatorName=** パラメーターを更新します。 例えば、次のようにします。

```
InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

3. recovery agent (または iSCSI ターゲット) がインストールされているシステムで以下のステップを実行します。
   a) recovery agent を開始します。「IBM Spectrum Protect サーバーの選択」ダイアログおよび「スナップショットの選択」ダイアログを実行して、「**マウント**」をクリックします。
   b)「マウント宛先の選択」ダイアログで、「iSCSI ターゲットのマウント」を選択します。
   c) ターゲット名を作成します。 その名前が固有であること、および iSCSI イニシエーターを実行するシステムから識別できることを確認してください。 例えば、次のようにします。

```
iscsi-mount-tsm4ve
```

   d) ステップ 1 で記録した iSCSI イニシエーター名を入力し、「**OK**」をクリックします。
   e) マウントしたばかりのボリュームが、「マウントされたボリューム」フィールドに表示されることを確認します。
4. ステップ 1 で選択したイニシエーター・システムで iSCSI イニシエーター・プログラムを見つけて開始します。
   a) 次のコマンドを発行して、iSCSI サービスが実行されていることを確認します。
   Red Hat Enterprise Linux:

```
service iscsi status
```

   SUSE Linux Enterprise Server:

```
service open-iscsi status
```

   サービスが実行されていない場合は、次のコマンドを発行してサービスを開始します。
   Red Hat Enterprise Linux:

```
service iscsi start
```

   SUSE Linux Enterprise Server:

```
service open-iscsi start
```

   b) 次のコマンドを発行して、iSCSI ターゲットに接続します。

```
iscsiadm -m discovery -t sendtargets -p <IP/hostname of
recovery agent  system> --login
```

   c) 次のコマンドを発行して、新規のロー・デバイスが使用可能であることを確認します。

```
fdisk -l
```

5. ファイル・システムをマウントします。
   非 LVM ボリュームの場合は、次のコマンドを発行します。この例では、新規デバイスは /dev/sdb1 です。

```
mkdir /mountdir
mount /dev/sdb1 /mountdir
```

   LVM ボリュームの場合は、Linux ゲスト上で次のタスクを実行します。

a. Linux システム上で vgimportclone スクリプトが使用できることを確認します。 このスクリプトは、基本 (デフォルト) の LVM パッケージには含まれていません。結果として、このスクリプトを提供するレベルに LVM パッケージを更新することが必要になる場合があります。

b. **vgimportclone** コマンドを発行し、新規の基本ボリューム・グループ名 (VolGroupSnap01) を含めます。例えば、次のようにします。

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```

c. **lvchange** コマンドを発行し、論理ボリュームにアクティブのマークを付けます。 例えば、次のようにします。

```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```

d. 以下のコマンドを発行し、ボリュームをマウントします。

```
mkdir /mountdir
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```

6. ファイル・リストア操作が完了した後、以下のコマンドを発行します。

- 非 LVM ボリュームの場合、次のコマンドを発行します。

  a. ファイル・システムのアンマウント:

  ```
  umount /dev/sdb1 /mountdir
  ```

  b. ボリュームを削除します。ボリュームがボリューム・グループに属している場合、最初に次のコマンドを発行して、ボリュームをボリューム・グループから除去します。

  ```
  vgreduce <your_volume_group> /dev/sdb1
  ```

  その後、次のコマンドを発行して、ボリュームを削除します。

  ```
  pvremove /dev/sdb1
  ```

  c. 単一ターゲットからのログアウト:

  ```
  iscsiadm --mode node --targetname <target_name> --logout
  ```

  d. すべてのターゲットからのログアウト:

  ```
  iscsiadm --mode node --logout
  ```

- LVM ボリュームの場合は、Linux ゲスト上で次のタスクを実行します。

  a. ファイル・システムのアンマウント:

  ```
  unmount /mountdir
  ```

  b. 論理ボリュームの削除:

  ```
  lvm lvremove LogVol00
  ```

  c. ボリューム・グループの削除:

  ```
  lvm vgremove VolGroupSnap01
  ```

  d. 単一ターゲットからのログアウト:

  ```
  iscsiadm --mode node --targetname <target_name> --logout
  ```

  e. すべてのターゲットからのログアウト:

  ```
  iscsiadm --mode node --logout
  ```

Windows Windows システム上の iSCSI 装置の手動構成

この手順では、iSCSI マウント操作時に使用される Windows システムの構成方法について説明します。 スナップショットは、IBM Spectrum Protect サーバー・ストレージからマウントされます。

始める前に

このタスクを実行する前に、以下の iSCSI 要件を確認してください。

- iSCSI マウント中に、iSCSI ターゲットが recovery agent システム上に作成されます。 任意のシステムから iSCSI ターゲットに接続し、バックアップ・データを含めるボリュームを作成することができます。 また、その後でこのボリュームを他のシステムからマウントすることもできます。
- iSCSI ターゲットに接続する必要があるシステムでは、iSCSI イニシエーターが必要です。
- データをリストアするシステム上に、iSCSI イニシエーターがインストールされていることを確認してください。
- recovery agent システムに、Microsoft iSCSI イニシエーターは必要ありません。

このタスクを実行する前に、以下のディスクおよびボリュームの要件を確認してください。

- 1 つのボリュームが複数のディスクにわたる場合、必要なすべてのディスクをマウントする必要があります。 ミラーリングされたボリュームが使用される場合は、ミラーリングされたディスクの 1 つのみをマウントしてください。 1 つのディスクをマウントすると、時間のかかる同期操作がなくなります。
- 複数の動的ディスクがバックアップ・システムで使用される場合、これらのディスクは同じグループに割り当てられます。 その結果、1 つのディスクのみをマウントする場合、Windows Disk Manager は一部のディスクが欠落していると見なして、エラー・メッセージを発行する可能性があります。 このメッセージは無視してください。 データの一部が他のディスクにある場合を除いて、バックアップされたディスク上のデータは引き続きアクセス可能です。 この問題は、すべての動的ディスクをマウントすることによって解決できます。

このタスクについて

iSCSI マウント操作時に使用される Windows システムを構成するには、以下のタスクを実行します。

手順

1. recovery agent システムで、LAN ファイアウォールと Windows クライアント・ファイアウォール内でポート 3260 を開きます。

   データをリストアするシステム上の iSCSI イニシエーター名を記録します。

   iSCSI イニシエーター名が、「コントロール パネル」の iSCSI イニシエーター構成ウィンドウに表示されます。例えば、次のようにします。

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. recovery agent (または iSCSI ターゲット) がインストールされているシステムで以下の作業を実行します。

   a) recovery agent GUI を開始します。 「**IBM Spectrum Protect サーバーの選択**」ダイアログおよび「**スナップショットの選択**」ダイアログを実行して、「**マウント**」をクリックします。

   b)「**マウント宛先の選択**」ダイアログで、「**iSCSI ターゲットのマウント**」を選択します。

   c) ターゲット名を作成します。 その名前が固有であること、および iSCSI イニシエーターを実行するシステムから識別できることを確認してください。 例えば、次のようにします。

   ```
   iscsi-mount-tsm4ve
   ```

   d) ステップ 1 で記録した iSCSI イニシエーター名を入力し、「**OK**」をクリックします。

   e) マウントしたばかりのボリュームが、「**マウントされたボリューム**」フィールドに表示されることを確認します。

f) iSCSI ネットワークで Recovery Agent を使用し、その Recovery Agent がデータ・ムーバーを使用しない場合は、C:¥ProgramData¥Tivoli¥TSM¥RecoveryAgent¥mount¥RecoveryAgent.conf ファイルにアクセスして、[IMOUNT] タグと **Target IP** パラメーターを指定します。

```
[IMOUNT config]
Target IP=<IP address of the network card on the system
that exposes the iSCSI targets.>
```

例えば、次のようにします。

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

Target IP パラメーターの追加または変更後、Recovery Agent GUI または Recovery Agent CLI を再始動します。

3. ステップ 1 で選択したイニシエーター・システムで iSCSI イニシエーター・プログラムを見つけて開始します。
   a) iSCSI ターゲットに接続します。
      1) ステップ 2 で「**ターゲット:**」ダイアログで使用された recovery agent (iSCSI ターゲット) の TCP/IP アドレスを、「ターゲット」タブに入力します。 「**クイック接続**」をクリックします。
      2)「**クイック接続**」ダイアログに、ステップ 2c で指定されたターゲット名に一致するターゲットが表示されます。そのターゲットがまだ接続されていない場合は、このターゲットを選択し、「**接続**」をクリックします。
   b) イニシエーター・システムで、「**コントロール パネル**」 > 「**管理ツール**」 > 「**コンピューターの管理**」 > 「**記憶域**」 > 「**ディスクの管理**」に進みます。
      1) マウントされた iSCSI ターゲットが **Type=Foreign** としてリストされている場合は、「**形式の異なるディスク**」を右クリックして、「**形式の異なるディスクのインポート**」を選択します。 「**形式の異なるディスク グループ**」が選択されます。 「**OK**」をクリックします。
      2) 次の画面に、外部ディスクのタイプ、状態、およびサイズが表示されます。 「**OK**」をクリックして、ディスクがインポートされるまで待ちます。
      3) ディスクのインポートが完了したら、**F5** (最新表示) を押します。 マウントされた iSCSI スナップショットが表示され、割り当てられたドライブ名が記載されています。 ドライブ名が自動的に割り当てられない場合は、必要な区画を右クリックし、「**ドライブ文字またはパスの変更**」を選択します。「**追加**」をクリックし、ドライブ名を選択します。
4. Windows Explorer (または、その他のユーティリティー) を開き、ファイル・リストア操作に使用するマウント済みスナップショットを参照します。
5. ファイルがリストアされたら、以下のタスクを実行します。
   a)「**iSCSI イニシエーター・プロパティー**」ダイアログを使用して、各 iSCSI ターゲットを切断します。
   b) recovery agent GUI でボリュームを選択して「**マウント解除**」をクリックし、ステップ 2 でマウントしたボリュームをマウント解除します。

Linux Linux システム上のマウント・プロキシー・ノードの手動構成

マウント・プロキシー・ノードをリモート Linux システムに追加するには、このタスクを実行します。

始める前に

標準的な Data Protection for VMware vSphere GUI 環境では、各マウント・プロキシー・ノードごとに個別の dsm.sys ファイル・スタンザが使用されます。 この手順のすべてのステップは、バックアップ・サーバーにインストールされたデータ・ムーバーを使用して実行します。

このタスクについて
このタスクでは、データ・ムーバー・オプションを更新し、IBM Spectrum Protect サーバーへの接続を確認することで、マウント・プロキシー・ノードをセットアップします。

手順

1. dsm.sys ファイルのマウント・プロキシー・ノードに関するスタンザで、以下のオプションを指定します。

   NODENAME
   以前に定義されたマウント・プロキシー・ノードの名前を指定します。 IBM Spectrum Protect スケジュールは、このノードに関連付けられます。

   PASSWORDACCESS
   パスワードが (ユーザー・プロンプトではなく) 自動的に生成されるようにするには、GENERATE を指定します。

   MANAGEDSERVICES
   Web クライアントとスケジューラーの両方 (schedule webclient) を管理するようにクライアント・アクセプターに指示するには、このオプションを指定します。

   TCPSERVERADDRESS
   IBM Spectrum Protect サーバーの TCP/IP アドレスを指定します。

   TCPPORT
   IBM Spectrum Protect サーバーの TCP/IP ポート・アドレスを指定します。

   COMMMETHOD
   IBM Spectrum Protect サーバーで使用される通信方式を指定します。 マウント・プロキシー・ノードの場合、通信方式として TCP/IP を指定する必要があります。 別の方式を指定した場合、操作は失敗します。

   HTTPPORT
   このオプションは、TCP/IP ポート・アドレスを指定し、複数のクライアント・アクセプター・サービス (CAD) が使用されている場合にのみ指定する必要があります。 例えば、2 つのマウント・プロキシー・ノード (および 2 つの CAD サービス) がある場合、各マウント・プロキシー・ノードのオプション・ファイルで異なる HTTPPORT 値を指定する必要があります。

   制約事項 : dsm.sys ファイルの LAN フリー・オプションを有効 (ENABLELANFREE YES) にしないでください。このオプションは、マウント・プロキシー・ノードの場合はサポートされません。

   以下は、これらの設定が指定された dsm.sys ファイルの例を示しています。

```
Servername     tsm_server1
        NODename datacenter1_MP_LNX
        PASSWORDAccess generate
        MANAGEDServices schedule webclient
        TCPServeraddress tsmserver.myco.com
        TCPPort 1500
        COMMMethod tcpip
        HTTPPORT    1583
```

2. 次のコマンドを発行し、マウント・プロキシー・ノード用の VMware vCenter ユーザーおよびパスワードを設定します。
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
3. -asnodename および -optfile のコマンド・ライン・パラメーターを指定して、データ・ムーバーのコマンド・ライン・セッションを開始します。
   `dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
   初回サインオンの後に、パスワードを求めるプロンプトが出されないことを確認してください。

   重要 : IBM Spectrum Protect スケジューラーの失敗を防止するために、asnodename オプションが dsm.sys ファイル・スタンザ (Linux) で設定されていないことを確認してください。 スケジューラーは、IBM Spectrum Protect サーバーに対して、asnodename (データ・センター・ノード) ではなく、nodename (マウント・プロキシー・ノード) に関連付けられたスケジュールを照

会します。 asnodename が dsm.sys で設定されていると、asnodename (nodename ではなく) に関連付けられたスケジュールが照会されます。 その結果、スケジューリング操作は失敗します。

4. 次のコマンドを発行して、IBM Spectrum Protect サーバーとの接続を確認します。
   ```
   dsmc query session
   ```
   このコマンドは、セッションに関する情報 (現行ノード名、セッションが確立された時刻、サーバー情報、およびサーバー接続情報を含む) を表示します。
5. 以下のタスクを実行して、クライアント・アクセプター・サービス (CAD) およびデータ・ムーバー・スケジューラー・サービスをセットアップします。
   - dsm.sys ファイルのマウント・プロキシー・ノードに関するスタンザで、以下のオプションを指定します。
     - managedservices オプションに次の 2 つのパラメーターを指定します。
       ```
       managedservices schedule webclient
       ```
       この設定は、クライアント・アクセプターが Web クライアントとスケジューラーの 両方を管理することを指示します。
     - スケジュールとエラー情報を、デフォルトのファイル以外のログ・ファイルに送信したい場合は、schedlogname オプションおよび errorlogname オプションを指定します。 各オプションには、ログ情報を保管する先の完全修飾パスおよびファイル名が含まれている必要があります。 例えば、次のようにします。
       ```
       schedlogname /vmsched/dsmsched_mp_lnx.log
       errorlogname /vmsched/dsmerror_mp_lnx.log
       ```
   - クライアント・アクセプター・サービスを開始します。

     インストール・プログラムは、クライアント・アクセプター・デーモン (dsmcad) の始動スクリプトを /etc/init.d に作成します。クライアント・アクセプター・デーモンは、スケジューラー・タスクまたは Web クライアントを管理する前に開始する必要があります。root として、次のコマンドを使用してデーモンを開始します。
     ```
     service dsmcad start
     ```
     システムの再始動後にクライアント・アクセプター・デーモンが自動的に開始されるようにするには、シェル・プロンプトで以下のようにサービスを追加します。
     ```
     # chkconfig --add dsmcad
     ```
6. クライアント・アクセプターとエージェントが正しくセットアップされていることを確認します。
   a. リモート・システムにログオンします。
   b. Web ブラウザーを使用して、次のアドレスとポートを使用し、HOST1 システムに接続します。
      ```
      http://HOST1.xyz.yourcompany.com:1581
      ```

Windows リモート Windows システム上のマウント・プロキシー・ノードの手動構成

マウント・プロキシー・ノードをリモート Windows システムに追加するには、このタスクを実行します。2 つ目の Windows マウント・プロキシー・ノードを環境に追加する場合は、このタスクが必要です。

始める前に
このタスクを進める前に、1 次 Windows マウント・プロキシー・ノードが構成されていることを確認してください。

このタスクについて
リモート Windows マウント・プロキシー・システムで以下のステップを実行します。

手順

1. リモート Windows マウント・プロキシー・システムに以下の製品をインストールします。
   - recovery agent
   - IBM Spectrum Protect データ・ムーバー

   IBM Spectrum Protect for Virtual Environments ダウンロード・イメージ上にある両方の製品にアクセスします。 ステップバイステップのインストール手順は、以下の IBM Knowledge Center で参照可能です。
   21 ページの『Windows システムへの Data Protection for VMware コンポーネントのインストール』
2. 作成された Windows マウント・プロキシー・ノードからサンプル・オプション・ファイルの内容を取り出し、それをリモート Windows マウント・プロキシー・システム上のオプション・ファイルに追加します。
   a) 1 次 Windows マウント・プロキシー・システム上で、Data Protection for VMware vSphere GUI の「**構成**」ウィンドウに進みます。
   b)「**タスク**」リストで「**TSM 構成の編集**」をクリックします。 構成ノートブックのロードには多少時間がかかる場合があります。
   c)「**マウント・プロキシー・ノード・ペア**」ページに移動し、「**マウント・プロキシー・ペアの追加**」をクリックします。
   d) 表の「1 次ノード」列で、保留中のロケーションがある Windows マウント・プロキシー・ノードを見つけ、「**新規設定**」をクリックします。
   e)「**1 次ノード**」と「**Linux パートナー・ノード**」の両方のノード・パスワードをメモします。このパネルを使用して、パスワードを変更または適切なパスワードを作成することができます。
   f)「**マウント・プロキシー設定**」ダイアログに表示されるサンプル `dsm.opt` ファイルの内容をコピーします。
   g) サンプル `dsm.opt` ファイルの内容をリモート Windows マウント・プロキシー・システム上のオプション・ファイルに貼り付け (追加) します。 役割がリモート・マウント・プロキシー・ノードであることを識別できるように、オプション・ファイルに名前を付けます。
   例: `dsm.REMOTE1_MP_WIN.opt`.

   制約事項 : オプション・ファイルの LAN フリー・オプションを有効 (ENABLELANFREE YES) にしないでください。このオプションは、マウント・プロキシー・ノードの場合はサポートされません。
3. マウント・プロキシー・ノード用の VMware vCenter ユーザーおよびパスワードを設定するには、以下のデータ・ムーバー・コマンドを発行します。

   ヒント : dsmc コマンド・ラインを開始するには、Windows の「**スタート**」メニューを開き、「**プログラム**」→「**IBM Spectrum Protect**」→「**バックアップ・クライアントのコマンド・ライン**」をクリックします。

```
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
-optfile=dsm.REMOTE1_MP_WIN.opt
```

4. 次のコマンドを発行して、IBM Spectrum Protect サーバーとの接続を確認します。

```
dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
```

   このコマンドは、セッションに関する情報 (現行ノード名、セッションが確立された時刻、サーバー情報、およびサーバー接続情報を含む) を表示します。
5. 以下のステップを実行して、クライアント・アクセプター・サービス (CAD) およびデータ・ムーバー・スケジューラー・サービスをセットアップします。

このステップでは、IBM Spectrum Protect クライアント GUI の構成ウィザードを使用して、CAD およびスケジューラー・サービスをセットアップします。 デフォルトでは、リモート・クライアント・エージェント・サービスもウィザードを使用してセットアップされます。 このタスクに IBM Spectrum Protect クライアント・サービス構成ユーティリティー (dsmcutil) を使用する場合は、リモート・クライアント・エージェント・サービスも必ずインストールしてください。
「**ユーティリティー**」>「**セットアップ・ウィザード**」に進み、ファイル・メニューから IBM Spectrum Protect クライアント構成ウィザードを開始します。

a) 「TSM Web クライアントの構成」を選択します。 プロンプトに従って情報を入力します。

1) 「いつサービスを開始しますか?」オプションで、「Windows のブート時に自動で行う」を選択します。

2) 「このウィザードの完了時にサービスを開始しますか?」オプションで「はい」を選択します。

操作が正常に完了したら、ウィザードのウェルカム・ページに戻り、ステップ b に進みます。

ヒント: 同じシステム上で複数のマウント・プロキシー・ノードを構成する場合、各クライアント・アクセプター・インスタンスごとに別のポート値を指定する必要があります。

b) 「TSM クライアント・スケジューラーの構成」を選択します。 プロンプトに従って情報を入力します。

1) スケジューラー名を入力する場合は、必ず「スケジューラーを管理するためのクライアント・アクセプター・デーモン (CAD) の使用」オプションを選択してください。

2) 「いつサービスを開始しますか?」オプションで、「Windows のブート時に自動で行う」を選択します。

3) 「このウィザードの完了時にサービスを開始しますか?」オプションで「はい」を選択します。

6. クライアント・アクセプターおよびエージェントが正しくセットアップされていることを確認します。 Web ブラウザーを使用して、次のアドレスとポートを使用し、HOST1 システムに接続します。

```
http://HOST1.xyz.yourcompany.com:1581
```

Linux Windows リモート Windows システムの 2 次サーバーでのファイル・リストア機能の手動構成

リモート Windows システムの 2 次サーバーでファイル・リストア機能を手動で構成できます。このタスクを実行するには、2 次ファイル・リストア・マウント・プロキシー・ノードのペアが 2 次 IBM Spectrum Protect サーバーを使用可能にするためにデプロイされていることを確認してください。このタスクは複数ドメインの環境に実装することも可能です。

始める前に

Windows および Linux の両方のマウント・プロキシー仮想マシンが使用可能で、実行中であることが必要です。各 2 次サーバーには、ファイル・リストア操作用の 2 次マウント・プロキシー・ノード・ペアが必須です。マウント・プロキシー VM では、それぞれその **Microsoft iSCSI イニシエーター・サービス** も開始されていなければなりません。詳しくは、Windows Microsoft iSCSI Initiator Service の開始および Linux マウント・プロキシー・ノード・ペアの構成の失敗 (ANS3144W) - Linux を参照してください。

Windows マウント・プロキシー VM は以下の前提条件を満たしている必要があります。

- ハードウェアとソフトウェアの要件: Data Protection for VMware に記載されている最小ハードウェア要件に対応。
- リストアする VM ゲストと同じドメインのメンバーである。

注: 複数ドメインの環境では、マウント・プロキシー・マシンは、仮想マシン・ユーザーがメンバーである同じドメインのメンバーでなければなりません。

手順

1. マウント・プロキシー・ノード・ペアを以下のように作成します。

a) ファイル・リストア機能のために 2 つの新規マウント・プロキシー・マシンを選択します。必要な場合は、IBM Spectrum Protect とともにインストールします。

- Windows インストール・プロセス中に > 「**拡張インストール・タイプ (Installation Type Advanced)**」 > 「**データ・ムーバー機能のみ (Data Mover feature only)**」を選択します。
- Linux インストール・プロセス中に「**Data Protection for VMware データ・ムーバー)**」を選択します。

b) Windows

Windows マウント・プロキシーを以下のように作成します。

1)「**データ・ムーバー**」タブで、「**新規データ・ムーバー**」を選択します。

2) データ・ムーバー名の末尾がストリング REMOTE_MP_WIN であることを確認します。

注 : Windows と Linux のデータ・ムーバー名が一致しない場合、または末尾のストリングが適切ではない場合は、マウント・プロキシー・ノード・ペアは作成されません。代わりに、データ・ムーバーとして処理されます。

3) Windows VM のデータ・ムーバー・ホスト名の IP アドレスを指定します。

4) vCenter のユーザー名とパスワードを指定します。

5)「**追加**」をクリックします。

注 : 不要なスケジュール・サービスも作成されます。そのスケジュール・サービスは削除したり無視したりすることができます。

c) Linux

Linux マウント・プロキシーを以下のように作成します。

1)「**データ・ムーバー**」タブで、「**新規データ・ムーバー**」を選択します。

2) データ・ムーバー名は Windows マウント・プロキシーに使用されたのと同じであるものの、末尾がストリング REMOTE_MP_LNX であることを確認します。

注 : Windows のデータ・ムーバー名が一致しない場合、またはストリングの末尾が適切ではない場合は、マウント・プロキシー・ノード・ペアは作成されません。代わりに、データ・ムーバーとして処理されます。

3) Linux VM のデータ・ムーバー・ホスト名の IP アドレスを指定します。

4) vCenter のユーザー名とパスワードを指定します。

5)「**追加**」をクリックします。

6) コマンド・ラインから次のコマンドを実行します。

```
iscsiadm -m discovery -t sendtargets -p partner mount proxy
```

ここで *partner mount proxy* は、Linux パートナー・マウント・プロキシーの IP アドレスです。

d)「**マウント・プロキシー**」タブの選択後、「**最新表示**」をクリックして、Windows と Linux の両方のマウント・プロキシーが表示されており、検証済みの状態になっていることを確認します。

2. 次のように、新規マウント・プロキシー・ノード・ペアでファイル・リストア操作を実行します。

a) 新規 Windows マウント・プロキシー・マシン上で、ファイル・リストア・オプション・ファイルを以下のように編集します。

```
C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\frConfig.props
```

ファイル・リストア・オプション・ファイルの編集については、47 ページの『ファイル・リストア・オプション』を参照してください。

b) frConfig.props ファイル内に以下の変更内容を適用します。

```
default_mp_address=LOCALHOST
default_mp_nodename=node_name_of_new_windows_mount_proxy
enable_filerestore=true
```

ここで *node_name_of_new_windows_mount_proxy* は、新規 Windows マウント・プロキシーに関連付けられているノード名を指定します。

c) IBM Spectrum Protect for Virtual Environments Web サーバーを再始動して、マウント・プロキシーでサービスを再開します。

d) コマンド・プロンプトで以下のコマンドを入力し、新規 Windows マウント・プロキシーに関連付けられたオプション・ファイルを使用して、ファイル・リストア操作のためのドメイン・ユーザーとパスワードを設定します。

```
dsmc set password -type=domain cldev1.local\frank secret -
optfile=dsm.node_name_of_new_windows_mount_proxy.opt
```

ここで *secret* はパスワードを指定し、*node_name_of_new_windows_mount_proxy* は新規 Windows マウント・プロキシーに関連付けられているノード名を指定します。

注 : 上記コマンドで `clidev1.local\frank` は、ドメイン `clidev1.local` のユーザーです。このユーザーは、Windows マウント・プロキシーが作成されているドメインのメンバーであることも必要です。詳しくは、Windows ファイル・リストアの前提条件を参照してください。

e) この 2 次サーバーのファイル・リストア・ユーザー・インターフェースを 開始するには、Windows マウント・プロキシーの以下の URL を入力します。

```
https://hostname:9081/FileRestoreUI/
```

ここで *hostname* は、ファイル・リストア・ユーザー・インターフェースをホストする Windows マウント・プロキシーのホスト名を指定します。

Linux システムでの複数のクライアント・アクセプター・サービスの手動構成

特定の環境下では、複数の dsmcad サービスを単一の Linux クライアント・ホスト上で使用することが効果的な場合があります。

このタスクについて

このタスクは、システムの始動時に複数の dsmcad インスタンスが自動的に実行および開始されるようにセットアップします。

手順

1. dsm.sys ファイル内で 2 つの固有なノード・スタンザを作成します (デフォルトでは、このファイルは `/opt/tivoli/tsm/client/ba/bin/` にあります):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
   COMMMethod         TCPip
   TCPPort            1500
   TCPServeraddress   localhost
   nodename           node1
   errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
   schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
   managedservices    webclient sched
   httpport           1581
   passwordaccess     generate

SErvername node2
   COMMMethod         TCPip
   TCPPort            1500
   TCPServeraddress   localhost
   nodename           node2
   errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
   schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
   managedservices    webclient sched
   httpport           1582
   passwordaccess     generate
```

ヒント: 特定の includes/exclude オプションを組み込むことが、これらのノードを区別するのに効果的な場合があります。 そうしない場合、同じデータが 2 つのノード名を使用してバックアップされる可能性があります。

2. 2 つの dsm.opt ファイル (各ノードについて 1 つ) を作成します (デフォルトでは、これらのファイルは /opt/tivoli/tsm/client/ba/bin にあります):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. 両方のノードの資格情報を使用してログインし、passwordaccess generate を有効にします。

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. デフォルトの rc.dsmcad init スクリプトのコピーを 2 つ作成します (デフォルトでは、このスクリプトは /opt/tivoli/tsm/client/ba/bin にあります):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. rc.dsmcad-node1 を編集します。
   a) Red Hat Enterprise Linux ディストリビューションの場合は、以下の行を変更します。

   ```
   daemon $DSMCAD_BIN
   ```

   この行を、次のように変更します。

   ```
   daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
   ```

   b) SUSE Linux Enterprise Server ディストリビューションの場合は、以下の行を変更します。

   ```
   startproc $DSMCAD_BIN
   ```

   この行を、次のように変更します。

   ```
   startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
   ```

6. rc.dsmcad-node2 を編集します。
   a) Red Hat Enterprise Linux ディストリビューションの場合は、以下の行を変更します。

   ```
   daemon $DSMCAD_BIN
   ```

   この行を、次のように変更します。

   ```
   daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
   ```

   b) SUSE Linux Enterprise Server ディストリビューションの場合は、以下の行を変更します。

   ```
   startproc $DSMCAD_BIN
   ```

   この行を、次のように変更します。

   ```
   startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
   ```

7. /etc/init.d/ に新規行を作成し、2 つの新規の rc.dsmcad init スクリプトを指します。 これらのリンクにより、Linux init サービスがシステムの始動時に dsmcad サービスを開始できるようになります。

```
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
# ls -la dsm*
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

8. 2 つの新規 rc スクリプトを **chkconfig** に登録します。

```
# chkconfig --add dsmcad-node1
# chkconfig --add dsmcad-node2
```

9. **service dsmcad start** コマンドを使用して構成をテストし、スクリプトが問題なくロードおよび開始されることを確認します。

```
# service dsmcad-node1 start
Starting dsmcad-node1:                                     [  OK  ]
# service dsmcad-node2 start
Starting dsmcad-node2:                                     [  OK  ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

この例では、ページ書式の都合で、このコマンド・テキストを 2 行に分けてあります。

10. 再始動し、2 つの dsmcad インスタンスが自動的に開始されたことを確認します。

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

この例では、ページ書式の都合で、このコマンド・テキストを 2 行に分けてあります。

VMCLI 構成ファイルの変更

VMCLI 構成ファイル (vmcliConfiguration.xml) には、Data Protection for VMware vSphere GUI の設定が含まれています。

Data Protection for VMware のインストール・プロセスでは、vCenter Server の IP アドレス、および Web ブラウザーで GUI にアクセスできるかどうかをユーザーが指定する必要があります。ただし、いったんインストールした後は、サーバーの IP アドレスと GUI アクセス方式をインストーラーで変更することができません。

これらの設定を更新する場合は、VMCLI 構成ファイル (vmcliConfiguration.xml) を手動で編集することができます。このファイルはインストール中に以下の場所に作成されます。
Windows システムの場合:
C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥tsmVmGUI
Linux システムの場合:
/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/

Web ブラウザーで GUI にアクセスできるかどうかを変更するには、**<enable_direct_start></enable_direct_start>** パラメーターに以下の値のいずれかを入力します。

- *yes* GUI は、Web ブラウザーで直接アクセスすることができます。例えば、次のようにします。

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* GUI は、Web ブラウザーで直接アクセスすることはできません。例えば、次のようにします。

```
<enable_direct_start>no</enable_direct_start>
```

vSphere 保護で GUI を使用するには、 **<mode></mode>** パラメーターに以下の値を指定します。

- *vcenter* GUI を vSphere 保護に使用します。 例えば、次のようにします。

```
<mode>vcenter</mode>
```

vCenter Server の IP アドレスを変更するには、**<mode>vcenter</mode>** が設定されていることを確認し、**<vcenter_url><vcenter_url>** パラメーターに IP アドレスを指定します。 例えば、次のようにします。

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

vCenter Server の IP アドレスの先頭には、`https://` 値を指定する必要があります。vCenter Server の IP アドレスの末尾には、`/sdk` 値が必要です。

vmcliConfiguration.xml ファイルの例

以下の `vmcliConfiguration.xml` ファイルは vSphere 保護用に構成され、GUI の Web ブラウザーによるアクセスが有効になっています。

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
    <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
    <interruptDelay>900000</interruptDelay>
    <mode>vcenter</mode>
    <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
    <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

付録 B 増分永久増分バックアップ戦略へのマイグレーション

この手順を使用して、既存のバックアップ・スケジュール、ポリシー、および データ・ムーバー・ノードを永久増分バックアップ戦略で使用するためにマイグレーションします。

始める前に

Data Protection for VMware バージョン 6.2 および 6.3 で実装されていた永久増分フルバックアップ 戦略を使用することができます。永久増分フルバックアップ 戦略を引き続き使用する場合、ポリシーまたはスケジュールの変更は必要ありません。以下の手順の説明に従って、必ず、ご使用のデータ・ムーバー・ノードのみをバージョン 6.4 (以降) にアップグレードしてください。 ただし、永久増分バックアップ戦略を使用する場合は、データ・ムーバー・ノードをバージョン 6.4 (以降) に更新することに加え、この永久増分の増分バックアップ 戦略に移動するそれらのデータ・ムーバー・ノードのスケジュールとポリシーも 更新する必要があります。

既存の Data Protection for VMware スケジュールを増分永久増分バックアップ戦略にマイグレーションするには、以下の手順に記載されているタスクを完了する必要があります。

重要 :

- いくつかのタスクは離散的ですが、増分永久増分戦略の恩恵を完全に受けるためには、最終的にすべてのアプリケーションとコンポーネントをアップグレードする 必要があります。 本書では、それぞれのタスクの実行をガイドするためのすべての情報を提供します。
- マイグレーション・プロセス全体を完了するには、いくつかの方法が使用可能です。ただし、本書に記載されている方法は、標準的な Data Protection for VMware 環境に効果的な方法と考えられています。
- この手順でマイグレーションするスケジュールは、Data Protection for VMware vSphere GUI のバックアップ・ウィザードを使用して作成されたスケジュールです。マイグレーションするスケジュールを 手動で作成した場合は、この手順で識別されるスケジュールの更新も手動で行う必要があります。

このタスクについて

手順

1. 単一の vCenter を保護しているすべての vStorage バックアップ・サーバーをアップグレードします。すべてのデータ・ムーバー・ノードでこのアップグレードが同時に完了するようにしてください。
   - このアップグレードでは、vStorage バックアップ・サーバーに IBM Spectrum Protect データ・ムーバーのバージョン 6.4 以降をインストールする必要があります。
   - 離散的タスクのため、ステップ 1 の後にすぐにステップ 2 またはステップ 3 を完了する必要はありません。データ・ムーバー・ノードをアップグレードした後に、既存の環境で VM のバックアップを続行することができます。ステップ 2 とステップ 3 は、都合の良い時に完了することができます。

   ヒント : ご使用環境で複数の vStorage バックアップ・サーバーを使用している場合は、1 つのサーバーのみをアップグレードすることを検討してください。そして、サーバーが正常に動作することを確認してから、残りの vStorage バックアップ・サーバーをアップグレードしてください。
2. 永久増分の増分バックアップを実装するために、バックアップ・ポリシーおよびバックアップ・スケジュールを更新します。

   管理コマンド・ライン・クライアント (dsmadmc) でコマンドを発行して、IBM Spectrum Protect サーバーで以下のバックアップ・ポリシー・タスクを完了します。

   a. ユーザーの永久増分の増分バックアップに適したドメインおよびポリシー・セットの管理クラスを作成します。この例は、ドメイン `domain1` およびポリシー・セット `prodbackups` の管理クラス

mgmt_ifincr28 を作成します。この管理クラス名は、28 個のバックアップ・バージョンを保存する永久増分の増分バックアップ戦略を記述するために使用されます。

```
define mgmtclass domain1 prodbackups mgmt_ifincr28
description="Retain 28 backup versions"
```

b. 永久増分の増分バックアップのバックアップ・コピー・グループを作成します。以下の例は、ドメイン domain1、ポリシー・セット prodbackups、および管理クラス mgmt_ifincr28 の標準的なバックアップ・コピー・グループを作成します。

```
define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
```

standard type=backup 項目はデフォルト値であり、指定する必要はありません。それらは、コピー・グループ名が STANDARD であり、コピー・グループのタイプが backup である (archive ではない) ことを示すためにこの例に含まれています。

c. 適切なバージョン、保存、および有効期限の設定でバックアップ・コピー・グループを更新します。

要確認 : Data Protection for VMware バージョン 6.2 および 6.3 では、バックアップのバージョン、保存、および有効期限は、バックアップ・チェーンの細分度レベルに基づいています。 この方式は、永久増分フルバックアップと 永久増分の増分バックアップが (6.2 および 6.3 の永久増分フルバックアップ戦略の一部として) 取得されている場合でも、バージョンの有効期限ではフルバックアップのみがカウントされることを意味します。Data Protection for VMware バージョン 6.4 (以降) では、バックアップのバージョン、保存、有効期限は、単一バックアップの細分度レベルに基づいています。この方式は、バージョンの有効期限で永久増分フルバックアップと 永久増分の増分バックアップの両方がカウントされることを意味します。

verexists パラメーターは、サーバーに保存する VM バックアップ・バージョンの最大数を指定します。永久増分の増分バックアップ操作によりこの数を超えた場合、サーバーは、サーバー・ストレージに存在する最も古いバックアップ・バージョンを有効期限切れにします。この例では、verexists=28 が指定されています。この値は、最大 28 個の VM バックアップ・バージョンがサーバーに保存されることを意味します。

retextra パラメーターは、VM バックアップ・バージョンが非アクティブになった後にこのバージョンを保存する最大日数を指定します。この例では、retextra=nolimit を指定しています。 この値は、最大数の非アクティブの VM バックアップ・バージョンが無期限に保存されることを意味します。ただし、verexists が指定された場合、nolimit の値は verexists の値に置き換えられます。その結果、この例では、最大 28 個の非アクティブ VM バックアップ・バージョンがサーバーに保存されます。

このステップに記載されている設定に基づいて、バックアップ・コピー・グループは以下のように更新されます。

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

この例では、既存の Data Protection for VMware バージョン 6.3 環境は、以下のホストとスケジュールで構成されています。

- 2 つの ESX ホスト (esxhost1、esxhost2) を含む ESX クラスター (esxcluster)。
- bup_esxcluster_full スケジュールは、データ・ムーバー・ノード dm1 を使用して各 ESX ホストの週次の永久増分フルバックアップを 実行する。
- bup_esxcluster_incr スケジュールは、データ・ムーバー・ノード dm2 を使用して各 ESX ホストの日次の永久増分の増分バックアップを実行する。

Data Protection for VMware vSphere GUI で、以下のバックアップ・スケジュール・タスクを完了します。

a. vSphere Client の「ソリューションとアプリケーション」ウィンドウのアイコンをクリックして 、Data Protection for VMware vSphere GUI を開始します。

b.「**始めに**」ウィンドウで、「**バックアップ**」タブをクリックして、「**バックアップ・スケジュールの管理**」ウィンドウを開きます。

c. 更新するバックアップ・スケジュール (永久増分フルバックアップまたは 増分バックアップに使用される) を見つけます。この手順では、永久増分フル bup_esxcluster_full スケジュールが使用されます。

d. スケジュールを右クリックし、「**プロパティー**」を選択します。

e.「**スケジュール**」ページに移動し、「**バックアップ方法**」ドロップダウン・リストから「**増分**」を選択します。

f.「**OK**」をクリックして更新を保存します。

g. 永久増分の増分バックアップに使用されるバックアップ・スケジュールを見つけます。スケジュールを右クリックし、「**削除**」を選択します。永久増分フル bup_esxcluster_full スケジュールは永久増分の増分に更新されたため、この永久増分の増分スケジュールはもう必要ありません。

3. これで永久増分の増分バックアップ・スケジュールを取得したので、データ・ムーバー・ノードを統合してそれらの数を削減することができます。

この例では、2 つのデータ・ムーバー・ノードを 1 つのデータ・ムーバー・ノードに統合します。

a) vStorage バックアップ・サーバーで、コマンド・プロンプトを開き、dm1 のオプション・ファイルがあるディレクトリーに移動します。

b) テキスト・エディター (メモ帳など) を使用して、以下のオプションでこのファイルを更新します。

1) vmmaxparallel を指定して、dm1 によって一度にバックアップされる VM の数を制御します。

```
vmmaxparallel=2
```

デフォルト値および最小値は 1 です。最大値は 50 です。

ヒント: 除去するデータ・ムーバー・ノード 1 つにつき、vmmaxparallel 値を 1 増加します。

あるいは、vmlimitperhost を指定して、dm1 によって同じ ESX ホストから一度にバックアップされる VM の数を制御することができます。

```
vmlimitperhost=1
```

このオプションは、ホストが過負荷になるのを防止する場合に有用です。デフォルト値は 0 (制限なし) です。最小値は 1 です。最大値は 50 です。

c) IBM Spectrum Protect サーバーにログオンします。管理コマンド・ライン・クライアント (dsmadmc) を使用して、サーバーに接続できる同時 VM バックアップ・セッションの最大数を指定します。例えば、次のようにします。

```
maxsessions=4
```

デフォルト値は 25 です。最小値は 2 です。

4. 更新されたデータ・ムーバー・ノードが正しく機能していることを確認します。

a) vSphere Client の「ソリューションとアプリケーション (Solutions and Applications)」ウィンドウでアイコンをクリックして、Data Protection for VMware vSphere GUI を開始します。

b)「**始めに**」ウィンドウで、「**構成**」タブをクリックして、「**構成状況**」ページを表示します。

c)「**構成状況**」ページで、ステップ 1 で保護された vCenter を選択します。データ・ムーバー・ノードをクリックし、「**状況の詳細**」ペインでその状況情報を表示します。

ノードに警告またはエラーが表示されている場合は、そのノードをクリックし、「**状況詳細 (Status Details)**」ペインの情報を使用して問題を解決します。 次に、ノードを選択してから「**選択したノードの検証 (Validate Selected Node)**」をクリックして、問題が解決したかどうか確認します。「最新表示」をクリックして、すべてのノードの再テストを行います。

タスクの結果

各タスクが正常に完了したら、その環境を永久増分の増分バックアップ戦略に使用することができます。

制限: 増分永久フルバックアップ・タイプから増分永久増分バックアップ・タイプにスケジュールをマイグレーションした後は、以下の制限に注意してください。

- VM (ファイル・スペース) ごとに、マイグレーションされたスケジュールを 再び永久増分フルバックアップ・タイプに変更することはサポートされない。
- マイグレーションされたファイル・スペースで、IBM Spectrum Protect データ・ムーバーの前のバージョンを使用することはサポートされない。
- ファイル・スペースに 1 つ (以上) の永久増分の増分バックアップが含まれている場合、永久増分フルバックアップはサポートされない。

verexists パラメーターによるバージョン管理の例

このスケジュールのマイグレーション例では、Data Protection for VMware バージョン 6.3 は、以下の 2 つのバックアップ・スケジュールを使用します。

- `-mode=full`: 週次の永久増分フルバックアップが (日曜日に) スケジュールされており、サーバーに保存する VM バックアップ・バージョンの最大数は 4 個 (`verexists=4`) である。
- `-mode=incr`: 平日の永久増分の増分バックアップが (月曜日から土曜日まで) スケジュールされている。

4 週間の期間に取られるバックアップの数は 28 個です。

- 4 個の永久増分フルバックアップ (週次のフルバックアップ 1 個 × 4 週間)
- 24 個の永久増分の増分バックアップ (平日の増分バックアップ 6 個 × 4 週間)

Data Protection for VMware バージョン 6.3 ではフルバックアップのみがカウントされるため、`verexists=4` の値が、28 個すべてのバックアップを保存します。

Data Protection for VMware バージョン 6.4 (以降) での同一レベルの保護と永久増分の増分バックアップ戦略を提供するには、以下のスケジュールを作成します。
`-mode=iffull`: 日次の永久増分フルバックアップがスケジュールされており 、`verexists` パラメーターは 28 に設定されます。
4 週間の期間に取られるバックアップの数は 28 個です。

- 1 個の永久増分フルバックアップ (初期バックアップ × 1 日)
- 27 個の永久増分の増分バックアップ (日次の永久増分バックアップ × 27 日)

Data Protection for VMware バージョン 6.4 (以降) では永久増分フルバックアップと 永久増分の増分バックアップの両方がカウントされるため、値 `verexists=28` では、28 個すべてのバックアップを保存します。

付録 C IBM Spectrum Protect 製品ファミリーのアクセシビリティー機能

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーが情報技術コンテンツを快適に使用できるように支援します。

概要

IBM Spectrum Protect ファミリーの製品は、以下の主要なアクセシビリティー機能を備えています。

- キーボードのみによる操作
- スクリーン・リーダーを使用する操作

IBM Spectrum Protect ファミリーの製品では、US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) および Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) に確実に準拠するために、最新の W3C 標準である WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) を使用します。 アクセシビリティー機能を利用するには、最新リリースのスクリーン・リーダーと、この製品によってサポートされる最新の Web ブラウザーを使用してください。

IBM Knowledge Center の製品資料は、アクセシビリティーに対応しています。 IBM Knowledge Center のアクセシビリティー機能については、Accessibility section of the IBM Knowledge Center help (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility)に記載されています。

キーボード・ナビゲーション

この製品は、標準のナビゲーション・キーを使用します。

インターフェース情報

ユーザー・インターフェースには、毎秒 2 回から 55 回フラッシュするコンテンツは含まれません。

Web ユーザー・インターフェースは、カスケーディング・スタイル・シートを使用することで、コンテンツを適切にレンダリングし、使いやすさを実現しています。 このアプリケーションは、視覚に障害のあるユーザーがシステム表示設定を使用するための、同等の方式 (ハイコントラスト・モードなど) を備えています。 デバイスまたは Web ブラウザーの設定を使用して、フォント・サイズを制御することができます。

Web ユーザー・インターフェースには、アプリケーション内の機能領域に素早く移動できる WAI-ARIA ナビゲーション・ランドマークが含まれます。

ベンダー・ソフトウェア

IBM Spectrum Protect 製品ファミリーには、IBM 使用許諾契約書の対象とならない特定のベンダー・ソフトウェアが含まれています。 これらの製品のアクセシビリティー機能について、IBM は一切の保証責任を負いません。 ベンダーの製品に関するアクセシビリティー情報については、該当のベンダーにお問い合わせください。

関連アクセシビリティー情報

標準の IBM ヘルプ・デスクおよびサポートの各 Web サイトに加え、IBM では、聴覚障害を持つユーザーまたは聴覚機能が低下しているユーザーが販売サービスやサポート・サービスにアクセスするのに使用できる TTY 電話サービスを用意しています。

TTY サービス
800-IBM-3383 (800-426-3383)
(北アメリカ内)

IBM のアクセシビリティーへの取り組みの詳細については、IBM Accessibility (www.ibm.com/able) を参照してください。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。この資料は、IBM から他の言語でも提供されている可能性があります。 ただし、これを入手するには、本製品または当該言語版製品を所有している必要がある場合があります。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。 日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。 これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。 ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 *103-8510*
東京都中央区日本橋箱崎町 *19* 番 *21* 号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。 国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、 改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、 自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。 実際の結果は、異なる可能性があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。 より具体性を与えるために、それらの例には、個人、企業、ブランド、 あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、 名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。 お客様は、 サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション ・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、 IBM に対価を支払うことなくこれを複製し、 改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。 従って IBM は、 これらのサンプル・プログラムについて信頼性、 利便性もしくは機能性があることをほのめかしたり、保証することはできません。 これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物には、次のように、著作権表示を入れていただく必要があります。「© (お客様の会社名) (西暦年)」。 このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。© Copyright IBM Corp. _年を入れる_.

商標

IBM、 IBM ロゴ、 および ibm.com® は、 世界の多くの国で登録された International Business Machines Corp. の商標です。 他の製品名およびサービス名等は、 それぞれ IBM または各社の商標である場合があります。 現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe は、Adobe Systems Incorporated の米国およびその他の国における登録商標です。

Linear Tape-Open、LTO、および Ultrium は、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

Intel および Itanium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、および Windows NT は、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

VMware、VMware vCenter Server、および VMware vSphere は VMware, Inc. または子会社の米国およびその他の国における登録商標または商標です。

製品資料に関するご使用条件

これらの資料は、 以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用条件
IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用
これらの資料は、すべての著作権表示その他の所有権表示を していただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの

資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的利用

これらの資料は、すべての著作権表示その他の所有権表示を していただくことを条件に、お客様の企業内に限り、複製、配布、および表示することが できます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、 お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権利

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、 データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、 ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。 これらの資料は、特定物として現存するままの状態で提供され、 商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも 含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。 IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。 ご使用の「ソフトウェア・オファリング」が、 これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、 以下の具体的事項をご確認ください。

この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie などの各種テクノロジーの使用について詳しくは、「IBM オンラインでのプライバシー・ステートメントのハイライト」(http://www.ibm.com/privacy/jp/ja/)、「IBM オンラインでのプライバシー・ステートメント」(http://www.ibm.com/privacy/details/jp/ja) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』というタイトルのセクション、および「IBM Software Products and Software-as-a-Service Privacy Statement」(http://www.ibm.com/software/info/product-privacy) を参照してください。

用語集

この用語集には、IBM Spectrum Protect 製品ファミリーの用語および定義が記載されています。

IBM Spectrum Protect 用語集を参照してください。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

アクセシビリティー機能 119
アップグレード
  概要 28
  Linked Mode 31
  Linux
    サイレント 30
  V6.x から
    標準 28
  vCenter
    Linked Mode 31
  Windows 64 ビット
    サイレント 29
アンインストール
  Linux
    サイレント・モード 34
    標準的 31
  Windows 64 ビット
    サイレント・モード 33
    標準的 31
インストール
  インストール可能コンポーネント 1
  コンポーネント 20
  システム要件 11
  ソフトウェア要件 11
  ハードウェア要件 11
  パッケージのダウンロード 20
  パッケージの入手 20
  必要な通信ポート 15
  ユーザー権限 14
  ロードマップ 9
  Data Protection for VMware 1
  Linux
    インストール・ウィザードの使用 22
  Windows
    インストール・ウィザードの使用 21
インストール・ウィザード
  Linux
    インストール・ウィザードの使用 22
  Windows
    インストール・ウィザードの使用 21
インストール可能コンポーネント
  データ・ムーバー 7
  ファイル・リストア GUI 7
  Data Protection for VMware vSphere GUI 3
  Data Protection for VMware コマンド・ライン・インターフェース 6
  IBM Spectrum Protect vSphere Client プラグイン 6
インストール環境の変更 36, 37
インストール手順
  Linux
    クリーン 23
    サイレント 25
  Windows 64 ビット
インストール手順 (続き)
  Windows 64 ビット (続き)
    サイレント Suite インストーラー 24

[カ行]

鍵ストアのアクセス権限
  サード・パーティーの証明書 62
管理者特権
  Data Protection for VMware vSphere GUI 68
キーボード 119
クライアント・アクセプター (client acceptor)
  構成 110
計画
  概要 9
  権限 14
  システム要件 11
  必要な通信ポート 15
  ロードマップ 9
権限
  インストール 14
  権限 14
  Data Protection for VMware vSphere GUI
    操作 68
構成
  概要 39
  拡張タスク 83
  既存の構成 44
  クライアント・アクセプター (client acceptor) 110
  初期構成 39, 40
  タグ付けサポートの有効化 50
  データ・ムーバー・ノード
    vSphere 環境 85–87, 89
  テープ・ストレージ 98
  ファイル・リストア
    オプション 47
  ファイル・リストアを有効にする 45
  マウント・プロキシー・ノード
    Linux 104
    Windows 106, 108
  ロケール設定 78
  Data Protection for VMware のワークシート 27
  IBM Spectrum Protect ノード
    vSphere 環境 83
  iSCSI マウント 100, 103
  recovery agent GUI 71
  SSL 60
  TLS 通信 60
  VMCLI
    vSphere 環境 93
  VMCLI 構成ファイル 112
  vSphere 環境
    コマンド・ライン・チェックリスト 95
  Web ブラウザー通信 60
構成ウィザード 39, 40
構成ノートブック 44
コンポーネント

コンポーネント (続き)
インストール可能コンポーネント 20
データ・ムーバー 7
ファイル・リストア GUI 7
Data Protection for VMware vSphere GUI 3
Data Protection for VMware コマンド・ライン・インターフェース 6
IBM Spectrum Protect vSphere Client プラグイン 6
Recovery Agent 5

[サ行]

サード・パーティーの証明書
鍵ストアのアクセス権限 62
証明書署名要求の作成 64
証明書署名要求の送信 64
署名付き証明書の受信 64
TLS の構成 62
サーバーとのセキュア通信の使用可能化
TLS の構成 61, 75–77
サービス 81
サイレント・アップグレード
Linux 30
Windows 64 ビット 29
サイレント・アンインストール
Linux
サイレント・モード 34
Windows 64 ビット
サイレント・モード 33
サイレント・インストール
Linux 25
Windows 64 ビット
サイレント Suite インストーラー 24
資格情報
権限 14
システム要件 11
証明書署名要求の作成
サード・パーティーの証明書 64
証明書署名要求の送信
サード・パーティーの証明書 64
署名付き証明書の受信
サード・パーティーの証明書 64
処理オプション
使用 56, 58
資料 v
身体障害 119
スケジュール
作成 43
追加のバックアップ・サーバー 43
ソフトウェア要件 11

[タ行]

タグ付けサポート
有効にする 50
通信ポート
インストール 15
データ・ムーバー
ノード
vSphere 環境での構成 85–87, 89
Windows での構成 87, 89
テープ・ストレージ
構成 98
デフォルトのバックアップ・サーバー
構成 41
デフォルトのバックアップ・サーバーの構成 41
登録キー 70

[ハ行]

ハードウェア要件 11
バックアップ
管理 43
個別バックアップの実行 43
バックアップ・サーバー
構成 42
追加のバックアップ・サーバー 42
ファイル・リストア
オプション 47, 49
オプションの構成 47
前提条件 12
有効にする 45
ロギングの構成 48
Linux 環境 46
ファイル・リストア GUI 7
変更
概要 36
ポート
インストール 15

[マ行]

マイグレーション
スケジュール 115
マルチサーバー環境の構成 41

[ラ行]

リストア
オプション 47, 49
オプションの構成 47
前提条件 12
ファイル 12, 47–49
ロギングの構成 48
Recovery Agent 5
リストア操作
実行 44
リストア操作 44
ロギング
ファイル・リストア 48
ロケール
設定 78

D

Data Protection for VMware
インストール可能コンポーネント 1
計画 9
パッケージのダウンロード 20
Data Protection for VMware vSphere GUI
権限
操作 68
Data Protection for VMware コマンド・ライン・インターフェース 6
Data Protection for VMware バージョン 8.1.10 の新機能 vii

G

GUI
    Data Protection for VMware vSphere GUI 27

I

IBM Knowledge Center v
IBM Spectrum Protect vSphere Client プラグイン 6
IBM Spectrum Protect ノード
    構成
        vSphere 環境 83
iSCSI マウント
    構成 100, 103

K

Knowledge Center v

L

Linux
    アップグレード
        サイレント 30
    アンインストール
        サイレント・モード 34
        標準的 31
    インストール手順
        クリーン 23
        サイレント 25

R

Recovery Agent 5
recovery agent GUI
    オプション 71
    構成 71

S

SSL
    構成 60, 61, 75–77

T

TLS 通信
    構成 60
TLS の構成
    サード・パーティーの証明書 62
    サーバーとのセキュア通信の使用可能化 61, 75–77
    認証局 62

U

user
    権限 14

V

VMCLI
    vSphere 環境での構成 93
VMCLI 構成ファイル
VMCLI 構成ファイル (続き)
    変更 112
    vmcliConfiguration.xml 112
vSphere GUI 27

W

Windows 64 ビット
    アップグレード
        サイレント 29
    アンインストール
        サイレント・モード 33
        標準的 31
    インストール手順
        サイレント Suite インストーラー 24

プログラム番号:　5725-X00