

IBM Spectrum Protect for Virtual
Environments
バージョン 8.1.10

Data Protection for Microsoft Hyper-V イ
ンストールとユーザーズ・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、[277 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 Microsoft Hyper-V
Installation and User's 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

© Copyright International Business Machines Corporation 2011, 2020.

目次

本書について.....	vii
本書の対象読者.....	vii
資料.....	vii
バージョン 8.1.10 の新機能.....	ix
第 1 章 Microsoft Hyper-V 仮想マシンの保護.....	1
Hyper-V 仮想マシンのバックアップ.....	1
Volume Shadow Copy Service (VSS) を使用した VM バックアップ.....	1
Resilient Change Tracking (RCT) を使用した VM のバックアップ.....	2
Hyper-V 仮想マシンのリストア.....	4
Hyper-V 操作のユーザー・インターフェース.....	5
IBM Spectrum Protect ノードの使用法.....	6
仮想マシン・レベルでのポリシー管理.....	8
永久増分バックアップ戦略.....	8
Windows PowerShell を使用したスナップショット管理.....	8
Hyper-V バックアップ操作の制約事項.....	9
資料リソース.....	10
第 2 章 Data Protection for Microsoft Hyper-V のインストールおよびアップグレード.....	13
Data Protection for Microsoft Hyper-V のインストール計画.....	13
インストールされる機能.....	13
システム要件.....	13
必要な通信ポート.....	14
Data Protection for Microsoft Hyper-V のアップグレード.....	15
異なるバージョンとの互換性.....	15
IBM Spectrum Protect サーバー上のノードの名前変更.....	16
ノード名のカスタマイズ.....	18
RCT バックアップに関するアップグレードの考慮事項.....	20
VSS バックアップから RCT バックアップへのマイグレーション.....	20
インストール・ウィザードを使用したアップグレード.....	21
Data Protection for Microsoft Hyper-V コンポーネントのインストール.....	21
インストール・パッケージのダウンロードおよび解凍.....	22
ウィザードを使用したインストール.....	22
Data Protection for Microsoft Hyper-V のアンインストール.....	27
サイレント・モードでのインストール.....	28
サイレント・モードでのアンインストール.....	29
Windows Server Core システムへのインストール.....	30
Windows Server Core システムでのアンインストール.....	31
Linux マウント・プロキシのインストール.....	32
Linux マウント・プロキシ機能のアンインストール.....	36
ファイル・リストア機能の削除.....	36
第 3 章 Data Protection for Microsoft Hyper-V の構成.....	39
ウィザードを使用した Data Protection for Microsoft Hyper-V の構成.....	39
Data Protection for Microsoft Hyper-V のセキュリティ設定の構成.....	42
IBM Spectrum Protect サーバー V8.1.1 以前または V7.1.7 以前に接続するためのセキュリティ設定の構成.....	43
環境でファイル・リストア操作を使用可能にする.....	44

ファイル・リストア操作のための Linux マウント・プロキシの構成.....	45
ファイル・リストア操作のオプションの変更.....	48
ファイル・リストア操作のオプション.....	48
Data Protection for Microsoft Hyper-V ログ・アクティビティの 構成.....	49
Data Protection for Microsoft Hyper-V ログ・アクティビティ・オプション.....	50
IBM Spectrum Protect リカバリー・エージェント GUI の構成.....	51
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.....	54
iSCSI デバイスの手動構成.....	57
拡張構成.....	59
Data Protection for Microsoft Hyper-V 操作用のデフォルト以外のポート番号の構成.....	59
Windows Server 2012 クラスターのスケジュール済み VM バックアップの調整.....	59

第 4 章 Data Protection for Microsoft Hyper-V 管理コンソールを使用したデータの管理 63

管理コンソールの開始.....	63
管理コンソールのナビゲート.....	64
「ナビゲーション」 ペイン.....	64
「結果」 ペイン.....	65
「アクション」 ペイン.....	73
Data Protection for Microsoft Hyper-V の構成の検証.....	74
ホストまたはクラスターのマシンのバックアップ・スケジュールの管理.....	75
仮想マシンの危険ポリシーの設定.....	76
Hyper-V ホストまたはクラスターのスケジュール・ヒストリーの表示.....	77
仮想マシンのバックアップ状況とバックアップ・ヒストリーの表示.....	78
仮想マシンのアドホック・バックアップの開始.....	79
仮想マシンのリストア.....	80
Data Protection for Microsoft Hyper-V のベスト・プラクティス.....	82

第 5 章ファイル・リストア操作の概要..... 85

ファイル・リストア・タスク.....	85
ファイル・リストア的前提条件.....	86
ファイルをリストアするためのログイン.....	88
仮想マシン・バックアップからファイルのリストア.....	88

第 6 章ゲスト内アプリケーションの保護..... 91

Hyper-V 環境での Microsoft Exchange Server データの保護.....	91
ソフトウェアのインストールおよび構成.....	91
バックアップ操作の管理.....	100
データのリストア.....	103
IBM Spectrum Protect ファイル・スペース情報.....	107
Hyper-V 環境での Microsoft SQL Server データの保護.....	107
ソフトウェアのインストールおよび構成.....	108
バックアップ操作の管理.....	116
データのリストア.....	120
仮想マシンのフルバックアップを確認するためのサンプル・スクリプト.....	124
IBM Spectrum Protect ファイル・スペース情報.....	125
ゲスト仮想マシンのアプリケーション保護のトラブルシューティング.....	126
ゲスト仮想マシン上での VSS バックアップ操作およびリストア操作のトラブルシューティング.....	127

第 7 章インスタント・アクセス操作の実行..... 131

コマンド・ラインからの VM バックアップの整合性の検証.....	131
コマンド・ラインを使用したインスタント・アクセス・リソースの解放.....	134
Data Protection for Microsoft Hyper-V 管理コンソール からのインスタント・アクセス操作の実行..	136
Data Protection for Microsoft Hyper-V 管理コンソール からのインスタント・アクセス VM の除去...	137
Hyper-V ホストが再始動した後のインスタント・アクセス VM の制約事項.....	138

第 8 章 Windows PowerShell コマンドレットを使用した仮想マシンの保護.....	139
PowerShell コマンドレットを使用する準備.....	139
Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット.....	141
PowerShell コマンドレットを使用して実行できるタスク.....	145
第 9 章 コマンド解説.....	151
構文図の読み方.....	151
Backup VM.....	153
Expire.....	160
Query VM.....	161
Restore VM.....	165
仮想マシンのリストア操作のプレビュー.....	171
第 10 章 オプションの解説.....	175
Dateformat.....	175
Detail.....	177
Domain.vmfull.....	177
Exclude.vmdisk.....	180
Inactive.....	182
Include.vm.....	183
Include.vmdisk.....	184
INCLUDE.VMSNAPSHOTATTEMPTS.....	186
INCLUDE.VMTSMVSS.....	187
データ・ムーバーからアプリケーション保護バックアップをリストアする場合のシャドー・コ ピーの考慮事項.....	189
mode.....	190
Mbobjrefreshtresh.....	191
Mbpctrefreshtresh.....	192
Noprompt.....	193
Numberformat.....	193
Pick.....	195
Pitdate.....	195
Pittime.....	195
Skipsystemexclude.....	196
Timeformat.....	197
vmautostartvm.....	198
Vmbackdir.....	199
Vmctlmc.....	199
Vmmaxbackupsessions.....	200
Vmmaxparallel.....	202
Vmmaxpersnapshot.....	203
vmmaxrestoreparalleldisks.....	205
Vmmaxrestoreparallelvms.....	206
Vmmaxrestoresessions.....	210
vmmaxsnapshotretry.....	212
Vmmaxvirtualdisks.....	213
Vmmc.....	214
Vmprocessvmwithphysdisks.....	215
Vmskipmaxvirtualdisks.....	216
Vmskipphysdisks.....	217
Vmrestoretype.....	218
第 11 章 マウントおよびファイル・リストア.....	221

IBM Spectrum Protect リカバリー・エージェント の構成.....	221
スナップショットのマウントの概要.....	222
マウントのガイドライン.....	223
ファイル・リストアの概要.....	223
ファイル・リストアのガイドライン.....	224
1 つ以上のファイルをリストア	225
第 12 章 IBM Spectrum Protect リカバリー・エージェント コマンド.....	229
マウント.....	229
Set_connection.....	233
Help.....	233
Recovery Agent コマンド・ライン・インターフェースの戻りコード.....	234
第 13 章 パフォーマンスの最適化.....	237
バックアップ操作の最適化.....	237
複数の仮想マシンの並列バックアップ (最適化されたバックアップ).....	239
リストア操作の最適化.....	239
複数の仮想マシンの並列リストア (最適化されたリストア).....	241
付録 A トラブルシューティング.....	243
Data Protection for Microsoft Hyper-V 操作のトラブルシューティング	246
Data Protection for Microsoft Hyper-V のトレース・オプション.....	247
付録 B Data Protection for Microsoft Hyper-V メッセージ.....	249
付録 C アクセシビリティー	275
特記事項	277
用語集	281
索引.....	283

本書について

本書は、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V の概要、プランニング、およびユーザー指示について記載しています。

本書の対象読者

本書は、サポートされている環境のいずれかにおいて、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V を使用したバックアップ・ソリューションの実装を担当する管理者およびユーザーを対象にしています。

本書では、読者が次のアプリケーションについて理解していることを前提としています。

- Hyper-V 役割がインストールされた Microsoft Windows Server 2019
- Hyper-V 役割がインストールされた Microsoft Windows Server 2016
- Hyper-V 役割がインストールされた Microsoft Windows Server 2012 または 2012 R2
- IBM Spectrum Protect バックアップ/アーカイブ・クライアント
- IBM Spectrum® Protect サーバー

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: Data Protection for Microsoft Hyper-V バージョン 8.1.10 には、いくつかの更新内容が導入されています。

この製品資料内の新規情報および変更情報は、その箇所の左側に縦棒 (|) を付けて示してあります。

このリリースでは、以下のような更新内容が使用可能です。

保守の更新情報

このリリースでは、文書に小規模な変更が加えられています。

現行および以前の V8.1 リリースの新機能および更新内容のリストについては、[Data Protection for Microsoft Hyper-V の更新内容](#)を参照してください。

第 1 章 Microsoft Hyper-V 仮想マシンの保護

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V は、Microsoft Hyper-V 環境で仮想マシン (VM) のストレージ管理サービスを提供するライセンス製品です。

Data Protection for Microsoft Hyper-V は、IBM Spectrum Protect バックアップ/アーカイブ・クライアントと連携して、以下のオペレーティング・システムで Hyper-V 仮想マシンを保護します。

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Hyper-V 仮想マシンのバックアップ

Data Protection for Microsoft Hyper-V は、Hyper-V 仮想マシン (VM) の永久増分 - フルバックアップまたは永久増分 - 増分バックアップを作成します。VM の整合スナップショットが取られ、VM は IBM Spectrum Protect サーバーにバックアップされます。

ローカル・ディスク、Storage Area Network (SAN) 接続ディスク、またはクラスター共有ボリューム (CSV) 上にある Hyper-V VM をバックアップすることができます。例えば、Hyper-V クラスター環境の CSV に保管されているか、またはリモート・システム上にある Server Message Block (SMB) ファイル共有に保管されている VM をバックアップすることができます。リモート共有上の Hyper-V サーバーでサポートされる任意のゲスト・オペレーティング・システムは、IBM Spectrum Protect が直接サポートするかどうかに関係なく、バックアップが可能です。

以下のバックアップ・タイプが、VHDX ディスク・フォーマットを使用する仮想ディスクを備えた Microsoft Hyper-V VM でサポートされています。

永久増分 - フルバックアップ

IBM Spectrum Protect サーバーへのスナップショット・ディスク・データのバックアップを作成します。

永久増分 - 増分バックアップ

前回の永久増分 - フルバックアップまたは永久増分 - 増分バックアップ以降に変更されたブロックのスナップショットを作成します。

Windows Server 2012 または Windows Server 2012 R2 オペレーティング・システムで Hyper-V ホストを実行中の場合、Microsoft Volume Shadow Copy Service (VSS) を使用して、VM の整合スナップショットを作成します。各バックアップ間に VM で発生した変更は、スナップショット差分処理ファイルで追跡されます。

Hyper-V ホストを Windows Server 2016 以降のオペレーティング・システムで稼働している場合、Windows API によってスナップショットが作成され、Resilient Change Tracking (RCT) を使用して、各バックアップ操作間での VHDX ディスクの変更を追跡します。

Volume Shadow Copy Service (VSS) を使用した仮想マシン・バックアップ

Windows Server 2012 および 2012 R2 での Hyper-V バックアップの場合、Microsoft Volume Shadow Copy Service (VSS) を使用して、バックアップ操作中に仮想マシン (VM) の整合スナップショットを作成します。

初期の永久増分 - フルバックアップ操作中に、クライアントは、仮想マシン・ハード・ディスク (VHDX) のスナップショットを作成し、その内容を IBM Spectrum Protect サーバーに送信します。初期スナップショット後に発生した変更は、スナップショット差分処理ファイル (.avhdx) に保管されます。後続の永久増分 - 増分バックアップ操作では、前回のバックアップ以降に変更されたデータのみがバックアップされます。

永久増分 - フルバックアップを作成する前に永久増分 - 増分バックアップを実行する場合、クライアントが永久増分 - フルバックアップを実行します。

スナップショットと VSS バックアップとの連携

バックアップ操作後に発生する VM の変更を追跡するために、各 VM バックアップ中、新しいスナップショット差分処理ファイル (.avhdx) が作成されます。この差分スナップショットは、次の増分バックアップの書き込みを収集するために Hyper-V ホストに保存されます。

前のリリースの Data Protection for Microsoft Hyper-V では、スナップショットに 1 つの VM のみが含まれます。この動作により、取られなければならないスナップショットが多すぎたため、クラスター・バックアップ操作中にスケジュールの競合が生じる場合があります。Data Protection for Microsoft Hyper-V バージョン 8.1.2 で導入された vmmaxpersnapshot オプションを使用すると、複数の VM を 1 つのスナップショットにグループ化することによって、バックアップ操作で取られるスナップショットの数を減らすことができます。詳しくは、59 ページの『[Windows Server 2012 および Windows Server 2012 R2 クラスターのスケジュール済み VM バックアップの調整](#)』を参照してください。

Resilient Change Tracking (RCT) を使用した仮想マシンのバックアップ

Microsoft Windows Server 2016 以降のバージョンでの Hyper-V バックアップの場合、Resilient Change Tracking (RCT) 機能が仮想マシン (VM) のバックアップに使用されます。

RCT は、組み込まれた Change Block Tracking 機能を Hyper-V VM ディスクに提供する機能です。Data Protection for Microsoft Hyper-V は RCT を使用して、バックアップ操作間で発生する、VM ディスク (VHDX) の変更を追跡します。これらの変更は、データ・ブロック・レベルで追跡されます。前回のバックアップ操作以降に変更されたブロックのみが、次の永久増分 - 増分バックアップの候補になります。

また、Windows Server 2016 は、Microsoft Volume Shadow Copy Service (VSS) を使用することなく、バックアップ・スナップショット (チェックポイントとも呼ばれる) を直接作成する機能を備えています (ただし、VSS は、アプリケーション整合バックアップのために VM を静止させるために Windows ゲスト VM 内部で引き続き使用されます)。

複数の VM を単一のスナップショットにグループ化することができます。ただし、アプリケーションをホストするゲスト VM でアプリケーション保護が有効にされている場合、VM スナップショットは個別に取得されます。アプリケーション保護について詳しくは、91 ページの『[第 6 章 ゲスト内アプリケーションの保護](#)』を参照してください。

RCT を使用する VM バックアップ操作では、Hyper-V VM がバージョン 6.2 以降であることが必要です。

ご使用の VM が Windows Server 2012 R2 以前のオペレーティング・システムで作成され、後で Windows Server 2016 ホスト・サーバーに移動された (または、ホスト・サーバーが Windows Server 2016 にアップグレードされた) 場合、バックアップの前に、VM をオフラインにし、VM バージョンをアップグレードする必要があります。VM バージョンをアップグレードするには、Hyper-V Manager または **Update-VMVersion** cmdlet を使用します。

Data Protection for Microsoft Hyper-V V8.1.0 は VSS を使用して、Windows Server 2016 の Hyper-V 環境で VM をバックアップします。V8.1.2 から、Windows Server 2016 以降の環境におけるすべての Hyper-V VM バックアップ操作では、RCT を使用します。V8.1.0 からアップグレードする場合、以前の VSS バックアップには RCT 変更追跡情報がないため、初めて Data Protection for Microsoft Hyper-V V8.1.10 を使用して Windows Server 2016 で VM をバックアップするときに、永久差分 - フルバックアップが作成されます。

RCT を使用して VM をバックアップした後、その VM での VSS バックアップの実行に Data Protection for Microsoft Hyper-V V8.1.0 を使用できなくなります。

スナップショットと RCT バックアップとの連携

VM の永久増分 - フルバックアップ操作中に、VM ディスクのスナップショットが作成され、スナップショットの内容が IBM Spectrum Protect サーバーにバックアップされます。このスナップショットは、バックアップ操作の完了後、自動的に削除されます。

次の永久増分 - 増分バックアップ中に、新しいスナップショットが作成され、変更されたデータを判別するために以前のバックアップ操作からの RCT 変更追跡情報に照らして検証されます。変更されたブロックのみが IBM Spectrum Protect サーバーにバックアップされます。

バックアップ操作後に、スナップショットは Hyper-V によって VM とマージされ、スナップショット差分処理ファイル (.avhdx) が自動的に削除されます。このプロセスは、Windows Server 2012 および 2012

R2 のオペレーティング・システムでの VSS スナップショット処理 (増分の変更を保管するためにスナップショット差分処理ファイルが VM に保持される) とは異なります。

手動で作成するか、別のバックアップ製品を使用して作成するスナップショットは、RCT プロセスで作成されるバックアップ・チェーンに影響を与えません。Data Protection for Microsoft Hyper-V RCT バックアップ操作の前後に手動で、またはサード・パーティー製のバックアップ製品を使用してスナップショットを作成できます。Data Protection for Microsoft Hyper-V による次の増分バックアップ操作は、前のバックアップ操作からの RCT 変更追跡情報に基づいて行われます。

RCT バックアップに使用可能な機能

Windows Server 2012 および 2012 R2 で機能する大部分の Data Protection for Microsoft Hyper-V 機能は、Windows Server 2016 にも適用されます。

ただし、VSS バックアップと RCT バックアップでは、スナップショット操作が異なります。詳しくは、[2 ページの『スナップショットと RCT バックアップとの連携』](#)を参照してください。

クラスター共有ボリューム (CSV) を使用したホスト・フェイルオーバーのサポートは、V8.1.0 以前から変更されていませんが、Hyper-V クラスター・オペレーティング・システムのローリング・アップグレード中に VM バックアップを実行することはサポートされていません。

RCT バックアップの照会方法

query VM コマンドを使用すると、IBM Spectrum Protect サーバーにバックアップされた VM に関する情報を表示できます。バックアップ操作に関する詳細情報を表示するには、**query vm** コマンドで **-detail** パラメーターを使用してください。詳しくは、[161 ページの『Query VM』](#)を参照してください。

また、**backup vm -preview** コマンドを使用して、**backup vm** コマンドに使用できる VM ディスク・ロケーションを表示することもできます。詳しくは、[153 ページの『Backup VM』](#)を参照してください。

関連概念

[15 ページの『Data Protection for Microsoft Hyper-V のアップグレード』](#)

旧バージョンから Data Protection for Microsoft Hyper-V バージョン 8.1.10 にアップグレードする際に実行する必要があるタスクを確認します。

[9 ページの『Hyper-V バックアップ操作の制約事項』](#)

Hyper-V バックアップ操作を開始する前に、制約事項を確認してください。すべての Hyper-V バックアップ操作に適用される制約事項もあれば、Windows Server 2012 または 2012 R2 もしくは Windows Server 2016 の環境上の Hyper-V バックアップのみに適用される制約事項もあります。

[1 ページの『Volume Shadow Copy Service \(VSS\) を使用した仮想マシン・バックアップ』](#)

Windows Server 2012 および 2012 R2 での Hyper-V バックアップの場合、Microsoft Volume Shadow Copy Service (VSS) を使用して、バックアップ操作中に仮想マシン (VM) の整合スナップショットを作成します。

関連タスク

[20 ページの『VSS バックアップから RCT バックアップへのマイグレーション』](#)

Data Protection for Microsoft Hyper-V バージョン 8.1.2 以降で Resilient Change Tracking (RCT) バックアップ機能を利用するには、Microsoft Volume Shadow Copy Service (VSS) から RCT に仮想マシン (VM) バックアップ操作をマイグレーションします。

関連資料

[243 ページの『トラブルシューティング』](#)

Data Protection for Microsoft Hyper-V の問題に対する解決方法が記載されています。

Hyper-V 仮想マシンのリストア

Hyper-V 仮想マシン (VM) のリストアには、複数の方法を使用できます。すなわち、仮想マシン全体をリストアするか、仮想マシン全体を代替ロケーションにリストアするか、仮想マシンから個々のファイルをリストアすることができます。

フル VM リストア

Hyper-V VM 全体のリストア

各 Hyper-V VM のバックアップは、IBM Spectrum Protect サーバーから単一のエンティティとしてリストアされます。Hyper-V サーバーがホストするすべてのゲスト・オペレーティング・システムは、そのゲスト・オペレーティング・システムが IBM Spectrum Protect によってサポートされているかどうかとは関係なく、リストアが可能です。

Data Protection for Microsoft Hyper-V のリストア操作は、実動ディスク上の同じブロックが 1 回のみリストアされることを確実にします。仮想マシンに関連した IBM Spectrum Protect サーバー管理クラス・ポリシーにしたがって、旧バックアップ・バージョンは有効期限が切れます。

代替ロケーションへの Hyper-V VM 全体のリストア

Hyper-V VM は、代替 VM 名、または Hyper-V ホスト上の代替ロケーション、もしくはその両方にリストアすることができます。Data Protection for Microsoft Hyper-V 管理コンソールを使用して、別の Hyper-V ホストに Hyper-V 仮想マシンをリストアすることもできます。別のホストに VM をリストアする際にコマンド・ラインを使用する必要がある場合は、VM のリストア先となる Hyper-V ホストからリストア操作を実行する必要があります。

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

IBM Spectrum Protect ファイル・リストア・インターフェースを使用して、Web ベースのインターフェースで 1 つ以上のファイルをリストアします。ファイル所有者は、管理者からの最小限の支援で、VM バックアップからファイルの検索、位置指定、およびリストアを行うことができます。ヘルプ・デスク担当者も、ファイル・リストア・インターフェースを使用して、ファイル所有者に代わりファイルをリストアすることができます。

詳細については、85 ページの『[第 5 章 ファイル・リストア操作の概要](#)』を参照してください。

Recovery Agent を使用したファイルのリストア

このリストア方法は、ゲスト内マウント操作を実行する場合のみ使用します。ファイルは、Internet Small Computer Systems Interface (iSCSI) ターゲットまたは区画からアクセスされるマウント済みの仮想マシン・ディスクから手動でコピーされます。この方式では、IBM Spectrum Protect リカバリー・エージェントをインストールする必要があります。

詳細については、221 ページの『[第 11 章 マウントおよびファイル・リストア](#)』を参照してください。

ヒント : Data Protection for Microsoft Hyper-V の旧バージョンでは、Recovery Agent を使用した VM ディスクのマウントおよびファイルのリストアのための機能を提供していました。この機能は引き続き Recovery Agent によってサポートされますが、IBM Spectrum Protect リストア・インターフェースが推奨方式です。

インスタント・アクセス

バックアップ・データの検証のために一時 VM が作成されますが、その VM はリストアされません。

データ・ムーバー・コマンド・ライン・インターフェース、Data Protection for Microsoft Hyper-V 管理コンソール、または Windows PowerShell コマンドレットを使用して、インスタント・アクセス操作を実行することができます。

詳しくは、以下のトピックを参照してください。

- [131 ページの『コマンド・ラインからの VM バックアップの整合性の検証』](#)
- [136 ページの『Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス操作の実行』](#)
- [149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』](#)

Hyper-V 操作のユーザー・インターフェース

Data Protection for Microsoft Hyper-V Hyper-V 操作の実行には複数のユーザー・インターフェースを使用できます。データ・ムーバーは、Hyper-V ホスト・サーバーまたはクラスター内の各ホストにインストールされている必要があります。

Data Protection for Microsoft Hyper-V 操作には、以下のユーザー・インターフェースが使用できます。

Data Protection for Microsoft Hyper-V 管理コンソール

仮想マシン (VM) バックアップの管理、VM バックアップのモニター、アドホック・バックアップ操作とリストア操作の実行、および構成の更新などの日常のバックアップ管理タスクの実行に使用できるグラフィカル・ユーザー・インターフェース。

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

ファイル所有者やヘルプ・デスク担当者が、管理者からの最小限の支援で 1 つ以上のファイルを VM バックアップからリストアするために使用できる、Web ベースのインターフェース。管理者は、ファイル・リストア・インターフェースの URL を提供します。

データ・ムーバー

バックアップ/アーカイブ・クライアントとも呼ばれるコンポーネント。バックアップ操作とリストア操作中に IBM Spectrum Protect サーバーとの間で両方向にデータを移動します。

データ・ムーバーには、バックアップ操作、照会操作、リストア操作などの操作に使用できるコマンド・ライン・インターフェース (dsmc コマンド) が組み込まれています。

Data Protection for Microsoft Hyper-V コマンドレット

PowerShell スクリプトで Data Protection for Microsoft Hyper-V 操作を自動化するのに役立つ Windows PowerShell コマンドレット。

IBM Spectrum Protect リカバリー・エージェント

仮想マウント機能とファイル・リストア機能を提供するエージェント。

次の図は、Windows Server 2016 以降および Windows Server 2012 の環境における Data Protection for Microsoft Hyper-V の概要を示しています。

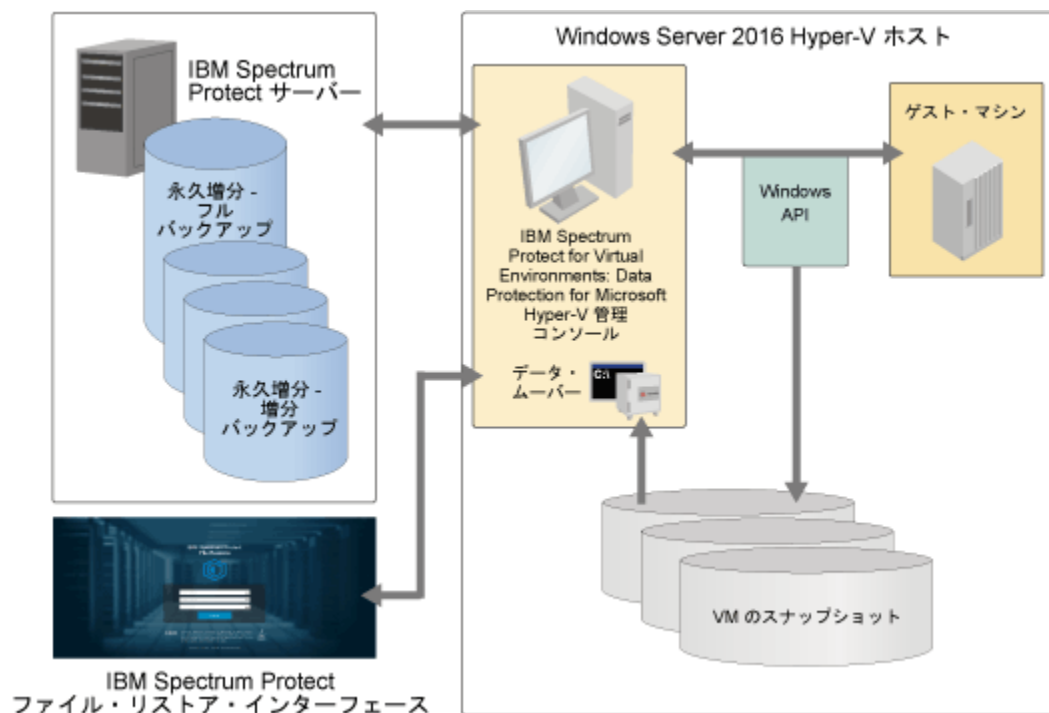


図 1. Windows Server 2016 環境における Data Protection for Microsoft Hyper-V の概要

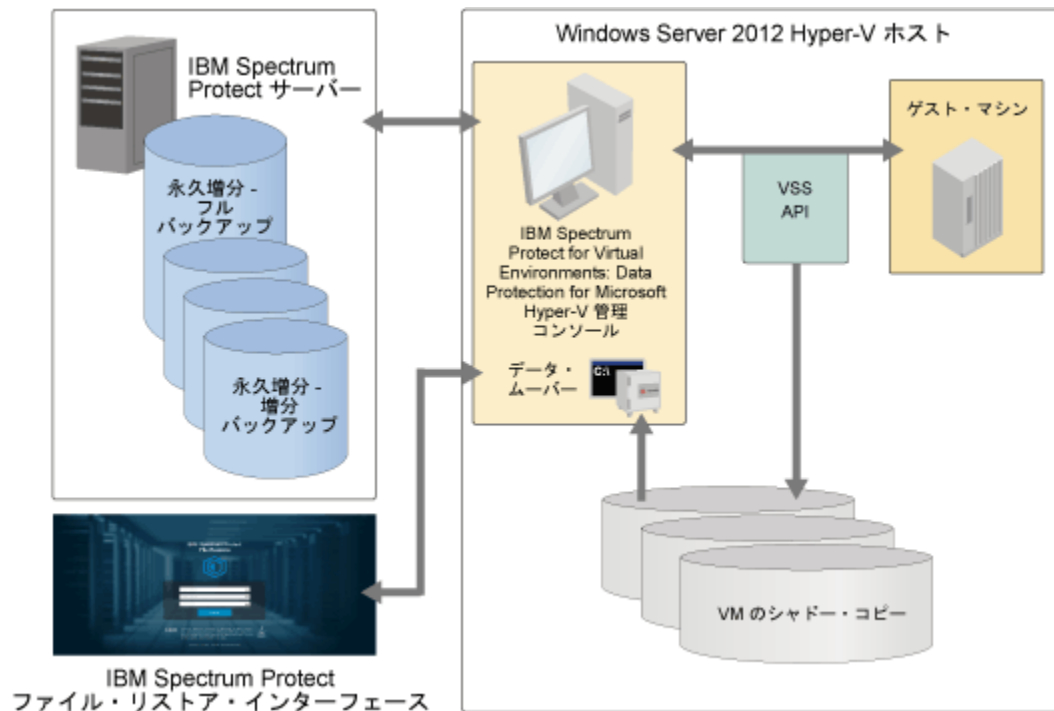


図 2. Windows Server 2012 環境における Data Protection for Microsoft Hyper-V の概要

Data Protection for Microsoft Hyper-V での IBM Spectrum Protect ノードの使用方法

Data Protection for Microsoft Hyper-V は、バックアップ操作、リストア操作、またはマウント操作中に、IBM Spectrum Protect ノードを介して VM と通信します。

ノードは、データ・ムーバー、Data Protection for Microsoft Hyper-V、またはその他のアプリケーション・クライアントがインストールされているシステムを表します。このシステムは、IBM Spectrum Protect サーバーに登録されています。各ノードには、サーバーに対してシステムを識別するために使用される固有の名（ノード名）があります。VM データへの通信、ストレージ・ポリシー、権限、およびアクセスは、ノードに基づいて定義されます。

Data Protection for Microsoft Hyper-V 環境で最も基本的なノード構成は、2 つのノード、すなわちデータ・ムーバー・ノードとターゲット・ノードで構成されます。

- データ・ムーバー・ノードは、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。IBM Spectrum Protect サーバーでこのノードの下にデータは保管されません。
- ターゲットは、IBM Spectrum Protect サーバーで VM データが保管されるノード名です。

クラスター環境のノード構成は、クラスターの名前に関連付けられているターゲット・ノードと、クラスター内のホストごとに 1 つのデータ・ムーバー・ノードで構成されます。

マウント操作の場合、ホスト・システムごとにマウント・プロキシ・ノード・ペアが必要です。マウント・プロキシ・ノードは、マウントされた VM ディスクに iSCSI 接続経由でアクセスする Linux® または Windows のプロキシ・システムを表します。これらのノードにより、マウントされた VM ディスク上のファイル・システムが、プロキシ・システム上のマウント・ポイントとしてアクセス可能になります。それにより、ファイル・リストア・インターフェースを使用して個々のファイルをリストアしたり、Recovery Agent を使用して、マウント・ポイントからローカル・ディスクにファイルをコピーすることでそれらのファイルを取得することができます。マウント・プロキシ・ノードはペアで作成され、プロキシの機能を果たす Windows または Linux システムごとに Hyper-V ホスト・ノードが必要です。

構成を簡素化するために、Data Protection for Microsoft Hyper-V 構成ウィザードは、バックアップ操作、リストア操作、およびファイル・リストア操作に必要な各種ノードを自動的に作成します。また、構成ウィザードは、IBM Spectrum Protect サーバー上のノードを登録し、必要なプロキシ関係を作成し、ロー

カル・オプション・ファイルを作成し、ローカル Windows ホスト上のデータ・ムーバー・ノードに対してサービスを構成して開始します。

作成されるノードのタイプは、ご使用の Hyper-V 環境、およびファイル・リストア機能を有効にしたかどうかによって決まります。作成されるノード名は、クラスター名またはホスト名、およびノード・タイプに基づく特定の命名規則に従います。カスタム・ノード名は使用できません。

Data Protection for Microsoft Hyper-V V8.1.2 以前からアップグレードするときに、IBM Spectrum Protect サーバーですでに定義されているノードがある場合、サーバーでノード名を更新する必要があります。詳細については、[16 ページの『IBM Spectrum Protect サーバー上のノードの名前変更』](#)を参照してください。

以下の表に、Data Protection for Microsoft Hyper-V 環境におけるさまざまなノード・タイプの比較を示しています。

表 1. 構成ウィザードで構成されるノードのタイプ		
ノード・タイプ	命名規則	説明
ターゲット・ノード	スタンドアロン・ホストの場合: <i>hostname_HV_TGT</i> クラスターの場合: <i>clustername_HV_TGT</i>	IBM Spectrum Protect サーバーですべての VM バックアップが保管されているノード名。 クラスターの場合、クラスター内のどのホストがバックアップするかに関係なく、VM は単一のノード名 (クラスター・ノード) で IBM Spectrum Protect サーバー上の単一のコンテナにバックアップされます。
データ・ムーバー・ノード	<i>hostname_HV_DM</i>	IBM Spectrum Protect サーバー上でターゲット・ノードにデータをバックアップするノード。データ・ムーバー・ノード下にはデータは保管されません。 クラスターの場合、クラスター内のホストごとにデータ・ムーバー・ノードが作成されます。
Windows マウント・プロキシ・ノード	<i>hostname_HV_MP_WIN</i>	ファイル・リストア・インターフェースのマウント操作に必要な、マウント・プロキシ・ノード・ペア内の 2 つのノードの内の 1 つ。 クラスターの場合、クラスター内のホストごとに Windows マウント・プロキシ・ノードが作成されます。
Linux マウント・プロキシ・ノード	<i>hostname_HV_MP_LNX</i>	ファイル・リストア・インターフェースのマウント操作に必要な、マウント・プロキシ・ノード・ペア内の 2 つのノードの内の 1 つ。 クラスターの場合、クラスター内のホストごとに Linux マウント・プロキシ・ノードが作成されます。

デフォルトのノード名に以下のように接頭部および接尾部を追加することもできます:
prefix_hostname_HV_TGT_suffix。手順については、[18 ページの『ノード名のカスタマイズ』](#)を参照してください。

仮想マシン・レベルでのポリシー管理

Hyper-V 仮想マシン・バックアップのストレージ要件は、IBM Spectrum Protect サーバーの管理クラスによって決まります。

仮想マシンごとに異なるポリシーを設定することができます。デフォルト管理クラスにより、すべての Hyper-V バックアップのストレージ特性が決まりますが、デフォルトの管理クラスを指定変更したり、Hyper-V 制御ファイルに使用する管理クラスを指定したりすることができます。

vmmc オプションを使用して、Hyper-V 仮想マシン・バックアップのデフォルト管理クラスを変更できます。また、vmctlmc オプションを使用して、Hyper-V 制御ファイルのデフォルト管理クラスを変更できます。

関連資料

[214 ページの『Vmmc』](#)

vmmc オプションは、デフォルト管理クラス以外の管理クラスを使用して仮想マシン・バックアップを保管するために使用します。

[199 ページの『Vmctlmc』](#)

このオプションは、仮想マシンの制御ファイルのバックアップ時に使用する管理クラスを指定します。

永久増分バックアップ戦略

永久増分バックアップ戦略は、データの高速リカバリーを提供しつつ、バックアップ・ウィンドウを最小化します。

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V では、永久増分バックアップと呼ばれるバックアップ戦略が提供されています。このバックアップ・ソリューションでは、フルバックアップは最初に 1 回行うだけで済みます。その後は、一連の増分バックアップが継続的 (永久) に行われます。永久増分バックアップ・ソリューションには、以下の利点があります。

- ネットワークでの送信データ量が削減される。
- すべての増分バックアップには、前回のバックアップ以降に変更されたブロックしか含まれていないため、データの増大が削減される。
- 変更済みブロックのみが識別されるため、バックアップ・ターゲットとの比較が必要ない。
- クライアント・システムへの影響が最小化される。
- バックアップ・ウィンドウの長さが削減される。
- 初期フルバックアップのスケジュールを 別個のスケジュールとして設定する必要がない: 永久増分バックアップを最初に実行すると、永久増分フルバックアップが自動的にデフォルトで実行されます。

この他にも、リストアされたバックアップに属する最新バージョンのブロックのみがリストアされるため、リストア・プロセスが最適化されます。実動ディスク上の同じ領域がリカバリーされるのは 1 回のみであるため、同じブロックに複数回書き込みが行われることはありません。これらの利点の結果として、永久増分は、望ましいバックアップ戦略です。

Windows PowerShell を使用したスナップショット管理

Microsoft Hyper-V システムでは、Windows PowerShell "cmdlets"を使用して、Hyper-V 仮想マシン用に IBM Spectrum Protect で作成されたスナップショットを削除する (取り消す) ことができます。

これらのコマンドレットは、Hyper-V システムでのみ使用できます。Microsoft System Center Virtual Machine Manager からスナップショットを削除することはできません。

Hyper-V システムは、スナップショットを含む仮想ハード・ディスクや、差分 (永久増分) スナップショットのチェーンに関連した仮想ハード・ディスクを編集しないように警告するメッセージを発行します。代わりに、コマンドレットを使用してスナップショットを管理することで、データ損失のリスクを最小限に抑えます。

Hyper-V に使用可能なコマンドレットのリストについては、<http://technet.microsoft.com/en-us/library/hh848559.aspx> にアクセスして、使用可能なコマンドレットの情報をお読みください。-**SnapshotType Recovery** パラメーターを指定した **Get-VMSnapshot** コマンドレットを使用して、仮想マシン (VM) に関連付けられたスナップショットを取得します。スナップショットを削除するには、**Remove-VMSnapshot** コマンドレットを使用します。スナップショットを除去すると、そのスナップショットがスナップショット差分ファイル (AVHDX ファイル) に書き込んだ情報がマージされて、VM のハード・ディスク (VHDX ファイル) に戻されます。

VM のスナップショットが複数のタイプで存在する場合は、スナップショットを削除する際にスナップショット・タイプによって結果をフィルタリングすることができます。例えば、スナップショット・タイプが「**recovery**」であるスナップショットのみを削除するには、次のコマンドレットを実行します。

```
get-vmnapshot * | where snapshottype -eq recovery | remove-vmnapshot
```

Hyper-V バックアップ操作の制約事項

Hyper-V バックアップ操作を開始する前に、制約事項を確認してください。すべての Hyper-V バックアップ操作に適用される制約事項もあれば、Windows Server 2012 または 2012 R2 もしくは Windows Server 2016 の環境上の Hyper-V バックアップのみに適用される制約事項もあります。

すべての Hyper-V バックアップに適用される制約事項

同じホスト上で並行バックアップ操作またはリストア操作を実行することはできません。例えば、同じホスト上で同時に 2 つ以上の **backup vm** コマンドまたは **restore vm** コマンドを実行した場合、一方のバックアップ操作またはリストア操作が失敗し、エラー・メッセージが発行されます。Data Protection for Microsoft Hyper-V バージョン 8.1.6 以降、Data Protection for Microsoft Hyper-V 管理コンソールは、同じホストに対して実行依頼されたバックアップ・タスクおよびリストア・タスクをキューに入れます。ホスト上でアクティブになるバックアップ・タスクあるいはリストア・タスクは 1 つのみです。追加のバックアップ・タスクあるいはリストア・タスクは、アクティブ・タスクが完了するまで保留中状態になります。アクティブ・タスクが完了すると、次の保留中タスクがアクティブになります。

Data Protection for Microsoft Hyper-V は、VHDX ディスク形式のみで Microsoft Hyper-V 仮想マシン (VM) に対する永久増分 - フルバックアップ操作および永久増分 - 増分バックアップ操作をサポートします。VHD ディスク形式で Hyper-V VM をバックアップする必要がある場合は、バージョン 7.1 のバックアップ/アーカイブ・クライアント (Data Protection for Microsoft Hyper-V なし) を使用して、フル VM のイメージ・バックアップを作成します。V7.1 バックアップ/アーカイブ・クライアントのコマンド **dsmc backup vm vmname -vmbackuptype=hypervfull -mode=full** を発行して、Microsoft Hyper-V 仮想マシンの VHD ディスクまたは VHDX ディスク上のすべてのオブジェクトのイメージ・バックアップを作成します。オプションで、Microsoft の資料に記載されている指示に従い、.vhd ファイルを .vhdx フォーマットに変換します。

VM のバックアップ操作に対する Data Protection for Microsoft Hyper-V のサポートは、英語の 7 ビット ASCII 文字のみを含む VM 名と Hyper-V ホストまたはクラスター名に限定されます。他の言語文字を使用する VM 名と Hyper-V ホストまたはクラスター名は、現時点ではサポートされません。その他の文字制限は、243 ページの『[仮想マシンおよび Hyper-V ホストまたはクラスターの名前にサポート対象外の文字がある](#)』にリストされています。

Microsoft Windows Management Instrumentation (WMI) サービス (**winmgmt**) は、Data Protection for Microsoft Hyper-V、IBM Spectrum Protect バックアップ/アーカイブ・クライアント、および IBM Spectrum Protect リカバリー・エージェント がインストールされているシステムで実行されなければなりません。WMI サービスが実行されていない場合、操作は失敗します。したがって、WMI サービスをオフにしないでください。

物理互換モードのロー・デバイス・マップ (RDM) ディスク、独立ディスク、あるいはゲスト内 iSCSI を介してゲストに直接接続されたディスク上で Exchange Server データベースがホストされていないことを確認してください。

共有仮想ハード・ディスクを使用して VM をバックアップすることはできません。

スナップショット差分バックアップ操作は、Hyper-V 環境ではサポートされません。Data Protection for Microsoft Hyper-V 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ール・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。

Windows Server 2012 および 2012 R2 での VM バックアップのみに適用される制約事項

Data Protection for Microsoft Hyper-V は、物理ディスク (iSCSI ディスクなどのパススルー・ディスク) が接続された VM をバックアップしません。この制約事項が生じるのは、Data Protection for Microsoft Hyper-V が、バックアップ操作に Volume Shadow Copy Service (VSS) を使用し、VSS が物理ディスクのスナップショットを作成できないからです。物理ディスクが接続された VM をバックアップしようとすると、物理ディスクを使用するその VM のバックアップ操作が失敗しますが、それ以外の VM のバックアップ操作は続行します。

Windows Server 2012 R2 オペレーティング・システム上の Hyper-V 構成は、Windows Server 2012 と互換性がありません。その結果、Windows Server 2012 R2 から Windows Server 2012 へのリストア操作は失敗します。ただし、Windows Server 2012 から Windows Server 2012 R2 へのリストア操作は正常に行われます。詳しくは、Microsoft サポート技術情報に進み、記事 2868279 を検索してください。

Windows Server 2012 オペレーティング・システムでは、1 つの VM ディスクにつき複数のバックアップ・セッションを実行することはできません。しかし、それ以外のサポートされているすべての Windows オペレーティング・システム (Windows Server 2012 R2、Windows Server 2016、およびそれ以降のオペレーティング・システム) では、1 つの VM ディスクにつき複数のバックアップ・セッションを実行できます。また、サポートされているすべての Windows オペレーティング・システム (Windows Server 2012 を含む) では、1 つの VM ディスクにつき複数のリストア・セッションを実行できます。

Windows Server 2016 以降での VM バックアップのみに適用される制約事項

Hyper-V クラスター・オペレーティング・システムのローリング・アップグレード中に VM バックアップ操作を実行することはできません。

Data Protection for Microsoft Hyper-V が変更追跡情報を取得できない場合、永久増分 - フルバックアップが実行されます。

Data Protection for Microsoft Hyper-V は、Paused 状態である VM のアプリケーション整合スナップショットを作成することはできません。Paused 状態で VM のクラッシュ整合スナップショットのみを作成できます。例えば、dsm.opt ファイルで以下のオプションを設定します。

```
INCLUDE.VMSNAPSHOTATTEMPTS VM_name 1 1
```

Windows Server 2016 のみ: Data Protection for Microsoft Hyper-V を Windows Server 2016 の Nano Server にインストールすることはできません。ただし、Data Protection for Microsoft Hyper-V を Windows Server 2016 で使用すると、Nano Server ゲスト VM のクラッシュ整合バックアップを作成することができます。

既知の問題と制約事項の最新の更新については、[技術情報 1993768](#) を参照してください。

資料リソース

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ソフトウェアは、仮想マシンの保護に役立つ複数のコンポーネントを提供します。このため、個々のタスクを支援するさまざまな資料リソースが提供されています。

表 2. Data Protection for Microsoft Hyper-V に関する資料リソース		
資料	内容	位置
IBM Spectrum Protect for Virtual Environments Data Protection for Microsoft Hyper-V インストールとユーザーのガイド	概要情報、戦略計画、インストール、構成、バックアップおよびリストアのシナリオ、ならびにコマンド・ライン・リファレンス。	IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSERB6/landing/welcome_sserb6.html)

表 2. Data Protection for Microsoft Hyper-V に関する資料リソース (続き)

資料	内容	位置
Data Protection for Microsoft Hyper-V 管理コンソール GUI のオンライン・ヘルプ	Hyper-V ゲスト仮想マシン、構成、バックアップ管理およびバックアップのモニターに関連したバックアップおよびリストアのタスク。	<p>以下のいずれかの方式を使用して、Data Protection for Microsoft Hyper-V 管理コンソールを開始します。</p> <ul style="list-style-type: none"> • Windows システムで、「スタート」 > 「IBM Spectrum Protect」 > 「DP for Hyper-V 管理コンソール」をクリックします。 • 管理者コマンド・プロンプト・ウィンドウを開き、以下のコマンドを入力します。 <code>"C:\Program Files\IBM\SpectrumProtect\DPHyperV\DpHv.msc"</code> <p>ヘルプにアクセスするには、以下のいずれかの方法を使用します。</p> <ul style="list-style-type: none"> • Data Protection for Microsoft Hyper-V 管理コンソールのメインページで、「始めに」セクションのリンクをクリックします。 • メニュー・バーで、「ヘルプ」 > 「Data Protection for Microsoft Hyper-V のヘルプ」をクリックします。
IBM Spectrum Protect ファイル・リストア・インターフェースのオンライン・ヘルプ	VM バックアップの個々のファイルおよびフォルダーをリストアします。	<p>ファイル・リストア管理者によって提供される URL を使用して、ファイル・リストア・インターフェースを開始します。</p> <p>「ヘルプ」 > 「製品資料」をクリックして、ヘルプにアクセスします。</p>

表 2. Data Protection for Microsoft Hyper-V に関する資料リソース (続き)		
資料	内容	位置
データ・ムーバー・コマンド・ライン・クライアントのオンライン・ヘルプ	Hyper-V ゲスト仮想マシンに関連したバックアップおよびリストアのタスク。	<p>次のいずれかの方法を使用してデータ・ムーバー・コマンド・ライン・クライアントを開始します。</p> <ul style="list-style-type: none"> • Windows システムで、「スタート」> IBM Spectrum Protect > 「バックアップ/アーカイブ・コマンド・ライン (Backup-Archive Command Line)」に進みます。 • 管理者コマンド・プロンプト・ウィンドウを開き、バックアップ/アーカイブ・クライアントのインストール・ディレクトリーに変更します (cd "C:\Program Files\Tivoli\tsm\baclient")。 dsmc.exe を実行します。 <p>ヘルプにアクセスするには、以下のいずれかの方法を使用します。</p> <ul style="list-style-type: none"> • コマンド・ライン・クライアントを開始した後、Protect> プロンプトで help と入力してヘルプの目次を表示します。 • 独自のウィンドウでヘルプを表示するには、管理者コマンド・プロンプト・ウィンドウを開き、バックアップ/アーカイブ・クライアントのインストール・ディレクトリーに変更します (cd "C:\Program Files\Tivoli\tsm\baclient")。 <p>dsmc.exe help を実行して、ヘルプの目次を表示します。コマンドの末尾にトピックのタイトルを付加してトピックのヘルプを表示することもできます。例えば、dsmc help options は、クライアント・オプションの使用法を説明するヘルプ・トピックを表示します。dsmc help backup vm は、backup vm コマンドのヘルプを表示します。</p>

第 2 章 Data Protection for Microsoft Hyper-V のインストールおよびアップグレード

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V のインストールには、計画、インストール、およびアップグレードのタスクが含まれます。

Data Protection for Microsoft Hyper-V のインストール計画

Data Protection for Microsoft Hyper-V をインストールする前に、インストールされる機能を把握し、システム要件を確認してください。

インストールされる機能

Data Protection for Microsoft Hyper-V のすべての機能は、インストール・スイートの一部です。

通常の Data Protection for Microsoft Hyper-V のインストールでは、以下のコンポーネントがインストールされます。

- IBM Spectrum Protect 個のデータ・ムーバー
- Data Protection for Microsoft Hyper-V 管理コンソール
- IBM Spectrum Protect ファイル・リストア機能
- Data Protection for Microsoft Hyper-V PowerShell コマンドレット
- IBM Spectrum Protect リカバリー・エージェント
- IBM Spectrum Protect Web サーバー
- IBM Spectrum Protect Java™ 仮想マシン (JVM)

これらの機能およびそのサポート・パッケージを個別にインストールする必要はありません。インストールの手順については、[22 ページの『Data Protection for Microsoft Hyper-V の標準インストールの実行』](#)を参照してください。

ゲスト内アプリケーション保護のリストア操作用にデータ・ムーバーのみをインストールする場合は、[26 ページの『Data Protection for Microsoft Hyper-V データ・ムーバーのみのインストール』](#)を参照してください。リカバリー・エージェントは、データ・ムーバーのインストールに含まれています。IBM Spectrum Protect リカバリー・エージェントを個別にインストールすることはできなくなりました。

Data Protection for Microsoft Hyper-V をリモートで管理する場合は、別個の Windows ホストに Data Protection for Microsoft Hyper-V 管理コンソールのみをインストールします。詳しくは、[24 ページの『Data Protection for Microsoft Hyper-V 管理コンソール のみのインストール』](#)を参照してください。PowerShell コマンドレットはこのインストールに含まれています。

Data Protection for Microsoft Hyper-V は、Server Core オプションを使用してインストールされた Windows Server オペレーティング・システムの Hyper-V ホストにインストールすることもできます。そして、Data Protection for Microsoft Hyper-V 管理コンソールを別の Windows Server または Windows 10 クライアントにインストールして、リモート側で Data Protection for Microsoft Hyper-V を管理することができます。詳しくは、[30 ページの『Windows Server Core システムへの Data Protection for Microsoft Hyper-V のインストールおよび構成』](#)を参照してください。

システム要件の判別

Data Protection for Microsoft Hyper-V では、最低限のハードウェア、ディスク・スペース、メモリー、およびソフトウェアが必要です。

次の表は、Data Protection for Microsoft Hyper-V のインストールに必要な最小ハードウェア要件を示しています。

表 3. Data Protection for Microsoft Hyper-V の最小ハードウェア要件		
コンポーネント	最小要件	推奨
システム	x64 プロセッサ	適用外
メモリー	4 GB RAM	16 GB RAM
利用可能なハード・ディスク	2 GB	3.5 GB
NIC カード	1 NIC - 100 Mbps	1 NIC - 10 Gbps

Data Protection for Microsoft Hyper-V を使用するには、Hyper-V 役割が Microsoft Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、または Windows Server 2019 オペレーティング・システムにインストールされている必要があります。Hyper-V サーバー (Windows ハイパーバイザーのみを含むスタンドアロン製品) もサポートされています。

Windows Server 2012 または 2012 R2 システムでは、頑強性とパフォーマンスを確保するために、ソフトウェア・プロバイダーではなく、VSS ハードウェア・プロバイダーを使用してください。

Windows Server 2016 のみ: Data Protection for Microsoft Hyper-V を Windows Server 2016 の Nano Server にインストールすることはできません。ただし、Data Protection for Microsoft Hyper-V を Windows Server 2016 で使用すると、Nano Server ゲスト VM のクラッシュ整合バックアップを作成することができます。

Linux システム上でアプリケーション整合バックアップやファイル・リストア操作を行うには、Linux Integration Services (LIS) が Linux 仮想マシン (VM) および Linux マウント・プロキシにインストールされている必要があります。詳しくは、[技術情報 0880755](#) を参照してください。

Data Protection for Microsoft Hyper-V の詳細なソフトウェア要件およびハードウェア要件については、[技術情報 1505139](#) のバージョン 8.1.10 のセクションを参照してください。

Microsoft Exchange Server または Microsoft SQL Server をホストする VM のアプリケーション保護のソフトウェア要件について詳しくは、[技術情報 2017347](#) を参照してください。

ファイル・リストア機能の前提条件は、[86 ページの『ファイル・リストアの前提条件』](#)を参照してください。

必要な通信ポート

Data Protection for Microsoft Hyper-V をインストールする前に、ファイアウォールで特定の通信ポートが開いていることを確認します。

Data Protection for Microsoft Hyper-V は、以下の TCP ポートを使用します。各コンピューターのそれぞれのファイアウォールで、これらのポートが開いている必要があります。

表 4. Data Protection for Microsoft Hyper-V に必要な通信ポート			
コンピューター	機能	インバウンド TCP ポート	アウトバウンド TCP ポート
Hyper-V ホスト	すべて	1581, 1582, 3260, 9081	135, 445, 1500, 1581, 9081
Windows VM	ファイル・リストア、アプリケーション保護	135, 445	適用されません。
Linux マウント・プロキシ	ファイル・リストア	1581	22, 1581, 3260
Linux VM	ファイル・リストア	22	適用されません。

以下の表は、各コンポーネントで使用するポートを示しています。

表 5. コンポーネントによって使用される通信ポート	
コンポーネント	TCP ポート
SSH	22
WMI	135, 445
IBM Spectrum Protect サーバー (server)	1500
クライアント・アクセプター (CAD)	1581, 1582
iSCSI	3260
REST API	9081

制約事項: iSCSI トラフィックをサポートするには、Hyper-V ホスト上の Windows マウント・プロキシと Linux マウント・プロキシが同じサブネット上になければなりません。

これらのポートのいずれかが構成中に変更された場合、ファイアウォール規則を更新する必要があります。

Data Protection for Microsoft Hyper-V のアップグレード

旧バージョンから Data Protection for Microsoft Hyper-V バージョン 8.1.10 にアップグレードする際に実行する必要があるタスクを確認します。

異なるバージョンとの互換性

複数のクラスターおよびホストを使用する環境では、Data Protection for Microsoft Hyper-V は、以降のバージョンとの互換性があります。

Data Protection for Microsoft Hyper-V をご使用の環境内の複数のクラスターおよびホストにデプロイする場合、インストールされる製品バージョンは新しいバージョンと互換性があります。具体的には、ご使用の環境に新規バージョンの Data Protection for Microsoft Hyper-V が導入された場合、以前のバージョンの Data Protection for Microsoft Hyper-V 管理コンソールおよび PowerShell コマンドレットは、新しいバージョンに接続することができます。この互換性により、環境内のすべての Data Protection for Microsoft Hyper-V デプロイメントを最新レベルに更新する時間的な猶予が生じます。

ただし、Data Protection for Microsoft Hyper-V 管理コンソール または PowerShell コマンドレットでは Data Protection for Microsoft Hyper-V の旧バージョンに接続できません。メッセージにより、以前のデプロイメントを新しいデプロイメントにアップグレードするか、以前のデプロイメントで提供された管理コンソールまたは PowerShell コマンドレットを使用するようプロンプトが出されます。

例

以下の表は、Data Protection for Microsoft Hyper-V が複数のクラスターまたはホストにデプロイされている環境での、旧バージョンの Data Protection for Microsoft Hyper-V (V8.1.4 および V8.1.6) と Data Protection for Microsoft Hyper-V V8.1.10 の間の互換性を示しています。

この例では、Data Protection for Microsoft Hyper-V V8.1.4 または V8.1.6 と Data Protection for Microsoft Hyper-V V8.1.10 は、環境内の異なるクラスターにインストールされています。

表 6. 互換性の例		
Data Protection for Microsoft Hyper-V 管理コンソールまたはコマンドレットのバージョン	Data Protection for Microsoft Hyper-V のバージョン	互換性の有無
V8.1.4 または V8.1.6	V8.1.10	あり。すべての操作が、V8.1.4 または V8.1.6 デプロイメントに接続されている場合と同様に機能します。

表 6. 互換性の例 (続き)

Data Protection for Microsoft Hyper-V 管理コンソールまたはコマンドレットのバージョン	Data Protection for Microsoft Hyper-V のバージョン	互換性の有無
V8.1.10	V8.1.4 または V8.1.6	なし。V8.1.4 または V8.1.6 デプロイメントを最新バージョンにアップグレードするか、以前のデプロイメントで提供された管理コンソールまたは PowerShell コマンドレットを使用してください。

IBM Spectrum Protect サーバー上のノードの名前変更

ご使用の環境を Data Protection for Microsoft Hyper-V バージョン 8.1.2 以前から V8.1.10 にアップグレードする場合、事前にお客様と IBM Spectrum Protect サーバー管理者でサーバー上のノードを名前変更する必要があります。

このタスクについて

IBM Spectrum Protect で既存のノード名を変更する場合、ステップ 16 ページの『1』で説明されている命名規則を使用する必要があります。

制約事項：構成ウィザードを使用して Data Protection for Microsoft Hyper-V を構成する場合、Data Protection for Microsoft Hyper-V V8.1.2 以前で作成された古い仮想マシン (VM) バックアップをリストアする前に、構成を完了する必要があります。そうしないと、Data Protection for Microsoft Hyper-V 管理コンソールで古い VM バックアップをリストアできません。

手動で Data Protection for Microsoft Hyper-V を構成し、データ・ムーバー・コマンド・ラインを使用して VM をリストアする場合、構成ウィザードを実行するまで古いノード名は引き続き使用できます。

手順

IBM Spectrum Protect サーバー管理者は、以下のステップを実行します。

1. **RENAME NODE** サーバー・コマンドを使用して、既存の Hyper-V ノード名 (asnodename オプションにより指定) を、以下の命名規則に準拠する新規ターゲット・ノード名に名前変更します。

- ・ スタンドアロン Hyper-V ホスト環境の場合: *hostname_HV_TGT*
- ・ クラスター環境の場合: *clustername_HV_TGT*

例えば、クラスター・ノード名が Cluster1 のクラスターの場合、新規ターゲット・ノード名は Cluster1_HV_TGT または *prefix_Cluster1_HV_TGT_suffix* になります。

デフォルトのノード名に接頭部および接尾部を追加することもできます。例えば、*prefix_hostname_HV_TGT_suffix* あるいは *prefix_clustername_HV_TGT_suffix* などです。

ノード名への接頭部および接尾部の追加の手順については、18 ページの『ノード名のカスタマイズ』を参照してください。

制約事項：これらの命名規則に準拠していないノード名を使用することはできません。Data Protection for Microsoft Hyper-V 構成ウィザードを実行すると、新しい命名規則を使用する新しいターゲット・ノード、および関連付けられたデータ・ムーバー・ノードは、自動的に IBM Spectrum Protect サーバーに登録されます。また、必要な Windows サービスがローカル Windows ホストで構成されます。

2. **UPDATE SCHEDULE** サーバー・コマンドを使用して、以下の必須パラメーターで既存のスケジュールを更新します。
 - ・ スケジュール定義に ACTION=BACKUP パラメーターと SUBACTION=VM パラメーターを指定します。
 - ・ オプション・ストリングを以下のように更新します。

- スタンドアロン・ホスト名の場合: `options=' -asnodename=hostname_HV_TGT -domain.vmfull="all-vm" '` または `options=' -asnodename=prefix_hostname_HV_TGT_suffix -domain.vmfull="all-vm" '`
- クラスター名の場合: `options=' -asnodename=clustername_HV_TGT -domain.vmfull="all-vm" '` または `options=' -asnodename=prefix_clustername_HV_TGT_suffix -domain.vmfull="all-vm" '`

詳細については、75 ページの『[ホストまたはクラスターのマシンのバックアップ・スケジュールの管理](#)』を参照してください。

3. オプション: IBM Spectrum Protect サーバーで **REPLICATE NODE** コマンドを発行して、ノード複製パラメーターを更新します。

- スタンドアロン・ホストの場合、`hostname_HV_TGT` または `prefix_hostname_HV_TGT_suffix` ノードでデータを複製します。
- クラスターの場合、`clustername_HV_TGT` または `prefix_clustername_HV_TGT_suffix` ノードでデータを複製します。

Hyper-V ホストで以下のタスクを実行します。

4. スタンドアロン・ホスト上またはクラスター内のすべてのホスト上で Data Protection for Microsoft Hyper-V を V8.1.10 にアップグレードします。

手順については、22 ページの『[Data Protection for Microsoft Hyper-V の標準インストールの実行](#)』を参照してください。

5. Hyper-V ホストで構成ウィザードを実行します。クラスターの場合、クラスター内のいずれかのホスト (通常は、ローカル Windows ホスト) でウィザードを実行します。

手順については、39 ページの『[ウィザードを使用した Data Protection for Microsoft Hyper-V の構成](#)』を参照してください。

6. Data Protection for Microsoft Hyper-V 管理コンソールで「**バックアップ管理**」ウィンドウを使用して、スケジュールを新しいターゲット・ノード名に関連付けます。

手順については、75 ページの『[ホストまたはクラスターのマシンのバックアップ・スケジュールの管理](#)』を参照してください。

7. Data Protection for Microsoft Hyper-V 管理コンソールのバックアップ操作とリストア操作を実行して、構成を検証します。

手順については、以下を参照してください。

- [79 ページの『仮想マシンのアドホック・バックアップの開始』](#)
- [80 ページの『仮想マシンのリストア』](#)

8. 構成が検証された後、以下のクリーンアップ・タスクを実行します。

- IBM Spectrum Protect サーバー管理者は、**REMOVE NODE** サーバー・コマンドを使用して古いデータ・ムーバー・ノードを削除します。
- Hyper-V 管理者は、スタンドアロン・ホストまたはクラスター内の各ホストで **dsmcutil remove** コマンドを実行して、古いクラスター・ノードやデータ・ムーバー・ノード用に作成されたサービスを削除します。

詳しくは、[Dsmcutil コマンド: 必須指定のオプションおよび例の REMove コマンド](#)を参照してください。

タスクの結果

Data Protection for Microsoft Hyper-V を使用してご使用の Hyper-V VM を保護することができます。

バックアップ・ヒストリーの表示のヒント: ノード更新前に生成されたバックアップ・ヒストリーは使用できなくなりました。ただし、「**リストア**」ウィザードまたはコマンド・ラインを使用して、引き続きすべてのバックアップのリストアが可能です。ノードの更新後は、最初のバックアップ操作やそれ以降のバックアップ操作のバックアップ・ヒストリーを使用できます。

クラスター構成でのノード更新直後、VM バックアップを表示およびリストアできるのは、クラスター・ビューからのみであり、ホスト・ビューからは実行できません。ホスト・ビューには、ホスト・ノードが所有する VM のみが含まれています。ノードの更新後、バックアップはホスト・ノードによって所有されていません。バックアップが正常に実行されると、VM は、ホスト・ビューから再びバックアップおよびリストアすることができます。

次のタスク

状況によっては、以下のタスクの 1 つまたは両方を完了する必要があります。

- IBM Spectrum Protect サーバー管理者は、**QUERY PROXY NODE** サーバー・コマンドを発行して、ターゲット・ノードにデータ・ムーバー・ノードのプロキシ権限が付与されていることを確認します。
- Hyper-V 管理者は、Hyper-V ホストで、クライアント・アクセプター・サービスを再始動します。

IBM Spectrum Protect サーバー管理者は、更新ノードのバックアップ・レポートが正しく表示されるようにするために、スケジュールを実行します。

関連概念

6 ページの『[Data Protection for Microsoft Hyper-V での IBM Spectrum Protect ノードの使用方法](#)』

Data Protection for Microsoft Hyper-V は、バックアップ操作、リストア操作、またはマウント操作中に、IBM Spectrum Protect ノードを介して VM と通信します。

ノード名のカスタマイズ

デフォルトのノード名に接頭部または接尾部、あるいはその両方を追加することができます。この方法で、構成ウィザードに自動的に生成されるノード名をカスタマイズできます。

このタスクについて

構成ウィザードを使用して Data Protection for Microsoft Hyper-V を構成する場合、作成されるノードは、以下のデフォルトの命名規則に準拠します。

```
hostname_HV_TGT (またはクラスターの場合は clustername_HV_TGT)
hostname_HV_DM
hostname_HV_MP_WIN (ファイル・リストア機能が有効にされている場合)
hostname_HP_MP_LNX (ファイル・リストア機能が有効にされている場合)
```

ただし、ノード名をカスタマイズすることができます。例えば、複数のテナントが同じサーバー上でそれぞれの仮想マシン (VM) をホストするマルチテナント環境をサポートするために、ノード名のカスタマイズが必要な場合があります。テナントをベースにノードを差別化するために、接頭部または接尾部、あるいはその両方をデフォルトのノード名に追加することができます。

新規の Data Protection for Microsoft Hyper-V 構成または既存の構成のノード名をカスタマイズすることができます。

手順

ノード名をカスタマイズするには、以下の手順を実行します。

1. スタンドアロン環境またはクラスター環境の Hyper-V ホスト上の `C:\IBM\SpectrumProtect\webservers\usr\servers\veProfile\tsmVmGUI` ディレクトリーに、`hvConfig.props` という名前のテキスト・ファイルを作成します。
2. `hvConfig.props` ファイルを編集し、以下の 2 つのステートメントをファイルに追加します。

```
node_prefix=prefix
node_suffix=suffix
```

ここで、`prefix` はノード名の先頭に追加するテキスト・ストリングで、`suffix` はノード名に付加するテキスト・ストリングです。

接頭部のみ指定することも、接尾部のみ指定することも、接頭部と接尾部の両方を指定することもできます。ノード名の長さの合計 (接頭部、接尾部、またはその両方を含む) が 64 文字を超えてはなりません。

テキスト・ストリングをブランクのままにする場合、あるいはステートメントを削除する場合は、デフォルトのノード名は変更されないまま残ります。接頭部および接尾部をいずれも使用しない場合は、`hvConfig.props` ファイルを作成しないでください。

この結果として作成される、カスタマイズされたノード名は、以下のパターンに従います。

```
prefix_hostname_HV_TGT_suffix (またはクラスターの場合は prefix_clustername_HV_TGT_suffix)
prefix_hostname_HV_DM_suffix
prefix_hostname_HV_MP_WIN_suffix (ファイル・リストア機能が有効にされている場合)
prefix_hostname_HP_MP_LNX_suffix (ファイル・リストア機能が有効にされている場合)
```

3. クラスター環境では、クラスター内の各ホスト上に `C:\¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥tsmVmGUI ¥hvConfig.props` ファイルを作成し、各ホストで同じプロパティを指定します。

重要: 構成ウィザードを実行する前に、クラスター内のすべてのホストにこのファイルがなければなりません。

4. 以前にデフォルトのノード名を使用して Data Protection for Microsoft Hyper-V を構成した場合は、IBM Spectrum Protect サーバー上でノードの名前を変更する必要があります。

手順については、[16 ページの『IBM Spectrum Protect サーバー上のノードの名前変更』](#)を参照してください。

5. Hyper-V ホストで構成ウィザードを実行します。ノードの命名規則に接頭部、接尾部、またはその両方が追加されます。

タスクの結果

例えば、Data Protection for Microsoft Hyper-V ノード名に接頭部「SP」と接尾部「DEPT1」を追加するとします。次のステートメントを `C:\¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥tsmVmGUI¥hvConfig.props` ファイルに追加しました。

```
node_prefix=SP
node_suffix=DEPT1
```

MYHOST という名前のスタンドアロン・ホストの場合、構成ウィザードを実行すると以下のノードが作成されます (ファイル・リストア機能が有効にされている場合)。

```
SP_MYHOST_HV_TGT_DEPT1
SP_MYHOST_HV_DM_DEPT1
SP_MYHOST_HV_MP_WIN_DEPT1
SP_MYHOST_HV_MP_LNX_DEPT1
```

クラスター名が MYCLUSTER で、ホスト HOSTA と HOSTB が属するクラスターがある場合、以下のノードが作成されます (ファイル・リストア機能が有効にされている場合)。

```
SP_MYCLUSTER_HV_TGT_DEPT1
SP_HOSTA_HV_DM_DEPT1
SP_HOSTA_HV_MP_WIN_DEPT1
SP_HOSTA_HV_MP_LNX_DEPT1
SP_HOSTB_HV_DM_DEPT1
SP_HOSTB_HV_MP_WIN_DEPT1
SP_HOSTB_HV_MP_LNX_DEPT1
```

次のタスク

Get-DpHvHostConfiguration Windows PowerShell コマンドレットを実行して、**node_prefix** パラメーターおよび **node_suffix** パラメーターの値を確認することができます。

例えば、PowerShell プロンプトから次のようなコマンドレットを入力します。


```
PS C:\Users\administrator> Get-DpHvHostConfiguration -Session $session
```

関連概念

6 ページの『[Data Protection for Microsoft Hyper-V での IBM Spectrum Protect ノードの使用方法](#)』

Data Protection for Microsoft Hyper-V は、バックアップ操作、リストア操作、またはマウント操作中に、IBM Spectrum Protect ノードを介して VM と通信します。

RCT バックアップに関するアップグレードの考慮事項

Data Protection for Microsoft Hyper-V バージョン 8.1.2 以降にアップグレードする前に、Windows Server 2016 での仮想マシン (VM) バックアップ操作に適用される考慮事項を検討してください。

- Hyper-V 環境を Windows Server 2012 または 2012 R2 から Windows Server 2016 にアップグレードする場合、仮想マシンの VM バージョンは自動的に更新されません。環境が Windows Server 2016 にアップグレードされた後、Hyper-V 管理者は VM を新規バージョンに更新する必要があります。Data Protection for Microsoft Hyper-V V8.1.2 以降は、新規 VM バージョンに更新されていない VM のバックアップを行いません。

VM バージョンを更新する前に、ゲスト VM がオフラインになっていることを確認してください。VM バージョンの更新は、Hyper-V Manager 内で、または [Update-VMVersion](#) cmdlet で行うことができます。

- Resilient Change Tracking (RCT) を使用する VM バックアップ操作には、Hyper-V VM がバージョン 6.2 以降であることが必要です。

Data Protection for Microsoft Hyper-V V8.1.0 以前は、VSS バックアップ方式を使用して以前の VM バージョンを引き続きサポートします。

関連タスク

20 ページの『[VSS バックアップから RCT バックアップへのマイグレーション](#)』

Data Protection for Microsoft Hyper-V バージョン 8.1.2 以降で Resilient Change Tracking (RCT) バックアップ機能を利用するには、Microsoft Volume Shadow Copy Service (VSS) から RCT に仮想マシン (VM) バックアップ操作をマイグレーションします。

VSS バックアップから RCT バックアップへのマイグレーション

Data Protection for Microsoft Hyper-V バージョン 8.1.2 以降で Resilient Change Tracking (RCT) バックアップ機能を利用するには、Microsoft Volume Shadow Copy Service (VSS) から RCT に仮想マシン (VM) バックアップ操作をマイグレーションします。

始める前に

- Hyper-V VM がバージョン 6.2 以降であることを確認してください。VM バージョンは、Hyper-V Manager で判別するか、[Get-VM](#) cmdlet を実行して判別することができます。
- Hyper-V 環境を Windows Server 2012 または 2012 R2 から Windows Server 2016 にマイグレーションする場合、Hyper-V VM の VM バージョンは自動的に更新されません。VM が Data Protection for Microsoft Hyper-V によってバックアップされる前に、VM を新しいバージョンに更新しておく必要があります。

VM の VM バージョンを更新する前に、ゲスト VM をオフラインにしていることを確認してください。VM バージョンの更新は、Hyper-V Manager 内で、または [Update-VMVersion](#) cmdlet を使用して行うことができます。

手順

VSS バックアップを RCT にマイグレーションするには、以下の手順を実行します。

1. Data Protection for Microsoft Hyper-V V8.1.10 を Windows Server 2016 オペレーティング・システムの Hyper-V ホスト・サーバーにインストールし、構成します。
2. VM で永久増分 - フルバックアップ操作を実行します。

Windows Server 2016 以降の環境におけるすべての Data Protection for Microsoft Hyper-V バックアップ操作は、RCT バックアップを使用します。

タスクの結果

- 以前の VSS バックアップには RCT 変更追跡情報がないため、初めて Data Protection for Microsoft Hyper-V V8.1.10 を使用して VM をバックアップするときに、永久差分 - フルバックアップが作成されます。
- RCT を使用する VM の最初のバックアップ後に、VSS バックアップは使用不可になります。
- Data Protection for Microsoft Hyper-V V8.1.10 では、V8.1.0 で Windows Server 2016 にバックアップされた VM を引き続きリストアできます。後続の VM バックアップでは RCT が使用されます。

関連概念

[2 ページの『Resilient Change Tracking \(RCT\) を使用した仮想マシンのバックアップ』](#)

Microsoft Windows Server 2016 以降のバージョンでの Hyper-V バックアップの場合、Resilient Change Tracking (RCT) 機能が仮想マシン (VM) のバックアップに使用されます。

[1 ページの『Volume Shadow Copy Service \(VSS\) を使用した仮想マシン・バックアップ』](#)

Windows Server 2012 および 2012 R2 での Hyper-V バックアップの場合、Microsoft Volume Shadow Copy Service (VSS) を使用して、バックアップ操作中に仮想マシン (VM) の整合スナップショットを作成します。

インストール・ウィザードを使用した Data Protection for Microsoft Hyper-V のアップグレード

インストール・ウィザードを使用して、Data Protection for Microsoft Hyper-V バージョン 8.1.10 にアップグレードすることができます。

Data Protection for Microsoft Hyper-V をアップグレードする前に、以下の情報を確認してください。

- アップグレードの前に、旧バージョンをアンインストールしないでください。最初に旧バージョンをアンインストールしてから新規バージョンをインストールすることで Data Protection for Microsoft Hyper-V をアップグレードすると、アップグレードは新規インストールとして処理されます。その結果、インストール後に初めて Data Protection for Microsoft Hyper-V 管理コンソールを開始したときに、構成ウィザードが自動的に開き、構成をすべてやり直す必要があります。
- Data Protection for Microsoft Hyper-V は、デフォルトの場所 (C:\Program Files\IBM\SpectrumProtect) にのみインストールできます。以前に Data Protection for Microsoft Hyper-V をデフォルト以外の場所にインストールした場合、前バージョンからのプログラム・ファイルは、ログ・ファイルとトレース・ファイルを除き、アップグレード時にデフォルトのインストール場所に移動します。
- デフォルト以外の場所にインストールした旧バージョンの Data Protection for Microsoft Hyper-V からアップグレードする場合は、Data Protection for Microsoft Hyper-V V8.1.10 にアップグレードする前に、IBM Spectrum Protect のすべてのクライアント・アクセプター・サービスとエージェント・サービスを必ず停止してください。これらのサービスは、一般的に「サービス」ウィンドウで「TSM クライアント・アクセプター」および「TSM リモート・クライアント・エージェント」と呼ばれています。これらのサービスをアップグレードの前に停止しておく、アップグレード・プロセス中に余計な遅延が生じないことが保証されます。

Data Protection for Microsoft Hyper-V V8.1.10 にアップグレードするには、[21 ページの『Data Protection for Microsoft Hyper-V コンポーネントのインストール』](#)の手順に従ってください。ただし、以下の制限事項があります。インストール・ウィザードでは、旧バージョンの Data Protection for Microsoft Hyper-V のインストールに使用したのと同じインストール・タイプを選択する必要があります。例えば、旧バージョンのインストールで「標準インストール」を選択した場合は、このアップグレードでも「標準インストール」を選択する必要があります。

Data Protection for Microsoft Hyper-V コンポーネントのインストール

Data Protection for Microsoft Hyper-V コンポーネントをすべてインストールするには、標準インストールを実行します。その後、各自のユース・ケースの必要に応じて、個別のコンポーネントをインストールすることができます。

ヒント: 同じ手順を使用して、Data Protection for Microsoft Hyper-V をアップグレードすることができます。ただし、アップグレードを開始する前に、[15 ページの『Data Protection for Microsoft Hyper-V のアップグレード』](#)の情報を確認してください。

インストール・パッケージのダウンロードおよび解凍

Data Protection for Microsoft Hyper-V をインストールする前に、インストール・パッケージをダウンロードし、そのパッケージからインストール・ファイルを解凍しておく必要があります。

始める前に

最新情報、更新、および保守フィックスについては、[IBM Spectrum Protect for Virtual Environments - IBM Support](#) にアクセスしてください。

手順

1. Data Protection for Microsoft Hyper-V パッケージを [IBM Passport Advantage®](#) または [Fix Central](#) からダウンロードします。
2. ダウンロードした圧縮インストール・ファイルを解凍します。
 - a) ダウンロードした圧縮インストール・パッケージを、ローカル・ディスクまたはネットワーク・アクセス可能な共有にコピーします。必ず、インストール・ファイルを空のディレクトリー (`extract_folder`) に解凍します。
 - b) インストール・ファイルを同じディレクトリーに解凍するために、圧縮インストール・パッケージをダブルクリックします。

デフォルトでは、解凍されたファイルは `extract_folder\TSMHYPERV_WIN` ディレクトリー内の現行のディスク・ドライブに保管されます。

インストール・プログラムが、このディレクトリー内に別の Data Protection for Microsoft Hyper-V インストール・ファイルを検出した場合は、古いファイルを上書きするかどうかを指定するように求めるプロンプトが出されます。ファイルの上書きに関するプロンプトが出された場合は、「(A)lways」を入力して既存のファイルを上書きします。この選択により、現行のインストールからのファイルのみが確実に使用されるようになります。

タスクの結果

Data Protection for Microsoft Hyper-V インストール・プログラム (`spinstall.exe`) は、`extract_folder\TSMHYPERV_WIN` ディレクトリーにあります。

次のタスク

[Data Protection for Microsoft Hyper-V をインストールします。](#)

インストール・ウィザードを使用した Data Protection for Microsoft Hyper-V 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 Microsoft Hyper-V の標準インストールを実行したり、使用可能なコンポーネントを個別にインストールしたりします。

Data Protection for Microsoft Hyper-V の標準インストールの実行

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ソフトウェアの標準インストール用の手順について説明します。

始める前に

クラスター環境では、クラスター内の各ホストに Data Protection for Microsoft Hyper-V パッケージを確実にインストールしてください。

Data Protection for Microsoft Hyper-V がインストールされている各ホストでは、Data Protection for Microsoft Hyper-V と通信するために使用される HTTPS ポートが、ファイアウォールで開いていることを確認してください。特に他のポートを指定しない限り、デフォルトのポート番号 9081 が使用されます。

Data Protection for Microsoft Hyper-V バージョン 8.1.2 以前からアップグレードする場合は、[16 ページの『IBM Spectrum Protect サーバー上のノードの名前変更』](#)のタスクを実行します。

Data Protection for Microsoft Hyper-V をアップグレードする場合は、[15 ページの『Data Protection for Microsoft Hyper-V のアップグレード』](#)の情報を確認してください。

22 ページの『インストール・パッケージのダウンロードおよび解凍』の説明どおりに、インストール・パッケージをダウンロードして解凍していることを確認してください。

このタスクについて

標準インストールには、Data Protection for Microsoft Hyper-V のすべての機能 (データ・ムーバー、Data Protection for Microsoft Hyper-V 管理コンソール、PowerShell コマンドレット、IBM Spectrum Protect リカバリー・エージェント など) が含まれています。

リモート管理用に Data Protection for Microsoft Hyper-V 管理コンソールのみをインストールするには、24 ページの『Data Protection for Microsoft Hyper-V 管理コンソール のみのインストール』を参照してください。PowerShell コマンドレットはこのインストールに含まれています。

ゲスト内アプリケーション保護のリストア操作用にデータ・ムーバーのみをインストールするには、26 ページの『Data Protection for Microsoft Hyper-V データ・ムーバーのみのインストール』を参照してください。リカバリー・エージェントは、データ・ムーバーのインストールに含まれています。

制約事項: Data Protection for Microsoft Hyper-V インストーラーは、Windows オペレーティング・システムで **diskpart** コマンドを使用して自動マウント機能を自動的に使用不可にします。このアクションは、IBM Spectrum Protect ファイル・リストア・インターフェースで正しいドライブ名割り当てを表示し、システムで予約済みのディスクを非表示にするのに必要です。

ファイル・リストア操作を実行する予定がない場合、または誤ったドライブ名割り当てやシステム予約ディスクがファイル・リストア・インターフェースに表示されることを気にしない場合、インストールの完了後に自動マウント機能を使用可能にすることができます。

手順

単一の Hyper-V ホストまたはクラスター内の各ホストで、以下のステップを実行します。

1. 22 ページの『インストール・パッケージのダウンロードおよび解凍』
2. インストール・プログラムを開始するために、spinstall.exe ファイルをダブルクリックします。インストール・プロセスで使用する言語を選択し、「次へ」をクリックします。
3. 「**IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V** スイートの **InstallShield ウィザードへようこそ (Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite)**」ページで、「次へ」をクリックします。
4. 「**ご使用条件**」ページで、ご使用条件の条項を読みます。「**使用条件の条項に同意します**」をクリックし、「次へ」をクリックします。ご使用条件の条項に同意しない場合、インストールは終了し、「**キャンセル**」をクリックしてインストール・ウィザードを終了する必要があります。
5. 「**インストール先フォルダー (Installation Destination Folder)**」ページで、インストール場所をメモし、「次へ」をクリックします。

Data Protection for Microsoft Hyper-V は、デフォルトの場所 (C:\Program Files\IBM\SpectrumProtect) にのみインストールできます。以前に Data Protection for Microsoft Hyper-V をデフォルト以外の場所にインストールした場合、前バージョンからのプログラム・ファイルは、ログ・ファイルとトレース・ファイルを除き、アップグレード時にデフォルトのインストール場所に移動します。

6. 「**インストール・タイプ**」ページで、「**標準インストール**」をクリックします。すぐにリストア・プロセスが始まります。インストール処理が開始された後、選択内容を変更することはできません。

ヒント: Data Protection for Microsoft Hyper-V、JVM、データ・ムーバー、Web サーバー、フレームワーク、および Recovery Agent のパッケージがインストールされるため、インストール・プロセスは完了までに数分間かかることがあります。

7. 「**インストール・ウィザード完了 (Install Wizard Completed)**」ページで、「**完了**」をクリックしてインストール・ウィザードを終了します。

ウィザードがクローズした直後に、Data Protection for Microsoft Hyper-V 管理コンソールが開始します。

構成ウィザードをすぐに開始しない場合は、「**Data Protection for Microsoft Hyper-V 管理コンソールを今すぐ起動します (Launch Data Protection for Microsoft Hyper-V Management Console now)**」ボックスの選択を解除し、「完了」をクリックしてウィザードを終了します。

タスクの結果

Data Protection for Microsoft Hyper-V がインストールされました。

以下のインストール済みコンポーネントが、Windows オペレーティング・システムの「**プログラムと機能**」コントロール・パネルに表示されます。

- IBM Spectrum ProtectClient
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ライセンス
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V スイート
- IBM Spectrum Protect for Virtual Environments: フレームワーク
- IBM Spectrum Protect for Virtual Environments: Recovery agent
- IBM Spectrum Protect JVM
- IBM Spectrum Protect WebServer

次のタスク

バックアップ操作またはリストア操作を試行するか、ファイル・リストア・インターフェースを使用する場合は、事前にウィザードを使用した [Data Protection for Microsoft Hyper-V の構成](#) のタスクを実行してください。

Hyper-V 仮想マシン・ディスクのバックアップをマウントしてファイルのリストアを試行する前に、[51 ページの『IBM Spectrum Protect リカバリー・エージェント GUI の構成』](#)で説明されている作業を実行してください。

Data Protection for Microsoft Hyper-V 管理コンソール のみのインストール

Data Protection for Microsoft Hyper-V のリモート管理用に Data Protection for Microsoft Hyper-V 管理コンソールのみを Windows ホストにインストールすることができます。

始める前に

Data Protection for Microsoft Hyper-V 管理コンソールとの通信に使用する HTTPS ポートがファイアウォールで開いていることを確認します。別のポートを使用する場合を除き、デフォルト・ポートは 9081 です。詳細については、[14 ページの『必要な通信ポート』](#)を参照してください。

[22 ページの『インストール・パッケージのダウンロードおよび解凍』](#)の説明どおりに、インストール・パッケージをダウンロードして解凍していることを確認してください。

このタスクについて

このインストールには、Data Protection for Microsoft Hyper-V 管理コンソール、Data Protection for Microsoft Hyper-V PowerShell コマンドレット、および Data Protection for Microsoft Hyper-V ライセンス・ファイルのみが含まれます。

制約事項：Data Protection for Microsoft Hyper-V インストーラーは、Windows オペレーティング・システムで **diskpart** コマンドを使用して自動マウント機能を自動的に使用不可にします。このアクションは、IBM Spectrum Protect ファイル・リストア・インターフェースで正しいドライブ名割り当てを表示し、システムで予約済みのディスクを非表示にするのに必要です。

ファイル・リストア操作を実行する予定がない場合、または誤ったドライブ名割り当てやシステム予約ディスクがファイル・リストア・インターフェースに表示されることを気にしない場合、インストールの完了後に自動マウント機能を使用可能にすることができます。

手順

リモートで Data Protection for Microsoft Hyper-V を管理するために使用する Windows コンピューター上で、以下のステップを実行します。

1. 22 ページの『インストール・パッケージのダウンロードおよび解凍』
2. インストール・プログラムを開始するために、spinstall.exe ファイルをダブルクリックします。インストール・プロセスで使用する言語を選択し、「次へ」をクリックします。
3. 「**IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V** スイートの **InstallShield** ウィザードへようこそ (Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite)」ページで、「次へ」をクリックします。
4. 「ご使用条件」ページで、ご使用条件の条項を読みます。「使用条件の条項に同意します」をクリックし、「次へ」をクリックします。ご使用条件の条項に同意しない場合、インストールは終了し、「キャンセル」をクリックしてインストール・ウィザードを終了する必要があります。
5. 「インストール先フォルダー (Installation Destination Folder)」ページで、インストール場所をメモし、「次へ」をクリックします。

Data Protection for Microsoft Hyper-V は、デフォルトの場所 (C:\Program Files\IBM\SpectrumProtect) にのみインストールできます。以前に Data Protection for Microsoft Hyper-V をデフォルト以外の場所にインストールした場合、前バージョンからのプログラム・ファイルは、ログ・ファイルとトレース・ファイルを除き、アップグレード時にデフォルトのインストール場所に移動します。

6. 「インストール・タイプ」ページで、「**拡張インストール**」をクリックします。
7. 「**拡張インストール**」ページで、「**Data Protection for Microsoft Hyper-V 管理コンソールのみのインストール**」をクリックします。すぐにリストア・プロセスが始まります。インストール処理が開始された後、選択内容を変更することはできません。

ヒント: インストール・プロセスでは、必要なパッケージのインストールが完了するまでに数分かかる場合があります。

8. 「インストール・ウィザード完了 (Install Wizard Completed)」ページで、「完了」をクリックしてインストール・ウィザードを終了します。

ウィザードがクローズした直後に、Data Protection for Microsoft Hyper-V 管理コンソールが開始します。

構成ウィザードをすぐに開始しない場合は、「**Data Protection for Microsoft Hyper-V 管理コンソールを今すぐ起動します (Launch Data Protection for Microsoft Hyper-V Management Console now)**」ボックスの選択を解除し、「完了」をクリックしてウィザードを終了します。

タスクの結果

Data Protection for Microsoft Hyper-V 管理コンソール がインストールされました。

以下のインストール済みコンポーネントが、Windows オペレーティング・システムの「**プログラムと機能**」コントロール・パネルに表示されます。

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ライセンス
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V スイート

次のタスク

Data Protection for Microsoft Hyper-V 管理コンソール を構成するには、以下の手順を実行します。

1. 構成ウィザードが自動的に開かない場合は、Data Protection for Microsoft Hyper-V 管理コンソール を開始するために「**スタート**」 > 「**IBM Spectrum Protect**」 > 「**DP for Hyper-V 管理コンソール**」をクリックします。
2. 「**Data Protection for Hyper-V への接続**」ウィンドウで、管理するスタンドアロン・ホストまたはクラスター内のホストのホスト名と資格情報を入力します。

3.『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』のタスクを実行します。

Set-DpHvMmcLoginPreferences コマンドレットを使用して、ログオンする推奨ホストを指定することもできます。詳細については、139 ページの『第 8 章 Windows PowerShell コマンドレットを使用した仮想マシンの保護』を参照してください。

関連タスク

30 ページの『Windows Server Core システムへの Data Protection for Microsoft Hyper-V のインストールおよび構成』

Data Protection for Microsoft Hyper-V は、Server Core オプションを使用してインストールされた Windows Server オペレーティング・システムの Hyper-V ホストにインストールして構成できます。

Data Protection for Microsoft Hyper-V データ・ムーバーのみのインストール

仮想マシン (VM) のバックアップ操作とリストア操作、およびゲスト内アプリケーション保護のリストア操作に、Data Protection for Microsoft Hyper-V データ・ムーバーをインストールすることができます。このインストールでは、ファイル・リストア操作の Windows マウント・プロキシもインストールされます。

始める前に

- ファイアウォールで通信ポートが開いていることを確認します。開く必要があるポートのリストについては、14 ページの『必要な通信ポート』を参照してください。
- 22 ページの『インストール・パッケージのダウンロードおよび解凍』の説明どおりに、インストール・パッケージをダウンロードして解凍していることを確認してください。
- ゲスト内アプリケーションを保護するためにデータ・ムーバーをインストールする場合は、データ・ムーバーのインストール前に、以下のトピックの指示に従うようにしてください。
 - 91 ページの『Microsoft Exchange Server のアプリケーション保護のためのソフトウェアのインストールと構成』
 - 108 ページの『Microsoft SQL Server のアプリケーション保護のソフトウェアのインストールと構成』

このタスクについて

データ・ムーバーのインストールには、VM のバックアップ操作とリストア操作、およびゲスト内アプリケーション保護のリストア操作に使用されるデータ・ムーバーが含まれます。また、このインストールには、ファイル・リストア操作のマウント・プロキシも含まれます。さらに、このインストールにはリカバリー・エージェントも含まれます。

制約事項: Data Protection for Microsoft Hyper-V インストーラーは、Windows オペレーティング・システムで **diskpart** コマンドを使用して自動マウント機能を自動的に使用不可にします。このアクションは、IBM Spectrum Protect ファイル・リストア・インターフェースで正しいドライブ名割り当てを表示し、システムで予約済みのディスクを非表示にするのに必要です。

手順

アプリケーション・データをホストしている Windows マウント・プロキシ・マシンまたはゲスト VM で、以下のステップを実行します。

- 22 ページの『インストール・パッケージのダウンロードおよび解凍』
- インストール・プログラムを開始するために、spinstall.exe ファイルをダブルクリックします。インストール・プロセスで使用する言語を選択し、「次へ」をクリックします。
- 「IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V スイートの InstallShield ウィザードへようこそ (Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite)」ページで、「次へ」をクリックします。
- 「ご使用条件」ページで、ご使用条件の条項を読みます。「使用条件の条項に同意します」をクリックし、「次へ」をクリックします。ご使用条件の条項に同意しない場合、インストールは終了し、「キャンセル」をクリックしてインストール・ウィザードを終了する必要があります。

5. 「インストール先フォルダー (Installation Destination Folder)」 ページで、インストール場所をメモし、「次へ」をクリックします。

Data Protection for Microsoft Hyper-V は、デフォルトの場所 (C:\Program Files\IBM\SpectrumProtect) にのみインストールできます。以前に Data Protection for Microsoft Hyper-V をデフォルト以外の場所にインストールした場合、前バージョンからのプログラム・ファイルは、ログ・ファイルとトレース・ファイルを除き、アップグレード時にデフォルトのインストール場所に移動します。

6. 「インストール・タイプ」 ページで、「拡張インストール」をクリックします。
7. 「拡張インストール」 ページで、「データ・ムーバー機能またはマウント・プロキシのインストール (Install the data mover feature or mount proxy)」をクリックします。すぐにリストア・プロセスが始まります。インストール処理が開始された後、選択内容を変更することはできません。

ヒント: インストール・プロセスでは、必要なパッケージのインストールが完了するまでに数分かかる場合があります。

8. 「インストール・ウィザード完了 (Install Wizard Completed)」 ページで、「完了」をクリックしてインストール・ウィザードを終了します。

タスクの結果

Data Protection for Microsoft Hyper-V データ・ムーバーがインストールされました。

以下のインストール済みコンポーネントが、Windows オペレーティング・システムの「プログラムと機能」コントロール・パネルに表示されます。

- IBM Spectrum ProtectClient
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ライセンス
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V スイート
- IBM Spectrum Protect for Virtual Environments: フレームワーク
- IBM Spectrum Protect for Virtual Environments: Recovery agent
- IBM Spectrum Protect JVM
- IBM Spectrum Protect WebServer

次のタスク

アプリケーション保護のためのソフトウェアのインストールおよび構成について詳しくは、以下のいずれかのトピックを参照してください。

- [91 ページの『Microsoft Exchange Server のアプリケーション保護のためのソフトウェアのインストールと構成』](#)
- [108 ページの『Microsoft SQL Server のアプリケーション保護のソフトウェアのインストールと構成』](#)

Data Protection for Microsoft Hyper-V のアンインストール

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V 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。

始める前に

制約事項: IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V スイートのアンインストールの一環として IBM Spectrum Protect リカバリー・エージェント をアンインストールするか、Recovery Agent を別個にアンインストールすることができます。IBM Spectrum Protect リカバリー・エージェント をアンインストールする前に、すべての仮想ボリュームをアンマウントする必要があります。そうしないと、Recovery Agent を次回再インストールするときに、これらのマウント済み仮想ボリュームをアンマウントできません。

手順

1. 「コントロールパネル」を開き、「プログラムのアンインストール」をクリックします。
2. IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V スイートをアンインストールします。
 - a) 「プログラムのアンインストールまたは変更」ページで、「**IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V スイート**」を選択して、「アンインストール」をクリックします。
 - b) 「InstallShield ウィザード」の「プログラムの削除」ページで、「削除」をクリックします。
ヒント: アンインストール・プロセスは、完了するまでに数分間かかる場合があります。
 - c) アンインストールが完了したら、「**InstallShield ウィザード完了 (InstallShield Wizard Completed)**」ページで「終了」をクリックします。プログラムのリストを最新表示するには、「**最新表示**」アイコンをクリックします。
3. Data Protection for Microsoft Hyper-V ライセンスのアンインストール:
 - a) 「プログラムのアンインストールまたは変更」ページで、「**IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ライセンス (IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V License)**」を選択し、「アンインストール」をクリックします。
 - b) プロンプトが表示されたら、「はい」をクリックします。
4. IBM Spectrum Protect Web サーバーのアンインストール:
 - a) 「プログラムのアンインストールまたは変更」ページで、**IBM Spectrum Protect 「Web サーバー」**を選択し、「アンインストール」をクリックします。
 - b) プロンプトが表示されたら、「はい」をクリックします。
5. IBM Spectrum Protect Java 仮想マシン (JVM) のアンインストール:
 - a) 「プログラムのアンインストールまたは変更」ページで、「**IBM Spectrum Protect JVM**」を選択し、「アンインストール」をクリックします。
 - b) プロンプトが表示されたら、「はい」をクリックします。

次のタスク

ファイル・リストア機能は別に削除する必要があります。詳細については、[36 ページの『ファイル・リストア機能の削除』](#)を参照してください。

サイレント・モードでの Data Protection for Microsoft Hyper-V のインストール

すべての Data Protection for Microsoft Hyper-V およびデータ・ムーバー機能を、単一のシステムにサイレント・インストールできます。データ・ムーバーのみ、または Data Protection for Microsoft Hyper-V 管理コンソールのみをサイレント・モードでインストールするという選択もできます。

始める前に

[22 ページの『インストール・パッケージのダウンロードおよび解凍』](#)の説明どおりに、インストール・パッケージをダウンロードして解凍していることを確認してください。

このタスクについて

制約事項: すべての機能がデフォルトの場所にインストールされます。Data Protection for Microsoft Hyper-V およびデータ・ムーバー機能をデフォルト以外の場所にサイレント・インストールすることはできません。

手順

1. 管理者としてコマンド・プロンプトを開き、次のコマンドを入力します。

```
cd extract_folder\TSMHYPERV_WIN
```

2. 以下のいずれかの方法を使用して、サイレント・モードで Data Protection for Microsoft Hyper-V をインストールします。

- すべての Data Protection for Microsoft Hyper-V およびデータ・ムーバー機能をサイレント・インストールするには、次のコマンドを入力します。

```
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。

```
The Virtual Volume Driver is not yet registered. Recovery Agent can register the driver now. During registration, a Microsoft Windows Logo warning may be displayed. Accept this warning to allow the registration to complete. Do you want to register the Virtual Volume Driver now?
```

IBM Spectrum Protect リカバリー・エージェント 操作を続行するには、**Yes** と入力して仮想ボリューム・ドライバーを登録します。

- データ・ムーバーのみをサイレント・モードでインストールするには、次のコマンドを入力します。

```
spinstall.exe /silent  
ISFeatureInstall=Client,Java,WebServer,Framework,HyperV,RecoveryAgent  
ComponentsToInstallRA="LAP,mount,shell"
```

- Data Protection for Microsoft Hyper-V 管理コンソールのみをサイレント・モードでインストールするには、次のコマンドを入力します。

```
spinstall.exe /silent ISFeatureInstall=HyperV
```

サイレント・モードでの Data Protection for Microsoft Hyper-V 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 Microsoft Hyper-V 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

最初に Suite インストーラーを使用して Data Protection for Microsoft Hyper-V をアンインストールしてから、Windows PowerShell コマンドレットを実行して、以下のコンポーネントを削除する必要があります。

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ライセンス
- IBM Spectrum Protect WebServer
- IBM Spectrum Protect Java 仮想マシン (JVM)

ヒント：インストール済みの Data Protection for Microsoft Hyper-V コンポーネントのリストを表示するには、PowerShell コマンド・プロンプトから管理者として次のコマンドを発行します。

```
Get-WmiObject -class Win32_Product | Where-Object name -match `"  
"IBM Spectrum Protect*" | Format-List Version,InstallDate,Name,InstallLocation
```

以下の手順を使用して、Windows Server Core システムから Data Protection for Microsoft Hyper-V をアンインストールすることもできます。

ヒント：PowerShell コマンドを発行するには、管理モードで PowerShell コマンド・プロンプトを実行する必要があります。

手順

- インスタント・アクセス操作を実行した場合は、作成されたすべてのインスタント・アクセス仮想マシンを除去します。

手順については、[137 ページの『Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス VM の除去』](#)を参照してください。

- 実行中のすべての IBM Spectrum Protect サービスを停止します。通常、サービスの名前は TSM で始まります。

例えば、PowerShell コマンド・プロンプトから次のコマンドを実行することができます。

```
stop-service TSM*
```

3. コマンド・プロンプトから次のコマンドを発行します。

```
cd extract_folder¥TSMHYPERV_WIN
```

ここで `extract_folder` は、Data Protection for Microsoft Hyper-V インストールを解凍したフォルダーです。

4. Suite インストーラーを使用して Data Protection for Microsoft Hyper-V をアンインストールするには、PowerShell コマンド・プロンプトから次のコマンドを発行します。

```
Start-Process -FilePath ".¥spinstall.exe" -ArgumentList "/silent /remove" -wait
```

5. 残りのコンポーネントを除去するには、PowerShell コマンド・プロンプトから次のコマンドレットを実行します。あるいは、次のコマンドレットをスクリプトに組み込んで自動化してください。

```
$ve = "IBM Spectrum Protect for Virtual Environments:"
$lic = "$ve Data Protection for Microsoft Hyper-V License"
$ws = "IBM Spectrum Protect WebServer"
$jvm = "IBM Spectrum Protect JVM"

Get-WmiObject -class Win32_Product -Filter "Name='$lic'" | Invoke-WmiMethod `
-Name "Uninstall" | Select-Object ReturnValue
Get-WmiObject -class Win32_Product -Filter "Name='$ws'" | Invoke-WmiMethod `
-Name "Uninstall" | Select-Object ReturnValue
Get-WmiObject -class Win32_Product -Filter "Name='$jvm'" | Invoke-WmiMethod `
-Name "Uninstall" | Select-Object ReturnValue
```

タスクの結果

アンインストール操作の完了後に構成情報を保存する場合、構成ファイルとプロパティ・ファイルは以下のフォルダーにあります。

- C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥tsmVmGUI
- C:¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥frGUI
- C:¥Program Files¥IBM¥SpectrumProtect¥DPHyperV
- C:¥Program Files¥Tivoli¥TSM¥baclient

関連タスク

28 ページの『サイレント・モードでの Data Protection for Microsoft Hyper-V のインストール』

すべての Data Protection for Microsoft Hyper-V およびデータ・ムーバー機能を、単一のシステムにサイレント・インストールできます。データ・ムーバーのみ、または Data Protection for Microsoft Hyper-V 管理コンソールのみをサイレント・モードでインストールするという選択もできます。

Windows Server Core システムへの Data Protection for Microsoft Hyper-V のインストールおよび構成

Data Protection for Microsoft Hyper-V は、Server Core オプションを使用してインストールされた Windows Server オペレーティング・システムの Hyper-V ホストにインストールして構成できます。

始める前に

Data Protection for Microsoft Hyper-V がインストールされている各ホストでは、Data Protection for Microsoft Hyper-V と通信するために使用される HTTPS ポートが、ファイアウォールで開いていることを確認してください。特に他のポートを指定しない限り、デフォルトのポート番号 9081 が使用されます。

このタスクについて

Server Core ではローカル・ユーザー・インターフェースがサポートされていないため、スタンドアロン・ホストまたはクラスター内の各ホストに Data Protection for Microsoft Hyper-V をサイレント・インストールする必要があります。

Data Protection for Microsoft Hyper-V の管理は、別のデプロイメントの Data Protection for Microsoft Hyper-V 管理コンソール を使用し、それをスタンドアロン・ホストまたはクラスター内のホストにポイントすることにより行う必要があります。

手順

1. スタンドアロン・ホスト上またはクラスター内のすべてのホスト上で、Data Protection for Microsoft Hyper-V のサイレント・インストールを実行します。
手順については、[28 ページの『サイレント・モードでの Data Protection for Microsoft Hyper-V のインストール』](#)を参照してください。
2. Data Protection for Microsoft Hyper-V をリモート側で管理するには、Data Protection for Microsoft Hyper-V 管理コンソール を別の Windows Server または Windows 10 のオペレーティング・システムに別個にインストールする必要があります。
手順については、[24 ページの『Data Protection for Microsoft Hyper-V 管理コンソール のみのインストール』](#)を参照してください。
3. 構成ウィザードが自動的に開かない場合は、Data Protection for Microsoft Hyper-V 管理コンソール を開始するために「スタート」>「**IBM Spectrum Protect**」>「**DP for Hyper-V 管理コンソール**」をクリックします。
4. 「**Data Protection for Hyper-V への接続**」ウィンドウで、管理するスタンドアロン・ホストまたはクラスター内のホストのホスト名と資格情報を入力します。
5. [ウィザードを使用して Data Protection for Microsoft Hyper-V を構成します。](#)

タスクの結果

Data Protection for Microsoft Hyper-V 管理コンソール を使用して、Server Core オプションを使用してインストールしたオペレーティング・システムのスタンドアロン・ホストまたはクラスター内のホストの Data Protection for Microsoft Hyper-V の日次操作をリモート側から管理できます。

次のタスク

Set-DpHvMmcLoginPreferences コマンドレットを使用して、ログオンする推奨ホストを指定することもできます。詳細については、[139 ページの『第 8 章 Windows PowerShell コマンドレットを使用した仮想マシンの保護』](#)を参照してください。

関連概念

[63 ページの『Data Protection for Microsoft Hyper-V 管理コンソールを使用したデータの管理』](#)
Data Protection for Microsoft Hyper-V 管理コンソールは、Data Protection for Microsoft Hyper-V の日常の動作の管理に役立つ単一の環境を提供します。

関連タスク

[59 ページの『Data Protection for Microsoft Hyper-V 操作のデフォルト以外のポート番号の構成』](#)
Data Protection for Microsoft Hyper-V Web サーバーまたは REST API サービスで、デフォルトのポート番号を使用しない場合は、Windows PowerShell コマンドレットを使用して、異なるポート番号を構成できます。

Windows Server Core システムからの Data Protection for Microsoft Hyper-V のアンインストール

サイレント・モードを使用して、Windows Server Core システムから Data Protection for Microsoft Hyper-V をアンインストールできます。

手順については、[29 ページの『サイレント・モードでの Data Protection for Microsoft Hyper-V のアンインストール』](#)を参照してください。

関連タスク

[30 ページの『Windows Server Core システムへの Data Protection for Microsoft Hyper-V のインストールおよび構成』](#)

Data Protection for Microsoft Hyper-V は、Server Core オプションを使用してインストールされた Windows Server オペレーティング・システムの Hyper-V ホストにインストールして構成できます。

Linux マウント・プロキシ機能のインストール

ファイル・リストア操作で使用するために Linux のゲスト仮想マシン (VM) にマウント・プロキシをインストールするための指示に従ってください。

古いバージョンからの Linux マウント・プロキシ機能のアップグレード

マウント・プロキシ機能が既に Linux 仮想マシンにインストールされている場合、Data Protection for Microsoft Hyper-V バージョン 8.1.10 の Linux マウント・プロキシにアップグレードすることができます。

始める前に

アップグレードする Linux マウント・プロキシのバージョンが Windows マウント・プロキシのバージョンと同じであることを確認してください。例えば、Windows マウント・プロキシが V8.1.10 である場合、Linux マウント・プロキシも V8.1.10 でなければなりません。

V8.1.4 の Linux マウント・プロキシからアップグレードする場合、最初に Linux マウント・プロキシをアンインストールする必要があります。次のコマンドを発行して、V8.1.4 の Linux マウント・プロキシをアンインストールすることができます。

```
rpm -e TIVsm-BACit.x86_64 TIVsm-BA.x86_64
rpm -e TIVsm-APIcit.x86_64 TIVsm-API64.x86_64
rpm -e gskcrypt64.linux.x86_64.rpm gskssl64.linux.x86_64
```

V8.1.6 からアップグレードする場合、Linux マウント・プロキシをアンインストールする必要はありません。

手順

- V8.1.10 の Linux データ・ムーバー・パッケージをインストールすることで、マウント・プロキシ機能を直接アップグレードします。

手順については、以下のトピックを参照してください。

- [32 ページの『Linux システムへのマウント・プロキシ機能のインストール』](#)
- [34 ページの『サイレント・モードでの Linux マウント・プロキシ機能のインストール』](#)

次のタスク

Hyper-V ホスト上で Data Protection for Microsoft Hyper-V 管理コンソール から構成ウィザードを再起動したり、/etc/adsm ディレクトリー内の暗号化されたパスワード・ファイルを削除したりしない限り、アップグレード後に Linux マウント・プロキシ・パスワードをリセットする必要はありません。

また、アップグレード後に Linux システムを再始動する必要もありません。単純に、**kill -9** コマンドを発行して既存のアクティブな **dsmcad** プロセスを停止します。その後、**dsmcad** プロセスを再開して、V8.1.10 のクライアント・アクセプターを開始します。

Linux システムへのマウント・プロキシ機能のインストール

Linux ゲスト仮想マシン (VM) でファイル・リストア操作を実行する計画の場合は、Linux Data Protection for Microsoft Hyper-V データ・ムーバー・パッケージを使用して Linux システムにマウント・プロキシ機能をインストールする必要があります。

始める前に

古いバージョンの Linux マウント・プロキシからアップグレードする場合は、[32 ページの『古いバージョンからの Linux マウント・プロキシ機能のアップグレード』](#) の情報を確認してください。

このタスクについて

ファイル・リストア・インターフェースのマウント操作には、マウント・プロキシ・ノードが必要です。マウント・プロキシ・ノードにより、VM バックアップのマウントされた VM ディスク上のファイル・システムが、ファイル・リストア操作のマウント・ポイントとしてアクセス可能になります。

Linux マウント・プロキシ・ソフトウェアは、Linux データ・ムーバー・パッケージに含まれています。標準の Windows Data Protection for Microsoft Hyper-V インストール・パッケージには含まれていません。Linux パッケージを個別にダウンロードしてインストールする必要があります。

手順

root ユーザーとして以下のステップを実行して、マウント・プロキシ機能をインストールします。

1. インストール・パッケージをダウンロードして解凍します。
 - a) 以下のいずれかの Web サイトから、Linux Data Protection for Microsoft Hyper-V データ・ムーバー・インストール・パッケージをダウンロードします。

- [パスポート・アドバンテージ](#)
- [Fix Central](#)

通常、ダウンロード・パッケージの名前は 8.x.x.x-TSM4HYPERV.tar.gz です。例えば、バージョン 8.1.10 の場合、パッケージの名前は 8.1.10.0-TSM4HYPERV.tar.gz です。

ヒント: 最新の情報、更新、および保守フィックスについては、[IBM サポート・ポータル](#)にアクセスしてください。

- b) Linux データ・ムーバー・パッケージを、インストール・ファイルを保管するロケーションにコピーします。
例えば、次のディレクトリを作成し、インストール・パッケージをそのディレクトリにコピーします。

```
/extract_folder
```

- c) インストール・パッケージ・ディレクトリに移動します。例えば、次のとおりです。

```
cd /extract_folder
```

- d) 次のコマンドを発行して、インストール・パッケージからインストール・ファイルを解凍します。

```
tar -xvzf 8.1.10.0-TSM4HYPERV.tar.gz
```

インストール・ファイルは、CD ディレクトリに解凍されます。例えば、インストール・ファイルは次のディレクトリに保存されます。

```
/extract_folder/CD
```

2. インストール・ファイルが含まれているディレクトリに移動します。例えば、次のコマンドを発行します。

```
cd /extract_folder/CD/Linux/DataProtectionForHyperV
```

3. 次のコマンドを発行して、Data Protection for Microsoft Hyper-V インストール・ウィザードを開始します。

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

4. インストール・プロセスで使用する言語を選択し、「OK」をクリックします。
5. 以下のように、インストール・ウィザードの各ページを完了します。

ページ	アクション
ようこそ	「次へ」をクリックします。

ページ	アクション
ソフトウェアのご使用条件	ソフトウェア・ライセンスのご使用条件に同意して、「次へ」をクリックします。
インストール・ディレクトリーの検出	インストール・ディレクトリー (/opt/tivoli/tsm/) を確認し、「次へ」をクリックします。
カスタム	「 Data Protection for Hyper-V データ・ムーバー (Data Protection for Hyper-V Data Mover) 」がチェックされていることを確認し、「次へ」をクリックします。
プリインストールの要約	インストールの要約を確認します。インストールを続行するには、「インストール」をクリックします。
作業を進める前に、この情報を確認しておいてください	「次へ」をクリックします。
インストールの完了	「完了 (Done)」をクリックします。

タスクの結果

ヒント: インストール・ウィザードを実行しない場合は、以下の方法を使用して、マウント・プロキシ機能をインストールすることができます。

- コンソールからインストールするには、コマンド `./install-Linux.bin -i console` を発行します。
- サイレント・モードでインストールするには、[34 ページの『サイレント・モードでの Linux マウント・プロキシ機能のインストール』](#)を参照してください。

次のタスク

ファイル・リストア操作のために Linux マウント・プロキシを構成します。手順については、[45 ページの『ファイル・リストア操作のための Linux マウント・プロキシの構成』](#)を参照してください。

関連タスク

[36 ページの『Linux システムへのマウント・プロキシ機能のアンインストール』](#)

Linux ゲスト仮想マシン (VM) 上でファイル・リストア操作を実行する必要がなくなった場合は、Linux マウント・プロキシ・システム上のマウント・プロキシ機能を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 マウント・プロキシ機能のインストール

Linux ゲスト仮想マシン (VM) でファイル・リストア操作を実行する計画の場合は、Linux Data Protection for Microsoft Hyper-V データ・ムーバー・パッケージを使用して Linux システムにマウント・プロキシ機能をインストールする必要があります。マウント・プロキシ機能を対話式でインストールしない場合は、サイレント・モードでインストールすることができます。

始める前に

古いバージョンの Linux マウント・プロキシからアップグレードする場合は、[32 ページの『古いバージョンからの Linux マウント・プロキシ機能のアップグレード』](#)の情報を確認してください。

このタスクについて

ファイル・リストア・インターフェースのマウント操作には、マウント・プロキシ・ノードが必要です。マウント・プロキシ・ノードにより、VM バックアップのマウントされた VM ディスク上のファイル・システムが、ファイル・リストア操作のマウント・ポイントとしてアクセス可能になります。

Linux マウント・プロキシ・ソフトウェアは、Linux データ・ムーバー・パッケージに含まれています。標準の Windows Data Protection for Microsoft Hyper-V インストール・パッケージには含まれていません。Linux パッケージを個別にダウンロードしてインストールする必要があります。

手順

root ユーザーとして、Linux ゲスト VM で以下のステップを実行します。

1. インストール・パッケージをダウンロードして解凍します。

- a) 以下のいずれかの Web サイトから、Linux Data Protection for Microsoft Hyper-V データ・ムーバー・インストール・パッケージをダウンロードします。

- [パスポート・アドバンテージ](#)
- [Fix Central](#)

通常、ダウンロード・パッケージの名前は 8.x.x.x-TSM4HYPERV.tar.gz です。例えば、バージョン 8.1.10 の場合、パッケージの名前は 8.1.10.0-TSM4HYPERV.tar.gz です。

ヒント: 最新の情報、更新、および保守フィックスについては、[IBM サポート・ポータル](#)にアクセスしてください。

- b) Linux データ・ムーバー・パッケージを、インストール・ファイルを保管するロケーションにコピーします。

例えば、次のディレクトリーを作成し、インストール・パッケージをそのディレクトリーにコピーします。

```
/extract_folder
```

- c) インストール・パッケージ・ディレクトリーに移動します。例えば、次のとおりです。

```
cd /extract_folder
```

- d) 次のコマンドを発行して、インストール・パッケージからインストール・ファイルを解凍します。

```
tar -xvzf 8.1.10.0-TSM4HYPERV.tar.gz
```

インストール・ファイルは、CD ディレクトリーに解凍されます。例えば、インストール・ファイルは次のディレクトリーに保存されます。

```
/extract_folder/CD
```

2. インストール・ファイルが含まれているディレクトリーに移動します。例えば、次のコマンドを発行します。

```
cd /extract_folder/CD/Linux/DataProtectionForHyperV
```

3. 次のコマンドを発行してサイレント・モードでインストールを開始し、Data Protection for Microsoft Hyper-V の使用許諾条件を受け入れます。

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

次のタスク

ファイル・リストア操作のために Linux マウント・プロキシーを構成します。手順については、[45 ページの『ファイル・リストア操作のための Linux マウント・プロキシーの構成』](#)を参照してください。

関連タスク

[32 ページの『Linux システムへのマウント・プロキシー機能のインストール』](#)

Linux ゲスト仮想マシン (VM) でファイル・リストア操作を実行する計画の場合は、Linux Data Protection for Microsoft Hyper-V データ・ムーバー・パッケージを使用して Linux システムにマウント・プロキシー機能をインストールする必要があります。

Linux システムへのマウント・プロキシ機能のアンインストール

Linux ゲスト仮想マシン (VM) 上でファイル・リストア操作を実行する必要がなくなった場合は、Linux マウント・プロキシ・システム上のマウント・プロキシ機能をアンインストールすることができます。

始める前に

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。

このタスクについて

デフォルトでは、Linux マウント・プロキシ機能のアンインストール時に行われる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。

手順

Linux マウント・プロキシ機能を除去するには、以下のステップを実行します。

1. アンインストール・プログラムが含まれているディレクトリに移動します。
例えば、次のコマンドを発行して、アンインストール・プログラムのデフォルト・ロケーションに移動します。

```
/opt/tivoli/tsm/_uninst/DPHyperV
```

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 Linux マウント・プロキシをアンインストールします。
 - インストール・ウィザードを使用して Linux マウント・プロキシをアンインストールするには、次のコマンドを発行します。

```
./Uninstall_Data_Protection_for_Hyper-V -i swing
```

- コンソールを使用して Linux マウント・プロキシをアンインストールするには、次のコマンドを発行します。

```
./Uninstall_Data_Protection_for_Hyper-V -i console
```

- Linux マウント・プロキシをサイレント・アンインストールするには、次のコマンドを発行します。

```
./Uninstall_Data_Protection_for_Hyper-V -i silent
```

関連タスク

36 ページの『ファイル・リストア機能の削除』

ファイル・リストア操作を実行する必要がなくなった場合、構成ファイルを更新してファイル・リストア機能を削除することができます。Data Protection for Microsoft Hyper-V をアンインストールする場合、ファイル・リストア機能を削除するために同じ構成ファイルを更新する必要があります。

ファイル・リストア機能の削除

ファイル・リストア操作を実行する必要がなくなった場合、構成ファイルを更新してファイル・リストア機能を削除することができます。Data Protection for Microsoft Hyper-V をアンインストールする場合、ファイル・リストア機能を削除するために同じ構成ファイルを更新する必要があります。

このタスクについて

ファイル・リストア機能と関連するサービスを削除するには、**frConfig.props** ファイルを更新して、マウント・プロキシ・ノードと関連するサービスを削除します。

手順

Hyper-V ホストまたはクラスターで、以下の手順を実行します。

1. 以下のオプションを変更して、`C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\frConfig.props` ファイルを手動で編集します。

```
enable_filerestore=true
```

オプションを以下のように変更します。

```
enable_filerestore=false
```

2. Windows オペレーティング・システムの「サービス」コントロール・パネルを開き、マウント・プロキシ・ノードに関連するサービスを削除します。
通常、それらのサービスは、TSM CAD - *hostname_HV_MP_platform* および TSM Agent - *hostname_HV_MP_platform* という名前です。
3. `REMOVE NODE` コマンドを使用して、IBM Spectrum Protect サーバーのマウント・プロキシ・ノードを削除します。

タスクの結果

ファイル・リストア機能が、Hyper-V ホストまたはクラスターから除去されます。IBM Spectrum Protect for Virtual Environments Derby Database サービスも IBM Spectrum Protect Web Server サービスも再始動する必要はありません。

次のタスク

Linux ゲスト仮想マシン上でファイル・リストア操作を実行した場合は、Linux マウント・プロキシ機能をアンインストールする必要があります。手順については、[36 ページの『Linux システムへのマウント・プロキシ機能のアンインストール』](#)を参照してください。

第 3 章 Data Protection for Microsoft Hyper-V の構成

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ソフトウェアを正
常にインストールした後、バックアップ操作およびリストア操作を実行する前に Data Protection for
Microsoft Hyper-V を構成する必要があります。IBM Spectrum Protect リカバリー・エージェント を使用し
てゲスト VM でマウント操作を実行する場合は、Recovery Agent も構成する必要があります。

ヒント : Data Protection for Microsoft Hyper-V 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。その後は、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。

ウィザードを使用した Data Protection for Microsoft Hyper-V の構成

構成ウィザードを使用して、スタンドアロン Hyper-V ホスト環境またはクラスター環境に対して Data
Protection for Microsoft Hyper-V の初期構成を行ったり、構成を更新したりすることができます。このウィ
ザードを使用すると、Data Protection for Microsoft Hyper-V のファイル・リストア操作を有効にすること
もできます。

始める前に

- Data Protection for Microsoft Hyper-V バージョン 8.1.2 以前からアップグレードするときに、IBM Spectrum Protect サーバーですでに定義されているノードがある場合、[16 ページの『IBM Spectrum Protect サーバー上のノードの名前変更』](#)のタスクを実行します。
- Data Protection for Microsoft Hyper-V がインストールされている Hyper-V ホストには、仮想マシン (VM) バックアップの保管に使用される IBM Spectrum Protect サーバーとのネットワーク接続が必要です。
- パフォーマンスの向上を図るために、Hyper-V ホストと IBM Spectrum Protect サーバー間に少なくとも 10 Gb の接続を使用してください。
- IBM Spectrum Protect サーバー管理者アカウントのログイン資格情報が必要です。
- Secure Sockets Layer (SSL) 通信を使用するセキュア IBM Spectrum Protect サーバーに接続する必要があります。構成ウィザードを実行中に、セキュリティ証明書が自動的にダウンロードされます。
- クラスター環境では、クラスター内の各ホストに Data Protection for Microsoft Hyper-V パッケージを確実にインストールしてください。すべてのホストにパッケージをインストールした後、クラスター内のいずれかのホストでインストール・ウィザードを実行します。構成ウィザードは、構成を完了するために各ホストに接続します。

Data Protection for Microsoft Hyper-V ソフトウェアがインストールされていないノードは、クラスター構成から省略され、このソフトウェアがインストールされているその他のノードの構成に影響を与えません。後でノードをクラスターに追加する場合は、そのノードに Data Protection for Microsoft Hyper-V をインストールし、(ローカル側で、またはクラスター内の他のノードから) そのノードに対して構成ウィザードを実行します。

- Data Protection for Microsoft Hyper-V がインストールされている各ホストでは、Data Protection for Microsoft Hyper-V と通信するために使用される HTTPS ポートが、ファイアウォールで開いていることを確認してください。特に他のポートを指定しない限り、デフォルトのポート番号 9081 が使用されます。
- 構成ウィザードにより、ホスト名またはクラスター名に基づいて使用するノード名が決まります。デフォルトのノード名を使用することも、接頭部および接尾部を追加してノード名をカスタマイズすることもできます。ノード名をカスタマイズする場合は、構成ウィザードを実行する前に、[18 ページの『ノード名のカスタマイズ』](#)で説明されているステップを実行する必要があります。

このタスクについて

構成を簡素化するために、構成ウィザードは、バックアップ操作、リストア操作、およびオプションのファイル・リストア操作に必要なノードを自動的に作成します。また、構成ウィザードは、IBM Spectrum Protect サーバー上のノードを登録し、ローカル Windows ホストでサービスを構成します。

Data Protection for Microsoft Hyper-V に使用されるノードのタイプについては、6 ページの『[Data Protection for Microsoft Hyper-V での IBM Spectrum Protect ノードの使用方法](#)』を参照してください。

手順

Data Protection for Microsoft Hyper-V を構成するには、Hyper-V ホスト上で以下のステップを実行します。クラスター環境の場合、Data Protection for Microsoft Hyper-V がインストールされているクラスター内の任意のホストで以下のステップを実行します。

1. 「スタート」 > 「**IBM Spectrum Protect**」 > 「**DP for Hyper-V 管理コンソール**」をクリックして、Data Protection for Microsoft Hyper-V 管理コンソールを開始します。

あるいは、コマンド・プロンプトで以下のコマンドを発行します。

```
"C:\Program Files\IBM\SpectrumProtect\DPHyperV\DpHv.msc"
```

2. プロンプトが出されたら、Data Protection for Microsoft Hyper-V 管理コンソール にログオンします。Hyper-V ホストへのログオンに使用する場合と同じ資格情報を入力します。

Hyper-V およびクラスターの操作をすべて行うには、使用するアカウントは、マシンのローカル管理者グループのメンバーである必要があります。

3. Data Protection for Microsoft Hyper-V 管理コンソールを初めて構成する場合、構成ウィザードが自動的に開きます。

スタンドアロン・ホスト環境で既存の構成を変更する場合は、「ナビゲーション」ペインでホストをクリックし、「アクション」ペインで「**構成**」をクリックします。クラスター環境では、ナビゲーション・ペインでクラスター・ノードをクリックして選択し、「**構成**」をクリックします。

4. ウィザードの各ページの指示に従い、「次へ」をクリックして次のページに進みます。

ページ	アクション
始める前に	「次へ」をクリックして、ウィザードを開始します。
バックアップ・サーバー	<p>VM バックアップの保管に使用される IBM Spectrum Protect サーバーに関する情報を入力します。</p> <p>バックアップ・サーバー・アドレス IBM Spectrum Protect サーバーのホスト名または IP アドレス。</p> <p>バックアップ・サーバーの SSL ポート TLS 1.2 を有効にした SSL プロトコルを使用して、管理接続を可能にするサーバー・ポートのポート番号を指定します。デフォルトのポート番号が表示されます。ご使用のサーバーが別のポートを使用するように構成されている場合を除いて、デフォルトのポート番号を受け入れます。</p> <p>管理資格情報 IBM Spectrum Protect サーバー管理者のユーザー名とパスワード。管理者にはシステム特権が必要であり、サーバー上のクライアント・ノードを登録できなければなりません。</p>
証明書の受け入れ	<p>このウィンドウが表示されるのは、初めて IBM Spectrum Protect サーバーに接続しようとする場合、または既存のセキュリティー証明書が無効になった場合のみです。「受け入れる」をクリックして、証明書を自動的にダウンロードしてインポートします。</p> <p>V8.1.1 以前の V8 サーバー、または V7.1.7 以前のサーバーに接続するときに、ダウンロード処理が失敗した場合は、43 ページの『IBM Spectrum Protect サーバ</p>

ページ	アクション
	<p>ー V8.1.1 以前または V7.1.7 以前に接続するためのセキュリティ設定の構成』を参照してください。</p>
クラスターおよび ホスト構成	<p>使用可能なオプションは次のとおりです。</p> <p>ポリシー・ドメイン リストからポリシー・ドメインを選択します。ポリシー・ドメインには、VM バックアップが IBM Spectrum Protect サーバーで保持される期間および保持される VM バックアップのバージョン数を決定するルールが含まれています。デフォルトのポリシー・ドメインは STANDARD です。</p> <p>ターゲット・ノード名 VM バックアップが IBM Spectrum Protect サーバー上で保管されているノード名を表示します。クラスターの場合、クラスター内のどのノードがバックアップを実行しているかに関係なく、すべての VM バックアップがターゲット・ノードの下に保管されます。</p> <p>ノード定義 スタンドアロン・ホストまたはクラスター内の複数ホストのノード定義を表示します。ノードのタイプについては、7 ページの表 1 を参照してください。</p> <p>ファイル・リストアの有効化 ファイル・リストア Web インターフェースを使用して VM バックアップから個々のファイルをリストアする場合、このボックスにチェック・マークを付けます。このチェック・ボックスを選択すると、各ホストのマウント・プロキシ・ノード・ペアが自動的にリストに追加されます。</p> <p>このノード・ペアは、マウントされた VM ディスクに iSCSI 接続経由でアクセスする Linux および Windows のプロキシ・システムを表します。これらのノードにより、マウントされた VM ディスク上のファイル・システムが、ファイル・リストア操作のマウント・ポイントとしてアクセス可能になります。</p> <p>初期構成時に、「ファイル・リストアの有効化」にデフォルトでチェックが入ります。</p> <p>ファイル・リストア設定 このボタンをクリックしてファイル・リストア管理者の資格情報を入力します。</p>
ファイル・リストア設定	<p>このウィンドウは、ファイル・リストア機能を有効にしている場合のみ表示されます。ファイル・リストア管理者の資格情報を入力します。アカウントは、すべての VM でローカル管理権限を持つ Windows ドメイン・ユーザー・アカウントでなければなりません。</p>
要約	<p>設定を確認して、「次へ」をクリックし、構成を完了します。</p>
結果	<p>構成の結果が表示されます。構成が正常に完了しなかった場合、エラーのリストが表示されます。エラーを修正し、構成を再実行してください。</p> <p>ファイル・リストア機能が正常に構成された場合、ホスト、Linux マウント・プロキシ、およびファイル・リストア URL に関する情報が、ファイル・リストア結果表に表示されます。「コピー」をクリックすると、すべての情報がクリップボードにコピーされます。</p> <p>44 ページの『環境でファイル・リストア操作を使用可能にする』の説明に従って、ファイル・リストア構成を完了する必要があります。</p>

タスクの結果

ウィザードが正常に完了すると、コマンド・プロンプト、PowerShell コマンドレット、または Data Protection for Microsoft Hyper-V 管理コンソールを使用してバックアップおよびリストア操作を実行できます。

ユーザーの便宜のために、「アクション」ペインの「ファイル・リストア」をクリックして、ファイル・リストア・インターフェースを開くこともできます。

次のタスク

Data Protection for Microsoft Hyper-V 管理コンソールまたは **Test-DpHvConfiguration** PowerShell コマンドレットを実行して、構成を検証することができます。詳しくは、以下を参照してください。

- 74 ページの『Data Protection for Microsoft Hyper-V の構成の検証』
- 145 ページの『Data Protection for Microsoft Hyper-V コマンドレットの例』

Set-DpHvMmcLoginPreferences コマンドレットを使用して、ログオンする推奨ホストを指定することもできます。詳細については、139 ページの『第 8 章 Windows PowerShell コマンドレットを使用した仮想マシンの保護』を参照してください。

ファイル・リストア機能を有効にして Data Protection for Microsoft Hyper-V を構成し、初期構成の後に構成ウィザードを再実行した場合、Linux マウント・プロキシ・ノードのパスワードをリセットする必要があります。パスワードをリセットするには、以下のいずれかの方法を使用します。

方法 1

Linux マウント・プロキシで、IBM Spectrum Protect 管理者が **dsmc** コマンドを実行し、プロンプトが表示されたら IBM Spectrum Protect 管理者ユーザー ID およびパスワードを入力します。

方法 2

次の手順を実行します。

1. IBM Spectrum Protect 管理者が、IBM Spectrum Protect サーバー・コンソール上で UPDATE NODE サーバー・コマンドを実行して、Linux マウント・プロキシ・ノードのパスワードをリセットします。
2. Linux マウント・プロキシ・ノードの所有者は、Linux マウント・プロキシ上で **dsmc** コマンドを実行します。プロンプトが出されたら、所有者はデフォルトの Linux マウント・プロキシ・ノード ID と新規 Linux マウント・プロキシ・ノード・パスワード (IBM Spectrum Protect サーバー管理者から取得) を入力します。

関連タスク

59 ページの『Data Protection for Microsoft Hyper-V 操作のデフォルト以外のポート番号の構成』

Data Protection for Microsoft Hyper-V Web サーバーまたは REST API サービスで、デフォルトのポート番号を使用しない場合は、Windows PowerShell コマンドレットを使用して、異なるポート番号を構成できます。

Data Protection for Microsoft Hyper-V のセキュリティ設定の構成

IBM Spectrum Protect サーバーに安全に接続するのに必要な設定は、接続先のサーバー・バージョンによって異なります。

このタスクについて

IBM Spectrum Protect バージョン 8.1.2 以降および V7.1.8 のサーバーは、Transport Layer Security (TLS) 1.2 を使用してサーバーとクライアント間のすべての通信を暗号化する、強化されたセキュリティ・プロトコルを提供します。Data Protection for Microsoft Hyper-V とサーバーは、Secure Sockets Layer (SSL) プロトコルを使用して相互に通信するように自動的に構成されます。証明書は自動的に配布されます。

構成ウィザードを使用して Data Protection for Microsoft Hyper-V を構成する場合、セキュリティ証明書を受け入れるように求めるプロンプトが出されます。証明書を取得し、インポートするための手動のステ

ップは不要です。詳しくは、[39 ページの『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』](#)を参照してください。

旧バージョンの IBM Spectrum Protect サーバーに接続するときに、証明書の自動ダウンロード・プロセスが失敗する場合、セキュリティ証明書を手動でダウンロードし、インポートしてから、構成ウィザードを実行する必要があります。詳細については、[43 ページの『IBM Spectrum Protect サーバー V8.1.1 以前または V7.1.7 以前に接続するためのセキュリティ設定の構成』](#)を参照してください。

IBM Spectrum Protect サーバー V8.1.1 以前または V7.1.7 以前に接続するためのセキュリティ設定の構成

Data Protection for Microsoft Hyper-V が Transport Layer Security (TLS) プロトコルを使用して IBM Spectrum Protect サーバーのバージョン 8.1.1 以前または V7.1.7 以前と通信できます。

このタスクについて

TLS 1.2 を有効にした SSL を使用するようにサーバーが構成される場合、構成ウィザードからセキュリティ証明書を受け入れると、証明書を伴うトラストストアが自動的に作成されます。ただし、自動ダウンロード・プロセスが失敗した場合は、手動でトラストストアを作成し、構成ウィザードを再実行する必要があります。

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。

このツールは C:\Program Files\Common Files\Tivoli\TSM\jvm80406\jre\bin ディレクトリにあります。この位置は、使用する Java ソフトウェアのバージョンに基づいて変更される場合があります。

手順

スタンドアロン Hyper-V ホストで、以下のステップを実行します。クラスター環境では、クラスター内のホストごとに以下のステップを実行します。

1. IBM Spectrum Protect サーバー管理者から必要な証明書を取得し、ホスト上の任意の場所 (c:\cert ディレクトリなど) にダウンロードします。
2. コマンド・プロンプトで次のコマンドを実行して、トラストストア・ディレクトリに変更します。

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

このフォルダーが存在しない場合は、作成します。

3. 次のコマンドを発行して、証明書をインポートします。

```
"C:\Program Files\Common Files\Tivoli\TSM\jvm80406\jre\bin \keytool.exe" -
importcert -alias my-cert -file "cert-filename" -keystore tsm-ve-
truststore.jks -storepass password
```

ここで、

-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-filename"

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の名前。例えば、
"C:\cert\cert256.arm" です。

-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。

4. Data Protection for Microsoft Hyper-V 管理コンソールを開始します。

手順については、[63 ページの『Data Protection for Microsoft Hyper-V 管理コンソールの開始』](#)を参照してください。

5. 「構成」をクリックして、構成ウィザードを開きます。

6. 「バックアップ・サーバー」ページで、「バックアップ・サーバーの **SSL ポート**」フィールドにポート番号を指定します。このポートは、TLS 1.2 を有効にした SSL プロトコルを使用して、管理接続を可能にするサーバー・ポートです。
7. ウィザードを完了します。

タスクの結果

ウィザードが正常に完了すると、コマンド・プロンプト、PowerShell コマンドレット、または Data Protection for Microsoft Hyper-V 管理コンソールを使用してバックアップおよびリストア操作を実行できます。

環境でファイル・リストア操作を使用可能にする

管理者によってファイル・リストア機能が使用可能になっている場合、ファイル所有者は最小限の支援を受けてファイルをリストアできます。

このタスクについて

構成ウィザードを使用してファイル・リストア機能を使用可能にする場合、ファイル・リストア操作に必要なソフトウェアが、スタンドアロン Hyper-V ホスト上またはクラスター内の各ホスト上のデータ・ムーバー・ノードにインストールされます。

クラスター環境では、クラスター内の各ホスト上のファイル・リストア・ソフトウェアは、相互に独立しています。ファイル所有者がファイル・リストア・インターフェースにログオンできるようにするために、ホスト名と、ファイル所有者のデータを含む仮想マシン (VM) 名が、ファイル・リストア URL が必要です。

手順

1. 構成ウィザードを開始するために、「ナビゲーション」ペインからホストまたはクラスターを選択し、「**構成**」をクリックします。
2. ウィザードの各ページの指示に従います。手順については、39 ページの『[ウィザードを使用した Data Protection for Microsoft Hyper-V の構成](#)』を参照してください。
 - a) 「**クラスターおよびホスト構成**」ページが表示されたら、「**ファイル・リストアの有効化**」チェック・ボックスにチェック・マークを付けます。
 - b) ファイル・リストアを初めて使用可能にする場合は、ファイル・リストア管理者の資格情報を入力するように求めるプロンプトが出されます。管理者アカウントは、すべての VM でローカル管理権限を持つ Windows ドメイン・ユーザー・アカウントでなければなりません。
3. オプション: Linux ゲスト VM でファイル・リストア操作を実行する予定の場合は、「**結果**」ページのファイル・リストア結果表で「**コピー**」をクリックして、ファイル・リストア URL および Linux マウント・プロキシ・オプションをクリップボードにコピーします。Linux マウント・プロキシを構成するときに、マウント・プロキシ・オプションを `dsm.sys` ファイルに貼り付けることができます。

このファイル・リストア情報は、構成後にいつでも「**アクション**」ペインの「**プロパティ**」をクリックして取得することも可能です。

Linux マウント・プロキシの構成について詳しくは、45 ページの『[ファイル・リストア操作のための Linux マウント・プロキシの構成](#)』を参照してください。

4. ウィザードの構成を完了します。
5. 「**結果**」ペインで VM を選択し、「**アクション**」ペインで「**ファイル・リストア**」をクリックして、ファイル・リストア・インターフェースにアクセスできることを確認します。
6. ファイル・リストア URL の以下のテンプレートに基づいて、ファイル所有者ごとにカスタム URL を構成します。

```
https://<dphvhost>:9081/FileRestoreUI/login?  
vmName=<guestvm_name>&vmHost=<guestvm_host>&vmPlatform=<guestvm_platform>
```

ここで、

dphvhost

Data Protection for Microsoft Hyper-V をインストールし、構成した Hyper-V ホスト。

guestvm_name

ファイル所有者のデータを含むゲスト VM の名前。

guestvm_host

ゲスト VM をホストしている VM ホストの名前。 *guestvm_host* の値は、コンピューター名、IP アドレスまたは DNS 名のいずれかです。

guestvm_platform

ゲスト VM のオペレーティング・システム。 **LINUX** または **WINDOWS** のいずれかの値を指定します。

例えば、Data Protection for Microsoft Hyper-V が Cluster1 と呼ばれるホストにインストールされ、ファイル所有者のデータが、VM ホスト HostB 上の MyVM-Win2k26 と呼ばれる Windows ゲスト VM にある場合、ファイル・リストア URL は次のようになります。

`https://Cluster1:9081/FileRestoreUI/login?vmName=MyVM-Win2k16&vmHost=HostB&vmPlatform=WINDOWS`

ファースト・パス: また、ホスト、VM を選択し、「アクション」ペインで「ファイル・リストア」をクリックして、ファイル・リストア URL を取得することもできます。Web ブラウザーに表示される URL アドレスをコピーできます。

ヒント: 非デフォルト・ポート番号を使用する場合、ポート 9081 を構成したポートと置き換えます。使用されているポート番号を表示するには、[59 ページの『Data Protection for Microsoft Hyper-V 操作のデフォルト以外のポート番号の構成』](#)を参照します。

7. 以下のシナリオに応じてファイル・リストア URL を配布します。

- ヘルプ・デスク・モデルの場合、Hyper-V またはファイル・リストア管理者は、カスタム URL を各ファイル所有者に送信します。
- セルフサービス・モデルの場合、Hyper-V またはファイル・リストア管理者は、所有者が独自のファイル・リストア URL を作成できるように、ファイル所有者に手順を送信します。ファイル所有者への手順のステップ [44 ページの『6』](#) から URL に関する情報を使用できます。

ヒント: クラスター内の異なるホストにいつでもフェイルオーバーできます。この状態では、更新されたゲスト VM を使用した新しい URL をファイル所有者に送信するか、またはファイル所有者が、どのホストが VM をホストするかを判別するために問い合わせる必要があります。

タスクの結果

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して、個々のファイルおよびフォルダーをリストアすることができます。

ファイル・リストア操作のための Linux マウント・プロキシの構成

Linux ゲスト仮想マシン (VM) でファイル・リストア操作を準備するには、Linux マウント・プロキシを構成する必要があります。

始める前に

以下のタスクが完了していることを確認します。

- Hyper-V ホストまたはクラスター上で Data Protection for Microsoft Hyper-V 構成ウィザードを実行して、ファイル・リストア機能を有効にする。手順については、[39 ページの『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』](#)を参照してください。
- Linux システムにマウント・プロキシをインストールする。手順については、[32 ページの『Linux システムへのマウント・プロキシ機能のインストール』](#)を参照してください。

このタスクについて

構成ウィザードでファイル・リストア機能を使用可能にすると、スタンドアロン・ホストまたはクラスター内の各ホストのマウント・プロキシ・ノード・ペアが、プロキシ関係の定義と一緒に IBM Spectrum Protect サーバーに自動的に登録されます。ゲスト VM のファイル・リストア操作を有効にするには、構成ウィザードで提供される Linux マウント・プロキシ・オプションを `dsm.sys` ファイルに追加して、Linux マウント・プロキシを構成する必要があります。

以下の手順では、マウント・プロキシ・ノード・オプションを更新し、IBM Spectrum Protect サーバーとの接続を検証することによって、マウント・プロキシ・ノードをセットアップします。

手順

Linux マウント・プロキシ・システムで以下の手順を実行します。

1. クライアント・ユーザー・オプション・ファイル (`dsm.opt`) がインストール・ディレクトリー (`opt/tivoli/tsm/client/ba/bin`) に存在しない場合は、テキスト・エディターでそのファイルを作成します。
2. `dsm.opt` ファイルをテキスト・エディターで開き、以下のステートメントをファイルに追加します。

```
servername MPNODE_hostname_HV_MP_LNX
```

ここで、*hostname* は Windows Hyper-V ホストの名前です。

このステートメントがファイル内の唯一のステートメントであることを確認します。変更を保存してファイルを閉じます。

3. テキスト・エディターで `dsm.sys` ファイルを開きます。構成ウィザードの「**Linux マウント・プロキシ・オプション**」ウィンドウからマウント・プロキシ・オプションをコピーし、ファイルに貼り付けます。

例えば、以下のスタンザを `dsm.sys` ファイルに貼り付けます。

```
SERVERNAME          MPNODE_hostname_HV_MP_LNX
NODENAME             hostname_HV_MP_LNX
PASSWORDAccess       generate
TCPServeraddress     backup_server_address
TCPPort              1500
HTTPPort             1581      ** Must be unique for each node
COMMMethod            tcpip
ERRORLOGName          dsmererror.hostname_HV_MP_LNX.log
```

ここで、*hostname* は Hyper-V ホストの名前、*backup_server_address* は VM をバックアップする IBM Spectrum Protect サーバーのホスト名または IP アドレスです。

変更を保存して、`dsm.sys` ファイルを閉じます。

4. `-asnodename` および `-optfile` のコマンド・ライン・パラメーターを指定して、マウント・プロキシ・システムでコマンド・ライン・セッションを開始します。

```
dsmc -asnodename=hyperv_target_node -optfile=dsm.opt
```

ここで、*hyperv_target_node* は、VM バックアップが保管される Hyper-V ノード名です。Hyper-V ターゲット・ノードには、以下の命名規則があります。

- ・スタンドアロン・ホスト環境の場合: *hostname_HV_TGT*
- ・クラスター環境の場合: *clustername_HV_TGT*

初回サインオン時に、ユーザー ID とパスワードを求めるプロンプトが出されます。IBM Spectrum Protect サーバー管理者 ID とパスワードを入力します。

初回サインオンが行われた後は新規パスワードが生成および保管されるため、パスワードを求めるプロンプトが再度出されることはありません。

パスワードを求めるプロンプトが出されないようにするには、**dsmc** コマンドを再度実行します。パスワードのプロンプトが出された場合、**passwordaccess generate** オプションが **dsm.sys** ファイルに設定されていることを確認し、手順 46 ページの『4』をもう一度繰り返してください。

5. 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、セッション開始時刻、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。

6. 以下のアクションを実行して、クライアント・アクセプター・サービス (CAD) をセットアップします。

- a) **/etc/init.d/dsmcad** ファイルで以下の環境変数を設定します。

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

- b) インストール・プログラムは、クライアント・アクセプター (**dsmcad**) の始動スクリプトを **/etc/init.d** ディレクトリーに作成します。クライアント・アクセプターは、スケジューラー・タスクを管理する前に開始する必要があります。

root ユーザー ID でログインし、以下のコマンドを使用してクライアント・アクセプターを開始するようにしてください。

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

```
service dsmcad start
```

システムの再始動後にクライアント・アクセプターが自動的に開始できるようにするには、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
```

次のタスク

Linux マウント・プロキシ・ノードが正しくセットアップされていることを確認します。

1. [Hyper-V ホストまたはクラスターで Data Protection for Microsoft Hyper-V 管理コンソール](#) を開始します。
2. Linux VM を選択し、「アクション」ペインの「ファイル・リストア」をクリックしてファイル・リストア・インターフェースに進みます。
3. Linux ゲスト VM に対してファイル・リストア操作を実行できることを確認します。

ファイル・リストア機能を有効にして Data Protection for Microsoft Hyper-V を構成し、初期構成の後に構成ウィザードを再実行した場合、Linux マウント・プロキシ・ノードのパスワードをリセットする必要があります。パスワードをリセットするには、以下のいずれかの方法を使用します。

方法 1

Linux マウント・プロキシで、IBM Spectrum Protect 管理者が **dsmc** コマンドを実行し、プロンプトが表示されたら IBM Spectrum Protect 管理者ユーザー ID およびパスワードを入力します。

方法 2

次の手順を実行します。

1. IBM Spectrum Protect 管理者が、IBM Spectrum Protect サーバー・コンソール上で **UPDATE NODE** サーバー・コマンドを実行して、Linux マウント・プロキシ・ノードのパスワードをリセットします。
2. Linux マウント・プロキシ・ノードの所有者は、Linux マウント・プロキシ上で **dsmc** コマンドを実行します。プロンプトが出されたら、所有者はデフォルトの Linux マウント・プロキシ・ノード ID と新規 Linux マウント・プロキシ・ノード・パスワード (IBM Spectrum Protect サーバー管理者から取得) を入力します。

ファイル・リストア操作のオプションの変更

管理者がファイル・リストア操作を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 Microsoft Hyper-V 管理コンソール 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。
変更するオプションを判別するには、[48 ページの『ファイル・リストア操作のオプション』](#)を参照してください。
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・リストア操作のオプション

`frConfig.props` ファイルのオプションは、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。

backup_info_duration_hours=num_hrs

最新のバックアップ・アクティビティーに関する情報をローカル Data Protection for Microsoft Hyper-V Derby データベースで保存する期間(時間)を指定します。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。

enable_contact_info=false | true

IBM Spectrum Protect ファイル・リストア・インターフェースで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提供するかどうかを指定します。

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

Data Protection for Microsoft Hyper-V 管理コンソール ウィザードは、**enable_filerestore** オプションを上書きする可能性があります、**true** 値のみに上書きします。ファイル・リストア機能を使用不可にしたい場合は、手動でこのオプションを **false** に設定する必要があります。

Data Protection for Microsoft Hyper-V ログ・アクティビティーの構成

管理者が Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・リストア操作がログの形式および記録方法を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、Data Protection for Microsoft Hyper-V 管理コンソール または 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 Microsoft Hyper-V 管理コンソール 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。

変更するオプションを判別するには、50 ページの『Data Protection for Microsoft Hyper-V ログ・アクティビティ・オプション』を参照してください。

3. 変更を保存して、FRLog.config ファイルを閉じます。
4. 次のように、GUI Web サーバーを再始動します。
 - a) 「スタート」 > 「コントロールパネル」 > 「システムとセキュリティ」 > 「管理ツール」 > 「サービス」をクリックします。
 - b) **IBM Spectrum Protect for Virtual Environments** 「Web サーバー」を右クリックし、「再始動」をクリックします。

タスクの結果

Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・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。

Data Protection for Microsoft Hyper-V ログ・アクティビティ・オプション

FRLog.config オプションは、Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・リストア操作に関するロギング情報の内容および形式を制御します。

以下のオプションにより、Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・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、Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・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、Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・リストア・アクティビティに関連する内部 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 `install_directory/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs` です。

FR.API.LOG=ON | OFF

Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・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。

- 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。
- ロギングを無効にする場合は、OFF を指定します。

IBM Spectrum Protect リカバリー・エージェント GUI の構成

マウント操作およびファイル・リストア操作用に IBM Spectrum Protect リカバリー・エージェント GUI をセットアップする必要があります。

始める前に

これらの構成タスクは、IBM Spectrum Protect リカバリー・エージェント GUI を使用する前に完了する必要があります。

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。IBM Spectrum Protect リカバリー・エージェント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. IBM Spectrum Protect リカバリー・エージェント GUI 内の「**IBM Spectrum Protect 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。

次のオプションを指定します。

サーバー・アドレス

IBM Spectrum Protect サーバーの 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・ノードを使用して、ターゲット・ノード内にある 仮想マシン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・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」権限を付与されているノードです。

一般的に、`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 (仮想マシン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・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・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 ページを終了します。

この方法を使用する場合、IBM Spectrum Protect リカバリー・エージェント ユーザーはプロキシ・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・ノード内の特定の仮想マシン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、仮想マシン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` という名前の仮想マシン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 (仮想マシン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 ページを終了します。

この方法を使用する場合、バックアップされた仮想マシン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仮想マシン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。

Direct

このオプションは、ターゲット・ノード (仮想マシン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 (仮想マシン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 ページを終了します。

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、IBM Spectrum Protect リカバリー・エージェント では、パスワード・ストア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パスワード・ストア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。

パスワード・ストレージについて詳しくは、[パスワード・ストレージの保護](#)を参照してください。

IBM Spectrum Protect リカバリー・エージェント は、保護対象の仮想マシン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

バックアップ・プロキシ・ホスト上で実行している IBM Spectrum Protect リカバリー・エージェント は、仮想ボリューム上のデータの変更を書き込みキャッシュに保存します。デフォルトでは、書き込みキャッシュが使用可能になっており、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% になっています。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。

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。

要件: 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有効期限が切れ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。このオプションは、デフォルトでは選択されていません。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。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有効期限が切れる場合があります。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能になったり、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・コピーは操作中に有効期限が切れ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。

IBM Spectrum Protect リカバリー・エージェントでは、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除去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。

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

- b) この場合、以下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。

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・リソースを追加することを検討してください。

- 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その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。プリインストールされている 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**」を検索します。

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も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\System32 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\System32\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

iSCSI デバイスの手動構成

iSCSI マウント操作時に使用する Windows システムを構成する必要があります。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、iSCSI ターゲットは IBM Spectrum Protect リカバリー・エージェント システムで作成されます。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 イニシエーターは、iSCSI ターゲットへの接続が必要なすべてのシステムで必要になります。
- データのリストア先のシステムに 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。
- IBM Spectrum Protect リカバリー・エージェント 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思われ、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. IBM Spectrum Protect リカバリー・エージェント 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に 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、次のとおりです。

```
iqn.1991-05.com.microsoft:hostname
```

2. IBM Spectrum Protect リカバリー・エージェント (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) IBM Spectrum Protect リカバリー・エージェント 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、次のとおりです。

```
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。

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 IBM Spectrum Protect リカバリー・エージェント (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) 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**」ダイアログを使用して、各 iSCSI ターゲットを切断します。
- b) IBM Spectrum Protect リカバリー・エージェント GUI でボリュームを選択し、「**取り外し**」をクリックして、ステップ 2 からのボリュームを取り外します。

拡張構成

拡張構成タスクを使用して、Data Protection for Microsoft Hyper-V の構成をさらにカスタマイズします。

Data Protection for Microsoft Hyper-V 操作のデフォルト以外のポート番号の構成

Data Protection for Microsoft Hyper-V Web サーバーまたは REST API サービスで、デフォルトのポート番号を使用しない場合は、Windows PowerShell コマンドレットを使用して、異なるポート番号を構成できます。

このタスクについて

Web サーバーに割り当てられるデフォルトのポート番号は、Data Protection for Microsoft Hyper-V 管理コンソール、ファイル・リストア・インターフェース、および PowerShell コマンドレットにサービスを提供します。

ポート番号を変更するには、以下の手順を実行します。

手順

1. 139 ページの『[Data Protection for Microsoft Hyper-V で PowerShell コマンドレットを使用する準備](#)』の指示に従って PowerShell を開始してください。
2. オプション: 以下のコマンドレットを実行して、使用されているポート番号を表示します。
 - Web サーバー・ポートを表示するには、**Show-DpHvHttpsPort** コマンドレットを使用します。
 - REST API ポートを表示するには、**Show-DpHvMmcLoginPreferences** コマンドレットを使用します。

このコマンドレットは、Data Protection for Microsoft Hyper-V 管理コンソールのログイン設定 (REST API ポート番号など) を表示します。この設定は、管理コンソールが最初に実行されるときに作成されます。管理コンソールの実行前にこのコマンドレットを実行すると、情報は返されません。
3. デフォルトのポート番号を変更するには、以下のコマンドレットを使用します。
 - Web サーバー・ポートを変更するには、**Set-DpHvHttpsPort** コマンドレットを使用します。例えば、Web サーバーのポート番号を 9082 に変更するには、以下のコマンドレットを使用します。

```
Set-DpHvHttpsPort -httpsPort 9082
```

クラスター内のすべてのホストが同じ HTTPS ポートを使用する必要があります。

- REST API ポートを変更するには、**Set-DpHvMmcLoginPreferences** コマンドレットを使用します。例えば、REST API のポート番号を 9082 に変更するには、以下のコマンドレットを使用します。

```
Set-DpHvMmcLoginPreferences -RestApiPort 9082
```

ヒント: 詳しくは、**Get-Help cmdlet_name** コマンドを使用してください。

Windows Server 2012 および Windows Server 2012 R2 クラスターのスケジュール済み VM バックアップの調整

Data Protection for Microsoft Hyper-V バージョン 8.1.2 から、より多くの仮想マシン (VM) を、クラスター内の複数のノードにわたって並行してバックアップできるようになりました。クラスター・ノードのバックアップ操作は、リカバリー可能条件で障害が発生したスナップショットを持つボリュームでスナップショットを常に再試行します。また、スナップショット内の VM 数を調整すると、Hyper-V ホストに対するスナップショットのワークロードを減らすことができます。

バックアップ中にスナップショットが取られる方法を調整するには、以下のオプションを使用できます。

- `vmmaxparallel` オプションを使用して、IBM Spectrum Protect サーバーに並行して送信される VM 数を制御します。このオプションの設定は、パフォーマンスに最も顕著な影響があります。
- `vmmaxpersnapshot` オプションを使用して、バックアップ操作中に作成される各スナップショットに含むことができる VM 数を制御します。

クラスターをバックアップする前に、環境に合わせてこれらの 2 つのオプションの値を検討し、調整してください。

クラスター・バックアップ操作を調整するには、以下の一般的な方法を使用します。

1. コンテナ・プールを使用する、適切なサイズと構成の IBM Spectrum Protect サーバーを使用することを計画します。サーバーのサイズ設定方法については、[IBM Spectrum Protect Blueprints](#) を参照してください。
2. まず始めに、`vmmaxpersnapshot` オプションと `vmmaxparallel` オプションのデフォルト値を使用します。
3. バックアップ・スケジュールを実行し、結果 (バックアップがスケジュール時間内に完了したかどうか、または発生したスナップショットの再試行回数が多すぎたかどうかなど) をメモします。
4. ご使用の環境で機能するように `vmmaxparallel` オプションの値を調整します。例えば、値を 10 に設定します。
5. `vmmaxpersnapshot` の値を、発生する再試行回数を最小化する値に調整します。再試行回数はバックアップ統計で報告されます。

スナップショット当たりの VM 数を少なくする場合は、バックアップ操作の実行に必要なスナップショット数を増やします。このようにスナップショット数を増やすと、CSV での VM のクラスター・バックアップ操作時に遅延が生じる可能性があります。この遅延が生じるのは、一度に 1 つのスナップショットしか作成できず、スケジュール内の他のノードのバックアップ操作がスナップショット作成中に遅延するためです。スナップショットの VM の数を増やすことで、バックアップ操作で取られるスナップショットの数を減らすことができます。

スナップショットに含める VM の数を判別するには、以下の要因を検討してください。

- より多くの VM を持つスナップショットは、完了までに時間がかかり、システムの負荷を増やします。VM の数が増えるほどスナップショットの継続期間が長くなることを意味し、それによってシステム・パフォーマンスへの影響が生じる可能性があります。
- `vmmaxpersnapshot` オプションと `vmmaxparallel` オプションが連携して、バックアップ操作で取られるスナップショット数が決まります。`vmmaxparallel` オプションは、同時にバックアップできる VM の数を指定します。Data Protection for Microsoft Hyper-V は、`vmmaxparallel` 設定に対応するのに必要な数のスナップショットを取ります。

VM は、VM 用のスナップショットの作成に必要なボリュームに基づいてソートされ、選択されます。1 組のボリュームを共有する 1 組の VM に対して、1 つのスナップショットが作成されます。そのため、スナップショット数は、VM で使用されるボリュームに応じて異なります。スナップショット当たりの VM 数が、`vmmaxpershapshot` オプションの値を超えることはありません。

次の表は、さまざまな `vmmaxpersnapshot` および `vmmaxparallel` の設定で、スナップショット当たりで処理できる VM 数の例を示しています。これらの例では、すべての VM が同じボリューム上にあることを前提としています。

表 7. <code>vmmaxpersnapshot</code> および <code>vmmaxparallel</code> の設定で処理されるスナップショットと VM (同一ボリューム上) の数		
<code>vmmaxpersnapsho</code> <code>t</code> の設定	<code>vmmaxparallel</code> の 設定	作成されるスナップショット数
10	20	各スナップショットに 10 個の VM がある、2 つのスナップショットが作成されます。処理中の VM の数が <code>vmmaxparallel</code> 設定より小さい場合は、別のスナップショットが取られます。

表 7. <i>vmmaxpersnapshot</i> および <i>vmmaxparallel</i> の設定で処理されるスナップショットと VM (同一ボリューム上) の数 (続き)		
<i>vmmaxpersnapsho</i> <i>t</i> の設定	<i>vmmaxparallel</i> の 設定	作成されるスナップショット数
20	20	20 個の VM を含む 1 つのスナップショットが作成されます。
20	10	20 個の VM を含む 1 つのスナップショットが作成され、最初の実行時に <i>vmmaxparallel</i> 設定のために 10 個の VM がバックアップされます。残りの 10 個の VM は、2 回目の実行時にバックアップされます (2 番目のスナップショットは不要です)。

また、*vmmaxsnapshotretry* オプションを使用して、最初のスナップショットがリカバリー可能条件で失敗した場合に、VM のスナップショット操作を再試行する最大回数を指定することができます。

関連概念

9 ページの『[Hyper-V バックアップ操作の制約事項](#)』

Hyper-V バックアップ操作を開始する前に、制約事項を確認してください。すべての Hyper-V バックアップ操作に適用される制約事項もあれば、Windows Server 2012 または 2012 R2 もしくは Windows Server 2016 の環境上の Hyper-V バックアップのみに適用される制約事項もあります。

関連資料

203 ページの『[Vmmaxpersnapshot](#)』

vmmaxpersnapshot オプションは、Hyper-V スナップショットに組み込む 仮想マシン (VM) の最大数を指定するために使用します。スナップショットの VM は、IBM Spectrum Protect サーバーにバックアップされます。

212 ページの『[vmmaxsnapshotretry](#)』

最初のスナップショットが失敗した際、リカバリー可能条件である場合に、*vmmaxsnapshotretry* オプションを使用して仮想マシン (VM) のスナップショット操作を再試行する最大回数を指定します。

202 ページの『[Vmmaxparallel](#)』

vmmaxparallel オプションを使用すると、データ・ムーバーの単一インスタンスを使用して、複数の仮想マシン (VM) の並列バックアップを構成できます。このオプションは、一度に IBM Spectrum Protect サーバーにバックアップできる VM の最大数を指定します。

第 4 章 Data Protection for Microsoft Hyper-V 管理コンソールを使用したデータの管理

Data Protection for Microsoft Hyper-V 管理コンソールは、Data Protection for Microsoft Hyper-V の日常の動作の管理に役立つ単一の環境を提供します。

Data Protection for Microsoft Hyper-V 管理コンソールを使用して、アドホック・バックアップやリスト操作を開始したり、Hyper-V ホストまたはクラスターにあるすべての仮想マシン (VM) に関する最新のバックアップ情報を表示したりすることもできます。

この情報には保護されていない危険な状態にある VM の ID が含まれます。危険な状態にある理由は、VM が一度もバックアップされていないため、あるいは危険ポリシーで設定された時間間隔内にバックアップが行われなかったためです。危険ポリシーは、以前にバックアップされた VM のみに適用されます。

ヒント : 構成ウィザードを使用して Data Protection for Microsoft Hyper-V を最初に構成したり、その構成を更新したりすることもできます。詳しくは、39 ページの『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』を参照してください。

Data Protection for Microsoft Hyper-V 管理コンソールの開始

Data Protection for Microsoft Hyper-V の日常の操作を管理するには、Data Protection for Microsoft Hyper-V 管理コンソールを開始し、ログオン資格情報を入力します。

手順

1. 「スタート」 > 「IBM Spectrum Protect」 > 「DP for Hyper-V 管理コンソール」をクリックして、Data Protection for Microsoft Hyper-V 管理コンソールを開始します。

あるいは、コマンド・プロンプトで以下のコマンドを発行します。

```
"C:\Program Files\IBM\SpectrumProtect\DPHyperV\DpHv.msc"
```

2. プロンプトが出されたら、Data Protection for Microsoft Hyper-V 管理コンソールにログオンします。Hyper-V ホストへのログオンに使用する場合と同じ資格情報を入力します。

Hyper-V およびクラスターの操作をすべて行うには、使用するアカウントは、コンピューターのローカル管理者グループのメンバーである必要があります。

ヒント : Data Protection for Microsoft Hyper-V を構成していない場合、または構成が不完全である場合、自動的に構成ウィザードが表示されます。詳細については、39 ページの『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』を参照してください。

3. 接続先のホストに関連付けられているセキュリティー証明書が認識されない場合、あるいは Data Protection for Microsoft Hyper-V 管理コンソールがインストールされているサーバー上にない場合は、新しい証明書のインストールを求めるプロンプトが表示されます。

スタンドアロン・ホストまたはクラスター内の各ホストに対して、以下のステップを実行します。

- a) 「<host name> への接続の保護」ウィンドウで、「証明書の表示」をクリックします。

その他のオプション (現行セッションの証明書警告を無視する「はい」、接続を停止する「いいえ」、または今後すべての証明書の警告を無視する「このコンピューターへの接続について今後確認しない」など) を選択すると、Data Protection for Microsoft Hyper-V に接続できなくなります。

- b) 「証明書」ウィンドウの「一般」タブで、「証明書のインストール」をクリックします。

- c) 「証明書のインポート ウィザード」ウィンドウのウェルカム・ページで、ストア・ロケーション (「現在のユーザー」または「ローカル コンピューター」) を選択し、「次へ」をクリックします。

- d) 「証明書ストア」ページで、「証明書をすべて次のストアに配置する」をクリックし、「参照」をクリックします。

- e) 「証明書ストアの選択」ウィンドウで、「信頼されたルート証明機関」を選択し、「OK」をクリックします。
- f) 「証明書ストア」ページで「次へ」をクリックします。
- g) 「証明書のインポート ウィザードの完了」ページで選択内容を確認して、「完了」をクリックします。
- h) 「セキュリティ警告」ウィンドウで「はい」をクリックし、証明書をインストールします。
- i) 確認ウィンドウで「OK」をクリックします。

証明書を拒否した場合、Data Protection for Microsoft Hyper-V に接続することはできません。

次のタスク

Data Protection for Microsoft Hyper-V 管理コンソールを使用して、仮想マシン・バックアップを管理し、その状況をモニターすることができます。

一定の非活動状態の期間後、Data Protection for Microsoft Hyper-V 管理コンソールとの接続がタイムアウトになる場合があります。タイムアウトが生じた場合、「再接続 - セッションの有効期限切れ (Reconnect - Session Expired)」ウィンドウに資格情報を入力するように求められます。

カスタム・コンソールでの実行のヒント : Data Protection for Microsoft Hyper-V 管理コンソール を、Hyper-V マネージャーやクラスター・フェイルオーバー・マネージャーなどと一緒に単一のコンソールで実行できるように、カスタム Microsoft 管理コンソールに追加することができます。

1. 空の Microsoft 管理コンソールを、コマンド・プロンプトから **mmc** コマンドを発行して開始します。
2. 「ファイル」 > 「スナップインの追加と削除」をクリックします。
3. 「Data Protection for Microsoft Hyper-V」を選択して、「追加」をクリックします。
4. その他のスナップイン、例えば、「Hyper-V Manager」および「フェイルオーバー クラスタ マネージャー」を選択して追加します。
5. .msc ファイルに名前を付けて保管するには、「ファイル」 > 「名前を付けて保存」をクリックします。
6. カスタム・コンソールを開始するには、保存した .msc ファイルを実行します。

Data Protection for Microsoft Hyper-V 管理コンソールのナビゲート

バックアップ操作の日次管理を実行するには、Data Protection for Microsoft Hyper-V 管理コンソールを使用します。仮想マシンのバックアップ操作をモニターし、バックアップおよびリストア操作を実行し、構成を更新することができます。

Data Protection for Microsoft Hyper-V 管理コンソールには、3つの主な作業域、すなわち「ナビゲーション」ペイン、「結果」ペイン、および「アクション」ペインがあります。これらの作業域に関する情報を示します。

「ナビゲーション」ペイン

左側にある「Data Protection for Hyper-V」というラベルの「ナビゲーション」ペインには、Hyper-V 環境内のクラスターまたはホストを表示するツリー・ビューがあります。クラスター・ビューでは、クラスター・ノードの下位ノードが、クラスター内の各ホストを表します。

「ナビゲーション」ペインでホストまたはクラスターを選択すると、選択されたホストまたはクラスター内の仮想マシン (VM) のバックアップ状況、およびスケジュール実行の履歴が、「結果」ペインの「仮想マシン」ビューと「スケジュール・ヒストリー」ビューに表示されます。選択されたクラスター、ホスト、または VM に使用可能なアクションのリストは、管理コンソールの右側にある「アクション」ペインにも表示されます。

「結果」 ペイン

Data Protection for Microsoft Hyper-V 管理コンソールの中央にある「結果」ペインは、選択されたクラスターまたはホストの仮想マシン・バックアップおよびバックアップ・スケジュール・ヒストリーに関する詳細情報を表示します。

このワークスペースには、「**仮想マシン**」と「**スケジュール・ヒストリー**」というラベルが付いた 2 つのビューが含まれています。「結果」ペイン内の対応するタブをクリックして、各ビューを表示します。

「仮想マシン」 ビュー

結果ペインの「**仮想マシン**」ビューには、クラスターまたはホスト内の各仮想マシン (VM) のデータ保護状況と、個々の VM のバックアップ・ヒストリーが表示されます。

「**フィルター**」フィールドに VM 名のすべてまたは一部を入力し、名前にその文字列を含む VM のみを表示できます。また、「**最新表示**」をクリックすると、表の内容を更新できます。

VM 表

「仮想マシン」ビューの上部には、ホストまたはクラスターの VM の表が示され、VM ごとに前回のバックアップ操作に関する詳細情報が表示されます。以下のデータが表に表示されます。

表 8. VM 表の列の説明	
列	説明
名前	VM の名前。
Host	「ナビゲーション」ペインでクラスターが選択される場合、VM の現在アクティブなホストの名前。VM 状況が「 削除済み 」である場合、ホスト名が引き続き表示されます。 ただし、環境が Data Protection for Microsoft Hyper-V バージョン 8.1.2 以前からアップグレードされている場合、フィールドは、VM バックアップが V8.1.10 で実行されるまで空のままです。
状態	選択された VM の状態。VM の状況は以下のいずれかになります。 オフ VM は電源オフになります。 実行 VM は電源オンで稼働しています。 一時停止 VM の現在の状態は保持されますが、VM に割り振られているメモリーは使用し続けたまま、プロセッサ・リソースが解放されます。 保存済み VM の現在の状態は保持されますが、VM に割り振られているメモリーとプロセッサ・リソースは解放されます。 項目が表示されない場合は、ご使用の環境から VM は削除されていますが、バックアップが IBM Spectrum Protect サーバーにまだ存在しています。

表 8. VM 表の列の説明 (続き)	
列	説明
状況	<p>VM のデータ保護状況。VM の保護状況は、以下のいずれかです。</p> <p>危険 危険ポリシーで指定された時間制限内に、最新のバックアップ操作が行われませんでした。</p> <p>バックアップなし VM のバックアップ操作が構成されましたが、バックアップが実行されませんでした。</p> <p>標準 危険ポリシーで指定された時間制限内に、バックアップ操作が行われました。</p> <p>無視 VM の危険警告を抑止するように、危険ポリシーが設定されています。</p> <p>削除済み VM が Hyper-V 環境から削除されましたが、そのバックアップはリストア可能です。</p> <p>インスタント・アクセス VM はインスタント・アクセス・モードで実行されています。インスタント・アクセス VM は、VM バックアップの一時コピーであり、バックアップ・データの検証などの操作に使用されます。</p>
前回のバックアップ	正常に終了した最後のバックアップ操作の日付。
転送されたデータ	バックアップ操作中に IBM Spectrum Protect サーバーに送信されたデータの量。
期間	バックアップ操作の実行にかかった時間。
バックアップ・タイプ	実行されたバックアップ操作のタイプ (フルまたは差分)。
Schedule	正常に終了した最後のバックアップ中に実行されたスケジュールの名前。

バックアップ・ヒストリー表

「バックアップ・ヒストリー」表には、VM 表で選択した単一の仮想マシン (VM) の以前にスケジュールされたバックアップまたはアドホック・バックアップのタスクの詳細が表示されます。複数の VM を選択した場合、「バックアップ・ヒストリー」表にデータは表示されません。

「バックアップ・ヒストリー」表に表示されるバックアップ・タスクの数は、IBM Spectrum Protect サーバーの **SET EVENTRETENTION** コマンドで設定された日数によって異なります。

以下のデータが表に表示されます。

表 9. 「バックアップ・ヒストリー」表の列の説明	
列	説明
最終実行時刻	前回のバックアップ実行の実際の開始日時。

表 9. 「バックアップ・ヒストリー」表の列の説明 (続き)	
列	説明
状況	<p>バックアップ操作の状況。</p> <p>成功 バックアップ操作は正常に完了しました。</p> <p>失敗 バックアップ操作でエラーが検出され、この操作は完了しませんでした。</p> <p>進行中 バックアップ操作が進行中です。</p>
期間	バックアップ操作の期間。
エラー・コード	バックアップ操作が失敗した場合、エラー・コードが表示されます。バックアップ操作が正常に完了した場合は、ゼロ (0) が表示されます。
転送されたデータ	バックアップ操作中に IBM Spectrum Protect サーバーに送信されたデータの量。
バックアップ・タイプ	<p>VM に対して実行されたバックアップ操作のタイプ。</p> <p>差分 前回のバックアップ (フルまたは増分) 以降に変更されたブロックをバックアップします。</p> <p>完全 VM 全体のスナップショットがバックアップされます。</p>
バックアップ・ホスト	VM がバックアップされたときに VM のデータ・ムーバーが含まれているホスト。クラスターの場合、フェイルオーバー・クラスタリングのためにこのデータ・ムーバー・ホストが変更される可能性があります。

タスク表

「タスク」表は、Data Protection for Microsoft Hyper-V 管理コンソール の開始以降に開始した最近のタスクのリストを表示します。

詳細については、[70 ページの『タスク表』](#)を参照してください。

アクティブ・タスクに関する詳細情報を表示することもできます。詳細については、[70 ページの『タスクの詳細』](#)を参照してください。

関連タスク

[136 ページの『Data Protection for Microsoft Hyper-V 管理コンソール からのインスタント・アクセス操作の実行』](#)

Data Protection for Microsoft Hyper-V 管理コンソール から、簡単にインスタント・アクセス操作を実行することができます。

[137 ページの『Data Protection for Microsoft Hyper-V 管理コンソール からのインスタント・アクセス VM の除去』](#)

インスタント・アクセス仮想マシン (VM) が不要になった場合は、Data Protection for Microsoft Hyper-V 管理コンソールを使用してその VM を除去することができます。

「スケジュール・ヒストリー」ビュー

「結果」ペインの「スケジュール・ヒストリー」ビューに、Hyper-V ホストまたはクラスターに関連付けられているバックアップ・スケジュールの実行履歴が表示されます。

「最新表示」をクリックすると、表の内容を更新できます。

スケジュール・ヒストリー表

スケジュール・ヒストリー表には、ホストまたはクラスターのバックアップ・スケジュールの履歴が表示されます。

表示されるバックアップ・ヒストリーのリストの数は、IBM Spectrum Protect サーバーで **SET EVENTRETENTION** コマンドによって設定された日数により異なります。

以下のデータがスケジュール・ヒストリー表に表示されます。

表 10. スケジュール・ヒストリー表の列の説明	
列	説明
スケジュール開始時刻	スケジュールが開始された実際の日時。スケジュールが未実行であった場合、スケジュールされた開始時刻が表示されます。
名前	スケジュールの名前。
状況	<p>スケジュールの状況は、スケジュールに関連付けられているすべてのデータ・ムーバーに基づいています。以下の状態が表示されます。</p> <p>成功 すべてのデータ・ムーバーのスケジュールの実行が完了しました。バックアップされたか、バックアップが失敗した個々の VM の詳細が、2 番目の表に表示されます。</p> <p>失敗 少なくとも 1 つのデータ・ムーバーでスケジュールの実行が完了しませんでした。</p> <p>進行中 すべてのデータ・ムーバーでスケジュールが開始し、完了していません。</p> <p>仕損じ スケジュールの開始時間帯内で、1 つ以上のデータ・ムーバーでスケジュールが開始できませんでした。</p>
成功した VM	スケジュール実行中に正常にバックアップされた VM の数。
VM 障害	スケジュール実行中にバックアップが失敗した VM の数。スケジュールが未実行か失敗した場合、ダッシュ (-) が表示されます。
期間	スケジュールが実行された時間の長さ。最初のスケジュール・アクティビティの開始から、最後のスケジュール・アクティビティまでの期間が測定されます。スケジュールが未実行か失敗した場合、ダッシュ (-) が表示されます。

スケジュールの詳細表

スケジュール・ヒストリー表でスケジュールの項目を選択すると、「**スケジュールの詳細**」表に、選択したスケジュール実行でバックアップされた仮想マシン (VM) のリストが表示されます。

複数のノードが 1 つのスケジュールに関連付けられている場合、表示される仮想マシン (VM) の数は、そのスケジュール実行に関するすべてのデータ・ムーバー・ノードからの情報を反映します。

「**フィルター**」フィールドに VM 名のすべてまたは一部を入力し、名前にその文字列を含む VM のみを表示できます。

以下のデータが表に表示されます。

表 11. 「スケジュールの詳細」表の列の説明	
列	説明
名前	VM の名前。
状況	VM のバックアップ状況。 成功 VM は正常にバックアップされました。 失敗 VM のバックアップに失敗しました。
開始時刻	VM バックアップ操作が開始された日時。
理由	VM バックアップが失敗した場合は、エラー・コードが提供されます。バックアップ操作が成功した場合は、ゼロ (0) が表示されます。
期間	バックアップ操作の期間。
転送されたデータ	バックアップ操作中に IBM Spectrum Protect サーバーに送信されたデータの量。
バックアップ・タイプ	VM に対して実行されたバックアップ操作のタイプ。 差分 前回のバックアップ (フルまたは増分) 以降に変更されたブロックをバックアップします。 完全 VM 全体のスナップショットがバックアップされます。
バックアップ・ホスト	VM バックアップ操作の実行に使用されるデータ・ムーバーが含まれているホスト。クラスターの場合、フェイルオーバー・クラスタリングのためにこのデータ・ムーバー・ホストが変更される可能性があります。

タスク表

「**タスク**」表は、Data Protection for Microsoft Hyper-V 管理コンソールの開始以降に開始した最近のタスクのリストを表示します。

詳細については、[70 ページの『タスク表』](#)を参照してください。

アクティブ・タスクに関する詳細情報を表示することもできます。詳細については、[70 ページの『タスクの詳細』](#)を参照してください。

タスク表

「タスク」表は、Data Protection for Microsoft Hyper-V 管理コンソールの開始以降に始まった最新のバックアップ・タスクまたはリストア・タスクのリストを表示します。

タスクの同じリストが、「仮想マシン」ビューまたは「スケジュール・ヒストリー」ビューに表示されます。バックアップ操作やリストア操作などの、長時間実行されるタスクをモニターできます。

以下のボタンをクリックすることで、さらに多くのアクションを実行できます。

停止

実行中のタスクを取り消します。

削除完了

すべての完了タスクを表から除去します。実行中のタスクは除去されません。

詳細の表示

「タスクの詳細」ペインを開き、アクティブ・タスクに関する詳細情報を表示します。「詳細の表示」ボタンは、「タスクの詳細」ペインが閉じている場合에만表示されます。詳細については、[70 ページの『タスクの詳細』](#)を参照してください。

詳細を非表示

「タスクの詳細」ペインを閉じます。「詳細の非表示」ボタンは、「タスクの詳細」ペインが開いている場合にのみ表示されます。

以下のデータが「タスク」表に表示されます。

表 12. 「タスク」表の列の説明	
列	説明
Host	タスクが実行中のホスト。
タスク	実行中のタスクのタイプ（「バックアップ」、「リストア」、または「リストア - インスタント・アクセス」）。
状況	タスクの状況（「作業中」、「成功」、または「失敗」）。
開始時刻	タスクの開始日時。
期間	タスクの実行にかかった時間、またはタスクが実行していた時間。
メッセージ	タスクが失敗した場合、関連したエラー・メッセージが表示されます。タスクが正常に完了した場合は、メッセージは表示されません。 メッセージ・フィールドには、進行中のタスクの状況メッセージも表示されます。

タスクの詳細

「タスクの詳細」ペインには、「タスク」表で選択されたアクティブ・タスクに関する詳細情報が表示されます。また、タスクの詳細をクリップボードにコピーすることもできます。

「タスクの詳細」ペインを開くには、「タスク」表で実行中のタスクを選択し、「詳細の表示」をクリックします。

「タスクの詳細」ペインを閉じるには、「詳細の非表示」をクリックします。

ゼロ以外のエラー・コードに関する詳細情報を表示するには、「エラー情報」をクリックします。

以下の表は、「タスクの詳細」ペインのリスト・ボックスに表示されるデータについて説明しています。

表 13. 「タスクの詳細」 ペインのデータの説明	
ボックス名	説明
操作のタイプ	<p>操作のタイプ (「IFINCREMENTAL バックアップ」や「IFFULL バックアップ」など) を表示します。</p> <p>処理中の VM の名前がリスト・ボックスにリストされます。VM 名をクリックして、「状況」ボックスおよび「メッセージ」ボックスに詳細を表示することができます。</p>
状況	<p>タスクに関する状況情報を表示します。この情報は、タスクの実行中に更新されます。</p> <p>検査されたオブジェクト 操作中に検査されたオブジェクトの総数。</p> <p>バックアップされたオブジェクト 操作中にバックアップされたオブジェクトの総数。</p> <p>失敗したオブジェクト 操作中に失敗したオブジェクトの総数。詳しくは、<code>dsmererror.hostname_HV_DM.log</code> ファイルを参照してください。</p> <p>合計バイト数 操作中に転送された合計バイト数。</p> <p>集約ネットワーク 操作中に IBM Spectrum Protect サーバー に転送された合計バイト数を合計経過時間で除算した値。</p> <p>エラー・コード 操作中に生成されたすべての戻りコード。 「エラー情報」をクリックすると、戻りコードに関する詳細情報が表示されます。詳細については、72 ページの『IBM Spectrum Protect エラー情報』を参照してください。</p>
メッセージ	<p>タスク中に生成されたすべてのメッセージを表示します。</p> <p>時刻 メッセージが発行された日時を表示します。</p> <p>メッセージ タスク中に発行されたメッセージのリストを表示します。</p>

ヒント: 「コピー」をクリックして、タスクの詳細をクリップボードにコピーすることができます。このタスクの詳細は、「タスクの詳細」ペインで表示された情報に、そのタスクに相当する Windows PowerShell コマンドレットを加えたものと同じです。

例えば、アクティブ・タスク中に以下の詳細がクリップボードにコピーされます。

```
KINGSTON7      Backup      Working      9/5/2018 1:55:52 PM      00.00.00:40
IFINCREMENTAL backup
```

```
VM Name
kingston19
```

```
Status
Objects inspected: 1
Objects backed up: 0
Objects failed: 0
Total bytes: 0.00 Bytes
Aggregate network: 0 KB/sec
Return code: 0
```

```
Messages
9/5/2018 1:56:11 PM Comparing...
```

```
PowerShell
Backup-DpHvVM -session $sessKINGSTON7 -vmName kingsont19 -node IFINCREMENTAL
-AppConsistentAttempt 2 -CrashConsistentAttempt 0 -diskProtrection 0
```

制約事項: 複数の VM をバックアップしており、「**随時バックアップ**」ウィンドウで特定の仮想ディスクを組み込んでいない場合、すべての VM のバックアップ操作が正常に完了した場合でも、バックアップ操作中にタスクの詳細が表示されるのは 1 つの VM についてのみです。

例えば、「**随時バックアップ**」ウィンドウの「**データ保護**」フィールドで「**ディスク 1 のみを組み込む**」を選択したとします。Data Protection for Microsoft Hyper-V 管理コンソールでのバックアップ操作で複数の VM (VM1、VM2、および VM3) をバックアップする場合、「**タスクの詳細**」ペインには、バックアップ操作中に詳細が表示されるのは VM1 についてのみです。

この制約事項は、Data Protection for Microsoft Hyper-V 管理コンソールにのみ適用されます。データ・ムーバー・コマンド・ラインでのバックアップ操作には影響しません。

IBM Spectrum Protect エラー情報

「**タスクの詳細**」ペインでタスクの状況にゼロ以外の戻りコードが含まれている場合は、「**エラー情報**」をクリックして、戻りコードに関する詳細情報を表示することができます。「**IBM Spectrum Protect エラー情報**」ウィンドウに、詳細なエラー情報が表示されます。

「**エラー情報**」ウィンドウでは、以下の情報を確認できます。

- エラー・コード。
- エラー・メッセージ。
- メッセージに関する資料が含まれる Web サイトへのリンク。
- データ移動プログラム・ノードの名前。
- ホスト名。
- エラー・ログ・ファイルの名前。
- データ・ムーバー・ノードに関するエラー・ログのセクション。タスク開始時刻からタスク終了時刻までの最大 200 行を表示します。

エラー・ログ・ファイルをダウンロードしたり、ウィンドウに表示されているエラー・ログのセクションをコピーしたりすることもできます。

ログのダウンロード

エラー・ログ・ファイルをダウンロードします。「**ログのダウンロード**」をクリックすると、ファイルが保存されたかどうかを示すウィンドウが開きます。ファイルが保存されている場合は、保存されているファイル名が表示され、ログを **Notepad** で開くかを確認するプロンプトが表示されます。

コピー

表示されているエラー・ログのセクションをコピーし、それをクリップボードに貼り付けます。

閉じる

エラー情報ウィンドウを閉じます。

ヒント: 以下の PowerShell コマンドレットを使用して、戻りコードに関する詳細情報を返すこともできます。

- **Get-DpHvRCInfo**
- **Get-DpHVLogSection**
- **Get-DpHvLog**

詳細については、[141 ページ](#)の『Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット』を参照してください。

「アクション」ペイン

Data Protection for Microsoft Hyper-V 管理コンソールの右側の「アクション」ペインは、「ナビゲーション」ペインで選択された項目、および「結果」ペインで選択された VM に対して使用可能なアクションのリストを表示します。

「アクション」ペインには、ホストまたはクラスター用に 1 つのセクション、VM 用に 1 つのセクションが含まれています。

ホストまたはクラスター・レベルで適用されるアクション

ログアウト

Data Protection for Microsoft Hyper-V からログアウトします。

接続

Data Protection for Microsoft Hyper-V にログインします。

バックアップ管理

バックアップ・スケジュールを単一の Hyper-V ホスト環境またはクラスター環境に割り当てます。

構成

構成ウィザードを開いて、Data Protection for Microsoft Hyper-V の構成を更新します。

プロパティ

Data Protection for Microsoft Hyper-V の現行の構成を表示します。構成を更新するには、「構成」をクリックします。

「表示」 > 「カスタマイズ」

Data Protection for Microsoft Hyper-V 管理コンソールに表示される内容をカスタマイズします。

最新表示

Data Protection for Microsoft Hyper-V 管理コンソールの内容を最新表示します。

Help

Data Protection for Microsoft Hyper-V 管理コンソール のオンライン・ヘルプを開きます。

VM レベルで適用されるアクション

バックアップ

1 つ以上の VM をバックアップします。

リストア

「リストア」ウィザードを使用して、単一の VM をリストアします。

ファイル・リストア

Web ブラウザーでファイル・リストア・インターフェースを開きます。ファイル・リストア機能を有効に設定している場合のみ使用できます。

危険な状態を設定

1 つ以上の VM に危険ポリシーを設定します。

Help

Data Protection for Microsoft Hyper-V 管理コンソール のオンライン・ヘルプを開きます。

Data Protection for Microsoft Hyper-V の構成の検証

構成ウィザードを実行した後、Data Protection for Microsoft Hyper-V 管理コンソールを使用して、構成プロセス中に作成されたノードの構成を検証することができます。ノード構成を検証することで、システム操作の潜在的な問題を防ぐことができます。

このタスクについて

ノードの構成を検証する際には、以下のタイプの情報が表示されます。

- データ・ムーバー・ノードに関する情報 (ホスト名、オペレーティング・システム、エラー・ログの場所など)
- ファイル・リストア機能が有効にされている場合は、マウント・プロキシ・ノードに関する情報 (ホスト名、オペレーティング・システム、エラー・ログの場所、リカバリー・エージェントの状態、マウント・プロキシ・ノードの iSCSI 状況など)。

手順

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインからクラスターまたはホストを選択します。
3. 「アクション」ペインで、「プロパティ」をクリックします。
4. 「プロパティ」ウィンドウで「ノードの検証」ページを選択し、ノード情報を表示します。

「一般」ページおよび「ノードの検証」ページに表示されるデータは、ナビゲーション・ペインで選択したノードによって異なります。クラスター・ノードを選択した場合は、クラスター内のすべての有効なノードに関する情報が表示されます。ホストを選択した場合は、そのホストに関連するデータのみが表示されます。

5. 検証するノードを「ノード情報」ボックスから選択し、「ノードの検証」をクリックします。

ヒント: Linux マウント・プロキシ・ノードを選択した場合は、「ノードの検証」ボタンが無効になります。Linux マウント・プロキシ情報を表示するには、Windows マウント・プロキシ・ノード (通常は、リスト内の次の項目) を選択し、「ノードの検証」をクリックします。次に、「ノード情報」ボックスで Linux マウント・プロキシ・ノードを再度選択すると、Linux マウント・プロキシ情報が「状況の詳細」ボックスに表示されます。

6. 「状況の詳細」ボックスに表示される結果を確認して、検証で検出された問題を解決します。

ヒント: 「状況の詳細」ボックス内のコンテンツをハイライトし、**Ctrl+C** を押すことで、結果をクリップボードに保存することができます。その後、そのコンテンツをテキスト文書に貼り付けて、参照用に保存することができます。

7. 「プロパティ」ウィンドウを閉じるには、「クローズ」をクリックします。

次のタスク

構成の問題を解決した後、Data Protection for Microsoft Hyper-V 管理コンソールを再始動して、構成を再検証することができます。

ヒント: **Test-DpHvConfiguration** PowerShell コマンドレットを使用して構成を検証することもできます。詳細については、[145 ページの『Data Protection for Microsoft Hyper-V コマンドレットの例』](#)を参照してください。

ホストまたはクラスターのマシンのバックアップ・スケジュールの管理

スケジュールを選択して、Hyper-V ホストまたはクラスター内の VM を自動的にバックアップする頻度および時点を指定することができます。

このタスクについて

スケジュールは、VM を自動でバックアップするために、IBM Spectrum Protect サーバー管理者によってセットアップされます。

スケジュールを Data Protection for Microsoft Hyper-V に使用できるようにするには、IBM Spectrum Protect サーバー管理者が、Hyper-V VM のバックアップ専用のスケジュールのリストをセットアップする必要があります。スケジュール定義には以下のパラメーターおよびオプションが含まれている必要があります。

- `-domain.vmfull="all-vm"` オプションが、オプション・ストリングで指定される必要があります。`-domain.vmfull` には、これ以外のパラメーターは必要ありません。
- スケジュールには `ACTION=BACKUP` および `SUBACTION=VM` パラメーターが含まれている必要があります。

例えば、管理者は次の **DEFINE SCHEDULE** サーバー・コマンドを使用してスケジュールを定義します。

```
define schedule hyperv_domain_name schedule_name
description=schedule_description action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=hypervfull
-mode=IFIncremental -domain.vmfull="all-vm"'
```

Hyper-V 管理者は、「バックアップ管理」ウィンドウを使用して、データ・ムーバーをスケジュールに関連付けます。`-asnodename=` オプションは、スケジュール定義に自動的に追加されます。例えば、スタンドアロン・ホストの場合、次のオプションが追加されます。

```
-asnodename=Hyper-V_host_HV_TGT
```

クラスター環境の場合、次のオプションが追加されます。

```
-asnodename=clustername_hv_tgt
```

システム構成によっては、ノード名に接頭部および接尾部を含めることもできます。詳細については、[18 ページの『ノード名のカスタマイズ』](#)を参照してください。

ヒント：サーバー管理者は、IBM Spectrum Protect Operations Center を使用して Hyper-V のスケジュールを定義することもできます。

一部の VM を除外する必要がある場合、オプション・ストリングの `-domain.vmfull` オプションに `-vm` パラメーターを指定します。例えば、`TestVm1` という名前の VM を除くすべての VM をバックアップするには、オプション・ストリングで次のパラメーターを指定します。

```
-domain.vmfull="all-vm;-vm=TestVM1"
```

スケジュール・バックアップ操作に単一の VM を含める場合は、オプション・ストリングで次のパラメーターを指定します。以下の例で、VM は `TestVM1` という名前です。

```
-domain.vmfull="all-vm;-vm=*;vm=TestVM1"
```

バックアップ・スケジュールをホストまたはクラスターに関連付けることによって、そのホストまたはクラスターにバックアップ・ポリシーを設定します。また、ホストまたはクラスターからスケジュールのアソシエーションを除去することもできます。

クラスター環境で、選択したスケジュールがクラスター内のすべてのホストに適用されます。クラスターの一部であるホストに別のスケジュールを割り当てることはできません。

手順

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインで、スタンドアロン・ホストまたはクラスターをクリックします。
3. 「アクション」ペインで、「バックアップ管理」をクリックします。

スケジュールの要約が表に表示されます。スケジュールの以下のプロパティが表示されます。

スケジュール名

スケジュールの名前。

繰り返し

スケジュールが繰り返される頻度。

ホスト名

スケジュールに関連付けられているデータ・ムーバー・ノードに対応するホストのリスト。

説明

スケジュールの説明。

4. 「バックアップ管理」ウィンドウでスケジュールを選択し、以下のアクションのいずれかを実行します。

- 選択したスケジュールをクラスターまたはホストに関連付け、ウィンドウを変更内容で更新するには、「**スケジュールの割り当て**」をクリックします。

スケジュールがクラスターまたはホストに割り当てられると、スケジュール定義のオプション・ストリング内の `-asnodename` が、ターゲット・ノード (`hostname_HV_TGT` または `clustername_HV_TGT`) と一緒に指定されます。このターゲット・ノードに関するスケジュールのみが表示されるか、または他のターゲット・ノードに関連付けられていないスケジュールが表示されます。

ターゲット・ノード名には、接頭部および接尾部を含めることもできます。例えば、`prefix_hostname_HV_TGT_suffix` あるいは `prefix_clustername_HV_TGT_suffix` などです。

- 選択したスケジュールのアソシエーションをクラスターまたはホストから除去するには、「**スケジュールの割り当て解除**」をクリックします。

スケジュールのアソシエーションをクラスターまたはホストから除去されると、`asnodename` オプションがスケジュール定義のオプション・ストリングから除去され、クラスターまたはホストに関連したノードがアソシエーションから除去されます。

5. 「クローズ」をクリックして、ウィンドウをクローズします。

仮想マシンの危険ポリシーの設定

Hyper-V 仮想マシン (VM) は、バックアップ操作が失敗したり行われなかったりしたために、保護されていない危険な状態になっている場合があります。指定された時間間隔でバックアップ操作が実行されなかった場合に、VM が危険であるとして表示するかどうかを指定するポリシーを VM に対して設定することができます。

このタスクについて

デフォルトで、各 VM は IBM Spectrum Protect サーバーに設定されたポリシーを使用します。Data Protection for Microsoft Hyper-V 管理コンソールでクラスター・ビューまたはホスト・ビューで選択された 1 つ以上の VM に対して、デフォルト・ポリシーを使用することも、カスタム・ポリシーを設定することも、ポリシーを無視することもできます。

「仮想マシン」ペインの「状況」列は、ホストまたはクラスター内の各 VM のデータ保護状況を示します。データ保護の状態は以下のとおりです。

危険

危険ポリシーで指定された時間制限内に、最新のバックアップ操作が行われませんでした。

バックアップなし

VM のバックアップ操作が構成されましたが、バックアップが実行されませんでした。

標準

危険ポリシーで指定された時間制限内に、バックアップ操作が行われました。

無視

VM の危険警告を抑止するように、危険ポリシーが設定されています。

削除済み

VM が Hyper-V 環境から削除されましたが、そのバックアップはリストア可能です。

インスタント・アクセス

VM はインスタント・アクセス・モードで実行されています。インスタント・アクセス VM は、VM バックアップの一時コピーであり、バックアップ・データの検証などの操作に使用されます。

危険ポリシーは、バックアップされた VM のみに割り当てることができます。VM が一度もバックアップされていない場合、「危険な状態を設定」アクションが使用不可になります。

手順

デフォルトの危険ポリシーを使用する、選択された VM に対してカスタム危険ポリシーを選択する、あるいは選択された VM で危険ポリシーを無視するように設定するには、以下のステップを実行します。

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインで、ホストまたはクラスターをクリックし、VM テーブル内の 1 つ以上の VM をクリックします。
3. 「アクション」 > 「危険な状態を設定」をクリックします。
4. 「危険な状態を設定」ウィンドウで以下のいずれかのアクションを実行します。

アクション	ステップ
デフォルトの危険ポリシーを使用する	「デフォルト」をクリックして、デフォルト期間の 1 日を受け入れます。
VM の危険警告を抑止する	「無視」をクリックします。
カスタム危険ポリシーを設定する	「カスタム」をクリックし、スライダーを動かして、前回のバックアップ以降の時間間隔を設定します。デフォルト値は 6 時間です。

5. 設定を保存するには、「危険な状態を設定」をクリックします。
6. ウィンドウを閉じるには、「クローズ」をクリックします。

タスクの結果

VM の危険ポリシーを「デフォルト」または「カスタム」に設定すると、ポリシーで設定した時間制限内にバックアップ操作が実行されなかった場合、その VM に対して「危険」状況が表示されます。VM が一度もバックアップされていない場合も危険であると見なされ、「バックアップなし」の状況が表示されます。

VM の危険ポリシーが「無視」に設定されると、バックアップに状況にかかわらず、VM のリスク状況は「無視」と表示されます。

Hyper-V ホストまたはクラスターのスケジュール・ヒストリーの表示

Hyper-V ホストまたはクラスターに関連付けられているバックアップ・スケジュールの実行履歴を表示できます。この履歴には、スケジュールが実行された日時、スケジュール実行の状況、およびバックアップが正常に行われたか、失敗した仮想マシン (VM) の数が含まれます。

このタスクについて

スケジュールに対して表示される実行の数は、IBM Spectrum Protect サーバーで **SET EVENTRETENTION** コマンドによって設定された日数により異なります。

手順

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインで、ホストまたはクラスターをクリックし、「スケジュール・ヒストリー」タブをクリックします。

クラスターまたはホストに関連付けられているすべてのバックアップ・スケジュールの実行履歴を表示できます。また、スケジュールを選択して、「[スケジュールの詳細](#)」表で、そのスケジュールに関連付けられている VM のバックアップ状況を表示することもできます。

詳しくは、[68 ページの『「スケジュール・ヒストリー」ビュー』](#)を参照してください。

関連情報

[SET EVENTRETENTION \(イベント・レコードの保存期間の設定\)](#)

仮想マシンのバックアップ状況とバックアップ・ヒストリーの表示

ホストまたはクラスター内のスケジュールされた仮想マシン (VM) バックアップの状況を表示すると、注意が必要な VM を識別できます。また、個々の VM のバックアップ・ヒストリーを表示することもできます。

手順

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインから、ホストまたはクラスターをクリックします。
3. 「**仮想マシン**」タブをクリックします。
4. VM 表で、ホストまたはクラスター内の VM の最新のスケジュール済みバックアップ操作の状況を表示します。

状況が「**危険**」である VM は、スケジュールされた前回のバックアップが未実行であったか、エラーで完了したことを示しています。

5. VM のバックアップ・ヒストリーを表示するために、VM 表から VM を選択します。

その VM に固有のバックアップ・ヒストリーが「**バックアップ・ヒストリー**」表に表示されます。

「**バックアップ・ヒストリー**」表に表示されるバックアップ・タスクの数は、IBM Spectrum Protect サーバーの **SET EVENTRETENTION** コマンドで設定された日数によって異なります。

詳細については、[65 ページの『「仮想マシン」ビュー』](#)を参照してください。

ヒント: データ・ムーバー・コマンド (**dsmc**) を使用して VM バックアップに関する情報にアクセスする場合は、**dsmc** コマンドで以下のオプションを指定してください。

- クラスターの場合、以下のオプションを指定します。

```
-optfile=hostname_HV_DM.opt  
-asnodename=clustername_HV_TGT
```

- スタンドアロン・ホストの場合、以下のオプションを指定します。

```
-optfile=hostname_HV_DM.opt  
-asnodename=hostname_HV_TGT
```

システム構成によっては、ノード名に接頭部および接尾部を含めることもできます。この場合、**dsmc** コマンドで以下のオプションを指定します。

- クラスターの場合、以下のオプションを指定します。

```
-optfile=prefix_hostname_HV_DM_suffix.opt  
-asnodename=prefix_clustername_HV_TGT_suffix
```

- スタンドアロン・ホストの場合、以下のオプションを指定します。


```
-optfile=prefix_hostname_HV_DM_suffix.opt  
-asnodename=prefix_hostname_HV_TGT_suffix
```

例えば、IBM Spectrum Protect サーバー上の VM バックアップに関する情報を照会するには、以下のコマンド構文を使用します。

```
dsmc query vm vmname -optfile=hostname_HV_DM.opt -asnodename=clustername_HV_TGT
```

-asnodename オプションと -optfile オプションを **dsmc query vm** コマンドに指定しない場合、このコマンドの出力は、Data Protection for Microsoft Hyper-V 管理コンソール における VM バックアップの結果と一致しません。

次のタスク

スケジュールの実行を待たずに危険 VM をバックアップする必要がある場合は、その VM を選択し、「アクション」ペインから「バックアップ」をクリックします。

関連タスク

18 ページの『ノード名のカスタマイズ』

デフォルトのノード名に接頭部または接尾部、あるいはその両方を追加することができます。この方法で、構成ウィザードに自動的に生成されるノード名をカスタマイズできます。

関連情報

[SET EVENTRETENTION \(イベント・レコードの保存期間の設定\)](#)

仮想マシンのアドホック・バックアップの開始

仮想マシン (VM) のアドホック・バックアップを開始すると、スケジュールの実行を待つことなくバックアップ操作が直ちに開始されます。

このタスクについて

通常、Hyper-V ホストまたはクラスターは、スケジュールの実行時にバックアップされます。ただし、バックアップ・スケジュールが未実行であったことに気付いた場合、または VM バックアップがエラーで完了した場合、アドホック・バックアップを開始できます。また、スケジュールされたバックアップ・サービスから除外された VM のアドホック・バックアップを開始することも可能です。

手順

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインで、ホストまたはクラスターをクリックします。
3. 「仮想マシン」ビューの VM 表で、VM をクリックします。
例えば、データ保護状況が「危険」である VM をクリックします。
4. 「アクション」ペインの VM セクションで「バックアップ」をクリックします。
5. 「アドホック・バックアップ」ウィンドウで以下のフィールドに入力します。

オプション	説明
バックアップ・タイプ	<p>実行するバックアップのタイプを選択します。</p> <p>差分 前回のバックアップ (フルまたは増分) 以降に変更されたブロックをバックアップします。最新の増分バックアップが前回のバックアップに追加されます。この VM のフルバックアップが存在しない場合は、自動的にフルバックアップが実行されます。そのため、フルバックアップが存在するかどうかを確認する必要はありません。</p> <p>完全 VM 全体のスナップショットがバックアップされます。フルバックアップが完了した後、追加でフルバックアップを行う必要はありません。</p>

オプション	説明
データ整合性	<p>Windows Server 2016 オペレーティング・システム上の Hyper-V ホストまたはクラスターでのみ使用可能です。</p> <p>スナップショットのタイプを選択し、バックアップ操作中に使用される方法を再試行します。</p> <p>常にアプリケーションと整合 バックアップが失敗する前に、アプリケーション整合バックアップを作成するために静止スナップショットを 2 回試行します。</p> <p>アプリケーション整合性を試行 静止スナップショットを 1 回試行し、最後に非静止のマシン整合スナップショットを 1 回試行します。</p> <p>マシン整合性のみ 静止スナップショットを完了できない VM に対して非静止スナップショットを 1 回だけ試行します。</p>
ディスク保護	<p>バックアップに組み込む VM ディスクを選択します。ディスクはディスク番号で識別されます。</p> <p>VM 内のすべてのディスクをバックアップするか、ディスク 1 のみをバックアップするか、ディスク 1 を除くすべてのディスクをバックアップすることができます。ディスク 1 には通常、オペレーティング・システムが含まれています。</p>

6. バックアップ操作を開始してウィンドウを閉じるには、「バックアップ」をクリックします。

タスクの結果

開始したバックアップ操作が、「仮想マシン」ビューまたは「スケジュール・ヒストリー」ビューの下部にあるタスク・リストに表示されます。

仮想マシンのリストア

IBM Spectrum Protect サーバー上にあるバックアップから仮想マシン (VM) をリストアすることができます。

このタスクについて

VM のリストア操作では、IBM Spectrum Protect サーバーに保管されている VM バックアップからリストアする前に、その VM はシャットダウンされて削除されます。リストア操作では、その後、バックアップの実行時と同じコンテンツおよび構成で VM が再作成されます。VM は削除される前にシャットダウンされますが、リストア操作を開始する前に手動で VM をシャットダウンして、進行中のアプリケーション・アクティビティを正常に停止することが推奨されます。

Data Protection for Microsoft Hyper-V 管理コンソールを使用して、データを新規 VM にリストアしたり、既存の VM をリストア・データで置き換えたりすることができます。

手順

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインで、クラスター・ビューまたはホスト・ビューのホストをクリックします。
3. 「仮想マシン」ビューの VM 表で VM を選択します。
例えば、データ保護状況が「正常」である VM をクリックします。

ヒント: 任意の VM で、削除されたにもかかわらず、そのバックアップが IBM Spectrum Protect サーバーで引き続き使用可能な VM をリストアする必要がある場合は、「削除済み」状況の VM を選択します。

4. 「アクション」ペインで、「リストア」をクリックします。

5. 該当する場合、「リストア」ウィザードで以下のページを完了します。ウィザードで選択するオプションによって、表示されるページが異なります。

ウィザード・ページ	アクション
始める前に	「次へ」をクリックして、ウィザードを開始します。
リストア・ポイントの選択	<p>カレンダーで強調表示された日付にリストア・ポイントが含まれます。リストア・ポイントは、リストア操作に使用できる VM バックアップです。一部の VM には、1 日あたり複数のリストア・ポイントがあります。</p> <p>「使用可能なリストア・ポイント」リストから日付とリストア・ポイントを選択してください。VM のサイズは、使用可能なリストア・ポイントの横にリストされます。VM は、バックアップされたときの状態にリストアされます。</p>
オプションの選択	<p>VM を作成するか、選択したリストア・ポイントからのデータで既存の VM を置き換えます。使用可能なオプションは次のとおりです。</p> <p>新規仮想マシンの作成 選択したリストア・ポイントからのデータで VM を作成します。このオプションがデフォルトです。</p> <p>既存の仮想マシンの置き換え 選択したリストア・ポイントからのデータで既存の VM を置き換えます。VM ID は維持されます。</p> <p>仮想マシン名 VM を作成する場合、新しい VM のデフォルト名は、元の VM 名にリストア操作の日付が付加されたものになります。デフォルト名を使用したくない場合は、Hyper-V ホストまたはクラスター内の別の VM でまだ使用されていない VM 名を入力フィールドに入力してください。</p> <p>既存の VM を置き換える場合、元の VM 名が表示されます。更新はできません。</p> <p>仮想マシンのリストア先 VM を作成する場合、その VM をリストアできる先のホストを選択します。</p> <p>既存の VM を置き換える場合、VM はその VM を所有するホストにリストアされます。このフィールドは選択可能ではありません。</p>
ストレージの選択	<p>このページが表示されるのは、リストア・ポイントからのデータを使用して VM を作成する場合のみです。</p> <p>VM を作成するホスト上の位置を入力します。デフォルトの位置は C:\ProgramData\Microsoft\Windows\Hyper-V\Virtual Machines です。</p>
要約	ウィザードで選択したオプションを確認します。「次へ」をクリックして、リストア操作を開始します。
結果	「完了」をクリックしてウィザードを閉じます。

タスクの結果

開始したリストア操作が、「仮想マシン」ビューまたは「スケジュール・ヒストリー」ビューの下部にあるタスク・リストに表示されます。

リストア操作が完了した後、選択した位置に VM がリストアされます。

次のタスク

クラスター内のホストの場合、削除済みの VM をリストアした場合、あるいは新しい VM 名で VM をリストアした場合は、Microsoft Failover Cluster Manager、System Center Virtual Machine Manager、または PowerShell コマンドレットを使用して、リストアした VM を高可用性のために構成する必要があります。高可用性のために VM を構成する方法については、Microsoft の資料を参照してください。

Data Protection for Microsoft Hyper-V のベスト・プラクティス

ベスト・プラクティスに従うと、Data Protection for Microsoft Hyper-V の操作の管理に役立つ機能を活用できます。

スケジュールされたバックアップ操作から仮想マシンを除外

仮想マシン (VM) で保守操作が行われる場合、または定期的にバックアップする必要がないテスト VM である場合、その VM をスケジュールされたバックアップ操作から除外できます。すべてのデータ・ムーバーでクライアント・オプション・ファイル (dsm.opt) を更新するのではなく、IBM Spectrum Protect サーバーのスケジュール定義で VM を除外することを検討してください。

IBM Spectrum Protect サーバー管理者がこのタスクを実行するには、サーバー上のスケジュール定義のオプション・ストリングに `-vm=vmname1,vmname2` パラメーターを追加します。

例えば、管理者は IBM Spectrum Protect サーバー上で以下のスケジュールを定義したとします。

```
define schedule hyperv_domain_name schedule_name
description=schedule_description action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=Hyper-V_host_hv_tgt -mode=IFIncremental
-domain.vmfull="all-vm"
```

testvm1 という名前の VM をスケジュールされたバックアップ操作から除外するには、次のようにスケジュール定義の `-domain.vmfull` オプションを更新します。

```
define schedule hyperv_domain_name schedule_name
description=schedule_description action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=Hyper-V_host_hv_tgt -mode=IFIncremental
-domain.vmfull="all-vm;-vm=testvm1"
```

名前 testvm で始まる 1 つ以上の VM を除外するには、次のようにスケジュール定義の `-domain.vmfull` オプションを更新します。

```
define schedule hyperv_domain_name schedule_name
description=schedule_description action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=Hyper-V_host_hv_tgt -mode=IFIncremental
-domain.vmfull="all-vm;-vm=testvm*"
```

`-domain.vmfull` オプションについて詳しくは、[177 ページの『Domain.vmfull』](#)を参照してください。

ヒント: システム構成によっては、ノード名に接頭部および接尾部を含めることもできます。詳細については、[18 ページの『ノード名のカスタマイズ』](#)を参照してください。

管理クラスへの仮想マシンの再バインド

クライアント・オプション・ファイルの vmmc オプションによって仮想マシン (VM) にバインドされた管理クラスをオーバーライドする必要がある場合は、`include.vm` オプションを使用して VM を新しい管理クラスにバインドできます。

クラスター環境では、すべてのホスト上のオプション・ファイル (dsm.opt) で、`include.vm` オプションを設定する必要があります。

例えば、テスト環境内の VM をバックアップする必要があるものの、STANDARD 管理クラスで指定されているテスト VM バックアップに同じ保存期間を設定したくないものとします。この場合、テスト VM をバックアップの保存期間が短い管理クラスに再バインドすることができます。

例えば、`testvm` で名前が始まるすべての VM を `NONPRODMC` という名前の管理クラスで再バインドするには、以下のステートメントをクライアント・オプション・ファイル (`dsm.opt`) に追加します。

```
include.vm vmtest* NONPRODMC
```

`include.vm` オプションの詳細と例については、[214 ページの『Vmmc』](#)を参照してください。

第5章 ファイル・リストア操作の概要

Web ベースのインターフェースから 管理者からの最小限の支援でファイルをリストアする場合、ファイル・リストア・インターフェースを使用できます。ファイル・リストア機能の構成後、管理者は、ファイル所有者またはヘルプ・デスク担当者にファイル・リストア URL を送信し、ファイルを見つけてリストアできるように支援します。

Web ベース・インターフェースでは、ファイルを手動でコピーするためのファイル・マネージャー・アプリケーションが不要です。ファイル所有者がファイルをリストアする際は、リストア・ポイントを指定して、ファイルを検索または参照して位置指定し、リストア操作を開始します。

構成が完了すると、ファイルにアクセスまたはリストアする際に管理者と対話する必要ありません。構成プロセス中に、管理者はファイル所有者に対して、ファイル所有者のデータが含まれている仮想マシン (VM) へのアクセス権を付与します。管理者がファイル・リストア・リソースをモニターできるように、そのデータはローカル VM 資格情報でアクセスできます。ファイル所有者の権限は管理する必要がありません。

どのユーザーも、ファイル・リストア・インターフェースで、IBM Spectrum Protect ファイル・リストア・インターフェースについて理解するためのデモンストレーション・ビデオを見ることができます。ファイル・リストア・インターフェースに最初にログオンすると、「Find and Restore Files」および「Monitoring Restores」のビデオが表示されます。ビデオは英語でのみ利用可能です。

関連概念

85 ページの『ファイル・リストア・タスク』

さまざまなタイプのユーザーが、ファイル・リストア機能をセットアップして使用します。ファイル所有者、ヘルプ・デスク担当者、および管理者が担当するタスク・セットはそれぞれ異なります。

関連タスク

88 ページの『ファイルをリストアするためのログイン』

IBM Spectrum Protect ファイル・リストア・インターフェースにログインし、管理者からの最小限の支援でファイルをリストアすることができます。

ファイル・リストア・タスク

さまざまなタイプのユーザーが、ファイル・リストア機能をセットアップして使用します。ファイル所有者、ヘルプ・デスク担当者、および管理者が担当するタスク・セットはそれぞれ異なります。

ファイル所有者

ファイル所有者は、仮想マシン (VM) 上にテキスト文書、スプレッドシート、およびプレゼンテーション・ファイルなどのビジネス・データを維持します。

ファイル所有者は、個々のファイルおよびフォルダーをリストアするために以下のタスクを実行します。

- 88 ページの『ファイルをリストアするためのログイン』
- 88 ページの『仮想マシン・バックアップからファイルのリストア』

ヘルプ・デスク担当者

ヘルプ・デスク環境の担当者は、ファイル所有者がデータをリストアする際に支援します。

ヘルプ・デスク担当者は、ファイル所有者に特定のファイル・リストア URL を提供するか、ファイル所有者に代わってファイルをリストアします。

ヘルプ・デスク担当者は、以下のタスクを実行します。

- ファイル・リストア URL をファイル・リストア管理者または Data Protection for Microsoft Hyper-V 管理コンソールから取得します。詳しくは、44 ページの『環境でファイル・リストア操作を使用可能にする』のステップ 5 を参照してください。
- 88 ページの『ファイルをリストアするためのログイン』

- [88 ページの『仮想マシン・バックアップからファイルのリストア』](#)

ファイル・リストア管理者

管理者は、Microsoft Hyper-V 環境における、ソフトウェアのインストール、IBM Spectrum Protect サーバーへの VM バックアップ操作のスケジュール、およびユーザー・アカウントと権限の管理を担当します。

管理者は、ファイル・リストア用に環境をセットアップするために、以下のタスクを実行します。

1. [44 ページの『環境でファイル・リストア操作を使用可能にする』](#)
2. Linux ゲスト VM でファイル所有者がファイル・リストア操作を実行する予定の場合は、以下のタスクを実行します。
 - a. [32 ページの『Linux マウント・プロキシー機能のインストール』](#)
 - b. [45 ページの『ファイル・リストア操作のための Linux マウント・プロキシーの構成』](#)
3. バックアップ操作が予期したとおりに実行されることを確認するには、スケジュールされたバックアップが実行されるまで待つか、または [VM のアドホック・バックアップ操作を実行](#)します。

ファイル・リストア操作用に環境の準備ができたなら、管理者は、以下のオプション・タスクを実行できます。

- [48 ページの『ファイル・リストア操作のオプションの変更』](#)
- [49 ページの『Data Protection for Microsoft Hyper-V ログ・アクティビティの構成』](#)

ファイル・リストア操作を使用する必要がなくなった場合、以下の手順に従って、ファイル・リストア機能を削除することができます。

- [36 ページの『ファイル・リストア機能の削除』](#)

ファイル・リストアの前提条件

IBM Spectrum Protect 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ます。

ファイル・リストア機能を有効にするには、Hyper-V ホスト・システムに IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V がインストールされている必要があります。

マウント・プロキシー・データ・ムーバーや ISCSI サービスを含めて、ファイル・リストア Web サービスと基礎の Data Protection for Microsoft Hyper-V 環境がインストールされ、構成され、作動可能でなければなりません。

Hyper-V 管理者は、ファイル・リストア Web インターフェースに接続するための URL をファイル所有者に提供する必要があります。構成ウィザードを使用して Data Protection for Microsoft Hyper-V を構成し、ファイル・リストア機能を使用可能にすると、ウィザードの終了時に URL が提供されます。詳細については、[39 ページの『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』](#)を参照してください。

Hyper-V 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 Hyper-V 仮想マシン (VM) に適用されます。

- ファイル・リストア操作中、VM が実行されている必要があります。
- Windows VM は、IBM Spectrum Protect バックアップ/アーカイブ・クライアントがインストールされている Hyper-V ホストと同じ Windows ドメインに属している必要があります。
- VM 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、VM 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、VM からファイルをリストアしようとししないでください。
- ユーザーがリストア対象のファイルを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。

- Linux ゲスト VM の場合、その VM に対するローカル・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、およびその他のネットワーク認証方式を介して利用することはできません。
- Red Hat Enterprise Linux 6 オペレーティング・システム上の Linux ゲスト VM では、**sshd** デーモン構成ファイル (/etc/ssh/sshd_config) 内の ChallengeResponseAuthentication オプションが 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。次のいずれかのステートメントを指定できます。

```
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

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 (バックアップ/アーカイブ・クライアント) が、Hyper-V ホスト・システムにインストールされます。

Hyper-V ホスト・システムは、リストアするファイルが含まれている VM 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・プロキシの前提条件

マウント・プロキシ・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・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 VM 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 オペレーティング・システムは、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を提供します。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・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。

Windows マウント・プロキシ・システムおよび Linux マウント・プロキシ・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。

- ネットワーク共有を作成してアクセスするために、ローカル管理者権限を持つ Windows ドメイン・ユーザーが必要です。管理者は、これらの資格情報を Data Protection for Microsoft Hyper-V 構成ウィザードに入力して、環境をファイル・リストア操作に使用可能にします。
- 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 VM 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 VM にログインしてファイルをリモート VM 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。
- 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への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・アカウントに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・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・リストア操作はサポートされません。ディスク・ストレージからファイルをリストアする方法を推奨します。

ファイルをリストアするためのログイン

IBM Spectrum Protect ファイル・リストア・インターフェースにログインし、管理者からの最小限の支援でファイルをリストアすることができます。

始める前に

ファイル・リストア・インターフェースの URL を管理者から取得していることを確実にしてください。

このタスクについて

このインターフェースにログインすると、ユーザーの都合のよいときにファイルを見つけてリストアすることができます。

手順

1. Web ブラウザーを開いて、管理者から受け取った URL を入力し、ファイル・リストア・インターフェースにアクセスします。
2. ファイルが含まれる仮想マシン (VM) のネットワーク名または IP アドレスを入力します。
例えば、myhost.mycompany.com のように入力します。
3. ファイルへのアクセスに使用するユーザー・アカウントを入力します。
 - Windows ゲスト・オペレーティング・システムの場合、Windows_domain_name¥user_name フォーマットを使用します。
 - Linux ゲスト・オペレーティング・システムの場合、Linux ゲスト VM へのログオンに使用するユーザー名を使用します。
4. ユーザー・アカウントのパスワードを入力して、「**ログイン**」をクリックします。

関連タスク

88 ページの『[仮想マシン・バックアップからファイルのリストア](#)』
ファイルを見つけて、希望の場所にリストアします。

仮想マシン・バックアップからファイルのリストア

ファイルを見つけて、希望の場所にリストアします。

始める前に

IBM Spectrum Protect ファイル・リストア・インターフェースにログインしていることを確認します。ファイルをリストアするには、事前にバックアップが存在する必要があります。

このタスクについて

オペレーティング・システム上に表示する権限を持っているファイルとディレクトリーのみが表示されます。

手順

1. 以下の手順を実行して、バックアップを選択します。
 - a) カレンダーの日付をクリックします。
 - b) 必要な場合、「**利用可能なバックアップ**」フィールドで時刻を選択します。
 - c) 「**バックアップの選択**」をクリックします。仮想マシンのディスクまたはディレクトリーが表に表示されます。
2. オプション: デフォルトのバックアップが必要とするものではない場合は、以下の手順を実行して、別のバックアップを選択します。
 - a) カレンダーをクリックします。
 - b) カレンダーの日付をクリックします。

c) 必要な場合は、時刻を選択します。

d) 「**バックアップの変更**」をクリックします。

制約事項: バックアップの日付または時刻を変更すると、行ったファイル選択がすべて失われます。ただし、新しいバックアップは、直前に探索したディレクトリーにロードされます。そのディレクトリーが利用不可の場合、バックアップはトップ・ディレクトリーにロードされます。

仮想マシンのディスクまたはディレクトリーが表に表示されます。

3. リストアするファイルを選択するには、以下の手順を実行します。

a) 表内のディスクまたはディレクトリーをクリックして、サブディレクトリーとファイルを表示します。

b) オプション: 現在のディレクトリーとサブディレクトリーでファイルを 検索するには、「**検索**」フィールドに名前を入力して、**Enter** を押します。その結果は、検出された順序で表示されます。

c) リストアする 1 つ以上のファイルとディレクトリーを選択します。

コンテンツが含まれないディレクトリーを選択した場合、空のディレクトリーはリストアされません。

4. ファイルをリストアする場所を選択します。

- ・ ファイルとディレクトリーを元の場所にリストアするには、「**復元先**」 > 「**元の場所**」を選択します。

- ・ ファイルとディレクトリーを別の場所にリストアするには、「**復元先**」 > 「**別の場所**」を選択します。


5. 選択を行った後、「**復元**」をクリックします。

別のディレクトリーにファイルをリストアする場合は、仮想マシン上の既存のディレクトリーを選択するか、リストアされたファイルを配置するディレクトリーを作成します。次に、「**リストア**」をクリックします。

同じ名前のファイルが存在する場合、リストアされたファイルの元の変更日時がファイル名に追加されます。同じファイルの後続のリストアでは、元の変更日時の後に数値 (*N*) が含まれます。

例: t2.2015-03-07-07-28-03_1.txt

次のタスク

リストア・アイコン () をクリックして、アクティブな最新のリストアに関する情報を表示します。デフォルトでは、情報は、リストアが完了してから 7 日間保持されます。

リストアがエラーまたは警告で終了した場合、「**詳細**」をクリックして、追加情報を表示します。エラーまたは警告情報を保存するには、「**エクスポート**」をクリックして、.CSV 形式で情報を保存します。

第 6 章 ゲスト内アプリケーションの保護

Data Protection for Microsoft Hyper-V を使用して、Microsoft Hyper-V 環境のゲスト仮想マシン内で稼働する Microsoft Exchange Server および Microsoft SQL Server を保護することができます。

Hyper-V 環境での Microsoft Exchange Server データの保護

Hyper-V ゲスト仮想マシン (VM) で実行されている Microsoft Exchange Server ワークロードの場合、ゲスト VM のアプリケーション整合バックアップを取得することができます。元のデータベースやメールボックスが損傷を受けたり、失われたりした場合に、データベース・レベルまたはメールボックス・レベルのバックアップをリカバリーできます。

Hyper-V 環境では、以下の製品が連携して Microsoft Exchange Server データを保護します。

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V バージョン 8.1.10
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Exchange Server バージョン 8.1.6 以降

これらのソフトウェア・オファリングが連携することで、Microsoft Exchange Server データのバックアップに他のソフトウェア製品が使用されていない場合に、Hyper-V 環境内の Microsoft Exchange Server データを保護します。

Microsoft Exchange Server のアプリケーション・データをバックアップおよびリストアするために必要な権限については、[技術情報 1647986](#) を参照してください。

Microsoft Exchange Server のアプリケーション保護のソフトウェア要件については、[技術情報 2017347](#) を参照してください。

Microsoft Active Directory のサポート：クラスター環境または非クラスター環境内の Hyper-V ホストとゲストは、同じ Active Directory インスタンスを使用する必要があります。ホストとゲストが別個の Active Directory インスタンスを使用することはできません。

Microsoft Exchange Server のアプリケーション保護のためのソフトウェアのインストールと構成

Microsoft Exchange Server データをホストするゲスト仮想マシン (VM) を保護するために、Hyper-V ホストおよびゲスト VM でインストールと構成のステップを完了する必要があります。ステップバイステップの指示を使用して、ゲスト内アプリケーションを保護できるようにご使用の環境を稼働させることができます。

始める前に

[技術情報 2017347](#) でソフトウェア要件を確認してください。

このタスクについて

以下の表には、その後のタスクで示される例として使用されている名前をリストしています。コマンドやオプションの例を使用する場合、その例は、使用している環境の該当する Hyper-V ホストとゲスト VM の名前に置き換えてください。

名前のタイプ	例
Hyper-V ホストまたはクラスターの名前	Kingston5
Microsoft Exchange Server をホストしているゲスト VM の名前	Kingston40

VM ゲスト上の Microsoft Exchange Server データを保護するために、Data Protection for Microsoft Hyper-V および Data Protection for Microsoft Exchange Server をインストール、セットアップ、および構成するには、以下の手順を実行します。

手順

1. 92 ページの『[ステップ 1 \(Hyper-V ホスト\): Data Protection for Microsoft Hyper-V のインストールおよび構成](#)』
2. 93 ページの『[ステップ 2 \(ゲスト VM\): Data Protection for Microsoft Exchange Server のインストールおよび構成](#)』
3. 95 ページの『[ステップ 3 \(Hyper-V ホスト\): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成](#)』
4. 98 ページの『[ステップ 4 \(ゲスト VM\): データベースのリストア](#)』
5. 99 ページの『[オプション: 仮想マシン名の変更後のアプリケーション保護の構成](#)』

ステップ 1 (Hyper-V ホスト): Data Protection for Microsoft Hyper-V のインストールおよび構成

Data Protection for Microsoft Hyper-V をインストールおよび構成して、Microsoft Exchange Server データをホストしているゲスト仮想マシン (VM) を正常にバックアップできることを確認します。

始める前に

Data Protection for Microsoft Hyper-V バージョン 8.1.2 以前からアップグレードする場合は、IBM Spectrum Protect サーバー上の既存の Hyper-V ノードの名前を `clustername_hv_tgt` (クラスターの場合) または `hostname_hv_tgt` (スタンドアロン・ホストの場合) に変更します。Hyper-V ノード名は、`asnodename` オプションで指定されたノード名です。

例えば、サーバー上の Hyper-V ノードの名前を `KINGSTON_HV_TGT` に変更します。詳しくは、[16 ページ](#)の『[IBM Spectrum Protect サーバー上のノードの名前変更](#)』を参照してください。

[14 ページ](#)の『[必要な通信ポート](#)』の説明に従って、ファイアウォールで通信ポートが開いていることを確認します。

手順

Hyper-V ホストまたはクラスターで、以下のタスクを実行します。

1. Data Protection for Microsoft Hyper-V をインストールします。

手順については、[22 ページ](#)の『[Data Protection for Microsoft Hyper-V の標準インストールの実行](#)』を参照してください。
2. 構成ウィザードを完了して Data Protection for Microsoft Hyper-V を構成します。

手順については、[39 ページ](#)の『[ウィザードを使用した Data Protection for Microsoft Hyper-V の構成](#)』を参照してください。

要確認: 「クラスターおよびホスト」ウィザード・ページに表示される、あるいは Data Protection for Microsoft Hyper-V 管理コンソールで「**アクション**」>「**プロパティ**」をクリックすると表示されるターゲット・ノード名を記録します。ターゲット・ノード名の末尾は `_HV_TGT` です。Data Protection for Microsoft Exchange Server で構成ウィザードを実行する場合は、ターゲット・ノード名が必要です。
3. Data Protection for Microsoft Hyper-V 管理コンソールを使用して、Microsoft Exchange Server をホストしている VM をバックアップします。

手順については、[79 ページ](#)の『[仮想マシンのアドホック・バックアップの開始](#)』を参照してください。
4. オプション: Exchange Server のデータベース可用性グループ (DAG) に属しているデータベースのパスシブ・コピーをバックアップします。`dsmc backup vm` コマンドを使用して、`vmpreferdagpassive yes` オプションを指定します。

通常はパスシブ・コピーのバックアップにより、実動データベース内のアクティブ・コピーのパフォーマンスへの影響が軽減されます。使用できる有効なパスシブ・コピーがない場合は、アクティブ・データベース・コピーがバックアップされます。

次のタスク

VM が正常にバックアップされたら、[93 ページの『ステップ 2 \(ゲスト VM\): Data Protection for Microsoft Exchange Server のインストールおよび構成』](#)に進みます。

関連情報

[Vmpreferdagpassive](#)

ステップ 2 (ゲスト VM): Data Protection for Microsoft Exchange Server のインストールおよび構成

Data Protection for Microsoft Exchange Server を使用してデータベースをバックアップできるようにするには、ステップを実行して Data Protection for Microsoft Exchange Server をインストールおよび構成し、Microsoft Exchange Server データベースをバックアップします。

始める前に

[92 ページの『ステップ 1 \(Hyper-V ホスト\): Data Protection for Microsoft Hyper-V のインストールおよび構成』](#)の手順を完了している必要があります。

Microsoft Exchange Server データベースおよびメールボックスが Hyper-V 仮想ディスク上でホストされていることを確認してください。

物理ハード・ディスク、独立ディスク、あるいはゲスト内 iSCSI を介してゲストに直接接続されたディスク上でホストされている Microsoft Exchange Server データベースがないことを確認します。

手順

Microsoft Exchange Server データをホストしているゲスト仮想マシン (VM) 上で以下のステップを実行します。

1. Data Protection for Microsoft Exchange Server をインストールします (まだインストールされていない場合)。

インストールの手順については、[IBM Spectrum Protect for Mail の製品資料](#)を参照してください。

ヒント: インストール手順の説明に従って、Data Protection for Microsoft Exchange Server 構成ウィザードを実行しないでください。このウィザードは、[ステップ 93 ページの『3』](#)で実行します。以前に Data Protection for Microsoft Exchange Server をインストールし、ウィザードを実行している場合は、[ステップ 93 ページの『3』](#)で再実行する必要があります。

2. Data Protection for Microsoft Hyper-V インストール・パッケージからデータ・ムーバー機能をインストールします。

インストール・ウィザードで拡張インストール・オプションを選択し、「**データ・ムーバー機能またはマウント・プロキシのインストール (Install the data mover feature or mount proxy)**」をクリックして、アプリケーション保護サポートをインストールします。

詳細については、[26 ページの『Data Protection for Microsoft Hyper-V データ・ムーバーのみのインストール』](#)を参照してください。

3. 「**スタート**」 > 「**DP for Exchange 管理コンソール**」をクリックし、Data Protection for Microsoft Exchange Server 管理コンソールを開きます。

構成ウィザードが自動的に開きます。

構成ウィザードが自動的に開始されない場合は、管理コンソールのツリー・ビューに移動し、「**IBM Spectrum Protect**」 > 「**ダッシュボード**」 > 「**管理 (Manage)**」 > 「**構成**」 > 「**ウィザード (Wizards)**」をクリックします。「**IBM Spectrum Protect 構成ウィザード (IBM Spectrum Protect Configuration Wizard)**」をダブルクリックします。

4. 構成ウィザードの「**IBM Spectrum Protect ノード名 (IBM Spectrum Protect Node Names)**」ページで、VSS リクエスター、Data Protection for Microsoft Exchange Server、および Hyper-V ターゲット・ノードの名前をそれぞれのフィールドに入力します。「**DP Exchange VSS サポートを構成しない (Do not configure DP Exchange VSS Support)**」チェック・ボックスがクリアされていることを確認します。

以下の表に構成手順で使用されるノード名の例が示されています。

フィールド名	ノード名の例
VSS リクエスター	KINGSTON40_VSS
Data Protection for Exchange	KINGSTON40_EXC
Hyper-V ターゲット・ノード	KINGSTON5_HV_TGT

5. 構成ウィザードの「**IBM Spectrum Protect サーバー設定 (IBM Spectrum Protect Server Settings)**」ページで、以下のいずれかのステップを実行します。

- ウィザードを使用して IBM Spectrum Protect サーバーを構成する場合は、「**検討**」または「**編集**」を選択し、必要に応じてマクロを更新します。
- 手動でサーバーを構成するには、以下の手順を実行します。
 - ウィザードの最後のページで、マクロ・ファイルを開くリンクをクリックします。
 - マクロ・ファイルを更新して実行するか、マクロから適切なコマンドを発行します。その際に使用するコマンドは、ご使用の環境に必要なコマンドに合わせて調整してください。

例えば、fcm_pdexc という名前のポリシー・ドメインを使用するためにセットアップするとします。C:\¥Program Files¥Tivoli¥TSM¥baclient フォルダーから **dsmadmc** コマンドを実行し、次のコマンドを発行します。

```
register node KINGSTON40_VSS T_3_m_p_P_w userid=KINGSTON40_VSS
update node KINGSTON40_VSS T_3_m_p_P_w backdelete=yes force=yes
```

```
register node KINGSTON40_EXC T_3_m_p_P_w domain=fcm_pdexc
userid=KINGSTON40_EXC
update node KINGSTON40_EXC T_3_m_p_P_w backdelete=yes domain=fcm_pdexc
force=yes
```

```
grant proxynode target=KINGSTON40_EXC agent=KINGSTON40_VSS
```

force=yes オプションは、初回アクセス時に強制的にパスワードをリセットします。

場合によっては **dsmadmc** コマンドの実行時に次のエラー・メッセージが表示されます。

```
ANS1592E SSL プロトコルの初期化に失敗しました
```

このメッセージが表示された場合、使用している IBM Spectrum Protect サーバー管理者アカウントで **sessionsecurity** オプションが **transitional** に設定されていることを確認してください。

例えば、IBM Spectrum Protect サーバーにアクセスできるリモート・コンピューターから次のコマンドを発行します。

```
update admin myAdmin sessionsecurity=transitional
```

- 構成ウィザードを完了します。
- Data Protection for Microsoft Exchange Server 管理コンソールから次のようにデータベースをバックアップします。
 - 「**アクション**」ペインで、「**バックアップの宛先**」 > 「**TSM**」をクリックします。
 - 「**アクション**」ペインで、「**フルバックアップ**」をクリックします。
- オプション: メールボックスの履歴とデータベース・バックアップ内のメールボックスのロケーション情報に整合性が保たれるように、メールボックスの履歴情報を手動で更新します。

手順については、[101 ページの『Microsoft Exchange Server バックアップのメールボックス情報の更新』](#)を参照してください。

次のタスク

VSS バックアップが正常に完了したら、[95 ページの『ステップ 3 \(Hyper-V ホスト\): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成』](#)に進みます。

ゲスト VM 上のデータについて発生する可能性のあるリストアの問題を回避するために、[189 ページの『データ・ムーバーからアプリケーション保護バックアップをリストアする場合のシャドー・コピーの考慮事項』](#)の情報を確認してください。

ステップ 3 (Hyper-V ホスト): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成

Microsoft Exchange Server データをホストしているゲスト仮想マシン (VM) を保護するために、Data Protection for Microsoft Hyper-V を構成します。VM をバックアップし、バックアップ操作が正常に完了したことを確認します。

始める前に

[93 ページの『ステップ 2 \(ゲスト VM\): Data Protection for Microsoft Exchange Server のインストールおよび構成』](#)の手順を完了している必要があります。

Microsoft Exchange Server データベースをホストしている仮想ハード・ディスク (VHDX) が VM バックアップ操作から除外されていないことを確認します。手順については、[102 ページの『Microsoft Exchange Server ボリュームが仮想マシン・バックアップで除外されていないことの確認』](#)を参照してください。

オプション: バックアップ操作時には、ゲスト VM に対する統合サービスまたはゲスト・サービス・インターフェースが自動的に有効になります。手動で有効にする必要はありません。ただし、現行の状況を確認する場合、あるいは「**ゲスト・サービス (Guest Services)**」サービスを明示的に有効にする場合は、Hyper-V ホストまたはクラスターで以下のいずれかの方法を使用します。

- Hyper-V Manager から、以下を行います。
 1. VM を右クリックし、「設定」 > 「統合サービス」をクリックします。
 2. 「統合サービス」ウィンドウで、「**ゲスト・サービス (Guest Services)**」チェック・ボックスが選択されていることを確認します。
- 管理者として、PowerShell コマンド・プロンプトから、次のコマンドを発行します。

```
Get-VMIntegrationService -VMName Kingston40 `
Enable-VMIntegrationService -VMName Kingston40 -Name "Guest Service Interface"
```

このタスクについて

Microsoft Exchange Server をホストしている VM をバックアップする場合、Data Protection for Microsoft Hyper-V はアプリケーション整合性を提供します。これらのバックアップを使用して、整合した状態で VM をリカバリーすることができます。

このタイプのバックアップから、VM 全体をリカバリーすることなく選択したデータベースまたはメールボックスのみをリストアするには、VM スナップショットおよびバックアップの作成時に Microsoft Exchange Server の状態に関する情報を保存する必要があります。この情報は、VM のスナップショットの作成時に行われる Microsoft Volume Shadow Copy Services (VSS) 対話の一部として収集されます。

アプリケーション保護バックアップをリストアする場合のシャドー・コピーの考慮事項:

通常、シャドー・ストレージはボリュームの一部です。ただし、シャドー・ストレージ・スペースが、デフォルトで、または手動構成の結果として、別のボリューム上に構成される場合があります。この場合、VM バックアップ操作中に作成されたシャドー・コピーがリストア時に使用できないので、データベースのリストア操作は失敗することがあります。

バックアップ操作を開始する前に、[189 ページの『アプリケーション保護リストア中にはリストアされたボリュームでシャドー・コピーが使用可能でなければならない』](#)に記載されている情報を確認します。

Data Protection for Microsoft Hyper-V で Microsoft Exchange Server の Microsoft VSS メタデータを収集するには、バックアップ操作中に VM からこの情報を取得するように Data Protection for Microsoft Hyper-V を構成する必要があります。

この手順では、Microsoft Hyper-V Manager に示されているように、Kingston40 が Hyper-V ホストの例です。Kingston5 は、Microsoft Exchange Server をホストするゲスト VM の名前の例です。

Kingston40_vss は、Data Protection for Microsoft Exchange Server のインストール時に作成されるクライアント・ノードの名前です。これらの例は、使用している環境に合った適切な値に置き換えてください。

手順

別途指示された場合を除き、Hyper-V ホストまたはクラスターで以下のステップを実行します。

1. baclient フォルダーから、Microsoft Exchange Server をホストしているゲスト VM 用の Windows 資格情報を以下のように設定します。

- 特定の VM の資格情報を設定するには、コマンド・プロンプトで baclient フォルダーから次のコマンドを発行します。

```
dsmc set password -type=vmguest guest_VM_name "guest_admin_ID" guest_admin_pw  
-optfile=dsm.hostname_HV_DM.opt
```

- 特定の資格情報が設定されていないすべての VM の資格情報を設定するには、次のようにします。

```
dsmc set password -type=vmguest allvm "guest_admin_ID" guest_admin_pw  
-optfile=dsm.hostname_HV_DM.opt
```

ここで、

vmname

Microsoft Exchange Server をホストするゲスト VM の名前。この名前は、Hyper-V Manager で表示される VM 名です。

guest_admin_ID

ゲスト VM の管理者 ID。guest_admin_ID は、Windows のドメイン・アカウントまたはローカル・アカウントにすることができます。例えば、次のとおりです。

- ドメイン・アカウントの場合、domain\username 形式を使用します。
- ローカル・アカウントの場合、username 形式を使用します。

guest_admin_pw

ゲスト VM の管理者 ID のパスワード。

hyperv_hostname

Hyper-V ホストまたはクラスターの名前。

例えば、次のとおりです。

```
dsmc set password -type=vmguest Kingston40 "world¥alan" "@lanPwd!"  
-optfile=dsm.KINGSTON5_HV_DM.opt
```

set password コマンドで使用されるアカウントは、Hyper-V ホストまたはクラスターと、Exchange Server データをホストするゲスト VM の両方で有効でなければなりません。

dsmc set password コマンドは、データ・ムーバーをホストするシステム上で暗号化された、ゲスト VM 資格情報を保管します。ゲスト VM の管理者 ID およびパスワードには、以下の最小権限が必要です。

バックアップ権限: Microsoft Exchange Server 2013 および 2016: 「組織の管理」権限 (管理役割グループ「組織の管理」のメンバーシップ)。

2. baclient フォルダーから、アプリケーション保護のためにデータ・ムーバー・オプション・ファイルを構成します。

- a) データ・ムーバー・オプション・ファイル (dsm.hostname_HV_DM.opt) を編集のために開きます。例えば、次のコマンドを発行します。

```
notepad dsm.KINGSTON5_HV_DM.opt
```

- b) include.vmtsmvss guest_vm_name オプションを追加します。guest_vm_name パラメーターには、ワイルドカード文字を含めることができます。例えば、次のとおりです。


```
include.vmtsmvss Kingston40
```

または

```
include.vmtsmvss Kingston*
```

3. データベース・バックアップを Data Protection for Microsoft Exchange Server に表示できるようにするには、ゲスト VM で以下のステップを実行します。

- a) PowerShell コマンド・プロンプトで次のコマンドを実行して、ゲスト内で資格情報ファイルを生成し、プロンプトで指示されたらドメイン・ユーザー名 (*domain name¥user name*) とパスワードを入力します。

```
Get-Credential | Export-Clixml -Path `
"C:\program files\Tivoli\TSM\baclient\dsmcreds.xml"
```

ドメイン・ユーザーには、Exchange リストア権限が必要です。

- b) ゲスト VM で Exchange 管理シェルで次のコマンドを実行して、資格情報を検証します。

```
$cred = Import-CliXml -Path `
"C:\program files\Tivoli\TSM\baclient\dsmcreds.xml"
$Session = New-PSSession -Credential $cred -ConfigurationName `
Microsoft.Exchange -ConnectionUri `
http://<Exchange_server_name>/PowerShell?serializationLevel=Full `
-Authentication Kerberos
Import-PSSession -Session $Session
Get-MailboxDatabase -Server <Exchange_server_name>
```

メールボックス・データベースのリストが正しく表示されます。

4. Hyper-V ホストの baclient フォルダーから、**dsmc backup vm** コマンドを発行してゲスト VM をバックアップします。

例えば、次のとおりです。

```
dsmc backup vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt
-asnode=KINGSTON5_HV_TGT
```

5. **dsmc query vm** コマンドを実行して、バックアップ操作を確認します。VM 名は大/小文字を区別します。

例えば、baclient フォルダーから次のコマンドを発行します。

```
dsmc query vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt
-asnode=KINGSTON5_HV_TGT -detail
```

出力には、以下の例のようなテキストが含まれます (ただし、Microsoft Exchange Server のバージョンが異なる場合があります)。

```
Application protection type: TSM VSS
Application(s) protected: Microsoft Exchange Server 2016
```

6. baclient フォルダーから **dsmc set access** コマンドを使用して、ゲスト VM 上の VSS ノードが VM バックアップにアクセスしてリストアできるように許可します。

例えば、次のコマンドを発行します。

```
dsmc set access backup -type=vm Kingston40 kingston40_vss
-nodename=KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
```

ここで、Kingston40 は Microsoft Hyper-V マネージャーに表示されるゲスト VM の名前、kingston40_vss は Data Protection for Microsoft Exchange Server のインストール時に作成される IBM Spectrum Protect ノードです。このノード名は、Kingston40 VM 上のファイル C:¥Program Files¥Tivoli¥TSM¥baclient¥dsm.opt に示されています。

次の **dsmc query access** コマンドを発行すると、ノードがアクセスできる VM バックアップが表示されます。例えば、次のとおりです。

```
dsmc query access -nodename=KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
```

次のタスク

バックアップ操作が正常に完了したら、[98 ページの『ステップ 4 \(ゲスト VM\): データベースのリストア』](#)に進みます。

関連資料

[153 ページの『Backup VM』](#)

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

[187 ページの『INCLUDE.VMTSMVSS』](#)

関連情報

[Set Access](#)

[パスワードの設定](#)

ステップ 4 (ゲスト VM): データベースのリストア

アプリケーション保護が適切に構成されていることを検証するには、Data Protection for Microsoft Exchange Server でデータベースをリストアします。

始める前に

[95 ページの『ステップ 3 \(Hyper-V ホスト\): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成』](#)の手順を完了している必要があります。

ゲスト仮想マシン (VM) 上で以下の必要なサービスが稼働していることを確認します。

1. コマンド・プロンプトで、次のコマンドを発行します。

```
services.msc
```

2. サービスのリストで、「**IBM Spectrum Protect Recovery Agent サービス**」を見つけ、必要な場合はサービスを開始します。
3. サービスのリストで、「**Microsoft iSCSI Initiator Service**」を見つけます。必要に応じて、スタートアップの種類を「**自動**」に変更し、サービスを開始します。

手順

ゲスト VM で、以下の手順を実行します。

1. Data Protection for Microsoft Exchange Server 管理コンソールを開始します。
2. ツリーで「**Exchange Server**」インスタンスを選択します。
3. 「**リカバリー (Recover)**」タブにナビゲートし、「**最新表示**」をクリックします。
4. 「**VMVSS**」バックアップ方式のあるデータベース項目を選択します。
5. 「**アクション**」ペインで、「**リストア**」をクリックします。
6. リストア操作が完了したら、データベースおよび関連するメールボックスを確認します。

次のタスク

必要に応じてバックアップを管理し、データをリカバリーできるようになりました。詳しくは、以下を参照してください。

- [100 ページの『バックアップ操作の管理』](#)
- [103 ページの『データのリストア』](#)

アプリケーション保護のための構成ステップの完了後にゲスト VM の名前を変更した場合は、新しい VM 名でソフトウェアを再構成する必要があります。手順については、99 ページの『オプション: 仮想マシン名の変更後のアプリケーション保護の構成』を参照してください。

オプション: 仮想マシン名の変更後のアプリケーション保護の構成

アプリケーション保護構成の完了後にゲスト仮想マシン (VM) の名前を変更した場合、名前変更されたゲスト VM で Data Protection for Microsoft Hyper-V を再構成する必要があります。

始める前に

Microsoft Exchange Server をホストするゲスト VM を保護するためのソフトウェアのインストールおよび構成が完了している必要があります。

このタスクについて

このタスクは、アプリケーション保護によって保護されているゲスト VM の名前を変更した場合にのみ実行してください。

手順

1. Hyper-V ホストまたはクラスター上のデータ・ムーバーで、次のコマンドを発行します。

```
dsmc set password -type=vmguest new_vmguest_displayname  
guest_admin_ID guest_admin_pw
```

ここで、

new_vmguest_displayname

Microsoft Exchange Server をホストする新しいゲスト VM の名前。この名前は、Hyper-V Manager で表示される VM 名です。

guest_admin_ID

新しいゲスト VM の管理者 ID。guest_admin_ID は、Windows のドメイン・アカウントまたはローカル・アカウントでなければなりません。例えば、次のとおりです。

- ドメイン・アカウントの場合、domain\username 形式を使用します。
- ローカル・アカウントの場合、username 形式を使用します。

guest_admin_pw

新しいゲスト VM の管理者 ID のパスワード。

2. データ・ムーバー・オプション・ファイル (dsm.hostname_HV_DM.opt) で、次のように include.vmtsmvss オプションを更新します。

```
include.vmtsmvss new_vmguest_displayname
```

ここで、new_vmguest_displayname は Hyper-V Manager での新しいゲスト VM の表示名です。ワイルドカード文字を使用することができます。

3. Data Protection for Microsoft Hyper-V 管理コンソールを使用するか、コマンド・プロンプトから次のコマンドを発行して、データ・ムーバーの baclient フォルダーから新しいゲスト VM をバックアップします。

```
dsmc backup vm new_vmguest_displayname -optfile=dsm.hostname_HV_DM.opt  
-asnode=hostname_HV_TGT
```

4. baclient フォルダーから **dsmc set access** コマンドを使用して、新しいゲスト VM 上の VSS ノードが VM バックアップにアクセスしてリストアできるように許可します。
例えば、次のコマンドを発行します。

```
dsmc set access backup -type=VM new_vmguest_displayname vss_requestor_node  
-optfile=dsm.hostname_HV_DM.opt
```

ここで、

new_vmguest_displayname

Hyper-V Manager での新しいゲスト VM の表示名。

vss_requestor_node

Data Protection for Microsoft Exchange Server で構成された VSS リクエスターの名前。

hostname

Data Protection for Microsoft Hyper-V がインストールされている Hyper-V ホストまたはクラスターの名前。

5. オプション: VSS リクエスター・ノードは古い VM 名でバックアップされた VM へのアクセス権を既に持っているため、Data Protection for Microsoft Exchange Server 管理コンソールには、古い VM と新しい VM のどちらからバックアップされた VMVSS データベースも表示されます。

古い VM 名を持つ VM バックアップにアクセスしたくない場合は、古い VM バックアップへのアクセス権を削除する必要があります。Hyper-V ホスト上のデータ・ムーバーから、次のコマンドを発行します。

```
dsmc del access -optfile=dsm.hostname_HV_DM.opt -asnode=hostname_HV_TGT
```

アクセス・リストが表示されます。アクセス・リストから削除したい項目に対応する索引を入力します。

IBM Spectrum Protect サーバー上のスペースを節約したい場合は、**dsmc delete filespace** コマンドを発行して、古い VM のバックアップ・データが含まれるファイル・スペースを削除することができます。

重要: ファイル・スペースを削除すると、そのファイル・スペース内のすべてのバックアップ・バージョンが削除され、データをリストアすることはできなくなります。古い VM バックアップを削除する前に、そのデータが不要であることを確認してください。

バックアップ操作の管理

Microsoft Exchange Server データを保護するために環境を構成した後、仮想マシン (VM) のバックアップを個々にスケジュールすることができます。また、VM 上の Exchange Server データベース・バックアップ内のメールボックス情報を更新することができます。

仮想マシン・バックアップのスケジューリング

ご使用のデータの定期的な保護が確実に行われるように、仮想マシン (VM) バックアップをスケジュールします。

始める前に

Microsoft Exchange Server データベースをホストしている VM のバックアップを行う前に、データベースをマウントしてください。

デフォルトでは、バックアップ操作で仮想ハード・ディスク (VHDX) に許可される最大サイズは 2 TB に設定されています。ただし、`vmmaxvirtualdisks` オプションを使用して最大サイズを 8 TB まで増やすことができます。詳細については、[213 ページの『Vmmaxvirtualdisks』](#)を参照してください。

このタスクについて

Data Protection for Microsoft Hyper-V は、バックアップ処理を行う際に、データベース可用性グループ (DAG) 内の、取り外された状態、破損した状態、中断された状態、または正常ではない状態のゲスト Microsoft Exchange Server データベースをバイパスします。このような状態のデータベースは、VM のバックアップから除外され、リストアに使用できません。

手順

1. Data Protection for Microsoft Hyper-V 管理コンソールを開始します。
2. ナビゲーション・ペインで、スタンドアロン・ホストまたはクラスターをクリックします。
3. 「アクション」ペインで、「バックアップ管理」をクリックします。

4. 「バックアップ管理」ウィンドウでスケジュールを選択し、「スケジュールの割り当て」をクリックします。
5. ウィンドウを閉じるには、「クローズ」をクリックします。
6. スケジュールのソースに Microsoft Exchange Server をホストしている VM が含まれていることを確認します。
7. 以下のいずれかのサービスが稼働していることを確認します。
 - ・ クライアント・アクセプター (CAD) によって管理されているスケジューラーを使用する場合は、データ・ムーバー上でクライアント・アクセプター・サービスが稼働していることを確認してください。
 - ・ スタンドアロンのスケジューラーを使用する場合、そのスケジューラーのサービスが稼働していることを確認してください。

関連タスク

75 ページの『[ホストまたはクラスターのマシンのバックアップ・スケジュールの管理](#)』

スケジュールを選択して、Hyper-V ホストまたはクラスター内の VM を自動的にバックアップする頻度および時点を指定することができます。

Microsoft Exchange Server バックアップのメールボックス情報の更新

Microsoft Exchange Server データをホストしている仮想マシン (VM) をバックアップする際に、VM 上で Data Protection for Microsoft Exchange Server が検出されると、VM のバックアップとともにメールボックス履歴が自動的にアップロードされます。

このタスクについて

Data Protection for Microsoft Exchange Server が VM にインストールされていない限り、メールボックス履歴情報は Exchange Server データベースのバックアップ操作で自動的に更新されません。メールボックス履歴の自動アップロードは、dsm.opt ファイルで VMBACKUPMAILBOXHISTORY No を指定することで、無効にすることができます。

Data Protection for Microsoft Exchange Server コマンド・ライン・インターフェースを使用して、メールボックス履歴情報を手動で更新できます。

ヒント : Microsoft Exchange サーバーが入っている VM をバックアップする前に、このタスクを実行してください。こうすると、データベース・バックアップのメールボックス履歴とメールボックスのロケーション情報の一貫性を確保できます。

手順

Exchange Server データをホストしているゲスト VM で、以下のステップを実行します。

1. Exchange Server データベース・バックアップのメールボックス履歴情報のみを更新するには、次の例のように、**backup /UpdateMailboxInfoOnly** コマンドを発行します。

```
tdpexcc backup DB1 full /UpdateMailboxInfoOnly
```

ここで、DB1 はデータベース名、full はデータベース・バックアップのタイプです。

ヒント : Exchange 組織のすべてのメールボックスに関する情報を更新するには、データベース名としてアスタリスク (*) 文字を指定します。

2. オプション: 以下の手順を実行して、メールボックス情報が正しく更新されていることを確認します。
 - a) 次の例に示すように、**query /SHOWMAILBOXInfo** コマンドを発行して、IBM Spectrum Protect サーバー上のデータベース・バックアップのメールボックス情報を確認します。

```
tdpexcc query tsm /showmailboxinfo
```

- b) Microsoft 管理コンソール (MMC) を開始して、「メールボックスのリストア」ビューまたは「メールボックスのリストア・ブラウザー」ビューで、リストア対象として選択可能な更新済みメールボックスのリストを確認します。

バックアップの検証

バックアップを作成した後、Data Protection for Microsoft Exchange Server インターフェースから 仮想マシン・バックアップおよびデータベース・バックアップを照会できることを確認します。

手順

1. Microsoft 管理コンソール (MMC) から、Microsoft Exchange Server を選択します。
2. 「リカバリー」タブをクリックします。
3. 「表示」>「データベース」を選択します。 リストアできる Microsoft Exchange Server データベース・バックアップのリストが表示されます。

Data Protection for Microsoft Hyper-V を使用してバックアップされた Microsoft Exchange Server データベースは、vmvss バックアップ・メソッドとして識別されます。

Microsoft Exchange Server ボリュームが仮想マシン・バックアップで除外されていないことの確認

Hyper-V 仮想ハード・ディスク (VHDX) 内のボリュームには、Data Protection for Microsoft Hyper-V バックアップ処理から除外されていない Microsoft Exchange Server データベースが入っている必要があります。

始める前に

データベースが以下のタイプのディスク 上にないことを確認します。

- 物理ディスク
- 独立ディスク
- iSCSI 経由でゲスト・オペレーティング・システムに直接接続されているディスク

手順

1. 仮想マシン (VM) のバックアップに使用される Data Protection for Microsoft Hyper-V データ・ムーバー上のオプション・ファイル内の EXCLUDE.VMDISK ステートメントが、Microsoft Exchange Server ファイル、ファイル・スペース、データベース、およびメールボックスが含まれるボリュームをホストしている VHDX を誤って除外していないことを確認します。

例えば、次のとおりです。

- kingston40.vhdx ファイルには論理ボリューム C: が含まれます。
 - kingston40.vhdx ファイルには論理ボリューム E: および F: が含まれます。
 - kingston40_1.vhdx のディスク・ロケーション (IDE コントローラー番号およびデバイス・ロケーション) は IDE 1 0 です。
 - kingston40_2.vhdx のディスク・ロケーションは IDE 1 1 です。
 - バックアップする Microsoft Exchange Server データベース・ファイルは、E: ドライブおよび F: ドライブにあります。
2. データ・ムーバーに以下のステートメントあるいは同様のステートメントが含まれていないことを確認することで、VM バックアップから kingston40_2.vhdx を除外するステートメントがないことを確認します。

```
EXCLUDE.VMDISK KINGSTON40 "IDE 1 1"
```

```
EXCLUDE.VMDISK * "IDE 1 1"
```

あるいは、ほとんどのハード・ディスクを除外する場合は、以下のいずれかのステートメントを使用して、VM ディスクを明示的に組み込む必要があります。

```
INCLUDE.VMDISK KINGSTON40 "IDE 1 1"
```

```
INCLUDE.VMDISK * "IDE 1 1"
```


Include ステートメントと Exclude ステートメントは、dsm.opt ファイルに表示されているとおり、下から上に処理されます。目的を達成するには、ステートメントを正しい順序で入力します。

以下のように、コマンド・ライン・インターフェースから、VM ディスクの除外と組み込みを指定できます。

```
dsmc backup vm "KINGSTON40:-vmdisk=IDE 1 1" -asnode=KINGSTON5_HV_TGT
```

関連資料

[180 ページの『Exclude.vmdisk』](#)

EXCLUDE.VMDISK オプションは、仮想マシン・ディスクをバックアップ操作から除外します。

[184 ページの『Include.vmdisk』](#)

INCLUDE.VMDISK オプションは、バックアップ操作に仮想マシン (VM) ディスクを組み込みます。ディスク・ラベルを指定しない場合は、VM のすべてのディスクがバックアップされます。

データのリストア

アプリケーション保護機能が有効な仮想マシンをバックアップすると、元のデータベースやメールボックスが失われたり、損傷を受けたりした場合にこれらをリカバリーできます。

リカバリー操作は、Data Protection for Microsoft Hyper-V バックアップから Microsoft Exchange Server データベースまたはメールボックスのフルバックアップをリストアします。

仮想マシン (VM) 全体をリストアすると、VM 上のすべての Microsoft Exchange Server データベースおよびメールボックスがリストアされ、VM バックアップが行われた時点にリカバリーされます。

Microsoft iSCSI Initiator Service の開始

リカバリー操作に使用されるディスクをマウントするには、iSCSI プロトコルが使用されます。Microsoft iSCSI Initiator Service を開始して、データがリストアされるシステムの「スタートアップの種類」を「自動」に設定するようにします。

手順

Windows の「サービス」で、以下のステップを実行します。

1. 「サービス」リストで「**Microsoft iSCSI Initiator Service**」を右クリックします。
2. 「プロパティ」をクリックします。
3. 「全般」タブで、以下のオプションを設定します。
 - a) 「スタートアップの種類」リストで、「自動」を選択します。
 - b) 「開始」をクリックしてから「OK」をクリックします。

タスクの結果

「サービス」リストに、「**Microsoft iSCSI Initiator Service**」が、状況は「開始」、スタートアップの種類は「自動」で表示されます。

グラフィカル・ユーザー・インターフェースを使用したデータベース・バックアップのリストア

Data Protection for Microsoft Exchange Server グラフィカル・ユーザー・インターフェースを使用して、仮想マシン (VM) バックアップから Microsoft Exchange Server のフル・データベース・バックアップをリカバリーすることができます。

始める前に

バックアップ方式「VMVSS」を使用して Microsoft Exchange Server データベースをリストアする前に、Microsoft iSCSI Initiator Service が稼働していることを確認してください。このサービスが稼働していない場合は、サービスを開始します。手順については、[103 ページの『Microsoft iSCSI Initiator Service の開始』](#)を参照してください。

手順

1. VM からフル・データベース・リカバリーを開始するには、Data Protection for Microsoft Exchange Server 管理コンソール (MMC) を開始します。
2. ナビゲーション・ペインで、「データの保護およびリカバリー」ノードを展開して、Microsoft Exchange Server サーバーを選択します。
3. 「リカバリー」タブで、「データベースのリストア」を選択します。すべてのバックアップ (VM バックアップからのすべてのデータベース・バックアップを含む) がリストされます。
4. リストアするフル・データベース・バックアップを選択します。
5. 「アクション」ペインで、「リストア」をクリックします。

別の仮想マシンのバックアップのリストア

Data Protection for Microsoft Exchange Server を使用して、IBM Spectrum Protect サーバー 上の別の仮想マシン (VM) のバックアップにアクセスし、バックアップをリストアすることができます。

このタスクについて

データベースおよびメールボックスのバックアップを元のバックアップ・ノードとは異なるデータベース可用性グループ (DAG) ノードにリストアすることができます。

以下のシナリオでは、ご使用の仮想環境に Exchange VM の vm1 と vm2 があることを前提としています。

vm1 と vm2 上のデータベースおよびメールボックスのバックアップにアクセスしてリストアするために、vm2 上の Data Protection for Microsoft Exchange Server を使用可能にすることにします。

手順

1. vm1 と vm2 上の Microsoft Exchange Server データを保護するために、自己完結型アプリケーション保護を構成します。

手順については、以下を参照してください。

- [92 ページの『ステップ 1 \(Hyper-V ホスト\): Data Protection for Microsoft Hyper-V のインストールおよび構成』](#)
- [95 ページの『ステップ 3 \(Hyper-V ホスト\): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成』](#)

2. Hyper-V ホスト上で、データ・ムーバーのコマンド・ライン・インターフェースで **dsmc backup vm** コマンドを実行して vm1 および vm2 をバックアップします。
3. vm2 上で、Data Protection for Microsoft Exchange Server をインストールし、Hyper-V 環境での Exchange Server データ保護用にソフトウェアを構成します。

手順については、[93 ページの『ステップ 2 \(ゲスト VM\): Data Protection for Microsoft Exchange Server のインストールおよび構成』](#)を参照してください。

4. Hyper-V ホストで、vm2 上の Data Protection for Microsoft Exchange Server が vm1 および vm2 上のバックアップにアクセスできるようにするには、次の例に示すように **set access** コマンドを発行します。

```
dsmc set access backup -type=vm vm1 vm2_vss
```

```
dsmc set access backup -type=vm vm2 vm2_vss
```

5. vm2 または vm1 上のデータベースまたはメールボックスのバックアップをリストアします。

メールボックス・データのリストア

Data Protection for Microsoft Exchange Server は、メールボックス・データをデータベース・レベルでバックアップします。また、データベース・バックアップから個々のメールボックス項目をリストアします。

メールボックス・データのリストア、再配置および削除されたメールボックスのリストア、Mailbox Restore Browser を使用した対話式でのメールボックス・メッセージのリストアの各手順については、[IBM Spectrum Protect for Mail 製品資料](#)を参照してください。

コマンド・ライン・インターフェースを使用したデータのリストア

必要な場合、Data Protection for Microsoft Exchange Server コマンド・ライン・インターフェースを使用して、仮想マシンから Microsoft Exchange Server のフル・データベース・リカバリーを開始できます。

始める前に

バックアップ・タイプ「VMVSS」を使用して Microsoft Exchange Server データベースをリストアする前に、Microsoft iSCSI Initiator Service が稼働していることを確認してください。このサービスが稼働していない場合は、サービスを開始します。手順については、[103 ページの『Microsoft iSCSI Initiator Service の開始』](#)を参照してください。

手順

1. **query** コマンドを発行して、データベースのフルバックアップを検索します。

次の例では、exc_db10 という名前の Microsoft Exchange Server データベースのすべてのバックアップを検索します。

```
tdpexcc q tsm exc_db10

IBM Spectrum Protect for Mail:
Data Protection for Microsoft Exchange Server
Version 8, Release 1, Level 6.0 (C) Copyright
IBM Corporation 1997, 2018. All rights reserved.

...

Querying IBM Spectrum Protect server for a list of
data backups, please wait....

Connecting to IBM Spectrum Protect Server as node 'KINGSTON40_EXC'...
Connecting to Local DSM Agent 'exc'...
Using backup node 'KINGSTON40_EXC'...

    Exchange Server      : exc
    Database             : exc_db10

    Backup Date   Size   S   Type   Loc   Object Name
    -----
07/15/2018 19:17:26  5.40 B   A   full   Srv   20180715191726 (VMVSS)

The operation completed successfully. (rc = 0)
```

2. トランザクション・ログを適用せずにデータベースをリストアするには、以下のコマンドを発行します。

```
TDPEXCC RESTore databaseName FULL /BACKUPDEstination=TSM
/BACKUPMethod=VMVSS
```

次の出力例は、exc_db10 という名前の Microsoft Exchange Server データベースでコマンドを発行した結果です。

```
TDPEXCC RESTore exc_db10 FULL /BACKUPDEstination=TSM /BACKUPMethod=VMVSS
```

```
IBM Spectrum Protect for Mail:  
Data Protection for Microsoft Exchange Server  
Version 8, Release 1, Level 0.6 (C) Copyright  
IBM Corporation 1997, 2018. All rights reserved.
```

```
Connecting to IBM Spectrum Protect Server as node 'KINGSTON40_EXC'...
```

```
Connecting to Local DSM Agent 'exc'...  
Using backup node 'KINGSTON40_EXC'...
```

```
Starting Microsoft Exchange restore...  
Beginning VSS restore of 'exc_db10'...
```

```
Restoring 'exc_db10' via file-level copy from snapshot(s).  
This operation could take a while, please wait
```

```
...
```

```
The operation completed successfully. (rc = 0)
```

/INTODB パラメーターを追加することにより、データベースを別の場所にリストアすることができます。例えば、次のようにします。

```
TDPEXCC RESTore TestDB1 FULL /INTODB=Test2  
/BACKUPDEstination=TSM /BACKUPMethod=VMVSS
```

次のタスク

Data Protection for Microsoft Exchange Server コマンド・ライン・インターフェース **TDPEXCC** を使用して、活動状態にないバックアップをリストアできます。**restore** コマンドの発行時に、特定のバックアップのデータベース・オブジェクト名を指定します。

データベース・オブジェクト名を取得するには、以下のコマンドを入力します。

```
tdpexcc q tsm dbname full /all
```

データベース・オブジェクト名の値を入手したら、**TDPEXCC restore** コマンドの **/OBJect=objectname** パラメーター (ここで、*objectname* はデータベース・オブジェクト名) で、そのデータベース・オブジェクト名を指定します。例えば、次のとおりです。

```
TDPEXCC RESTore db44 FULL /OBJect=20180715191726 /BACKUPDEstination=TSM  
/BACKUPMethod=VMVSS
```

Windows PowerShell コマンドレットを使用したデータのリストア

必要な場合、Data Protection for Microsoft Exchange Server で Windows PowerShell コマンドレットを使用して、仮想マシンから Microsoft Exchange Server のフル・データベース・リカバリーを開始できます。

始める前に

バックアップ・タイプ「VMVSS」を使用して Microsoft Exchange Server データベースをリストアする前に、Microsoft iSCSI Initiator Service が稼働していることを確認してください。このサービスが稼働していない場合は、サービスを開始します。手順については、[103 ページの『Microsoft iSCSI Initiator Service の開始』](#)を参照してください。

手順

ゲスト VM で、以下の手順を実行します。

1. **query** コマンドレットを発行して、データベースのフルバックアップを検索します。
例えば、すべてのデータベース・フルバックアップを見つけるには、次のコマンドを入力します。

```
Get-DpExcBackup -Name * -FromExcServer *
```

2. データベースのリストア・コマンドレットを発行します。
例えば、次のとおりです。

```
Restore-DpExcBackup -Name ExchDb01 -Full `
-BackupDestination TSM -FromExcServer PALADIN20 `
-Intodb Zwen
```

3. 代替ロケーションにリストアするには、リストア・コマンドレットにパラメーター **intodb** を指定して発行します。
例えば、次のとおりです。

```
Restore-DpExcBackup -Name ExchDb01 -Full `
-BackupDestination TSM -FromExcServer PALADIN20 `
-Object 20140923100738 -Intodb ExchDb01_altRdb
```

IBM Spectrum Protect ファイル・スペース情報

ご使用の仮想マシン (VM) のファイルのファイル名や場所を知っている必要はないかもしれません。しかし、基礎となるファイル構造に関心がある場合は、Data Protection for Microsoft Hyper-V バックアップは、IBM Spectrum Protect サーバー上に Hyper-V ターゲット・ノードのノード名 (KINGSTON5_HV_TGT など) で保管されます。

以下の例は、Kingston40 と呼ばれる VM のファイル・スペース情報を示しています。

```
Protect: ORION>q file KINGSTON5_HV_TGT f=d

Node Name:          KINGSTON5_HV_TGT
Filespace Name:      \VMFULL-kingston40
Hexadecimal Filespace Name:
FSID: 61
Collocation Group Name:
Platform: TDP Hyper-V
Filespace Type: API:TSMVM
Is Filespace Unicode?: No
Capacity: 0 KB
Pct Util: 0.0
Last Backup Start Date/Time: 03/13/2018 21:29:17
Days Since Last Backup Started: 31
Last Full NAS Image Backup Completion Date/Time:
Days Since Last Full NAS Image Backup Completed:
Last Backup Date/Time From Client (UTC):
Last Archive Date/Time From Client (UTC):
Last Replication Start Date/Time:
Days Since Last Replication Started:
Last Replication Completion Date/Time:
Days Since Last Replication Completed:
Backup Replication Rule Name: DEFAULT
Backup Replication Rule State: Enabled
Archive Replication Rule Name: DEFAULT
Archive Replication Rule State: Enabled
Space Management Replication Rule Name: DEFAULT
Space Management Replication Rule State: Enabled
At-risk type: Default interval
At-risk interval:
```

Hyper-V 環境での Microsoft SQL Server データの保護

Hyper-V ゲスト仮想マシン (VM) で実行されている Microsoft SQL Server ワークロードの場合、ゲスト VM のアプリケーション整合バックアップを取得することができます。元のデータベースが損傷を受けたり、失われたりした場合には、データベース・レベルのバックアップをリカバリーできます。

以下の製品は、Hyper-V 環境で連携して Microsoft SQL Server データを保護します。

- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V バージョン 8.1.10
- IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft SQL Server バージョン 8.1.6 以降

Microsoft SQL Server のアプリケーション・データをバックアップおよびリストアするために必要な権限については、[技術情報 1647995](#) を参照してください。

Microsoft SQL Server のアプリケーション保護のソフトウェア要件については、[技術情報 2017347](#) を参照してください。

Microsoft SQL Server のアプリケーション保護のソフトウェアのインストールと構成

Microsoft SQL Server データをホストするゲスト仮想マシン (VM) を保護するために、Hyper-V ホストおよびゲスト VM でインストールと構成のステップを完了する必要があります。ステップバイステップの指示を使用して、ゲスト内アプリケーションを保護できるようにご使用の環境を稼働させることができます。

始める前に

[技術情報 2017347](#) でソフトウェア要件を確認してください。

このタスクについて

以下の表には、その後のタスクで示される例として使用されている名前をリストしています。コマンドやオプションの例を使用する場合、その例は、使用している環境の該当する Hyper-V ホストとゲスト VM の名前に置き換えてください。

名前のタイプ	例
Hyper-V ホストまたはクラスターの名前	Kingston5
Microsoft SQL Server をホストしているゲスト VM の名前	Kingston40

VM ゲスト上の Microsoft SQL Server データを保護するために、Data Protection for Microsoft Hyper-V および Data Protection for Microsoft SQL Server をインストール、セットアップ、および構成するには、以下の手順を実行します。

手順

1. [108 ページの『ステップ 1 \(Hyper-V ホスト\): Data Protection for Microsoft Hyper-V のインストールおよび構成』](#)
2. [109 ページの『ステップ 2 \(ゲスト VM\): Data Protection for Microsoft SQL Server のインストールおよび構成』](#)
3. [111 ページの『ステップ 3 \(Hyper-V ホスト\): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成』](#)
4. [114 ページの『ステップ 4 \(ゲスト VM\): データベースのリストア』](#)
5. [115 ページの『オプション: 仮想マシン名の変更後のアプリケーション保護の構成』](#)

ステップ 1 (Hyper-V ホスト): Data Protection for Microsoft Hyper-V のインストールおよび構成

Data Protection for Microsoft Hyper-V をインストールおよび構成して、Microsoft SQL Server データをホストしているゲスト仮想マシン (VM) を正常にバックアップできることを確認します。

始める前に

Data Protection for Microsoft Hyper-V バージョン 8.1.2 以前からアップグレードする場合は、IBM Spectrum Protect サーバー上の既存の Hyper-V ノードの名前を *clustername_hv_tgt* (クラスターの場合) または *hostname_hv_tgt* (スタンドアロン・ホストの場合) に変更します。Hyper-V ノード名は、asnodename オプションで指定されたノード名です。

例えば、サーバー上の Hyper-V ノードの名前を KINGSTON_HV_TGT に変更します。詳しくは、[16 ページの『IBM Spectrum Protect サーバー上のノードの名前変更』](#)を参照してください。

[14 ページの『必要な通信ポート』](#)の説明に従って、ファイアウォールで通信ポートが開いていることを確認します。

手順

Hyper-V ホストまたはクラスターで、以下のタスクを実行します。

1. Data Protection for Microsoft Hyper-V をインストールします。

手順については、[22 ページの『Data Protection for Microsoft Hyper-V の標準インストールの実行』](#)を参照してください。

2. 構成ウィザードを完了して Data Protection for Microsoft Hyper-V を構成します。

手順については、[39 ページの『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』](#)を参照してください。

要確認：「クラスターおよびホスト」ウィザード・ページに表示される、あるいは Data Protection for Microsoft Hyper-V 管理コンソールで「アクション」>「プロパティ」をクリックすると表示されるターゲット・ノード名を記録します。ターゲット・ノード名の末尾は _HV_TGT です。Data Protection for Microsoft SQL Server で構成ウィザードを実行する場合は、ターゲット・ノード名が必要です。

3. Data Protection for Microsoft Hyper-V 管理コンソールを使用して、Microsoft SQL Server をホストしている VM をバックアップします。

手順については、[79 ページの『仮想マシンのアドホック・バックアップの開始』](#)を参照してください。

次のタスク

VM が正常にバックアップされたら、[109 ページの『ステップ 2 \(ゲスト VM\): Data Protection for Microsoft SQL Server のインストールおよび構成』](#)に進みます。

ステップ 2 (ゲスト VM): Data Protection for Microsoft SQL Server のインストールおよび構成

Data Protection for Microsoft SQL Server を使用してデータベースをバックアップできるようにするには、ステップを実行して Data Protection for Microsoft SQL Server をインストールおよび構成し、Microsoft SQL Server データベースをバックアップします。

始める前に

[108 ページの『ステップ 1 \(Hyper-V ホスト\): Data Protection for Microsoft Hyper-V のインストールおよび構成』](#)の手順を完了している必要があります。

Microsoft SQL Server データベースが Hyper-V 仮想ディスク上でホストされていることを確認してください。

物理ディスク、独立ディスク、あるいはゲスト内 iSCSI を介してゲストに直接接続されたディスク上でホストされている Microsoft SQL Server データベースがないことを確認します。

Microsoft SQL Server データベースが単一のサーバー上にあり、いずれのタイプのクラスタリング (フェイルオーバー・クラスター、AlwaysOn 可用性グループ、AlwaysOn フェイルオーバー・クラスター・インスタンスなど) にも参加していないことを確認してください。

手順

Microsoft SQL Server データをホストしているゲスト仮想マシン (VM) 上で以下のステップを実行します。

1. Data Protection for Microsoft SQL Server をインストールします (まだインストールされていない場合)。

インストールの手順については、[IBM Spectrum Protect for Databases の製品資料](#)を参照してください。

ヒント：インストール手順の説明に従って、Data Protection for Microsoft SQL Server 構成ウィザードを実行しないでください。このウィザードは、[ステップ 110 ページの『3』](#)で実行します。以前に Data Protection for Microsoft SQL Server をインストールし、ウィザードを実行している場合は、[ステップ 110 ページの『3』](#)で再実行する必要があります。

2. Data Protection for Microsoft Hyper-V インストール・パッケージからデータ・ムーバー機能をインストールします。

インストール・ウィザードで拡張インストール・オプションを選択し、「**データ・ムーバー機能またはマウント・プロキシのインストール (Install the data mover feature or mount proxy)**」をクリックして、アプリケーション保護サポートをインストールします。

詳細については、26 ページの『Data Protection for Microsoft Hyper-V データ・ムーバーのみのインストール』を参照してください。

3. 「スタート」 > 「**DP for SQL 管理コンソール**」をクリックし、Data Protection for Microsoft SQL Server 管理コンソールを開きます。

構成ウィザードが自動的に開きます。

構成ウィザードが自動的に開始されない場合は、管理コンソールのツリー・ビューに移動し、「**IBM Spectrum Protect**」 > 「ダッシュボード」 > 「管理 (Manage)」 > 「構成」 > 「ウィザード (Wizards)」をクリックします。「**IBM Spectrum Protect 構成ウィザード (IBM Spectrum Protect Configuration Wizard)**」をダブルクリックします。

4. 構成ウィザードの「**IBM Spectrum Protect ノード名 (IBM Spectrum Protect Node Names)**」ページで、VSS リクエスター、Data Protection for Microsoft SQL Server、および Hyper-V ターゲット・ノードの名前をそれぞれのフィールドに入力します。「**DP SQL VSS サポートを構成しない (Do not configure DP SQL VSS Support)**」チェック・ボックスがクリアされていることを確認します。

以下の表に構成手順で使用されるノード名の例が示されています。

フィールド名	ノード名の例
VSS リクエスター	KINGSTON40_VSS
Data Protection for SQL	KINGSTON40_SQL
Hyper-V ターゲット・ノード	KINGSTON5_HV_TGT

5. 構成ウィザードの「**IBM Spectrum Protect サーバー設定 (IBM Spectrum Protect Server Settings)**」ページで、以下のいずれかのステップを実行します。

- ・ ウィザードを使用して IBM Spectrum Protect サーバーを構成する場合は、「検討」または「編集」を選択し、必要に応じてマクロを更新します。
- ・ 手動でサーバーを構成するには、以下の手順を実行します。

- a. ウィザードの最後のページで、マクロ・ファイルを開くリンクをクリックします。
- b. マクロ・ファイルを更新して実行するか、マクロから適切なコマンドを発行します。その際に使用するコマンドは、ご使用の環境に必要なコマンドに合わせて調整してください。

例えば、fcm_pdsql という名前のポリシー・ドメインを使用するためにセットアップするとします。C:\Program Files\Tivoli\TSM\baclient フォルダーから **dsmadm** コマンドを実行し、次のコマンドを発行します。

```
register node KINGSTON40_VSS T_3_m_p_P_w userid=KINGSTON40_VSS
update node KINGSTON40_VSS T_3_m_p_P_w backdelete=yes forcep=yes
```

```
register node KINGSTON40_SQL T_3_m_p_P_w domain=fcm_pdsql
userid=KINGSTON40_SQL
update node KINGSTON40_SQL T_3_m_p_P_w backdelete=yes domain=fcm_pdsql
forcep=yes
```

```
grant proxynode target=KINGSTON40_SQL agent=KINGSTON40_VSS
```

forcep=yes オプションは、初回アクセス時に強制的にパスワードをリセットします。

場合によっては **dsmadm** コマンドの実行時に次のエラー・メッセージが表示されます。

```
ANS1592E SSL プロトコルの初期化に失敗しました
```

このメッセージが表示された場合、使用している IBM Spectrum Protect サーバー管理者アカウントで sessionsecurity オプションが **transitional** に設定されていることを確認してください。

例えば、IBM Spectrum Protect サーバーにアクセスできるリモート・コンピューターから次のコマンドを発行します。

```
update admin myAdmin sessionsecurity=transitional
```

6. 構成ウィザードを完了します。
7. 十分な数の Microsoft SQL Server ログ・バックアップのバージョンおよび VM バックアップを保持するようにポリシーが設定されていることを確認します。
手順については、[118 ページの『バックアップのバージョンの管理』](#)を参照してください。
8. Data Protection for Microsoft SQL Server 管理コンソールから次のようにデータベースをバックアップします。
 - a) 「アクション」 ペインで、「バックアップ・メソッド」 > 「VSS」をクリックします。
 - b) 「アクション」 ペインで、「バックアップの宛先」 > 「TSM」をクリックします。
 - c) 「アクション」 ペインで、「フルバックアップ」をクリックします。

次のタスク

VSS バックアップが正常に完了したら、[111 ページの『ステップ 3 \(Hyper-V ホスト\): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成』](#)に進みます。

ゲスト VM 上のデータについて発生する可能性のあるリストアの問題を回避するために、[189 ページの『データ・ムーバーからアプリケーション保護バックアップをリストアする場合のシャドー・コピーの考慮事項』](#)の情報を確認してください。

ステップ 3 (Hyper-V ホスト): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成

Microsoft SQL Server データをホストしているゲスト仮想マシン (VM) を保護するために、Data Protection for Microsoft Hyper-V を構成します。VM をバックアップし、バックアップ操作が正常に完了したことを確認します。

始める前に

[109 ページの『ステップ 2 \(ゲスト VM\): Data Protection for Microsoft SQL Server のインストールおよび構成』](#)の手順を完了している必要があります。

Microsoft SQL Server データベースをホストしている仮想ハード・ディスク (VHDX) が VM バックアップ操作から除外されていないことを確認します。手順については、[119 ページの『Microsoft SQL Server ボリュームが仮想マシン・バックアップで除外されていないことの確認』](#)を参照してください。

オプション: バックアップ操作時には、ゲスト VM に対する統合サービスまたはゲスト・サービス・インターフェースが自動的に有効になります。手動で有効にする必要はありません。ただし、現行の状況を確認する場合、あるいは「**ゲスト・サービス (Guest Services)**」サービスを明示的に有効にする場合は、Hyper-V ホストまたはクラスターで以下のいずれかの方法を使用します。

- Hyper-V Manager から、以下を行います。
 1. VM を右クリックし、「設定」 > 「統合サービス」をクリックします。
 2. 「統合サービス」ウィンドウで、「**ゲスト・サービス (Guest Services)**」チェック・ボックスが選択されていることを確認します。
- 管理者として、PowerShell コマンド・プロンプトから、次のコマンドを発行します。

```
Get-VMIntegrationService -VMName Kingston40 `
Enable-VMIntegrationService -VMName Kingston40 -Name "Guest Service Interface"
```

このタスクについて

Microsoft SQL Server をホストしている VM をバックアップする場合、Data Protection for Microsoft Hyper-V はアプリケーション整合性を提供します。これらのバックアップを使用して、整合した状態で VM をリカバリーすることができます。

このタイプのバックアップから、VM 全体をリカバリーすることなく選択したデータベースのみをリストアするには、VM スナップショットおよびバックアップの作成時に Microsoft SQL Server の状態に関する情報を保存する必要があります。この情報は、VM のスナップショットの作成時に行われる Microsoft Volume Shadow Copy Services (VSS) 対話の一部として収集されます。

アプリケーション保護バックアップをリストアする場合のシャドー・コピーの考慮事項: 通常、シャドー・ストレージはボリュームの一部です。ただし、シャドー・ストレージ・スペースが、デフォルトで、または手動構成の結果として、別のボリューム上に構成される場合があります。この場合、VM バックアップ操作中に作成されたシャドー・コピーがリストア時に使用できないので、データベースのリストア操作は失敗することがあります。

バックアップ操作を開始する前に、[189 ページの『アプリケーション保護リストア中にはリストアされたボリュームでシャドー・コピーが使用可能でなければならない』](#)に記載されている情報を確認します。

Data Protection for Microsoft Hyper-V で Microsoft SQL Server の Microsoft VSS メタデータを収集するには、バックアップ操作中に VM からこの情報を取得するように Data Protection for Microsoft Hyper-V を構成する必要があります。

この手順では、Microsoft Hyper-V Manager に示されているように、Kingston40 が Hyper-V ホストの例です。Kingston5 は、Microsoft SQL Server をホストするゲスト VM の名前の例です。Kingston40_vss は、Data Protection for Microsoft SQL Server のインストール時に作成されるクライアント・ノードの名前です。例は、使用している環境に合った適切な値に置き換えてください。

手順

Hyper-V ホストまたはクラスターで、以下の手順を実行します。

1. baclient フォルダーから、Microsoft SQL Server をホストしているゲスト VM 用の Windows 資格情報を以下のように設定します。

- 特定の VM の資格情報を設定するには、コマンド・プロンプトで baclient フォルダーから次のコマンドを発行します。

```
dsmc set password -type=vmguest guest_VM_name "guest_admin_ID" guest_admin_pw  
-optfile=dsm.hostname_HV_DM.opt
```

- 特定の資格情報が設定されていないすべての VM の資格情報を設定するには、次のようにします。

```
dsmc set password -type=vmguest allvm "guest_admin_ID" guest_admin_pw  
-optfile=dsm.hostname_HV_DM.opt
```

ここで、

vmname

Microsoft SQL Server をホストするゲスト VM の名前。この名前は、Hyper-V Manager で表示される VM 名です。

guest_admin_ID

ゲスト VM の管理者 ID。guest_admin_ID は、Windows のドメイン・アカウントまたはローカル・アカウントにすることができます。例えば、次のとおりです。

- ドメイン・アカウントの場合、domain\username 形式を使用します。
- ローカル・アカウントの場合、username 形式を使用します。

guest_admin_pw

ゲスト VM の管理者 ID のパスワード。

hostname

Hyper-V ホストまたはクラスターの名前。

例えば、次のとおりです。

```
dsmc set password -type=vmguest Kingston40 "world¥alan" "@lanPwd!"  
-optfile=dsm.KINGSTON5_HV_DM.opt
```

set password コマンドで使用されるアカウントは、Hyper-V ホストまたはクラスターと、SQL Server データをホストするゲスト VM の両方で有効でなければなりません。

制約事項: ゲスト VM のログイン資格情報 (ユーザー名およびパスワード) は、Hyper-V ホストの資格情報と同じでなければなりません。

dsmc set password コマンドは、データ・ムーバーをホストするシステム上で暗号化された、ゲスト VM 資格情報を保管します。ゲスト VM の管理者 ID およびパスワードには、以下の最小権限が必要です。

バックアップ権限

db_backupoperator データベース役割を持つユーザーには、自己完結型アプリケーション・データのバックアップを実行する権限が付与されます。そのユーザーが SQL Server sysadmin 固定サーバー役割のメンバーの場合、ユーザーは Microsoft SQL Server インスタンスの任意のデータベースをバックアップできます。ユーザーは、そのユーザーが所有者であるデータベースもバックアップできますが、特定のデータベースに対するバックアップ権限がありません。ゲスト VM ユーザーは、ボリューム・シャドー・コピーを作成し、SQL サーバーのログを切り捨てる権限を持っている必要があります。

リストア権限

データベースが存在する場合、**dbcreator** 固定サーバー役割のメンバーであるか、データベース所有者であれば、リストア操作を実行することができます。Microsoft SQL Server sysadmin 固定サーバー役割を持つユーザーは、任意のバックアップ・セットからデータベースをバックアップする権限があります。その他のユーザーの場合、シチュエーションはデータベースが存在するかどうかによって異なります。

2. **baclient** フォルダーから、アプリケーション保護のためにデータ・ムーバー・オプション・ファイルを構成します。

- a) データ・ムーバー・オプション・ファイル (`dsm.hostname_HV_DM.opt`) を編集のために開きます。例えば、次のコマンドを発行します。

```
notepad dsm.KINGSTON5_HV_DM.opt
```

- b) `include.vmtsmvss guest_vm_name` オプションを追加します。`guest_vm_name` パラメーターには、ワイルドカード文字を含めることができます。例えば、次のとおりです。

```
include.vmtsmvss Kingston40
```

または

```
include.vmtsmvss Kingston*
```

あるいは、SQL Server ログを手動で保持し、VM のリストア後に SQL Server のトランザクションを特定のチェックポイントにリストアする予定の場合は、次のオプションを指定して、SQL Server ログが切り捨てられないようにします。

```
include.vmtsmvss Kingston40 OPTions=KEEPSqllog
```

3. **baclient** フォルダーから、**dsmc backup vm** コマンドを発行してゲスト VM をバックアップします。例えば、次のとおりです。

```
dsmc backup vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt  
-asnode=KINGSTON5_HV_TGT
```

4. **dsmc query vm** コマンドを実行して、バックアップ操作を確認します。VM 名は大/小文字を区別します。

例えば、**baclient** フォルダーから次のコマンドを発行します。

```
dsmc query vm Kingston40 -optfile=dsm.KINGSTON5_HV_DM.opt  
-asnode=KINGSTON5_HV_TGT -detail
```

出力には、以下の例のようなテキストが含まれます (ただし、Microsoft SQL Server のバージョンが異なる場合があります)。

```
Application protection type: TSM VSS  
Application(s) protected: Microsoft SQL Server 2017
```

5. **baclient** フォルダーから **dsmc set access** コマンドを使用して、ゲスト VM 上の VSS ノードが VM バックアップにアクセスしてリストアできるように許可します。
例えば、以下の例のようなコマンドを発行します。

```
dsmc set access backup -type=vm Kingston40 kingston40_vss  
-nodename=KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
```

ここで、Kingston40 は Microsoft Hyper-V マネージャーに表示されるゲスト VM の名前、kingston40_vss は Data Protection for Microsoft SQL Server のインストール時に作成される IBM Spectrum Protect ノードです。このノード名は、Kingston40 VM 上のファイル C:\Program Files\Tivoli\TSM\baclient\dsm.opt に示されています。

次の **dsmc query access** コマンドを発行すると、ノードがアクセスできる VM バックアップが表示されます。例えば、次のとおりです。

```
dsmc query access -nodename=KINGSTON5_HV_TGT -optfile=dsm.KINGSTON5_HV_DM.opt
```

次のタスク

バックアップ操作が正常に完了したら、[114 ページの『ステップ 4 \(ゲスト VM\): データベースのリストア』](#)に進みます。

関連資料

[153 ページの『Backup VM』](#)

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

[187 ページの『INCLUDE.VMTSMVSS』](#)

関連情報

[Set Access](#)

[パスワードの設定](#)

ステップ 4 (ゲスト VM): データベースのリストア

アプリケーション保護が適切に構成されていることを検証するには、Data Protection for Microsoft SQL Server でデータベースをリストアします。

始める前に

[111 ページの『ステップ 3 \(Hyper-V ホスト\): アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成』](#)の手順を完了している必要があります。

ゲスト仮想マシン (VM) 上で必要なサービスが稼働していることを確認します。

1. コマンド・プロンプトで、次のコマンドを発行します。

```
services.msc
```

2. サービスのリストで、「**IBM Spectrum Protect Recovery Agent サービス**」を見つけ、必要場合はサービスを開始します。
3. サービスのリストで、「**Microsoft iSCSI Initiator Service**」を見つけます。必要に応じて、スタートアップの種類を「**自動**」に変更し、サービスを開始します。

手順

ゲスト VM で、以下の手順を実行します。

1. Data Protection for Microsoft SQL Server 管理コンソールを開始します。
2. ツリーで「**SQL Server**」インスタンスを選択します。
3. 「**リカバリー (Recover)**」タブにナビゲートし、「**最新表示**」をクリックします。
4. 「**VMVSS**」バックアップ方式のあるデータベース項目を選択します。

5. 「アクション」 ペインで、「代替ロケーションにリストア (Restore to Alternate Location)」をクリックします。新規データベース名と、データベースがリストアされる新規ロケーションを指定します。
6. 「アクション」 ペインで、「リストア」をクリックします。
7. リストア操作が完了したら、データベースおよび関連する表を確認します。

次のタスク

必要に応じてバックアップを管理し、データをリカバリーできるようになりました。詳しくは、以下を参照してください。

- [116 ページの『バックアップ操作の管理』](#)
- [120 ページの『データのリストア』](#)

アプリケーション保護のための構成ステップの完了後にゲスト VM の名前を変更した場合は、新しい VM 名でソフトウェアを再構成する必要があります。手順については、[115 ページの『オプション: 仮想マシン名の変更後のアプリケーション保護の構成』](#)を参照してください。

オプション: 仮想マシン名の変更後のアプリケーション保護の構成

アプリケーション保護構成の完了後にゲスト仮想マシン (VM) の名前を変更した場合、名前変更されたゲスト VM で Data Protection for Microsoft Hyper-V を再構成する必要があります。

始める前に

Microsoft SQL Server をホストするゲスト VM を保護するためのソフトウェアのインストールおよび構成が完了している必要があります。

このタスクについて

このタスクは、アプリケーション保護によって保護されているゲスト VM の名前を変更した場合にのみ実行してください。

手順

1. Hyper-V ホストまたはクラスター上のデータ・ムーバーで、次のコマンドを発行します。

```
dsmc set password -type=vmguest new_vmguest_displayname guest_admin_ID  
guest_admin_pw
```

ここで、

new_vmguest_displayname

Microsoft SQL Server をホストする新しいゲスト VM の名前。この名前は、Hyper-V Manager で表示される VM 名です。

guest_admin_ID

新しいゲスト VM の管理者 ID。 *guest_admin_ID* は、Windows のドメイン・アカウントまたはローカル・アカウントでなければなりません。例えば、次のとおりです。

- ドメイン・アカウントの場合、 *domain¥username* 形式を使用します。
- ローカル・アカウントの場合、 *username* 形式を使用します。

guest_admin_pw

新しいゲスト VM の管理者 ID のパスワード。

2. データ・ムーバー・オプション・ファイル (*dsm.hostname_HV_DM.opt*) で、次のように *include.vmtsmvss* オプションを更新します。

```
include.vmtsmvss new_vmguest_displayname
```

ここで、 *new_vmguest_displayname* は Hyper-V Manager での新しいゲスト VM の表示名です。ワイルドカード文字を使用することができます。

3. Data Protection for Microsoft Hyper-V 管理コンソールを使用するか、コマンド・プロンプトから次のコマンドを発行して、データ・ムーバーの **baclient** フォルダーから新しいゲスト VM をバックアップします。

```
dsmc backup vm new_vmquest_displayname -optfile=dsm.hostname_HV_DM.opt  
-asnode=hostname_HV_TGT
```

4. **baclient** フォルダーから **dsmc set access** コマンドを使用して、新しいゲスト VM 上の VSS ノードが VM バックアップにアクセスしてリストアできるように許可します。
例えば、次のコマンドを発行します。

```
dsmc set access backup -type=VM new_vmquest_displayname vss_requestor_node  
-optfile=dsm.hostname_HV_DM.opt
```

ここで、

new_vmquest_displayname

Hyper-V Manager での新しいゲスト VM の表示名。

vss_requestor_node

Data Protection for Microsoft SQL Server で構成された VSS リクエスターの名前。

hostname

Data Protection for Microsoft Hyper-V がインストールされている Hyper-V ホストまたはクラスターの名前。

5. オプション: VSS リクエスター・ノードは古い VM 名でバックアップされた VM へのアクセス権を既に持っているため、Data Protection for Microsoft SQL Server 管理コンソールには、古い VM と新しい VM のどちらからバックアップされた VMVSS データベースも表示されます。

古い VM 名を持つ VM バックアップにアクセスしたくない場合は、古い VM バックアップへのアクセス権を削除する必要があります。Hyper-V ホスト上のデータ・ムーバーから、次のコマンドを発行します。

```
dsmc del access -optfile=dsm.hostname_HV_DM.opt -asnode=hostname_HV_TGT
```

アクセス・リストが表示されます。アクセス・リストから削除したい項目に対応する索引を入力します。

IBM Spectrum Protect サーバー上のスペースを節約したい場合は、**dsmc delete filespace** コマンドを発行して、古い VM のバックアップ・データが含まれるファイル・スペースを削除することができます。

重要: ファイル・スペースを削除すると、そのファイル・スペース内のすべてのバックアップ・バージョンが削除され、データをリストアすることはできなくなります。古い VM バックアップを削除する前に、そのデータが不要であることを確認してください。

バックアップ操作の管理

Microsoft SQL Server データを保護するために環境を構成した後、バックアップをスケジュールできます。仮想マシン (VM) のバックアップ操作と Microsoft SQL Server ログのバックアップ操作のためのスケジュールをセットアップできます。

仮想マシン・バックアップのスケジューリング

ご使用のデータの定期的な保護が確実に行われるように、仮想マシン (VM) バックアップをスケジュールします。

始める前に

デフォルトでは、バックアップ操作で仮想ハード・ディスク (VHDX) に許可される最大サイズは 2 TB に設定されています。ただし、**vmmaxvirtualdisks** オプションを使用して最大サイズを 8 TB まで増やすことができます。詳細については、[213 ページの『Vmmaxvirtualdisks』](#)を参照してください。

手順

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインで、スタンドアロン・ホストまたはクラスターをクリックします。
3. 「アクション」ペインで、「バックアップ管理」をクリックします。
4. 「バックアップ管理」ウィンドウでスケジュールを選択し、「スケジュールの割り当て」をクリックします。
5. ウィンドウを閉じるには、「クローズ」をクリックします。
6. スケジュールのソースに Microsoft SQL Server をホストしている VM が含まれていることを確認します。
7. 以下のいずれかのサービスが稼働していることを確認します。
 - ・ クライアント・アクセプター (CAD) によって管理されているスケジューラーを使用する場合は、データ・ムーバー上でクライアント・アクセプター・サービスが稼働していることを確認してください。
 - ・ スタンドアロンのスケジューラーを使用する場合、そのスケジューラーのサービスが稼働していることを確認してください。

Microsoft SQL Server ログ・バックアップのスケジューリング

仮想マシン・バックアップのスケジュールを作成した後、Microsoft SQL Server ログ・バックアップのスケジュールを作成できます。

このタスクについて

SQL Server ログのバックアップは、より細かいレベルのリカバリー・ポイントを提供します。現在のバックアップ頻度で十分なリカバリー・ポイントが提供される場合や、バックアップに `INCLUDE.VMTSMVSS vm_display_name OPTions=KEEPSqllog` オプションを指定しなかった場合には、SQL Server ログをバックアップする必要はないかもしれません。

手順

1. Microsoft SQL Server をホストしている仮想マシン (VM) から Data Protection for Microsoft SQL Server ユーザー・インターフェースを開始します。
2. ナビゲーション・ペインで、「管理」ノードを展開します。
3. 「管理」ノードの下で、右クリックして「スケジューリング」>「スケジューリング・ウィザード」を選択します。
4. 「スケジューリング・ウィザード」を開き、スケジュールの名前と時刻を確認します。
5. 「スケジュール・タスクの定義」ページで、「コマンド・ライン」を選択します。
6. アイコンをクリックし、SQL Server テンプレートを選択します。「次へ」をクリックします。
7. コマンド・ライン・インターフェースおよび SQL Server テンプレートを使用して、データベース・ログ・バックアップを指定します。例えば、次のようにします。

```
tdpsqlc backup * log /truncate=yes 2>&1
```

ヒント：あるいは、IBM Spectrum Protect 集中スケジューリング・サービスを使用して、Microsoft SQL Server バックアップをスケジュールすることができます。このサービスは、ユーザーが VM 上のすべての Microsoft SQL Server インスタンスのバックアップ・スケジュールを作成するのに役立ちます。

バックアップの検証

バックアップを作成した後、Data Protection for Microsoft SQL Server インターフェースから 仮想マシン・バックアップおよびデータベース・バックアップを照会できることを確認します。

手順

1. Microsoft 管理コンソール (MMC) から、Microsoft SQL Server を選択します。
2. 「リカバリー」タブをクリックします。

3. 「表示」 > 「データベース」を選択します。 リストアできる Microsoft SQL Server データベース・バックアップのリストが表示されます。

Data Protection for Microsoft Hyper-V を使用してバックアップされた Microsoft SQL Server データベースは、バックアップ・メソッド `vmvss` で識別されます。

Data Protection for Microsoft SQL Server を使用してバックアップされた Microsoft SQL Server ログは、バックアップ・メソッド `Legacy` で識別されます。

バックアップのバージョンの管理

Data Protection for Microsoft SQL Server を使用して、バックアップの有効期限を管理することができます。保存するスナップショット・バックアップの数やスナップショットの保存期間を指定できます。

このタスクについて

Microsoft SQL Server バックアップの保存を設定するには、以下の手順を実行します。この手順では、バックアップを 30 日間保存することを想定しています。

手順

1. 仮想マシン (VM) バックアップで使用する管理クラスで、保持パラメーターを定義します。例えば次のとおりです。

```
Retain extra versions = 30
Retain only versions = 30
Versions data exists = nolimit
Versions data deleted = nolimit
```

VM バックアップに使用する管理クラスを指定するには、データ・ムーバー・オプション・ファイルで `vmmc` オプションを使用します。

スケジュールされた VM バックアップは、Data Protection for Microsoft Hyper-V に関連付けられます。

2. Microsoft SQL Server バックアップで使用する管理クラスで、保持パラメーターを定義します。例えば次のとおりです。

```
Retain extra versions = 0
Retain only versions = 1
Versions data exists = nolimit
Versions data deleted = nolimit
```

Data Protection for Microsoft SQL Server エージェントで使用される `dsm.opt` ファイルに、Microsoft SQL Server バックアップの管理クラスを指定します。以下の `INCLUDE` オプションを参照してください。

```
INCLUDE *:\...\¥*log management_class_name
INCLUDE *:\...\¥log¥..¥* management_class_name
```

3. VM 上で Data Protection for Microsoft SQL Server が稼働している状態で、**inactivate** コマンドを発行して、Microsoft SQL Server 上のすべてのデータベースのすべてのアクティブ・ログ・バックアップを明示的に非アクティブ化します。例えば、次のとおりです。

```
tdpsqlc inactivate * log=* /OLDERTHAN=30
```

フル・データベース・バックアップが Data Protection for Microsoft Hyper-V によって実行されているため、Data Protection for Microsoft SQL Server によって作成されたログ・バックアップを明示的に非活動化する必要があります。この構成では、Microsoft SQL Server ログ・バックアップが非アクティブ化されてから、IBM Spectrum Protect サーバーがそのバックアップを削除するまでに、1 日の猶予期間ができます。

ヒント: ログ・バックアップは、そのログ・バックアップが関連付けられているフル・データベース・バックアップが保持されている場合にのみ、サーバー上に保持できます。管理クラスで、ログ・バックアップの **RETONLY** 値を、フル・データベース・バックアップの **RETEXTRA** パラメーターに一致するように設定します。

Microsoft SQL Server ボリュームが仮想マシン・バックアップで除外されていないことの確認

Hyper-V 仮想ハード・ディスク (VHDX) 内のボリュームには、Data Protection for Microsoft Hyper-V バックアップ処理から除外されていない Microsoft SQL Server データベースが入っている必要があります。

始める前に

データベースが以下のタイプのディスク 上にないことを確認します。

- 物理ディスク
- 独立ディスク
- iSCSI 経由でゲスト・オペレーティング・システムに直接接続されているディスク

手順

1. 仮想マシン (VM) のバックアップに使用される Data Protection for Microsoft Hyper-V データ・ムーバー上の EXCLUDE.VMDISK ステートメントが、Microsoft SQL Server ファイル、ファイル・スペース、およびデータベースが含まれるボリュームをホストしている VHDX を誤って除外していないことを確認します。

例えば、次のとおりです。

- kingston40.vhdx には論理ボリューム C: が含まれます。
 - kingston40.vhdx には論理ボリューム E: および F: が含まれます
 - kingston40_1.vhdx のディスク・ロケーション (IDE コントローラー番号およびデバイス・ロケーション) は IDE 1 0 です。
 - kingston40_2.vhdx のディスク・ロケーションは IDE 1 1 です。
 - バックアップする Microsoft SQL Server データベース・ファイルは、E: ドライブおよび F: ドライブにあります。
2. データ・ムーバーに以下のステートメントあるいは同様のステートメントが含まれていないことを確認することで、VM バックアップから kingston40_2.vhdx を除外するステートメントがないことを確認します。

```
EXCLUDE.VMDISK KINGSTON40 "IDE 1 1"  
EXCLUDE.VMDISK * "IDE 1 1"
```

あるいは、ほとんどのハード・ディスクを除外する場合は、以下のいずれかのステートメントを使用して、VM ディスクを明示的に組み込む必要があります。

```
INCLUDE.VMDISK KINGSTON40 "IDE 1 1"  
INCLUDE.VMDISK * "IDE 1 1"
```

Include ステートメントと Exclude ステートメントは、dsm.opt ファイルに表示されているとおり、下から上に処理されます。目的を達成するには、ステートメントを正しい順序で入力します。

以下のように、コマンド・ライン・インターフェースから、VM ディスクの除外と組み込みを指定できます。

```
dsmc backup vm "KINGSTON40:-vmdisk=IDE 1 1" -asnode=KINGSTON5_HV_TGT
```

関連資料

[180 ページの『Exclude.vmdisk』](#)

EXCLUDE.VMDISK オプションは、仮想マシン・ディスクをバックアップ操作から除外します。

[184 ページの『Include.vmdisk』](#)

INCLUDE.VMDISK オプションは、バックアップ操作に仮想マシン (VM) ディスクを組み込みます。ディスク・ラベルを指定しない場合は、VM のすべてのディスクがバックアップされます。

データのリストア

アプリケーション保護機能が有効な仮想マシンをバックアップすると、元のデータベースが失われたり、損傷を受けたりした場合にデータベースをリカバリーできます。

リカバリー操作は、Data Protection for Microsoft Hyper-V バックアップから Microsoft SQL Server データベースのフルバックアップをリストアします。

仮想マシン (VM) 全体をリストアすると、VM 上のすべての Microsoft SQL Server データベースがリストアされ、VM バックアップが行われた時点にリカバリーされます。このシナリオでは、その時点の後に作成されたバックアップをリストアおよびリカバリーすることはできません。

Microsoft iSCSI Initiator Service の開始

リカバリー操作に使用されるディスクをマウントするには、iSCSI プロトコルが使用されます。Microsoft iSCSI Initiator Service を開始して、データがリストアされるシステムの「スタートアップの種類」を「自動」に設定するようにします。

手順

Windows の「サービス」で、以下のステップを実行します。

1. 「サービス」リストで「**Microsoft iSCSI Initiator Service**」を右クリックします。
2. 「プロパティ」をクリックします。
3. 「全般」タブで、以下のオプションを設定します。
 - a) 「スタートアップの種類」リストで、「自動」を選択します。
 - b) 「開始」をクリックしてから「OK」をクリックします。

タスクの結果

「サービス」リストに、「**Microsoft iSCSI Initiator Service**」が、状況は「開始」、スタートアップの種類は「自動」で表示されます。

グラフィカル・ユーザー・インターフェースを使用したデータベース・バックアップのリストア

Data Protection for Microsoft SQL Server グラフィカル・ユーザー・インターフェースを使用して、仮想マシン (VM) バックアップから Microsoft SQL Server のフル・データベース・バックアップをリカバリーすることができます。

始める前に

バックアップ・タイプ「VMVSS」を使用して Microsoft SQL Server データベースをリストアする前に、Microsoft iSCSI Initiator Service が稼働していることを確認してください。このサービスが稼働していない場合は、サービスを開始します。手順については、[120 ページの『Microsoft iSCSI Initiator Service の開始』](#)を参照してください。

手順

1. VM からフル・データベース・リカバリーを開始するには、Data Protection for Microsoft SQL Server 管理コンソール (MMC) を開始します。
2. ナビゲーション・ペインで、「データの保護およびリカバリー」ノードを展開して、Microsoft SQL Server サーバーを選択します。
3. 「リカバリー」タブで、「データベースのリストア」を選択します。すべてのバックアップ (VM バックアップからのすべてのデータベース・バックアップを含む) がリストアされます。
4. リストアするフル・データベース・バックアップを選択します。
5. 「アクション」ペインで、「リストア」をクリックします。

コマンド・ライン・インターフェースを使用したデータのリストア

必要な場合、Data Protection for Microsoft SQL Server コマンド・ライン・インターフェースを使用して、仮想マシン (VM) から Microsoft SQL Server のフル・データベース・リカバリーを開始できます。

始める前に

バックアップ・タイプ「VMVSS」を使用して Microsoft SQL Server データベースをリストアする前に、Microsoft iSCSI Initiator Service が稼働していることを確認してください。このサービスが稼働していない場合は、サービスを開始します。手順については、[120 ページの『Microsoft iSCSI Initiator Service の開始』](#)を参照してください。

手順

1. **query** コマンドを発行して、データベースのフル・データベース・バックアップおよびログ・データベース・バックアップを検索します。

次の例では、sql_db10 という名前の Microsoft SQL Server データベースのすべてのバックアップを検索します。

```
tdpsqlc q tsm sql_db10

IBM Spectrum Protect for Databases:
Data Protection for Microsoft SQL Server
Version 8, Release 1, Level 6.0
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.

Connecting to IBM Spectrum Protect Server as node 'KINGSTON40_SQL'...

Querying IBM Spectrum Protect Server for Backups ....

Backup Object Information
-----

SQL Server Name ..... SQL40
SQL Database Name ..... sql_db10
Backup Method ..... VMVSS
Backup Location ..... Srv
Backup Object Type ..... Full
Mount Points Root Directory .....
Backup Object State ..... Active
Backup Creation Date / Time ..... 07/12/2018 13:08:45
Backup Size ..... 17.00 MB
Backup Compressed ..... Yes
Backup Encryption Type ..... None
Backup Client-Deduplicated ..... Yes
Backup Supports Instant Restore ..... No
Database Object Name ..... 20180712130845
Assigned Management Class ..... STANDARD
Backup Modified .....

The operation completed successfully. (rc = 0)
```

2. トランザクション・ログを適用せずにデータベースをリストアするには、以下のコマンドを発行します。

```
tdpsqlc restore databaseName /backupMethod=vmvss
```

以下の例は、sql_db10 と呼ばれる Microsoft SQL Server データベースを指定した場合のコマンドの出力を示しています。

```

tdpsqlc restore sql_db10 /backupmethod=vmvss /sqlserver=sql40
/fromsqlserver=sql40 /recovery=no

IBM Spectrum Protect for Databases:
Data Protection for Microsoft SQL Server
Version 8, Release 1, Level 6.0
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.

Connecting to SQL Server, please wait...

Querying IBM Spectrum Protect Server for Backups ....

Connecting to IBM Spectrum Protect Server as node 'KINGSTON40_SQL'...
Connecting to Local DSM Agent 'SQL40'...
Using backup node 'KINGSTON40_SQL'...
Starting Sql database restore...

Beginning VSS restore of 'sql_db10'...

Restoring 'sql_db10' via file-level copy from snapshot(s). This
process may take some time. Please wait

Files Examined/Completed/Failed: [ 2 / 2 / 0 ] Total Bytes: 3146070

VSS Restore operation completed with rc = 0
Files Examined : 2
Files Completed : 2
Files Failed : 0
Total Bytes : 3146070
Total LanFree Bytes : 0

The operation completed successfully. (rc = 0)

```

3. フル・データベース・リストア操作が正常に完了した後、ログをリストアするためのコマンドを発行します。
- 例えば、リストアされた Microsoft SQL データベース sql_db10 に基づいてすべてのログをリストアするには、以下のコマンドを発行します。

```

tdpsqlc restore databasename log=* /sqlsever=sql40 /fromserver=sql40
/recovery=yes

```

/stopat オプションを使用して、特定時点をより細かく指定することもできます。

```

tdpsqlc restore sql_db10 log=* /sqlserver=sql40
/fromsqlserver=sql40 /recovery=yes

IBM Spectrum Protect for Databases:
Data Protection for Microsoft SQL Server
Version 8, Release 1, Level 6.0
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.

Connecting to SQL Server, please wait...
Starting Sql database restore...
Connecting to IBM Spectrum Protect Server as node 'KINGSTON40_SQL'...
Querying IBM Spectrum Protect server for a list
of database backups, please wait...

Beginning log restore of backup object sql_db10¥20180712130845¥00000DB0,
1 of 3, to database sql_db10 ...

Beginning log restore of backup object sql_db10¥20180712130845¥00000DB0,
2 of 3, to database sql_db10 ....

Total database backups inspected: 3
Total database backups requested for restore: 3
Total database backups restored: 3
Total database skipped: 0
Throughput rate: 134.32 Kb/Sec
Total bytes transferred: 385,536
Total LanFree bytes transferred: 0
Elapsed processing time: 2.80 Secs
The operation completed successfully. (rc = 0)

```

次のタスク

Data Protection for Microsoft SQL Server コマンド・ライン・インターフェース **TDPSQLC** を使用して、アクティブ状態にないバックアップをリストアできます。**restore** コマンドの発行時に、特定のバックアップのデータベース・オブジェクト名を指定します。

データベース・オブジェクト名を取得するには、以下のコマンドを入力します。

```
tdpsqlc q tsm dbname full /all
```

データベース・オブジェクト名の値を入手したら、**TDPSQLC restore** コマンドの */OBJECT=objectname* パラメーターで、そのデータベース・オブジェクト名を指定します (*objectname* がデータベース・オブジェクト名です)。例えば、次のとおりです。

```
tdpsqlc restore db44 /object=20180712130845 /backupdestination=tsm  
/backupmethod=vmvss
```

Microsoft SQL Server ログ・バックアップのリストア

フル・データベース・リストアが正常に完了した後、Data Protection for Microsoft SQL Server を使用してトランザクション・ログをリストアすることができます。

手順

ゲスト VM で、以下の手順を実行します。

1. Data Protection for Microsoft SQL Server の Microsoft 管理コンソール (MMC) を開始します。
2. Microsoft SQL Server を選択し、「リカバリー」タブをクリックします。
3. **AutoSelect** オプションが **False** に設定されていることを確認してください。
4. **RunRecovery** オプションを **True** に変更します。
5. リカバリーする必要があるログを選択します。
6. 「リストア」をクリックします。

再配置および削除されたデータベースのリストア

仮想マシン (VM) のバックアップ後に再配置および削除されたデータベースおよびログ・ファイルをリストアするためのバックアップ・ソリューションには、Data Protection for Microsoft Hyper-V と Data Protection for Microsoft SQL Server が必要です。

始める前に

データベースおよびログ・ファイル・データをリストアする場所を決定します。

このタスクについて

バックアップをリストアし、バックアップからのフル・データベース・リストア操作を実行すると、Data Protection for Microsoft Hyper-V は、ファイルを元の場所にリストアします。

バックアップ・サイクル中にデータベース・ファイルまたはログ・ファイルが再配置された場合、Data Protection for Microsoft SQL Server は、ファイルを元の場所にリストアします。

バックアップ・サイクル中にデータベースまたはログ・ファイルが作成された場合、Data Protection for Microsoft SQL Server は、新規ファイルを再作成します。バックアップ・サイクル中にデータベース・ファイルまたはログ・ファイルが削除された場合、それらのファイルはリストアされません。

手順

1. Data Protection for Microsoft Hyper-V を使用して、VM をバックアップします。
以下の例で考えてみます。

VM **kingston40** をバックアップします。この VM には、2:00 PM 時点の Microsoft SQL Server データベース **moose** が含まれており、この Microsoft SQL Server データベースは、2:00 PM 時点の以下のファイルで構成されています。

- C:\sqlldbs\moose\moose.mdf
 - C:\sqlldbs\moose\moose_log.ldf
2. データベース・バックアップを代替の位置に再配置します。
以下の例で考えてみます。データベース moose を 6:00 PM に以下のロケーションに再配置します。
- E:\sqlldbs\moose\moose.mdf
 - F:\sqlldbs\moose\moose_log.ldf
3. データベース・バックアップにファイルを追加します。
以下の例で考えてみます。2つの新規ファイルを 7:00 PM にデータベース moose に追加します。現在、このデータベースは、以下のファイルで構成されています。
- E:\sqlldbs\moose\moose.mdf
 - F:\sqlldbs\moose\moose_log.ldf
 - E:\sqlldbs\moose\moose2.ndf
 - F:\sqlldbs\moose\moose2_log.ldf
4. Data Protection for Microsoft SQL Server を使用して、ログ・バックアップを実行します。
以下の例で考えてみます。ログ・バックアップを 9:00 PM に開始します。
5. データベース・バックアップをリストアします。
以下の例で考えてみます。
- moose データベース全体をリストアすることにします。
- **runrecovery=false** を指定して、Data Protection for Microsoft Hyper-V バックアップからフル・データベースをリストアします。
 - 9:00 p.m 時点で、ログ・バックアップをリストアして適用します。
- moose データベースは、以下の場所にリストアされます。
- C:\sqlldbs\moose\moose.mdf
 - C:\sqlldbs\moose\moose_log.ldf
 - E:\sqlldbs\moose\moose2.ndf
 - F:\sqlldbs\moose\moose2_log.ldf
- VM 全体のリストアでは、ファイルを元の場所にリストアします。ログ・バックアップを適用すると、再配置の後で追加されたファイルがリストアされます。

仮想マシンのフルバックアップを確認するためのサンプル・スクリプト

Microsoft SQL Server ログをバックアップする前に、仮想マシン (VM) の有効なフルバックアップがあることを確認してください。VM のフルバックアップの存在を確認する 1 つの手順は、スクリプトの使用をスケジュールすることです。

次のサンプル・スクリプトは、フルバックアップのインスタンスを検査し、VM のフルバックアップが存在する場合は、Microsoft SQL Server ログ・バックアップを実行します。このスクリプトは、IBM Spectrum Protect スケジューラーなどのスケジューラー・サービスと一緒に使用することができます。

```
@echo off
dsmc q vm sql01_SQL -detail -asnode=datacenter01 | find /c
"database-level recovery" > c:\temp.txt
SET /p VAR=<c:\temp.txt

if %VAR% == "1" (
tdpsqlc back * log
) ELSE (
echo "There is no full backup"
set ERRORLEVEL=1
)
```

このスクリプトにより、以下のような出力が生成されます。

```
IBM Spectrum Protect for Databases:  
Data Protection for Microsoft SQL Server  
Version 8, Release 1, Level 6.0  
(C) Copyright IBM Corporation 1997, 2018. All rights reserved.
```

```
Connecting to SQL Server, please wait...  
Starting SQL database backup...  
Connecting to IBM Spectrum Protect Server as node 'SQL01_SQL'...  
Using backup node 'SQL01_SQL'...  
AC05458W The IBM Spectrum Protect Server 'backup delete' setting for node (SQL01_SQL)  
is set to NO. It should be set to YES for proper operation. 処理は続行されます。  
Beginning log backup for database model, 1 of 2.  
Full: 0 Read: 87808 Written: 87808 Rate: 32.54 Kb/Sec  
Database Object Name: 20180703011509¥000007CC  
Backup of model completed successfully.  
Beginning log backup for database sqldb test2, 2 of 2.  
Full: 0 Read: 88832 Written: 88832 Rate: 132.44 Kb/Sec  
Database Object Name: 20180703011511¥000007CC  
Backup of sqldb test2 completed successfully.  
Total SQL backups selected: 4  
Total SQL backups attempted: 2  
Total SQL backups completed: 2  
Total SQL backups excluded: 2  
Total SQL backups deduplicated: 0  
Throughput rate: 51.85 Kb/Sec  
Total bytes inspected: 176,640  
Total bytes transferred: 176,640  
Total LanFree bytes transferred: 0  
Total bytes before deduplication: 0  
Total bytes after deduplication: 0  
Data compressed by: 0%  
Deduplication reduction: 0.00%  
Total data reduction ratio: 0.00%  
Elapsed processing time: 3.33 Secs  
The operation completed successfully. (rc = 0)
```

IBM Spectrum Protect サーバー上の IBM Spectrum Protect アクティビティ・ログおよび要約拡張表を使用して、VM バックアップが正常に完了したかどうかを判別することができます。

IBM Spectrum Protect ファイル・スペース情報

ご使用の仮想マシン (VM) のファイルのファイル名や場所を知っている必要はないかもしれません。しかし、基礎となるファイル構造に関心がある場合は、Data Protection for Microsoft Hyper-V バックアップは、IBM Spectrum Protect サーバー上に Hyper-V ターゲット・ノードのノード名 (KINGSTON5_HV_TGT など) で保管されます。

以下の例は、kingston40 と呼ばれる仮想マシンのファイル・スペース情報を示しています。

```
Protect: ORION>q file KINGSTON5_HV_TGT f=d

Node Name: KINGSTON5_HV_TGT
Filespace Name: ¥VMFULL-kingston40
Hexadecimal Filespace Name:
FSID: 61
Collocation Group Name:
Platform: TDP Hyper-V
Filespace Type: API:TSMVM
Is Filespace Unicode?: No
Capacity: 0 KB
Pct Util: 0.0
Last Backup Start Date/Time: 03/13/2018 21:29:17
Days Since Last Backup Started: 31
Last Full NAS Image Backup Completion Date/Time:
Days Since Last Full NAS Image Backup Completed:
Last Backup Date/Time From Client (UTC):
Last Archive Date/Time From Client (UTC):
Last Replication Start Date/Time:
Days Since Last Replication Started:
Last Replication Completion Date/Time:
Days Since Last Replication Completed:
Backup Replication Rule Name: DEFAULT
Backup Replication Rule State: Enabled
Archive Replication Rule Name: DEFAULT
Archive Replication Rule State: Enabled
Space Management Replication Rule Name: DEFAULT
Space Management Replication Rule State: Enabled
At-risk type: Default interval
At-risk interval:
```

ゲスト仮想マシンのアプリケーション保護のトラブルシューティング

Data Protection for Microsoft Hyper-V がアプリケーション・データをホストしている仮想マシン (VM) のアプリケーション保護用に構成されており、VM バックアップ操作時に問題が発生した場合は、ご使用の環境で問題の再現を試行してください。

中断されたアプリケーション保護バックアップ中に作成されたスナップショットを削除できない

Data Protection for Microsoft Hyper-V がアプリケーション・データをホストしている VM のアプリケーション保護用に構成されている場合、`dsmc backup vm vmname` コマンドを使用して、VM のアプリケーション保護バックアップを実行することができます。ただし、**Ctrl + C** キーを押してバックアップ操作を取り消した場合、バックアップ操作によって作成されたスナップショットは自動的に削除されません。さらに、そのスナップショットは、Hyper-V Manager を使用して削除することもできません。

この問題を解決するには、**-SnapshotType Recovery** パラメーターを指定した **Get-VMSnapshot** コマンドレットを実行してから、**Remove-VMSnapshot** コマンドレットを実行してスナップショットを手動で削除する必要があります。詳しくは、[8 ページの『Windows PowerShell を使用したスナップショット管理』](#)を参照してください。

Microsoft Exchange Server データベースのアプリケーション保護バックアップ中にメッセージ ANS4063W が生成される

ゲスト VM 上で資格情報ファイルを生成せずにデータ・ムーバーからゲスト VM をバックアップした場合、メッセージ ANS4063W が生成されます。

```
ANS4063W IBM Spectrum Protect アプリケーション保護は、
アプリケーション・メタファイル「APPPROTECTIONDBINFO.XML」を VM 「<name_name>」から
コピーすることができません。
このバックアップからの個別のデータベース・リストアはサポートされていません。
アプリケーション・ライターおよびデータベースの正常性を確認してください。
```

この問題を解決するには、以下の手順を実行します。

1. ゲスト VM で、PowerShell コマンド・プロンプトから次のコマンドを実行して、ゲスト内に資格情報ファイルを生成し、プロンプトで指示されたらドメイン・ユーザー名 (*domain name¥user name*) とパスワードを入力します。

```
Get-Credential | Export-Clixml -Path `
"C:\program files\Tivoli\TSM\baclient\dsmcreds.xml"
```

ドメイン・ユーザーには、Exchange リストア権限が必要です。

2. ゲスト VM で Exchange 管理シェルから次のコマンドを実行して、資格情報を検証します。

```
$cred = Import-Clixml -Path `
"C:\program files\Tivoli\TSM\baclient\dsmcreds.xml"
$Session = New-PSSession -Credential $cred -ConfigurationName `
Microsoft.Exchange -ConnectionUri `
http://<Exchange_server_name>/PowerShell?serializationLevel=Full `
-Authentication Kerberos
Import-PSSession -Session $Session
Get-MailboxDatabase -Server <Exchange_server_name>
```

3. Hyper-V ホストまたはクラスター上のデータ・ムーバーで、Data Protection for Microsoft Hyper-V を使用してゲスト VM をバックアップします。

手順については、[79 ページの『仮想マシンのアドホック・バックアップの開始』](#)を参照してください。

関連タスク

[127 ページの『ゲスト仮想マシン上での VSS バックアップ操作およびリストア操作のトラブルシューティング』](#)

ゲスト仮想マシン (VM) 上での Volume Shadow Copy Service (VSS) バックアップまたはリストアの処理中に問題が発生した場合は、ご使用の環境で問題の再現を試行してください。

ゲスト仮想マシン上での VSS バックアップ操作およびリストア操作のトラブルシューティング

ゲスト仮想マシン (VM) 上での Volume Shadow Copy Service (VSS) バックアップまたはリストアの処理中に問題が発生した場合は、ご使用の環境で問題の再現を試行してください。

このタスクについて

問題を再現しても、以下の情報を参照しても解決できない問題がある場合は、IBM サポートに連絡して支援を依頼してください。

VSS ライター・サービスが原因で VM バックアップが失敗する

VM バックアップが失敗する原因となっている VSS ライターをバイパスし、バックアップから除外することができます。

このタスクについて

VM バックアップの前は、VSS ライターは安定状態で、エラーはありません。VM バックアップ処理中に、VSS ライターでエラーが発生し、VM バックアップ全体が失敗することがあります。

例えば、Microsoft Forefront Protection VSS ライターがゲスト VM にインストールされている場合、VM バックアップは失敗し、VSS ライターの状況が *Retryable error* 状況、*Waiting for completion* 状況、または *Stable* 以外の状況に変わります。以下の手順を実行して、ライター・サービスを VM バックアップから除外します。

手順

1. ゲスト VM 上の VSS 管理コマンド・ライン・ツールで、**vssadmin list writers** コマンドを発行し、VSS ライターをリストします。

以下のコマンド例では、Microsoft Forefront Protection VSS Writer サービスが、ライター名、ID、およびインスタンス ID によって識別されています。

```
Writer name: 'FSCVSSWriter'
Writer Id: {68124191-7787-401a-8afa-12d9d7ccc6ee}
Writer Instance Id: {f4cc5385-39a5-463b-8ab4-aafb2b35e21e}
```

```
State: [1] Stable
Last error: No error
```

2. データ・ムーバー・オプション・ファイル `dsm.opt` または `dsm.sys` に、以下の例に示すように、`EXCLUDE.VMSYSTEMSERVICE` オプションとその後に *Writer Name* を追加します。

```
EXCLUDE.VMSYSTEMSERVICE FSCVSSWriter
```

ヒント: データ・ムーバー・マシンが Linux システム上にある場合、オプション・ファイルは `dsm.sys` です。ゲスト VM とデータ・ムーバー・マシンが異なる言語セットを使用している場合は、*Writer Name* の代わりに *Writer ID* または *Writer Instance Id* を指定します。

例えば、次のとおりです。

```
EXCLUDE.VMSYSTEMSERVICE {68124191-7787-401a-8afa-12d9d7ccc6ee}
```

タスクの結果

Microsoft Forefront Protection VSS Writer サービスがゲスト VM 上で実行されている場合でも、VM バックアップは正常に完了します。

スキップされたデータベースにはアプリケーション保護ファイル `APPPROTECTIONDBINFO.XML` がなく、警告メッセージがない

特定の条件下では、バックアップ操作時に、取り外された Exchange Server データベースがスキップされ、警告は発行されません。

このタスクについて

Microsoft Exchange Server を搭載したゲスト VM の VM バックアップ中は、以下の条件が存在します。

- Exchange Server はデータベース可用性グループ (DAG) のメンバーではありません。
- すべての Exchange Server データベースが取り外されます。

以下の警告メッセージが生成されます。

```
ANS4063W IBM Spectrum Protect アプリケーション保護は、
アプリケーション・メタファイル「APPPROTECTIONDBINFO.XML」を VM「<name_name>」から
コピーすることができません。
このバックアップからの個別のデータベース・リストアはサポートされていません。
```

```
ANS4063W IBM Spectrum Protect アプリケーション保護は、
アプリケーション・メタファイル「_____L」を VM「<vm_name>」から
コピーすることができません。
このバックアップからの個別のデータベース・リストアはサポートされていません。
```

この状況では、VM バックアップはフル VM リストアでのみ使用可能です。この VM バックアップからの個別のデータベース・リストアは使用できません。

この状況を防止するには、VM バックアップ操作を開始する前に、Exchange Server データベースをマウントします。

Exchange Server DAG データベースまたは Exchange Server データベースが取り外されていると、ゲスト VM の VM バックアップ操作では、以下の警告メッセージが生成されます。

```
ANS2234W 取り外されたデータベース <database> については、
dismounted database <database>
```

DAG のメンバーでなく、取り外されている Exchange Server データベースの場合、IBM Spectrum Protect は、データベースが取り外されていることを検出しません。その結果、ANS2234W ではなく、警告メッセージ ANS4063W が生成されます。

同じトランザクション内に重複排除されたデータと重複排除されていないデータが混在していることに起因するトランザクション・エラー

特定の条件下では、同じトランザクションに重複排除されたデータと重複排除されていないデータが混在していると、トランザクション・エラーが発生します。

このタスクについて

データ重複排除が有効になっている場合、VM のアプリケーション保護を使用する Data Protection for Microsoft Hyper-V のバックアップでは、dsmerror.log ファイルに以下のエラーが生成される可能性があります。

```
ANS0246E dsmEndTxn を発行してから、新規トランザクション・セッションを開始してください。
ANS5250E 予期しないエラーが見つかりました。
IBM Spectrum Protect function name : vmSendViaFile()
IBM Spectrum Protect function      : Failed sending file
                                      /tmp/tsmvmbackup/fullvm/vmtsmvss/member1/IIS CONFIG WRITER.XML
IBM Spectrum Protect return code   : 2070
IBM Spectrum Protect file          : vmmigration.cpp (1383)
```

このエラーはリカバリー可能であり、無視できます。このエラーが起こるのは、Data Protection for Microsoft Hyper-V が、重複排除されたデータと同じトランザクションで (サイズが小さいために重複排除から除外された) XML ファイルを送信しようとする場合です。Data Protection for Microsoft Hyper-V は、エラー・メッセージで示された XML ファイルを新規トランザクションで再送信します。

データベース・リストア操作中に PowerShell がメモリーを使い尽くす可能性がある

Data Protection for Microsoft Exchange Server 管理コンソールを使用して Microsoft Exchange Server データベースをリストアする場合、Windows PowerShell が以下のエラーで失敗する可能性があります。

```
APPCRASH
Not available
0
powershell.exe
10.0.14409.1005
584a185c
tsmapi64.dll
8.1.6.14
5af94075
c00000fd
000000000022df88
```

例外コード 0xc00000fd は、スタック・オーバーフロー例外が発生したことを示します。この問題を解決するには、**MaxMemoryPerShellMB** 割り当て量を使用して、PowerShell に割り振られるメモリーの最大量を増やします。

グループ・ポリシー・エディター (**gpedit.msc**) または PowerShell を使用して **MaxMemoryPerShellMB** 割り当て量の値を変更する方法について詳しくは、[https://msdn.microsoft.com/en-us/library/ee309367\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ee309367(v=vs.85).aspx) を参照してください。デフォルト値は 150 ですが、推奨される値は 1024 です。

第7章 インスタント・アクセス操作の実行

インスタント・アクセス操作を実行して、仮想マシン (VM) バックアップの整合性を検証したり、インスタント・アクセス操作で作成されたリソースをクリーンアップしたりすることができます。

このタスクについて

元の VM が削除された場合や、そのディスクやデータが破損したり使用できなくなった場合に、以前にバックアップされた VM イメージを使用してシステムを正常にリストアできるかを確認することができます。

インスタント・アクセス操作を実行すると、一時仮想マシンが作成されます。この一時 VM を使用してバックアップ・データを検証することはできますが、元の VM はリストアされません。

インスタント・アクセス操作を実行するには、データ・ムーバー・コマンド・ライン、Data Protection for Microsoft Hyper-V 管理コンソール、または Windows PowerShell コマンドレットを使用することができます。

クラスター環境でインスタント・アクセス操作を実行する場合、VM が稼働しているホスト、またインスタント・アクセス操作の開始元のホストに関係なく、任意のクラスター・ノードがそのホスト iSCSI サービスを使用してインスタント・アクセス操作を実行できます。

パフォーマンスのヒント：

インスタント・アクセス操作を頻繁に使用する場合は、仮想ボリュームの一時書き込みキャッシュのロケーションを変更することを検討してください。デフォルトのロケーションは、ローカル・ハード・ディスク (c:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\) 上です。このロケーションは、インスタント・アクセス・モードで稼働している VM から、電源オンの状態で一時的に VM ディスク書き込み変更を保管するために使用されます。

Hyper-V ゲストでの入出力 (I/O) 待ち時間を短縮するためには、IBM Spectrum Protect リカバリー・エージェント GUI を使用して Hyper-V ホスト上の最も高速なディスク (ソリッド・ステート・ドライブ (SSD) や SAN ボリュームなど) を一時書き込みキャッシュに指定してください。インスタント・アクセス・モードで稼働している VM に対して行われた変更は、一時的にしか保管されません。インスタント・アクセス VM をクリーンアップする際に、一時書き込みキャッシュは IBM Spectrum Protect サーバーに保管されません。一時書き込みキャッシュ・パス内のすべてのファイルが削除されます。ただし、VM の名前が付いたフォルダーはそのまま残ります。

仮想ボリューム書き込みキャッシュの設定の変更について詳しくは、[51 ページの『IBM Spectrum Protect リカバリー・エージェント GUI の構成』](#)を参照してください。

コマンド・ラインからの VM バックアップの整合性の検証

仮想マシン (VM) やディスクを Hyper-V ホストにリストアすることなく VM のバックアップ・イメージの整合性を検証するには、データ・ムーバー・コマンド・ラインでフル VM インスタント・アクセス操作を実行します。

始める前に

[131 ページの『第7章 インスタント・アクセス操作の実行』](#)に記載されている情報を確認します。

手順

Hyper-V ホストまたはクラスター上のデータ・ムーバー・コマンド・ラインで、以下のステップを実行します。

1. **restore vm** コマンドを使用して、VM インスタント・アクセス操作を実行します。

既存の VM が稼働しているため、新規名を **vmname** オプションに追加することで、一時 VM の新規名を指定する必要があります。また、操作がインスタント・アクセス・リストア操作であることを示すために、コマンド・ラインに **-VMRESToretype=INSTANTAccess** オプションを追加する必要があります。

一時 VM の電源が自動的にオンになるようにしたい場合、`-vmautostartvm=yes` オプションを使用します。

例えば、Orion という名前の VM のバックアップ・イメージをリストア操作に使用できるかを検証する必要があるとします。次のコマンドを入力して、インスタント・アクセス用に「Orion_verify」という名前の VM を準備します。この VM を使用して、バックアップ・イメージをリストアできるかを検証することができます。

```
dsmc restore vm Orion -vmname=Orion_verify -vmrestoretype=instantaccess
```

重要: リストアしている VM が静的 IP アドレスを使用している場合、元の VM と一時 VM の間でネットワーク IP アドレスの競合が発生します。この競合を回避するには、一時インスタント・アクセス VM の作成後に、その VM の IP アドレスを変更します。

2. オプション: 特定の日付または時刻から非アクティブまたはアクティブな VM バックアップを選択し、**inactive** オプションまたは **pick** オプション、あるいは **pittime** オプションまたは **pitdate** オプションを使用して、VM バックアップのバージョンをリストします。

例えば、Orion VM のバックアップ・バージョンのリストを表示するには、次のコマンドを発行します。

```
dsmc restore vm Orion -vmrestoretype=instantaccess -pick
```

インスタント・アクセス操作によって作成された一時データは、IBM Spectrum Protect リカバリー・エージェントのキャッシュに保管されます。

3. ディスクとデータの整合性を確認するには、**chkdsk** などのユーティリティー、あるいは任意のユーティリティーまたはアプリケーションを使用して、仮想ディスクおよびデータを検証します。一時 VM が整合性チェックに合格したら、インスタント・アクセス・リストア操作をサポートするために作成された一時リソースを除去することができます。

例

「Ritza2-VM」という名前の VM バックアップに対してインスタント・アクセス操作を実行し、VM を一時的に「Ritza2-VM_Verify」としてリストアします。この例では、ターゲット・ノード名は「RITZA_HV_TGT」で、データ・ムーバー・ノード名は「RITZA_HV_DM」です。


```
dsmc restore vm "Ritza2-VM" -vmname="Ritza2-VM_Verify" -vmrestoretype=instantaccess
-optfile="dsm.RITZA_HV_DM.opt" -asnode="RITZA_HV_TGT"
```

```
IBM Spectrum Protect
Command Line Backup-Archive Client Interface
  Client Version 8, Release 1, Level 7.0
  Client date/time: 07/19/2018 13:06:23
(c) Copyright by IBM Corporation and other(s) 1990, 2018. All Rights Reserved.
```

```
Node Name: RITZA_HV_DM
Session established with server ASANA2: Linux/x86_64
  Server Version 7, Release 1, Level 9.000
  Server date/time: 07/19/2018 13:04:32 Last access: 07/19/2018 13:03:56
```

```
Accessing as node: RITZA_HV_TGT
Restore function invoked.
```

Restore VM command started. Total number of virtual machines to process: 1

Restore of Virtual Machine 'Ritza2-VM' started

Starting instant access of VMware Virtual Machine 'Ritza2-VM' target node name='RITZA_HV_TGT', data mover node name='RITZA_HV_DM'

Starting Instant VM Access process

Restoring VM configuration information for 'Ritza2-VM'
Checking the state of the hypervisor host 'RITZA'...
Checking Hyper-V target path 'C:\ProgramData\Microsoft\Windows\Hyper-V' from host 'RITZA'

Gathering iSCSI information from Hyper-V host 'RITZA' ...

The Windows iSCSI Initiator name is "iqn.1991-05.com.microsoft:ritza.tsmdev.local".

Mounting a snapshot of VM 'Ritza2-VM' from disc 'Hard Disk 1'. Please wait...

Connecting the iSCSI targets with the data mover...

Creating a virtual machine on the hypervisor host...

Successful Full VM restore of Virtual Machine 'Ritza2-VM'
ANS2408I The virtual machine named 'Ritza2-VM_Verify' is ready for Instant Access

Successful instant access of VMware Virtual Machine 'Ritza2-VM' target node name='RITZA_HV_TGT', data mover node name='RITZA_HV_DM'

```
Total number of objects restored:          1
Total number of objects failed:            0
Total number of bytes transferred:         0 B
Data transfer time:                       0.00 sec
Network data transfer rate:               0.00 KB/sec
Aggregate data transfer rate:             0.00 KB/sec
Elapsed processing time:                   00:01:03
```

関連タスク

[134 ページの『コマンド・ラインを使用したインスタント・アクセス・リソースの解放』](#)

クリーンアップ操作を実行することで、インスタント・アクセス操作で作成されたリソースを解放することができます。

[136 ページの『Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス操作の実行』](#)

Data Protection for Microsoft Hyper-V 管理コンソールから、簡単にインスタント・アクセス操作を実行することができます。

関連資料

[218 ページの『Vmrestoretype』](#)

vmrestoretype オプションは、実行または照会するリストア操作のタイプを指定するために、**query VM** コマンドまたは **restore VM** コマンドで使います。

[198 ページの『vmautostartvm』](#)

vmautostartvm オプションを使用して、インスタント・アクセス処理中に作成された仮想マシン (VM) を自動的に電源オンするかどうかを指定します。このオプションは、**restore VM** **vmrestoretype=instantaccess** コマンドと一緒に使用した場合にのみ有効です。

141 ページの『Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット』

仮想マシン (VM) データの保護に使用できる Data Protection for Microsoft Hyper-V コマンドレットを検討します。

関連情報

149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』

コマンド・ラインを使用したインスタント・アクセス・リソースの解放

クリーンアップ操作を実行することで、インスタント・アクセス操作で作成されたリソースを解放することができます。

このタスクについて

一時インスタント・アクセス仮想マシン (VM) が存在するかどうかを判別してから、データ・ムーバー・コマンド・ラインでクリーンアップ操作を実行する必要があります。

手順

1. -VMRESToretype=INSTANTAccess オプションを指定して **query vm** コマンドを実行します。このコマンドは、インスタント・アクセス・モードで稼働しているすべての一時 VM を表示します。

```
dsmc query vm * -VMREST=INSTANTA
```

-Detail オプションを **query vm** コマンドに追加することで、各一時 VM の詳細情報を表示することができます。例えば、次のコマンドを発行します。

```
dsmc query vm vmname -VMREST=INSTANTA -detail
```

ここで、*vmname* は、一時 VM の名前を指定します。

2. インスタント・アクセス操作で作成されたリソースを除去します。

例えば、「Orion_verify」という名前の一時 VM 用に作成されたリソースを除去するには、次のコマンドを発行します。

```
dsmc restore vm Orion -vmname=Orion_verify -VMRESToretype=VMCleanup
```

-VMRESToretype=VMCleanup オプションは、一時 VM を Hyper-V ホストから削除し、マウント済みのすべての iSCSI マウントをアンマウントし、iSCSI デバイス・リストを Hyper-V ホストから消去します。VM を削除すると、すべての一時生成データも削除されます。

例

インスタント・アクセス・クリーンアップ操作を実行して、インスタント・アクセス操作で作成されたリソースを除去します。

以下の例は、一時 VM 「kingston30-avi_Verify」をクリーンアップするために使用されるコマンドを示しています。このケースでは、VM 名は「kingston30-avi」、ターゲット・ノード名は「KINGSTON10_HV_TGT」、データ・ムーバー・ノード名は「KINGSTON10_HV_DM」です。

```
dsmc restore vm "kingston30-avi" -vmname="kingston30-avi_Verify" -  
vmrestoretype=vmcleanup  
-optfile="dsm.KINGSTON10_HV_DM.opt" -asnode="KINGSTON10_HV_TGT"
```

IBM Spectrum Protect

Command Line Backup-Archive Client Interface

Client Version 8, Release 1, Level 7.0

Client date/time: 07/25/2018 09:13:01

(c) Copyright by IBM Corporation and other(s) 1990, 2018. All Rights Reserved.

Node Name: KINGSTON10_HV_DM

Session established with server ASANA2: Linux/x86_64

Server Version 7, Release 1, Level 9.000

Server date/time: 07/25/2018 09:11:54 Last access: 07/25/2018 09:09:33

Accessing as node: KINGSTON10_HV_TGT

Restore function invoked.

Restore VM command started. Total number of virtual machines to process: 1

Restore of Virtual Machine 'kingston30-avi' started

Starting cleanup of VMware Virtual Machine 'kingston30-avi_Verify' from snapshot of
'kingston30-avi' target node name='KINGSTON10_HV_TGT', data mover node
name='KINGSTON10_HV_DM'

Starting Instant VM Access cleanup process

Restoring VM configuration information for 'kingston30-avi'

Checking the state of the hypervisor host 'KINGSTON10'...

Powering off the virtual machine ...

Removing the virtual machine from the Hyper-V host...

Disconnecting iSCSI targets from the data mover...

Dismounting a snapshot of VM 'kingston30-avi' from target
'kingston30-avi9verify-hard8disk31'.

Please wait...

Cleanup operation of instant access VM 'kingston30-avi_Verify' completed successfully

Successful cleanup of VMware Virtual Machine 'kingston30-avi_Verify' from snapshot of
'kingston30-avi' target node name='KINGSTON10_HV_TGT', data mover node
name='KINGSTON10_HV_DM'

Total number of objects restored:	1
Total number of objects failed:	0
Total number of bytes transferred:	0 B
Data transfer time:	0.00 sec
Network data transfer rate:	0.00 KB/sec
Aggregate data transfer rate:	0.00 KB/sec
Elapsed processing time:	00:00:22

次のタスク

Restore-DpHvVm コマンドレットで **-restoreType VmCleanup** パラメーターを使用して、インスタント・アクセス・リソースを解放することもできます。詳細については、[149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』](#)を参照してください。

関連資料

[218 ページの『Vmrestoretype』](#)

vmrestoretype オプションは、実行または照会するリストア操作のタイプを指定するために、**query VM** コマンドまたは **restore VM** コマンドで使用します。

161 ページの『Query VM』

query VM コマンドは、正常に完了した仮想マシン (VM) のバックアップをリストし、検査するために使用します。

Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス操作の実行

Data Protection for Microsoft Hyper-V 管理コンソール から、簡単にインスタント・アクセス操作を実行することができます。

始める前に

131 ページの『第 7 章 インスタント・アクセス操作の実行』に記載されている情報を確認します。

このタスクについて

インスタント・アクセス操作を実行すると、一時仮想マシン (VM) が作成されます。この一時 VM を使用してバックアップ・データを検証することはできますが、元の VM はリストアされません。

手順

一時インスタント・アクセス VM を作成するには、Hyper-V ホストまたはクラスターで以下のステップを実行します。

1. Data Protection for Microsoft Hyper-V 管理コンソールを開始します。
2. ナビゲーション・ペインで、ホスト・ノードまたはクラスター・ノードをクリックします。
3. 「仮想マシン」ビューの VM 表で VM を選択します。
例えば、データ保護状況が「正常」である VM をクリックします。

ヒント:「削除済み」状態の VM に対してインスタント・アクセス操作を実行することもできます。

4. 「アクション」ペインで、「リストア」をクリックします。
5. 該当する場合、「リストア」ウィザードで以下のページを完了します。ウィザードで選択するオプションによって、表示されるページが異なります。

ウィザード・ページ	アクション
始める前に	「次へ」をクリックして、ウィザードを開始します。
リストア・ポイントの選択	カレンダーで強調表示された日付にリストア・ポイントが含まれます。リストア・ポイントは、リストア操作に使用できる VM バックアップです。一部の VM には、1 日あたり複数のリストア・ポイントがあります。 「使用可能なリストア・ポイント」リストから日付とリストア・ポイントを選択してください。VM のサイズは、使用可能なリストア・ポイントの横にリストされます。VM は、バックアップされたときの状態にリストアされます。
オプションの選択	インスタント・アクセス VM を作成するには、以下の手順を実行します。 a. 以下のいずれかのオプションをクリックします。 インスタント・アクセス仮想マシンの作成 インスタント・アクセス操作で使用する一時 VM を作成します。VM の電源をオンにしないでください。 インスタント・アクセス仮想マシンの作成および始動 インスタント・アクセス操作に使用する一時 VM を作成し、自動的に VM の電源をオンにします。

ウィザード・ページ	アクション
	b. 「 仮想マシン名 」フィールドに、一時インスタント・アクセス VM の新規名を入力します。 c. クラスタ構成の場合は、「 仮想マシンのリストア先 」フィールドで、インスタント・アクセス VM を作成するホストを選択します。元の VM と同じホストを選択することも、クラスタ内の別のホストを選択することもできます。
要約	ウィザードで選択したオプションを確認します。「 次へ 」をクリックして、リストア操作を開始します。
結果	「 完了 」をクリックしてウィザードを閉じます。

重要: リストアしている VM が静的 IP アドレスを使用している場合、元の VM と一時 VM の間でネットワーク IP アドレスの競合が発生します。この競合を回避するには、一時インスタント・アクセス VM の作成後に、その VM の IP アドレスを変更します。

タスクの結果

開始したリストア操作が、管理コンソールの結果ペインのタスク・リストに表示されます。

リストア操作が完了すると、インスタント・アクセス VM が「**仮想マシン**」ビューまたは「**スケジュール・ヒストリー**」ビューに表示されます。VM の「**VM タイプ**」列には、「**インスタント・アクセス**」タイプが表示されます。

インスタント・アクセス操作によって作成された一時データは、IBM Spectrum Protect リカバリー・エージェント のキャッシュに保管されます。

次のタスク

ディスクとデータの整合性を確認するには、**chkdsk** などのユーティリティー、あるいは任意のユーティリティーまたはアプリケーションを使用して、仮想ディスクおよびデータを検証します。一時 VM が整合性チェックに合格したら、インスタント・アクセス・リストア操作をサポートするために作成された一時リソースを除去することができます。

バックアップ・データの検証が完了した後、インスタント・アクセス VM を除去するには、[137 ページの『Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス VM の除去』](#)の指示に従ってください。

関連タスク

[131 ページの『コマンド・ラインからの VM バックアップの整合性の検証』](#)

仮想マシン (VM) やディスクを Hyper-V ホストにリストアすることなく VM のバックアップ・イメージの整合性を検証するには、データ・ムーバー・コマンド・ラインでフル VM インスタント・アクセス操作を実行します。

関連情報

[149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』](#)

Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス VM の除去

インスタント・アクセス仮想マシン (VM) が不要になった場合は、Data Protection for Microsoft Hyper-V 管理コンソールを使用してその VM を除去することができます。

このタスクについて

インスタント・アクセス VM を除去すると、一時 VM が Hyper-V ホストから削除され、マウント済みのすべての iSCSI マウントがアンマウントされ、iSCSI デバイス・リストが Hyper-V ホストから消去されます。VM を削除すると、すべての一時生成データも削除されます。

手順

インスタント・アクセス VM を除去するには、Hyper-V ホストで以下のステップを実行します。

1. [Data Protection for Microsoft Hyper-V 管理コンソール](#)を開始します。
2. ナビゲーション・ペインで、クラスター・ビューまたはホスト・ビューのホストをクリックします。
3. 「仮想マシン」ビューの VM 表で、除去するインスタント・アクセス VM を選択します。 インスタント・アクセス・モードになっている VM は、「状況」列の「インスタント・アクセス」項目で識別されます。
4. 「アクション」ペインで、「インスタント・アクセス VM の削除」をクリックします。

プロンプトが表示されたら、インスタント・アクセス VM を除去することを確認します。

関連タスク

[131 ページの『コマンド・ラインからの VM バックアップの整合性の検証』](#)

仮想マシン (VM) やディスクを Hyper-V ホストにリストアすることなく VM のバックアップ・イメージの整合性を検証するには、データ・ムーバー・コマンド・ラインでフル VM インスタント・アクセス操作を実行します。

関連情報

[149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』](#)

Hyper-V ホストが再始動した後のインスタント・アクセス VM の制約事項

Hyper-V ホストを再始動する場合、インスタント・アクセス操作で作成された仮想マシン (VM) に関する制約事項があります。

デフォルトでは、Hyper-V ホストを再始動すると、Hyper-V ホスト内の VM は保存済み状態に変更され、再始動後に自動的に始動します。このアクションは、インスタント・アクセス操作で作成された VM には適用されません。再始動の後、Recovery Agent によって提供されていたディスクは存在なくなっています。インスタント・アクセス VM へのアクセスを回復するには、クリーンアップしてからインスタント・アクセス操作を再実行する必要があります。

関連タスク

[137 ページの『Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス VM の除去』](#)

インスタント・アクセス仮想マシン (VM) が不要になった場合は、Data Protection for Microsoft Hyper-V 管理コンソールを使用してその VM を除去することができます。

[136 ページの『Data Protection for Microsoft Hyper-V 管理コンソールからのインスタント・アクセス操作の実行』](#)

Data Protection for Microsoft Hyper-V 管理コンソールから、簡単にインスタント・アクセス操作を実行することができます。

[134 ページの『コマンド・ラインを使用したインスタント・アクセス・リソースの解放』](#)

クリーンアップ操作を実行することで、インスタント・アクセス操作で作成されたリソースを解放することができます。

[131 ページの『コマンド・ラインからの VM バックアップの整合性の検証』](#)

仮想マシン (VM) やディスクを Hyper-V ホストにリストアすることなく VM のバックアップ・イメージの整合性を検証するには、データ・ムーバー・コマンド・ラインでフル VM インスタント・アクセス操作を実行します。

第 8 章 Windows PowerShell コマンドレットを使用した仮想マシンの保護

Microsoft Windows PowerShell コマンドレット (バージョン 3.0 以降) を使用して、Data Protection for Microsoft Hyper-V 操作を実行できます。

このタスクについて

PowerShell コマンドレットを使用する準備に関する情報、使用可能なコマンドレットのリスト、およびこれらのコマンドレットを使用する共通タスクが提供されています。

制約事項: PowerShell コマンドレットは、Data Protection for Microsoft Hyper-V REST API と対話して、仮想マシンを保護します。REST API と直接対話することはできません。提供された PowerShell コマンドレットを使用して Data Protection for Microsoft Hyper-V 操作を実行する必要があります。

Data Protection for Microsoft Hyper-V で PowerShell コマンドレットを使用する準備

Data Protection for Microsoft Hyper-V には、環境内で Data Protection for Microsoft Hyper-V 操作を管理するのに役立つ一連の Windows PowerShell コマンドレットが含まれています。

始める前に

Data Protection for Microsoft Hyper-V がインストールされているシステム上で、Microsoft Windows PowerShell 3 以降が使用可能であることを確認してください。どのバージョンの PowerShell がインストールされているのかを確認するには、PowerShell セッションで次のコマンドを入力します。

```
PS C:\> $PSVersionTable.PSVersion
```

Major 列の数字が PowerShell のバージョンです。

このタスクについて

PowerShell コマンド・ラインで対話式にコマンドレットを実行するか、Data Protection for Microsoft Hyper-V 操作の自動化に役立つスクリプトに組み込むことができます。

コマンドレットを使用するには、事前に以下の手順を実行する必要があります。

手順

1. Microsoft Windows PowerShell または Microsoft Windows PowerShell ISE セッションを管理者権限で開始します。
 - a) 「スタート」 > 「すべてのプログラム」 > 「アクセサリ」 > 「Windows PowerShell」をクリックします。
 - b) 「Windows PowerShell」を右クリックして、「管理者として実行」をクリックします。
2. 次のコマンドを発行して、実行ポリシーが RemoteSigned に設定されていることを確認します。

```
PS C:\> Get-ExecutionPolicy
```

別のポリシーが表示されている場合は、次のコマンドを発行して、実行ポリシーを RemoteSigned に設定します。

```
PS C:\> Set-ExecutionPolicy RemoteSigned
```

ヒント: Set-ExecutionPolicy コマンドは、一度しか実行できません。

3. コマンドレットを使用可能にするために、Data Protection for Microsoft Hyper-V PowerShell モジュールをインポートします。

```
PS C:\> Import-Module "C:\Program Files\IBM\SpectrumProtect\DPHyperV\dpvhvModule.dll"
```

4. セッション・コマンドレットを使用して、Data Protection for Microsoft Hyper-V に対して認証を行います。

```
$cred = Get-Credential -UserName user_name -message "credential"
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
```

ここで、

user_name

Data Protection for Microsoft Hyper-V がインストールされている Windows システムへのログインに使用するアカウントを指定します。

computer_name

Data Protection for Microsoft Hyper-V がインストールされているサーバーの名前を指定します。

5. 接続先のホストに関連付けられているセキュリティー証明書が認識されない場合、あるいはローカル・サーバー (PowerShell コマンドレットがインストールされているサーバー) 上でない場合、セッション・コマンドレットは失敗します。 **-Force** パラメーター (証明書を無視する場合) または **-CertificatePrompt** パラメーター (新規証明書のインストールを求めるプロンプトを表示する場合) を指定して、**New-DpHvSession** コマンドレットを再実行する必要があります。Features on Demand がインストールされているかどうかに関係なく、Windows Core OS では、**-Force** パラメーターを使用します。新規証明書のインストールの場合、**-CertificatePrompt** パラメーターはサポートされていません。

例えば、次のセッション・コマンドレットを実行します。

```
$cred = Get-Credential -UserName user_name -message "credential"
$session = New-DpHvSession -ComputerName computer_name -Credential $cred `
-CertificatePrompt
```

プロンプトが表示されたら、スタンドアロン・ホストまたはクラスター内の各ホストに対して、以下のステップを実行します。

- a) 「<host name> への接続の保護」ウィンドウで、「証明書の表示」をクリックします。
その他のオプション (現行セッションの証明書警告を無視する「はい」、接続を停止する「いいえ」、または今後すべての証明書の警告を無視する「このコンピューターへの接続について今後確認しない」など) を選択すると、Data Protection for Microsoft Hyper-V に接続できなくなります。
- b) 「証明書」ウィンドウの「一般」タブで、「証明書のインストール」をクリックします。
- c) 「証明書のインポート ウィザード」ウィンドウのウェルカム・ページで、ストア・ロケーション (「現在のユーザー」または「ローカル コンピューター」) を選択し、「次へ」をクリックします。
- d) 「証明書ストア」ページで、「証明書をすべて次のストアに配置する」をクリックし、「参照」をクリックします。
- e) 「証明書ストアの選択」ウィンドウで、「信頼されたルート証明機関」を選択し、「OK」をクリックします。
- f) 「証明書ストア」ページで「次へ」をクリックします。
- g) 「証明書のインポート ウィザードの完了」ページで選択内容を確認して、「完了」をクリックします。
- h) 「セキュリティー警告」ウィンドウで「はい」をクリックし、証明書をインストールします。
- i) 確認ウィンドウで「OK」をクリックします。

証明書を拒否した場合、**-Force** パラメーターを使用しない限り、Data Protection for Microsoft Hyper-V に接続することはできません。

6. [141 ページの『Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット』](#) で使用可能なコマンドレットのリストを参照します。

7. オプション: 各コマンドレットのオンライン・ヘルプを確認します。詳細については、[144 ページの『PowerShell コマンドレットのヘルプ情報の表示』](#)を参照してください。

次のタスク

コマンドレットを使用したスクリプトの作成、実行、モニター、およびトラブルシューティングについては、Windows PowerShell 3.0 以降の資料を参照してください。Windows PowerShell コマンドレット、一貫性のある命名パターン、パラメーター、引数、および構文について詳しくは、[Microsoft TechNet: Windows PowerShell ファースト ステップ ガイド](#)を参照してください。

Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット

仮想マシン (VM) データの保護に使用できる Data Protection for Microsoft Hyper-V コマンドレットを検討します。

以下の表に、Data Protection for Microsoft Hyper-V で使用可能なコマンドレットを示します。

表 14. Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット	
コマンドレット名	説明
Backup-DpHvVm	Hyper-V VM をバックアップします。 関連: dsmc backup vm
Get-DpHvBackup	VM バックアップに関する情報を表示します。 関連コマンド: dsmc query vm
Get-DpHvBackupSchedule	Hyper-V ホストまたはクラスター内の VM の適格なバックアップ・スケジュールのリストを表示します。 適格なスケジュールは、IBM Spectrum Protect サーバー管理者が定義する必要があり、Hyper-V VM のターゲットとなるドメインに対して定義されなければなりません。 スケジュール定義には以下のパラメーターおよびオプションが含まれている必要があります。 <ul style="list-style-type: none">• -domain.vmfull="all-vm" オプションが、オプション・ストリングで指定される必要があります。• スケジュールには ACTION=BACKUP および SUBACTION=VM パラメーターが含まれている必要があります。
Get-DpHvHostConfiguration	IBM Spectrum Protect サーバーからの Hyper-V ホストの構成情報を表示します。
Get-DpHvIaVm	インスタント・アクセス・モードの VM のリストを表示します。VM の属性も表示されます。 インスタント・アクセス VM は、インスタント・アクセス操作用に作成される一時 VM です。詳細については、 149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』 を参照してください。

表 14. Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット (続き)	
コマンドレット名	説明
Get-DpHvLastSuccessfulBackup	<p>ホストまたはクラスターで実行された、最近の VM バックアップ操作に関する情報を表示します。</p> <p>以下の情報が戻されます。VM バックアップの危険状況、バックアップ日付、バックアップの期間、送信されたデータの量、バックアップのタイプ、VM が属するホスト (クラスターの場合)、および実行されたスケジュールの名前。</p>
Get-DpHvLog	ノードに関するエラー・ログ項目を返します。ログ項目をファイルに保存し、ファイル名を指定することができます。
Get-DpHVLogSection	開始行番号と表示する行数を指定すると、エラー・ログのセクションが返されます。
Get-DpHvPolicyDomain	<p>IBM Spectrum Protect サーバー上のポリシー・ドメインのリストを表示します。</p> <p>関連コマンド: dsmadmc q domain</p>
Get-DpHvRCInfo	戻りコードに関する情報を表示します。
Get-DpHvScheduleHistory	<p>実行されたスケジュールのリストを表示します。</p> <p>戻される各スケジュールには、スケジュール実行の開始時刻、スケジュールの名前、スケジュールの状況、バックアップされたかバックアップに失敗した VM の数、およびスケジュール実行の期間を含むことができます。</p>
Get-DpHvScheduleHistoryDetail	<p>スケジュール実行でバックアップされた VM ごとの情報を表示します。</p> <p>戻される各バックアップ・タスクには、VM の名前、バックアップの状況、バックアップの開始時刻、および失敗したバックアップのエラー・コードを含むことができます。</p>
Get-DpHvTask	完了したタスクと実行中のタスクに関する情報を表示します。
Get-DpHvVvm	<p>Hyper-V ホストで、VM インベントリーの情報を表示します。</p> <p>関連コマンド: dsmc show vm</p>
Get-DpHvVMAtRisk	<p>VM の現行の危険ポリシーを表示します。危険ポリシーにより、バックアップ操作が指定の時間内に行われなかった場合に、VM が危険として表示される時点が決まります。</p> <p>危険ポリシーは危険タイプで構成されます。危険タイプは数値であり、0 (BYPASS)、1 (CUSTOM)、または 2 (DEFAULT) です。カスタム危険タイプには、危険間隔 (時間単位) があります。</p>

表 14. Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット (続き)	
コマンドレット名	説明
Get-DpHvVMBackupHistory	IBM Spectrum Protect サーバー上の要約拡張表から VM のバックアップ・ヒストリーを表示します。 戻される各バックアップ・タスクには、バックアップの最終実行時間、バックアップの状況、バックアップの期間、送信されたデータの量、VM が属するホスト (クラスターの場合)、および戻されたエラー・コードがある場合はそのエラー・コードを含むことができます。
Get-DpHvVmBackupTaskHistory	Data Protection for Microsoft Hyper-V 上でローカルに保管された VM バックアップ・タスク・ヒストリーを表示します。
Get-DpHvVmRestoreTaskHistory	Data Protection for Microsoft Hyper-V 上でローカルに保管された VM リストア・タスク・ヒストリーを表示します。
New-DpHvFsInfo	Set-DpHvVmAtRisk コマンドレットで使用するための FsInfo オブジェクトを作成します。FsInfo オブジェクトは、IBM Spectrum Protect ファイル・スペース ID、および危険ポリシーを設定する VM の名前を指定します。
New-DpHvNodeInfo	Set-DpHvHostConfiguration コマンドレットで使用するための NodeInfo オブジェクトを作成します。NodeInfo オブジェクトは、Hyper-V ホスト上のノード名とノード・タイプを指定します。
New-DpHvSession	Data Protection for Microsoft Hyper-V に対して認証し、PowerShell コマンドレット・セッションを開始します。
Receive-DpHvTask	バックアップまたはリストアのタスクをモニターします。
Remove-DpHvSession	Data Protection for Microsoft Hyper-V のセッションを閉じます。
Restore-DpHvVm	Hyper-V VM をリストアします。 インスタント・アクセス操作を実行して、VM バックアップをリストアできるかどうかを検証することもできます。詳しくは、149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』を参照してください。 関連コマンド: dsmc restore vm
Set-DpHvBackupSchedule	スケジュールを Hyper-V ホストまたはクラスター上のデータ・ムーバーに関連付けます。 ノードをスケジュールに関連付け、ノードをスケジュールから除去し、ターゲット・ノードをスケジュールに関連付けることができます。
Set-DpHvHostConfiguration	Data Protection for Microsoft Hyper-V 操作のために Hyper-V ホストを構成します。

表 14. Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット (続き)	
コマンドレット名	説明
Set-DpHvHttpsPort	IBM Spectrum Protect Web サーバーに使用される HTTPS ポートを設定します。
Set-DpHvMmcLoginPreferences	Data Protection for Microsoft Hyper-V 管理コンソールの設定を行います。
Set-DpHvVmAtRisk	1 つ以上の VM に危険ポリシーを設定します。危険ポリシーにより、バックアップ操作が指定の時間内に行われなかった場合に、VM が危険として表示される時点が決まります。 危険ポリシーは危険タイプで構成されます。危険タイプは数値であり、0 (BYPASS)、1 (CUSTOM)、または 2 (DEFAULT) です。カスタム危険タイプには、危険間隔 (時間単位) があります。
Set-ServerConnection	Hyper-V ホストに関する IBM Spectrum Protect サーバー接続情報を保管し、サーバーとの接続を確認します。
Show-DpHvHttpsPort	IBM Spectrum Protect Web サーバーのポート情報を表示します。
Show-DpHvMmcLoginPreferences	Data Protection for Microsoft Hyper-V 管理コンソールの設定を表示します。
Stop-DpHvTask	バックアップまたはリストア・タスクを取り消します。
Test-DpHvConfiguration	Data Protection for Microsoft Hyper-V の構成を検証します。
Test-DomainCredentials	Windows ドメイン・ユーザーの資格情報を確認します。

コマンドレットの共通タスクのリストについては、[145 ページの『Data Protection for Microsoft Hyper-V コマンドレットの例』](#)を参照してください。

PowerShell コマンドレットのヘルプ情報の表示

PowerShell コマンドレットにはオンライン・ヘルプが用意されています。特定のコマンドレットの詳細を表示するには、**Get-Help** コマンドレットにコマンドレット名を指定して実行します。

```
Get-Help cmdlet_name
```

例えば、次のとおりです。

```
Get-Help Backup-DpHvVm
```

次は、**Backup-DpHvVm** コマンドレットの場合の例です。コマンドレットのサンプルを確認するには、次のように入力します。

```
Get-Help Backup-DpHvVm -examples
```

詳細情報を表示するには、次のように入力します。

```
Get-Help Backup-DpHvVm -detailed
```

技術情報を表示するには、次のように入力します。

```
Get-Help Backup-DpHvVm -full
```

オンライン製品情報を表示するには、次のように入力します。


```
Get-Help Backup-DpHvVm -online
```

IFINCREMENTAL パラメーターなど、特定のパラメーターについては、次のように入力します。

```
help Backup-DpHvVm -Parameter IFINCREMENTAL
```

ヘルプを別のウィンドウで表示するには、**help** コマンドに **-ShowWindow** パラメーターを組み込みます。

Data Protection for Microsoft Hyper-V コマンドレットの例

Hyper-V 仮想マシン (VM) の保護に役立つ Data Protection for Microsoft Hyper-V コマンドレットの例が用意されています。

コマンドレットを使用する前に、[139 ページの『Data Protection for Microsoft Hyper-V で PowerShell コマンドレットを使用する準備』](#)の手順を確実に完了してください。

よく使用される Data Protection for Microsoft Hyper-V タスクの例が用意されています。

ヒント:

- 各コマンドレットでパラメーターを指定します。パラメーターを表示するには、次の **help** コマンドを発行します。

```
help cmdlet_name -ShowWindow
```

- コマンドレットのオンライン・ヘルプが利用できます。詳細については、[144 ページの『PowerShell コマンドレットのヘルプ情報の表示』](#)を参照してください。
- 例に特に注記がない限り、*user_name* は、Data Protection for Microsoft Hyper-V がインストールされているコンピューターへのログインに使用するアカウントを指定します。*computer_name* は、Data Protection for Microsoft Hyper-V がインストールされているサーバーの名前を指定します。

例

[145 ページの『例 1: 1 つ以上の VM をバックアップする』](#)

[146 ページの『例 2: VM バックアップを照会する』](#)

[146 ページの『例 3: Hyper-V ホストが Data Protection for Microsoft Hyper-V 操作用に構成されているかどうかを確認する』](#)

[146 ページの『例 4: Hyper-V ホストに関する IBM Spectrum Protect サーバー接続情報を保管し、接続を検証する』](#)

[146 ページの『例 5: IBM Spectrum Protect サーバーに関するポリシー情報を表示する』](#)

[146 ページの『例 6: Data Protection for Microsoft Hyper-V 操作用に Hyper-V ホストを構成する』](#)

[147 ページの『例 7: Hyper-V ホストで、VM インベントリを表示する』](#)

[147 ページの『例 8: ホストまたはクラスター上の VM のバックアップ状況を表示する』](#)

[147 ページの『例 9: VM の危険ポリシーを設定する』](#)

[148 ページの『例 10: スケジュール実行の履歴を表示する』](#)

[148 ページの『例 11: スケジュールをホストまたはクラスター上のデータ・ムーバーに関連付ける』](#)

[148 ページの『例 12: 1 つ以上の VM をリストアする』](#)

[149 ページの『例 13: Data Protection for Microsoft Hyper-V の構成の検証』](#)

[149 ページの『例 14: コマンドレットの実行による VM バックアップの整合性の検証』](#)

例 1: 1 つ以上の VM をバックアップする

1 つ以上の VM の「永久差分 - 差分」バックアップを実行します。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
$vmList = @("vm1","vm2")
$task = Backup-DpHvVm -Session $session -VmName $vmList -mode IFINCREMENTAL
$taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
```

```

while ("running" -eq $taskInfo.taskState) {
    start-sleep -seconds 30
    $taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
    if ($taskInfo.hasMoreData) {
        $results = Receive-DpHvTask -Session $session -TaskId $task.taskId
        write-verbose -verbose ("Started {0} Duration {1:g} Transferred `
                                {2:N2} MB" -f $results.startTime, ((Get-Date)-$results.startTime), `
                                ($results.totalBytesTransferred/1MB))
    }
}

$results = Receive-DpHvTask -Session $session -TaskId $task.taskId
$results

Remove-DpHvSession -Session $session

```

この例では、Data Protection for Microsoft Hyper-V との PowerShell コマンドレット・セッションを開始し、VM をバックアップし、VM バックアップを照会し、バックアップ・ジョブをモニターし、バックアップの完了時にセッションを終了します。

例 2: VM バックアップを照会する

IBM Spectrum Protect サーバー・ファイル・スペースに照会し、すべての VM バックアップの一般情報を表示します。

```

$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
$bks = Get-DpHvBackup -Session $session
$bks
Remove-DpHvSession -Session $session

```

例 3: Hyper-V ホストが Data Protection for Microsoft Hyper-V 操作用に構成されているかどうかを確認する

```

$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
Get-DpHvHostConfiguration -Session $session
Remove-DpHvSession -Session $session

```

例 4: Hyper-V ホストに関する IBM Spectrum Protect サーバー接続情報を保管し、接続を検証する

```

$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
Set-ServerConnection -Session $session -SPServerName server_name -SPAdmin `
    admin_name -SPAdminPwd admin_password -SPServerSSLPort port
Remove-DpHvSession -Session $session

```

例 5: IBM Spectrum Protect サーバーに関するポリシー情報を表示する

ドメイン名、デフォルト管理クラス、説明、バックアップ保存とアーカイブ保存の期間などの情報を表示します。

```

$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
Get-DpHvPolicyDomain -Session $session
Remove-DpHvSession -Session $session

```

例 6: Data Protection for Microsoft Hyper-V 操作用に Hyper-V ホストを構成する

次の例では、以下のタスクを実行して Hyper-V ホストを構成します。

- ターゲット・ノード (クラスター・ノード) を登録します。
- データ・ムーバー・ノードを登録し、バックアップ操作用に構成します (オプション・ファイルを構成し、クライアント・アクセプター・サービスとスケジューラー・サービスを作成します)。
- 要求された場合、ファイル・リストア環境を構成します (Windows および Linux のマウント・プロキシ・ノードを登録し、オプション・ファイルとクライアント・アクセプター・サービスを作成します)。

ファイル・リストア機能が使用可能である場合、ファイル・リストア資格情報は、ドメイン・ユーザーおよびパスワードでなければなりません。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
Set-ServerConnection -Session $session -SPServerName server_name -SPAdmin `
    admin_name -SPAdminPwd admin_password -SPServerSSLPort port
$nodesList = @(New-DpHvNodeInfo -NodeName node_name -NodeType node_type)
Set-DpHvHostConfiguration -Session $session -PolicyDomain policy_domain_name `
    -RegisterTargetNode -TargetNode target_node -NodeList $nodesList -EnableFR `
    -FRDomainUser domain_name\user_name -FRDomainPwd password
Remove-DpHvSession -Session $session
```

例 7: Hyper-V ホストで、VM インベントリを表示する

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
$vms = Get-DpHvVm -Session $session
$vms
Remove-DpHvSession -Session $session
```

例 8: ホストまたはクラスター上の VM のバックアップ状況を表示する

次の例は、ホストまたはクラスター上の前回の VM バックアップに関する情報を戻します。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred
$lastBackups = Get-DpHvLastSuccessfulBackup -Session $session
$vmName = $lastBackups | select -first 1 -ExpandProperty name
$vmBackupHistory = Get-DpHvVMBackupHistory -Session $session -vmName $vmName
$vmBackupHistory
Remove-DpHvSession -Session $session
```

例 9: VM の危険ポリシーを設定する

危険ポリシーにより、スケジュールされたバックアップ操作が指定の時間内に行われなかった場合、VM が保護されていない危険な状態であると判別されます。

以下の例の前半部分によって、バックアップされたすべての VM についての危険情報が表示されます。例の後半部分によって、「SQL」で開始するすべての VM の危険値が 12 時間まで更新されます。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

$lastBackups = Get-DpHvLastSuccessfulBackup -Session $session

# 1 - display the current at risk value for all vms

$i = 0
$atRiskList = @()
foreach ($backup in $lastBackups) {
    $activity = "Checking at risk value for {0}" -f $backup.name
    Write-Progress -activity $activity -status "Progress:" -percentcomplete `
        ($i++/$lastBackups.count*100)
    $atRisk = Get-DpHvVmAtRisk -session $session -VmName $backup.name
    $atRiskList += [pscustomobject]@{VM=$backup.name;AtRiskType=`
        $atRisk.AtRiskType;AtRiskInterval=$atRisk.AtRiskInterval}
}
$atRiskList | Out-GridView -Title "VM Risk Status" -PassThru

# 2 - set the at-risk value for all VMS that begin with SQL to a custom interval
# of 12 hours

$sqlVms = $lastBackups | where name -like "sql*"
$fsList = @()
foreach ($vm in $sqlVms) {
    $fsList += New-DpHvFsInfo -vmName $vm.Name -fsId $vm.FileSpaceId
}
Set-DpHvVmAtRisk -session $session -AtRiskType CUSTOM -AtRiskInterval 12 `
    -FsList $fsList

Remove-DpHvSession -Session $sess
```

例 10: スケジュール実行の履歴を表示する

次の例では、スケジュールされたアクティビティの 要約が表示され、その後に、最新のスケジュール済みアクティビティの詳細が表示されます。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

$schedHistory = Get-DpHvScheduleHistory -Session $session
$sh = $schedHistory | Sort-Object actualstarttime -Descending | Select-Object `
-First 1
$schedHistoryDetail = Get-DpHvScheduleHistoryDetail -Session $session -ScheduleName
    $sh.Name -StartTime $sh.ActualStartTime -EndTime $sh.EndTime -NodeList `
    $sh.NodeList

#"Schedule History Summary"
$schedHistory |
    select actualstarttime,name,status,vmsucceeded,vmfailures,duration,nodelist | `
    sort actualstarttime -desc | ft -AutoSize

#"Details of most recent scheduled activity"
$schedHistoryDetail |
    select starttime,datamover,targetnode,name,status,duration,datatransmitted,`
    backuptype| ft -AutoSize

Remove-DpHvSession -Session $session
```

例 11: スケジュールをホストまたはクラスター上のデータ・ムーバーに関連付ける

スケジュールのアソシエーションを確認するには、IBM Spectrum Protect サーバーで QUERY ASSOCIATION コマンドを実行します。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

# Get a list of schedules from the IBM Spectrum Protect server
$scheduleList = Get-DpHvBackupSchedule -Session $session
$scheduleList | format-table -autosize

# Associate the schedule with the data mover node
Set-DpHvBackupSchedule -Session $sess -ScheduleName "sched0" -Operation define `
    -DmNodesList hyperv1_HV_DM

# Remove the schedule association
Set-DpHvBackupSchedule -Session $sess -ScheduleName "sched0" -Operation remove `
    -DmNodesList hyperv1_HV_DM

Remove-DpHvSession -Session $sess
```

例 12: 1 つ以上の VM をリストアする

backupIDs を参照して複数の VM をリストアします。その際に、新しい名前と新規リストア宛先でリストアします。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

# Restore a single VM with default parameters
$task = Restore-DpHvVm -Session $session -vmname "vm1"
$taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
while ("running" -eq $taskInfo.taskState) {
    start-sleep -seconds 30
    $taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
    if ($taskInfo.hasMoreData) {
        $results = Receive-DpHvTask -Session $session -TaskId $task.taskId
        write-verbose -verbose ("Started {0} Duration {1:g} Transferred `
            {2:N2} MB" -f $results.startTime, ((Get-Date)-$results.startTime), `
            ($results.totalBytesTransferred/1MB))
    }
}

$results = Receive-DpHvTask -Session $session -TaskId $task.taskId
$results
```

```
# restore multiple vms
$task = Restore-DpHvVm -Session $session -vmname vm1,vm2 -backupId 111111,222222 `
    -newVmName vm1_restored,vm2_restored -targetPath c:\restored,c:\restored
$taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
while ("running" -eq $taskInfo.taskState) {
    start-sleep -seconds 30
    $taskInfo = Get-DpHvTask -Session $session -TaskId $task.taskId
    if ($taskInfo.hasMoreData) {
        $results = Receive-DpHvTask -Session $session -TaskId $task.taskId
        write-verbose ("Started {0} Duration {1:g} Transferred `
            {2:N2} MB" -f $results.startTime, ((Get-Date)-$results.startTime),`
            ($results.totalBytesTransferred/1MB))
    }
}
$results = Receive-DpHvTask -Session $session -taskId $task.taskId
$results

# Get the restore history of VMs
$vmRestoreHistory = Get-DpHvVmRestoreTaskHistory -Session $session
$vmRestoreHistory

Remove-DpHvSession -Session $session
```

例 13: Data Protection for Microsoft Hyper-V の構成の検証

構成ウィザードを実行した後、**Test-DpHvConfiguration** コマンドレットを使用して、以下の構成情報を確認することができます。

- デフォルトのデータ・ムーバー・ノードに関する情報(コンピューター名、オペレーティング・システム、およびエラー・ログの場所など)
- デフォルトのマウント・プロキシ・ノードに関する情報(コンピューター名、オペレーティング・システム、エラー・ログの場所、リカバリー・エージェントの状態、マウント・プロキシ・ノードの iSCSI 状況など)。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

$out1 = Test-DpHvConfiguration -session $session -nodetype DMNODE
$out2 = Test-DpHvConfiguration -session $session -nodetype MPNODE

Remove-DpHvSession -Session $session
```

例 14: コマンドレットの実行による VM バックアップの整合性の検証

VM をバックアップした後、インスタント・アクセス操作を実行して VM バックアップの整合性を検証することができます。**Restore-DpHvVm** コマンドレットで **InstantAccess** パラメーターを使用することで、検証プロセスを自動化することができます。

以下の例は、Ganymede という名前の VM のバックアップ・イメージの整合性を検証する場合のステップを示しています。

1. Ganymede という名前のバックアップ・イメージをリストア操作に使用できるかを検証します。次のコマンドレットを実行して、Ganymede_verify という名前の VM をインスタント・アクセス操作用に準備し、新規のインスタント・アクセス VM の電源を自動的にオンにします。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

$vmName = "Ganymede"
$newVmName = "Ganymede_verify"
$restoreType = "InstantAccess"
$targetPath = "D:\SSD1\RecoveryAgent\mount"

Restore-DpHvVm -Session $session -VmName $vmName -NewVmName $newVmName `
    -TargetPath $targetPath -restoreType $restoreType -AutoStart

Remove-DpHvSession -Session $session
```

重要: リストアしている VM が静的 IP アドレスを使用している場合、元の VM と一時 VM の間でネットワーク IP アドレスの競合が発生します。この競合を回避するには、一時インスタント・アクセス VM の作成後に、その VM の IP アドレスを変更します。

2. VM Ganymede がインスタント・アクセス・モードで稼働していることを確認するには、**Get-DpHvIaVm** コマンドレットを実行して、IBM Spectrum Protect サーバーに対してインスタント・アクセス VM を照会します。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

Get-DpHvIaVm -VmName Ganymede -Session $session

Remove-DpHvSession -Session $session
```

3. **Ganymede_verify** という名前のインスタント・アクセス VM で検証ツールを実行して、バックアップ・イメージをリストアできるかを検証します。

ディスクとデータの整合性を確認するには、**chkdsk** などのユーティリティー、あるいは任意のユーティリティーまたはアプリケーションを使用して、仮想ディスクおよびデータを検証します。一時 VM が整合性チェックに合格したら、インスタント・アクセス・リストア操作をサポートするために作成された一時リソースを除去することができます。

4. 次のコマンドレットを実行して、**Ganymede_verify** という名前のインスタント・アクセス VM を除去します。

```
$cred = Get-Credential -Message "Enter credentials" -UserName user_name
$session = New-DpHvSession -ComputerName computer_name -Credential $cred

$vmName = "Ganymede"
$newVmName = "Ganymede_verify"
$restoreType = "VmCleanup"
$targetPath = "D:\SSD1\RecoveryAgent\mount"

Restore-DpHvVm -Session $session -VmName $vmName -NewVmName $newVmName `
    -TargetPath $targetPath -restoreType $restoreType

Remove-DpHvSession -Session $session
```

関連資料

141 ページの『[Data Protection for Microsoft Hyper-V 用の PowerShell コマンドレット](#)』

仮想マシン (VM) データの保護に使用できる Data Protection for Microsoft Hyper-V コマンドレットを検討します。

第9章 コマンド解説

以下のセクションでは、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V 操作に使用されるクライアント・コマンドについて詳しく説明しています。

これらのコマンドは、IBM Spectrum Protect バックアップ/アーカイブ・コマンド・ライン・クライアントから発行します。Windows システム上で次のいずれかの方法を使用して、コマンド・ライン・クライアントを開始してください。

- ・「スタート」>「名前別のアプリケーション (Apps by name)」> **IBM Spectrum Protect** > 「バックアップ/アーカイブ・コマンド・ライン (Backup-Archive Command Line)」に進みます。
- ・管理者コマンド・プロンプト・ウィンドウを開き、バックアップ/アーカイブ・クライアントのインストール・ディレクトリに変更します (`cd "C:\Program Files\Tivoli\tsm\baclient"`)。
dsmc.exe を実行します。

コマンドやオプションのオンライン・ヘルプにアクセスするには、以下のコマンドを発行します。

```
dsmc help
```

オンライン・ヘルプに掲載されている情報は、IBM Spectrum Protect バックアップ/アーカイブ・クライアント、IBM Spectrum Protect for Virtual Environments: Data Protection for VMware、および Data Protection for Microsoft Hyper-V に適用されるものです。

構文図の読み方

コマンドを入力するために構文図を読み取るには、線の経路に従ってください。左から右へ、上から下へと読んでください。

- ・ **▶▶——** 記号は、構文図の始まりを示します。
- ・ 行の末尾にある **——▶** 記号は、構文図が次の行に続いていることを示します。
- ・ 行の先頭にある **▶——** 記号は、構文図が前の行から続いていることを示します。
- ・ **——▶◀** 記号は、構文図の終わりを示します。

キーワードや変数などの構文項目は次のようになります。

- ・ 主経路の線上 (必須要素)
- ・ 主経路より上 (デフォルト要素)
- ・ 主経路より下 (オプション要素)

記号

以下の記号は、構文図に示されているとおりに入力してください。

- ・ * アスタリスク
- ・ {} 中括弧
- ・ : コロン
- ・ , コンマ
- ・ = 等号
- ・ - ハイフン
- ・ () 括弧
- ・ . ピリオド
- ・ スペース
- ・ " 引用符

- ' 単一引用符

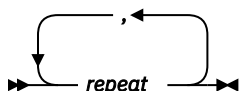
変数

<var_name> のようなイタリック体の小文字項目は、変数を表します。この例では、**cmd_name** コマンドを入力する際に <var_name> を指定できます。

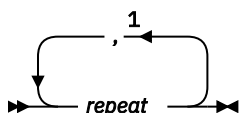
➡ cmd_name — <var_name> ➡

繰り返し

左へ戻る矢印は、その項目を繰り返して使用できることを意味しています。その矢印の中にある文字は、反復使用される項目をその文字で区切る必要があることを示しています。



矢印の横にある脚注 (1) は、その項目の繰り返し可能な回数の限度を表しています。



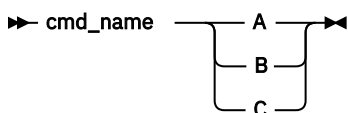
注:

¹ repeat は 5 回まで指定します。

必須選択項目

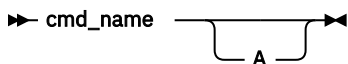
複数の項目が縦に並んでおり、そのうち 1 つが主経路 (水平の直線) 上にある場合は、その中から項目を 1 つ指定する必要があります。

次の例では、A、B、または C を選択する必要があります。

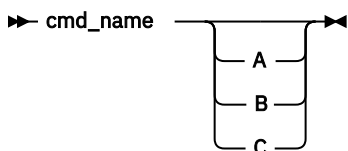


オプションの選択項目

項目が主経路よりも下にある場合、その項目はオプションです。最初の例では、A を選択するか、または何も選択しなくてもかまいません。



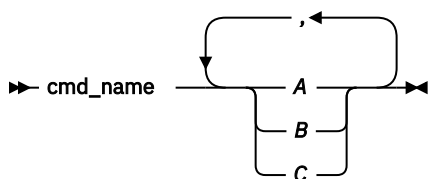
複数の項目が主経路より下に縦に並んでいる場合、それらの項目はすべてオプションです。2 番目の例では、A、B、または C を選択するか、何も選択しなくてもかまいません。



繰り返し可能選択項目

複数の項目が縦に並び、その後に左に戻る矢印がある場合は、その中から複数の項目を選択できるか、場合によっては1つの項目を繰り返し指定できることを示しています。

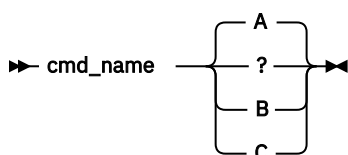
次の例では、A、B、またはCを任意の組み合わせで選択できます。



デフォルト値

デフォルト値は主経路より上にあります。変更しない限り、デフォルトが選択されます。または、デフォルトを明示的に選択できます。デフォルトを変更するには、主経路より下に縦に並んでいるオプションを指定します。

この例では、Aがデフォルトです。Aを変更するには、BまたはCを選択します。

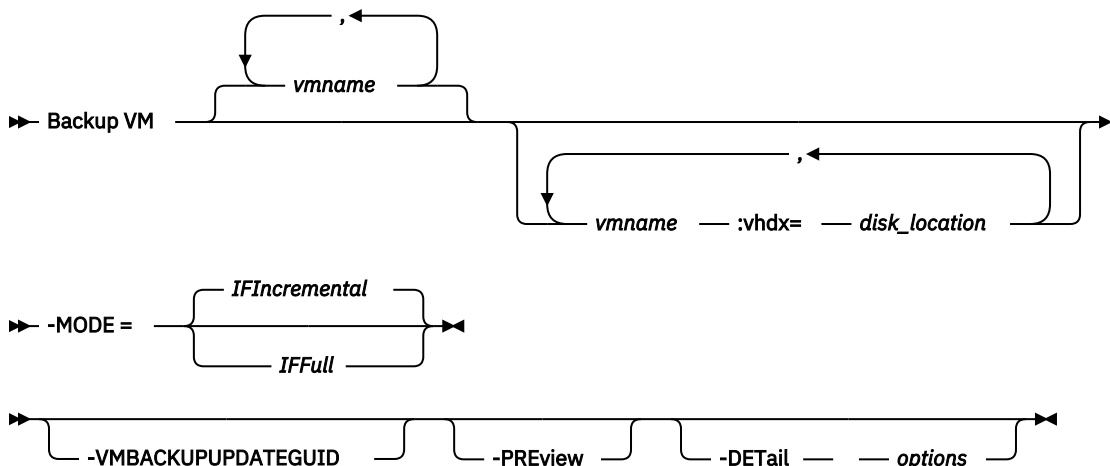


Backup VM

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

ローカル・ディスク、SAN 接続ディスク、クラスター共有ボリューム (CSV) 上に存在する Hyper-V ゲスト、あるいはリモート・ファイル・サーバー共有上に存在するゲストをバックアップすることができます。リモート・ファイル・サーバー共有は、Windows Server 2012 以降のシステム上になければなりません。また、リモート・ファイル共有は、ファイル・サーバー VSS エージェント・サービスがサーバーにインストールされている Server Message Block (SMB) 3.0 でなければなりません。

構文



パラメーター

vmname

バックアップしたい仮想マシンの名前を指定します。複数の仮想マシンを指定するには、複数の仮想マシン名をコンマで区切るか (vm1, VM2, Vm5)、domain.vmfu11 オプションを使用します。名前は大/小文字を区別するため、「Hyper-V Manager」 > 「仮想マシン」ビューの Hyper-V ホストで表示される大/小文字と一致する必要があります。

仮想マシン名にはワイルドカードを使用することができます。

制約事項: 「aggregate」という単語を VM 名として使用しないでください。「aggregate」という単語は、IBM Spectrum Protect のメッセージの VM 名フィールド用に予約されます。単語「aggregate」が VM 名として含まれているメッセージには、データ・ムーバーごとにバックアップされるすべての VM ゲストの合計値を表す統計が表示されます。

vmname:vhdX=disk_location

このパラメーターは、Hyper-V 仮想マシンのバックアップ操作に組み込む仮想マシン・ハード・ディスク (VHDx) を指定します。

vmname 変数は、バックアップする VM の名前を指定します。ワイルドカード文字を使用すると、パターンに一致する VM 名を選択できます。アスタリスク (*) は任意の文字のシーケンスと一致します。疑問符 (?) は、任意の単一文字と一致します。

:vhdX=disk_location キーワードは、バックアップ操作に組み込む VM ディスクのロケーションを指定します。ディスク・ロケーションは、「controller_type controller_number disk_location_number_inside_controller」というフォーマットで指定されます。コントローラー・タイプは「SCSI」または「IDE」でなければなりません。例えば、次のとおりです。

```
dsmc backup vm "vm1:VHDx=IDE 1 0"
```

「Hyper-V Manager」でディスク・ロケーション情報を取得できます。「仮想マシン」ビューで、VM を右クリックし、「設定」をクリックします。「設定」ウィンドウの「ハードウェア」セクションで、IDE コントローラーまたは SCSI コントローラーを見つけ、「ハード・ディスク」をクリックしてハード・ディスクの設定を表示します。コントローラー番号とディスク・ロケーションが「コントローラー」フィールドと「ロケーション」フィールドに表示されます。また、Windows PowerShell cmdlet **Get-VMHardDiskDrive** を実行してディスク・ロケーション情報を取得することもできます。

制約事項: 「aggregate」という単語を VM 名として使用しないでください。「aggregate」という単語は、IBM Spectrum Protect のメッセージの VM 名フィールド用に予約されます。単語「aggregate」が VM 名として含まれているメッセージには、データ・ムーバーごとにバックアップされるすべての VM ゲストの合計値を表す統計が表示されます。

vhdX= キーワードの前に除外演算子 (-) を指定すると、バックアップ操作から VM ディスクを除外することができます。例えば、次のように **-vhdX=** を使用して、VM のバックアップ操作から VM ディスクを除外します。

```
dsmc backup vm "vm1:-VHDx=IDE 1 0:-VHDx=SCSI 0 1"
```

組み込み、または除外を行う複数の VM ディスクを指定する場合、**vhdX=** または **-vhdX=** キーワードと関連値は、間にスペース文字を入れずにコロンで区切ります。例えば、次のとおりです。

```
dsmc backup vm "*: -VHDx=IDE 1 0: -VHDx=SCSI 0 1"
```

複数の VM 名と VM ディスクを指定する場合、VM 名と関連値は、間にスペース文字を入れずにセミコロンで区切ります。例えば、次のとおりです。

```
dsmc backup vm "vm1:-VHDx=IDE 1 0:-VHDx=SCSI 0 1;vm2:-VHDx=IDE 1 0:-VHDx=SCSI 0 1"
```

-MODE

コマンド・ラインで **-mode** パラメーターを追加することによって、仮想マシンのバックアップ時に使用するバックアップ・モードを指定する必要があります。以下のモードを指定できます。

IFFull

「永久増分 - フル」モード。このモードでは、仮想マシンのディスク上で使用されたすべてのブロックのスナップショットがサーバーにバックアップされます。このバックアップには、構成情報およびすべてのディスクが含まれます。

IFIncremental

「永久増分 - 増分」モード。このモードでは、前回の永久増分バックアップ操作 (フルまたは増分のいずれでも) 以降に変更されたブロックのスナップショットが作成されます。このバックアップには、構成情報およびすべてのディスクが含まれます。この値がデフォルトです。

-VMBACKUPUPDATEGUID

このオプションは、バックアップしている仮想マシンのグローバル固有 ID (GUID) を更新します。このパラメーターは、以下のシナリオのみで使用するためのものです。

既にバックアップされている ORION という名前の仮想マシンをリストアします。しかし、実動環境で稼働している ORION をシャットダウンしてコピーを置き換える前に、リストアされた仮想マシンの構成を、既存の ORION と置き換えて使用する前に検証したいと考えています。

1. 次のように、ORION 仮想マシンをリストアし、新規の名前を付けます。dsmc restore vm Orion -vmname=Orion2
2. ORION2 仮想マシンを更新して検証し、ORION という名前の既存の仮想マシンを置き換える準備ができているかを判別します。
3. ORION の電源をオフにして削除します。
4. ORION2 の名前を ORION に変更します。
5. 「永久増分 - フル」バックアップまたは「永久増分 - 増分」バックアップを使用して次に ORION をバックアップするときに、**-VMBACKUPUPDATEGUID** パラメーターを **backup vm** コマンドに追加します。このオプションにより、IBM Spectrum Protect サーバー上の GUID が更新され、ORION 仮想マシンの保管済みバックアップに新規 GUID が関連付けられます。増分バックアップのチェーンは保持されます。既存のバックアップを削除し、新規バックアップを置き換える必要はありません。

-PREView

このパラメーターは、仮想マシンにある仮想ハード・ディスクのラベルを含め、仮想マシンに関する追加情報を表示します。

-preview オプションを発行した場合、バックアップ操作は開始されません。バックアップ操作を開始するには、-preview オプションを指定せずに backup コマンドを発行する必要があります。

-preview オプションと -detail オプションの両方をコマンドで使用すると、バックアップの実行時に含まれるサブディスクに関する情報を表示できます。サブディスクは、VHDX ファイルのスナップショットの取得時に作成される AVHDX ファイルです。

-DETail

このパラメーターは、仮想マシンに関する詳細情報を表示します。バックアップ操作に関与するディスクに関する詳細を表示するには、このオプションを -preview と一緒に使用してください。

-detail オプションを発行した場合、バックアップ操作は開始されません。バックアップ操作を開始するには、-detail オプションを指定せずに backup コマンドを発行する必要があります。

仮想マシンのバックアップ操作に関する戻りコード

仮想マシンのバックアップ操作は、次の表で示された戻りコードで完了する可能性があります。

表 15. backup vm コマンドからの戻りコード	
戻りコード	説明
0	1 つ以上の仮想マシンをバックアップするコマンドが正常に完了しました。
8	複数の仮想マシンをバックアップするコマンドが、そのコマンドの対象となっていた仮想マシンの一部でのみ成功しました。ログ・ファイルを調べて、対象の各仮想マシンの処理状況を判別してください。

表 15. backup vm コマンドからの戻りコード (続き)

戻りコード	説明
12	<p>以下のいずれかのエラー状態が発生したことを示します。</p> <ul style="list-style-type: none"> バックアップ・コマンドが、バックアップ操作のターゲットであったいずれかの仮想マシンをバックアップできませんでした。 バックアップ・コマンドが失敗し、指定されたすべての仮想マシンが検査される前に停止しました。 <p>ログ・ファイルを調べて、障害の理由を判別してください。</p>

最終統計に関するヒント: 複数のバックアップ・セッションを実行している場合、最終統計の「**Data transfer time**」フィールドに表示される値は、「**Elapsed processing time**」フィールドの値より高くなる場合があります。データ転送時間は、各バックアップでネットワークを介してデータを送信するのに要した時間の合計です。この数値には、データが送信される前にデータ・ムーバーがディスクからデータを読み取るのに要した時間も、サーバー・トランザクションが完了するまで待機した時間も含まれません。操作で複数の並行セッションを使用してデータを移動している場合 (マルチセッションのバックアップ操作など)、この数値が経過処理時間より大きくなる可能性があります。この値には、バックアップ操作中にファイルが変更された場合など、再試行のために複数回データを送信するのに要した時間が含まれます。

コマンドの例

1. 以下のコマンドは、「VM1」という名前の Hyper-V 仮想マシンの「永久増分 - 増分」バックアップを開始します。

```
dsmc backup vm VM1 -mode=ifincremental
```

2. Windows Server 2016 以降のオペレーティング・システムの場合: 以下のコマンドは、「vm2」という仮想マシンの永久増分の RCT 増分バックアップから IDE ディスク (コントローラー番号 1 でディスク・ロケーション 0) と SCSI ディスク (コントローラー番号 0 でディスク・ロケーション 1) を除外します。

```
dsmc backup vm "vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1" -mode=ifincremental
```

3. Windows Server 2016 以降のオペレーティング・システムの場合: 以下のコマンドが「VM05」という仮想マシンの永久増分の増分 RCT バックアップのプレビューを表示します。

```
dsmc backup vm VM05 -mode=ifincremental -preview
```

コマンド出力で、-preview パラメーターは、仮想マシンの VHDX ラベルを表示します。-detail パラメーターを -preview パラメーターと一緒に指定する場合、Hyper-V RCT バックアップの追加情報は表示されません。

Backup VM command started. Total number of virtual machines to process: 1

1. VM Name: VM05

```
Domain Keyword:      VM05
Mode:                Incremental Forever - Incremental
Target Node Name:    NODE14
Data Mover Node Name: NODE14
Cluster Resource:    No

Disk[1]
Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05.vhdx
Capacity:           15.00 GB
Size:               10.91 GB
Status:             included
Disk Type:          VHDX
Number of Subdisk:  0
Controller Location: IDE 0 0

Disk[2]
Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\
    VM05_Disk2.vhdx
Capacity:           2.00 GB
Size:               132.00 MB
Status:             included
Disk Type:          VHDX
Number of Subdisk:  0
Controller Location: SCSI 0 1
```

Total number of virtual machines processed: 1

4. Windows Server 2012 または 2012 R2 の場合: 以下のコマンドが「VM03」という Hyper-V 仮想マシンの永久増分の増分バックアップを開始します。

```
dsmc backup vm VM03 -mode=ifincremental -preview
```

コマンド出力で、`-preview` パラメーターは、仮想マシンの VHDX ラベルを表示します。

1. VM Name: VM03

```
Domain Keyword:      all-vm
Mode:                Incremental Forever - Incremental
Target Node Name:    NODE14_HV_DM
Data Mover Node Name: NODE14_HV_DM
Cluster Resource:    No

Disk[1]
Name: \\NODE14\d$\Hyper-V\VM03\VM03\Virtual Hard Disks\VM03.vhdx
Capacity:           64.00 GB
Size:               28.91 GB
Status:             excluded
Disk Type:          VHDX
Number of Subdisk:  1
```

`-detail` パラメーターを `-preview` パラメーターと一緒に指定する場合、VHDX ラベルとそれらのサブディスクが表示されます。以下の出力例は、省略して 1 つの仮想マシンと 1 つのディスクに関する情報のみを表示しています。

1. VM Name: VM03

```
Domain Keyword:      all-vm
Mode:                Incremental Forever - Incremental
Target Node Name:    NODE14_HV_DM
Data Mover Node Name: NODE14_HV_DM
Cluster Resource:    No

Disk[1]
Name: ¥¥NODE14¥d$¥Hyper-V¥VM03¥VM03¥Virtual Hard Disks¥VM03.vhdx
Capacity:           64.00 GB
Size:               28.91 GB
Status:             excluded
Disk Type:          VHDX
Number of Subdisk:  1

Subdisk[1]
Name: ¥¥NODE14¥d$¥Hyper-V¥VM03¥VM03¥Virtual Hard Disks¥
    VM03_94F6257B-5C61-45F1-BD62-3323DCF26954.avhdx
Capacity:           64.00 GB
Size:               180.00 MB
Status:             excluded
Disk Type:          AVHDX
```

オプション・ファイルの例

domain.vmfull オプションは、特定の仮想マシンを処理するために使用されます。以下の例では、domain.vmfull オプションは次のように指定されています。

```
domain.vmfull VM04,VM05
```

次のコマンドは、domain.vmfull オプションで指定された 仮想マシンのフルバックアップのプレビューを表示します。このコマンドは、各仮想マシンに関するプレビュー情報を表示します。

```
dsmc backup vm -mode=iffull -preview
```

次の出力は、Windows Server 2016 以降のオペレーティング・システムで表示されます。

```
Backup VM command started. Total number of virtual machines to process: 2
```

1. VM Name: VM04

```
Domain Keyword:      VM04
Mode:                Incremental Forever - Full
Target Node Name:    NODE14
Data Mover Node Name: NODE14
Cluster Resource:    No

Disk[1]
Name: ¥¥node14¥d$¥Hyper_V_Virtual_Machine¥VM04¥Virtual Hard Disks¥VM04.vhdx
Capacity:           36.00 GB
Size:               9.16 GB
Status:             included
Disk Type:          VHDX
Number of Subdisk:  0
Controller Location: IDE 0 0
```

2. VM Name: VM05

```
Domain Keyword:      VM05
Mode:                Incremental Forever - Full
Target Node Name:    NODE14
Data Mover Node Name: NODE14
Cluster Resource:    No

Disk[1]
Name: ¥¥node14¥d$¥Hyper_V_Virtual_Machine¥VM05¥Virtual Hard Disks¥VM05.vhdx
Capacity:           15.00 GB
Size:               10.91 GB
Status:             included
Disk Type:          VHDX
Number of Subdisk:  0
Controller Location: IDE 0 0

Disk[2]
```

```
Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\
VM05_Disk2.vhdx
Capacity:      2.00 GB
Size:          132.00 MB
Status:        included
Disk Type:     VHDX
Number of Subdisk: 0
Controller Location: SCSI 0 1
```

Total number of virtual machines processed: 2

次の出力は、Windows Server 2012 および 2012 R2 で表示されます。

Backup VM command started. Total number of virtual machines to process: 2

1. VM Name: VM04

```
Domain Keyword:    all-vm
Mode:              Incremental Forever - Incremental
Target Node Name:  NODE14_HV_DM
Data Mover Node Name: NODE14_HV_DM
Cluster Resource:  No
```

Disk[1]

```
Name: ¥¥NODE14¥d$¥Hyper-V¥VM04¥VM04¥Virtual Hard Disks¥VM04.vhdx
Capacity:      64.00 GB
Size:          28.91 GB
Status:        excluded
Disk Type:     VHDX
Number of Subdisk: 1
```

Subdisk[1]

```
Name: ¥¥NODE14¥d$¥Hyper-V¥VM04¥VM04¥Virtual Hard Disks¥
VM04_94F6257B-5C61-45F1-BD62-3323DCF26954.avhdx
Capacity:      64.00 GB
Size:          180.00 MB
Status:        excluded
Disk Type:     AVHDX
```

2. VM Name: VM05

```
Domain Keyword:    all-vm
Mode:              Incremental Forever - Incremental
Target Node Name:  NODE14_HV_DM
Data Mover Node Name: NODE14_HV_DM
Cluster Resource:  No
```

Disk[1]

```
Name: ¥¥NODE14¥d$¥Hyper-V¥disks¥Windows 10.vhdx
Capacity:      20.00 GB
Size:          18.75 GB
Status:        excluded
Disk Type:     VHDX
Number of Subdisk: 1
```

Subdisk[1]

```
Name: ¥¥NODE14¥d$¥Hyper-V¥disks¥
Windows 10_15F8A5AA-C104-4C74-8F68-B57B27592F8A.avhdx
Capacity:      20.00 GB
Size:          112.00 MB
Status:        excluded
Disk Type:     AVHDX
```

Disk[2]

```
Name: ¥¥NODE14¥e$¥Hyper-V¥disks¥Windows10_disk2¥Windows10_disk2.vhdx
Capacity:      5.00 GB
Size:          5.00 GB
Status:        excluded
Disk Type:     VHDX
Number of Subdisk: 1
```

Subdisk[1]

```
Name: ¥¥NODE14¥e$¥Hyper-V¥disks¥Windows10_disk2¥
Windows10_disk2_15F8A5AA-C104-4C74-8F68-B57B27592F8A.avhdx
Capacity:      5.00 GB
Size:          4.00 MB
Status:        excluded
Disk Type:     AVHDX
```

Disk[3]

```
Name: ¥¥NODE14¥e$¥Hyper-V¥disks¥Windows10_disk2¥Windows10_disk5.vhdx
Capacity: 1.00 GB
Size: 1.00 GB
Status: included
Disk Type: VHDX
Number of Subdisk: 1

Subdisk[1]
Name: ¥¥NODE14¥e$¥Hyper-V¥disks¥Windows10_disk2¥
Windows10_disk5_15F8A5AA-C104-4C74-8F68-B57B27592F8A.avhdx
Capacity: 1.00 GB
Size: 4.00 MB
Status: included
Disk Type: AVHDX
```

```
Total number of virtual machines processed: 2
ANS1900I 戻りコード 0
ANS1901I 最高の戻りコードは 0 でした。
```

関連資料

[177 ページの『Detail』](#)

管理クラス、ファイル・スペース、およびバックアップ情報を表示する場合に、`detail` オプションを使用します。

[177 ページの『Domain.vmfull』](#)

`domain.vmfull` オプションは、仮想マシンのフル・イメージ・バックアップ操作に組み込む仮想マシン (VM) を指定します。

[191 ページの『Mbobjrefreshthresh』](#)

`mbobjrefreshthresh` (メガブロック・オブジェクト最新表示しきい値) オプションは、しきい値を定義する数値です。任意の 128 MB のメガブロックを記述するのに必要な IBM Spectrum Protect オブジェクトの数がこの値を超えた場合、メガブロック全体が最新表示され、前のバックアップでそのエリアを表すのに使用されたオブジェクトは有効期限が切れます。

[192 ページの『Mbpctrefreshthresh』](#)

`mbpctrefreshthresh` (メガブロック・パーセンテージ最新表示しきい値) オプションは、しきい値を定義する数値です。任意の 128 MB のメガブロックを記述するのに必要なオブジェクトの IBM Spectrum Protect パーセンテージの数値がこの値を超える場合、メガブロック全体が最新表示され、前のバックアップでそのエリアを表すのに使用されたオブジェクトは有効期限が切れます。

[190 ページの『mode』](#)

`mode` オプションを使用して、特定のバックアップ操作の実行時にバックアップ・モードを指定します。

[161 ページの『Query VM』](#)

query VM コマンドは、正常に完了した仮想マシン (VM) のバックアップをリストし、検査するために使用します。

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

Expire

expire コマンドは、IBM Spectrum Protect サーバー上の仮想マシン (VM) の現行のバックアップを非アクティブ化する場合に使用します。

対話モードで作業しているときには、オブジェクトが期限切れになる前にプロンプトで通知されます。

expire コマンドは、ローカル・ホストから VM を削除しません。ローカル・ホスト上にまだ存在する VM を期限切れにした場合、その VM は、バックアップ処理から除外しない限り、次の増分バックアップ時に再度バックアップされます。

構文

➡ EXpire — — OBJTYPE=VM — — vmname — options ➡

パラメーター

OBJTYPE=VM vmname

vmname は、VM の名前を指定します。指定された VM のアクティブ・バックアップが、IBM Spectrum Protect サーバー上で期限切れになります。VM 名にワイルドカード文字を含めることはできません。

objtype=VM を指定した場合、expire コマンドは vmname パラメーターで指定された VM のフル VM バックアップ (MODE=IFFULL) のみを期限切れにします。

表 16. Expire コマンド: 関連オプション

オプション	使用先
dateformat 175 ページの『Dateformat』	クライアント・オプション・ファイル (dsm.opt) またはコマンド・ライン。
noprompt 193 ページの『Noprompt』	コマンド・ラインのみ。
numberformat 193 ページの『Numberformat』	クライアント・オプション・ファイル (dsm.opt) またはコマンド・ライン。
pick 195 ページの『Pick』	コマンド・ラインのみ。
timeformat 197 ページの『Timeformat』	クライアント・ユーザー・オプション・ファイル (dsm.opt) またはコマンド・ライン。

例

タスク

vm_test という名前の VM の現行バックアップを非活動化します。

コマンド: dsmc expire -objtype=VM vm_test

Query VM

query VM コマンドは、正常に完了した仮想マシン (VM) のバックアップをリストし、検査するために使用します。

Microsoft Hyper-V 仮想マシンに対する Query VM

query vm コマンドを使用して、バックアップされた Hyper-V 仮想マシンを判別します。

サポートされるクライアント

このコマンドは、Hyper-V ホスト・システム上にインストールされている Windows クライアントで有効です。

構文

➡ Query VM — — vmname — options ➡

パラメーター

vmname

照会したい仮想マシンのホスト名を指定します。仮想マシン名は大/小文字を区別します。コマンドで VM 名を指定する場合、名前にワイルドカード文字を含めることはできません。

仮想マシン名を省略した場合、コマンドは、IBM Spectrum Protect サーバー上にあるすべての VM バックアップを表示します。

表 17. Query VM コマンド: Hyper-V 仮想マシン照会の関連オプション。

オプション	使用先
detail	コマンド・ライン。各ディスク (ラベル、名前) とそのディスクの情報 (保護、あるいは除外)、および永久増分バックアップのパフォーマンス統計の詳細を表示します。
inactive	コマンド・ライン。
pitdate	コマンド・ライン。
pittime	コマンド・ライン。
vmrestoretype	コマンド・ライン。

例

タスク

Hyper-V ホスト上の Data Protection for Microsoft Hyper-V によってバックアップされたすべての仮想マシンをリストします。

```
dsmc query vm
```

Query VM の例 (Hyper-V)

以下の例は、バックアップ済みのすべての Hyper-V 仮想マシンに関する要約情報を表示する **query VM** コマンドを示しています。

```
dsmc query vm
```

Query Virtual Machine for Full VM backup

# Machine	Backup Date	Mgmt Class	Size	Type	A/I	Location	Virtual
1	03/19/2017 17:54:34	STANDARD	17.00 GB	IFFULL	A	SERVER	DeptA_VM05
2	03/20/2017 01:51:34	STANDARD	15.00 GB	IFINCR	A	SERVER	DeptA_VM05
3	03/20/2017 01:46:19	STANDARD	36.00 GB	IFFULL	A	SERVER	DeptA_VM04

以下の **-detail** オプションを指定した **query VM** コマンドは、バックアップされている Hyper-V VM に関する情報を表示します。詳細な出力には、実行されたバックアップのタイプ、仮想マシンのサイズ、仮想マシンのディスクに関する情報、および統計が含まれます。

```
dsmc query vm -detail
```

Query Virtual Machine for Full VM backup

#	Backup Date	Mgmt Class	Size	Type	A/I Location	Virtual Machine
1	03/19/2017 17:54:34	STANDARD	17.00 GB	IFFULL	A SERVER	DeptA_VM05
The size of this incremental backup: n/a The number of incremental backups since last full: 0 The amount of extra data: 0 The IBM Spectrum Protect objects fragmentation: 0 Backup is represented by: 99 IBM Spectrum Protect objects Application protection type: n/a Backup is compressed: No Backup is deduplicated: No Snapshot type: Hyper-V RCT Application Consistent Disk[1]Name: DeptA_VM05.vhdx Disk[1]Location: IDE 0 0 Disk[1]Status: Protected Disk[2]Name: DeptA_VM05_Disk2.vhdx Disk[2]Location: SCSI 0 1 Disk[2]Status: Protected Disk[3]Name: Disk 7 2.00 GB Bus 0 Lun 4 Target 0 Disk[3]Location: SCSI 0 0 Disk[3]Status: Skipped: Physical disk Disk[4]Name: Disk 8 2.50 GB Bus 0 Lun 5 Target 0 Disk[4]Location: SCSI 0 2 Disk[4]Status: Skipped: Physical disk						
2	03/20/2017 01:51:34	STANDARD	15.00 GB	IFINCR	A SERVER	DeptA_VM_W2k08R2
The size of this incremental backup: 544.00 KB The number of incremental backups since last full: 1 The amount of extra data: 0 The IBM Spectrum Protect objects fragmentation: 2 Backup is represented by: 37 IBM Spectrum Protect objects Application protection type: n/a Backup is compressed: No Backup is deduplicated: No Snapshot type: Hyper-V RCT Crash Consistent Disk[1]Name: DeptA_VM_W2k08R2.vhdx Disk[1]Location: IDE 0 0 Disk[1]Status: Protected						
3	03/20/2017 01:46:19	STANDARD	36.00 GB	IFFULL	A SERVER	DeptA_VM04
The size of this incremental backup: n/a The number of incremental backups since last full: 0 The amount of extra data: 0 The IBM Spectrum Protect objects fragmentation: 0 Backup is represented by: 79 IBM Spectrum Protect objects Application protection type: n/a Backup is compressed: No Backup is deduplicated: No Snapshot type: Hyper-V RCT Application Consistent Disk[1]Name: DeptA_VM04.vhdx Disk[1]Location: IDE 0 0 Disk[1]Status: Protected						
----- All averages are calculated only for incremental forever backups displayed above. The average size of incremental backup: 544.00 KB The average number of incremental backups since last full: 0 The average overhead of extra data: 0 The average objects fragmentation: 0 The average number of objects per backup: 71						

詳細出力には、以下の情報のようなスナップショット・タイプとディスク情報も含まれています。

Snapshot type

VM バックアップ操作中に取られたスナップショットのタイプ:

Hyper-V RCT Application Consistent

Windows Server 2016 で Resilient change Tracking (RCT) を使用して作成された静止スナップショット。

Hyper-V RCT Crash Consistent

Windows Server 2016 で Hyper-V RCT を使用して作成された非静止スナップショット。

Hyper-V VSS

Windows Server 2012 または Windows Server 2012 R2 で Volume Shadow Copy Service (VSS) で作成されたスナップショット。

Disk[n]Location

VM ディスク n のディスク・ロケーション、ここで n は番号です。ディスク・ロケーションは、ディスク・コントローラー・タイプの「IDE」または「SCSI」、その後続くコントローラー番号およびデバイス・ロケーション番号から構成されています。

Disk[n]Status

VM ディスク n のバックアップ状況、ここで n は番号です。

Protected

VM ディスク上のデータがバックアップされることを示します。

Skipped: Excluded by user

VM ディスクは `exclude.vmdisk` オプションに指定されているように、バックアップ操作中に除外されることを示します。

Skipped: Physical disk

VM ディスクが物理ディスク (パススルー・ディスク) であること、そのデータがバックアップされていないことを示します。ディスク構成情報情報のみがバックアップされます。

以下の例は、DeptA_VM_W2k08R2 という名前の特定の仮想マシンの詳細出力をリストするために使用する構文です。

```
dsmc query vm DeptA_VM_W2k08R2 -detail

Query Virtual Machine for Full VM backup
```

#	Backup Date	Mgmt Class	Size	Type	A/I	Location	Virtual Machine
1	03/20/2017 01:51:34	STANDARD	15.00 GB	IFINCR	A	SERVER	DeptA_VM_W2k08R2

The size of this incremental backup: 544.00 KB
The number of incremental backups since last full: 1
The amount of extra data: 0
The IBM Spectrum Protect objects fragmentation: 2
Backup is represented by: 37 IBM Spectrum Protect objects
Application protection type: n/a
Backup is compressed: No
Backup is deduplicated: No
Snapshot type: Hyper-V RCT Crash Consistent
Disk[1]Name: Jimmy_VM_Windows2008R2.vhdx
Disk[1]Location: IDE 0 0
Disk[1]Status: Protected

All averages are calculated only for incremental forever backups displayed above.
The average size of incremental backup: 544.00 KB
The average number of incremental backups since last full: 1
The average overhead of extra data: 0
The average objects fragmentation: 2
The average number of objects per backup: 37

以下のコマンドは、インスタント・アクセス操作により作成された、インスタント・アクセス・モードで実行中のすべての一時 VM を表示します。

```
q vm * -vmrestoretype=instantaccess
```

関連資料

[180 ページの『Exclude.vmdisk』](#)

EXCLUDE.VMDISK オプションは、仮想マシン・ディスクをバックアップ操作から除外します。

[215 ページの『Vmprocessvmwithphysdisks』](#)

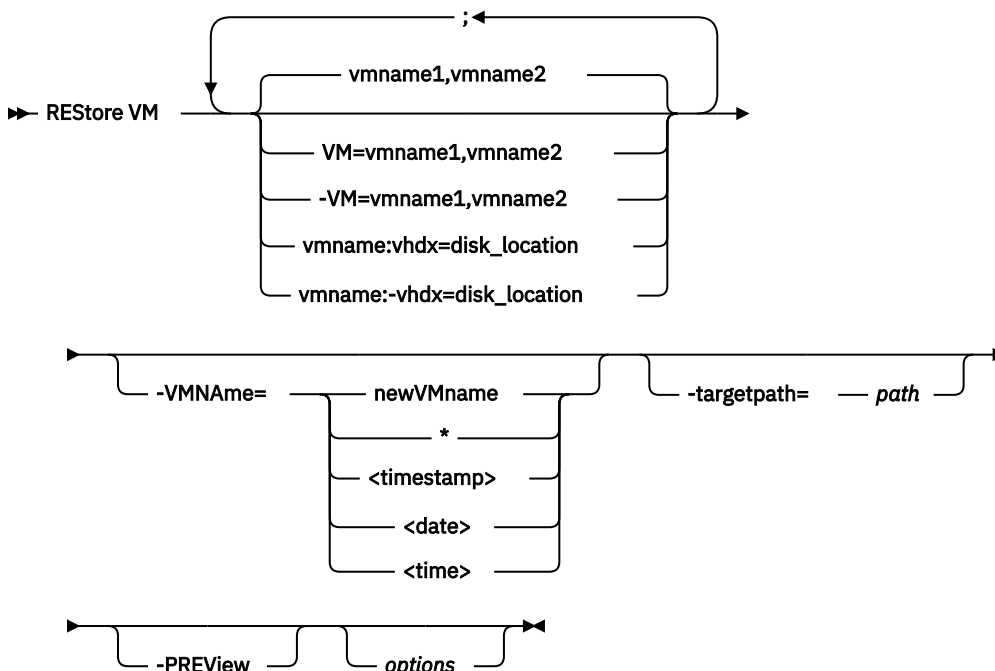
vmprocessvmwithphysdisks オプションを使用して、VM に 1 つ以上の物理ディスク (パススルー・ディスク) がプロビジョニングされている場合に Hyper-V RCT 仮想マシン (VM) バックアップを処理するかどうかを制御します。

Restore VM

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

リストアしようとしている仮想マシンが Hyper-V ホスト・サーバー上にある場合、IBM Spectrum Protect サーバーに保管されているイメージからリストアされる前に、その VM はシャットダウンされ削除されます。その後、リストア操作により、内容と構成がバックアップが行われた時と同一のものになるように VM が作成されます。VM は削除される前にシャットダウンされますが、**restore vm** コマンドを実行する前に手動で VM をシャットダウンして、進行中のアプリケーション・アクティビティーを正常に停止することが推奨されます。

構文



パラメーター

スペースが含まれているパラメーターは、引用符 (") で囲む必要があります。

vmname

リストアする 1 つ以上の VM の名前を指定します。この名前は VM 表示名です。複数の VM 名をコンマで区切ります (例: vm1, vm2, vm5)。テンプレート VM をバックアップしていた場合、vmname パラメーターではリストアするテンプレート VM の名前を指定できます。

ワイルドカード文字を使用すると、パターンに一致する VM 名を選択できます。アスタリスク (*) は任意の文字のシーケンスと一致します。疑問符 (?) は、任意の単一文字と一致します。例えば、次のとおりです。

- **restore vm VM_TEST*** は、「VM_TEST」で始まる名前を持つすべての仮想マシンをリストアします。

- **restore vm VM??** は、文字「VM」で始まり、その後に 2 文字が続く名前を持つすべての VM をリストアします。

リストアする VM を 1 つ以上指定する必要があります。

vm=vmname

vm= キーワードは、次の値のセットが、VM の名前のリストであることを指定します。**vm=** キーワードはデフォルトであり、必須ではありません。

VM 名にはワイルドカード文字を使用できます。**vmname** パラメーターの指定については、[165 ページの『vmname』](#) を参照してください。

次の例では、**vm=** が指定されており、コンマがマシン名の区切りに使用されています。

```
restore vm vm=my_vm1,my_vm2
```

-vm=vmname

vm= キーワードの前に除外演算子 (-) を指定すると、リストア操作から VM を除外することができます。

任意の VM 名パターンで開始する VM グループなど、VM バックアップの大規模なグループから VM のリストを除外するには **-vm=** キーワードを使用します。例えば、名前の先頭に **Dept99_** が付くすべての VM をリストアする一方で **vm2** をリストアしないようにする場合、以下のコマンドを発行します。

```
restore vm vm=Dept99_*;-vm=Dept99_vm2
```

-vm= キーワードを指定してワイルドカード文字を使用すると、パターンに一致する VM 名を除外できます。例えば次のとおりです。

- ホスト名に **test** が含まれているすべてのファイルを除外します。

```
-vm=*test*
```

- **test20**、**test25**、**test29**、および **test2A** などの名前を持つすべての VM を組み込みます。

```
vm=test2?
```

制約事項: 除外演算子 (-) を使用して VM ホスト・ドメインを除外することはできません。除外演算子は、VM 名レベルでのみ機能します。

vmname:vhdxdisk_location

このパラメーターは、Hyper-V VM リストア操作に組み込む VM ハード・ディスク (VHDX) を指定します。このオプションを指定するのは、すべてのディスクではなく、1 つ以上の特定のディスクをリストアする場合のみです。

vmname 変数は、リストアする VM の名前を指定します。ワイルドカード文字を使用すると、パターンに一致する VM 名を選択できます。アスタリスク (*) は任意の文字のシーケンスと一致します。疑問符 (?) は、任意の単一文字と一致します。

:vhdxdisk_location キーワードは、リストア操作に組み込む VM ディスクのロケーションを指定します。ディスク・ロケーションは、「**controller_type controller_number disk_location_number_inside_controller**」というフォーマットで指定されます。コントローラー・タイプは「SCSI」または「IDE」でなければなりません。例えば、次のとおりです。

```
dsmc restore vm "vm1:vhdxdisk_location=IDE 1 0"
```

組み込みを行う複数の VM ディスクを指定する場合、**vhdxdisk_location** キーワードと関連値は、間にスペース文字を入れずにコロンで区切ります。例えば、次のとおりです。

```
dsmc restore vm "*:vhdxdisk_location=IDE 1 0:vhdxdisk_location=SCSI 0 1"
```

複数の VM 名と VM ディスクを指定する場合、VM 名と関連値は、間にスペース文字を入れずにセミコロンで区切ります。例えば、次のとおりです。

```
dsmc restore vm "vm1:vhdX=IDE 1 0:vhdX=SCSI 0 1;vm2:vhdX=IDE 1 0:vhdX=SCSI 0 1"
```

リストアする各ディスクに、以下の考慮事項が適用されます。

- リストア操作を開始する前に、ディスクが VM 上に存在している必要があります。ディスクが存在しない場合、ディスクを作成する必要があります。 **-preview** パラメーターを使用して、元のディスク名と容量を特定することができます。
- 既存のディスクが、リストアするディスク以上のサイズでなければなりません。
- 既存のディスク・ロケーションは、リストアするディスクと同じでなければなりません。
- 既存のディスク上のデータは、すべて上書きされます。

指定されたディスクのみがリストアされます。VM 上のその他のディスクは変更されません。

ディスクのリストア先の VM は、リストア操作を開始する前に電源をオフにする必要があります。

vmname:-vhdX=disk_location

vmname 変数は、リストアする VM の名前を指定します。ワイルドカード文字を使用すると、パターンに一致する VM 名を選択できます。アスタリスク (*) は任意の文字のシーケンスと一致します。疑問符 (?) は、任意の単一文字と一致します。

この **-vhdX=disk_location** オプションは、1 つ以上の仮想ディスクのディスク・ロケーションを指定して、リストア操作から除外する場合に使用します。例えば、次のように **-vhdX=** を使用して、VM のリストア操作から VM ディスクを除外します。

```
dsmc restore vm "vm1:-vhdX=IDE 1 0:-vhdX=SCSI 0 1"
```

除外を行う複数の VM ディスクを指定する場合、**-vhdX=** キーワードと関連値は、間にスペース文字を入れずにコロンで区切ります。例えば、次のとおりです。

```
dsmc restore vm "*:-vhdX=IDE 1 0:-vhdX=SCSI 0 1"
```

複数の VM 名と VM ディスクを指定する場合、VM 名と関連値は、間にスペース文字を入れずにセミコロンで区切ります。例えば、次のとおりです。

```
dsmc restore vm "vm1:-vhdX=IDE 1 0:-vhdX=SCSI 0 1;vm2:-vhdX=IDE 1 0:-vhdX=SCSI 0 1"
```

-VMName=

VM= パラメーターで指定した名前を使用しない場合、リストア後の VM の新規名を指定します。新しい VM 名は二重引用符で囲むようにしてください。

newVMname

リストアされた VM に使用する新規 VM 名を指定します。

リストアされた仮想マシンの名前では以下の文字はサポートされていません。

```
: ; ' \ / " ? , < > |
```

サポートされない文字を含む **restore** コマンドは、エラー・メッセージ **ANS9117E** で失敗します。

***** (アスタリスク) 記号は、リストアされている VM の元の名前を表すメタキャラクターです。アスタリスクの前後に有効な文字を指定すると、リストアされる VM の名前に接頭語または接尾語が作成されます。

リストアされた仮想マシンの名前では以下の文字はサポートされていません。

```
: ; ' \ / " ? , < > |
```

サポートされない文字を含む **restore** コマンドは、エラー・メッセージ **ANS9117E** で失敗します。

***** 記号は以下の方法で使用できます。

- リストアされた VM の元の VM 名を使用するには **vmname="*"** と指定します。

- リストアされた VM の元の VM 名に接尾部を追加します。例えば、元の VM 名が VM1 と VM2 の場合、接尾部「_restored」を元の VM に追加するために、以下のコマンドを指定します。

```
dsmc restore vm VM1,VM2 -VMName="*_restored"
```

リストアされた VM の名前は VM1_restored と VM2_restored になります。

- リストアされた VM の元の VM 名の前に接頭部を挿入します。例えば、元の VM 名が VM3 の場合、接頭部「new_」を VM3 に挿入するために、以下のコマンドを指定します。

```
dsmc restore vm VM3 -vmname="new_*
```

リストアされた VM の名前は new_VM3 になります。

<timestamp>

リストアされた VM の名前にリストア操作の日時を示すタイム・スタンプを追加します。

<timestamp> パラメーターはキーワードなので、大括弧 (「<」と「>」) で囲む必要があります。

タイム・スタンプ・ストリングの形式は、dsm.opt ファイルの DATEFORMAT オプションと TIMEFORMAT オプションにより決まります。<timestamp> パラメーターによって返されるタイム・スタンプの区切り文字にはダッシュが使用されます。

例えば、VM5 と VM6 という名前の 2 台の VM をリストアし、リストアされた VM 名にリストアの日時を追加する場合、以下のコマンドを発行します。

```
dsmc restore vm VM5,VM6 -vmn="*_<timestamp>"
```

リストアされた VM の名前は VM5_06-22-2017_14-56-55 と VM6_06-22-2017_14-56-55 になります。

<date>

リストアされた VM の名前にリストア操作の日付を追加します。<date> パラメーターはキーワードなので、大括弧 (「<」と「>」) で囲む必要があります。

日付ストリングの形式は、dsm.opt ファイルの DATEFORMAT オプションにより決まります。

<date> パラメーターによって返される日付の区切り文字にはダッシュが使用されます。

例えば、VM3 という名前の VM の前に接頭部「new_」を挿入し、リストアされた VM 名にリストアの日付を追加するには、以下のコマンドを発行します。

```
dsmc restore vm VM3 -vmname="new_*_<date>"
```

リストアされた VM の名前は new_VM3_06-22-2017 になります。

<time>

リストアされた VM の名前にリストア操作の時刻を追加します。<time> パラメーターはキーワードなので、大括弧 (「<」と「>」) で囲む必要があります。

タイム・ストリングの形式は、dsm.opt ファイルの TIMEFORMAT オプションにより決まります。

<time> パラメーターによって返される時刻の区切り文字にはダッシュが使用されます。

例えば、VM8 という名前の VM の後に接尾部「_today_」を追加し、リストアされた VM 名にリストアの時刻を追加するには、以下のコマンドを発行します。

```
dsmc restore vm VM8 -vmn="*_today_<time>"
```

リストアされた VM の名前は VM8_today_14-56-55 になります。

-targetpath=

VM のリストア先のパスを指定します。

このパラメーターは、-vmname パラメーターが指定されている場合には必須ですが、指定されていない場合にはオプションです。VM を代替パスにリストアする場合は、このパラメーターを使用します。

-PREVIEW

このパラメーターは、VM をリストアせずにリストア操作の結果を確認する場合に使用します。 -

preview パラメーターは、リストアされる VM のリストと、仮想ハード・ディスクの名前やディスクのサイズなどの VM について情報を提供します。

restore vm コマンドで **-preview** パラメーターを発行した場合、リストア操作は開始されません。リストア操作は、**-preview** パラメーターがコマンドから削除された場合のみ開始されます。

詳しくは、171 ページの『仮想マシンのリストア操作のプレビュー』を参照してください。

表 18. Restore VM コマンド: Hyper-V 仮想マシンのリストア時の関連オプション

オプション	使用先
inactive	コマンド・ライン
pick	コマンド・ライン
pitdate	コマンド・ライン
pittime	コマンド・ライン
replace	コマンド・ライン、クライアント・オプション・ファイル、またはクライアント・プリファレンス・エディター。
vmbackdir	コマンド・ライン、クライアント・オプション・ファイル。
vmmaxrestoreparalleldisks	コマンド・ライン、オプション・ファイル
vmmaxrestoresessions	コマンド・ライン、オプション・ファイル
vmmaxrestoreparallelvm	コマンド・ライン、オプション・ファイル
vmrestoretype	コマンド・ライン
vmautostartvm	コマンド・ラインまたはクライアント・オプション・ファイル。

ヒント: クラスター内のホストの場合、削除済みの VM をリストアした場合、あるいは新しい VM 名で VM をリストアした場合は、Microsoft Failover Cluster Manager、System Center Virtual Machine Manager、または PowerShell コマンドレットを使用して、リストアした VM を高可用性のために構成する必要があります。高可用性のために VM を構成する方法については、Microsoft の資料を参照してください。

最終統計に関するヒント: 複数のリストア・セッションを実行している場合、最終統計の「**Data transfer time**」フィールドに表示される値は、「**Elapsed processing time**」フィールドの値より高くなる場合があります。データ転送時間は、各リストア操作でネットワークを介してデータを送信するのに要した時間の合計です。この数値には、データが送信される前にデータ・ムーバーがディスクからデータを読み取るのに要した時間も、サーバー・トランザクションが完了するまで待機した時間も含まれません。操作で複数の並行セッションを使用してデータを移動している場合 (マルチセッションのリストア操作など)、この数値が経過処理時間より大きくなる可能性があります。この値には、再試行操作のために複数回データを送信するのに要した時間が含まれます。

例

タスク

VM1 という名前の仮想マシンの最新バックアップ・バージョンを、バックアップされた元のドライブおよびパスにリストアします。

```
dsmc restore vm VM1 -vmrestoretype=noninstant
```

タスク

vm1 という名前の仮想マシンの最新バックアップ・バージョンを、バックアップされた元のドライブおよびパスにリストアします。プロンプトを表示せずに既存の仮想マシンを置き換えます。

```
dsmc restore vm vm1 -replace=yes
```

タスク

VM1 という名前のバックアップ済み仮想マシンを新規名 (vm2) にリストアします。

```
dsmc restore vm VM1 -VmName=vm2
```

タスク

vm1 という名前のバックアップ済み仮想マシンをリストアし、新規名 (vm2) を割り当てます。vm2 が既に存在する場合、その仮想マシンを上書きする前にプロンプトを発行します。

```
dsmc restore vm vm1 -VmName=vm2 -replace=prompt
```

タスク

vm1 という名前の仮想マシンを、仮想マシンの名前を変更せずに特定のドライブおよびパスにリストアします。

```
dsmc restore vm vm1 -targetpath="E:¥New Path"
```

タスク

vm1 という名前の仮想マシンをリストアしますが、その名前を vm2 に変更し、新規パスにリストアします。

```
dsmc restore vm vm1 -VmName=vm2 -targetpath=F:¥NewPath
```

タスク

-pick および -inactive を使用して、vm1 という名前の仮想マシンのアクティブ/非アクティブ・バックアップを表示します。リストからリストアするバックアップを選択します。

```
dsmc restore vm vm1 -pick -inactive
```

タスク

コマンド・ラインからインスタント・アクセス操作を実行します。手順については、[131 ページの『第7章 インスタント・アクセス操作の実行』](#)を参照してください。

タスク

VM のリストから、4 つの VM を並行して c:¥hypervrestore フォルダーにリストアします。このリストア操作では、リストアされる VM ごとに 5 つのセッションを割り振り、VM ごとに並行で最大 2 つのディスクをリストアします。これらの VM を、リストア操作の日時が付加された VM 名にリストアします。

```
dsmc restore vm vm1,vm2,vm3,vm4,vm5,vm6,vm7,vm8 -vmmaxrestoreparallelvm=4  
-vmmaxrestoresessions=20 -vmmaxrestoreparalleldisks=2  
-vmname="*_<timestamp>" -targetpath=c:\hypervrestore
```

タスク

パターン vm* に一致するすべての VM のうち、4 つの VM を並行して c:¥hypervrestore フォルダーにリストアします。このリストア操作では、リストアされる VM ごとに 5 つのセッションを割り振り、VM ごとに並行で最大 2 つのディスクをリストアします。これらの VM を、リストア操作の日時が付加された VM 名にリストアします。

```
dsmc restore vm vm* -vmmaxrestoreparallelvm=4 -vmmaxrestoresessions=20  
-vmmaxrestoreparalleldisks=2 -vmname="*_<timestamp>"  
-targetpath=c:\hypervrestore
```

タスク

vm5 を除く、パターン vm* に一致するすべての VM のうち、4 つの VM を並行して c:¥hypervrestore フォルダーにリストアします。このリストア操作では、リストアされる VM ごとに 5 つのセッションを割り振り、VM ごとに並行で最大 2 つのディスクをリストアします。これらの VM を、リストア操作の日時が付加された VM 名にリストアします。

```
dsmc restore vm vm=vm*; -vm=vm5 -vmmaxrestoreparallelvm=4  
-vmmaxrestoresessions=20 -vmmaxrestoreparalleldisks=2  
-vmname="*_<timestamp>" -targetpath=c:\hypervrestore
```

関連資料

205 ページの『[vmmaxrestoreparalleldisks](#)』

単一の仮想マシン (VM) で複数の仮想ディスクを同時にリストアするには、`vmmaxrestoreparalleldisks` オプションを指定します。

206 ページの『[Vmmaxrestoreparallelvms](#)』

`vmmaxrestoreparallelvms` オプションは、同時にリストアできる仮想マシンの数を制御します。

210 ページの『[Vmmaxrestoresessions](#)』

`vmmaxrestoresessions` オプションは、仮想マシン (VM) の最適化されたリストア操作に組み込むことができる IBM Spectrum Protect サーバー セッションの最大数を定義します。

仮想マシンのリストア操作のプレビュー

-preview パラメーターを使用すると、仮想マシン (VM) をリストアすることなく、リストア操作の結果を検証できます。-preview パラメーターは、リストアされる VM のリストとそれら VM に関する情報を提供します。**restore vm** コマンドと共に -preview パラメーターを使用する方法を調べるには、示されているオプションに関する情報と、**restore vm -preview** コマンドの例を確認してください。

-preview パラメーターがオプションとその値を戻すのは、そのオプションがデフォルト 値をオーバーライドするか、デフォルトが存在しない場合のみです。

restore vm コマンドで -preview パラメーターを発行した場合、リストア操作は開始されません。リストア操作は、-preview パラメーターがコマンドから削除された場合のみ開始されます。

任意の有効な **restore vm** コマンドで -preview パラメーターを使用できます。

例

タスク

すべての VM を `d:\vmstorage` ディレクトリーの新規 VM にリストアする操作をプレビューします。新規 VM 名は、元の VM 名にリストアのタイム・スタンプが付加されて構成されます。

次のコマンドを発行します。

```
dsmc restore vm * -vmname="*_<timestamp>" -targetpath=d:\vmstorage\
-preview
```

コマンド出力:

```
IBM Spectrum Protect
Command Line Backup-Archive Client Interface
  Client Version 8, Release 1, Level 7.0
  Client date/time: 10/02/2018 14:20:25
(c) Copyright by IBM Corporation and other(s) 1990, 2019. All Rights Reserved.

Node Name: HYPERVTEST
Session established with server ASANA2: Linux/x86_64
  Server Version 7, Release 1, Level 9.000
  Server date/time: 10/02/2018 14:18:30  Last access: 10/02/2018 14:05:26

Restore function invoked.

Restore VM command started.  Total number of virtual machines to process: 3
1.  Virtual machine name: 'HEISENBERG.RESTORED'
    Mode: 'Incremental Forever - Incremental'
    Backup time: IFINCR 07/20/2018 06:59:16

    Disk 1 label:          'Hard Disk 1'
    Disk 1 name:          'IDE 0 0|HEISENBERG (Windows 2012 R2) Disk 1.vhdx'
    Disk 1 status:        Selected
    Disk 1 capacity:      136,365,211,648
    Disk 1 data to send:  9,965,666,304

    Destination name:      'HEISENBERG.RESTORED_10-02-2018_14-20-34'
```



```

Target Path:                'd:\vmstorage¥'

2.    Virtual machine name: 'fremont1vm8'
      Mode: 'Incremental Forever - Full'
      Backup time: IFFULL 07/31/2018 11:33:43

      Disk 1 label:          'Hard Disk 1'
      Disk 1 name:           'IDE 0 0|fremont1vm8.vhdx'
      Disk 1 status:         Selected
      Disk 1 capacity:       42,949,672,960
      Disk 1 data to send:   8,426,356,736

      Destination name:      'fremont1vm8_10-02-2018_14-20-34'
      Target Path:           'd:\vmstorage¥'

3.    Virtual machine name: 'HEISENBERG (Windows 2012 R2)'
      Mode: 'Incremental Forever - Incremental'
      Backup time: IFINCR 09/17/2018 09:39:01

      Disk 1 label:          'Hard Disk 1'
      Disk 1 name:           'IDE 0 0|HEISENBERG (Windows 2012 R2) Disk 1.vhdx'
      Disk 1 status:         Selected
      Disk 1 capacity:       136,365,211,648
      Disk 1 data to send:   9,730,785,280

      Disk 2 label:          'Hard Disk 2'
      Disk 2 name:           'IDE 1 1|Data Disk 1.vhdx'
      Disk 2 status:         Selected
      Disk 2 capacity:       2,147,483,648
      Disk 2 data to send:   134,217,728

      Disk 3 label:          'Hard Disk 3'
      Disk 3 name:           'SCSI 0 0|Data Disk 2.vhdx'
      Disk 3 status:         Selected
      Disk 3 capacity:       1,073,741,824
      Disk 3 data to send:   100,663,296

      Destination name:      'HEISENBERG (Windows 2012 R2)_10-02-2018_14-20-34'
      Target Path:           'd:\vmstorage¥'

```

タスク

「fremont1vm8」という名前以外のすべての VM を d:\vmstorage ディレクトリーの新規 VM にリストアする操作をプレビューします。新規 VM 名は、元の VM 名にリストアのタイム・スタンプが付加されて構成されます。

次のコマンドを発行します。

```

dsmc restore vm vm=*;-vm=fremont1vm8 -vmname="*_<timestamp>"
-targetpath=d:\vmstorage\ -preview

```

コマンド出力:

```

IBM Spectrum Protect
Command Line Backup-Archive Client Interface
  Client Version 8, Release 1, Level 7.0
  Client date/time: 10/02/2018 14:24:13
(c) Copyright by IBM Corporation and other(s) 1990, 2019. All Rights Reserved.

Node Name: HYPERVTEST
Session established with server ASANA2: Linux/x86_64
  Server Version 7, Release 1, Level 9.000
  Server date/time: 10/02/2018 14:22:17 Last access: 10/02/2018 14:18:37

Restore function invoked.

Restore VM command started. Total number of virtual machines to process: 2
1.    Virtual machine name: 'HEISENBERG.RESTORED'

```

```
Mode: 'Incremental Forever - Incremental'
Backup time: IFINCR 07/20/2018 06:59:16

Disk 1 label:          'Hard Disk 1'
Disk 1 name:           'IDE 0 0|HEISENBERG (Windows 2012 R2) Disk 1.vhdx'
Disk 1 status:         Selected
Disk 1 capacity:       136,365,211,648
Disk 1 data to send:   9,965,666,304

Destination name:      'HEISENBERG.RESTORED_10-02-2018_14-24-21'
Target Path:           'd:\vmstorage\'
```

```
2. Virtual machine name: 'HEISENBERG (Windows 2012 R2)'
Mode: 'Incremental Forever - Incremental'
Backup time: IFINCR 09/17/2018 09:39:01

Disk 1 label:          'Hard Disk 1'
Disk 1 name:           'IDE 0 0|HEISENBERG (Windows 2012 R2) Disk 1.vhdx'
Disk 1 status:         Selected
Disk 1 capacity:       136,365,211,648
Disk 1 data to send:   9,730,785,280

Disk 2 label:          'Hard Disk 2'
Disk 2 name:           'IDE 1 1|Data Disk 1.vhdx'
Disk 2 status:         Selected
Disk 2 capacity:       2,147,483,648
Disk 2 data to send:   134,217,728

Disk 3 label:          'Hard Disk 3'
Disk 3 name:           'SCSI 0 0|Data Disk 2.vhdx'
Disk 3 status:         Selected
Disk 3 capacity:       1,073,741,824
Disk 3 data to send:   100,663,296

Destination name:      'HEISENBERG (Windows 2012 R2)_10-02-2018_14-24-21'
Target Path:           'd:\vmstorage\'
```

関連資料

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

第 10 章 オプションの解説

以下のセクションでは、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V 操作に使用される各クライアント・オプションについて詳しく説明しています。

それぞれのオプションに関する情報には、以下が含まれています。

- 説明
- 構文図
- パラメーターの詳細な説明
- クライアント・オプション・ファイルでのオプションの使用例 (該当する場合)
- コマンド・ラインでのオプションの使用例 (該当する場合)

コマンド・ラインの例が「適用しません」のオプションは、コマンド・ラインやスケジュールされたコマンドで使用できません。

Dateformat

dateformat オプションは、日付の表示または入力に使用する形式を指定します。

このオプションは、使用しているメッセージ・リポジトリの言語のデフォルト日付形式を変更したい場合に使用します。

デフォルトの場合、バックアップ/アーカイブ・クライアントと管理クライアントは、クライアントの開始時に有効なロケール定義からフォーマット情報を取得します。ロケール定義のセットアップ方法の詳細については、ローカル・システム側のドキュメンテーションを参照してください。

expire コマンドで **dateformat** オプションを使用することができます。

コマンドに **dateformat** オプションを組み込む場合は、**fromdate** オプションと **pitdate** オプションの前に指定する必要があります。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (**dsm.opt**) に入れます。このオプションは、プリファレンス・エディターの「地域設定」タブの「日付形式」ドロップダウン・リストで設定できます。

構文

➡ **DATEformat** — — *format_number* ➡

パラメーター

format_number

次のフォーマットの 1 つを使用して日付を表示します。使用したい日付形式に対応する番号を選択します。

1

MM/DD/YYYY

これは、以下の使用可能翻訳の場合のデフォルトです。

- 米国英語
- 中国語 (繁体字)
- 韓国語

2

DD-MM-YYYY

これは、以下の使用可能翻訳の場合のデフォルトです。

- ブラジル・ポルトガル語
- イタリア語

3

YYYY-MM-DD

これは、以下の使用可能翻訳の場合のデフォルトです。

- 日本語
- 中国語 (簡体字)
- ポーランド語

4

DD.MM.YYYY

これは、以下の使用可能翻訳の場合のデフォルトです。

- ドイツ語
- フランス語
- スペイン語
- チェコ語
- ロシア語

5

YYYY.MM.DD

これは、以下の使用可能翻訳の場合のデフォルトです。

- ハンガリー語

6

YYYY/MM/DD

7

DD/MM/YYYY

例

オプション・ファイル:

dateformat 3

コマンド・ライン:

-date=3

このオプションは、初期コマンド・ラインおよび対話モードでのみ有効です。このオプションを対話モードで使用した場合には、このオプションが指定されたコマンドにのみ影響が及びます。そのコマンドが完了すると、値は対話式セッションの開始時の値に戻ります。この値は、初期コマンド・ラインまたはサーバーが強制するオプションによって指定変更されない限り、dsm.opt ファイルの値です。

日時形式の指定についてのその他の考慮事項

このオプションで指定する日時形式は、日時を入力データとして処理するオプションの使用時に使用する必要があります。例: totime、fromtime、todate、fromdate、および pittime。

例えば timeformat オプションを TIMEFORMAT 4 と指定する場合、fromtime や totime オプションに指定する値は、12:24:00pm のような時刻に指定する必要があります。TIMEFORMAT 4 で指定する時刻の整数は 12 以下でなければならないため、13:24:00 と指定しても無効です。オプションに指定できる時間の値を最大で 24 とし、コンマを区切り文字として使用したい場合は、TIMEFORMAT 2 を指定する必要があります。

Detail

管理クラス、ファイル・スペース、およびバックアップ情報を表示する場合に、**detail** オプションを使用します。

detail を **query vm** コマンドと共に使用すると、以下の統計が表示されます。

- バックアップのすべてのメガブロックにおいて、単一メガブロックの記述に必要な IBM Spectrum Protect オブジェクトの平均数。
- ファイル・スペースのすべてのメガブロックに対して、単一メガブロックの記述に必要な IBM Spectrum Protect オブジェクトの平均数。
- 前回のフルバックアップが実動ディスクから作成された以降に作成されたバックアップの数。

query vm で戻る値は、ヒューリスティック (Mbjrefreshthresh オプションおよび Mbpctrefreshthresh オプションを参照) を微調整する際に役立ち、メガブロックの最新表示用の値トリガーを微調整できます。

構文

► DETail ◄

パラメーター

このオプションにパラメーターはありません。

例

コマンド・ライン:

```
dsmc query vm -detail
```

Domain.vmfull

domain.vmfull オプションは、仮想マシンのフル・イメージ・バックアップ操作に組み込む仮想マシン (VM) を指定します。

Microsoft Hyper-V 仮想マシンでの Domain.vmfull

Hyper-V VM のバックアップでは、**backup vm** コマンドの実行時に **domain.vmfull** オプションを使用して、Hyper-V VM 名を指定することなく、処理する Hyper-V VM を指定します。

次のいずれかの方法を使用して、どの VM が処理されるかを指定できます。

- **VM=** オプションを使用して仮想マシンの名前を指定します。
- 複数の仮想マシン名をコンマ区切りのリストで与えます。
- ワイルドカード構文を使用して、名前のパターンに一致する仮想マシンを処理させます。
- **vmname:vhdX=** オプションを使用して、VM の Hyper-V バックアップ操作時に組み込むまたは除外する VM ハード・ディスク (VHDX) を指定します。
- **all-vm** ドメイン・レベル・パラメーターを使用します。**VM=** キーワードを使用して 1 つ以上の仮想マシン (VM) を組み込んだり、**-VM=** 構文を使用して VM を除外したりすることもできます。

domain.vmfull オプションで指定する仮想マシンが処理されるのは、仮想マシンまたは仮想マシンのリストを指定せずに **backup vm** コマンドをコマンド・ラインで入力した場合のみです。



重要: Microsoft Hyper-V 操作では、`domain.vmfull` オプションに有効なドメイン・レベル・パラメーターは **all-vm** のみです。VM= キーワードを使用して 1 つ以上の仮想マシンを組み込んだり、-VM= 構文を使用して仮想マシンを除外したりすることもできます。

サポートされるクライアント

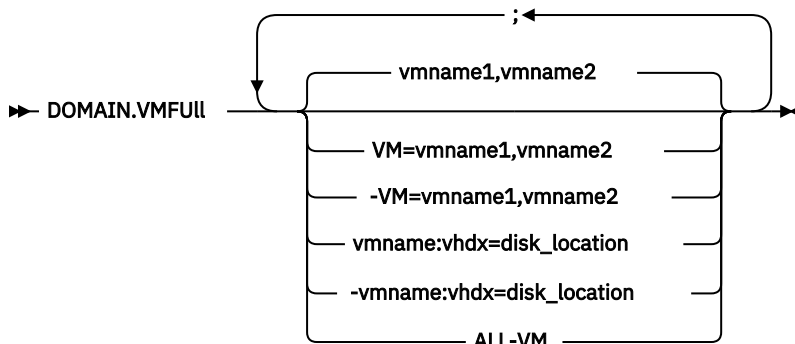
このオプションは、サポートされる Windows クライアントで使用可能です。このオプションはサーバーでも定義できます。

オプション・ファイル

このオプションは、コマンド・ラインを使用するかまたはプリファレンス・エディターの「**VM バックアップ**」タブを使用して、クライアント・オプションに設定します。

制約事項: プリファレンス・エディターでは、`vmname:vhdX=vhdX_location` パラメーターを設定できません。この設定は、オプション・ファイルに設定するか、**backup vm** コマンドの実行時にコマンド・ラインに指定してください。

Microsoft Hyper-V 仮想マシンの構文



構文規則: 複数のキーワードを指定する場合は、セミコロンで区切る必要があります。セミコロンの後にスペースを入れることはできません。複数のマシン名やドメイン・ネームはコンマで区切り、スペース文字は入れないでください。例えば、`vm=vmname` を参照してください。

パラメーター

vmname

処理する仮想マシンの名前を定義します。仮想マシンのホスト名のリストはコンマで名前を区切って指定できます (`vm1, VM2, Vm5`)。名前は大/小文字を区別するため、「**Hyper-V Manager**」 > 「**仮想マシン**」ビューの Hyper-V ホストで表示される大/小文字と一致する必要があります。

vm=vmname

vm= キーワードは、次の値のセットが、仮想マシンの名前のリストであることを指定します。vm= キーワードはデフォルトであり、必須ではありません。

次の例では、vm= が指定されておらず、コンマがマシン名の区切りに使用されています。

```
domain.vmfull my_vm1,my_vm2
```

vm= および -vm= などの複数のキーワードを指定する場合、キーワードが参照する値はセミコロンで区切り、間にスペース文字は入れないでください。

```
domain.vmfull vm=my_vm1;vm=my_vm2
domain.vmfull -vm=my_vm3;-vm=my_vm4
```

ワイルドカード文字を使用すると、パターンに一致する仮想マシン名を選択できます。アスタリスク (*) は任意の文字のシーケンスと一致します。疑問符 (?) は、任意の単一文字と一致します。例えば次のとおりです。

- ホスト名に「test」が含まれているすべてのファイルを除外する: `-vm=*test*`
- 「test20」、「test25」、「test29」、「test2A」などの名前を持つすべての仮想マシンを組み込む:

```
vm=test2?
```

`vm=` キーワードの前に除外演算子 (-) を指定すると、バックアップ操作から仮想マシンを除外することができます。例えば、`-vm` は、ドメイン・レベル・バックアップ ALL-VM から特定のマシン (1 つまたは複数) を除外するために使用されます。1 つの仮想マシンの名前が「vm1」の場合、ドメイン内のすべての仮想マシンをバックアップするが、仮想マシン「vm1」はバックアップしないようにすることができます。次のオプションを設定します。

```
domain.vmfull all-vm;-vm=vm1
```

除外演算子 (-) は、ALL-VM のドメインを除外するためには使用できません。除外演算子は、仮想マシン名レベルでのみ機能します。

vmname:vhdxd=vhdxd_location

このオプションは、Hyper-V 仮想マシンのバックアップ操作に組み込む仮想マシン・ハード・ディスク (VHDX) のロケーションを指定します。

`vmname` 変数は、バックアップする仮想マシンの名前を指定します。ワイルドカード文字を使用すると、パターンに一致する仮想マシン名を選択できます。アスタリスク (*) は任意の文字のシーケンスと一致します。疑問符 (?) は、任意の単一文字と一致します。

`:vhdxd=disk_location` キーワードは、バックアップ操作に組み込む仮想マシン・ディスクのロケーションを指定します。`disk_location` 変数により指定されるディスク・ロケーションは、先頭が「SCSI」または「IDE」で、その後にコントローラー番号およびデバイス・ロケーション番号を続けて指定する必要があります。例えば、次のとおりです。

```
domain.vmfull "vm1:VHDX=IDE 1 0"
domain.vmfull "vm*:VHDX=SCSI 0 1"
domain.vmfull "vm?:VHDX=SCSI 0 1"
```

`vhdxd=` キーワードの前に除外演算子 (-) を指定すると、バックアップ操作から仮想マシン・ディスクを除外することができます。例えば、`-vhdxd=` を使用して、仮想マシンのバックアップ操作から VM ディスクを除外します。例えば、次のとおりです。

```
domain.vmfull "vm1:-VHDX=IDE 1 0"
```

組み込み、または除外を行う複数の仮想マシン・ディスクを指定する場合、`vhdxd=` または `-vhdxd=` キーワードと関連値は、間にスペース文字を入れずにコロンで区切ります。例えば、次のとおりです。

```
domain.vmfull "vm1:vhdxd=IDE 1 0:vhdxd=SCSI 0 1"
```

複数の仮想マシン名と仮想マシン・ディスクを指定する場合、VM 名と関連値は、間にスペース文字を入れずにセミコロンで区切ります。例えば、次のとおりです。

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"
domain.vmfull "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1;vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

all-vm

このオプションは、**backup vm** 操作で、Hyper-V ホストが認識しているすべての Hyper-V ホストを処理することを指定します。

Microsoft Hyper-V 仮想マシンの例

オプション・ファイル:

すべての仮想マシンをフル VM バックアップ操作に組み込みます。

```
domain.vmfull all-vm
```

名前の接尾部分が `_test` である仮想マシン以外のすべての仮想マシンをフル VM バックアップに組み込みます。

```
domain.vmfull all-vm;-vm=*_test
```

すべての仮想マシンをフル VM バックアップ操作に組み込みますが、仮想マシン `testvm1` および `testvm2` は除外します。

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

仮想マシンの `vm1` および `vm2` の Hyper-V バックアップ操作に、IDE ディスク (コントローラー番号 1 でディスク・ロケーション 0) と SCSI ディスク (コントローラー番号 0 でディスク・ロケーション 1) を組み込みます。

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"
```

制約事項: オプション・ファイルあるいはコマンド・ラインでの単一のドメイン指定で、`all-vm` オプションと `vmname:-vhdx=` オプションを一緒に使用することはできません。例えば、`domain1 = all-vm:-VHDX=SCSI 0 0` は無効です。

関連資料

180 ページの『[Exclude.vmdisk](#)』

`EXCLUDE.VMDISK` オプションは、仮想マシン・ディスクをバックアップ操作から除外します。

184 ページの『[Include.vmdisk](#)』

`INCLUDE.VMDISK` オプションは、バックアップ操作に仮想マシン (VM) ディスクを組み込みます。ディスク・ラベルを指定しない場合は、VM のすべてのディスクがバックアップされます。

215 ページの『[Vmprocessvmwithphysdisks](#)』

`vmprocessvmwithphysdisks` オプションを使用して、VM に 1 つ以上の物理ディスク (パススルー・ディスク) がプロビジョニングされている場合に Hyper-V RCT 仮想マシン (VM) バックアップを処理するかどうかを制御します。

Exclude.vmdisk

`EXCLUDE.VMDISK` オプションは、仮想マシン・ディスクをバックアップ操作から除外します。

`EXCLUDE.VMDISK` オプションは、**backup vm** 操作から除外される仮想マシンのディスクのラベルを指定します。**backup vm** コマンドでディスクを除外する場合、コマンド・ライン・パラメーターが、オプション・ファイルの `EXCLUDE.VMDISK` ステートメントをすべてオーバーライドします。

Microsoft Hyper-V 仮想マシンに対する EXCLUDE.VMDISK

`EXCLUDE.VMDISK` オプションを使用して、仮想マシン・ディスクを Hyper-V バックアップ操作から除外します。

サポートされるクライアント

このオプションは、すべてのサポート対象の Windows クライアントで使用できます。

オプション・ファイル

このオプションは、クライアント・オプション・ファイルに設定します。コマンド・ライン・パラメーターがオプション・ファイルのステートメントをオーバーライドします。

構文

```
►► EXCLUDE.VMDISK — vmname disk_location ◄◄
```

パラメーター

vmname

backup vm 操作から除外するディスクを含む VM の名前を指定します。この名前は、仮想マシンの表示名です。各 EXCLUDE.VMDISK ステートメントに指定できる VM 名は 1 つのみです。除外する VM ごとに、追加の EXCLUDE.VMDISK ステートメントを指定してください。

VM 名に指定できるアスタリスク (*) は任意の文字ストリングと一致し、疑問符 (?) は任意の単一文字と一致します。VM 名がスペース文字を含む場合は、VM 名を引用符 (") で囲みます。

ヒント: VM 名が大括弧文字 ([]) または (|) のような特殊文字を含む場合、VM 名が正確に一致しないことがあります。VM 名に特殊文字が含まれる場合は、疑問符 (?) を使用してその特殊文字を表してください。

例えば、"Windows VM3 [2012R2]" という名前の VM のバックアップから SCSI 仮想マシン・ディスクを除外するには、オプション・ファイルで次の構文を使用します。

```
EXCLUDE.VMDISK "Windows VM3 ?2012R2?" "SCSI 0 1"
```

disk_location

Hyper-V バックアップ操作から除外する仮想マシン・ハード・ディスク (VHDX) のロケーションを指定します。ディスク・ロケーション・ラベルは、先頭が「SCSI」または「IDE」で、その後にコントローラー番号およびデバイス・ロケーション番号を続けて指定する必要があります。ワイルドカード文字は使用できません。

ヒント: 特定の VM 内のディスクのロケーションを判別するには、-preview オプションを指定して **backup vm** コマンドを使用します。構文については、「**VM のバックアップ**」のトピックを参照してください。

例

オプション・ファイル

オプション・ファイルの以下のステートメントで、先頭が WinVM のすべての仮想マシンから Windows システム・ディスクを除外します。

```
exclude.vmdisk WinVM* "IDE 0 0"
```

仮想マシン vm1 に IDE コントローラー番号が 1、デバイス・ロケーションが 0 の仮想ディスクが含まれているとします。この仮想マシン・ディスクを **backup vm** 操作から除外するには、オプション・ファイルに以下のステートメントを指定します。

```
EXCLUDE.VMDISK vm1 "IDE 1 0"
```

仮想マシン vm2 に SCSI コントローラー番号 0 で、デバイス・ロケーションが 1 の仮想マシン・ディスクが含まれているとします。オプション・ファイルに以下のステートメントを指定して、このディスクをバックアップ操作から除外します。

```
EXCLUDE.VMDISK vm2 "SCSI 0 1"
```

コマンド・ライン

以下のコマンド・ラインには、ディスクが除外されることを示すために、vhdx= キーワードの前に除外演算子 (-) を使用する例が示されています。

仮想マシン vm1 のバックアップ操作から IDE ディスク (コントローラー番号 1 でデバイス・ロケーション 0) を除外します。

```
dsmc backup vm "vm1:-vhdx=IDE 1 0"
```

仮想マシン vm2 のバックアップ操作から SCSI ディスク (コントローラー番号 0 でデバイス・ロケーション 1) を除外します。

```
dsmc backup vm "vm2:-vhdx=SCSI 0 1"
```

制約事項: コマンド・ライン上およびオプション・ファイル内のどちらの場合も `all-vm` オプションを `vmname:-vhdx=` オプションと一緒に使用することはできません。

除外対象のディスクを使用する Hyper-V VM のリストアに関するヒント

VM リストア操作時、VM ディスクはバックアップ操作から除外されているために、リストアされないことを示す通知メッセージが表示されます。リストア操作では、元のディスク・ファイルがリストア宛先フォルダーに引き続き存在するかどうかを検証されます。元のディスク・ファイルがまだ存在している場合、リストアされた VM に再接続されます。あるいは、空のディスク・ファイルが同じ属性 (ファイル名、ディスク・サイズ、ブロック・サイズなど) で作成され、その空のディスク・ファイルがリストアされた VM に接続されます。

リストア操作後、リストアされた VM 内のコントローラーとディスクの順序は元の VM と同じままです。リストアされた VM の今後のバックアップ操作のために `EXCLUDE.VMDISK` オプション内のディスク・ロケーションを調整する必要はありません。

ただし、SCSI コントローラーを手動で削除する場合、後続のすべての SCSI コントローラーの番号は変更されます。例えば、「SCSI 0」を削除すると、次の SCSI コントローラー (当初は「SCSI 1」) が「SCSI 0」になります。この場合、`EXCLUDE.VMDISK` オプション内の VM ディスク・ロケーションを更新する必要があります。

「SCSI 0 0」などのディスクのロケーション情報は、バックアップ、リストア、および照会の操作のメッセージに表示されます。

関連資料

[153 ページの『Backup VM』](#)

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

[177 ページの『Domain.vmfull』](#)

`domain.vmfull` オプションは、仮想マシンのフル・イメージ・バックアップ操作に組み込む仮想マシン (VM) を指定します。

[184 ページの『Include.vmdisk』](#)

`INCLUDE.VMDISK` オプションは、バックアップ操作に仮想マシン (VM) ディスクを組み込みます。ディスク・ラベルを指定しない場合は、VM のすべてのディスクがバックアップされます。

Inactive

`inactive` オプションを使用すると、活動状態と非活動状態の両方のオブジェクトを表示することができます。

`inactive` オプションは、**query vm** および **restore vm** コマンドで使用できます。

重要: リストア操作中に `inactive` オプションを使用するときは、すべてのバージョンが予測できない順序でリストアされるため、`pick` オプションも使用してください。`pitdate` を使用する場合、このオプションは暗黙的なオプションになります。

構文

➡ `INActive` ➡

パラメーター

このオプションにパラメーターはありません。

例

コマンド・ライン:

```
dsmc restore vm VM1 -inactive
```

Include.vm

このオプションは、vmc オプションで指定された管理クラスをオーバーライドします。

vmc オプションで指定された管理クラスは、すべてのバックアップに適用されます。include.vm オプションを使用して、1つ以上の仮想マシンに対してその管理クラスをオーバーライドすることができます。vmctlmc オプションで指定された管理クラスについては、include.vm オプションがオーバーライドしたり影響を及ぼしたりすることはありません。vmctlmc オプションは、バックアップされた仮想マシンの制御ファイルを特定の管理クラスにバインドします。

オプション・ファイル

このオプションは、クライアント・オプション・ファイルに設定します。

構文

```
➤ INCLUDE.VM — — vmname — ————— mgmtclassname —
```

パラメーター

vmname

必須のパラメーターです。指定した管理クラスにバインドする仮想マシンの名前を指定します。それぞれの include.vm ステートメントには、1つの仮想マシンのみを指定できます。ただし、各仮想マシンを特定の管理クラスにバインドするためには、いくつでも必要な数の include.vm ステートメントを指定することができます。

仮想マシン名にはワイルドカードを含めることができます。アスタリスク (*) は任意の文字ストリングに一致します。疑問符 (?) は単一の文字に対応します。仮想マシン名にスペース文字が含まれている場合は、名前を二重引用符 (") で囲んでください。

ヒント: 仮想マシン名に特殊文字が含まれている場合は、仮想マシン名を指定する時に特殊文字の代わりに疑問符のワイルドカードを入力してください。

mgmtclassname

オプションのパラメーターです。指定された仮想マシンをバックアップする時に使用する管理クラスを指定します。このパラメーターが指定されていない場合、管理クラスはデフォルトで、vmc オプションによって指定されたグローバル仮想マシン管理クラスに設定されます。

例

IBM Spectrum Protect サーバーに以下の管理クラスが存在しており、アクティブになっていると想定します。

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

例 1

クライアント・オプション・ファイルに含まれている以下の include.vm ステートメントは、VMTEST で始まる名前を持つすべての仮想マシンを、MCFORTESTVMS と呼ばれる管理クラスにバインドします。

```
include.vm vmtest* MCFORTESTVMS
```

例 2

クライアント・オプション・ファイルに含まれている以下の `include.vm` ステートメントは、WHOPPER VM1 [PRODUCTION] という名前の仮想マシンを、MCFORPRODVMS と呼ばれる管理クラスにバインドします。

```
include.vm "WHOPPER VM1 ?PRODUCTION?" MCFORPRODVMS
```

この仮想マシン名はスペース文字を含んでいるため、引用符で囲む必要があります。さらに、仮想マシン名の中の特殊文字に一致させるために、疑問符のワイルドカードが使用されています。

例 3

クライアント・オプション・ファイル内の以下の `include.vm` ステートメントは、VM1 という名前の仮想マシンを、MCUNIQUEVM という名前の管理クラスにバインドします。

```
include.vm VM1 MCUNIQUEVM
```

関連資料

214 ページの『Vmmc』

vmmc オプションは、デフォルト管理クラス以外の管理クラスを使用して仮想マシン・バックアップを保管するために使用します。

Include.vmdisk

INCLUDE.VMDISK オプションは、バックアップ操作に仮想マシン (VM) ディスクを組み込みます。ディスク・ラベルを指定しない場合は、VM のすべてのディスクがバックアップされます。

INCLUDE.VMDISK オプションは、**backup vm** 操作に組み込む VM ディスクのラベルを指定します。

backup vm コマンドでディスクを組み込む場合、コマンド・ライン・パラメーターが、オプション・ファイルの INCLUDE.VMDISK ステートメントをすべてオーバーライドします。

Microsoft Hyper-V 仮想マシンに対する INCLUDE.VMDISK

INCLUDE.VMDISK オプションを使用して、VM ディスクを Hyper-V バックアップ操作に組み込みます。

サポートされるクライアント

このオプションは、すべてのサポート対象の Windows クライアントで使用できます。

オプション・ファイル

このオプションは、クライアント・オプション・ファイルに設定します。コマンド・ライン・パラメーターがオプション・ファイルのステートメントをオーバーライドします。

構文

➡ INCLUDE.VMDISK — *vmname disk_location* ➡

パラメーター

vmname

backup vm 操作に組み込むディスクを含む VM の名前を指定します。この名前は、仮想マシンの表示名です。各 INCLUDE.VMDISK ステートメントに指定できる VM 名は 1 つのみです。組み込む VM ディスクごとに、追加の INCLUDE.VMDISK ステートメントを指定してください。

VM 名に指定できるアスタリスク (*) は任意の文字ストリングと一致し、疑問符 (?) は任意の単一文字と一致します。VM 名がスペース文字を含む場合は、VM 名を引用符 (" ") で囲みます。

ヒント: VM 名が大括弧文字 ([]) または (|) のような特殊文字を含む場合、VM 名が正確に一致しないことがあります。VM 名に特殊文字が含まれる場合は、疑問符 (?) を使用してその特殊文字を表してください。

例えば、"Windows VM3 [2012R2]" という名前の仮想マシンのバックアップに SCSI VM ディスクを組み込むには、オプション・ファイルで次の構文を使用します。

```
INCLUDE.VMDISK "Windows VM3 ?2012R2?" "SCSI 0 1"
```

disk_location

Hyper-V バックアップ操作に組み込む VM ディスクのロケーションを指定します。ディスク・ロケーション・ラベルは、先頭が「SCSI」または「IDE」で、その後にコントローラー番号およびデバイス・ロケーション番号を続けて指定する必要があります。ワイルドカード文字は使用できません。

ヒント: 特定の仮想マシン内のディスクのロケーションを判別するには、-preview オプションを指定して **backup vm** コマンドを使用します。構文については、「**VM のバックアップ**」のトピックを参照してください。

例

オプション・ファイル

仮想マシン vm1 のコントローラー番号 1 およびデバイス・ロケーション 0 に IDE VM ディスク (VHDX) が含まれているとします。この VHDX を **backup vm** 操作に組み込むには、オプション・ファイルに以下のステートメントを指定します。

```
INCLUDE.VMDISK vm1 "IDE 1 0"
```

仮想マシン vm2 のコントローラー番号 0 およびデバイス・ロケーション 1 に SCSI VM ディスクが含まれているとします。この VHDX をバックアップ操作に組み込むには、オプション・ファイルに以下のステートメントを指定します。

```
INCLUDE.VMDISK vm2 "SCSI 0 1"
```

コマンド・ライン

仮想マシン vm1 のバックアップ時に単一の IDE ディスク (コントローラー番号 1 でデバイス・ロケーション 0) を組み込みます。

```
dsmc backup vm "vm1:vhdX=IDE 1 0"
```

仮想マシン vm2 のバックアップ操作に SCSI ディスク (コントローラー番号 0 でデバイス・ロケーション 1) を組み込みます。

```
dsmc backup vm "vm2:vhdX=SCSI 0 1"
```

関連資料

[153 ページの『Backup VM』](#)

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

[177 ページの『Domain.vmfull』](#)

domain.vmfull オプションは、仮想マシンのフル・イメージ・バックアップ操作に組み込む仮想マシン (VM) を指定します。

[180 ページの『Exclude.vmdisk』](#)

EXCLUDE.VMDISK オプションは、仮想マシン・ディスクをバックアップ操作から除外します。

INCLUDE.VMSNAPSHOTATTEMPTS

INCLUDE.VMSNAPSHOTATTEMPTS オプションを使用して、スナップショットの障害が原因で失敗した仮想マシン (VM) バックアップ操作についてのスナップショット 試行の合計回数を決定します。

サポートされるクライアント

このオプションは、Windows Server 2016 オペレーティング・システムで実行する Hyper-V ホストの VM をバックアップするように構成されている、サポート対象の Windows クライアントで使用できます。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) で有効です。サーバー上でクライアント・オプション・セットに組み込むこともできます。コマンド・ラインでは無効です。

構文

➡ INCLUDE.VMSNAPSHOTATTEMPTS — *vmname* — *num_with_quiescing* →

▶ — *num_without_quiescing* ◀

パラメーター

vmname

スナップショットの障害によってバックアップ試行が失敗した場合の、スナップショット 試行の合計回数を指定する仮想マシンの名前を指定する必須の定位置パラメーター。この名前は、仮想マシンの表示名です。

各 INCLUDE.VMSNAPSHOTATTEMPTS ステートメントで指定することができる仮想マシンは 1 つだけです。ただし、別の仮想マシンについてスナップショット 試行の合計回数を構成する場合は、以下の方法を使用することができます。

- このオプションを適用する各仮想マシンに対し、失敗したスナップショットを再試行するために必要な数の INCLUDE.VMSNAPSHOTATTEMPTS ステートメントを指定します。
- *vmname* パラメーター値にワイルドカード文字を使用して、ワイルドカード・パターンに一致する仮想マシン名を選択します。アスタリスク (*) は任意の文字ストリングに一致します。疑問符 (?) は単一の文字に対応します。仮想マシン名にスペース文字が含まれている場合は、名前を二重引用符 (") で囲んでください。

ヒント: 仮想マシン名に特殊文字が含まれている場合は、仮想マシン名を指定する時に特殊文字の代わりに疑問符 (?) のワイルドカードを入力してください。

num_with_quiescing

以下のアクションを指定する定位置パラメーターです。

Hyper-V RCT バックアップ操作の場合:

num_with_quiescing パラメーターは、アプリケーション整合バックアップを作成するために静止を使用してスナップショットを試行する回数を指定します。

0 から 10 の範囲で値を指定できます。デフォルト値は 2 です。

num_without_quiescing

Hyper-V RCT バックアップ操作の場合:

num_without_quiescing オプションは、*num_with_quiescing* オプションで指定した回数の試行が完了した後、静止を行わずにスナップショットを試みる回数を指定します。

0 から 10 の範囲で値を指定できます。デフォルト値は 0 です。

重要: このパラメーターが VM バックアップに適用された場合、そのバックアップはクラッシュ整合と見なされます。その結果、オペレーティング・システム、ファイル・システム、およびアプリケーションの整合性は保証されなくなります。include.vmsnapshotattempts 0 0 エントリは無効です。バックアップ操作では、少なくとも 1 つのスナップショットが必要です。

例

Hyper-V の例:

例 1

LinuxVM で始まるすべての Hyper-V VM に対するクラッシュ整合バックアップ時に合計 2 回のスナップショット試行を行うには、クライアント・オプション・ファイルに以下のステートメントを指定します。

```
INCLUDE.VMSNAPSHOTATTEMPTS LinuxVM* 0 2
```

例 2

仮想マシン VM1 に対して 3 回のスナップショット試行 (アプリケーション整合スナップショット試行を 2 回、それらが失敗した場合はクラッシュ整合スナップショット試行を 1 回) を行うには、クライアント・オプション・ファイルに以下のステートメントを指定します。

```
INCLUDE.VMSNAPSHOTATTEMPTS VM1 2 1
```

INCLUDE.VMTSMVSS

INCLUDE.VMTSMVSS オプションを使用して、アプリケーション・データをホストするゲスト仮想マシン (VM) のバックアップ操作中のアプリケーション保護を有効にします。

INCLUDE.VMTSMVSS オプションは、ゲスト VM 上のアプリケーションに、間もなくバックアップが行われることを通知します。このオプションにより、アプリケーションでは、トランザクション・ログの切り捨てとトランザクションのコミットが可能になるため、バックアップ完了時には整合性のある状態から再開できます。Microsoft SQL Server トランザクション・ログの切り捨てを抑止するために、オプション・パラメーターを指定することができます。

このオプションによって VM が組み込まれた場合は、アプリケーション保護が提供されます。つまり、データ・ムーバーは、VSS ライターを凍結してから解凍し、オプションで、アプリケーション・ログを切り捨てます。VM がこのオプションにより保護されていない場合、アプリケーション保護は、Hyper-V によって提供されます。Hyper-V は、VSS ライターを凍結してから解凍しますが、アプリケーション・ログを切り捨てません。

重要: **diskshadow revert** 操作がリストア中に必要である場合、アプリケーション保護バックアップを開始する前に、Microsoft SQL Server データベースまたは Microsoft Exchange Server データベースなどのアプリケーション・データベースが非ブート・ドライブ (ブート・ドライブ以外のドライブ) 上にあることを確認してください。

オプション・ファイル

このオプションは、データ・ムーバー・オプション・ファイルに設定します。このオプションは、プリファレンス・エディターやコマンド・ラインで設定することはできません。

構文

```
➡ INCLUDE.VMTSMVSS — vmname — — OPTions=KEEPSqllog ➡
```

パラメーター

vmname

静止させるアプリケーションが含まれている VM の名前を指定します。この名前は、Hyper-V Manager での VM 表示名です。INCLUDE.VMTSMVSS ステートメント 1 つにつき 1 つの VM を指定してください

い。例えば、Windows VM3 [2012R2] という名前の VM を組み込むには、オプション・ファイルで次の構文を使用します。

```
INCLUDE.VMTSMVSS "Windows VM3 [2012R2]"
```

このオプションですべての VM を保護するには、ワイルドカードとしてアスタリスクを使用します (INCLUDE.VMTSMVSS *)。任意の単一文字に一致する疑問符 (?) も使用することができます。例えば、INCLUDE.VMTSMVSS vm?? を指定すると、vm で始まり、その後に任意の 2 文字が続く名前 (vm10、vm11、vm17 など) を持つすべての VM が保護されます。

ヒント: VM 名が大括弧文字 ([または]) のような特殊文字を含む場合、VM 名が正確に一致しないことがあります。VM 名に特殊文字が含まれている場合は、疑問符文字 (?) を使用して、VM 名で使用されている特殊文字に一致させることができます。

このパラメーターにはデフォルト値はありません。アプリケーション保護を有効にするには、保護する VM を 1 つ以上の INCLUDE.VMTSMVSS ステートメントに組み込む必要があります。ディスクに保護したいアプリケーション・データが入っている場合は、VM のディスクを除外 (EXCLUDE.VMDISK オプションを使用して) していないことを確認します。

OPTions=KEEPSqllog

Microsoft SQL Server のみの場合: INCLUDE.VMTSMVSS ステートメントで OPTions KEEPSqllog パラメーターを指定すると、データ・ムーバー・ノードにインストールされたデータ・ムーバーが SQL Server を稼働している VM をバックアップする際に、このパラメーターによって SQL Server ログが切り捨てられなくなります。

このパラメーターを指定すると、SQL サーバー管理者は SQL サーバー・ログを手動でバックアップ、および場合によっては切り捨てることのできるため、ログを保存し、VM がリストアされた後に特定のチェックポイントに SQL トランザクションをリストアするために使用できます。

このオプションを指定すると、SQL ログは切り捨てられず、サーバーに次のメッセージが表示されてログに記録されます。

```
ANS4179I IBM Spectrum Protect application protection
did not truncate the Microsoft SQL Server logs on VM 'VM'.
```

OPTIONS=KEEPSQLLOG オプションを除去して、バックアップ完了時の SQL ログの切り捨てを有効にすることができます。

注: クライアントは SQL ログ・ファイルをバックアップしません。SQL 管理者は、ログ・ファイルをバックアップして、データベースがリストアされた後に適用できるようにする必要があります。

例

オプション・ファイル

vm_example という名前の VM のアプリケーション保護を構成します。

```
INCLUDE.VMTSMVSS vm_example
```

SQL Server の場合: vm11、vm12、および vm15 のアプリケーション保護を構成します。

```
INCLUDE.VMTSMVSS vm11
INCLUDE.VMTSMVSS vm12
INCLUDE.VMTSMVSS vm15 options=keepsqlllog
```

コマンド・ライン

適用外; このオプションはコマンド・ラインで指定することはできません。

関連概念

[189 ページの『データ・ムーバーからアプリケーション 保護バックアップをリストアする場合のシャドー・コピーの考慮事項』](#)

Windows 仮想マシン (VM) では、データ・ムーバーからアプリケーション保護バックアップをリストアしようとする場合、アプリケーション保護バックアップのリストア時のシャドー・コピーの制約事項に注意してください。

関連資料

Exclude.vmdisk

EXCLUDE.VMDISK オプションは、仮想マシン・ディスクをバックアップ操作から除外します。

Include.vmdisk

INCLUDE.VMDISK オプションは、バックアップ操作に仮想マシン (VM) ディスクを組み込みます。ディスク・ラベルを指定しない場合は、VM のすべてのディスクがバックアップされます。

186 ページの『INCLUDE.VMSNAPSHOTATTEMPTS』

INCLUDE.VMSNAPSHOTATTEMPTS オプションを使用して、スナップショットの障害が原因で失敗した仮想マシン (VM) バックアップ操作についてのスナップショット試行の合計回数を決定します。

データ・ムーバーからアプリケーション保護バックアップをリストアする場合のシャドー・コピーの考慮事項

Windows 仮想マシン (VM) では、データ・ムーバーからアプリケーション保護バックアップをリストアしようとする場合、アプリケーション保護バックアップのリストア時のシャドー・コピーの制約事項に注意してください。

シャドー・ストレージのスペース不足

アプリケーション保護バックアップのフル VM リストアを実行すると、リストアされた VM にはシステム・プロバイダー・スナップショットが存在します。アプリケーションがディスクに書き込むにつれて、シャドー・ストレージ・スペースは、ディスク・スペースを使い尽くすまで増大します。

通常、バックアップ時にアプリケーション保護が使用された場合、データベースのリストアにはアプリケーション保護リストアのみを使用します。アプリケーションをリストアすると、ボリュームが自動的に復帰します。ただし、フル VM をリストアする必要がある場合は、シャドー・コピーを手動で復帰または削除する必要があります。

VM 全体をリストアした後、リストアが正常に完了し、データが破損していないことを確認してください。データが破損していない場合は、シャドー・コピーを削除します。データが破損している場合は、シャドー・コピーを復帰させてデータ整合性を回復します。

リストアされた各ボリュームのルート・ディレクトリーにある dsmShadowCopyID.txt ファイルを確認することで、どのシャドー・コピーを削除あるいは復帰するかを判別することができます。このファイルには、スナップショット試行中に作成されたシャドー・コピーのスナップショット ID が含まれます。

diskshadow コマンド **delete shadows** を使用してこれらの ID を削除するか、**revert** コマンドを使用してシャドー・コピーを復帰させることができます。削除または復帰が完了したら、dsmShadowCopyID.txt ファイル削除することもできます。

重要: 復帰操作が成功するには、Microsoft SQL Server データベースまたは Microsoft Exchange Server データベースなどのアプリケーション・データベースが非ブート・ドライブ (ブート・ドライブ以外のドライブ) 上に存在しなければなりません。

アプリケーション保護リストア中にはリストアされたボリュームでシャドー・コピーが使用可能でなければならない

場合によっては、VM バックアップの開始前に、アプリケーション整合シャドー・コピーを作成するために、アプリケーション保護バックアップ操作で Volume Shadow Copy Service (VSS) を使用場合があります。シャドー・コピーの作成後に加えられた変更はすべて、シャドー・ストレージに保存されます。

シャドー・コピーがアプリケーションのリストア中に使用できない場合、データベースのリストアは失敗する可能性があります。リストアされたボリュームをアプリケーション整合状態に戻すには、リストア時にシャドー・コピーが使用されます。シャドー・コピーが使用できない場合、リストアされたデータは不整合状態になります。

以下の状態により、シャドー・コピーが使用不可になる場合があります。

- 通常、シャドー・ストレージはボリュームの一部です。ただし、シャドー・ストレージ・スペースが、デフォルトで、または手動で、別のボリュームにあるように構成される場合があります。この場合、VM バックアップ操作中に作成されたシャドー・コピーがリストア時に使用できないので、データベースのリストアは失敗することがあります。
- シャドー・ストレージがあるボリュームがバックアップ時に除外されたため、シャドー・ストレージは使用できません。

この問題には、以下の回避策が使用できます。

- VM バックアップを実行する前に、**vssadmin add shadowstorage** コマンドを使用して、ゲスト VM で使用可能なボリュームごとにシャドー・コピー・ストレージのアソシエーションを追加します。例えば、ボリューム E: でボリューム E: のシャドー・ストレージ・ロケーションを設定するには、次のコマンドを発行します。

```
vssadmin add shadowstorage /for=E: /on=E: /maxsize=unbounded
```

重要: VM に既存の VSS スナップショットがある場合、**vssadmin add shadowstorage** コマンドが失敗する可能性があります。VSS スナップショットを作成したのと同じアプリケーションを使用して、それらの VSS スナップショットを削除する必要があります。

例えば、LOCAL バックアップの宛先を持つ Exchange データベースの VSS バックアップが IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server によって作成された場合、その VSS バックアップを削除するには、Data Protection for Microsoft Exchange Server アプリケーションを使用します。認識できない VSS スナップショットが存在する場合、その VSS スナップショットを削除するには、Windows **diskshadow** コマンド **delete shadows** を使用します。

また、シャドー・ストレージを保持するボリュームがバックアップ操作から除外されないようにしてください。

- 手動でスナップショットを戻して、データベース・ファイルのアプリケーション整合性を実現します。
 1. IBM Spectrum Protect リカバリー・エージェント を使用して、VM バックアップ内のすべてのディスクをマウントします。
 2. Windows **diskshadow** コマンドを対話式モードで開始します。
 3. 対話式 **diskshadow** モードで、次のコマンドを発行します。

```
list shadows all
```

4. マウントされた各ドライブのルート・ディレクトリーで、dsmShadowCopyID.txt ファイルを見つけます。このファイルには、ボリューム復帰操作に必要な VSS シャドー・コピーのグローバル固有 ID (GUID) が含まれています。
5. dsmShadowCopyID.txt ファイルを開き、データベース・ファイルが置かれているボリュームの GUID を識別します。
6. 対話式 **diskshadow** モードで、次のコマンドを発行します。

```
revert GUID
```

ここで、*GUID* は、dsmShadowCopyID.txt ファイルで識別されたスナップショット GUID です。

復帰操作が成功するには、アプリケーション・データベースが非ブート・ドライブ上に存在しなければなりません。

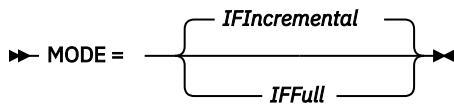
mode

mode オプションを使用して、特定のバックアップ操作の実行時にバックアップ・モードを指定します。

mode オプションは、**backup vm** コマンドで使用できます。このパラメーターは、Hyper-V 仮想マシンのフルイメージ・バックアップ、永久増分のフルバックアップ、または永久増分の増分バックアップのいずれを実行するかを指定します。

mode オプションは、ロー論理装置のバックアップ時には影響を与えません。

構文



パラメーター

IFIncremental

Hyper-V 仮想マシンの永久増分の増分バックアップを実行することを指定します。永久増分の増分バックアップでは、前回のバックアップ以降に変更されたディスク・ブロックのみをバックアップします。これがデフォルトのバックアップ・モードです。

クライアントがバックアップ・データを暗号化するように構成されている場合、仮想マシンのバックアップにはこのバックアップ・モードを使用できません。

IFFull

Hyper-V 仮想マシンの永久増分フルバックアップを実行することを指定します。永久増分フルバックアップは、仮想マシンのディスク上で使用されているブロックすべてをバックアップします。デフォルトでは、mode=ifincremental を指定した場合 (あるいは mode オプションをデフォルトのままにした場合) でも、Hyper-V 仮想マシンの最初のバックアップは永久増分のフルバックアップ (mode=iffull) になります。後続のバックアップは、デフォルトの mode=ifincremental になります。

クライアントがバックアップ・データを暗号化するように構成されている場合、仮想マシンのバックアップにはこのバックアップ・モードを使用できません。

例

タスク

msvm1 という名前の Windows Hyper-V VM の永久増分フル VM バックアップを実行します

```
dsmc backup vm msvm1 -mode=iffull
```

タスク

msvm1 という名前の Windows Hyper-V VM の永久増分の増分バックアップを実行します

```
dsmc backup vm msvm1 -mode=ifincremental
```

関連資料

[153 ページの『Backup VM』](#)

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

Mbobjrefreshthresh

mbobjrefreshthresh (メガブロック・オブジェクト最新表示しきい値) オプションは、しきい値を定義する数値です。任意の 128 MB のメガブロックを記述するのに必要な IBM Spectrum Protect オブジェクトの数がこの値を超えた場合、メガブロック全体が最新表示され、前のバックアップでそのエリアを表すのに使用されたオブジェクトは有効期限が切れます。

仮想マシンをバックアップすると、データは IBM Spectrum Protect サーバーに 128 MB 単位 (メガブロックと呼ばれる) で保管されます。実動ディスク上のエリアが変更し、新しい増分バックアップが実行される場合、以前にバックアップされたデータに行われた変更を表す新しいメガブロックが作成されます。増分バックアップのたびに新しいメガブロックが作成されるため、結果的にメガブロックは IBM Spectrum

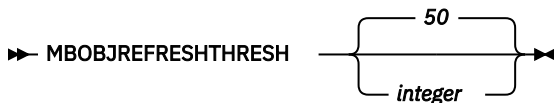
Protect データベースのパフォーマンスに悪影響を与え、さらには、ほとんどの IBM Spectrum Protect 操作に悪影響を及ぼす可能性があります。

仮想マシンのバックアップごとの実動データを表す IBM Spectrum Protect オブジェクトの数を見積もる場合に、このオプションを使用します。例えば、IBM Spectrum Protect オブジェクトの数がこの値を超える場合、メガブロックは最新表示されます。このアクションは、128 MB ブロック全体が IBM Spectrum Protect サーバーにコピーされ、単一の IBM Spectrum Protect オブジェクトとして表されることを意味しています。最小値は 2 で、最大値は 8192 です。デフォルト値は、50 です。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) で有効です。サーバー上でクライアント・オプション・セットに組み込むこともできます。コマンド・ラインでは無効です。

構文



パラメーター

指定できる最小値は 2 メガブロックで、最大値は 8192 メガブロックです。デフォルトは 50 メガブロックです。

例

このオプションを設定すると、更新されたメガブロックを表すのに必要なオブジェクトの数が 20 を超える場合に、メガブロックの最新表示を起動します。

```
MBOBJREFRESHTHRESH 20
```

Mbpctrefreshthresh

mbpctrefreshthresh (メガブロック・パーセンテージ最新表示しきい値) オプションは、しきい値を定義する数値です。任意の 128 MB のメガブロックを記述するのに必要なオブジェクトの IBM Spectrum Protect パーセンテージの数値がこの値を超える場合、メガブロック全体が最新表示され、前のバックアップでそのエリアを表すのに使用されたオブジェクトは有効期限が切れます。

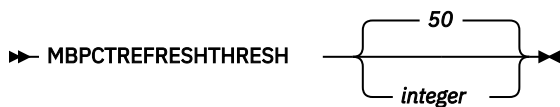
仮想マシンをバックアップすると、データは IBM Spectrum Protect サーバーに 128 MB 単位 (メガブロックと呼ばれる) で保管されます。実動ディスク上のエリアが変更し、新しい増分バックアップが実行される場合、以前にバックアップされたデータに行われた変更を表す新しいメガブロックが作成されます。増分バックアップのたびに新しいメガブロックが作成されるため、結果的にメガブロックは IBM Spectrum Protect データベースのパフォーマンスに悪影響を与え、さらには、ほとんどの IBM Spectrum Protect 操作に悪影響を及ぼす可能性があります。

仮想マシンごとにバックアップされる追加データの量を見積もる場合にこのオプションを使用します。例えば、実動ディスクの 128 MB ブロックが指定されたパーセンテージを超えて変更された場合、128 MB ブロック全体が IBM Spectrum Protect サーバーにコピーされます。ブロックは、単一の IBM Spectrum Protect オブジェクトとして表示されます。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) で有効です。サーバー上でクライアント・オプション・セットに組み込むこともできます。コマンド・ラインでは無効です。

構文



パラメーター

指定できる最小値は 1 パーセントで、最大値は 99 パーセントです。デフォルトは 50 パーセントです。

例

このオプションを設定すると、実動ディスク上のメガブロックのオブジェクトの 50 パーセント (またはそれ以上) が変更された場合に、メガブロック最新表示を起動します。

```
MBPCTREFRESHTHRESHOLD 50
```

Noprompt

noprompt オプションは、**expire** コマンドで表示される確認プロンプトを抑止します。

noprompt オプションは、**expire** コマンドで使用します。

構文

```
➡ NOPrompt ➡
```

パラメーター

このオプションにパラメーターはありません。

例

コマンド・ライン:

```
dsmc expire -noprompt c:¥home¥project¥*
```

Numberformat

numberformat オプションは、数値を表示する際に使用するフォーマットを指定します。

このオプションは、使用しているメッセージ・リポジトリの言語のデフォルト数値形式を変更したい場合に使用します。

デフォルトの場合、フォーマット情報はクライアントの呼び出し時に有効なロケール定義から取得されます。ロケール定義のセットアップ方法の詳細については、ローカル・システム側のドキュメンテーションを参照してください。

numberformat オプションは、**expire** コマンドにのみ使用できます。

オプション・ファイル

このオプションは、クライアント・ユーザー・オプション・ファイル (dsm.opt) に入れます。このオプションは、プリファレンス・エディターの「地域設定」タブの「数値形式」フィールドで設定できます。

構文

```
➡ NUMberformat — — number ➡
```

パラメーター

number

次のフォーマットのいずれかを使用して数値を表示します。使用したい数値形式と対応する数値 (0-6) を指定してください。

0

ロケール指定の日付形式を使用します。これがデフォルトです (Mac OS X には適用されません)。

1

1,000.00

これは、以下の使用可能翻訳の場合のデフォルトです。

- 米国英語
- 日本語
- 中国語 (繁体字)
- 中国語 (簡体字)
- 韓国語

2

1,000,00

3

1 000,00

これは、以下の使用可能翻訳の場合のデフォルトです。

- フランス語
- チェコ語
- ハンガリー語
- ポーランド語
- ロシア語

4

1 000.00

5

1.000,00

これは、以下の使用可能翻訳の場合のデフォルトです。

- ブラジル・ポルトガル語
- ドイツ語
- イタリア語
- スペイン語

6

1'000,00

例

オプション・ファイル:

num 4

コマンド・ライン:

-numberformat=4

このオプションは、初期コマンド・ラインおよび対話モードでのみ有効です。このオプションを対話モードで使用した場合には、このオプションが指定されたコマンドにのみ影響が及びます。そのコマンドが完了すると、値は対話式セッションの開始時の値に戻ります。この値は、初期コマンド・ラインまたはサーバーが強制するオプションによって指定変更されない限り、dsm.opt ファイルの値です。

Pick

pick オプションは、入力したファイル指定と一致するバックアップ・バージョン、またはアーカイブ・コピーのリストを作成します。

このリストから、処理するバージョンが選択できます。**inactive** オプションを含めると、活動状態と非活動状態の両方のオブジェクトを表示することができます。

pick オプションは、**restore vm** コマンドで使用します。

構文

➡ PITick ➡

パラメーター

このオプションにパラメーターはありません。

例

コマンド・ライン:

```
dsmc restore vm vmfin* -pick -inactive
```

Pitdate

pitdate オプションは、バックアップの最新バージョンを表示またはリストアしたい特定時点を設定するために **pittime** オプションと一緒に使用します。

指定された日時またはそれ以前にバックアップされていて、指定の日時以前に削除されていないファイルが処理されます。この日付と時刻より後で作成されたバックアップ・バージョンは無視されます。

pitdate オプションは、**query vm** コマンドと **restore vm** コマンドで使用します。

pitdate を使用する場合、**inactive** オプションと **latest** オプションは、暗黙的なオプションになります。

構文

➡ PITDate = — — date ➡

パラメーター

date

適切な日付を指定します。

例

コマンド・ライン:

```
dsmc restore vm vmfin3 -pitdate=02/21/2014
```

Pittime

pittime オプションは、最新バージョンのバックアップを表示またはリストアする特定時点を設定するために **pitdate** オプションと共に使用します。

指定された日時またはそれ以前にバックアップされていて、指定の日時以前に削除されていないファイルが処理されます。この日付と時刻より後で作成されたバックアップ・バージョンは無視されます。

pitdate オプションを指定しない場合は、このオプションは無視されます。

pitttime オプションは、**query vm** コマンドと **restore vm** コマンドで使用します。

構文

►► PITTime = — — time ►►

パラメーター

time

指定された日付の時刻を指定します。時刻を指定しないと、デフォルトの 23:59:59 になります。

例

コマンド・ライン:

```
dsmc query vm vmfin1 -pitt=06:00:00 -pitd=02/03/2014
```

Skipsystemexclude

IBM Spectrum Protect for Virtual Environments クライアントがデフォルトでスキップする 特定のオペレーティング・システム・ファイルに対する exclude ステートメントを処理する方法を指定するには、skipsystemexclude オプションを使用します。

デフォルトで、IBM Spectrum Protect for Virtual Environments クライアントは、仮想マシン (VM) バックアップ操作中にシステム・リカバリーに通常必要ない特定の Windows オペレーティング・システム・ファイルスキップします。これらのファイルには、Windows システム・ファイル、一時インターネット・ファイル、「ゴミ箱」内のファイルがあります。

このオプションを使用すると、これらのオペレーティング・システム・ファイルに対する exclude ステートメントの処理をスキップすることができます。これらの exclude ステートメントを処理しないことによって、VM のバックアップにかかる時間を短縮できる場合があります。

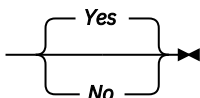
サポートされるクライアント

このオプションは、Windows オペレーティング・システムの IBM Spectrum Protect for Virtual Environments クライアントにのみ有効です。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) またはコマンド・ラインで有効です。

構文

►► SKIPSYSTemexclude 

パラメーター

Yes

VM バックアップ操作中に特定の Windows オペレーティング・システム・ファイルに対する exclude ステートメントの処理をスキップするには、このパラメーターを指定します。このパラメーターがデフォルトです。

No

Windows オペレーティング・システム・ファイルの exclude ステートメントを処理するには、このパラメーターを指定します。このパラメーターを選択し、Hyper-V ホストのファイル・バックアップを実行すると、オペレーティング・システム・ファイルは除外されます。

例

オプション・ファイル

```
SKIPSYSTemexclude yes
```

コマンド・ライン

```
dsmc backup vm -SKIPSYST=yes
```

```
dsmc incr -skipsyst=no
```

Timeformat

timeformat オプションは、システム時刻を表示および入力する形式を指定します。

このオプションは、使用しているメッセージ・リポジトリの言語のデフォルト時刻形式を変更したい場合に使用します。

デフォルトの場合、フォーマット情報はクライアントの呼び出し時に有効なロケール定義から取得されます。ロケール定義のセットアップ方法の詳細については、ローカル・システム側のドキュメンテーションを参照してください。

timeformat オプションは、**expire** コマンドにのみ使用できます。

コマンドに timeformat オプションを組み込む場合には、fromtime、pittime、および totime オプションの前に入れる必要があります。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) に入れます。このオプションは、プリファレンス・エディターの「地域設定」タブの「時刻形式」フィールドで設定できます。

構文

➡ TIMEformat — — *format_number* ➡

パラメーター

format_number

ここにリストされたフォーマットの 1 つで時刻を表示します。使用するフォーマットに対応するフォーマット番号を選択します。コマンドに timeformat オプションを組み込む場合は、pittime オプションの前に指定する必要があります。

- | | |
|----------|--------------|
| 1 | 23:00:00 |
| 2 | 23,00,00 |
| 3 | 23.00.00 |
| 4 | 12:00:00 A/P |
| 5 | A/P 12:00:00 |

例

オプション・ファイル:

```
timeformat 4
```

コマンド・ライン:

```
-time=3
```

このオプションは、初期コマンド・ラインおよび対話モードでのみ有効です。このオプションを対話モードで使用了場合には、このオプションが指定されたコマンドにのみ影響が及びます。そのコマンドが完了すると、値は対話式セッションの開始時の値に戻ります。この値は、初期コマンド・ラインまたはサーバーが強制するオプションによって指定変更されない限り、`dsm.opt` ファイルの値です。

日時形式の指定についてのその他の考慮事項

このオプションで指定する日時形式は、日時を入力データとして処理するオプションの使用時に使用する必要があります。例: `totime`、`fromtime`、`todate`、`fromdate`、および `pittime`。

例えば `timeformat` オプションを `TIMEFORMAT 4` と指定する場合、`fromtime` や `totime` オプションに指定する値は、`12:24:00pm` のような時刻に指定する必要があります。 `TIMEFORMAT 4` で指定する時刻の整数は 12 以下でなければならないため、`13:24:00` と指定しても無効です。オプションに指定できる時間の値を最大で 24 とし、コンマを区切り文字として使用したい場合は、`TIMEFORMAT 2` を指定する必要があります。

vmautostartvm

`vmautostartvm` オプションを使用して、インスタント・アクセス処理中に作成された仮想マシン (VM) を自動的に電源オンするかどうかを指定します。このオプションは、**restore VM** `vmrestoretype=instantaccess` コマンドと一緒に使用した場合にのみ有効です。

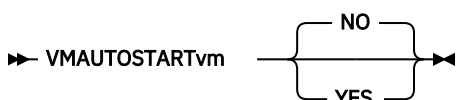
サポートされるクライアント

このオプションは、サポートされる Windows クライアントで使用可能です。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (`dsm.opt`) に入れるか、コマンド・ラインに指定してください。

構文



パラメーター

NO

インスタント・アクセス用に作成された VM は自動的に開始されません。VM を手動で開始する必要があります。このパラメーターがデフォルト設定です。デフォルトでは、既存の VM との競合の可能性を回避するために、VM をパワーオンの前に再構成する機会が得られます。

YES

インスタント・アクセス用に作成された VM は自動的に開始されます。

例

オプション・ファイル:

`VMAUTOSTARTvm NO`

コマンド・ライン:

```
dsmc restore vm Oslo -VMRESToretype=INSTANTAccess -vmname=Oslo_verify  
-VMAUTOSTARTvm=YES
```

Vmbackdir

vmbackdir オプションは、クライアントが Microsoft Hyper-V 仮想マシンの仮想マシンのフル VM バックアップおよびリストア操作中に作成される制御ファイルを保存する一時ディスク・ロケーションを指定します。

データ・ムーバー・ノード上のクライアントは、仮想マシンのフル VM バックアップを開始するときに、バックアップされる仮想マシンとそのデータに関連付けられたファイル内にメタデータを作成します。メタデータを含むファイルは制御ファイルと呼ばれます。

フル VM バックアップ操作中、バックアップが完了し、仮想マシンのデータと制御ファイルの両方がサーバー・ストレージに保存されるまで、メタデータはデータ・ムーバー・ノード上のディスクに保存されます。フル VM リストア操作では、制御ファイルがサーバーからコピーされ、データ・ムーバー・ディスクに一時保管されます。制御ファイルはそこで仮想マシンとそのデータのリストアに使用されます。バックアップ操作またはリストア操作完了すると、制御ファイルは不要になり、クライアントは一時ディスク・ロケーションから制御ファイルを削除します。

このオプションで指定するディレクトリーは、フル VM バックアップからの制御情報を収容するのに十分なフリー・スペースがあるドライブ上になければなりません。

オプション・ファイル

このオプションは、クライアント・オプション・ファイルに設定するか、**backup vm** または **restore vm** コマンドのオプションとしてコマンド・ラインに指定します。

構文

➡ VMBACKDir — directory ➡

パラメーター

directory

制御ファイルが保管されるバックアップ・サーバー上のパスを指定します。

デフォルトは `c:\mnt\%tsmvmbbackup%\fullvm\` です。

例

オプション・ファイル:

VMBACKD c:\mnt\%tsmvmbbackup%

コマンド・ライン:

dsmc backup vm -VMBACKUPT=fullvm -VMBACKD=G:\virtual_machine\control_files\

dsmc restore vm -VMBACKUPT=fullvm -VMBACKD=G:\san_temp\

Vmctlmc

このオプションは、仮想マシンの制御ファイルのバックアップ時に使用する管理クラスを指定します。

デフォルトでは、仮想マシンの制御ファイルは、デフォルト管理クラスにバインドされています。vmmc オプションを使用すると、仮想マシンのデータ・ファイルと仮想マシンの制御ファイルのバインド先に異なる管理クラスを指定できます。vmctlmc オプションは、仮想マシンの制御ファイルのデフォルト管理クラスと vmmc オプションをオーバーライドします。

ある特定の状況では、制御ファイルを、データ・ファイルとは異なる管理クラスにバインドすることが適切または必要な場合があります。

仮想マシン・データ・ファイルがテープにバックアップされる場合は、vmctlmc オプションが必要です。仮想マシンの制御ファイルは、テープにマイグレーションしないディスク・ベースのストレージ・プールにバックアップする必要があります。ストレージ・プールは、ランダム・アクセス・ボリュームと順次フ

ファイル・ボリュームで構成できます。また、ストレージ・プールは重複排除プールにすることもできます。
vmctlmc オプションを使用して、そのようなストレージ・プールにデータを保存する管理クラスを指定します。

制約事項: vmctlmc オプションに指定される管理クラスは、仮想マシンの制御ファイルの宛先ストレージ・プールのみ決定します。制御ファイルの保存は、vmmc オプション (指定した場合)、またはデフォルト管理クラスによって決定されます。仮想マシン制御ファイルの保存は、常に仮想マシン・データ・ファイルの保存と一致します。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル `dsm.opt` に入れます。

構文

➡ VMCTLmc — *class_name* ➡

パラメーター

class_name

仮想マシンの制御ファイルのバックアップに適用する管理クラスを指定します。このオプションを設定しない場合、vmmc オプションで指定された管理クラスが使用されます。このオプションを設定せず、vmmc オプションも設定されていない場合は、ノードのデフォルト管理クラスが使用されます。

例

オプション・ファイル:

vmctlmc diskonlymc

コマンド・ライン:

適用しません。

Vmmxbackupsessions

vmmxbackupsessions オプションは、最適化されたバックアップ操作に組み込むことができる、仮想マシン (VM) データをサーバーに送信する IBM Spectrum Protect サーバー セッションの最大数を指定します。

最適化されたバックアップ操作とは、VM レベル、仮想ディスク・レベル、あるいはサブディスク・レベルでの並列バックアップ機能が有効にされたバックアップ操作です。

vmmxbackupsessions オプションは、vmmxparallel オプションと連携して、バックアップ操作を最適化し、Hyper-V 環境のホストでバックアップ操作により発生する可能性があるリソースの量を制御できます。これらのオプションの値を調整して、ご使用の環境でバックアップ操作に最適なパフォーマンスを提供する組み合わせを見つけてください。

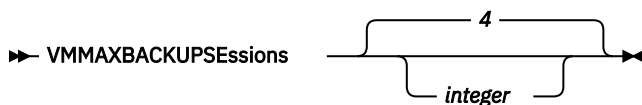
サポートされるクライアント

このオプションは、Windows Server 2012 R2、Windows Server 2016、およびそれ以降のオペレーティング・システム上のデータ・ムーバーで使用できます。このオプションは、Windows Server 2012 上のデータ・ムーバーではサポートされません。

オプション・ファイル

このオプションは、データ・ムーバー・オプション・ファイル (`dsm.hostname_HV_DM.opt`) で使用する場合、あるいはコマンド・ラインで **backup vm** コマンドを使用する場合に有効です。また、IBM Spectrum Protect サーバー のクライアント・オプション・セットに組み込むこともできます。

構文



パラメーター

integer

バックアップ操作中に作成できる IBM Spectrum Protect サーバー セッションの最大数を指定します。デフォルトは 4 です。最大値は 100 です。

ヒント: 構成ウィザードを使用して Data Protection for Microsoft Hyper-V を構成する場合、デフォルトは 16 です。この値は、データ・ムーバー・オプション・ファイルで自動的に更新されます。

vmmxbackupsessions オプションを vmmxparallel オプションまたは maxnummp サーバー・パラメーターと一緒に使用する場合、以下の情報を確認してください。

vmmxparallel

vmmxparallel オプションは、ある一時点で IBM Spectrum Protect サーバーにバックアップできる VM の最大数を指定します。vmmxbackupsessions オプションの値は、vmmxparallel オプションの値以上である必要があります。

この値が vmmxparallel オプションより小さい場合、次のメッセージが返され、値が vmmxparallel オプションと同じ値に変更されます。

ANS9995W The value of the VMMAXBACKUPSESSIONS option is *number_value*.
この値は、VMMAXPARALLEL オプションの値 *number_value* 以上である必要があります。値は、VMMAXPARALLEL オプションの値に設定されます。

maxnummp

maxnummp サーバー・パラメーターは、ストレージ・プールのコピー宛先が FILE または TAPE の場合に、ノードが IBM Spectrum Protect サーバーで利用できるマウント・ポイントの最大数を指定します。maxnummp パラメーター設定は、vmmxparallel および vmmxbackupsessions のオプション設定値以上である必要があります。データ・ムーバーの複数インスタンスがファイルをバックアップしている場合、あるいは単一データ・ムーバーが並列バックアップを実行する場合に、追加のマウント・ポイントが必要になることがあります。

vmmxparallel オプションまたは vmmxbackupsessions オプションの値が maxnummp パラメーターの値を超えている場合、ANS0266I およびその他のメッセージが表示されます。メッセージに応じて、データ・ムーバーは、maxnummp パラメーターで指定された数に一致するように vmmxparallel オプションの値を減らすか、指定された VM に対して追加セッションが開かれることを禁止します。いずれの場合も、バックアップ操作は続行されます。

追加の ANS0266I エラーが検出された場合、データ・ムーバーは、vmmxparallel 値を 1 ずつ減らし、バックアップ操作の続行を試行します。vmmxparallel を 1 まで減らしても ANS0266I エラーが生成される場合は、バックアップ操作は終了されて、次のエラーが発行されます。

ANS5228E A backup VM operation failed because VMMAXPARALLEL was reduced to 1 and the client still cannot obtain a server mount point.

ノードが追加の並列バックアップ・セッションをサポートできるように maxnummp パラメーターの値を増やしたい場合は、サーバー管理者に連絡してください。

例

オプション・ファイル

VMMAXBACKUPS 10

コマンド・ライン:

dsmc backup vm -VMMAXBACKUPS=10

関連タスク

239 ページの『複数の仮想マシンの並列バックアップ (最適化されたバックアップ)』

並列バックアップ処理では、複数の仮想マシン (VM) を同時にバックアップすることができ、VM バックアップ操作のパフォーマンスを最適化できます。

関連資料

202 ページの『Vmmxparallel』

vmmxparallel オプションを使用すると、データ・ムーバーの単一インスタンスを使用して、複数の仮想マシン (VM) の並列バックアップを構成できます。このオプションは、一度に IBM Spectrum Protect サーバーにバックアップできる VM の最大数を指定します。

153 ページの『Backup VM』

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

237 ページの『バックアップ操作の最適化』

仮想マシン (VM) のバックアップ操作を最適化するためには、vmmxparallel オプションの設定を調整します。このオプションを使用すると、Hyper-V ホストに悪影響を及ぼすことなくバックアップ操作を最適化することができます。

Vmmxparallel

vmmxparallel オプションを使用すると、データ・ムーバーの単一インスタンスを使用して、複数の仮想マシン (VM) の並列バックアップを構成できます。このオプションは、一度に IBM Spectrum Protect サーバーにバックアップできる VM の最大数を指定します。

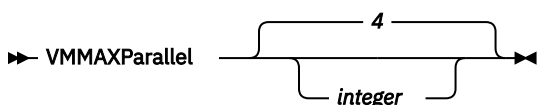
最適化されたバックアップ操作とは、VM レベル、仮想ディスク・レベル、あるいはサブディスク・レベルでの並列バックアップ機能が有効にされたバックアップ操作です。

vmmxparallel オプションは、vmmxbackupsessions オプションと連携してバックアップ操作を最適化し、バックアップで Hyper-V ホスト上に作成できるリソースの量を制御するのに役立ちます。これらのオプションの値を調整して、ご使用の環境におけるバックアップで最適なパフォーマンスを得られる値を見つけてください。

オプション・ファイル

このオプションは、データ・ムーバー・オプション・ファイル (dsm.hostname_HV_DM.opt) で使用する場合、あるいはコマンド・ラインで **backup vm** コマンドを使用する場合に有効です。サーバー上でクライアント・オプション・セットに組み込むこともできます。

構文



パラメーター

integer

並列バックアップ操作中に、一度にバックアップできる VM の最大数を指定します。デフォルトは 4 です。最大値は 50 です。

ヒント: クライアント・サイドのデータ重複排除を使用している場合は、重複排除セッションが各 VM で開始されます。この重複排除セッションは、vmmxparallel セッションの 1 つとしてカウントされません。

vmmxparallel オプションを vmmxbackupsessions オプションまたは maxnummp サーバー・パラメーターと組み合わせて使用する場合は、以下の情報を確認してください。

vmmaxbackupsessions

vmmaxbackupsessions は、最適化されたバックアップ操作に組み込むことができる、IBM Spectrum Protect サーバーに VM データを送信するセッションの最大数を指定します。vmmaxbackupsessions オプションの値は、vmmaxparallel オプションの値以上である必要があります。

maxnummp

maxnummp サーバー・パラメーターは、ストレージ・プールのコピー宛先が FILE または TAPE の場合に、ノードが IBM Spectrum Protect サーバーで利用できるマウント・ポイントの最大数を指定します。maxnummp パラメーター設定は、vmmaxparallel および vmmaxbackupsessions のオプション設定値以上である必要があります。データ・ムーバーの複数インスタンスがファイルをバックアップしている場合、あるいは単一データ・ムーバーが並列バックアップを実行する場合に、追加のマウント・ポイントが必要になることがあります。

vmmaxparallel オプションまたは vmmaxbackupsessions オプションの値が maxnummp パラメーターの値を超えている場合、ANS0266I およびその他のメッセージが表示されます。メッセージに応じて、データ・ムーバーは、maxnummp パラメーターで指定された数に一致するように vmmaxparallel オプションの値を減らすか、指定された VM に対して追加セッションが開かれることを禁止します。いずれの場合も、バックアップ操作は続行されます。

追加の ANS0266I エラーが検出された場合、データ・ムーバーは、vmmaxparallel 値を 1 ずつ減らし、バックアップ操作の続行を試行します。vmmaxparallel を 1 まで減らしても ANS0266I エラーが生成される場合は、バックアップ操作は終了されて、次のエラーが発行されます。

```
ANS5228E A backup VM operation failed because VMMAXPARALLEL was reduced
to 1 and the client still cannot obtain a server mount point.
```

ノードが追加の並列バックアップ・セッションをサポートできるように maxnummp パラメーターの値を増やしたい場合は、サーバー管理者に連絡してください。

例

オプション・ファイル
VMMAXP 10

コマンド・ライン
dsmc backup vm -vmmaxp=10

関連資料

153 ページの『Backup VM』

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

177 ページの『Domain.vmfull』

domain.vmfull オプションは、仮想マシンのフル・イメージ・バックアップ操作に組み込む仮想マシン (VM) を指定します。

237 ページの『バックアップ操作の最適化』

仮想マシン (VM) のバックアップ操作を最適化するためには、vmmaxparallel オプションの設定を調整します。このオプションを使用すると、Hyper-V ホストに悪影響を及ぼすことなくバックアップ操作を最適化することができます。

Vmmaxpersnapshot

vmmaxpersnapshot オプションは、Hyper-V スナップショットに組み込む仮想マシン (VM) の最大数を指定するために使用します。スナップショットの VM は、IBM Spectrum Protect サーバーにバックアップされます。

スナップショットの VM の数を増やすことで、バックアップ操作で取られるスナップショットの数を減らすことができます。この機能は、クラスター共有ボリューム (CSV) のクラスター・バックアップ操作時に発生する可能性がある、スケジュールの競合を減らします。

より多くの VM を持つスナップショットは、完了までに時間がかかり、システムの負荷を増やします。VM の数が増えるほどスナップショットの継続期間が長くなることを意味し、それによってパフォーマンスへの影響が生じる可能性があります。

このオプションは、Windows Server 2012 および Windows Server 2012 R2 オペレーティング・システムでの Hyper-V バックアップ操作でのみ有効です。

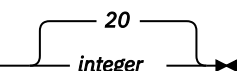
サポートされるクライアント

このオプションは、サポートされるすべての Windows クライアントに有効です。このオプションはサーバーでも定義できます。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) または **Backup VM** コマンドのコマンド・ラインで有効です。サーバー上でクライアント・オプション・セットに組み込むこともできます。プリファレンス・エディターには設定できません。

構文

➡ VMMAXPERSnapshot 

パラメーター

integer

Hyper-V スナップショットに含めることができる VM の最大数を指定します。デフォルトは 20 です。最大値は 100 です。最小値は 1 です。

VM のいくつかがローカル・ボリューム上にあり、いくつかがクラスター共有ボリューム (CSV) 上にある場合、スナップショットの VM 数は vmmxpersnapshot 設定より少なくなる可能性があります。スナップショットに含める VM に関して、ローカル・ボリュームの VM と CSV ボリュームの VM を混在させることはできません。

VM が複数の異なるボリューム上にある場合、ボリュームにまたがるスナップショットの作成を避けるため、スナップショットの VM の数は最大数より少なくなることがあります。例えば、ボリューム A に 4 つの VM があり、ボリューム B に 1 つの VM があるとします。最大数の設定が 5 であっても、スナップショットが取られるのは (ボリューム A の) 4 つの VM のみです。2 番目のスナップショットはボリューム B 用に取られます。

例

オプション・ファイル

```
vmmxpersnapshot 10
```

コマンド・ライン

```
dsmc backup vm -vmmxpers=10
```

関連概念

[59 ページの『Windows Server 2012 および Windows Server 2012 R2 クラスターのスケジュール済み VM バックアップの調整』](#)

Data Protection for Microsoft Hyper-V バージョン 8.1.2 から、より多くの仮想マシン (VM) を、クラスター内の複数のノードにわたって並行してバックアップできるようになりました。クラスター・ノードのバックアップ操作は、リカバリー可能条件で障害が発生したスナップショットを持つボリュームでスナップショットを常に再試行します。また、スナップショット内の VM 数を調整すると、Hyper-V ホストに対するスナップショットのワークロードを減らすことができます。

関連資料

[212 ページの『vmmxpersnapshotretry』](#)

最初のスナップショットが失敗した際、リカバリー可能条件である場合に、`vmmaxsnapshotretry` オプションを使用して仮想マシン (VM) のスナップショット 操作を再試行する最大回数を指定します。

vmmaxrestoreparalleldisks

単一の仮想マシン (VM) で複数の仮想ディスクを同時にリストアするには、`vmmaxrestoreparalleldisks` オプションを指定します。

オープンするディスク・セッションの数を最大 10 個指定できます。ディスク・リストア・セッションの最大数は `vmmaxrestoresessions` オプションによって指定されます。使用可能なセッションは、`vmmaxrestoreparalleldisks` オプションによって指定されたディスク・セッション数の間で割り振られ、ディスク当たりのセッション数は直近の整数に切り下げられます。

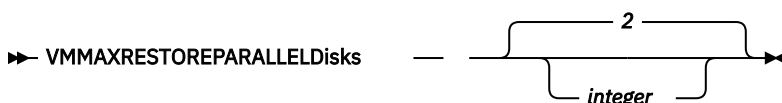
サポートされるクライアント

このオプションは、サポートされる Windows クライアントで使用可能です。

オプション・ファイル

このオプションは、データ・ムーバー・オプション・ファイル (`dsm.hostname_HV_DM.opt`) またはコマンド・ラインの **restore vm** コマンドで有効になります。また、IBM Spectrum Protect サーバー のクライアント・オプション・セットに組み込むこともできます。

構文



パラメーター

integer

同時にリストアできる仮想ハード・ディスクの数を指定します。デフォルトは 2 です。最大値は 10 です。

例

タスク

VM **vm1** のリストア操作における仮想ディスクに対し、同時リストア操作する数を最大 10 に設定します。

```
dsmc restore vm vm1 -vmmaxrestoreparalleldisks=10 -vmmaxrestoresessions=20
```

このコマンドにより、仮想ディスク当たり 2 つの同時リストア・セッションが割り当てられます。

関連資料

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

[206 ページの『Vmmaxrestoreparallelvms』](#)

`vmmaxrestoreparallelvms` オプションは、同時にリストアできる仮想マシンの数を制御します。

[210 ページの『Vmmaxrestoresessions』](#)

`vmmaxrestoresessions` オプションは、仮想マシン (VM) の最適化されたリストア操作に組み込むことができる IBM Spectrum Protect サーバー セッションの最大数を定義します。

[239 ページの『リストア操作の最適化』](#)

仮想マシン (VM) リストア操作を最適化するためには、`vmmaxrestoresessions`、`vmmaxrestoreparallelvms`、および `vmmaxrestoreparalleldisks` の各オプションの設定を調整します。これらのオプションを使用すると、Hyper-V ホスト上のリソースのバランスを取りながらリストア操作を最適化することができます。

Vmmaxrestoreparallelvms

`vmmaxrestoreparallelvms` オプションは、同時にリストアできる仮想マシンの数を制御します。

このオプションは、並行してリストアする VM の数を増やして、リストア操作のパフォーマンスを向上させるために使用します。

同時にリストアする VM の数として最大 10 を指定できます。デフォルト値は 2 です。

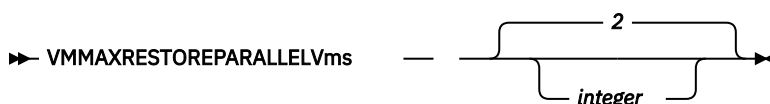
サポートされるクライアント

このオプションは、サポートされる Windows クライアントで使用可能です。

オプション・ファイル

このオプションは、データ・ムーバー・オプション・ファイル (`dsm.opt`) または **restore vm** コマンドのコマンド・ラインで有効です。サーバー上でクライアント・オプション・セットに組み込むこともできます。

構文



パラメーター

integer

同時にリストアできる VM の最大数を指定します。デフォルトは 2 です。最大値は 10 です。

リストア・セッションの数を制限するために `vmmaxrestoresessions` オプションを使用する場合、そのセッション数は VM の数以上でなければなりません。この設定により、VM ごとに少なくとも 1 つのセッションが使用可能であることが保証されます。

同時に複数の仮想ディスクをリストアするために、`vmmaxparalleldisks` オプションを使用する場合、その仮想ディスクの数はセッションの数以下でなければなりません。

例

タスク

VM の VM1、VM2、VM3、VM4、および VM5 に関して最大 5 つの仮想マシンの同時リストアを設定します。

```
dsmc restore vm vm=VM1,VM2,VM3,VM4,VM5 -VMMAXRESTOREPARALLELVms=5  
-VMMAXRESTORESsessions=10 -VMMAXRESTOREPARALLELDisks=2  
-asnode=kingston23_HV_TGT -optfile=dsm.KINGSTON23_HV_DM.opt -replace=yes
```

このコマンドは、最大 5 つの並列 VM リストア操作を割り当てます。各 VM は一度に 1 つまでの仮想ディスクを並列でリストアすることが可能で、ディスクごとに 2 つのリストア・セッションを割り当てることができます。

コマンド出力:

```
IBM Spectrum Protect  
Command Line Backup-Archive Client Interface  
Client Version 8, Release 1, Level 7.4  
Client date/time: 10/05/2018 15:01:01
```


(c) Copyright by IBM Corporation and other(s) 1990, 2019. All Rights Reserved.

Node Name: KINGSTON23_HV_DM
Session established with server ASANA2: Linux/x86_64
Server Version 7, Release 1, Level 9.000
Server date/time: 10/05/2018 14:59:09 Last access: 10/05/2018 14:58:18

Accessing as node: KINGSTON23_HV_TGT
Restore function invoked.

Restore VM command started. Total number of virtual machines to process: 5

Restore of Virtual Machine 'VM1' started

Restore of Virtual Machine 'VM2' started

Restore of Virtual Machine 'VM3' started

Restore of Virtual Machine 'VM4' started

Restore of Virtual Machine 'VM5' started

Starting Full VM restore of 'Hyper-V' Virtual Machine 'VM1' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring VM configuration information for 'VM1'
Restoring virtual disks for virtual machine 'VM1'
Total disks to restore : 1
Disks to restore concurrently : 1
Maximum Sessions per disk : 2

Using 2 session(s) to restore virtual machine 'VM1' Disk 1 .
Restoring 'VM1' Hard Disk 1
Type : IFINCR
Timestamp : 10/05/2018 14:59:23
Bytes to restore : 1,073,741,824

< 670.25 MB> [-]
Starting Full VM restore of 'Hyper-V' Virtual Machine 'VM2' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring VM configuration information for 'VM2'
Restoring 1,073,741,824 'VM1' e:\Hyper-V\VM1\Virtual Machines\1G.vhdx [Done]
Restoring virtual disks for virtual machine 'VM2'
Total disks to restore : 1
Disks to restore concurrently : 1
Maximum Sessions per disk : 2

Using 2 session(s) to restore virtual machine 'VM2' Disk 1 .
Restoring 'VM2' Hard Disk 1
Type : IFFULL
Timestamp : 10/05/2018 14:59:24
Bytes to restore : 1,073,741,824

Restoring 0 VM1 [Done]

< 1.69 GB> [-]
Starting Full VM restore of 'Hyper-V' Virtual Machine 'VM3' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring VM configuration information for 'VM3'
Successful Full VM restore of Virtual Machine 'VM1'

Restore processing finished.

Successful Full VM restore of 'Hyper-V' Virtual Machine 'VM1' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

```

Starting Full VM restore of 'Hyper-V' Virtual Machine 'VM4' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring 1,073,741,824 'VM2' e:\Hyper-V\VM2\Virtual Hard Disks\1G.vhdx [Done]
Restoring VM configuration information for 'VM4'
Restoring virtual disks for virtual machine 'VM3'
    Total disks to restore      : 1
    Disks to restore concurrently : 1
    Maximum Sessions per disk   : 2

Using 2 session(s) to restore virtual machine 'VM3' Disk 1 .
Restoring 'VM3' Hard Disk 1
    Type      : IFFULL
    Timestamp : 10/05/2018 14:59:27
    Bytes to restore : 1,073,741,824

Restoring virtual disks for virtual machine 'VM4'
    Total disks to restore      : 1
    Disks to restore concurrently : 1
    Maximum Sessions per disk   : 2

Restoring          0      VM2 [Done]
Using 2 session(s) to restore virtual machine 'VM4' Disk 1 .
Restoring 'VM4' Hard Disk 1
    Type      : IFFULL
    Timestamp : 10/05/2018 14:59:32
    Bytes to restore : 1,073,741,824

Successful Full VM restore of Virtual Machine 'VM2'

Restore processing finished.

Successful Full VM restore of 'Hyper-V' Virtual Machine 'VM2' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Starting Full VM restore of 'Hyper-V' Virtual Machine 'VM5' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring VM configuration information for 'VM5'
Restoring 1,073,741,824 'VM3' e:\Hyper-V\VM3\Virtual Hard Disks\1G.vhdx [Done]
Restoring virtual disks for virtual machine 'VM5'
    Total disks to restore      : 1
    Disks to restore concurrently : 1
    Maximum Sessions per disk   : 2

Using 2 session(s) to restore virtual machine 'VM5' Disk 1 .
Restoring 'VM5' Hard Disk 1
    Type      : IFFULL
    Timestamp : 10/05/2018 14:59:51
    Bytes to restore : 1,073,741,824

Restoring 1,073,741,824 'VM4' e:\Hyper-V\VM4\Virtual Hard Disks\1G.vhdx [Done]
Restoring          0      VM3 [Done]
Restoring          0      VM4 [Done]
Successful Full VM restore of Virtual Machine 'VM3'

Restore processing finished.

Successful Full VM restore of 'Hyper-V' Virtual Machine 'VM3' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Successful Full VM restore of Virtual Machine 'VM4'

Restore processing finished.
Restoring 1,073,741,824 'VM5' e:\Hyper-V\VM5\Virtual Hard Disks\1G.vhdx [Done]

Successful Full VM restore of 'Hyper-V' Virtual Machine 'VM4' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring          0      VM5 [Done]
Successful Full VM restore of Virtual Machine 'VM5'

Restore processing finished.

Successful Full VM restore of 'Hyper-V' Virtual Machine 'VM5' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

```

```

Total number of objects restored:          5
Total number of objects failed:           0
Total number of bytes transferred:        5.00 GB
Data transfer time:                       66.95 sec
Network data transfer rate:               78,307.54 KB/sec
Aggregate data transfer rate:             72,000.19 KB/sec
Elapsed processing time:                   00:01:12

```

タスク

VM1 および VM2 の VM に対して最大 2 つの同時 VM リストア操作を設定します。

```

dsmc restore vm vm=VM1,VM2 -VMMAXRESTOREPARALLELVms=2
-VMMAXRESTORESessions=10 -VMMAXRESTOREPARALLELDisks=1
-asnode=kingston23_HV_TGT -optfile=dsm.KINGSTON23_HV_DM.opt
-replace=yes

```

このコマンドは、VM に 1 つのディスクしか含まれていないと仮定して、VM ごとにディスク当たり 4 つのセッションがある 2 つの同時 VM リストア操作を割り当てます。

ヒント: -VMMAXRESTORESessions=50 を設定しても、VM にはディスクが 1 つしか含まれていないため、ディスクごとに 4 つのセッションしか存在しません。

コマンド出力:

```

IBM Spectrum Protect
Command Line Backup-Archive Client Interface
  Client Version 8, Release 1, Level 7.4
  Client date/time: 10/05/2018 15:21:36
(c) Copyright by IBM Corporation and other(s) 1990, 2019. All Rights Reserved.

Node Name: KINGSTON23_HV_DM
Session established with server ASANA2: Linux/x86_64
  Server Version 7, Release 1, Level 9.000
  Server date/time: 10/05/2018 15:19:44  Last access: 10/05/2018 15:00:10

Accessing as node: KINGSTON23_HV_TGT
Restore function invoked.

Restore VM command started.  Total number of virtual machines to process: 2

Restore of Virtual Machine 'VM1' started

Restore of Virtual Machine 'VM2' started

Starting Full VM restore of 'Hyper-V' Virtual Machine 'VM1' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring VM configuration information for 'VM1'
Restoring virtual disks for virtual machine 'VM1'
  Total disks to restore          : 1
  Disks to restore concurrently   : 1
  Maximum Sessions per disk      : 4

Using 4 session(s) to restore virtual machine 'VM1' Disk 1 .
Restoring 'VM1' Hard Disk 1
  Type          : IFINCR
  Timestamp     : 10/05/2018 14:59:23
  Bytes to restore : 1,073,741,824

< 909.25 MB> [ - ]
Starting Full VM restore of 'Hyper-V' Virtual Machine 'VM2' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring VM configuration information for 'VM2'
Restoring 1,073,741,824 'VM1' e:\Hyper-V\VM1\Virtual Machines\1G.vhdx [Done]
Restoring virtual disks for virtual machine 'VM2'
  Total disks to restore          : 1
  Disks to restore concurrently   : 1
  Maximum Sessions per disk      : 4

```

```

Using 4 session(s) to restore virtual machine 'VM2' Disk 1 .
Restoring 'VM2' Hard Disk 1
  Type           : IFFULL
  Timestamp      : 10/05/2018 14:59:24
  Bytes to restore : 1,073,741,824

Restoring          0    VM1 [Done]
Successful Full VM restore of Virtual Machine 'VM1'

Restore processing finished.

Successful Full VM restore of 'Hyper-V' Virtual Machine 'VM1' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Restoring 1,073,741,824 'VM2' e:¥Hyper-V¥VM2¥Virtual Hard Disks¥1G.vhdx [Done]
Restoring          0    VM2 [Done]
Successful Full VM restore of Virtual Machine 'VM2'

Restore processing finished.

Successful Full VM restore of 'Hyper-V' Virtual Machine 'VM2' target node
name='KINGSTON23_HV_TGT', data mover node name='KINGSTON23_HV_DM'

Total number of objects restored:          2
Total number of objects failed:           0
Total number of bytes transferred:        2.00 GB
Data transfer time:                      30.08 sec
Network data transfer rate:              69,703.69 KB/sec
Aggregate data transfer rate:            45,697.11 KB/sec
Elapsed processing time:                  00:00:45

```

関連タスク

[241 ページの『複数の仮想マシンの並列リストア \(最適化されたリストア\)』](#)

並列リストア処理では、複数の仮想マシン (VM) を同時にリストアすることができ、VM リストア操作のパフォーマンスを最適化できます。

関連資料

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

[210 ページの『Vmmxrestoresessions』](#)

vmmxrestoresessions オプションは、仮想マシン (VM) の最適化されたリストア操作に組み込むことができる IBM Spectrum Protect サーバー セッションの最大数を定義します。

[205 ページの『vmmxrestoreparalleldisks』](#)

単一の仮想マシン (VM) で複数の仮想ディスクを同時にリストアするには、vmmxrestoreparalleldisks オプションを指定します。

[239 ページの『リストア操作の最適化』](#)

仮想マシン (VM) リストア操作を最適化するためには、vmmxrestoresessions、vmmxrestoreparallelvms、および vmmxrestoreparalleldisks の各オプションの設定を調整します。これらのオプションを使用すると、Hyper-V ホスト上のリソースのバランスを取りながらリストア操作を最適化することができます。

Vmmxrestoresessions

vmmxrestoresessions オプションは、仮想マシン (VM) の最適化されたリストア操作に組み込むことができる IBM Spectrum Protect サーバー セッションの最大数を定義します。

最適化されたリストア操作とは、仮想ディスクのサブディスク・レベルでの並列リストア機能が有効にされたリストア操作です。

リストアされているディスクごとに 1 つ以上のセッションが割り振られる必要があります。

vmmaxrestoresessions の値が、vmmaxrestoreparalleldisks の値と vmmaxrestoreparallelvms の値を乗算した数より小さい場合、実行時に vmmaxrestoreparalleldisks の値と vmmaxrestoreparallelvms の値を乗算した数に自動的に調整されます。

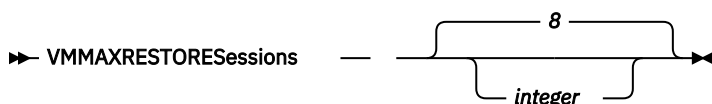
サポートされるクライアント

このオプションは、サポートされる Windows クライアントで使用可能です。

オプション・ファイル

このオプションは、データ・ムーバー・オプション・ファイル (dsm.hostname_HV_DM.opt) またはコマンド・ラインの **restore vm** コマンドで有効になります。また、IBM Spectrum Protect サーバー のクライアント・オプション・セットに組み込むこともできます。

構文



パラメーター

integer

リストア操作中に作成される IBM Spectrum Protect サーバー セッションの数を指定します。デフォルトは 8 です。最大値は 100 です。

例

オプション・ファイル

VM_MAXRESTORES 10

コマンド・ライン:

dsmc restore vm -VM_MAXRESTORES=10

関連タスク

[241 ページの『複数の仮想マシンの並列リストア \(最適化されたリストア\)』](#)

並列リストア処理では、複数の仮想マシン (VM) を同時にリストアすることができ、VM リストア操作のパフォーマンスを最適化できます。

関連資料

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

[205 ページの『vmmaxrestoreparalleldisks』](#)

単一の仮想マシン (VM) で複数の仮想ディスクを同時にリストアするには、vmmaxrestoreparalleldisks オプションを指定します。

[206 ページの『Vmmaxrestoreparallelvms』](#)

vmmaxrestoreparallelvms オプションは、同時にリストアできる仮想マシンの数を制御します。

[239 ページの『リストア操作の最適化』](#)

仮想マシン (VM) リストア操作を最適化するためには、vmmaxrestoresessions、vmmaxrestoreparallelvms、および vmmaxrestoreparalleldisks の各オプションの設定を調整します。これらのオプションを使用すると、Hyper-V ホスト上のリソースのバランスを取りながらリストア操作を最適化することができます。

vmmaxsnapshotretry

最初のスナップショットが失敗した際、リカバリー可能条件である場合に、vmmaxsnapshotretry オプションを使用して仮想マシン (VM) のスナップショット操作を再試行する最大回数を指定します。

VM のバックアップ中に一時的な条件が原因で VM のスナップショットが失敗した場合、Data Protection for Microsoft Hyper-V は自動的に、vmmaxsnapshotretry オプションによって指定された回数までスナップショット操作を再試行します。最大再試行回数に達した後、さらにスナップショットが失敗した場合、VM のスナップショット操作は再試行されず、バックアップ試行は失敗となります。

例えば、同じボリュームにある VM のバックアップに対してほぼ同時に 2 つのバックアップ要求が開始されたことによって、リカバリー可能条件が生じる場合があります。バックアップ操作では、同じ VM に対して別のバックアップが実行されている間、バックアップを開始できないためにスナップショットが失敗したという報告が行われます。この場合、Data Protection for Microsoft Hyper-V は最初の VM バックアップが完了した後にスナップショット操作を再試行します。

最初のエラーがリカバリー可能でない場合、スナップショットは試行されません。例えば、最初のスナップショット・プロセス中に Volume Shadow Copy Services (VSS) ライターでエラーが発生すると、バックアップ処理は停止し、Data Protection for Microsoft Hyper-V はスナップショット操作を再試行しません。

このオプションは、Windows Server 2012 および Windows Server 2012 R2 オペレーティング・システムでの Hyper-V バックアップ操作でのみ有効です。

サポートされるクライアント

このオプションは、サポートされるすべての Windows クライアントに有効です。このオプションはサーバーでも定義できます。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) または **Backup VM** コマンドのコマンド・ラインで有効です。サーバー上でクライアント・オプション・セットに組み込むこともできます。プリファレンス・エディターには設定できません。

構文

➡ VMMAXSNAPSHOTretry 

パラメーター

integer

最初のスナップショット試行がリカバリー可能条件で失敗した場合に、VM のスナップショット操作を再試行する最大回数を指定します。デフォルトは 20 です。最大値は 30 です。最小値は 1 です。

例えば、vmmaxsnapshotretry 操作を 12 に設定すると、VM バックアップ操作中に最初のスナップショットが失敗した後、Data Protection for Microsoft Hyper-V はスナップショット操作を最大 12 回再試行します。再試行が 12 回に達した後もスナップショットが失敗した場合、それ以上は再試行されず、バックアップ試行は失敗となります。

次のスナップショット再試行は、必ず 10 分以上経過した後に行われます。失敗した VM が現在バックアップ中の VM を含むスナップショットに含まれている場合、試行間隔の時間は長くなります。他の VM のバックアップ操作が完了し、スナップショットがバックアップ操作によって除去されてからでないと、再試行を実行できません。

例

オプション・ファイル

vmmaxsna 12

コマンド・ライン

```
dsmc backup vm -vmmaxsna=12
```

関連概念

59 ページの『Windows Server 2012 および Windows Server 2012 R2 クラスターのスケジュール済み VM バックアップの調整』

Data Protection for Microsoft Hyper-V バージョン 8.1.2 から、より多くの仮想マシン (VM) を、クラスター内の複数のノードにわたって並行してバックアップできるようになりました。クラスター・ノードのバックアップ操作は、リカバリー可能条件で障害が発生したスナップショットを持つボリュームでスナップショットを常に再試行します。また、スナップショット内の VM 数を調整すると、Hyper-V ホストに対するスナップショットのワークロードを減らすことができます。

関連資料

203 ページの『Vmmaxpersnapshot』

vmmaxpersnapshot オプションは、Hyper-V スナップショットに組み込む 仮想マシン (VM) の最大数を指定するために使用します。スナップショットの VM は、IBM Spectrum Protect サーバーにバックアップされます。

Vmmaxvirtualdisks

vmmaxvirtualdisks オプションは、バックアップ操作に含める Hyper-V 仮想マシン・ディスク (VHDX) の最大サイズを指定します。

vmmaxvirtualdisks オプションと vmskipmaxvirtualdisks オプションを一緒に使用して、データ・ムーバーがバックアップ操作時に大容量の仮想マシン (VM) ディスクを処理する方法を指定します。

- vmmaxvirtualdisks オプションを設定して、組み込む VM ディスクの最大サイズを指定します。
- vmskipmaxvirtualdisks オプションを設定して、最大サイズを超えていない VM ディスクをバックアップします (このサイズを超える VM ディスクは除外されます)。設定しない場合、操作は失敗します。

サポートされるクライアント

このオプションは、Hyper-V 仮想マシンをバックアップするデータ・ムーバーとして稼働する、サポート対象の Windows クライアントに有効です。

オプション・ファイル

クライアント・オプション・ファイル (dsm.opt) で vmmaxvirtualdisks オプションを設定します。このオプションは、コマンド・ライン・パラメーターとして **backup vm** コマンドにも指定できます。

構文



パラメーター

size

バックアップ操作に組み込む VM ディスクの最大サイズをテラバイト (TB) 単位で指定します。この範囲は 2 から 8 の整数 (デフォルトは 2) です。最大は 8 TB (8192 GB に相当) です。

バックアップ操作に組み込まれる VM ディスク・サイズが常に最大サイズであるようにするには、999 を指定します。常に最大値が設定されるようにするには、この値を使用することが最も効率的な方法です。この値を使用すると、オプション・ファイルを何度も変更する必要がなくなります。

vmskipmaxvirtualdisks yes オプションも指定した場合、指定された最大サイズ以下の VM ディスクはバックアップされ、指定された最大サイズより大きい VM ディスクは除外されます。

`vmskipmaxvirtualdisks no` オプションも指定すると、指定された最大サイズより VM ディスクが大きい場合はバックアップ操作が失敗します。

例

オプション・ファイル:

`vmmaxvirtualdisks 3`

コマンド・ライン:

5 TB 以下の VM ディスクをバックアップし、5 TB より大きい VM ディスクを除外するには、次のようになります。

```
backup vm VM1 -vmmaxvirtualdisks=5 -mskipmaxvirtualdisks=yes
```

3 TB 以下の VM ディスクをバックアップし、VM ディスクが 3 TB より大きい場合はバックアップ操作が失敗するようにするには、次のようになります。

```
backup vm VM1 -vmmaxvirtualdisks=3 -mskipmaxvirtualdisks=no
```

8 TB 以下の VM ディスクをバックアップし、8 TB より大きい VM ディスクを除外するには、次のようになります。

```
backup vm VM1 -vmmaxvirtualdisks=8 -mskipmaxvirtualdisks=yes
```

または、

```
backup vm VM1 -vmmaxvirtualdisks=999 -mskipmaxvirtualdisks=yes
```

Vmmc

`vmmc` オプションは、デフォルト管理クラス以外の管理クラスを使用して仮想マシン・バックアップを保管するために使用します。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (`dsm.opt`) に入れるか、コマンド・ラインに指定してください。

構文

➡ **VMMC** — *management_class_name* ➡

パラメーター

management_class_name

バックアップされた仮想マシン・データに適用する管理クラスを指定します。このオプションを設定しない場合、ノードのデフォルト管理クラスが使用されます。

例

タスク:

`myVirtualMachine` という名前の仮想マシンのバックアップを実行し、`myManagmentClass` という名前の管理クラスに従ってバックアップを保存します。

```
dsmc backup vm "myVirtualMachine" -vmmc=myManagmentClass
```

Vmprocessvmwithphysdisks

vmprocessvmwithphysdisks オプションを使用して、VM に 1 つ以上の物理ディスク (パススルー・ディスク) がプロビジョニングされている場合に Hyper-V RCT 仮想マシン (VM) バックアップを処理するかどうかを制御します。

VM は、Hyper-V サーバーに直接接続される物理ディスクのストレージにアクセスできます。この物理ディスクはパススルー・ディスクと呼ばれます。

このオプションを yes に設定すると、物理ディスクのデータはバックアップ操作から除外されますが、その物理ディスクの構成情報は VM バックアップで保存されます。リストア操作時に、vmskipphysdisks no オプションを設定して、物理ディスク構成をリストアできます。元の物理ディスクは、使用可能である場合、リストアされた VM に再接続されます。

このオプションは、Windows Server 2016 での RCT バックアップにのみ有効です。このオプションは、Windows Server 2012 または Windows Server 2012 R2 の Hyper-V VSS バックアップには適用されません。

サポートされるクライアント

このオプションが有効なのは、Windows Server 2016 以降のオペレーティング・システムのクライアントでのみ有効です。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) に入れるか、**backup vm** コマンドのコマンド・ライン・パラメーターとして指定してください。

構文



パラメーター

No

VM のバックアップ操作は、1 つ以上の物理ディスクが検出された場合に失敗します。この値がデフォルトです。

Yes

1 つ以上の物理ディスクを含む VM がバックアップされます。このオプションは、物理ディスク上のデータをバックアップせずに物理ディスク構成をバックアップします。

例

オプション・ファイル:

```
VMPROCESSVMWITHPHYSDISKS Yes
```

コマンド・ライン:

```
dsmc backup vm vmlocal-vmprocessvmwithphysd=yes
```

関連資料

217 ページの『Vmskipphysdisks』

物理ディスクのボリュームに関連付けられている論理装置番号 (LUN) が使用可能な場合、`vmskipphysdisks` オプションを使用して、Hyper-V 仮想マシン (VM) に関連付けられている物理ディスク (パススルー・ディスク) の構成情報をリストアします。

Vmskipmaxvirtualdisks

`vmskipmaxvirtualdisks` オプションは、バックアップ操作で最大ディスク・サイズを越えている仮想マシン (VM) ディスクを処理する方法を指定します。

`vmskipmaxvirtualdisks` オプションと `vmmaxvirtualdisks` オプションを一緒に使用して、データ・ムーバーがバックアップ操作時に大容量の VM ディスクを処理する方法を指定します。

- `vmskipmaxvirtualdisks` オプションを設定して、最大サイズを超えていない VM ディスクをバックアップします (このサイズを超える VM ディスクは除外されます)。設定しない場合、操作は失敗します。
- `vmmaxvirtualdisks` オプションを設定して、組み込む VM ディスクの最大サイズを指定します。

サポートされるクライアント

このオプションは、Hyper-V 仮想マシンをバックアップするデータ・ムーバーとして稼働する、すべてのサポート対象の Windows クライアントに有効です。

オプション・ファイル

クライアント・オプション・ファイル (`dsm.opt`) で `vmskipmaxvirtualdisks` オプションを設定します。このオプションは、コマンド・ライン・パラメーターとして **backup vm** コマンドにも指定できます。

構文



パラメーター

No

仮想マシンに最大サイズより大きい VM ディスクが 1 つ以上ある場合に、バックアップ操作が失敗することを指定します。この設定がデフォルト値です。

Yes

バックアップ操作に最大サイズ以下の VM ディスクを含め、最大サイズより大きい VM ディスクを除外することを指定します。

例

オプション・ファイル:

```
vmskipmaxvirtualdisks yes
```

コマンド・ライン:

VM ディスクが 2 TB より大きい場合にバックアップ操作が失敗するようにするには、次のようにします。

```
backup vm VM1 -vmskipmaxvirtualdisks=no
```

VM ディスクが 5 TB より大きい場合にバックアップ操作が失敗するようにするには、次のようにします。

```
backup vm VM1 -vmskipmaxvirtualdisks=no -vmmaxvirtualdisks=5
```

8 TB 以下の VM ディスクをバックアップし、8 TB より大きい VM ディスクを除外するには、次のようにします。

```
backup vm VM1 -vmskipvirtualdisks=yes -vmmaxvirtualdisks=8
```

Vmskipphysdisks

物理ディスクのボリュームに関連付けられている論理装置番号 (LUN) が使用可能な場合、**vmskipphysdisks** オプションを使用して、Hyper-V 仮想マシン (VM) に関連付けられている物理ディスク (パススルー・ディスク) の構成情報をリストアします。

物理ディスクは VM スナップショットに含まれていないため、構成情報のみをリストアすることができ、ボリューム上にあったデータはリストアできません。

このオプションは、Windows Server 2016 での Hyper-V VM のリストアでのみ有効です。このオプションは、Windows Server 2012 または Windows Server 2012 R2 の Hyper-V ホストには適用されません。

サポートされるクライアント

このオプションが有効なのは、Windows Server 2016 以降のオペレーティング・システムのクライアントでのみ有効です。

オプション・ファイル

このオプションは、クライアント・オプション・ファイル (dsm.opt) に入れるか、**restore vm** コマンドのコマンド・ライン・パラメーターとして指定してください。

構文



パラメーター

NO

元の物理ディスクが使用可能な場合、この値を指定して **vmprocessvmwithphysdisks yes** オプションを指定してバックアップされた物理ディスク構成情報をリストアします。元の物理ディスクは、リストアされた VM に再接続されます。元の物理ディスクが見つからなかった場合、リストア・オプションは失敗します。この値がデフォルトです。

YES

vmprocessvmwithphysdisks yes オプションを使用してバックアップされた VM をリストアする必要があり、元の物理ディスクが見つからない場合に、この値を指定します。この設定を使用すると、クライアントは物理ディスクを見つける試行をスキップし、物理ディスク構成情報をリストアしません。

例

オプション・ファイル:

```
VMSKIPPHYSDISKS YES
```

コマンド・ライン:

```
dsmc restore vm vm123 -vmskipphysd=yes
```

関連資料

[215 ページの『Vmprocessvmwithphysdisks』](#)

vmprocessvmwithphysdisks オプションを使用して、VM に 1 つ以上の物理ディスク (パススルー・ディスク) がプロビジョニングされている場合に Hyper-V RCT 仮想マシン (VM) バックアップを処理するかどうかを制御します。

Vmrestoretype

vmrestoretype オプションは、実行または照会するリストア操作のタイプを指定するために、**query VM** コマンドまたは **restore VM** コマンドで使用します。

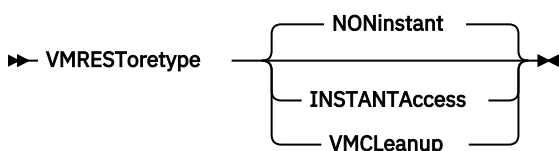
サポートされるクライアント

このオプションは、サポートされる Windows クライアントで使用可能です。

オプション・ファイル

このオプションは、**restore vm** コマンドまたは **query vm** コマンドのコマンド・ラインで指定する必要があります。このオプションをクライアント・オプション・ファイルの中で設定することはできません。

構文



パラメーター

noninstant

通常のフル VM リストア操作を実行することを指定します。これはデフォルトのリストア・タイプです。

instantaccess

VM バックアップを一時的にリストアすることを指定します。インスタント・リストアを実行する前に、一時的に VM をリストアしてバックアップの整合性をテストしたい場合は、このリストア・タイプを指定します。一時 VM に加えた変更は、どれも保存されません。

query vm コマンドでこのリストア・タイプを指定すると、コマンドは、インスタント・アクセス操作を実行している VM のリストを返します。

vmcleanup

選択した VM とそのコンポーネントのクリーンアップを実行することを指定します。

インスタント・アクセス操作では、このオプションは、一時 VM とそのすべてのコンポーネントを削除します。

例

コマンド・ライン:

Oslo という名前の VM のインスタント・アクセスを実行します。元の VM はまだ存在しています。そのため、-vmname オプションを使用して、新しい名前 Oslo_verify を割り当てます。

```
dsmc restore vm Oslo -vmrest=instantaccess -vmname=Oslo_verify
```

San_Jose という名前の仮想マシンの通常の (フル VM) リストアを実行します。

```
dsmc restore vm San_Jose
```

あるいは、通常のフル VM リストア操作を実行するために、以下のコマンドを使用することもできます。

```
dsmc restore vm San_Jose -vmrest=noninstant
```

アクティブなすべてのインスタント・アクセス・セッションを検出する照会を実行します。この照会は、インスタント・アクセス・モードで稼働しているすべての一時 VM を表示します。

```
dsmc query vm * -VMRESToretype=INSTANTAccess
```

Oslo という名前の VM およびそのすべてのコンポーネントをクリーンアップします。これらのコンポーネントには、VM 名に関連付けられている iSCSI マウント、デバイス、一時データなどがあります。

```
dsmc restore vm Oslo -vmrest=vmcleanup -vmname=Oslo_verify
```

関連タスク

[131 ページの『インスタント・アクセス操作の実行』](#)

インスタント・アクセス操作を実行して、仮想マシン (VM) バックアップの整合性を検証したり、インスタント・アクセス操作で作成されたリソースをクリーンアップしたりすることができます。

第 11 章 マウントおよびファイル・リストア

IBM Spectrum Protect リカバリー・エージェントを使用すると、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することができます。iSCSI プロトコルを使用して、ファイル・リストア操作でリモート・コンピューターからスナップショットにアクセスできます。

ヒント：Data Protection for Microsoft Hyper-V の旧バージョンでは、Recovery Agent を使用したスナップショットのマウントおよびファイルのリストアのための機能を提供していました。この機能は引き続き Recovery Agent によってサポートされますが、[85 ページの『第 5 章 ファイル・リストア操作の概要』](#)で説明されているように、IBM Spectrum Protect ファイル・リストア・インターフェースが推奨方式です。

この『マウントおよびファイル・リストア』コレクションの内容は、Recovery Agent 方式を選択するユーザー向けの参照として提供されています。

IBM Spectrum Protect リカバリー・エージェントの構成

IBM Spectrum Protect リカバリー・エージェントは、ファイル・リストアおよびディスク/ブロック・デバイスの公開を実行するためのさまざまな構成を提供します。

オフホストのファイル・リストア

これらの構成では、IBM Spectrum Protect リカバリー・エージェントを各仮想マシン・ゲストにインストールする必要はありません。代わりに、オフホストのインスタンスが複数の仮想マシンのファイル・リストアに責任を負います。この構成では、マウント・プロセスは選択されたディスク区画から仮想ボリュームを公開します。GPT ディスクの場合、区画を使用可能にするにはディスク全体を公開する必要があり、ディスクは iSCSI 接続されなければなりません。このタスクを実行するには、Recovery Agent GUI を使用します。

Recovery Agent に関連したノードを登録する必要があります。Recovery Agent ノードには、スナップショットが保管されているデータ・ノード (複数可) にアクセスするためのプロキシ権限が付与されている必要があります。スナップショットをオフホスト・サーバーにマウントすると、仮想ボリュームをネットワークで共有して、仮想マシン・ゲストへのアクセスを可能にすることができます。あるいは、任意のファイル共有方式により、マウントしたボリュームから仮想マシン・ゲストにファイルをコピーすることができます。

- ステップバイステップのリストア説明については、[225 ページの『1 つ以上のファイルをリストア』](#)を参照してください。

インゲストのファイル・リストア

これらの構成では、IBM Spectrum Protect リカバリー・エージェントを各仮想マシン・ゲストにインストールする必要があります。マウントおよびリストア・プロセスは、バックアップされたディスクからの単一区画に対して実行されます。

IBM Spectrum Protect リカバリー・エージェント ノード名には、一般に、それを実行している仮想マシンに対するアクセス権限のみが付与されます。これには、IBM Spectrum Protect バックアップ/アーカイブ・クライアントの **dsmt set access** コマンドが使用されます。一般に、リストア・プロセスは仮想マシンのゲスト・マシンにログインしたユーザーによって開始されます。

これらの構成の場合、必ず、特定の仮想マシンのゲスト・オペレーティング・システム要件と、サポートされるレベルの IBM Spectrum Protect リカバリー・エージェントを比較してください。特定のオペレーティング・システムがサポートされていない場合は、ファイル・リストアにオフホスト・ディスク/ブロック・デバイス公開の構成も使用できるかどうかを判別します。このタスクを実行するには、IBM Spectrum Protect リカバリー・エージェント GUI を使用します。

- 計画情報およびオペレーティング・システム・ベースのガイドラインについては、[221 ページの『第 11 章 マウントおよびファイル・リストア』](#)を参照してください。

- ステップバイステップのリストア手順については、[225 ページの『1 つ以上のファイルをリストア』](#)を参照してください。

オフホスト iSCSI ターゲット

この構成は、オフホスト IBM Spectrum Protect リカバリー・エージェントのインスタンスから iSCSI ターゲットを公開し、手動でインゲスト iSCSI イニシエーターを使用してディスク・スナップショットにアクセスします。この構成では、仮想マシンゲスト内に iSCSI イニシエーターをインストールする必要があります。この手法では、個々のディスク区画を公開するオフホストのファイル・リストアとは異なり、iSCSI LUN を公開します。このタスクを実行するには、IBM Spectrum Protect リカバリー・エージェント GUI を使用します。

この構成では、アクセスされる iSCSI デバイスがあるシステムの仮想マシンゲスト iSCSI イニシエーター名をユーザーが指定します。ディスク・スナップショットがマウントされた後、仮想マシンゲスト内の iSCSI イニシエーターを使用することにより、スナップショットを検出し、それにログインすることができます。

GUID パーティション・テーブル (GPT) ディスクを含んでいる仮想マシンをバックアップする場合、しかもボリュームを GPT ディスクにマウントしたい場合は、以下の手順を実行します。

1. GPT ディスクを iSCSI ターゲットとしてマウントします。
 2. Microsoft iSCSI イニシエーターを使用して、ターゲットにログオンします。
 3. Windows ディスク管理を開き、ディスクを検索してオンラインにします。その後、GPT ディスク内のボリュームを表示できます。
- 計画情報およびオペレーティング・システム・ベースのガイドラインについては、[221 ページの『第 11 章 マウントおよびファイル・リストア』](#)を参照してください。
 - ステップバイステップのリストア説明については、[225 ページの『1 つ以上のファイルをリストア』](#)を参照してください。

スナップショットのマウントの概要

IBM Spectrum Protect リカバリー・エージェントを使用すれば、スナップショットをマウントし、このスナップショットを使用してデータ・リカバリーを完了させることができます。

IBM Spectrum Protect リカバリー・エージェント GUI を使用してスナップショットをマウントします。Recovery Agent は、LAN を介して IBM Spectrum Protect サーバーに接続されているシステムにインストールして実行する必要があります。LAN フリー・パスでは、Recovery Agent コンポーネントの操作を使用できません。

マウント操作を実行する場合、以下の状態に注意してください。

- IBM Spectrum Protect リカバリー・エージェントがゲスト・マシン上にインストールされている場合、そのゲスト・マシンがバックアップ中のときは、いかなるファイル・システムまたはディスクに対しても、マウント操作を開始することはできません。バックアップが完了するまで待つか、マウント操作を実行する前にバックアップを取り消す必要があります。ロック機構は仮想マシン全体を対象にしているので、これらの操作は許可されません。
- スナップショット・バックアップ・インベントリを参照すると、仮想マシンのオペレーティング・システム・バージョンは、仮想マシンが最初に作成されたときに指定されたバージョンになっています。そのため、Recovery Agent が現行のオペレーティング・システムを反映しない場合があります。
- ネットワーク障害によりマウント操作が中断されると、ボリュームは不安定になります。メッセージがイベント・ログに発行されます。ネットワーク接続が再確立されると、別のメッセージがイベント・ログに発行されます。これらのメッセージは Recovery Agent GUI には発行されません。

最大 20 の iSCSI セッションがサポートされます。同じスナップショットを複数回にわたってマウントすることができます。Recovery Agent の複数インスタンスを使用して同じテープ・ストレージ・プールからスナップショットをマウントすると、以下のいずれかのアクションが行われます。

- 2 番目の Recovery Agent インスタンスは、最初のインスタンスが完了するまでブロックされる。

- 2 番目の Recovery Agent インスタンスは、最初のインスタンスのアクティビティを中断することがある。例えば、2 番目のインスタンスが、最初のインスタンスでのファイル・コピー処理を中断する可能性があります。
 - Recovery Agent は、同時に複数のサーバーまたはノードに接続できません。
- そのため、同じテープ・ボリューム上での Recovery Agent の並行セッションは避けてください。

マウントのガイドライン

スナップショットは読み取り専用モードまたは読み取り/書き込みモードでマウントできます。読み取り/書き込みモードでは、Recovery Agent は、データに加えた変更をメモリーに保存します。サービスが再始動されると、変更は失われます。

Recovery Agent は、以下の 2 つのうちのいずれかのモードで稼働します。

ユーザーがログインしていない

Recovery Agent はサービスとして稼働します。

ユーザーがログインしている

ユーザーが Recovery Agent を開始して GUI を使用するまで、Recovery Agent はサービスとして稼働し続けます。Recovery Agent および GUI を閉じると、サービスが再始動します。Recovery Agent とグラフィカル・ユーザー・インターフェースは、管理者のログイン資格情報で実行されている場合にのみ使用できます。アクティブになれるのは、常に Recovery Agent の 1 つのコピーのみです。

マウントされたボリュームが存在している場合に、「スタート」メニューから Mount を始動すると、次のメッセージが表示されます。

現在、一部のスナップショットがマウントされています。続行すると、これらのスナップショットがマウント解除されます。マウントされたボリュームがアプリケーションで現在使用されている場合は、そのアプリケーションが不安定になる可能性があることに注意してください。続行しますか？

「Yes」をクリックすると、マウントされたボリュームが使用中であってもアンマウントされます。

制約事項: スナップショットを iSCSI ターゲットとして公開していて、ダイナミック・ディスクのスナップショットがその元のシステムに対して表示されると、UUID が重複することになります。同様に、GPT ディスクのスナップショットがその元のシステムに対して表示されると、GUID が重複することになります。この重複を避けるため、動的ディスクと GPT ディスクを、その元のシステム以外のシステムに対して公開してください。例えば、元のディスクが存在しなくなっている場合を除き、これらのディスク・タイプをプロキシ・システムに対して公開します。

ファイル・リストアの概要

IBM Spectrum Protect リカバリー・エージェントを使用して、ファイル・レベル・リストア操作を効率的に実施し、仮想ボリュームにスナップショットをマウントすることでダウン時間を最小限に抑えることができます。

IBM Spectrum Protect リカバリー・エージェントは、以下のタスクに使用できます。

- 失われたファイルまたは損傷したファイルのバックアップからのリカバリー
- 仮想マシンのゲスト・ボリュームのマウントと仮想マシンのゲスト・ファイルのアーカイブの作成
- バッチ・レポート用データベース・アプリケーションのマウント

仮想ボリュームは、Windows エクスプローラなどの任意のファイル・マネージャーを使用して表示できます。スナップショット内のディレクトリーとファイルは、他のファイルと同じように表示および管理できます。ファイルを編集して変更を保存しても、変更されたデータはメモリーには保存されますがディスクには保存されないため、ボリュームのアンマウントを行うとその変更は失われます。変更はメモリーに書き込まれるため、読み取り/書き込みモードで動作している場合、IBM Spectrum Protect リカバリー・エージェントで大量の RAM が使用されることがあります。

変更されたファイルを別のボリュームにコピーしてから、ボリュームをアンマウントすることができます。

マウントするボリュームが書き込み可能である必要がある場合を除き、デフォルトの *read only* マウント・オプションが優先メソッドです。例えば、アーカイブ・アプリケーションが、アーカイブ・ボリュームに書き込みアクセスする必要がある場合などです。

IBM Spectrum Protect リカバリー・エージェント は、IBM Spectrum Protect サーバーからスナップショットをマウントします。IBM Spectrum Protect リカバリー・エージェント GUI で、「削除」をクリックし、IBM Spectrum Protect サーバーへの既存の接続を閉じます。別のサーバーや別のノードへの新規接続を設定できるようにするには、事前に既存の接続を削除する必要があります。「削除」をクリックする前に、すべてのボリュームをマウント解除してください。マウント・マシンにアクティブなマウント・セッションおよびリストア・セッションが存在する場合、除去操作は失敗します。サーバーからファイルのリストアを実行中に、そのサーバーへの接続を削除することはできません。まずすべての仮想デバイスをマウント解除し、リストア・セッションをすべて停止してからサーバーとの接続を切断する必要があります。そうしないと、接続は削除されません。

IBM Spectrum Protect リカバリー・エージェント をアンインストールする前に、すべての仮想ボリュームをアンマウントする必要があります。そうしないと、IBM Spectrum Protect リカバリー・エージェント が再インストールされた後で、これらのマウント済み仮想ボリュームをアンマウントできません。

ブロック・レベル・スナップショットのファイル情報のリストアは、ランダム・アクセス処理です。その結果、順次アクセス・デバイス (磁気テープなど) を使用する場合、処理が低速になる可能性があります。磁気テープに格納されているデータのファイル・リストアを実行するには、最初にデータをディスクまたはファイル・ストレージに移動することを検討してください。IBM Spectrum Protect サーバーの管理コマンド・ライン・クライアント (dsmadm) から **QUERY OCCUPANCY** コマンドを実行して、データが格納されている場所を確認することができます。その後、**MOVE NODEDATA** コマンドを実行し、データをディスクまたはファイル・ストレージに戻します。

Mount の 2 つのインスタンスにより、同じテープ・ストレージ・プールからスナップショットがマウントされると、以下のいずれかの結果が生じる可能性があります。

- 2 番目の Mount インスタンスは、最初のインスタンスが完了するまでブロックされる。
- 両方のマウントは成功するが、パフォーマンスが悪い。

ミラーリングされたボリュームからデータをリストアする場合、ミラーリングされたボリュームを含むディスクの一方のみをマウントしてください。両方のディスクをマウントすると、Windows がディスクの再同期を試行します。ただし、マウントされている場合は、両方のディスクに異なるタイム・スタンプが含まれます。その結果、すべてのデータが一方のディスクから他方のディスクにコピーされます。このデータ量を仮想ボリュームで対応することはできません。2 つのディスクにわたるボリュームからデータをリカバリーする必要があり、それらのディスクにミラーリングされたボリュームが含まれている場合は、以下のステップを実行してください。

1. 2 つのディスクをマウントします。
2. iSCSI イニシエーターを使用して、最初のディスクに接続します。
3. Windows Disk Manager を使用してこのディスクをインポートします。同期に関するすべてのメッセージを無視します。
4. 最初の (インポートされた) ディスクから、ミラーリングされた区画を削除します。
5. iSCSI イニシエーターを使用して、2 番目のディスクに接続します。
6. Windows Disk Manager を使用して、2 番目のディスクをインポートします。

これで両方のボリュームが使用可能です。

制約事項: IBM Spectrum Protect ノードに保管されているスナップショットからファイル・リストアを実行している間、このノードのパスワードを変更しないでください。

ファイル・リストアのガイドライン

IBM Spectrum Protect リカバリー・エージェント を使用して、ファイル・リストアを効率的に実施し、仮想ボリュームにスナップショットをマウントすることでダウン時間を最小限にすることができます。ファイル・リストアは、NTFS、FAT、または FAT32 のボリュームのスナップショットでサポートされます。

マウント機能を使用して、動的ディスクまたは GPT ベース・ディスクからの区画のスナップショットを、仮想ボリュームとしてマウントすることはできません。MBR ベースの基本ディスクからの区画のみを、仮

想ボリュームとしてマウントできます。仮想 iSCSI ターゲットを作成し、iSCSI イニシエーターを使用してシステムに接続することによって、GPT ディスク、動的ディスク、またはその他の任意の非 MBR もしくは非基本ディスクからのファイル・リストアが可能です。

動的ディスク上のデータのファイル・リストアを実行する場合、スナップショットをマウントするサーバーには、スナップショットを作成したノードと同じバージョンの Windows、またはそれより新しいバージョンの Windows が必要です。古いバージョンの Windows があるノードは、スナップショットがマウントされる CIFS 共有に旧ノード上のドライブをマップすることによって、動的ディスク上のファイルに間接的にアクセスできます。

重要: ファイル・リストア操作でリストアされたフォルダーおよびファイルに関連付けられた ACL 値は、リストアされたファイルに転送されません。ACL 値を維持するには、ターゲットからファイルをコピーするときに **XCOPY** コマンドを使用してください。

1 つ以上のファイルをリストア

IBM Spectrum Protect サーバー・ストレージにバックアップされた仮想マシンから、1 つ (または複数) のファイルをリストアできます。

始める前に

リストア操作で、インゲスト iSCSI イニシエーターを使用して仮想マシン ディスク・スナップショットにアクセスする場合、続行する前に以下の条件が存在することを確認してください。

- iSCSI デバイスが構成され、iSCSI イニシエーター・プログラムが実行中である。
- IBM Spectrum Protect リカバリー・エージェント GUI がインストールされているシステムとイニシエーター・システム間の LAN ファイアウォールで、ポート 3260 が開かれている。

このタスクについて

バックアップされた仮想マシン・ディスクをマウントして、マウントされたボリュームをファイル・リストア操作にエクスポートするには、以下のステップを実行します。

手順

1. IBM Spectrum Protect リカバリー・エージェント GUI を開始します。
Windows システム上で、「スタート」 > 「名前別のアプリケーション (Apps by name)」 > 「**IBM Spectrum Protect**」 > 「**IBM Spectrum Protect Recovery Agent**」に進みます。
IBM Spectrum Protect リカバリー・エージェント GUI は、仮想マシン・ゲストにインストールすることも、別個のホストにインストールすることもできます。
2. 「**IBM Spectrum Protect 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。
ターゲット・ノードは、バックアップが置かれている場所です。「ノードのアクセス方式」セクションで異なるノード名を指定することにより、ターゲット・ノードのデータへのアクセス・レベルを管理することができます。
3. リストから仮想マシンを選択します。
ヒント: リスト・ボックスの編集部分にマシン名の最初の数文字を入力することにより、仮想マシンを素早く検索できます。リストには、入力された文字と一致するマシンのみが示されます。マシン名では大文字小文字が区別されます。
仮想マシンがリストに表示されることがありますが、それを選択しても、スナップショット・リストが空である可能性があります。この状態は、以下のいずれかの理由により発生します。
 - その仮想マシンのスナップショットがまだ正常に完了していない。
 - **Fromnode** オプションが使用されたが、指定されたノードが選択された仮想マシンのリストアを許可されていない。
4. iSCSI 接続を使用してスナップショットをマウントします。

- a) IBM Spectrum Protect リカバリー・エージェント GUI の「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 ターゲットとしてマウント」をクリックします。
- c) ターゲットの名前を入力します。この名前は、マウントごとに固有でなければなりません。
- d) iSCSI イニシエーター名を入力します。

iSCSI イニシエーター名が、「iSCSI イニシエーター・プロパティ」ダイアログの「構成」タブに表示されます。例えば、次のとおりです。

```
iqn.1991-05.com.microsoft:hostname
```

5. iSCSI イニシエーターがインストールされているターゲット・システムで以下のステップを実行します。
 - a) 「ターゲット」タブをクリックします。
 - b) 「クイック接続」セクションで、IBM Spectrum Protect リカバリー・エージェント GUI がインストールされているシステムの IP アドレスまたはホスト名を入力します。
 - c) 「クイック接続」をクリックします。
 - d) 「クイック接続」ダイアログで、「ディスクカバーされたターゲット」フィールドの IP アドレスまたはホスト名を選択し、「接続」をクリックします。
 - e) 「状況 - 接続」が表示されたら、「完了」をクリックします。
 - f) 「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。
6. 任意のスナップショット日を選択します。選択したスナップショット内にバックアップされている 仮想マシンディスクのリストが表示されます。ディスクを選択し、「マウント」をクリックします。
7. 「マウント宛先の選択」ダイアログで、「選択済み区画からの仮想ボリュームの作成」をチェックします。選択されたディスク上で使用可能な区画のリストが表示されます。個々の区画について、そのサイズ、ラベル、およびファイル・システムのタイプが表示されます。
 - ・ ディスクが MBR ベースでない場合、エラー・メッセージが表示されます。
 - ・ デフォルトでは、ファイル・リストアに使用可能な区画のみが表示されます。
 - ・ 元のディスク上に存在していたすべての区画を表示するには、「マウント可能な区画のみを表示」チェック・ボックスをクリアしてください。
8. 必要な区画を選択します。

サポートされないファイル・システムを使用してフォーマットされた区画は選択できません。
9. 仮想ボリュームのマウント・ポイントとして、ドライブ名または空のフォルダーを指定します。
10. 「OK」をクリックして、ファイルをリカバリーするのに使用する仮想ボリュームを作成します。
11. 仮想ボリュームが作成されると、Windows エクスプローラーを使用して、任意の場所にファイルをコピーすることができます。

ヒント：ファイル・リストア操作でリストアされたフォルダーおよびファイルに関連付けられた ACL 値は、リストアされたファイルに転送されません。ACL 値を維持するには、ターゲットからファイルをコピーするときに **XCOPY** コマンドを使用してください。

関連タスク

51 ページの『IBM Spectrum Protect リカバリー・エージェント GUI の構成』

マウント操作およびファイル・リストア操作に IBM Spectrum Protect リカバリー・エージェント GUI をセットアップする必要があります。

57 ページの『iSCSI デバイスの手動構成』

iSCSI マウント操作時に使用する Windows システムを構成する必要があります。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。

第 12 章 IBM Spectrum Protect リカバリー・エージェント ト コマンド

Recovery Agent CLI は IBM Spectrum Protect リカバリー・エージェント へのコマンド・ライン API として表示できます。Recovery Agent CLI を使用して IBM Spectrum Protect リカバリー・エージェント に加えた変更は、即時に有効になります。

Recovery Agent CLI は、IBM Spectrum Protect リカバリー・エージェント を実行中の 1 つのシステムのみを管理する場合に使用できます。

Windows システムで、「スタート」 > 「名前別のアプリケーション (Apps by name)」 > 「IBM Spectrum Protect」 > 「Recovery Agent CLI」をクリックします。

マウント

mount コマンドは、IBM Spectrum Protect リカバリー・エージェント の各種タスクを完了するために使用します。

Recovery Agent CLI を使用すると、ボリュームおよびディスクのマウント (**mount add**) とアンマウント (**mount del**)、およびマウントされたボリュームのリスト表示 (**mount view**) を行うことができます。

mount コマンドを使用するには、IBM Spectrum Protect リカバリー・エージェント が実行中であることが必要です。 **set_connection** コマンドを使用して、RecoveryAgentShell.exe をマウント・アプリケーションに接続します。

スナップショットのマウントやアンマウントは、IBM Spectrum Protect リカバリー・エージェント が稼働しているシステム上で行われます。

ディスクをマウントするための構文

➤ RecoveryAgentShell.exe -c — mount — add — -rep — "tsm: — ip — = ➡

The diagram shows a horizontal line with a right-pointing arrow at its end. A bracket underneath the line spans from the start to a point before 'port'. Below this bracket is the text 'host name'. To the right of 'port' is an equals sign, followed by 'portNumber'. To the right of 'portNumber' is a space, then 'node', followed by another equals sign and 'nodeName'. A right-pointing arrow follows 'nodeName'.

► *vmname* — -type — disk — -disk — *disk number* — date — *date format* — -target ►

► "ISCSI: — target — = — *target_name* — initiator — = — *initiator_name*" ➤

区画をマウントするための構文

```

▶ RecoveryAgentShell.exe -c      — mount — add — -rep "tsm:" — ip — = ————— IP —————→
                                     |                               |
                                     +----- host_name -----+

▶ port — = — portNumber — node — = — nodeName →

▶ ————— pass — = — NodePassword" — -vmname →
|                               |
+----- -as_node — = — nodeName —+

▶ vmname — -disk ——— disk_number ——— date — date_format — -type partition →
                        |               |
                        +----- vhd_x —+

▶ -PartitionNumber — partNum — -target →

▶ ————— volume_letter —————→
|                               |
+----- "ISCSI: — target — = — target name — initiator — = — initiator name" —+

```

コマンド・タイプ

add

このコマンド・タイプは、IBM Spectrum Protect リカバリー・エージェントが稼働しているシステムにスナップショットのディスクまたはボリュームをマウントする場合に使用します。

以下に、**add** コマンド・タイプのタグおよびパラメーターをリストします。

-target

このタグは必須です。このタグは、次のターゲットの指定に使用します。

- ・ 仮想ボリューム - 区画のマウント専用
- ・ リパース・ポイント - 区画のマウント専用
- ・ iSCSI ターゲット

- rep

このタグは必須です。これは、スナップショットを保管している IBM Spectrum Protect サーバーと、バックアップにアクセスする IBM Spectrum Protect ノードの指定に使用します。例えば、次のようにします。

```
tsm: ip=<ip/host_name> port=<port_number>  
node=<node name> pass=<node password>
```

as_node オプションおよび from_node オプションも指定することができます。password フィールドが空の場合、IBM Spectrum Protect リカバリー・エージェント は保管済みノードのパスワードの使用を試行します。

-type

このタグは必須です。これは、ディスクまたは区画をマウントすることを指定します。オプションは以下のとおりです。

- type disk
- type partition

- VMname

このタグは必須です。これは、スナップショットのソースであるマシン名の指定に使用します。指定した値は大文字と小文字が区別されます。

-disk

このタグは必須です。これは、ソースがバックアップされたマウントされるマシンのディスク 番号の指定に使用します。

-date

このタグは必須です。これは、マウントするスナップショットの 日付を指定する場合に使用します。日付の形式は `yyyy-Mmm-dd hh:mm:ss` です。例えば、次のようにします。

```
-date "2013-Apr-12 22:42:52 AM"
```

アクティブな (または最新の) スナップショットを表示するには、`last snapshot` を指定します。

-PartitionNumber

このタグはオプションです。-type が `partition` の場合は、マウントする区画番号を入力します。

-ro|-fw

このタグは、マウントするボリュームを読み取り専用 (**-ro**) にするか、偽の書き込み (**-fw**) にするかを指定する場合に使用します。

-disk

このタグは必須です。これは、ソースがバックアップされたマウントされるマシンのディスク 番号の指定に使用します。

-ExpireProtect

このタグはオプションです。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有効期限が切れ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。以下の値のいずれかを指定できます。

Yes

スナップショットを期限切れから保護するには、**Yes** を指定します。この値がデフォルトです。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。

No

期限切れ保護を無効にするには **No** を指定します。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有効期限が切れる場合があります。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能になったり、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・コピーは操作中に有効期限が切れ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、**No** を指定して有効期限切れ保護を無効にします。

dump

このコマンド・タイプは、マウントに使用できるすべてのバックアップのリストを取得する場合に使用します。

以下に、**dump** コマンド・タイプのタグおよびパラメーターをリストします。

-rep

このタグは必須です。このタグは、スナップショットを保管している IBM Spectrum Protect サーバーを指定する場合と、バックアップにアクセスできる IBM Spectrum Protect ノードを指定する場合に使用します。例えば、次のとおりです。

```
tsm: ip=<IP/host name> port=<PortNumber>  
node=<NodeName> pass=<NodePassword>
```

-file

このタグはオプションです。このタグは、ダンプ・テキストを保管するファイル名の識別に使用します。このタグを指定しなかった場合、ダンプ・テキストは `stdout` に出力されるだけです。

remove

このタイプは、IBM Spectrum Protect サーバーへの接続を除去する場合に使用します。使用中の接続 (マウントされたボリュームが存在する場合など) を除去することはできません。

以下に、**remove** コマンド・タイプのタグをリストします。

- **-rep** - このタグは必須です。このタグは、除去する IBM Spectrum Protect サーバー接続を指定する場合に使用します。

view

このタイプは、マウントされているすべてのスナップショットのリストを表示するために使用します。このタイプにはタグはありません。

コマンドの例

次の例では、**-target** タグが使用されています。

- 次の例では、V: は仮想ボリュームのマウント・ターゲットです。

```
-target "V:"
```

- 次の例では、リパス・ポイント・ボリュームのマウント・ターゲットが指定されています。

```
-target "C:¥SNOWBIRD@FASTBACK¥Snowbird¥K¥Snowbird¥K¥¥¥"
```

- 次の例では、iSCSI ターゲットが指定されています。

```
-target "ISCSI: target=<target_name> initiator=<initiator_name>"
```

この例では、VM-03ent という名前の仮想マシンのスナップショットは、IP 10.10.10.01 を持つ IBM Spectrum Protect サーバーにあります。このスナップショットのディスク番号 1 が、IBM Spectrum Protect リカバリー・エージェント が稼働しているシステムにマウントされます。次のコマンドは、**add** タイプを指定してディスクをマウントする方法を示しています。

```
mount add -rep "tsm: ip=10.10.10.01 port=1500 node=tsm-ba pass=password"
-target "iscsi: target=test1 initiator=initiator_name" -type disk
-vmname VM-03ENT -disk 1 -date "2014-Jan-21 10:46:57 AM -ExpireProtect=Yes"
```

以下の例は、ダンプ・タイプの指定方法を示しています。

- バックアップ済みで使用可能なすべての VM をリストします。

```
mount dump -type TSM -for TSMVE -rep P -request
ListVM [-file <FileNameAndPath>]
```

- 仮想マシンの使用可能なすべてのディスク・スナップショットをリストします。

```
mount dump -type TSM -for TSMVE -rep P -request
ListSnapshots -VMName P [-file <FileNameAndPath>]
```

- あるディスク・スナップショットの、使用可能なすべての区画をリストします。

```
mount dump -type TSM -for TSMVE -rep P -request
ListPartitions -VMName P -disk P -date P [-file <FileNameAndPath>]
```

次の例では、ノード **NodeName** を使用して、IBM Spectrum Protect サーバー (10.10.10.01) との接続を除去します。

```
mount remove -rep "tsm: NodeName@ip"
```

以下は、**view** タイプの使用例です。

```
mount view
```

Hyper-V スナップショットのマウントの関連リンク

- [233 ページの『Set_connection』](#)
- [233 ページの『Help』](#)

Set_connection

set_connection コマンドは、指定された IBM Spectrum Protect リカバリー・エージェント を処理するように Recovery Agent CLI を設定します。

構文

► RecoveryAgentShell.exe -c — set_connection — mount_computer →

◀— IP address or host_name ▶◀

コマンド・タイプ

mount_computer

Recovery Agent CLI から、IBM Spectrum Protect リカバリー・エージェント がインストールされているシステムへの接続を設定する場合に、このコマンド・タイプを使用します。

以下に、**mount_computer** コマンド・タイプのパラメーターをリストします。

IP address or host_name

この変数は必須です。IBM Spectrum Protect リカバリー・エージェント がインストールされているシステムの IP アドレスまたはホスト名を指定します。

コマンドの例

次の例では、Recovery Agent CLI は、*ComputerName* ホスト上で IBM Spectrum Protect リカバリー・エージェント を処理するように設定されます。

```
set_connection mount_computer ComputerName
```

接続の設定の関連リンク

- [229 ページの『マウント』](#)
- [233 ページの『Help』](#)

Help

help コマンドは、サポートされるすべての Recovery Agent CLI コマンドのヘルプを表示します。

構文

► RecoveryAgentShell.exe -c — -h — command ▶◀

コマンド・タグ

-h

ヘルプ情報を表示するには、このコマンド・タグを使用します。

以下に、**mount_computer** コマンド・タイプのパラメーターをリストします。

command

この変数は必須です。ヘルプ情報が必要な Recovery Agent コマンドを指定してください。

コマンドの例

次の例では、Recovery Agent CLI は、*ComputerName* ホスト上で IBM Spectrum Protect リカバリー・エージェント を処理するように設定されます。

```
set_connection mount_computer ComputerName
```

接続の設定の関連リンク

- [229 ページの『マウント』](#)
- [233 ページの『Set_connection』](#)

Recovery Agent コマンド・ライン・インターフェースの戻りコード

戻りコードは、Recovery Agent CLI 操作の結果を識別する際のヒントになります。

以下の戻りコードを使用して、Recovery Agent CLI 操作の状況を確認します。

表 19. Recovery Agent CLI の戻りコード		
戻りコード	値	説明
0	FBC_MSG_MOUNT_SUCCESS	コマンドは正常に Data Protection for Microsoft Hyper-V マウントに送信されました。
0	FBC_MSG_DISMOUNT_SUCCESS	正常にスナップショットが取り外されました。
0	FBC_MSG_VIEW_SUCCESS	表示操作が正常に行われました。
0	FBC_MSG_DUMP_SUCCESS	ダンプ操作が正常に行われました。
0	FBC_MSG_REMOVE_SUCCESS	除去操作が正常に行われました。
1	FBC_MSG_MOUNT_FAIL	マウントが失敗しました (詳細については、マウント・ログを参照)。
2	FBC_MSG_MOUNT_DRIVER_ERROR	マウント・ドライバーのエラー
3	FBC_MSG_VOLUME_LETTER_BUSY	この名前のボリュームか、または再解析ポイントが使用中です。
4	FBC_MSG_MOUNT_WRONG_PARAMETERS	誤ったパラメーターがマウント・コマンドに割り当てられました (詳細については、マウント・ログを参照)。
5	FBC_MSG_MOUNT_ALREADY_MOUNTED	要求されたターゲットにジョブがすでにマウントされています。
6	FBC_MSG_MOUNT_WRONG_PERMISSIONS	許可が不十分です。
7	FBC_MSG_MOUNT_NETWORK_DRIVE	ネットワーク・マップ・ボリュームにマウントできません。
8	FBC_MSG_MOUNT_LOCKED_BY_SERVER	スナップショットがサーバーによってロックされました。
9	FBC_MSG_CAN_NOT_CHANGE_REPOSITORY	リポジトリを変更できません。
11	FBC_MSG_DISMOUNT_FAIL	マウントされたスナップショットの取り外しに失敗しました。

表 19. Recovery Agent CLI の戻りコード (続き)

戻りコード	値	説明
13	FBC_MSG_VIEW_FAIL	仮想ボリュームのリストの取得に失敗しました。
15	FBC_MSG_DUMP_FAIL	ダンプ・コマンド・リストの作成が失敗しました。
16	FBC_MSG_CONNECTION_FAILED	Data Protection for Microsoft Hyper-V マウントから切断されました。
17	FBC_MSG_CONNECTION_TIMEOUT	操作がタイムアウトになりました。
18	FBC_MSG_MOUNT_FAILED_TO_FIND_REPOSITORY	スナップショットを含む有効なリポジトリの検出に失敗しました。
19	FBC_MSG_MOUNT_JOB_NOT_FOUND	要求されたスナップショットの検出に失敗しました。
20	FBC_MSG_MOUNT_JOB_FOLDER_NOT_FOUND	要求されたスナップショット・データの検出に失敗しました。
22	FBC_MSG_CAN_NOT_REMOVE_REPOSITORY	選択されたリポジトリを削除できません。
23	FBC_MSG_REPOSITORY_GOT_MOUNTS	リポジトリにマウント済みのスナップショットがあります。
38	FBC_MSG_MOUNT_NOT_WRITABLE_VOLUME	マウント・ボリュームが書き込み不能です。
39	FBC_MSG_NO_TSM_REPOSITORY	IBM Spectrum Protect リポジトリが見つかりませんでした。
40	FBC_MSG_MOUNT_NOT_ALLOWED_AS_READONLY	iSCSI ターゲットを読み取り専用としてマウントすることはできません。
41	FBC_MSG_RESOURCE_BUSY_IN_TAPE_MODE	Data Protection for Microsoft Hyper-V はテープ・モードで稼働中のため、メディアはビジーです。
42	FBC_MSG_DISK_TYPE_NOT_SUPPORTED	このタイプのディスクでは、区画操作がサポートされていません。
43	FBC_MSG_MOUNT_INITIALIZING	操作が失敗し、Data Protection for Microsoft Hyper-V マウントが現在初期化中です。後でやり直してください。
44	FBC_MSG_CANNOT_LOCK_SNAPSHOT	スナップショットは、この操作中に有効期限が切れる場合、保護されません。詳しくは、資料を参照してください。

第 13 章 パフォーマンスの最適化

クライアント・オプションをコマンドで使用して、Data Protection for Microsoft Hyper-V 操作を制御します。ご使用の環境でパフォーマンスを調整するのに役立つオプションおよびパラメーターについて説明します。

パフォーマンスについて計画する場合、通常は、リカバリー・ポイント目標 (RPO) と目標復旧時間 (RTO) の目標があります。パフォーマンスが目標を満たすのに十分なものであることを確認する必要がありますが、ご使用の環境の Hyper-V ホストでのデータ保護により使用されるリソースのバランスを取ることも必要です。

Data Protection for Microsoft Hyper-V と IBM Spectrum Protect サーバー の間で転送されるデータの量は、操作やシナリオによって異なります。

バックアップ操作

バックアップ操作のために転送されるデータの量は、バックアップの状態によって異なります。

初期取り込みでのバックアップ

Data Protection for Microsoft Hyper-V をインストールするとき、仮想マシン (VM) はバックアップされず、VM ごとにフルバックアップ操作が必要になります。それらの初期バックアップ操作時には、大量のデータが転送されます。

Hyper-V ホストに VM を追加した後のバックアップ

ホストに VM を追加すると、VM はフルバックアップを必要とします。VM の数とサイズに応じて、対応する量のデータが転送されます。

クラスター化された環境では、VM がホスト・ノード間を移動する場合があります。クラスター用にバックアップされるデータの合計量は変わりませんが、特定のホストから転送されるデータの量は変わってきます。

初期取り込みの後のバックアップ (定常状態)

初期取り込み時に発生する初期のフルバックアップ操作の後に、増分バックアップ操作が発生します。増分バックアップ操作を、デフォルトで使用可能になる圧縮機能および重複排除機能と組み合わせると、転送されるデータの量はより少なくなります。バックアップ操作の大多数は増分バックアップです。

リストア操作

個々の VM または複数の VM をリストアすると、それに相当する量のデータが移動されます。RTO およびホストへの潜在的な影響を考慮して、オプションを調整してください。

災害復旧操作

災害復旧シナリオでは、ホストへの影響を軽減することよりスループットを最大化することを重視し、パラメーターを調整する必要がある場合があります。

バックアップ操作の最適化

仮想マシン (VM) のバックアップ操作を最適化するためには、`vmmaxparallel` オプションの設定を調整します。このオプションを使用すると、Hyper-V ホストに悪影響を及ぼすことなくバックアップ操作を最適化することができます。

バックアップ操作の概要

ここでは、`vmmaxparallel` オプションおよび `vmmaxbackupsessions` オプションの概要と、パフォーマンスを高めるためにこれらのオプションを構成する場合に考慮する必要がある要因について説明しています。

ヒント: これらのオプションの最適なデフォルト値を判別するためにパフォーマンス・テストが行われているので、値を変更する必要はない場合があります。最適な結果を得るには、最初はデフォルト値を使用して、バックアップ時間や Hyper-V ホストへの影響の度合いが目標を満たしているかを検討します。

デフォルト値を使用して限られた数の VM のバックアップ操作を実行してから、残りの VM のバックアップ時間を短縮したい場合にはこれらの値を大きくすることをお勧めします。

一般的に、オプション値を大きくすると、ネットワーク・スループットが向上します。しかしある時点で、この値を大きくしてもパフォーマンスが向上しなくなります。例えば、1 GB ネットワークを使用している場合、ネットワークが飽和状態になると、オプション値を大きくしてもスループットは向上しません。また、値を大きくすると CPU 使用率が上昇し、ホスト上のリソース・アベイラビリティに悪影響を及ぼす可能性があります。

また、ネットワークやプロセッサのリソースを他の操作と共有している場合、オプション値を大きくすると、それらの操作のパフォーマンスに悪影響を及ぼす可能性もあります。例えば、バックアップ操作に使用しているネットワークを VM による通常のネットワーク・トラフィックにも使用している場合、バックアップ操作中に VM でネットワーク速度の低下が発生する可能性があります。

スループットの向上を優先する場合は、デフォルト値を大きくしてください。ホストへの影響の最小化を優先する場合は、値を小さくしてください。

vmmaxparallel

vmmaxparallel オプションは、同時にバックアップできる VM の最大数を制御するために使用されます。vmmaxparallel の最適な値は、Hyper-V ホストの処理能力と、ホストと IBM Spectrum Protect サーバーの間の入出力のパフォーマンスによって異なります。

例えば、ビジーまたはスロー状態の LAN でデータをサーバーに移動する場合、各並列バックアップ操作の VM の数を制限する必要があるかもしれません。

同様に、Hyper-V ホストの処理能力が何らかの理由で制限されている場合も、VM の数を制限する必要がある場合があります。

パフォーマンスを最適化するには、Data Protection for Microsoft Hyper-V 環境では最小で 10 GB のネットワークを使用してください。

vmmaxbackupsessions

vmmaxbackupsessions オプションは、同時にバックアップ操作に組み込むことができるデータ移動セッションの最大数を制御するために使用されます。このオプションは許可されるセッションの最大数を設定しますが、Hyper-V ホスト上で稼働しているデータ・ムーバーは、着信ワークロードに基づいて実際に必要なセッション数を判別し、その数を使用します。

vmmaxbackupsessions オプションの値は、vmmaxparallel オプションの値以上である必要があります。値が vmmaxparallel オプションの値より小さい場合は、メッセージが返され、vmmaxparallel オプションと同じ値に変更されます。この変更により、セッションの数は存在する VM と同じ数になることが保証されます。

vmmaxbackupsessions オプションの最適な値を見つけるために、さまざまな値を試す必要がある場合があります。ディスパッチされた各 VM には必ず 1 つのセッションがあり、その後、追加セッションがディスパッチされた VM に適用されます。セッション数は、vmmaxbackupsessions オプションで指定された値を超えません。

ご使用のストレージ・システムのパフォーマンスがデータ・ムーバーとサーバーの間で使用可能なネットワーク速度より低速な場合、vmmaxbackupsessions オプションの値を大きくするメリットは限定的です。

制約事項 : Windows Server 2012 オペレーティング・システムでは、1 つの VM ディスクにつき複数のバックアップ・セッションを実行することはできません。しかし、それ以外のサポートされているすべての Windows オペレーティング・システム (Windows Server 2012 R2、Windows Server 2016、およびそれ以降のオペレーティング・システム) では、1 つの VM ディスクにつき複数のバックアップ・セッションを実行できます。

関連タスク

[239 ページの『複数の仮想マシンの並列バックアップ \(最適化されたバックアップ\)』](#)

並列バックアップ処理では、複数の仮想マシン (VM) を同時にバックアップすることができ、VM バックアップ操作のパフォーマンスを最適化できます。

関連資料

[202 ページの『Vmmaxparallel』](#)

vmmaxparallel オプションを使用すると、データ・ムーバーの単一インスタンスを使用して、複数の仮想マシン (VM) の並列バックアップを構成できます。このオプションは、一度に IBM Spectrum Protect サーバーにバックアップできる VM の最大数を指定します。

200 ページの『Vmmaxbackupsessions』

vmmaxbackupsessions オプションは、最適化されたバックアップ操作に組み込むことができる、仮想マシン (VM) データをサーバーに送信する IBM Spectrum Protect サーバー セッションの最大数を指定します。

複数の仮想マシンの並列バックアップ (最適化されたバックアップ)

並列バックアップ処理では、複数の仮想マシン (VM) を同時にバックアップすることができ、VM バックアップ操作のパフォーマンスを最適化できます。

始める前に

237 ページの『バックアップ操作の最適化』に記載されている情報を確認します。

手順

データ・ムーバー・システムで、以下の手順を実行します。

1. C:\Program Files\IBM\SpectrumProtect\baclient ディレクトリーに移動します。
2. データ・ムーバーのオプション・ファイル (dsm.hostname_HV_DM.opt) を、任意のテキスト・エディターで開きます。
3. オプション名と 1 つ以上のブランク・スペースを指定して、その後にオプション値を入力します。
例えば、次のようにします。

```
vmmaxparallel 5  
vmmaxbackupsessions 10
```

4. **backup vm** コマンドを発行します。
例えば、次のとおりです。

```
dsmc backup vm vm1
```

提供されている例を使用すると、VM レベル、仮想ディスク・レベル、またはサブディスク・レベルでの VM vm1 のバックアップ操作には、5 つの VM と 10 個のセッションを含めることができます。バックアップ操作は、ホストごとに 5 つの VM に制限されます。

関連資料

202 ページの『Vmmaxparallel』

vmmaxparallel オプションを使用すると、データ・ムーバーの単一インスタンスを使用して、複数の仮想マシン (VM) の並列バックアップを構成できます。このオプションは、一度に IBM Spectrum Protect サーバーにバックアップできる VM の最大数を指定します。

200 ページの『Vmmaxbackupsessions』

vmmaxbackupsessions オプションは、最適化されたバックアップ操作に組み込むことができる、仮想マシン (VM) データをサーバーに送信する IBM Spectrum Protect サーバー セッションの最大数を指定します。

153 ページの『Backup VM』

backup vm コマンドを使用して、Hyper-V 仮想マシンをバックアップします。

リストア操作の最適化

仮想マシン (VM) リストア操作を最適化するためには、vmmaxrestoresessions、vmmaxrestoreparallelvms、および vmmaxrestoreparalleldisks の各オプションの設定を調整し

ます。これらのオプションを使用すると、Hyper-V ホスト上のリソースのバランスを取りながらリストア操作を最適化することができます。

リストア操作の概要

ここでは、`vmmaxrestoresessions`、`vmmaxrestoreparallelvms`、および `vmmaxrestoreparallelvms` の各オプションの概要と、パフォーマンスのためにこれらのオプションを構成する場合に考慮する必要がある要因について説明しています。

ヒント：これらのオプションの最適なデフォルト値を判別するためにパフォーマンス・テストが行われているので、値を変更する必要はない場合があります。最適な結果を得るには、最初はデフォルト値を使用して、リストア時間や Hyper-V ホストおよび IBM Spectrum Protect サーバー への影響の度合いが目標を満たしているかを検討します。

デフォルト値を使用して限られた数の VM のリストア操作を実行してから、残りの VM のリストア時間を短縮したい場合にはこれらの値を大きくすることをお勧めします。

一般的に、オプション値を大きくすると、ネットワーク・スループットが向上します。しかしある時点で、この値を大きくしてもパフォーマンスが向上しなくなります。例えば、1 GB ネットワークを使用している場合、ネットワークが飽和状態になると、オプション値を大きくしてもスループットは向上しません。また、値を大きくすると CPU 使用率が上昇し、ホスト上のリソース・アベイラビリティに悪影響を及ぼす可能性があります。

ネットワークやプロセッサのリソースを他の操作と共有している場合、オプション値を大きくすると、それらの操作のパフォーマンスに悪影響を及ぼす可能性もあります。例えば、リストア操作に使用しているネットワークを VM による通常のネットワーク・トラフィックにも使用している場合、リストア操作中に VM でネットワーク速度の低下が発生する可能性があります。

スループットの向上を優先する場合は、デフォルト値を大きくしてください。ホストへの影響の最小化を優先する場合は、値を小さくしてください。

`vmmaxrestoresessions`

`vmmaxrestoresessions` オプションは、最適化されたリストア操作で一度に使用できる IBM Spectrum Protect サーバー セッションの最大数を制御します。このオプションは許可されるセッションの最大数を設定しますが、実際に必要なセッション数は、着信ワークロードに基づいて Hyper-V ホスト上で稼働しているデータ・ムーバーとネットワーク速度によって決まります。

最大のパフォーマンスを得るには、`vmmaxrestoresessions` オプションの最小値を、`vmmaxrestoreparallelvms` オプションの値と `vmmaxparallelvms` オプションの値を乗算した値以上にする必要があります。`vmmaxrestoresessions` オプションの値がこの最小値より小さい場合、実行時に適切な値に増やされます。

`vmmaxrestoresessions` オプションの最適な値を見つけるために、さまざまな値を試す必要がある場合があります。ディスパッチされた各 VM には必ず 1 つのセッションがあり、その後、追加セッションがディスパッチされた VM に適用されます。セッション数は、`vmmaxrestoresessions` オプションで指定された値を超えません。

ご使用のストレージ・システムのパフォーマンスがデータ・ムーバーとサーバーの間で使用可能なネットワーク速度より低速な場合、`vmmaxrestoresessions` オプションの値を大きくするメリットは限定的です。

例えば、`vmmaxrestoresessions` オプションの値を大きくすると、システム上のネットワーク・リソースやディスク・リソースの使用効率は向上しますが、ネットワーク転送やディスク速度の全性能を使い切らないようにするために、リストア・セッションの数を減らす必要が生じる場合があります。リストア・セッションの数を増やす必要がある場合は、ディスクを追加するか、Hyper-V ホスト上の異なるストレージ・プール間またはストレージ・デバイス間で VM を分割すること検討してください。

`vmmaxrestoreparallelvms`

`vmmaxrestoreparallelvms` オプションは、同時にリストアできる VM の最大数を制御するために使用されます。`vmmaxrestoreparallelvms` の最適な値は、Hyper-V ホストの処理能力と、ホストと IBM Spectrum Protect サーバー の間の入出力のパフォーマンスによって異なります。

例えば、ビジー状態または低速な LAN 経由でサーバーからデータを移動する場合、各並列リストア操作での VM の数を制限する必要がある場合があります。

同様に、Hyper-V ホストの処理能力が何らかの理由で制限されている場合も、VM の数を制限する必要があります。

パフォーマンスを最適化するには、Data Protection for Microsoft Hyper-V 環境では最小で 10 GB のネットワークを使用してください。

vmmaxrestoreparalleldisks

vmmaxrestoreparalleldisks オプションは、vmmaxrestoreparallelvms オプションの値やリストアされる VM の数に関係なく、VM ごとに同時にリストアできる仮想ディスクの最大数を制御するために使用されます。vmmaxrestoresessions オプションで指定されたセッションが十分な数である場合、データ・ムーバーは VM ごとに vmmaxrestoreparalleldisks オプションで指定された数の仮想ディスクを同時にリストアします。

関連タスク

[241 ページの『複数の仮想マシンの並列リストア \(最適化されたリストア\)』](#)

並列リストア処理では、複数の仮想マシン (VM) を同時にリストアすることができ、VM リストア操作のパフォーマンスを最適化できます。

関連資料

[210 ページの『Vmmaxrestoresessions』](#)

vmmaxrestoresessions オプションは、仮想マシン (VM) の最適化されたリストア操作に組み込むことができる IBM Spectrum Protect サーバー セッションの最大数を定義します。

[206 ページの『Vmmaxrestoreparallelvms』](#)

vmmaxrestoreparallelvms オプションは、同時にリストアできる仮想マシンの数を制御します。

[205 ページの『vmmaxrestoreparalleldisks』](#)

単一の仮想マシン (VM) で複数の仮想ディスクを同時にリストアするには、vmmaxrestoreparalleldisks オプションを指定します。

複数の仮想マシンの並列リストア (最適化されたリストア)

並列リストア処理では、複数の仮想マシン (VM) を同時にリストアすることができ、VM リストア操作のパフォーマンスを最適化できます。

始める前に

[239 ページの『リストア操作の最適化』](#)に記載されている情報を確認します。

このタスクについて

以下のオプションを使用して、リストア操作を最適化します。ご使用の環境で使用可能なリソースに応じて、数値を調整します。

- vmmaxrestoreparallelvms オプションを使用して、並列リストアされる VM の数を調整します。
- vmmaxrestoresessions オプションを使用して、リストア操作の IBM Spectrum Protect サーバー・セッションの数を、リストアされる各 VM に割り振ります。
- vmmaxrestoreparalleldisks オプションを使用して、各 VM で並列リストアする仮想ディスクの最大数を調整します。

手順

データ・ムーバー・コマンド・ラインで、以下の手順を実行します。

1. C:\¥Program Files¥IBM¥SpectrumProtect¥baclient ディレクトリーに移動します。
2. データ・ムーバーのオプション・ファイル (dsm.hostname_HV_DM.opt) を、任意のテキスト・エディターで開きます。

3. オプション名と 1 つ以上のブランク・スペースを指定して、その後にオプション値を入力します。
例えば次のとおりです。

```
vmmaxrestoreparallelvms 2  
vmmaxrestoresessions 8  
vmmaxrestoreparalleldisks 2
```

4. **restore vm** コマンドを発行します。
例えば、次のとおりです。

```
dsmc restore vm vm1,vm2,vm3 -vmname="*_<timestamp>"
```

この例で示された操作では、2 つの VM を並列でリストアし、各 VM で最大 4 つのセッション (合計 8 つのリストア・セッションを 2 つの VM で分割) を処理し、VM ごとに最大 2 つのディスクを並列で組み込むことができます。VM は、元の VM 名にリストア操作の日時が付加された名前を持つ新規 VM としてリストアされます。

関連資料

[165 ページの『Restore VM』](#)

restore vm コマンドを使用して、IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V によって以前にバックアップされた Microsoft Hyper-V 仮想マシン (VM) をリストアします。

[205 ページの『vmmaxrestoreparalleldisks』](#)

単一の仮想マシン (VM) で複数の仮想ディスクを同時にリストアするには、**vmmaxrestoreparalleldisks** オプションを指定します。

[206 ページの『Vmmaxrestoreparallelvms』](#)

vmmaxrestoreparallelvms オプションは、同時にリストアできる仮想マシンの数を制御します。

[210 ページの『Vmmaxrestoresessions』](#)

vmmaxrestoresessions オプションは、仮想マシン (VM) の最適化されたリストア操作に組み込むことができる IBM Spectrum Protect サーバー セッションの最大数を定義します。

付録 A トラブルシューティング

Data Protection for Microsoft Hyper-V の問題に対する解決方法が記載されています。

以下のトピックが参照可能です。

- [243 ページの『ログ・ファイルの検索』](#)
- [243 ページの『PowerShell コマンドレットを使用したトラブルシューティング』](#)
- [243 ページの『仮想マシン・バックアップが失敗し、0x800705B4 エラーが Hyper-V イベント・ログに書き込まれる』](#)
- [243 ページの『仮想マシンおよび Hyper-V ホストまたはクラスターの名前にサポート対象外の文字がある』](#)
- [244 ページの『ファイル・リストア・インターフェースが誤ったドライブ名割り当てとシステム予約済みディスクを表示する』](#)
- [244 ページの『SSL 接続を確立できない』](#)
- [244 ページの『エージェントの SSL 証明書が無効です。』](#)
- [245 ページの『VM バックアップ操作およびリストア操作は、別の VM 操作の進行中は開始できません。』](#)

ログ・ファイルの検索

Data Protection for Microsoft Hyper-V のログ・ファイルについては、以下のトピックを参照してください。

- [50 ページの『Data Protection for Microsoft Hyper-V ログ・アクティビティ・オプション』](#)
- [247 ページの『Data Protection for Microsoft Hyper-V のトレース・オプション』](#)

PowerShell コマンドレットを使用したトラブルシューティング

PowerShell コマンドレットを使用して、Data Protection for Microsoft Hyper-V 操作のトラブルシューティングを行えます。詳細については、[246 ページの『Data Protection for Microsoft Hyper-V 操作のトラブルシューティング』](#)を参照してください。

仮想マシン・バックアップが失敗し、0x800705B4 エラーが Hyper-V イベント・ログに書き込まれる

Windows Server 2016 での VM バックアップ操作中に、複数の VM ディスクを備えた仮想マシン (VM) の Resilient Change Tracking (RCT) フルバックアップを実行すると、このエラーが発生することがあります。スナップショット操作がタイムアウトになるか、サーバー上のファイル・スペースでスペースが不足します。

VM バックアップ操作が失敗する場合、0x800705B4 エラーがないか、Hyper-V イベント・ログを検索してください。このエラーが存在する場合は、以下の手順を実行して、スナップショット操作のパフォーマンスを向上させます。

1. Hyper-V VM が第 2 世代の VM であることを確認します。
2. 第 2 世代の VM に (SCSI ディスクと IDE ディスクの混合ではなく) SCSI ディスクのみが接続されていることを確認します。
3. Hyper-V スナップショット・フォルダーを、デフォルトのロケーション (C:\ProgramData\Microsoft\Windows\Hyper-V\Snapshots) から、Windows システム・ドライブでない高速ドライブ (例えば、D: ドライブ) に移動します。

仮想マシンおよび Hyper-V ホストまたはクラスターの名前にサポート対象外の文字がある

Data Protection for Microsoft Hyper-V は、仮想マシンおよび Hyper-V ホストまたはクラスターの名前に以下のいずれかの文字が含まれている場合、それらのバックアップをサポートしません。

"	二重引用符
'	単一引用符
:	コロン
;	セミコロン
*	アスタリスク
?	疑問符
,	コンマ
<	不等号 (より小さい)
>	不等号 (より大きい)
/	スラッシュ
\	円記号
	垂直バー

ファイル・リストア・インターフェースが誤ったドライブ名割り当てとシステム予約済みディスクを表示する

Windows の自動マウント機能が使用不可になっていることを確認してください。

デフォルトでは、Data Protection for Microsoft Hyper-V インストーラーが、**diskpart** コマンドにより自動マウント機能を自動的に使用不可にします。このアクションは、IBM Spectrum Protect ファイル・リストア・インターフェースで正しいドライブ名割り当てを表示し、システムで予約済みのディスクを非表示にするのに必要です。

Data Protection for Microsoft Hyper-V のインストール後、自動マウント機能がおそらく有効になっていました。自動マウント機能を無効にするには、**diskpart** コマンドを使用します。

SSL 接続を確立でない

SSL 証明書が何らかの理由で無効である場合 (Data Protection for Microsoft Hyper-V を再インストールして、古い SSL 証明書が削除されていない場合など)、Data Protection for Microsoft Hyper-V 管理コンソールに以下のメッセージが表示されることがあります。

GVM6065E SSL 接続を確立できませんでした。IBM Spectrum Protect の SSL 証明書がありません。有効な IBM Spectrum Protect 証明書が TSM-ve-trustore.jks RC=215 にあるかチェックしてください。

C:\¥IBM¥SpectrumProtect¥webserver¥usr¥servers¥veProfile¥tsmVmGUI¥truststores フォルダー内のファイルをすべて削除します。次に Data Protection for Microsoft Hyper-V 管理コンソールを再始動し、構成ウィザードを実行します。プロンプトが出されたらセキュリティ証明書を受け入れます。

エージェントの SSL 証明書が無効です。

リモート・クライアント・エージェントのセキュリティ証明書が無効であるか、最新のものではない場合、SSL 接続エラーが表示されることがあります。

例えば、C:\Program Files\Tivoli\TSM\baclient ディレクトリー内の証明書ファイル (dsmcert.sth、dsmcert.idx、および dsmcert.kdb) が削除されているか、破損している場合、データ・ムーバー・エラー・ログ (dsmererror.hostname_HV_DM.log) に以下のメッセージが表示されることがあります。

ANS1592E SSL プロトコルの初期化に失敗しました。

この問題の解決に使用する方法は、接続先の IBM Spectrum Protect サーバーのレベルに応じて異なります。

- IBM Spectrum Protect バージョン 8.1.2 以降のサーバー、または V7.1.8 以降の V7 サーバーに接続する場合は、以下の手順のいずれかを実行します。

- データ・ムーバー・ノードとマウント・プロキシ・ノードのクライアント・アクセプター・サービスを (ファイル・リストアが有効な場合は) 停止して、スタンドアロン・ホストまたはクラスターの任意のホストで Data Protection for Microsoft Hyper-V の構成ウィザードを再実行します。

詳細については、[39 ページの『ウィザードを使用した Data Protection for Microsoft Hyper-V の構成』](#)を参照してください。

- SESSIONSECURITY=TRANSITIONAL パラメーターを指定して、IBM Spectrum Protect サーバーのノード定義を更新します。Data Protection for Microsoft Hyper-V 管理コンソールから IBM Spectrum Protect サーバーにサインオンした場合、セキュリティ証明書が再作成されます。

詳しくは、[UPDATE NODE](#) を参照してください。

- IBM Spectrum Protect V8.1.1 以前の V8 サーバー、または V7.1.7 以前のサーバーに接続する場合は、[Dsmcutil コマンド: 必須オプションおよび例](#)を参照してください。

VM バックアップ操作およびリストア操作は、別の VM 操作の進行中は開始できません。

別の VM 操作の進行中にバックアップ操作またはリストア操開始された場合は、次のメッセージが表示されます。

ANS5176W 仮想マシンのバックアップまたはリストア操作が既に進行中であるため、要求された仮想マシンの操作を実行できません。最初の操作が完了した後でこの操作を再試行してください。

このメッセージは、以下の状態の場合に表示されます。

- VM のバックアップ操作またはリストア操作が開始されたときに、同じホストで別のバックアップ操作またはリストア操作が既に進行中の場合。
- VM のバックアップ操作またはリストア操作が開始されたときに、同じホスト上のいずれかの VM に対して別にスケジュールされたバックアップが実行中であるか、または他のユーザーが別のロケーションから操作を対話的に開始している場合。

このメッセージが表示された場合は、実行中の操作が終了するまで待機してから、バックアップ操作またはリストア操作を再開してください。

関連資料

[126 ページの『ゲスト仮想マシンのアプリケーション保護のトラブルシューティング』](#)

Data Protection for Microsoft Hyper-V がアプリケーション・データをホストしている仮想マシン (VM) のアプリケーション保護用に構成されており、VM バックアップ操作時に問題が発生した場合は、ご使用の環境で問題の再現を試行してください。

Data Protection for Microsoft Hyper-V 操作のトラブルシューティング

Microsoft Windows PowerShell コマンドレット・コマンドを実行して、Data Protection for Microsoft Hyper-V の問題を解決するための診断情報を取得できます。

始める前に

PowerShell コマンドレットを使用するように環境を準備していることを確認します。詳しくは、[139 ページの『Data Protection for Microsoft Hyper-V で PowerShell コマンドレットを使用する準備』](#)を参照してください。

手順

Data Protection for Microsoft Hyper-V 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。

1. 次のコマンドを発行して、PowerShell Viewer にログ・ファイル情報を表示します。

```
PS C:\> Show-DpHvApiLogEntries
```

以下のアクションのいずれかを使用して、PowerShell Viewer 内のログ情報を調査および共有することができます。

- 結果をフィルターに掛けるための条件を入力する。
- 「**条件の追加**」をクリックし、より詳細な指定で情報をフィルターに掛ける。
- 1 つ以上の行をクリックして、共有するためにそれらの内容を保存またはコピーする。

2. 次のコマンドを発行して、トレース・ファイルからトレース情報を表示します。

```
PS C:\> Show-DpHvApiTraceEntries
```

3. 詳細な診断情報パラメーターを検討するか、または IBM サポートに送信するためにログを収集するには、次のコマンドを発行して、圧縮ファイルにログを保存します。

```
PS C:\> Get-DpHvProblemDeterminationInfo -review
```

デフォルトでは、このコマンドは、デスクトップに DpHvProblemDetermination.zip ファイルを保存します。

ヒント: このコマンドが、デフォルトの「PowerShell」インターフェースでエラーを返した場合は、「PowerShell ISE」インターフェースを管理者として開始してください。その後、コマンドを再度実行してください。

4. オプション: 各 Data Protection for Microsoft Hyper-V コマンドレットでパラメーターを指定します。パラメーターを表示するには、次の **help** コマンドを発行します。

```
help cmdlet name -ShowWindow
```

関連資料

50 ページの『Data Protection for Microsoft Hyper-V ログ・アクティビティ・オプション』
FRLog.config オプションは、Data Protection for Microsoft Hyper-V 管理コンソールおよびファイル・リ
ストア操作に関するロギング情報の内容および形式を制御します。

247 ページの『Data Protection for Microsoft Hyper-V のトレース・オプション』

FRLog.config ファイルでトレース・オプションを設定することにより、Data Protection for Microsoft Hyper-V およびファイル・リストア操作中に発生する可能性のある問題のトラブルシューティングを行うことができます。

Data Protection for Microsoft Hyper-V のトレース・オプション

FRLog.config ファイルでトレース・オプションを設定することにより、Data Protection for Microsoft Hyper-V およびファイル・リストア操作中に発生する可能性のある問題のトラブルシューティングを行うことができます。

テキスト・エディターを使用して管理者モードで FRLog.config ファイル内のオプションを変更します。FRLog.config ファイルは、以下のディレクトリーにあります。

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

FR.API.TRACE= ON | OFF

推奨される詳細レベルで API アクティビティをトレースするかどうかを指定します。

注: DEBUG、TRACE、ALL の値もサポートされており、それぞれ、最小レベル、推奨レベル、最高レベルの詳細度を示します。

API_MAX_TRACE_FILES=number

作成または使用されるトレース・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_TRACE_FILE_SIZE=number

各トレース・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_TRACE_FILE_NAME=API_trace_file_name

API トレース・ファイルの名前を指定します。デフォルト値は fr_api.trace です。

API_TRACE_FILE_LOCATION=API_trace_file_location

API トレース・ファイルの場所を指定します。スラッシュ (/) を使用してロケーションを指定します。デフォルトのロケーションは *install_directory/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs* です。

付録 B Data Protection for Microsoft Hyper-V メッセージ

Data Protection for Microsoft Hyper-V から発行されるメッセージの説明と推奨アクションを提供しています。

GVM 接頭部で始まるメッセージが、番号の昇順で表示されています。一部のメッセージでは、メッセージ自体に説明とユーザー処置が提供されます。

GVM 接頭部で始まるいくつかのメッセージは、IBM Spectrum Protect for Virtual Environments: Data Protection for VMware と共有されます。

ANS 接頭部で始まるメッセージについては、[ANS 0000-9999 メッセージ](#)を参照してください。

GVM5900E	操作が失敗しました。戻りコード: <i>return code</i>
GVM5901E	内部エラーが発生しました: <i>type of error</i>
GVM5902E	IBM Spectrum Protect サーバーとの接続を確立できませんでした。

説明

サーバーが稼働していない可能性があります。

ユーザーの処置

サーバー・マシンとのネットワーク接続を確認します。サーバーが稼働していることを確認して、ログインを再試行してください。

GVM5903W	このデータを本当に削除しますか?
-----------------	------------------

説明

データの削除後にこのデータを回復することはできません。データを削除する前に、不要であるようにしてください。

ユーザーの処置

データを削除する場合は「OK」、このアクションを取り消す場合は「キャンセル」をクリックします。

GVM5904W	IBM Spectrum Protect サーバーとの接続がタイムアウトになりました。
-----------------	---

説明

考えられる原因として、操作の長時間実行、サーバー上の問題、または通信の問題が挙げられます。

ユーザーの処置

操作が長時間実行中の場合、その操作は完了しているか、まもなく完了する可能性があります。操作を再試

行する前に、予期される結果となっているか判別します。IBM Spectrum Protect サーバーのアクティビティ・ログで操作に関するエラーがないか確認してください。SSL を選択しないで SSL ポートを使用すると、このエラーを引き起こします。

GVM5905W	VM <i>VM name</i> は存在します。上書きしますか?
-----------------	-----------------------------------

GVM5906W	VM <i>VM name</i> は実行中です。システムの電源が切れていることを確認してから、「OK」を押して続行します。
-----------------	--

GVM5907I	サーバー名 <i>server name</i> のサーバー接続は正常に作成されました。OK をクリックして続行します。
-----------------	--

GVM5908W	IBM Spectrum Protect サーバーの定義が見つかりません。
-----------------	---------------------------------------

説明

サーバーの操作や照会を実行する場合は、事前に IBM Spectrum Protect サーバーの接続を定義する必要があります。

ユーザーの処置

サーバーを定義するには、以下のようにします。

1. 「構成」タブをクリックします。
2. 「構成設定の編集」アクション・リンクをクリックします。
3. 「IBM Spectrum Protect サーバー 資格情報」タブをクリックします。

GVM5909I	VM <i>VM name</i> は複数のデータ・ストアにまたがっています。これはその元の位置にしかリストアできません。
-----------------	---

GVM5910E	サーバー・データベース・ファイル <i>tsmserver.props</i> への書き込み中にエラーが発生しました
-----------------	--

説明

サーバー定義を tsmserver.props ファイルに書き込みできませんでした。

ユーザーの処置

このファイルは Data Protection for Virtual Environments のインストール・ディレクトリー内になければなりません。アクションを再試行する前に、ファイルが存在しており、ファイルが書き込み保護されていないことを確認します。

GVM5911E vCenter サーバーとの接続を確立できませんでした。

説明

サーバーが稼働していない可能性があります。

ユーザーの処置

これは、ネットワークの問題を示している可能性があります。サーバーが稼働していてマシンがアクセス可能であるようにしてください。アクションを再試行してください

GVM5912I vCenter サーバーとの接続が確立されました。

GVM5913E VMCLI の inquire_config コマンドが失敗しました。以下のメッセージがこのエラーについて説明しています。

説明

Derby データベースが稼働していない可能性があります。

ユーザーの処置

問題を修正してください。アクションを再試行してください

GVM5914I VMCLI の inquire_config コマンドが正常に完了しました。

GVM5915E インストールされている製品 (複数の場合あり) の判別に失敗しました。

説明

メッセージを参照してください。

ユーザーの処置

問題を修正してください。アクションを再試行してください

GVM5916I インストールされている製品 (複数の場合あり) が正常に判別されました。

GVM5917E 複数のリストア・ポイントが選択されましたが、それらは同じデータ・センター内にありません。

説明

異なるデータ・センターからのリストア・ポイントの選択は許可されません。リストア・ポイントはすべて同じデータ・センター内になければなりません。

ユーザーの処置

同じデータ・センターからリストア・ポイントを選択するか、あるいはリストア・ポイントを 1 つだけ選択してください。

GVM5918E 複数のリストア・ポイントが選択されましたが、それらは同じバックアップからのものではありません。

説明

異なるバックアップからのリストア・ポイントの選択は許可されません。リストア・ポイントはすべて同じバックアップ内になければなりません。

ユーザーの処置

IBM Spectrum Snapshot からのリストアの場合、すべてのリストア・ポイントが同じバックアップからのものでなければなりません。異なるバックアップからの複数の VM をリストアすることはできません。

GVM5919E 重要な構成ファイルが欠落しています: vmcliConfiguration.xml。

説明

ファイル vmcliConfiguration.xml が GUI の操作に必要ですが、GUI セッションの始動中に見つかりませんでした。これは異常な問題で、インストールの問題またはファイルの手動編集が原因の可能性があります。

ユーザーの処置

ファイルが正しいディレクトリー内にあるか、正しいアクセス権限が設定されているか、およびそのコンテンツに対して有効な構文になっているかを確認してください。GUI へのアクセスを再試行してください。

GVM5920E ファイル vmcliConfiguration.xml 内の無効な mode タグ。

説明

ファイル vmcliConfiguration.xml 内の xml タグ mode が GUI の操作に必要ですが、欠落しているか、誤った

値を持っています。これは、インストールの問題またはファイルの手動編集が原因の可能性があります。

ユーザーの処置

タグに有効な値が指定されていることを確認してください。GUI へのアクセスを再試行してください。

GVM5921E	ファイル vmcliConfiguration.xml 内の無効な enable_direct_start タグ。
-----------------	---

説明

ファイル **vmcliConfiguration.xml** 内の xml タグ **enable_direct_start** が GUI の操作に必要ですが、欠落しているか、誤った値を持っています。これは、インストールの問題またはファイルの手動編集が原因の可能性があります。

ユーザーの処置

タグに有効な値が指定されていることを確認してください。GUI へのアクセスを再試行してください。

GVM5922E	ファイル vmcliConfiguration.xml 内の、指定された mode タグに無効な URL タグ。
-----------------	---

説明

ファイル **vmcliConfiguration.xml** 内の、指定されている **mode** タグに対応する **URL** タグが GUI の操作に必要ですが、欠落しているか、誤った値を持っています。これは、インストールの問題またはファイルの手動編集が原因の可能性があります。

ユーザーの処置

URL タグに、指定された **mode** に有効な値が正しく指定されていることを確認してください。GUI へのアクセスを再試行してください。

GVM5923E	ファイル vmcliConfiguration.xml 内の無効な VMCLIPath タグ。
-----------------	---

説明

ファイル **vmcliConfiguration.xml** 内の xml タグ **VMCLIPath** が GUI の操作に必要ですが、欠落しているか、誤った値を持っています。これは、インストールの問題またはファイルの手動編集が原因の可能性があります。

ユーザーの処置

タグに有効な値が指定されていることを確認してください。GUI へのアクセスを再試行してください。

GVM5924E	ファイル vmcliConfiguration.xml 内の無効な interruptDelay タグ。
-----------------	--

説明

ファイル **vmcliConfiguration.xml** 内の xml タグ **interruptDelay** が GUI の操作に必要ですが、欠落しているか、誤った値を持っています。これは、インストールの問題またはファイルの手動編集が原因の可能性があります。

ユーザーの処置

タグに有効な値が指定されていることを確認してください。GUI へのアクセスを再試行してください。

GVM5925E	入力された VM 名 VM name が既存の VM と競合しています。別の名前を入力してください。
-----------------	---

GVM5926E	Web サーバーへの要求の処理中にエラーが発生しました。このエラーが解決されない場合は、 Web サーバーとのネットワーク接続を確認し、 Web サーバーが稼動中であることを確認します。 詳細: exception exception message
-----------------	--

GVM5927E	サーバーへの要求に時間がかかりすぎて完了できませんでした。このエラーが解決されない場合は、 Web サーバーとのネットワーク接続を確認し、 Web サーバーが稼動中であることを確認します。
-----------------	--

GVM5928E	Web サーバーからの応答の処理中にエラーが発生しました。 詳細: error
-----------------	--

GVM5929E	Web サーバー要求の作成中にエラーが発生しました。このエラーが解決されない場合は、 Web サーバーとのネットワーク接続を確認し、 Web サーバーが稼動中であることを確認します。 エラー: message
-----------------	---

GVM5930E	一致する装置クラスが見つかりません。ソース・ページに戻って再度選択してください。
-----------------	--

GVM5931E	一致するプロキシ・ノードが見つかりません。ソース・ページに戻って再度選択してください。
-----------------	---

GVM5932E	使用可能なプロキシ ESX ホストがありません。
-----------------	---------------------------------

GVM5933I	パスワードが正常に設定されました。
-----------------	-------------------

GVM5934E	パスワードの設定が失敗しました。 エラー: message
-----------------	---

説明

パスワードが間違っている可能性があるか、サーバーが稼働していません。

ユーザーの処置

パスワードが正しいことを確認して、アクションを再試行してください。あるいは、サーバー・マシンとのネットワーク接続を調べて、サーバーが稼働していることを確認してから、アクションを再試行してください。

GVM5935E	管理対象ドメインの獲得が失敗しました。 エラー: <i>message</i>
-----------------	--

GVM5936E	複数のリストア・ポイントが選択されましたが、それらは同じバックアップ・タイプではありません。
-----------------	--

説明

異なるタイプのリストア・ポイントの選択は許可されません。 リストア・ポイントはすべて IBM Spectrum Protect サーバー上または IBM Spectrum Snapshot リポジトリ内になければなりません。

ユーザーの処置

同じタイプのリストア・ポイントを選択するか、あるいはリストア・ポイントを1つだけ選択してください。

GVM5937E	バックアップ ID がヌルです。
-----------------	------------------

説明

内部エラーが発生しました。

ユーザーの処置

テーブルを最新表示し、アクションを再実行してください。

GVM5938E	タスク ID がヌルです。
-----------------	---------------

説明

内部エラーが発生しました。

ユーザーの処置

テーブルを最新表示し、アクションを再実行してください。

GVM5939E	ポップアップ・ウィンドウを開けませんでした。
-----------------	------------------------

説明

内部エラーが発生しました。

ユーザーの処置

アクションを再試行してください

GVM5940E	仮想マシン名がヌルです。
-----------------	--------------

説明

内部エラーが発生しました。

ユーザーの処置

テーブルを最新表示し、アクションを再実行してください。

GVM5941E	データ・ストアが存在しません。
-----------------	-----------------

説明

内部エラーが発生しました。

ユーザーの処置

テーブルを最新表示し、アクションを再実行してください。

GVM5942I	何も選択されませんでした。仮想マシン全体が付加されます。
-----------------	------------------------------

説明

何も選択されませんでした。

ユーザーの処置

アクションを続行するか、取り消してください。

GVM5943I	ドメインが正常に設定されました。
-----------------	------------------

GVM5944E	ドメインの設定が失敗しました。 エラー: <i>message</i>
-----------------	--

説明

サーバーが稼働していない可能性があります。

ファイル・ディレクトリーに対する許可が正しくない可能性があります。

ユーザーの処置

サーバー・マシンとのネットワーク接続を確認します。サーバーが稼働していることを確認し、アクションを再試行してください。

エラーが正しくない許可を示している場合は、SystemErr.log に示されているディレクトリーの許可を調べてください。

GVM5945E	このスケジュールでは、アクティブ・ドメインにない以下のデータ・センターを使用する必要があります。 データ・センター: <i>list</i>
-----------------	---

アクション: このスケジュールは更新されない可能性があります。代わりに、データ・センターを含めるようにドメイン構成を更新するか、またはこれらのデータ・センターに依存しない新しいスケジュールを作成してください。

詳細: スケジュールの定義は以下の通りです。

スケジュールの要約: *summary*

GVM5946E	このスケジュールでは、システムに認識されていない以下のデータ・センターを使用する必要があります。 データ・センター: <i>list</i> アクション: このスケジュールは更新されない可能性があります。代わりに、これらのデータ・センターに依存しない新しいスケジュールを作成してください。 詳細: スケジュール定義は以下のとおりです。 スケジュールの要約: <i>summary</i>
GVM5947E	このスケジュールでは、システムに認識されていない以下のホストを使用する必要があります。 ホスト: <i>list</i> アクション: このスケジュールは更新されない可能性があります。代わりに、これらのホストに依存しない新しいスケジュールを作成してください。 詳細: スケジュール定義は以下のとおりです。 スケジュールの要約: <i>summary</i>
GVM5948E	このスケジュールでは、システムに認識されていない以下のデータ・ストアを使用する必要があります。 データ・ストア: <i>list</i> アクション: このスケジュールは更新されない可能性があります。代わりに、これらのデータ・ストアに依存しない新しいスケジュールを作成してください。 詳細: スケジュール定義は以下のとおりです。 スケジュールの要約: <i>summary</i>
GVM5949E	このスケジュールでは、システムに認識されていない以下の仮想マシンを使用する必要があります。 仮想マシン: <i>list</i> アクション: このスケジュールは更新されない可能性があります。代わりに、これらの仮想マシンに依存しない新しいスケジュールを作成してください。

詳細: スケジュール定義は以下のとおりです。

スケジュールの要約: *summary*

GVM5950I	パスワードが正常に設定されました。 警告: <i>message</i>
説明 パスワードは正常に設定されましたが、警告が表示されました。	
ユーザーの処置 警告メッセージで説明されているアクションに従ってください。	
GVM5951E	Web サーバー要求の作成中にエラーが発生しました。このエラーが解決されない場合は、Web サーバーとのネットワーク 接続を確認し、Web サーバーが稼動中であることを確認します。 エラー: <i>error</i>
GVM5952E	次のコマンドには、サーバーからの確認応答が必要です: <i>""Command""</i>
説明 コマンドが出されたため、応答をする必要があります。一部のコマンドは確認応答が必要ですが、このような応答は Data Protection for Virtual Environments GUI から実行できません。	
ユーザーの処置 コマンドをコマンド・ラインから出してください。	
GVM5953E	次のコマンドはサーバーに認識されません: <i>""Command""</i>
説明 不明なコマンドがサーバーに対して出されました。このコマンドがサーバー・バージョンおよびプラットフォームに対して有効でないか、コマンド構文が誤っている可能性があります。	
ユーザーの処置 コマンドがサーバー・バージョンおよびプラットフォームに対して有効であることを確認し、コマンド構文が正しいことを確認してください。	
GVM5954E	次のコマンドの構文が誤っています: <i>""Command""</i> 。
説明 メッセージを参照してください。	

ユーザーの処置

構文を訂正し、コマンドをコマンド・ラインから出してください。IBM Spectrum Protect サーバーのアクティビティ・ログに、このコマンドの前後に出されたすべてのコマンドが表示されます。

GVM5955E 内部サーバー・エラーが発生しました。

説明

メッセージを参照してください。

ユーザーの処置

コマンドを再試行してください。これがうまくいかない場合には、お客様サポートに連絡してください。トレース情報および障害発生前に実行されたアクションに関する情報の提出を依頼される場合があります。

GVM5956E 要求の処理中にサーバーがメモリー不足になりました。IBM Spectrum Protect サーバーで不要なプロセスを閉じてから、操作を再試行してください。

説明

メッセージを参照してください。

ユーザーの処置

アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5957E データベース回復ログがフルです。

説明

メッセージを参照してください。

ユーザーの処置

アクションを再試行する前に、回復ログを拡張するか、IBM Spectrum Protect サーバー・データベースをバックアップしてください。IBM Spectrum Protect サーバーの管理者に連絡してください。

GVM5958E サーバー・データベースは満杯です。

説明

メッセージを参照してください。

ユーザーの処置

アクションを再試行する前に、サーバー・データベースを拡張してください。IBM Spectrum Protect サーバーの管理者に連絡してください。

GVM5959E サーバーのストレージ・スペースが不足しています。

説明

メッセージを参照してください。

ユーザーの処置

アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5960E このアクションを実行する許可がありません。システム権限を持つ管理者が、ご使用の権限レベルを変更して、このアクションの実行を許可することができます。

GVM5961E アクセスを試みているオブジェクトがサーバーに存在しません。

GVM5962E アクセスを試みているオブジェクトは、別のセッションまたはプロセスによって現在使用中です。あとでアクションを再試行してください。

GVM5963E 削除を試みているオブジェクトは、サーバーに定義された別のオブジェクトによって参照されています。このオブジェクトを削除する前に、別のオブジェクトを削除してください。

GVM5964E アクセスまたは削除を試みているオブジェクトが利用不能です。

説明

メッセージを参照してください。

ユーザーの処置

アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5965E 要求の処理中にサーバーにて入出力エラーが起きました。詳細については、オペレーティング・システム・イベントまたはエラー・ログを参照してください。

GVM5966E トランザクションにコミットできなかったため、アクションに失敗しました。

説明

メッセージを参照してください。

ユーザーの処置

あとでアクションを再試行してください。アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5967E	リソースのロック対立が起こったためアクションが失敗しました。
-----------------	--------------------------------

説明

メッセージを参照してください。

ユーザーの処置

あとでアクションを再試行してください。アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5968E	モード対立により、アクションが失敗しました。
-----------------	------------------------

説明

メッセージを参照してください。

ユーザーの処置

あとでアクションを再試行してください。アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5969E	サーバーが新規スレッドを開始できなかったために、アクションは失敗しました。
-----------------	---------------------------------------

説明

メッセージを参照してください。

ユーザーの処置

あとでアクションを再試行してください。アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5970E	サーバーは、このアクションを実行するライセンス交付を受けていません。ライセンスを購入している場合は、コマンド・ラインを使用してライセンスを登録してください。
-----------------	--

GVM5971E	無効な宛先が指定されました。
-----------------	----------------

説明

メッセージを参照してください。

ユーザーの処置

別の宛先を入力するか、有効な宛先を指定して構成を更新して、アクションを再試行してください。

GVM5972E	指定された入力ファイルをオープンできません。ファイル名およびディレクトリーの権限を検証してから、アクションを再試行してください。
-----------------	--

GVM5973E	指定された出力ファイルをオープンできません。ファイル名およびディレクトリーの権限を検証してから、アクションを再試行してください。
-----------------	--

GVM5974E	指定された出力ファイルへの書き込み中にエラーが発生しました。
-----------------	--------------------------------

説明

メッセージを参照してください。

ユーザーの処置

ファイル・システムに十分なスペースがあるようにします。詳細については、オペレーティング・システム・イベントまたはエラー・ログを確認してください。

GVM5975E	指定された管理者はこのサーバーに対して定義されていません。
-----------------	-------------------------------

説明

メッセージを参照してください。

ユーザーの処置

管理者名が正しく入力されているようにしてください。アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5976E	SQL ステートメントは処理することができません。
-----------------	----------------------------------

説明

SQL ステートメントの処理中に例外が発生しました。例外として、ゼロ除算、計算オーバーフロー、一時的に使用できないテーブル・ストレージ・スペース、およびデータ・タイプ・エラーなどが考えられます。

ユーザーの処置

SQL 照会を訂正し、再試行してください。

GVM5977E	この操作は、このオブジェクトに許可されていません。
-----------------	---------------------------

説明

メッセージを参照してください。

ユーザーの処置

アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5978E テーブルがサーバー・データベース内で見つかりません。

説明

メッセージを参照してください。

ユーザーの処置

アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5979E 指定したファイル・スペース名は、このファイル・スペース・タイプと互換性がありません。

説明

ユニコード・ファイル・スペース名は、非ユニコードの名前と互換性がありません。

ユーザーの処置

正しいタイプのファイル・スペース名を入力し、アクションを再試行してください。

GVM5980E 無効な TCP/IP アドレスが指定されました。TCP/IP アドレスを検証して、アクションを再試行してください。

GVM5981E 検索条件に一致するオブジェクトが見つかりません。

GVM5982E このサーバーでは、ご使用の管理 ID がロックされています。システム権限をもつ管理者が ID をアンロックできます。

GVM5983E アクションの実行中にサーバーへの接続が失われました。

説明

メッセージを参照してください。

ユーザーの処置

これは、ネットワークの問題を示している可能性があります。サーバーが稼働していてマシンがアクセス可能であるようにしてください。アクションを再試行してください。

GVM5984E ご使用の ID またはパスワードは、このサーバーでは無効です。

説明

メッセージを参照してください。

ユーザーの処置

IBM Spectrum Protect サーバーに対して有効な ID またはパスワードを入力してください。

GVM5985E このサーバーでは、ご使用のパスワードは有効期限が切れています。

説明

IBM Spectrum Protect のパスワードの有効期限が切れています。

ユーザーの処置

IBM Spectrum Protect サーバーでパスワードをリセットするか、IBM Spectrum Protect サーバー管理者に連絡してリセットを依頼してください。

GVM5986E サーバーは新規セッションを受け入れられません。セッションがこのサーバーに対して無効になっている場合、コマンド・ラインから **ENABLE SESSIONS** コマンドを出します。

GVM5987E 要求の処理中に通信障害が起こりました。あとでアクションを再試行してください。

GVM5988E 要求の処理中に、管理 API で内部エラーが発生しました。

GVM5989E 管理 API は、サーバーから送信されたコマンド文書を処理できません。

説明

XML コマンド文書を解析できません。ファイルを読み取ることができないか、ファイルが破壊されています。

ユーザーの処置

アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5990E 以下のコマンドは、1 つ以上の無効なパラメーターを含んでいます:
"**command**".

説明

Data Protection for Virtual Environments GUI はコマンドを実行しようとしたますが、API の呼び出しに 1 つ以上の無効なパラメーターが含まれていました。

ユーザーの処置

コマンドのパラメーターを確認してください。フィールドにテキストを入力した場合、パラメーターの誤りが見つかる可能性があります。見つかったら訂正します。アクティビティー・ログを表示すると、問題の原因を判別する上で役立ちます。アクションを再試行す

る前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5991E 要求の処理中に、管理 API は無効なパラメーターを検出しました。

説明

コマンドが管理 API を使用して実行されましたが、API メソッドに対するいずれかのパラメーターが無効でした。

ユーザーの処置

通常、これは内部エラーですが、異常なパラメーターによって引き起こされている可能性があります。例えば、<> & などの文字は問題の原因となります。コマンドのパラメーターを確認してください。フィールドにテキストを入力した場合、パラメーターの誤りが見つかる可能性があります。見つかったら訂正します。

GVM5992E このサーバーでの管理者権限レベルを判別できません。

説明

メッセージを参照してください。

ユーザーの処置

別の管理者 ID を使用します。アクションを再試行する前に、IBM Spectrum Protect サーバーの管理者にお問い合わせください。

GVM5993E 指定した名前のオブジェクトは、既にサーバーに存在します。別の名前を入力してください。

GVM5994E サーバーのバージョンが **Data Protection for Virtual Environments GUI** によってサポートされていません。

GVM5995E 内部エラーが発生しました。

説明

内部エラーを検出した後、操作が失敗しました。

ユーザーの処置

操作を再試行してください。これがうまくいかない場合には、お客様サポートに連絡してください。トレース情報および障害発生前に実行されたアクションに関する情報の提出を依頼される場合があります。

GVM5996E 操作が失敗しました。詳しくは、ログを確認してください。

GVM5997E 終了日時の形式が間違っています。yyyyMMddHHmmss の形式で終了日時を入力してください。

GVM5998E 申し訳ありません。バックアップ・タスクの説明はファイルに作成されませんでした。やり直してください。

説明

バックアップ・ウィザードの一般ページでは、通常バックアップ・タスクの説明を入力できます。

GVM5999E 入力した **ESXHOST** 名が長すぎます。短い名前に変更してください。

GVM6000E バックアップ ID が間違っています。やり直してください。

GVM6001E バックアップ・オブジェクト・ファイルの処理中にエラーが発生しました。後で再試行してください。

説明

バックアップ・ウィザードで「送信」をクリックすると、オブジェクト・リストがファイルに保管されます。このファイルを処理している時にエラーが発生しました。

GVM6002E バックアップ・オブジェクトが選択されていません。バックアップするソース・ノードを選択してください。

説明

バックアップ・タスクを開始するには、バックアップ・ウィザードのソース・ページでオブジェクトを選択する必要があります。

GVM6003E 開始日時の形式が間違っています。yyyyMMddHHmmss の形式で開始日時を入力してください。

GVM6004I バックアップ・タスク **Task Name** が開始しました。このタスクをすぐにモニターしますか？

GVM6005I バックアップ・タスクの削除が正常に完了しました。

GVM6006E バックアップ・タスクの削除に失敗しました。詳しくはログを確認してください。

GVM6007I リストア・タスク **Task ID** が正常に開始されました。このタスクをモニターしますか？

GVM6008E **Error Or Warning**

GVM6009I マウントされたバックアップ項目をリストアできませんでした。

GVM6010I 付加の結果は **status** です (タスク ID: **Task ID**)。詳しくは、イベント・リストを参照してください。

GVM6011I	切り離しの結果は status です (タスク ID: Task ID)。詳しくは、イベント・リストを参照してください。
GVM6012I	コマンドは正常に IBM Spectrum Protect サーバーに送信されました。 詳細: Server Messages
GVM6013E	IBM Spectrum Protect サーバーに送信されたコマンドが失敗しました。 エラー: Error Code Error Messages

説明

この問題の原因は、メッセージ・テキストに示されています。

ユーザーの処置

メッセージ・テキストに示されている情報に基づいて、問題を修正してください。その後、アクションを再試行してください。

GVM6014E	IBM Spectrum Protect サーバーの接続がありません。構成パネルで IBM Spectrum Protect サーバーを構成してください。
GVM6015E	選択された項目は 1 つのデータ・センターでのみ使用可能です。
GVM6018E	仮想マシン VM name が存在しています。リストアする前に、まずその仮想マシンを削除してください。
GVM6019E	ターゲット仮想マシン VM name が稼働中です。仮想マシンを閉じてから、仮想ディスクをリストアしてください。
GVM6020E	選択した仮想ディスクには、ターゲット仮想マシンに存在しているものがあります。その仮想ディスクをターゲット仮想マシンから削除してから、リストアを行ってください。
GVM6021E	VMCLI コマンドが失敗しました。 エラー: Error Messages

説明

この問題の原因は、メッセージ・テキストに示されています。

ユーザーの処置

メッセージ・テキストに示されている情報に基づいて、問題を修正してください。その後、アクションを再試行してください。

GVM6023E	IBM Spectrum Protect サーバーに送信されたコマンドが失敗しました。 エラー: Error Messages
-----------------	--

説明

この問題の原因は、メッセージ・テキストに示されています。

ユーザーの処置

メッセージ・テキストに示されている情報に基づいて、問題を修正してください。その後、アクションを再試行してください。

GVM6024E	「 summary.date.log 」形式のファイルがパス path 内で見つかりません。
GVM6025E	VMCLI inquire_config コマンドを使用して IBM Spectrum Snapshot インストール・パスを見つけることができません。
GVM6026E	バージョンを取得するための VMCLI コマンドが失敗しました。
GVM6027I	バックアップ・タスク Task ID が開始しました。このタスクをすぐにモニターしますか?
GVM6028E	Data Protection for Virtual Environments Web Server に接続できませんでした。

説明

Data Protection for Virtual Environments GUI は Web サーバーへの接続を試みました。操作は正常終了しませんでした。

ユーザーの処置

以下の 1 つ以上のステップを実行して、問題を判別を試みてください。

- **Data Protection for Virtual Environments Web** サーバーが稼働中であることを確認します。
- Web サーバー・マシンが稼働中であることを確認します。
- Web サーバー・マシンにネットワークを介してアクセス可能であることを確認します。

Data Protection for Virtual Environments GUI を閉じます。問題が解決したら、GUI を再始動してください。

GVM6029I	コマンドは正常にサーバーに送信されました。
GVM6030E	データ・センター datacenter name にホストが見つかりません。リスト

アする別のデータ・センターを選択します。

GVM6031W スケジュールには、必要なパラメーターがすべて含まれているわけではありません。スケジュールはプロパティ・ノートブックに表示できません。

説明

このスケジュールは、Data Protection for Virtual Environments GUI の外部で作成または変更された可能性があります。

ユーザーの処置

このスケジュールは、Data Protection for Virtual Environments GUI の外部で変更する必要があります。

GVM6032W 1つ以上の VM が存在します。リストア操作を続行して、既存の VM を上書きしますか？

GVM6033E 指定された管理者 ID には十分な特権がありません。

説明

試行中の操作では、IBM Spectrum Protect サーバー管理者 ID が少なくとも無制限ポリシー特権を持っている必要があります。

ユーザーの処置

IBM Spectrum Protect サーバー管理者に連絡して、管理 ID に無制限ポリシー特権を付与するように依頼してください。あるいは、無制限ポリシー特権を持っている代替 ID を使用して再試行してください。

GVM6034E ノード名 *node name* は既に使用されています。別のノード名を選択してください。

説明

選択されたノード名はサーバーに既に存在しています。別の名前を選択してください。

ユーザーの処置

使用する別のノード名を選択してください。このノードを再使用する場合は、「ノードの登録」チェック・ボックスを選択解除してください。

GVM6035E ノード名 *node name* がサーバーに定義されていません。入力したノード名がサーバーに存在することを確認してください。

説明

入力されたノード名がサーバーに存在しません。「ノードの登録」チェック・ボックスを選択しなかったため、入力するノード名は、以前に定義済みであり、サーバーに存在している必要があります。

ユーザーの処置

使用するつもり of ノード名を確認して、再入力してください。このノードを登録する場合は、「ノードの登録」チェック・ボックスを選択してください。

GVM6036E 入力フィールドのパスワードと検証フィールドのパスワードが一致していません。やり直してください。

説明

入力された新規パスワードが一致していません。

ユーザーの処置

フィールドをクリアして、両方のパスワード・フィールドに同じパスワードを入力してください。

GVM6037W 管理対象の 1つ以上のデータ・センターを選択してください。

説明

少なくとも 1つのデータ・センターを選択してください。

ユーザーの処置

1つ以上のデータ・センターを管理対象データ・センターのリストに追加してください。

GVM6038W 1つ以上のノードのパスワードが設定されていません。すべてのノードのパスワードが設定されていることを確認してください。

説明

あるノードで「ノードの登録」チェック・ボックスが設定されている場合、そのノードのパスワードが設定されている必要があります。

ユーザーの処置

登録するノードにパスワードを割り当ててください。

GVM6039I *datacenter name* にマップされるデータ・センター・ノードが見つかりませんでした。*datacenter name* に関連付けるデータ・センター・ノードをリストから選択してください。対応する新規データ・センター・ノードを構成ウィザードに作成させる

場合は、選択を空のままにしてください。

GVM6040I	IBM Spectrum Protect 管理 ID を入力せずに続行しますか? IBM Spectrum Protect 管理アクセス権限がないと、ウィザードはノード名の検証やノードの登録を行いません。代わりに、このウィザードの最後にマクロ・ファイルが生成され、実行するために IBM Spectrum Protect 管理者に提供されます。
GVM6041I	このタスクは必要ないか、前提条件タスクが失敗しているために、スキップされました。
GVM6042E	スクリプト・ファイル <i>file path</i> への書き込み中にエラーが発生しました。

説明

示されたファイル・パスでファイルに書き込もうとしたときにエラーが検出されました。

ユーザーの処置

操作を再試行してください。

GVM6043I	管理対象データ・センターが変更されました。データ・ムーバー・ページに移動して、現行のマッピングを確認または変更してください。
GVM6044I	vCenter ノード vCenter node および VMCLI ノード VMCLI node 構成用のデータ・センター・ノードが見つかりませんでした。ウィザードは、データ・センター・ノードのデフォルト・セットを生成します。
GVM6045E	入力されたパスワードは受け入れられません。別のパスワードを選択してください。

説明

IBM Spectrum Protect サーバーは、選択されたパスワードを受け入れることができませんでした。パスワードが特定のパスワード規則を満たしていないことが原因と考えられます。

ユーザーの処置

別のパスワードを使用して再試行してください。

GVM6046W	このチェック・ボックスのチェック・マークを外すことは、 IBM Spectrum Protect サーバーに既に定義されているノード名を指定しており、その名前が構成に使用されることを意味
-----------------	--

しています。このウィザードは管理アクセス権限を使用せずに進められているため、ノードが存在するかどうを確認できません。操作の内容を理解している場合にのみ続行してください。

説明

IBM Spectrum Protect 管理 ID を使用せずに構成ウィザードを使用しているため、十分注意する必要があります。構成ウィザードの実行終了時に生成されたマクロ・スクリプト・ファイルにエラーが含まれている可能性があります。値の妥当性検査が行われなかったためです。

ユーザーの処置

構成ウィザードを使用する場合は、適切な IBM Spectrum Protect 管理 ID を使用することを強くお勧めします。

GVM6047W	IBM Spectrum Protect ノード <i>node</i> は既に識別されています。デフォルト名以外の別の名前を使用する場合は、このフィールドを再編集してください。複数のデータ・センターに同じデータ・ムーバーを使用する場合は、「構成設定」を使用してこの編集を行ってください。
-----------------	---

説明

ノードは、この構成で既に使用されています。

ユーザーの処置

別のノード名を試してください。

GVM6048W	IBM Spectrum Protect ノード <i>node</i> に無効な文字が使用されているか、 64 文字を超えています。別の名前を選択して、このフィールドを再編集してください。
-----------------	---

説明

ノード名が無効か、64 文字を超えています。

ユーザーの処置

別のノード名を試してください。

GVM6049E	入力されたパスワードには無効な文字が含まれているため、このサーバーでは受け入れられません。有効な文字は、 <i>validCharsString</i> です。
-----------------	--

説明

パスワードに無効な文字が含まれているため、IBM Spectrum Protect サーバーは、選択されたパスワードを受け入れることができませんでした。

ユーザーの処置

有効な文字のみを含む別のパスワードを使用して再試行してください。

GVM6050E	入力されたパスワードは、以下の理由により、このサーバーでは受け入れられません。別のパスワードを選択してください。 エラー: <i>message</i>
-----------------	---

説明

IBM Spectrum Protect サーバーは、選択されたパスワードを受け入れることができませんでした。このパスワードが無効である理由がメッセージに示されています。

ユーザーの処置

規則を満たす別のパスワードを使用して再試行してください。

GVM6051E	フィルターが変更されました。続行する前に「フィルターの適用」を選択してください。
-----------------	--

説明

フィルター・パターンが変更された後は、それを適用する必要があります。

ユーザーの処置

「フィルターの適用」ボタンをクリックします。

GVM6052E	続行するには、データ・センターから少なくとも 1 つの項目を選択してください。
-----------------	---

説明

バックアップを実行するには、ホスト、ホスト・クラスター、または VM を選択する必要があります。

ユーザーの処置

データ・センター下で項目を選択します。

GVM6053E	選択項目がバックアップに許容される 512 文字の長さ制限を超えています。選択を変更してください。
-----------------	---

説明

選択項目をリストするために必要な文字数が 512 文字の制限を超えています。さらに、ホストが一部選択されている場合には、バックアップから除外される VM をリストするための文字数も必要です。

ユーザーの処置

複数のバックアップ・タスクを作成して、タスク当たりの選択項目数を少なくします。

GVM6054I	新しく追加された仮想マシンのチェック・ボックスを変更すると、ホスト・クラスター、ホスト、および仮想マシンのすべての選択がクリアされます。続行する場合は「OK」を押し、未変更のままにする場合は「キャンセル」を押します。
-----------------	--

説明

新しく追加された仮想マシンのチェック・ボックスの状態は、ソース・パネルで選択できるものに大きく影響するため、状態が変更されると、選択がクリアされます。

ユーザーの処置

続行する場合は「OK」を選択し、すべての選択を保持する場合は「キャンセル」を選択します。

GVM6055E	データ・センター・ノード <i>datacenter node name</i> には、vmcli 構成ファイルにマップされた IBM Spectrum Protect ノードがありません。
-----------------	---

説明

データ・センター・ノードは、vmcliprofile という名前の構成ファイル内に、対応する IBM Spectrum Protect ノードがリストされている必要があります。

ユーザーの処置

GUI の「構成」タブに移動し、「構成の編集」を選択してデータ・センターのマッピングを更新し、問題を修正します。「構成」タブに報告されている構成エラーが他にもあればすべて解決してください。

GVM6056E	IBM Spectrum Protect データ・センター・ノード <i>datacenter node name</i> は、vmcli 構成ファイル内の vCenter データ・センター名 <i>datacenter name</i> にマップされますが、 <i>datacenter name</i> が vCenter に存在しません。
-----------------	--

説明

vCenter データ・センター名が、vmcliprofile という名前の vmcli 構成ファイル内のデータ・センター・ノード

にマップされますが、そのデータ・センター名は vCenter に存在しません。

ユーザーの処置

GUI の「構成」タブに移動し、「構成の編集」を選択してデータ・センターのマッピングを更新し、問題を修正します。「構成」タブに報告されている構成エラーが他にもあればすべて解決してください。

GVM6057E	複数のデータ・センター <i>datacenter list</i> から項目を選択しました。これは許可されません。選択はすべて 1 つのデータ・センターから行う必要があります。
-----------------	---

説明

バックアップ・タスクは、1 つのデータ・センターからの項目のみをサポートします。これが既存のタスクである場合は、タスクの作成後の vCenter 構成の変更がこの問題の原因である可能性があります。

ユーザーの処置

選択項目を調べて修正し、すべての選択項目が同じデータ・センター下にあるようにします。

GVM6058E	選択された項目 <i>item list</i> が vCenter 内のデータ・センター <i>datacenter name</i> 下で見つかりません。選択項目を確認して選択解除してください。
-----------------	---

説明

当初に選択された項目が、バックアップ・タスクに関連付けられたデータ・センター下で見つからなくなっています。これは vCenter 構成の変更が原因であると考えられます。

ユーザーの処置

選択項目が現在、別のデータ・センター下にあるかどうかを調べます。見つからない項目を選択解除して、別のデータ・センター下で新たに選択を行うか、これらの項目用の新規バックアップ・タスクを作成してください。

GVM6062E	入力されたパスワードは短すぎるため、このサーバーでは受け入れられません。パスワードは、少なくとも <i>minPasswordLength</i> 文字必要です。
-----------------	---

説明

IBM Spectrum Protect サーバーは、選択されたパスワードが短すぎるために受け入れることができませんでした。

ユーザーの処置

必要な最小長さを超える別のパスワードを使用して再試行してください。

GVM6063E	Component はダウン・レベルであるため、 GUI で無効にされています。 component 用の GUI のみ使用できます。
-----------------	---

GVM6064E	現行設定の中で、 IBM Spectrum Protect サーバー項目の不一致が検出されました。 GUI で使用される IBM Spectrum Protect サーバー定義: <i>server1</i> バックアップが保管される IBM Spectrum Protect サーバー: <i>server2</i> 「サーバー定義のリセット」をクリックして、 IBM Spectrum Protect 定義をクリアし、新しい資格情報を入力します。あるいは『環境の再構成』をクリックして構成ウィザードを起動し、 Data Protection for Virtual Environments 環境を再構成します。
-----------------	---

説明

IBM Spectrum Protect は、vmcliprofile と現行 GUI の IBM Spectrum Protect サーバー接続の間で、不一致の IBM Spectrum Protect サーバー項目を検出しました。

ユーザーの処置

選択可能な 2 つのアクションのいずれかを選びます。IBM Spectrum Protect サーバー定義/資格情報をリセットするか、または構成ウィザードを使用して新しい環境をセットアップすることができます。

GVM6065E	SSL 接続を確立できませんでした。 IBM Spectrum Protect の SSL 証明書がありません。有効な IBM Spectrum Protect 証明書が TSM-ve-truststore.jks にあるかチェックしてください。
-----------------	--

説明

IBM Spectrum Protect サーバーは、SSL 接続を受け入れませんでした。SSL 鍵ストアがデフォルト・ロケーションにないか、あるいは、IBM Spectrum Protect 証明書が含まれていません。

ユーザーの処置

有効な証明書が **TSM-ve-truststore.jks** にあるかをチェックしてください。また、**TSM-ve-truststore.jks** が正しいデフォルト・ロケーションにあるかを確認してください。

GVM6066E 入力されたパスワードは長すぎるため、このサーバーでは受け入れられません。パスワードは、**maxPasswordLength** 文字を超えてはいけません。

説明

IBM Spectrum Protect サーバーは、選択されたパスワードが長すぎるために受け入れることができませんでした。

ユーザーの処置

許される最大の長さより短い別のパスワードを使用して再試行してください。

GVM6067E **SSL 接続を確立できませんでした。IBM Spectrum Protect の SSL 証明書が無効です。**

説明

IBM Spectrum Protect サーバーは、SSL 接続を受け入れませんでした。TSM-ve-truststore.jks には、無効な IBM Spectrum Protect SSL 証明書があります。

ユーザーの処置

新しい有効な IBM Spectrum Protect SSL 証明書を IBM Spectrum Protect サーバーから入手して、TSM-ve-truststore.jks に置いてください。

GVM6068E **非 SSL 接続を確立できませんでした。この IBM Spectrum Protect 管理 ID には、IBM Spectrum Protect SSL 接続が必要です。**

説明

IBM Spectrum Protect サーバーは、非 SSL 接続を受け入れませんでした。IBM Spectrum Protect サーバーでは、この管理者 ID で SSL を使用する必要があります。

ユーザーの処置

この管理者 ID では SSL を使用します。有効な IBM Spectrum Protect サーバーの SSL 証明書を含む TSM-ve-truststore.jks がデフォルト・ロケーションにインストールされていることを確認します。

GVM6069E 選択の結果、バックアップ・タスク定義で **count** 文字が必要になりましたが、これは **512** 文字の制限を超えています。原因は、長い仮想マシン除外リストにある可能性があります。このリストは、選択されなかったホスト下のすべての VM のリストです。選択されたホスト下の VM をより多くするように選択するか、あ

るいは、新しく追加された仮想マシン・チェック・ボックスで選択解除してください。

説明

新しく追加された仮想マシン・チェック・ボックスでの選択をする場合は、結果のバックアップ・タスクは、部分的に選択されたホストのすべての選択されない仮想マシンをリストすることになります。バックアップ・タスク定義には **512** 文字の制限があり、選択された項目と除外された VM の組み合わせがこの制限を超えるエラーとなります。

ユーザーの処置

新しく追加された仮想マシン・チェック・ボックスで選択解除するか、複数のバックアップ・タスクを作成して、タスク当たりの選択項目数を少なくします。

GVM6070E 仮想マシンの選択の結果、バックアップ・タスク定義で **count** 文字が必要になりましたが、これは **512** 文字の制限を超えています。複数のバックアップ・タスクを作成して、タスクあたりの仮想マシンの数を少なくするか、あるいは、新しく追加された仮想マシン・チェック・ボックスを利用して、選択されない VM が少ないホストはホスト全体を選択してしまうようにします。

説明

バックアップ・タスクの定義には **512** 文字の長さ制限があり、選択された項目の合計文字数がこの制限を超えています。

ユーザーの処置

複数のバックアップ・タスクを作成して、タスクあたりの仮想マシンの数を少なくするか、あるいは、新しく追加された仮想マシン・チェック・ボックスを利用して、個々の仮想マシンを選択する代わりに、ホストを選択するようにします (必要な場合、ホストあたり、小さな数の仮想マシンを選択解除できます)。

GVM6071E データ・センター・ノード **datacenter node name** のデータ・ムーバー・ノード・プロキシ関係がありません。「構成」タブまたは **IBM Spectrum Protect** サーバーのデータ・ムーバー関係を確認してください。

GVM6072E データ・センター **datacenter name** についてデータ・センター・ノードが定義されていません。「構成」タブのノード構成を確認してください。

GVM6073I	ノード <i>name name</i> は現在ロックされています。続行しようとする、構成ウィザードはこのノードをアンロックしようと試みます。
GVM6074E	IBM Spectrum Protect サーバー (<i>Address:Port</i>) との接続を確立できませんでした。サーバー・アドレスと管理ポート、サーバー・ポートまたは管理ポートが正しいことを確認してください。

説明

サーバーが稼働していないか、指定された管理ポートまたはサーバー管理ポートが正しくない可能性があります。

ユーザーの処置

IBM Spectrum Protect サーバー・マシンとのネットワーク接続を確認します。サーバーが稼働していることを確認して、ログインを再試行してください。また、サーバー・アドレスと管理ポートの情報が正しいことを確認してください。

GVM6075E	vCenter ユーザー名またはパスワードが無効です。やり直してください。
-----------------	--

説明

vCenter ユーザー名またはパスワードが無効です。

ユーザーの処置

ユーザー名またはパスワードを再度入力してください。

GVM6076E	この操作を実行する許可が拒否されました。別のユーザー名で試行してください。
-----------------	---------------------------------------

説明

vCenter のユーザー名が無効です。

ユーザーの処置

別のユーザー名を入力してください。

GVM6077I	IBM Spectrum Protect 管理 ID とパスワードが現在設定されていません。この情報がないと、GUI で実行できるアクションが制限されます。「構成設定」パネルに移動して ID とパスワードを設定する場合は、「OK」をクリックしてください。ID とパスワードを使用せずに続行する場合は、「キャンセル」をクリックしてください。
-----------------	--

GVM6078W	<p>現行 ID より権限が少ない管理 ID を選択しました。この ID を変更しますか?</p> <p>現行の IBM Spectrum Protect 権限レベル: <i>Current Level</i></p> <p>新規の IBM Spectrum Protect 権限レベル: <i>New Level</i></p> <p>現行の役割: <i>Current Role</i></p> <p>新規の役割: <i>New Role</i></p> <p>「OK」をクリックしてこれらの変更を受け入れるか、「キャンセル」をクリックして変更せずに終了します。</p>
-----------------	---

GVM6079I	<p>IBM Spectrum Protect 管理 ID の現行の役割と新規の役割は次のとおりです。これらの変更を見直して、確認します。</p> <p>現行の IBM Spectrum Protect 権限レベル: <i>Current Level</i></p> <p>新規の IBM Spectrum Protect 権限レベル: <i>New Level</i></p> <p>現行の役割: <i>Current Role</i></p> <p>新規の役割: <i>New Role</i></p> <p>「OK」をクリックしてこれらの変更を受け入れるか、「キャンセル」をクリックして変更せずに終了します。</p>
-----------------	--

GVM6080I	ID は変更されましたが、保存されませんでした。以前の ID がロードされます。
-----------------	--

GVM6081I	<p>現行の UI 役割では、VMCLI ノードのアンロックまたはリセットは許されません。変更を行うには、「サーバー資格情報」ページに進み、VMCLI ノードの更新に必要な特権を持つ IBM Spectrum Protect 管理 ID およびパスワードを入力してください。「OK」を選択してこれらの資格情報を保存してから、「構成設定」ノートブックを再度開くと、VMCLI ノード更新を行えます。</p>
-----------------	---

GVM6082I	<p>現行の UI 役割では、その他のパネルへのアクセスは許されません。「OK」を選択してこれらの資格情報を保存してから、「構成設定」ノートブックを再度開くと、他の更新を行えます。</p>
-----------------	--

GVM6083I	1 つ以上のデータ・センターに英語以外の文字が含まれています。ドメインは、適宜調整されます。
-----------------	--

GVM6084E	データ・センター <i>DataCenter Name</i> をドメインに追加できません。英語以外の文字が含まれているためです。
-----------------	---

説明

英語以外の文字が含まれているデータ・センターは、現在、サポートされていません。したがって、それらはドメインに追加できません。

ユーザーの処置

データ・センターはドメインに追加されません。

GVM6085W	ノード Node Name がサーバー上に既に存在しています。ノードの名前を New Node Name に変更しますか?
-----------------	---

説明

ノード名は、既に IBM Spectrum Protect サーバーに登録されています。

ユーザーの処置

ノードの名前を変更する場合は「はい」をクリックします。他の変更を行う場合は「いいえ」をクリックします。例: レジスター・ノードのクリックを解除して、ノードの名前を手動で変更します。

GVM6086W	ホスト Host Name の仮想マシンの名前 Invalid Virtual Machine Names に、サポートされない文字が含まれています。そのため、ユーザーの選択に関係なく、これらの仮想マシンはバックアップされません。これらの仮想マシンをバックアップするためには、名前変更する必要があります。
-----------------	--

説明

次の文字は、仮想マシンではサポートされません: ""'':;*?,<>/|.

ユーザーの処置

特定された仮想マシンを名前変更して、サポートされない文字を名前から削除してください。

GVM6087E	ホスト・クラスター Invalid Host Clusters の名前に、サポートされない文字が含まれています。これらのホスト・クラスターは、サポートされない文字を含んでいるため、バックアップ用として選択できません。これらのホスト・クラスターを名前変更するか、選択から削除してください。
-----------------	--

説明

次の文字は、ホスト・クラスター名ではサポートされません: ""'':;*?,<>/|.

ユーザーの処置

特定されたホスト・クラスターを名前変更して、サポートされない文字を名前から削除してください。あるいは、バックアップの選択から削除してください。

GVM6088E	ユーザーの選択により、空の、バックアップ用の仮想マシン・リストが作成されました。この問題は、選択されたすべての仮想マシンの名前に、サポートされない文字が含まれていることが原因が発生します。サポートされない文字が名前に含まれていない仮想マシンを選択するようにしてください。
-----------------	---

説明

次の文字は、仮想マシンではサポートされません: ""'':;*?,<>/|. これらの文字を含む仮想マシン名は、バックアップ・タスク定義から自動的に削除されます。この削除により、空のタスク定義が作成される可能性があります。

ユーザーの処置

特定された仮想マシンを名前変更して、サポートされない文字を名前から削除してください。あるいは、バックアップする別の仮想マシンを選択してください。

GVM6089E	フィルター・パターンは、サポートされない文字を含んでいるため、適用できません。サポートされない文字を削除するようにパターンを変更してから、再度フィルターを適用してください。
-----------------	--

説明

次の文字は、フィルター・パターンではサポートされません: ""'':;*?,<>/|.

ユーザーの処置

サポートされない文字を削除するようにフィルター・パターンを変更してから、再度フィルターを適用してください。

GVM6090E	この操作を実行するために、一時データ・ストアを使用できません。リストアの宛先データ・ストアに加えて、この一時データ・ストアが必要です。
-----------------	---

説明

この操作の一時的なリストア宛先として使用するために、データ・ストアが必要です。この一時データ・ストアは、実際のリストア宛先に使用されるデータ・ストアと同じ ESX ホストにある必要があります。ただし、その一時データ・ストアは、実際のリストア宛先に使用

されるものと同じデータ・ストアであってはいりません。

ユーザーの処置

データ・ストアを宛先 ESX ホストに追加します。そして、そのデータ・ストアを一時リストア宛先として選択します。

GVM6091E **opt** ファイル *file name* の作成中にエラーが発生しました。

説明

ファイルへの書き込みを試行中にエラーが検出されました。

ユーザーの処置

操作を再試行してください。

GVM6092E **service** の作成に失敗しました。データ・ムーバー・ノード *node name* に対してサービスが作成されませんでした。

説明

指定されたデータ・ムーバー・ノードに対する IBM Spectrum Protect サービスの作成を試行中に、エラーが検出されました。

ユーザーの処置

ご使用の環境を確認してください。また、ユーザーが操作を再試行する前に、ユーザーが適切な権限を持っていることを確認してください。

GVM6093E **service** 用のファイアウォールの作成に失敗しました。インストールされたサービスに対して、ファイアウォール・ルールを手動で追加してください。

説明

指定された実行可能ファイルに関するファイアウォール・ルールの追加を試行中に、エラーが発生しました。

ユーザーの処置

ご使用の環境を調べて、ユーザーが適切な権限を持っていることを確認してから、操作を再試行します。または、IBM Spectrum Protect クライアント・アクセプター、IBM Spectrum Protect エージェント、および IBM Spectrum Protect スケジューラーに対するルールをファイアウォールに手動で追加します。

GVM6094W ローカル・サービスが正常にセットアップされましたが、次の実行可能ファイルに対するファイアウォール

ル・アクセスを検証できませんでした:

agentExe
cadExe
schedExe

ローカル・サービスに関連して問題が発生した場合は、これらの実行可能ファイルに対してファイアウォール・アクセスが可能になっていることを確認してください。

説明

Microsoft ファイアウォールが無効になっているか、別のファイアウォールが適用されている可能性があります。

ユーザーの処置

環境を確認し、必要な場合は IBM Spectrum Protect クライアント・アクセプター、IBM Spectrum Protect エージェント、および IBM Spectrum Protect スケジューラーに対するルールを手動で追加します。

GVM6095E データ・ムーバー・ノード *node name* がサーバーに正常に登録されましたが、サービスが作成されませんでした。

説明

指定されたノードに対するサービスの作成を試行中に、エラーが発生しました。

ユーザーの処置

ご使用の環境を確認してください。また、ユーザーが操作を再試行する前に、ユーザーが適切な権限を持っていることを確認してください。

GVM6096E 理由コード *reason*
このエラーは、IBM Spectrum Protect データ・ムーバーによって報告されました。その他の説明はありません。詳しくは、アドレス '*address*' のデータ・ムーバー・ホスト・マシン *hostname* 上のエラー・ログ *errorLog* を確認してください。

説明

データ・ムーバーで、報告された理由コードを持つエラーが発生しました。

ユーザーの処置

指定されたホスト・マシンにログインしてエラー・ログを表示し、詳細情報を確認してください。

GVM6097W スキャン・スケジュール *schedule name* がサーバー上で正常に定義され、ノード *node name* に関連付けられましたが、スケジュールを実行するためのサービスが作成されませんでした。
詳細: **error**

説明

VMCLI ノード用の IBM Spectrum Protect サービスの作成を試行中に、次のいずれかのステップでエラーが検出されました。

1. VMCLI ノード用のオプション・ファイルを作成する。
2. VMCLI ノードのパスワードを次のステップ用の一時パスワードに設定する。
3. IBM Spectrum Protect クライアント・サービス構成ユーティリティーを実行してサービスを作成する。
4. IBM Spectrum Protect クライアント・サービス構成ユーティリティーを実行してクライアント・アクセプター・サービスを開始する。
5. VMCLI ノードのパスワードを再設定する。

ユーザーの処置

スケジュールを削除し、スケジュールを再作成してサービスを自動的に構成するか、手動でサービスを構成します。ご使用の環境を確認してください。また、ユーザーが操作を再試行する前に、ユーザーが適切な権限を持っていることを確認してください。

GVM6098W スキャン・スケジュール *schedule name* がサーバー上で正常に定義され、ノード *node name* に関連付けられましたが、スケジュールを実行するための **IBM Spectrum Protect** サービスが作成されました。ただし、**VMCLI** ノード・パスワードの再設定に失敗しました。
詳細: **error**

説明

VMCLI ノード・パスワードの再設定を試行中に、エラーが検出されました。

ユーザーの処置

構成設定を使用して、VMCLI ノード・パスワードを再設定します。

GVM6099W 警告: このタスクが取り消されると、リストアが不完全な仮想マシン上の作成済みデータはすべて失われ、その仮想マシンは **ESX** ホストから削除されます。
このタスクを取り消しますか?

説明

タスクの取り消しコマンドが実行依頼されます。取り消しの進行状況を確認するには、最新表示してください。

ユーザーの処置

選択したタスクを取り消すか、タスクに対して処理の続行を許可してください。

GVM6100W 取り外し操作によって **iSCSI** ディスクが削除されますが、**VM** やそのデータは削除されません。取り外しを続行する前に、以下の条件が存在することを確認してください。
-マウントされた **iSCSI** ディスクがリカバリーされている。
-ストレージ **vMotion** が **VM** からローカル・データ・ストアへのマイグレーションを完了している。
リカバリー操作が失敗し、**VM** およびそのデータを削除して **iSCSI** ターゲットを取り外す場合、「取り外しと削除」をクリックします。「取り外しと削除」は破壊アクションであり、インスタント・リストア操作の成功または失敗に関わらず、**VM** とそのデータを削除します。
この情報に基づいて、インスタント・リストア用に選択されている **VM** を取り外しますか?

説明

取り外し操作によって **iSCSI** ディスクが削除されますが、**VM** やそのデータは削除されません。取り外しを続行する前に、以下の条件が存在することを確認してください。-マウントされた **iSCSI** ディスクがリカバリーされている。ストレージ **vMotion** が **VM** からローカル・データ・ストアへのマイグレーションを完了している。リカバリー操作が失敗し、**VM** およびそのデータを削除して **iSCSI** ターゲットを取り外す場合、「取り外しと削除」をクリックします。「取り外しと削除」は破壊アクションであり、インスタント・リストア操作の成功または失敗に関わらず、**VM** とそのデータを削除します。

ユーザーの処置

「取り外し」をクリックして、インスタント・リストア操作用に選択されている仮想マシンを取り外します。「取り外しと削除」をクリックして、インスタント・リストア操作用に選択されている仮想マシンを取り外し、**ESX** ホストから削除して、ストレージ **vMotion** が実行されていないことを確認します。

GVM6101W 取り外し操作中に、仮想マシン上の作成済みデータはすべて失われ、その仮想マシンは **ESX** ホストから削除されます。

選択したインスタント・アクセス仮想マシンを取り外しますか？

説明

仮想マシン上の作成済みデータはすべて失われ、その仮想マシンは ESX ホストから削除されます。

ユーザーの処置

インスタント・アクセス仮想マシンを取り外す (クリーンアップする) には、「取り外し」をクリックします。

GVM6102E	異なるリストア・タイプで複数の仮想マシンを選択することは許可されていません。
-----------------	--

説明

異なるリストア・タイプの複数の仮想マシンのリストアはサポートされません。

ユーザーの処置

同じリストア・タイプの仮想マシンを選択してください。

GVM6103I	クリーンアップ・タスク <i>Task ID</i> が正常に開始されました。このタスクをモニターしますか？
-----------------	--

GVM6104W	このタスクを取り消しますか？
-----------------	----------------

説明

タスクの取り消しコマンドが実行依頼されます。取り消しの進行状況を確認するには、最新表示してください。

ユーザーの処置

選択したタスクを取り消すか、タスクに対して処理の続行を許可してください。

GVM6105I	現行の UI 役割では、バックアップ・プロパティ・ノートブックの参照は許可されていません。
-----------------	---

GVM6106I	現行の UI 役割では、ノードの編集は許可されていません。変更を加えるには、「構成設定」ノートブックを開いて「サーバー資格情報」ページに進み、ノードの更新に必要な特権を持つ IBM Spectrum Protect 管理 ID およびパスワードを入力してください。
-----------------	---

GVM6107E	理由コード <i>reason</i> このエラーは、 IBM Spectrum Protect データ・ムーバーによって報告されました。その他の説明はありません。詳しくは、データ・ムーバ
-----------------	--

ー・ホスト・マシン上のエラー・ログ「**dsmerror.log**」を確認してください。

説明

データ・ムーバーで、報告された理由コードを持つエラーが発生しました。

ユーザーの処置

データ・ムーバーがあるホスト・マシンにログインしてエラー・ログを表示し、詳細情報を確認してください。

GVM6108W	vCenter のログイン情報が必要です。
-----------------	------------------------------

説明

新規ローカル・データ・ムーバー (DM) サービスをインストールするには、vCenter 資格情報が必要です。

ユーザーの処置

続行するには vCenter 資格情報を入力してください。

GVM6109E	GUI にアクセスするために必要な特権がありません。
-----------------	-----------------------------------

説明

GUI コンテンツにアクセスするためには、ユーザーは必要な vSphere 特権を持っていない必要があります。

ユーザーの処置

ユーザーに必要な特権を追加してください。

GVM6110E	GUI にアクセスするために必要な権限がありません。
-----------------	-----------------------------------

説明

GUI コンテンツにアクセスするためには、ユーザーは必要な vSphere 権限を持っていない必要があります。

ユーザーの処置

ユーザーに必要な権限を追加してください。

GVM6111I	新規データ・センター (<i>name</i>) が検出されました。「データ・ムーバー・ノード」ページに進み、対応するデータ・センター・ノードを追加します。
-----------------	--

GVM6112W	以下の共有およびマウントが削除され、その中にあるデータにエンド・ユーザーはアクセス不能になります。 選択した共有およびマウントを取り外しますか? mounts
-----------------	--

説明

選択された共有およびマウントが削除されます。

ユーザーの処置

共有およびマウントを取り外す (クリーンアップする) には、「取り外し」をクリックします。

GVM6113I	取り外しタスク Task ID が正常に開始されました。このタスクをモニターしますか?
GVM6114W	オプション・ファイル file name の削除操作中にエラーが検出されました。

説明

削除操作中にエラーが検出されました。例えば、このエラーの原因として、不十分なユーザー権限、あるいはファイルが存在しなくなっていることが考えられます。

ユーザーの処置

オプション・ファイルが削除されたことを確認してください。このファイルがまだ存在する場合は、ファイルを手動で削除します。

GVM6115W	IBM Spectrum Protect サービス service の削除操作が失敗しました。
-----------------	---

説明

エラーのために、IBM Spectrum Protect サービスを削除できませんでした。

ユーザーの処置

環境を調べて、ユーザーにこの操作を実行する十分な権限があることを確認します。その後、操作を再試行してください。

GVM6116E	マウント・プロキシー・ノード node name の iSCSI を開始できません。
-----------------	--

説明

指定されたマウント・プロキシー・ノードの **iSCSI** サービスの開始を試行中に、エラーが検出されました。

ユーザーの処置

iSCSI サービスを手動で開始します。

GVM6117E	サーバー資格情報が無効か、必要な SSL 証明書を取得できなかったため、 IBM Spectrum Protect サーバーに接続できませんでした。
-----------------	--

説明

サーバーに接続するには **IBM Spectrum Protect** サーバーの正しいユーザー ID とパスワード、および **SSL** 証明書が必要です。

ユーザーの処置

「構成」>「タスク」>「**IBM Spectrum Protect** 構成の編集」>「サーバー資格情報」ノートブック・ページに進みます。ログイン資格情報が正しいことと、**IBM Spectrum Protect** 管理ポートに正しいポート番号が入力されていること、および「**SSL** の使用...」チェック・ボックスが選択されていることを確認します。サーバーの証明書を取得し、「詳細情報...」リンクに記載された手順を使用してトラストストアが作成されている必要があります。

GVM6118E	複数のプロバイダー VDC から組織 VDC を選択しました。バックアップ・タスクの場合は、選択されたすべての組織 VDC が同じプロバイダー VDC に属している必要があります。選択項目を変更して、操作をやり直してください。
-----------------	---

GVM6119E	次に示す vcloud リソース (vApp 、組織、組織 vDC) は、名前にサポートされない文字が含まれているので、選択対象として無効です: reslist
-----------------	---

説明

バックアップ・タスクを作成するには、**vcloud** リソース名に次のいずれかの文字が含まれていてはなりません: ""':;*?,<>|/.

ユーザーの処置

示されているリソースの名前を変更して、サポートされない文字を名前から削除します。あるいは、バックアップの選択から削除してください。

GVM6120E	異なる組織 VDC から vApp を選択しました。リストア・タスクの場合は、選択されたすべての vApp が同じ組織 VDC に属している必要があります。選択項目を変更して、操作をやり直してください。
-----------------	---

GVM6121E	vApp vApp name は存在します。リストアのターゲットとなる別の vApp 名を選択してください。
-----------------	---

GVM6122E	バックアップする項目の選択の結果、バックアップ・タスク定義で count 文字が必要になりましたが、これは 512 文字の制限を超えています。複数のバックアップ・タスクを
-----------------	---

作成して、タスク当たりの項目数を少なくします。

説明

バックアップ・タスクの定義には 512 文字の長さ制限があり、選択された項目の合計文字数がこの制限を超えています。

ユーザーの処置

複数のバックアップ・タスクを作成して、タスク当たりの項目数を少なくします

GVM6123E	組織 VDC ノードは、そのプロバイダー VDC ノードが組み込まれていないために組み込むことができません。最初に、プロバイダー VDC ノードの組み込み用チェック・ボックスを選択して、再試行してください。
GVM6124E	ノード名 <i>node name</i> は既に使用されています。「ノードの登録」チェック・ボックスのチェック・マークを外すか、別のノード名を選択してください。

説明

選択されたノード名はサーバーに既に存在しています。このノードを登録しないことを選択するか、別の名前を使用してください。

ユーザーの処置

使用する別のノード名を選択してください。この既存のノードを再使用する場合は、「ノードの登録」チェック・ボックスを選択解除してください。

GVM6125W	データ・ムーバー・ノード <i>node name</i> を本当に削除しますか?
GVM6126W	IBM Spectrum Protect ノード <i>node</i> は既に使用されています。デフォルト名以外の別の名前を使用する場合は、このフィールドを再編集してください。

説明

ノードは、この構成で既に使用されています。

ユーザーの処置

別のノード名を試してください。

GVM6127E	プロバイダー VDC が無効なため、組織 VDC ノードは登録できません。
GVM6128E	組織 VDC 名 <i>OVDC name</i> は無効です。サポートされる文字について詳しくは、「IBM Spectrum Protect 管

理者のための解説書」で **IBM Spectrum Protect** オブジェクトの命名に関するセクションを参照してください。

GVM6129I	このタスクは必要ないために、スキップされました。これ以上のアクションは不要です。
GVM6130W	Internet Explorer のバージョン <i>version</i> はサポートされていません。サポートされているバージョンまたは別のブラウザを利用してください。サポートされないこのブラウザの使用を続行すると、表示上の問題や機能上の問題が発生することがあります。

説明

Internet Explorer の実装はバージョン番号ごとに相違があるため、特定のバージョンのみがサポートされます。標準準拠ブラウザ (Mozilla Firefox など) の使用が推奨されています。ただし、vSphere クライアントからプラグインとして GUI にアクセスしている場合には、vSphere クライアントがインストールされているシステムにインストールされた Internet Explorer ブラウザーを使用するよう限定されます。

ユーザーの処置

サポートされるバージョンの Internet Explorer または他のブラウザを使用してください。サポートされるブラウザ・バージョンは、オンライン・ヘルプに記載されています。

GVM6131W	ブラウザ <i>version</i> はサポートされていません。サポートされているブラウザを利用してください。サポートされないこのブラウザの使用を続行すると、表示上の問題や機能上の問題が発生することがあります。
-----------------	--

説明

ブラウザの実装には相違があるため、特定のバージョンのみがサポートされます。

ユーザーの処置

サポートされるブラウザを利用してください。サポートされるブラウザ・バージョンは、オンライン・ヘルプに記載されています。

GVM6132E	代替の位置へのリストアのために選択した少なくとも 1 つの仮想マシンが既にデータ・センターに存在するため、リストアは行えません。宛先仮想マシンが既に存在する場合に代
-----------------	--

替の位置にリストアするには、リストア操作に 1 つだけ仮想マシンを選択し、宛先仮想マシンの新規名を選択します。重複する **VM: VM name**

説明

代替の位置にリストアする場合、宛先仮想マシンが既に存在してはなりません。

ユーザーの処置

単一の仮想マシン・リストア・ウィザードを使用することで、宛先仮想マシン名を変更することができます。

GVM6133W	ターゲットのデータ・ストアが見つかりません。別の宛先データ・ストアを選択してください。
GVM6134E	ユーザー <i>User Name</i> が管理対象データ・センターに対する権限がありません。システム管理者にお問い合わせください。
GVM6135E	このイベントについて仮想マシンを表示するために必要な許可がありません。
GVM6136E	この仮想マシンのリストア・ポイントを表示するために必要な許可がありません。
GVM6137E	一部の接続済みポイントを表示するために必要な許可がありません。
GVM6138E	このデータ・ストアのリストア・ポイントを表示するために必要な許可がありません。
GVM6139E	リストア・ポイントを切り離すために必要な許可がありません。
GVM6140E	ユーザー許可の処理中にエラーが発生しました。システム管理者にお問い合わせください。
GVM6141I	許可要件のために、一部のデータ・センターが表示されません。
GVM6142E	このタスクをキャンセルするための許可がありません。
GVM6143I	タスクはまだ開始状態にあります。タスクを更新して、取り消しを再試行してください。
GVM6147I	1 つ以上のデータ・センターと同じ名前を持っているために使用できないデータ・センターがあります。同じ名前のデータ・センターはサポートされていません。

GVM6148E	Windows ドメイン資格情報が誤っています。構成ウィザードを開き、「ファイル・リストア」ページに移動し、資格情報の入力を再試行します。
-----------------	---

説明

構成ウィザードの「ファイル・リストア」ページに入力された Windows ドメイン資格情報が間違っています。

システムの処置

処理は停止します。

ユーザーの処置

構成ウィザードを再実行して、正しい Windows ドメイン資格情報を再入力してください。

GVM6149E	VMCLI ノードが定義されていないために、このアクションを実行できません。解決するには、構成ウィザードを使用して VMCLI ノードを定義し、他のステップもウィザード内で実行します。
GVM6150E	vCloud Director ノードが定義されていないために、このアクションを実行できません。解決するには、構成ウィザードを使用して vCloud Director ノードを定義し、他のステップもウィザード内で実行します。
GVM6151E	IBM Spectrum Protect サーバーへの接続が動作していないために、このアクションを実行できません。接続の問題を修正して、このアクションを再試行してください。
GVM6152E	このタスクを実行するには、 IBM Spectrum Protect からプロバイダー VDC ノード <i>provider VDC node name</i> を使用する必要がありますが、このノードは vCloud Director 内で既知のプロバイダー VDC にマップされていません。このタスクは更新されない可能性があります。代わりに、このプロバイダー VDC に依存しない新規タスクを作成してください。
GVM6153E	次にリストする組織 VDC が選択されましたが、これらは IBM Spectrum Protect サーバーに対して構成されていません。このアクションを実行するには、これらの選択を削除する必要があります。 <i>org VDC name</i>
GVM6154I	現行の UI 役割では、ノード詳細の参照は許可されていません。

GVM6155E IBM Spectrum Protect サーバー *server name* への接続中にエラーが発生しました。管理者 ID またはパスワードが無効であるか、管理者ポート・フィールドに **TCPADMINPORT** 番号または **SSLTCPADMINPORT** 番号ではなく **TCPPORT** 番号が入力されました。

説明

メッセージを参照してください。

ユーザーの処置

「構成」タブから構成エディターを起動し、IBM Spectrum Protect サーバーに対して有効な ID またはパスワードを入力します。

GVM6156E IBM Spectrum Protect サーバー *server name* の管理ユーザー ID *admin id* のパスワードの有効期限が切れました。

説明

IBM Spectrum Protect の管理パスワードの有効期限が切れています。

ユーザーの処置

IBM Spectrum Protect サーバー管理者に連絡して、管理ユーザー ID のパスワードの再設定を依頼してください。

GVM6157E IBM Spectrum Protect サーバー・ポート番号 *tcp port* は正しくありません。このポートの予想値は、*tcp port from query* です。これは、**TCPPORT** オプションの値です。構成ウィザードを使用して、期待される値を入力してください。

説明

IBM Spectrum Protect サーバーのポート・フィールドに入力する値は、IBM Spectrum Protect サーバーの **TCPPORT** オプションに一致する必要があります。

ユーザーの処置

構成ウィザードを使用して、IBM Spectrum Protect サーバーのポート・フィールドを正しい値に変更します。

GVM6159E VMCLI コマンドの処理中にエラーが発生しました。GUI セッションは閉じられます。ログインして、操作を再試行してください。問題が解決しない場合は、管理者にお問い合わせください。

GVM6160E **frConfig.props** 構成ファイルへの書き込み中にエラーが発生しました。

説明

frConfig.props ファイルには、ファイル・レベル・リストア処理の構成オプションが含まれています。このエラーの理由として、以下の状態が考えられます。

- **frConfig.props** ファイルが Data Protection for Virtual Environments インストール・ディレクトリーにない。
- **frConfig.props** ファイルが書き込み保護されている。

システムの処置

処理は停止します。

ユーザーの処置

ファイルが Data Protection for Virtual Environments インストール・ディレクトリー内に存在していること、およびファイルが書き込み保護されていないことを確認します。

GVM6161E ファイル・レベル・リストア機能が有効になっている場合、ローカル・マウント・プロキシ・ノード・ペアを削除することはできません。

説明

ファイル・レベル・リストア処理には、ローカル・マウント・プロキシ・ノードが必要です。

ユーザーの処置

ファイル・レベル・リストア機能を無効にします。その後、マウント・プロキシ・ノード・ペアを削除するかどうかを選択します。

GVM6162E **frConfig.props** 構成ファイルの読み取り中にエラーが発生しました。

説明

frConfig.props ファイルには、ファイル・レベル・リストア処理の構成オプションが含まれています。ファイルを読み取ることができません。このエラーの一般的な理由は、ファイルが読み取り保護されていることです。

システムの処置

処理は停止します。

ユーザーの処置

ファイルが読み取り保護されていないことを確認します。

GVM6164W セキュリティー証明書が必要であるため、**IBM Spectrum Protect** サーバーに接続できませんでした。

説明

IBM Spectrum Protect サーバーとのセキュア接続には、接続を作成するための SSL 証明書が必要です。選択された IBM Spectrum Protect サーバーの証明書が見つかりませんでした。

ユーザーの処置

構成ウィザードの一部としてこのメッセージが表示された場合、SSL 証明書を取得して、このヘルプに記載された手順を使用してトラストストアを作成する必要があります。

GVM6165E 指定されたターゲット・ノード '**node-name**' は、ユーザー・セッションに保管されているノード '**node-name**' と一致しません。

説明

ホスト構成操作への入力ターゲット・ノードが接続セッションで保管されているターゲット・ノードと一致しません。

ユーザーの処置

正しいターゲット・ノード名で操作を再試行してください。

GVM6166E ユーザー・セッションが無効であるか、受け入れる SSL 証明書がありません。

説明

IBM Spectrum Protect サーバーの初期接続が SSL 証明書が必要であることを検出したために、この操作は同じ接続で再度呼び出す必要があります。この場合、接続は NULL であるか無効です。

ユーザーの処置

証明書を受け入れるための 2 度目の操作呼び出しが同じ初期接続を使用していることを確認してください。

GVM6167E **Windows** マウント・プロキシ・ノードおよび **Linux** マウント・プロキシ・ノードは、ファイル・リストアを有効にすることが必要です。

説明

ホスト構成操作で、マウント・プロキシ・ノードが 1 つ指定されているか、またはいずれのプロキシ・ノードも指定されていません。

ユーザーの処置

Windows マウント・プロキシ・ノードおよび **Linux** マウント・プロキシ・ノードが含まれるノード・リストを使用して操作を再試行してください。

GVM6168E ホストの構成に失敗しました。詳しくは、タスク・リストを確認してください。

説明

ホストの構成には、ターゲット・ノードの登録、データ・ムーバーの登録とバックアップとリストア用のサービスの作成、マウント・プロキシ・ノードの登録とファイル・レベル・リストア用のサービスの作成が含まれています。これらのタスクのいずれかでエラーが発生しました。

ユーザーの処置

エラーを修正し、操作を再試行してください。

GVM6169E **IBM Spectrum Protect** サーバーの構成中に予期しないエラーが発生しました。

説明

このエラーの理由として、以下の状態が考えられます。

- IBM Spectrum Protect サーバーへの接続を試行中に不明エラーが発生した。
- サーバー・データベース・ファイル **tsmsrvr.props** の書き込みの試行中に不明エラーが発生した。

ユーザーの処置

IBM Spectrum Protect サーバー・マシンとのネットワーク接続を確認します。サーバーが稼働していることを確認して、ログインを再試行してください。また、サーバー・ポート情報が正しいことを確認してください。

GVM6170E 予期しないエラーが発生しました。ノード '**node-name**' のポリシー・ドメインを取得できません。

説明

ターゲット・ノードが IBM Spectrum Protect サーバーに存在しないか、ノード照会中に内部エラーが発生しました。

ユーザーの処置

構成ウィザードを実行してターゲット・ノードを登録するか、ノードを別のポリシー・ドメインに更新してください。

GVM6171E	予期しないエラーが発生しました。スケジュール ' schedule-name ' が IBM Spectrum Protect サーバーに存在していません。	GVM6175E	HTTP 応答の TCP ポートを取得できません。 TSM クライアント・アクセプター (CAD) が稼働中であることを確認してください。
説明 スケジュールは操作中に誤って削除された可能性があります。		説明 このデータ・ムーバーの CAD サービスが実行されていません。	
ユーザーの処置 別のスケジュールを選択してください。		システムの処置 データ・ムーバー CAD サービスへの接続がないと操作は続行できません。	
GVM6172E	' domain-name ' は無効な Windows ドメインです。	GVM6176E	HTTP 応答の TCP ポートを解析したり検出したりすることができません。
説明 LOCALHOST またはコンピューター名は無効なドメインです。		説明 データ・ムーバー CAD サービスが実行されていること、ノードに適切なプロキシ関係が確立されていることを確認してください。	
ユーザーの処置 有効なドメインを入力してください。		ユーザーの処置 データ・ムーバー CAD サービスが実行されていること、ノードに適切なプロキシ関係が確立されていることを確認してください。	
GVM6173E	ユーザー名からドメインが欠落しています。	GVM6177E	TCP ポート・ストリング tcpport の解析中に例外が発生しました。
説明 入力されたユーザー名は、ドメインの一部ではありません。		説明 エージェントからの HTTP ストリームに TCP ポート番号が含まれていません。	
ユーザーの処置 ユーザー名は DOMAIN¥UserName フォーマットであることを確認してください。		システムの処置 データ・ムーバー CAD サービスへの接続がないと操作は続行できません。	
GVM6174E	アドレス httpurl 、 httpsurl に到達できません。 TSM クライアント・アクセプター (CAD) が稼働中であることを確認してください。	ユーザーの処置 データ・ムーバー CAD サービスが実行されていること、ノードに適切なプロキシ関係が確立されていることを確認してください。	
説明 このデータ・ムーバーの CAD サービスが実行されていません。		説明 エージェントの HTTP ストリームが無効な TCP ポート番号を返しました。	
システムの処置 データ・ムーバー CAD サービスへの接続がないと操作は続行できません。		システムの処置 データ・ムーバー CAD サービスへの接続がないと操作は続行できません。	
ユーザーの処置 データ・ムーバー CAD サービスが実行されていること、ノードに適切なプロキシ関係が確立されていることを確認してください。		ユーザーの処置 データ・ムーバー CAD サービスが実行されていること、ノードに適切なプロキシ関係が確立されていることを確認してください。	

付録 C IBM Spectrum Protect 製品ファミリーのアクセシビリティ機能

アクセシビリティ機能は、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。

概説

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 ファミリー製品は、最新の W3C 標準 [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/) が、[US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) (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](http://www.w3.org/TR/WCAG20/) (www.w3.org/TR/WCAG20/) に準拠するように使用されています。アクセシビリティ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、アクセシビリティに対応しています。IBM Knowledge Center のアクセシビリティ機能については、[the IBM Knowledge Center ヘルプの「Accessibility」セクション](http://www.ibm.com/support/knowledgecenter/about/releasesnotes.html#accessibility) (www.ibm.com/support/knowledgecenter/about/releasesnotes.html#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に対する取り組みについて詳しくは、[IBM Accessibility \(www.ibm.com/able\)](http://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を提供し、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認できません。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をお願いします。

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を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を提供され、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]

「アクション」ペイン

Data Protection for Microsoft Hyper-V 管理コンソール
73

アクセシビリティ機能 275

アップグレード

バージョンの互換性 15

ファイル・リストア用の Linux マウント・プロキシ 32

RCT バックアップ 20

アップグレード・タスク 15

アドホック・バックアップ

Data Protection for Microsoft Hyper-V 管理コンソール
79

アプリケーション保護

一般ヘルプ 127

概要 91

トラブルシューティング 126

VSS バックアップ操作およびリストア操作のトラブルシューティング 127

アプリケーション保護、Exchange Server の

Data Protection for Microsoft Exchange Server のインストールおよび構成 93

VM 名の変更後の構成 99

アプリケーション保護、Microsoft Exchange Server の

アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成 95

インストールおよび構成 91

概要 91

更新、メールボックス履歴情報の 101

スケジューリング、バックアップの 100

ステップ 1 の開始 92

ステップ 2 の開始 93

ステップ 3 の開始 95

ステップ 4 の開始 98

他の VM のバックアップのリストア 104

データのリストア 103

バックアップ、データの 100

バックアップの検証 102

表示、ファイル・スペース情報の 107

ボリュームが除外されていないことの確認 102

リストア、GUI を使用したデータベースの 103

リストア、コマンド・ラインを使用したデータの 105

リストア、コマンドレットを使用したデータの 106

リストア、データベースの 98

リストア、メールボックス・データの 104

Data Protection for Microsoft Hyper-V のインストールおよび構成 92

iSCSI サービスの開始 103

アプリケーション保護、Microsoft SQL Server の

アプリケーション保護のための Data Protection for Microsoft Hyper-V の構成 111

インストールおよび構成 108

概要 107, 108

管理、バックアップのバージョンの 118

アプリケーション保護、Microsoft SQL Server の (続き)

スケジューリング、SQL Server ログ・バックアップの 117

スケジューリング、バックアップの 116

ステップ 1 の開始 108

ステップ 2 の開始 109

ステップ 3 の開始 111

ステップ 4 の開始 114

データのリストア 120

バックアップ、データの 116

バックアップの検証 117

表示、ファイル・スペース情報の 125

ボリュームが除外されていないことの確認 119

リストア、GUI を使用したデータベースの 120

リストア、SQL Server ログ・バックアップの 123

リストア、コマンド・ラインを使用したデータベースの 121

リストア、再配置および削除されたデータベースの 123

リストア、データベースの 114

Data Protection for Microsoft Hyper-V のインストールおよび構成 108

Data Protection for Microsoft SQL Server のインストールおよび構成 109

iSCSI サービスの開始 120

VM バックアップを検証するためのスクリプト 124

アプリケーション保護、SQL Server の

VM 名の変更後の構成 115

アンインストール

Linux マウント・プロキシ 36

Server Core システムへの 31

アンインストール手順

サイレント 29

インスタント・アクセス

クリーンアップ 134

ホスト再始動の制約事項 138

リソースの除去 134

VM バックアップの検証 131

インスタント・アクセス VM の除去

Data Protection for Microsoft Hyper-V 管理コンソール
137

インスタント・アクセス操作の実行

Data Protection for Microsoft Hyper-V 管理コンソール
136

インストール

計画 13

ファイル・リストア用の Linux マウント・プロキシ 32

ホスト上のセキュリティ証明書 63, 139

Linux マウント・プロキシの概要 32

Server Core システムへの 30

インストール、サイレント・モードでの

ファイル・リストア用の Linux マウント・プロキシ 34

インストール・ウィザードを使用したアップグレード 21

インストールおよびアップグレード

概要 13

インストール可能な機能

Data Protection for Microsoft Hyper-V 13

インストール手順

インストール手順 (続き)

概要 [21](#)

計画 [13](#)

サイレント [28](#)

データ・ムーバー [26](#)

パッケージのダウンロード [22](#)

標準的 [22](#)

Data Protection for Microsoft Hyper-V 管理コンソール [24](#)

インストール・パッケージ

ダウンロード [22](#)

永久増分

description [8](#)

エラー [243](#)

オプション

ファイル・リストア [48](#)

dateformat [175](#)

detail [177](#)

domain.vmfll [177](#)

EXCLUDE.VMDISK [180](#)

inactive [182](#)

include.vm [183](#)

INCLUDE.VMDISK [184](#)

include.vmsnapshotattempts [186](#)

include.vmtsmvss [187](#)

mbobjrefreshthresh [191](#)

mbpctrefreshthresh [192](#)

mode [190](#)

noprompt [193](#)

numberformat [193](#)

pick [195](#)

pitdate [195](#)

pittime [195](#)

skipsystemexclude [196](#)

timeformat [197](#)

vmautostartvm [198](#)

vmbackdir [199](#)

vmbackupupdateguid [155](#)

vmmaxbackupsessions [200](#)

vmmaxparallel [202](#)

vmmaxparallelrestorevms [206](#)

vmmaxpersnapshot [203](#)

vmmaxrestoreparalleldisks [205](#)

vmmaxrestoresessions [210](#)

vmmaxsnapshotretry [212](#)

vmmaxvirtualdisks [213](#)

vmmc [214](#)

vmprocessvmwithphysdisks [215](#)

vmrestoretype [218](#)

vmskipmaxvirtualdisks [216](#)

vmskipphysdisks [217](#)

オプションの解説 [175](#)

オンライン・ヘルプ

PowerShell コマンドレット [141](#)

[力行]

開始

Data Protection for Microsoft Hyper-V 管理コンソール [63](#)

概要

アプリケーション保護 [91](#)

ノード [6](#)

保護、Exchange Server データの [91](#)

概要 (続き)

保護、SQL Server データの [107](#)

ポリシー管理 [8](#)

ユーザー・インターフェース [5](#)

Data Protection for Microsoft Hyper-V [1](#)

Data Protection for Microsoft Hyper-V 管理コンソール [63](#)

Hyper-V VM のバックアップ [1](#)

Hyper-V VM のリストア [4](#)

Hyper-V 環境 [5](#)

RCT を使用した VM のバックアップ [2](#)

VSS を使用した VM バックアップ [1](#)

カスタマイズ

ノード [18](#)

「仮想マシン」ビュー

Data Protection for Microsoft Hyper-V 管理コンソール [65](#)

管理、バックアップのバージョンの

保護、SQL Server データの [118](#)

管理クラス [8](#)

キーボード [275](#)

危険ポリシーの設定

Data Protection for Microsoft Hyper-V 管理コンソール [76](#)

グループ・バックアップ

活動/非活動オブジェクトの表示 [182](#)

「結果」ペイン

Data Protection for Microsoft Hyper-V 管理コンソール [65](#)

更新、メールボックス履歴情報の

保護、Exchange Server データの [101](#)

更新

ノード [16](#)

構成

概要 [39](#)

拡張タスク [59](#)

クラスター [39](#)

初期構成 [39](#)

スタンドアロン・ホスト [39](#)

セキュリティ設定 [39, 42](#)

デフォルトのポート番号 [59](#)

ファイル・リストア [39, 44](#)

ファイル・リストア・オプション [48](#)

ファイル・リストア用の Linux マウント・プロキシ [45](#)

IBM Spectrum Protect リカバリー・エージェント GUI

[51](#)

iSCSI マウント [57](#)

構成ウィザード

クラスター [39](#)

スタンドアロン・ホスト [39](#)

ファイル・リストア [39](#)

構成の検証

Data Protection for Microsoft Hyper-V 管理コンソール [74](#)

構文図

繰り返し値 [151](#)

必須選択項目 [151](#)

読み方 [151](#)

コマンド

マウント [229](#)

backup vm [153](#)

expire [160](#)

query VM [161](#)

restore vm [165](#)

コマンド (続き)

set_connection [233](#)

[サ行]

サーバーとのセキュア通信の使用可能化

TLS の構成 [54-56](#)

最大 VHDX サイズ

指定 [213](#)

処理方法 [216](#)

最大 VHDX サイズの指定 [213](#)

サイレント・アンインストール [29](#)

サイレント・インストール

データ・ムーバーのみ [28](#)

Data Protection for Microsoft Hyper-V 管理コンソールの
み [28](#)

削除、ファイル・リストア [36](#)

自己完結型アプリケーション保護 [187](#)

時刻形式

指定 [197](#)

システム 状態

活動/非活動オブジェクトの表示 [182](#)

資料 [vii, 10](#)

身体障害 [275](#)

スケジューリング、SQL Server ログ・バックアップの

保護、SQL Server データの [117](#)

スケジューリング、バックアップの

保護、Exchange Server データの [100](#)

保護、SQL Server データの [116](#)

スケジュールの設定

Data Protection for Microsoft Hyper-V 管理コンソール
[75](#)

スケジュール・ヒストリーの表示

Data Protection for Microsoft Hyper-V 管理コンソール
[77](#)

「スケジュール・ヒストリー」ビュー

Data Protection for Microsoft Hyper-V 管理コンソール
[68](#)

スナップイン

Data Protection for Microsoft Hyper-V 管理コンソール
[63](#)

スナップショット

マウント [222](#)

スナップショット管理 [8](#)

スナップショットの管理 [8](#)

スナップショットのマウント [222](#)

制御ファイル [199](#)

静止アプリケーション [187](#)

セキュリティ証明書のインポート

V8.1.2 または V7.1.8 より後のサーバー [39](#)

V8.1.2 または V7.1.8 より前のサーバー [43](#)

セキュリティ設定

構成 [42](#)

V8.1.2 または V7.1.8 より後のサーバーに接続 [39](#)

V8.1.2 または V7.1.8 より前のサーバーに接続 [43](#)

前提条件ステップ

PowerShell コマンドレット [139](#)

[タ行]

ターゲット・ノード (target node)

概要 [6](#)

「タスク」ペイン

「タスク」ペイン (続き)

Data Protection for Microsoft Hyper-V 管理コンソール
[70](#)

他の VM のバックアップのリストア

保護、Exchange Server データの [104](#)

通信ポート [14](#)

ディスク・スペース所要量

Windows クライアント [13](#)

データのリストア

保護、Exchange Server データの [103](#)

保護、SQL Server データの [120](#)

データ・ムーバー・ノード

概要 [6](#)

との再接続

Data Protection for Microsoft Hyper-V 管理コンソール
[63](#)

ドメイン

フル VM バックアップに組み込む [177](#)

トラブルシューティング

アプリケーション保護 [126](#)

VSS バックアップ操作およびリストア操作 [127](#)

トレース

オプション [247](#)

構成 [247](#)

[ナ行]

「ナビゲーション」ペイン

Data Protection for Microsoft Hyper-V 管理コンソール
[64](#)

名前変更

ノード [16, 18](#)

ノード

概要 [6](#)

カスタマイズ [18](#)

更新 [16](#)

接頭部 [18](#)

接尾部 [18](#)

名前変更 [16](#)

マイグレーション [16](#)

[ハ行]

ハードウェア要件

Windows クライアント [13](#)

始めに

Exchange Server データの保護、ステップ 1 [92](#)

Exchange Server データの保護、ステップ 2 [93](#)

Exchange Server データの保護、ステップ 3 [95](#)

Exchange Server データの保護、ステップ 4 [98](#)

Exchange Server データの保護の概要 [91](#)

Microsoft SQL Server データの保護、ステップ 1 [108](#)

SQL Server データの保護、ステップ 2 [109](#)

SQL Server データの保護、ステップ 3 [111](#)

SQL Server データの保護、ステップ 4 [114](#)

SQL Server データの保護の概要 [108](#)

バックアップ

永久増分

description [8](#)

最大 8 TB の VHDX [213, 216](#)

制限 [9](#)

大容量 VHDX [213, 216](#)

パフォーマンス、最適化 [237](#)

- バックアップ (続き)
 - 複数の VM [239](#)
 - 並列 [200](#), [202](#), [239](#)
 - ポリシー管理 [8](#)
 - ユーザー・インターフェース
 - description [5](#)
 - RCT バックアップ
 - description [2](#)
 - VSS バックアップ
 - description [1](#)
- バックアップ、データの
 - 保護、Exchange Server データの [100](#)
 - 保護、SQL Server データの [116](#)
- バックアップ状況
 - Data Protection for Microsoft Hyper-V 管理コンソール [78](#)
- バックアップの検証
 - 保護、Exchange Server データの [102](#)
 - 保護、SQL Server データの [117](#)
- バックアップ・ヒストリー
 - Data Protection for Microsoft Hyper-V 管理コンソール [78](#)
- バックアップ・ポリシーの設定
 - Data Protection for Microsoft Hyper-V 管理コンソール [75](#)
- パフォーマンス、最適化
 - バックアップ操作 [237](#)
 - リストア操作 [239](#)
- 日付形式
 - 指定 [175](#)
- 表示、ファイル・スペース情報の
 - 保護、Exchange Server データの [107](#)
 - 保護、SQL Server データの [125](#)
- ファイル
 - リストア・タスク (Windows) [225](#)
 - リストアの概要 [223](#)
- ファイル・スペース [177](#)
- ファイル・リストア
 - アップグレード、Linux マウント・プロキシの [32](#)
 - アンインストール、Linux マウント・プロキシの [36](#)
 - オプション [48](#)
 - オプションの構成 [48](#)
 - 共通タスク [85](#)
 - 構成 [44](#)
 - サイレント・モードでの Linux マウント・プロキシのインストール [34](#)
 - 削除 [36](#)
 - 前提条件 [86](#)
 - 手順 [88](#)
 - トレースの構成 [247](#)
 - 役割 [85](#)
 - ロギング・オプション [50](#)
 - ロギングの構成 [49](#)
 - ログイン [88](#)
 - description [85](#)
 - Linux マウント・プロキシのインストール [32](#)
 - Linux マウント・プロキシのインストールの概要 [32](#)
 - Linux マウント・プロキシの構成 [45](#)
- プレビュー
 - restore vm [171](#)
- 並列バックアップ [200](#), [202](#)
- ベスト・プラクティス
 - VM の除外 [82](#)
- ポート番号

- ポート番号 (続き)
 - 構成 [59](#)
- ホスト上のセキュリティ証明書
 - インストール [63](#), [139](#)
- ボリューム
 - リストア・タスク (Windows) [225](#)
 - リストアの概要 [223](#)
- ボリュームが除外されていないことの確認
 - 保護、Exchange Server データの [102](#)
 - 保護、SQL Server データの [119](#)

[マ行]

- マイグレーション
 - ノード [16](#)
- マウントおよびファイル・リストア [221](#)
- マウント・プロキシ・ノード
 - 概要 [6](#)
- メールボックス履歴情報
 - Microsoft Exchange Server バックアップの更新 [101](#)
- メッセージ
 - ANS 接頭部 [249](#)
 - Data Protection for Microsoft Hyper-V [249](#)
 - GVM 接頭語 [249](#)
- メモリー所要量
 - Windows クライアント [13](#)
- 問題判別 [243](#)

[ヤ行]

- 要件
 - 通信ポート [14](#)

[ラ行]

- リストア
 - オプション [48](#), [50](#)
 - オプションの構成 [48](#)
 - 活動/非活動オブジェクトの表示 [182](#)
 - 前提条件 [86](#)
 - 手順 [88](#)
 - バックアップ、特定時点の確立 [195](#)
 - バックアップ・バージョンのリストの作成 [195](#)
 - パフォーマンス、最適化 [239](#)
 - ファイル [48-50](#), [86](#), [88](#)
 - ファイル・リストア・タスク [85](#)
 - ファイル・リストアの説明 [85](#)
 - ファイル・リストアの役割 [85](#)
 - 複数の VM [241](#)
 - 並列 VM [241](#)
 - ユーザー・インターフェース
 - description [5](#)
 - ロギングの構成 [49](#)
 - ログイン [88](#)
 - Hyper-V VM
 - description [4](#)
 - リストア、GUI を使用したデータベースの
 - 保護、Exchange Server データの [103](#)
 - 保護、Exchange SQL データの [120](#)
 - リストア、SQL Server ログ・バックアップの
 - 保護、SQL Server データの [123](#)
 - リストア、コマンド・ラインを使用したデータの
 - 保護、Exchange Server データの [105](#)

リストア、コマンド・ラインを使用したデータベースの
保護、SQL Server データの [121](#)
リストア、コマンドレットを使用したデータの
保護、Exchange Server データの [106](#)
リストア、再配置および削除されたデータベースの
保護、SQL Server データの [123](#)
リストア、メールボックス・データの
保護、Exchange Server データの [104](#)
ロギング
ファイル・リストア [49](#)
Data Protection for Microsoft Hyper-V 管理コンソール
[49](#)
ログ
アプリケーション・ログの切り捨て [187](#)

B

backup vm コマンド [153](#)

D

Data Protection for Microsoft Hyper-V
アップグレード [15](#)
インストール・ウィザードを使用したアップグレード
[21](#)
トラブルシューティング
診断手順 [246](#)
トレースの構成 [247](#)
比較可能性 [15](#)
Data Protection for Microsoft Exchange Server の使用
[127](#)
Server Core でのアンインストール [31](#)
Server Core へのインストール [30](#)
Data Protection for Microsoft Hyper-V V8.1.10 の新機能 [ix](#)
Data Protection for Microsoft Hyper-V 管理コンソール
「アクション」 ペイン [73](#)
アドホック・バックアップの実行 [79](#)
インスタント・アクセス・クリーンアップ [137](#)
インスタント・アクセス操作 [136](#)
開始 [63](#)
概要 [63](#)
「仮想マシン」 ビュー [65](#)
危険ポリシーの設定 [76](#)
「結果」 ペイン [65](#)
構成の検証 [74](#)
スケジュールの設定 [75](#)
スケジュール・ヒストリーの表示 [77](#)
「スケジュール・ヒストリー」 ビュー [68](#)
スナップインとして [63](#)
「タスク」 ペイン [70](#)
「ナビゲーション」 ペイン [64](#)
バックアップ状況の表示 [78](#)
バックアップ・ヒストリーの表示 [78](#)
バックアップ・ポリシーの設定 [75](#)
ロギング・オプション [50](#)
ロギングの構成 [49](#)
ログイン [63](#)
description [64](#)
VM のリストア [80](#)
Data Protection for Microsoft Hyper-V 管理コンソールの再接
続 [63](#)
Data Protection for Microsoft Hyper-V 管理コンソールへのロ
グイン [63](#)

Data Protection for Microsoft Hyper-V の概要 [1](#)
Data Protection for Microsoft Hyper-V の機能
インストール可能 [13](#)
dateformat オプション [175](#)
description
Data Protection for Microsoft Hyper-V 管理コンソール
[64](#)
detail オプション [177](#)
domain.vmfull オプション [177](#)

E

exclude
EXCLUDE.VMDISK [180](#)
EXCLUDE.VMDISK [180](#)
expire コマンド [160](#)

G

GUI の使用 [63](#)

H

Hyper-V VM のバックアップ [1](#)
Hyper-V コマンドレット [8](#)
Hyper-V スナップショット
削除 [8](#)
ロールバック [8](#)
Hyper-V バックアップ操作の制約事項 [9](#)

I

IBM Knowledge Center [vii](#)
IBM Spectrum Protect リカバリー・エージェント GUI
オプション [51](#)
構成 [51](#)
inactive オプション [182](#)
include
INCLUDE.VMDISK [184](#)
include.vm オプション [183](#)
INCLUDE.VMDISK [184](#)
include.vmsnapshotattempts オプション [186](#)
include.vmtsmvss オプション [187](#)
iSCSI サービスの開始
保護、Exchange Server データの [103](#)
保護、SQL Server データの [120](#)
iSCSI マウント
構成 [57](#)

K

Knowledge Center [vii](#)

L

LAN 環境 [222](#)

M

Mbobjrefreshthresh [191](#)
Mbpctrefreshthresh [192](#)
Microsoft Exchange Server バックアップ

Microsoft Exchange Server バックアップ (続き)
メールボックス履歴の更新 [101](#)
mode オプション [190](#)
mount コマンド [229](#)

N

noprompt オプション [193](#)
numberformat
指定 [193](#)
numberformat オプション [193](#)

P

pick オプション [195](#)
pitdate [195](#)
pittime オプション [195](#)
PowerShell コマンドレット
使用 [139](#)
前提条件ステップ [139](#)
タスク [145](#)
入手、ヘルプ [141](#)
リスト [141](#)
VM の保護 [141](#), [145](#)
PowerShell コマンドレットを使用 [139](#)

Q

query
活動/非活動オブジェクトの表示 [182](#)
バックアップ、特定時点の確立 [195](#)
query VM コマンド [161](#)

R

RCT バックアップ
アップグレードの考慮事項 [20](#)
機能 [2](#)
へのマイグレーション [2](#)
description [2](#)
Resilient Change Tracking (RCT) バックアップ [2](#)
restore vm コマンド
プレビュー [171](#)

S

set_connection コマンド [233](#)
skipsystemexclude [196](#)
SSL
構成 [54-56](#)

T

timeformat オプション [197](#)
TLS の構成
サーバーとのセキュア通信の使用可能化 [54-56](#)

V

V8.1.10 の新機能 [ix](#)
VM の除外
ベスト・プラクティス [82](#)

VM の保護
PowerShell コマンドレット [141](#), [145](#)
VM のリストア
Data Protection for Microsoft Hyper-V 管理コンソール
[80](#)
VM バックアップを検証するためのスクリプト
保護、SQL Server データの [124](#)
VM 名の変更後の構成
保護、Exchange Server データの [99](#)
保護、SQL Server データの [115](#)
VM を今すぐバックアップ
Data Protection for Microsoft Hyper-V 管理コンソール
[79](#)
vmautostartvm [198](#)
vmbackdir オプション [199](#)
vmbackupupdateguid オプション [155](#)
vmctlmc オプション
オプション
vmctlmc [199](#)
vmmaxbackupsessions オプション [200](#)
vmmaxparallel オプション [202](#)
vmmaxparallelrestorevms オプション [206](#)
vmmaxpersnapshot オプション [203](#)
vmmaxrestoreparalleldisks オプション [205](#)
vmmaxrestoresessions オプション [210](#)
vmmaxsnapshotretry [212](#)
vmmaxvirtualdisks オプション [213](#)
vmmc オプション [8](#), [214](#)
vmprocessvmwithphysdisks オプション [215](#)
vmrestoretype オプション [218](#)
vmskipmaxvirtualdisks オプション [216](#)
vmskipphysdisks オプション [217](#)
Volume Shadow Copy Service (VSS) バックアップ
description [1](#)
VSS バックアップ
description [1](#)
VSS バックアップ Data Protection for Microsoft Hyper-V
Data Protection for Microsoft Exchange Server [127](#)

W

Windows Server 2012 でのクラスター・バックアップ
スケジュール競合の削減 [59](#)
Windows Server 2012 でのスケジュール済みクラスター・バ
ックアップ
調整 [59](#)
Windows クライアント
ディスク・スペース所要量 [13](#)
ハードウェア要件 [13](#)
メモリー所要量 [13](#)



プログラム番号: 5725-X00