

DL アプライアンスの Rapid Recovery 6.0

ユーザーズガイド

メモ、注意、警告

① **メモ:** メモでは、コンピュータを使いやすくするための重要な情報を説明しています。

△ **注意:** 注意では、ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

⚠ **警告:** 警告では、物的損害、けが、または死亡の原因となる可能性があることを示しています。

© 2016 Dell Inc. 無断転載を禁じます。この製品は、米国および国際著作権法、ならびに米国および国際知的財産法で保護されています。Dell、および Dell のロゴは、米国および/またはその管轄区域における Dell Inc. の商標です。本書で使用されているその他すべての商標および名称は、各社の商標である場合があります。

1 DL アプライアンスについて.....	11
導入アーキテクチャ.....	11
Smart Agent.....	13
DL アプライアンスの コア.....	13
スナップショットプロセス.....	14
災害復旧サイトまたはサービスプロバイダのレプリケーション.....	14
リカバリ.....	14
製品の特徴.....	14
リポジトリの理解.....	15
Rapid Recovery の重複排除.....	16
暗号化キーの理解.....	17
Rapid Recovery でのレプリケーション.....	18
保持とアーカイブ.....	21
仮想化とクラウド.....	22
アラートとイベント管理.....	23
ライセンスポータル.....	23
ウェブコンソール.....	23
サービス管理 API.....	23
2 DL アプライアンス コアの操作.....	24
Rapid Recovery Core Console について.....	24
Rapid Recovery Core Console へのアクセス.....	24
クイックスタートガイドについて.....	24
Rapid Recovery Core Console での移動.....	26
保護対象マシン メニューの表示.....	30
ナビゲーションメニューからのレプリケートされたマシンの表示.....	35
「リカバリポイントのみ」メニューの表示.....	35
カスタムグループ メニューの表示.....	36
「エラー」ダイアログボックスの使用.....	36
Core 設定.....	36
Rapid Recovery Core の設定.....	36
Core 設定のバックアップとリストア.....	65
Core レベルのツール.....	66
Core を設定するためのロードマップ.....	68
リポジトリ.....	69
DVM リポジトリの管理.....	69
セキュリティの管理.....	81
保護対象マシンに対する暗号化の適用または削除.....	81
暗号化キーの管理.....	84
クラウドアカウントの管理.....	91
クラウドアカウントについて.....	91

クラウドアカウントの追加.....	91
クラウドアカウントの編集.....	93
クラウドアカウント設定の構成.....	93
クラウドアカウントの削除.....	94
アーカイブアーカイブ.....	94
アーカイブについて.....	94
アーカイブの作成.....	94
スケジュール設定されたアーカイブの編集.....	97
スケジュール設定されたアーカイブの一時停止または再開.....	99
アーカイブジョブの強制実行.....	99
アーカイブのチェック.....	100
アーカイブのアタッチ.....	101
アーカイブのインポート.....	102
イベント.....	104
Rapid Recovery イベント.....	104
タスク、アラート、およびジャーナルを使用したイベントの表示.....	104
電子メール通知を理解する.....	107
システムイベントの通知グループは、SMTP の設定、通知テンプレート.....	111
通知グループの設定.....	111
繰り返し回数の削減の設定について.....	114
イベントの保持の設定.....	115
Rapid Appliance Self Recovery.....	115
RASR USB キーの作成.....	115
RASR の実行.....	116
Local Mount Utility.....	117
Local Mount Utility について.....	117
Local Mount Utility での Rapid Recovery Core マシンの操作.....	117
Local Mount Utility での保護対象マシンの操作.....	120
Local Mount Utility のトレイメニューの使用.....	123
3 アプライアンスの管理.....	124
アプライアンスのステータスの監視.....	124
Windows のバックアップ.....	124
バックアップステータス.....	125
Windows バックアップポリシー.....	126
ストレージのプロビジョニング.....	127
仮想ディスク用の容量割り当ての削除.....	128
Recovery and Update Utility.....	129
アプライアンスのアップグレード.....	129
アプライアンスの修復.....	129
4 ワークステーションとサーバーの保護.....	131
マシンの保護.....	131
Rapid Recovery によるマシンの保護について.....	131
保護対象マシンの診断情報へのアクセス.....	193

マシンの管理.....	195
マシンの削除.....	195
マシン上の操作のキャンセル.....	196
マシンのライセンス情報の表示.....	196
VM エクスポート.....	196
Rapid Recovery を使用した仮想マシンへのエクスポートについて.....	196
エクスポートの管理.....	208
過去のデータ管理.....	221
Rapid Recovery のデータ保持とアーカイブについて.....	222
保持ポリシーの管理.....	222
レプリケーション.....	227
Rapid Recovery でのレプリケーション.....	227
リカバリポイントチェーンとオフファン.....	231
レプリケーション開始のタイミング.....	232
シーディングの要件と戦略の決定.....	232
レプリケートされたデータ転送のパフォーマンスに関する考慮事項.....	234
自己管理ターゲット Core へのレプリケーション.....	235
入力方向および出力方向のレプリケーションの表示.....	238
レプリケーションの設定.....	240
サードパーティのターゲット Core へのレプリケート.....	241
既存のレプリケーションへのマシンの追加.....	245
ターゲット Core 上のシードドライブの消費.....	247
レプリケーション設定の管理.....	249
レプリケーションの削除.....	256
レプリケートされたデータのリカバリ.....	258
5 データのリカバリ.....	259
リカバリの管理.....	259
スナップショットとリカバリポイント.....	259
スナップショットとリカバリポイントの管理.....	259
保護対象マシンのリカバリポイントページの表示.....	259
リカバリポイントのマウント.....	261
リカバリポイントのマウント解除.....	262
Linux リカバリポイントの操作.....	263
スナップショット作成の強制実行.....	265
リカバリポイントの削除.....	265
孤立したリカバリポイントチェーンの削除.....	266
異なるリポジトリへの手動によるリカバリポイントの移行.....	267
データのリストア.....	267
Rapid Recovery を使用したデータのリストアについて.....	267
Live Recovery について.....	268
リカバリポイントからのデータのリストア.....	269
リカバリポイントからのボリュームの復元.....	269
クラスタとクラスタノードのリストアの実行.....	272
添付されたアーカイブからのリストア.....	273

Windows マシンの Bare Metal Restore について.....	274
Windows マシンのベアメタル復元について.....	274
Windows マシンのブート CD の作成について.....	279
BMR への Universal Recovery Console の使用.....	282
Linux マシンでの Bare Metal Restore の実行.....	289
Bare Metal Restore の確認。.....	298
6 レポートの生成と表示.....	303
Rapid Recovery レポートについて.....	303
Core Console からのレポートの生成.....	304
Core Console からスケジュールされたレポートの管理.....	307
レポートメニューの使用.....	311
レポートのツールバーの使用.....	312
ジョブレポートについて.....	314
ジョブサマリレポートについて.....	314
失敗レポートについて.....	315
サマリレポートについて.....	315
リポジトリレポートについて.....	316
Central Management Console.....	317
Rapid Recovery Central Management Console について.....	317
Rapid Recovery Central Management Console の設定.....	318
中央管理コンソールのコアレポートの理解.....	322
7 Rapid Recovery Command Line Management ユーティリティについて.....	324
コマンドこまんど.....	325
Archive.....	326
CancelActiveJobs.....	327
CheckRepository.....	328
CreateArchiveRepository.....	329
CreateBootCD.....	331
CreateRepository.....	332
DeleteRepository.....	333
Dismount.....	334
DismountArchiveRepository.....	335
EditEsxServer.....	336
Force.....	337
ForceAttach.....	338
ForceChecksum.....	338
ForceLogTruncation.....	339
ForceMount.....	340
ForceReplication.....	341
ForceRollup.....	342
ForceVirtualStandby.....	343
ヘルプ.....	344
List.....	344
マウント.....	346

MountArchiveRepository.....	347
NewCloudAccount.....	348
OpenDvmRepository.....	350
Pause.....	350
Protect.....	352
ProtectCluster.....	353
ProtectEsxServer.....	354
RemoveAgent.....	355
RemoveArchiveRepository.....	356
RemovePoints.....	357
RemoveScheduledArchive.....	358
RemoveVirtualStandby.....	359
レプリケート.....	360
レプリケーション.....	361
RestoreAgent.....	363
RestoreArchive.....	364
RestoreUrc.....	365
Resume.....	366
SeedDrive.....	368
StartExport.....	369
UpdateRepository.....	371
バージョン.....	372
VirtualStandby.....	373
ローカライゼーションローからいぜーしょん.....	376
付録 A: Core Console リファレンス.....	377
Core Console ユーザーインタフェースの表示.....	377
ボタンバー.....	378
アイコンバー.....	379
左側のナビゲーションメニュー.....	381
Protected Machines（保護されたマシン）ペインの表示.....	384
保護対象マシンのイベントの表示.....	387
保護されたマシンの More（詳細）メニューの表示.....	388
付録 B: Rapid Recovery PowerShell モジュールについて.....	390
PowerShell 使用の前提条件.....	391
powershell.exe.config.....	391
PowerShell の起動とモジュールのインポート.....	391
コマンドとコマンドレットの操作.....	391
コマンドレットのヘルプと例の取得.....	392
Rapid Recovery PowerShell モジュールコマンドレット.....	392
Edit-EsxiVirtualStandby.....	395
Edit-HyperVVirtualStandby.....	396
Edit-ScheduledArchive.....	397
Edit-VBVirtualStandby.....	399
Edit-VMVirtualStandby.....	401
Get-ActiveJobs.....	402

Get-Clusters.....	403
Get-CompletedJobs.....	404
Get-ExchangeMailStores.....	405
Get-Failed.....	406
Get-FailedJobs.....	407
Get-Mounts.....	409
Get-Passed.....	409
Get-ProtectedServers.....	410
Get-ProtectionGroups.....	411
Get-QueuedJobs.....	412
Get-RecoveryPoints.....	413
Get-ReplicatedServers.....	414
Get-Repositories.....	415
Get-ScheduledArchives.....	416
Get-SqlDatabases.....	416
Get-UnprotectedVolumes.....	417
Get-VirtualizedServers.....	418
Get-Volumes.....	419
New-Base.....	420
New-CloudAccount.....	421
New-EncryptionKey.....	422
New-EsxiVirtualStandby.....	423
New-HyperVVirtualStandby.....	425
New-Mount.....	426
Resume-Replication.....	428
New-Repository.....	429
New-ScheduledArchive.....	430
New-Snapshot.....	432
New-VBVirtualStandby.....	433
New-VMVirtualStandby.....	434
Push-Replication.....	435
Push-Rollup.....	436
Remove-Agent.....	437
Remove-Mount.....	438
Remove-Mounts.....	439
Remove-RecoveryPoints.....	440
Remove-Repository.....	441
Remove-ScheduledArchive.....	442
Remove-VirtualStandby.....	443
Resume-Replication.....	444
Resume-Snapshot.....	445
Resume-VirtualStandby.....	446
Resume-VMExport.....	447
Start-Archive.....	448
Start-AttachabilityCheck.....	449

Start-ChecksumCheck.....	450
Start-EsxiExport.....	451
Start-HypervExport.....	452
Start-LogTruncation.....	454
Start-MountabilityCheck.....	455
Start-Protect.....	456
Start-ProtectCluster.....	457
Start-RepositoryCheck.....	458
Start-RestoreArchive.....	459
Start-ScheduledArchive.....	460
Start-VBExport.....	461
Start-VirtualStandby.....	463
Start-VMExport.....	464
Stop-ActiveJobs.....	465
Suspend-Replication.....	466
Suspend-RepositoryActivity.....	468
Suspend-ScheduledArchive.....	469
Suspend-Snapshot.....	469
Suspend-VirtualStandby.....	470
Suspend-VMExport.....	471
Update-Repository.....	472
ローカライゼーションローからいぜーしょん.....	473
修飾子しゅうしょくし.....	473
付録 C: スクリプトによる Rapid Recovery ジョブの拡張.....	475
Rapid Recovery での PowerShell スクリプトの使用.....	475
PowerShell Scripting の前提条件.....	476
powershell.exe.config.....	476
PowerShell スクリプトのテスト.....	476
ローカライゼーションローからいぜーしょん.....	476
修飾子しゅうしょくし.....	476
PowerShell Scripting の入力パラメータ.....	477
AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents).....	477
AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer).....	477
BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs).....	479
ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks).....	479
DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange).....	479
ExportJobRequest (namespace Replay.Core.Contracts.Export).....	480
NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql).....	480
RollupJobRequest (namespace Replay.Core.Contracts.Rollup).....	480
TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer).....	481
TransferJobRequest (namespace Replay.Core.Contracts.Transfer).....	481
TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution).....	482
TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution).....	483
TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution).....	485
VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization).....	485

VolumeImageldsCollection (namespace Replay.Core.Contracts.RecoveryPoints).....	485
VolumeName (namespace Replay.Common.Contracts.Metadata.Storage).....	485
VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage).....	486
VolumeSnapshotInfo (namespace Replay.Common.Contracts.Transfer).....	486
VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer).....	486
PowerShell スクリプトのサンプル.....	487
PreTransferScript.ps1.....	487
PostTransferScript.ps1.....	487
PreExportScript.ps1.....	488
PostExportScript.ps1.....	488
PreNightlyJobScript.ps1.....	489
PostNightlyJobScript.ps1.....	490
Rapid Recovery での Bourne Shell スクリプティングの使用.....	492
Bourne Shell スクリプティングの前提条件.....	492
サポートされる転送および事後転送スクリプトパラメータ.....	493
Bourne Shell スクリプティングのテスト.....	493
Bourne Shell スクリプティングの入力パラメータ.....	493
TransferPrescriptParameters_VolumeNames.....	493
TransferPostscriptParameter.....	494
Bourne Shell スクリプトのサンプル.....	495
PreTransferScript.sh.....	495
PostTransferScript.sh.....	495
PostExportScript.sh.....	496
付録 D: Rapid Recovery API.....	497
対象読者.....	497
Rapid Recovery REST API の使用.....	497
Core および Agent API のダウンロードと表示.....	497
参考資料.....	499
デルについて.....	500
デルへのお問い合わせ.....	500
テクニカルサポート :	500
用語集.....	501

DL アプライアンスについて

Rapid Recovery（迅速な回復）ソフトウェアの DL アプライアンスは、バックアップ、レプリケーション、およびリカバリのソリューションで、ほぼゼロに近いリカバリタイム目標（RTO）およびリカバリポイント目標（RPO）を提供します。Rapid Recovery は、データ保護、災害復旧、データマイグレーション、データの管理を提供します。（類似する、あるいは類似しないハードウェアへの）ペアメタルリストアを実行する柔軟性があり、生成元に関係なく物理マシンまたは仮想マシンのバックアップをリストアすることができます。Rapid Recovery を使用すると、追加の冗長性とセキュリティを確保するために、1つまたは複数のターゲットをレプリケートすることができます。

お使いのアプライアンスは、バックアップ、レプリケーション、リカバリを単一のソリューションに組み合わせることで統合データ保護の新たな基準を打ち立てるものです。これは、仮想マシン（VM）、物理マシン、クラウド環境を保護するための最も高速で最も信頼性の高いバックアップとなるように設計されています。お使いのアプライアンスは、グローバル重複排除、圧縮、暗号化、レプリケーションのビルトイン機能で、ペタバイトのデータを処理できます。これは、任意のプライベートまたはパブリッククラウドインフラストラクチャに対して行われます。サーバーアプリケーションおよびデータは、データ保持とコンプライアンスのために、数分でリカバリできます。

お使いのアプライアンスは、VMware vSphere および Microsoft Hyper-V のプライベートクラウドまたはパブリッククラウド上でのマルチハイパーバイザー環境をサポートします。

Rapid Recovery は次のものを提供します

- ・ **柔軟性。**物理から仮想、仮想から物理、仮想から仮想、物理から物理への復元を含め、複数のプラットフォームに対してユニバーサルリカバリを実行することができます。
- ・ **クラウドの統合。**専有およびオープンソースの両方のプラットフォームをサポートするクラウドストレージベンダーを使用してクラウドをアーカイブし、レプリケーションすることができます。
- ・ **インテリジェントな重複排除。**一度にデータを保存し、それ以降に参照することにより（リポジトリまたは暗号化ドメインごとに1回）、ストレージ要件を減らすことができます。
- ・ **インスタントリカバリ。**弊社の Live Recovery（ライブリカバリ）機能を使用すると、残りのリストア操作を平行して残しつつ、重要データに最初にアクセスできます。
- ・ **ファイルレベルのリカバリ。**リモートロケーションからのオンプレミスかつファイルレベル、あるいはクラウドからデータをリカバリできます。
- ・ **仮想サポート。**拡張された仮想化のサポートには、VMware® ESXi™ 5 以上のエージェントなしの保護と自動検出、ならびに Microsoft® Hyper-V® の クラスタ共有ボリュームへのエクスポートが含まれます。

Rapid Recovery に関する詳細については、次のリソースを参照してください。

- ・ Dell Rapid Recovery 製品サポート Web サイト: <https://support.software.dell.com/rapid-recovery/>
- ・ のマニュアルのウェブサイト <https://support.software.dell.com/rapid-recovery/release-notes-guides/> および <http://www.dell.com/support/home/>

トピック：

- ・ [導入アーキテクチャ](#)
- ・ [製品の特徴](#)

導入アーキテクチャ

アプライアンスは、企業内で、またはマネージドサービスプロバイダにより提供されるサービスとして、柔軟に導入される拡張可能なバックアップおよびリカバリ製品です。導入のタイプは、顧客の規模と要件によって異なります。アプライアンスの導入準備

には、ネットワークストレージトポロジ、コアハードウェアと災害復旧インフラストラクチャ、およびセキュリティの計画が含まれます。

導入アーキテクチャは、ローカルおよびリモートのコンポーネントで構成されます。オフサイトリカバリ用に災害復旧サイトやマネージドサービスプロバイダを利用する必要のない環境では、リモートコンポーネントを省略することもできます。基本的なローカル導入は、コアと呼ばれるバックアップサーバーと、1台または複数台の保護対象マシンで構成されます。オフサイトコンポーネントは、DR サイトにおける完全なリカバリ機能を提供するレプリケーションを使用して有効になります。コアは、ベースイメージと増分スナップショットを使用して、保護対象エージェントのリカバリポイントを収集します。

また、アプライアンスは、包括的な保護と効果的なリカバリを実現するために、Microsoft Exchange と SQL の存在をそれぞれのデータベースとログファイルとともに検出し、依存関係に基づいてこれらのボリュームを自動的にグループ化できるため、アプリケーションウェアになっています。これにより、リカバリを実行するときに、不完全なバックアップが存在しないことが保証されます。バックアップは、アプリケーションウェアなブロックレベルのスナップショットを使用して実行されます。アプライアンスは、保護対象の Microsoft Exchange サーバーと SQL サーバーのログの切り捨ても実行できます。

次の図は、単純な導入を示しています。この図では、AppAssure エージェントソフトウェアが、ファイルサーバー、電子メールサーバー、データベースサーバー、仮想マシンなどのマシン上にインストールされ、単一のコアで保護されています。これには、構成要素として中央リポジトリも存在しています。ライセンスポータルは、ライセンスサブスクリプション、および環境内の保護対象マシンとコアに対するグループとユーザーを管理します。ライセンスポータルでは、お使いの環境に対してライセンス単位で、ログイン、アカウントのアクティブ化、ソフトウェアのダウンロード、および保護対象マシンとコアの導入を行うことができます。

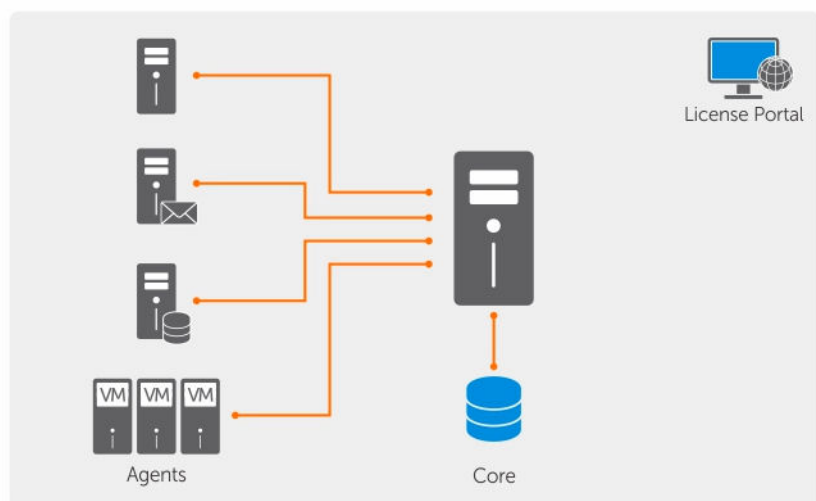


図 1. 基本的な導入アーキテクチャ

次の図に示されているように、複数の Core を導入することもできます。中央のコンソールが複数のコアを管理します。

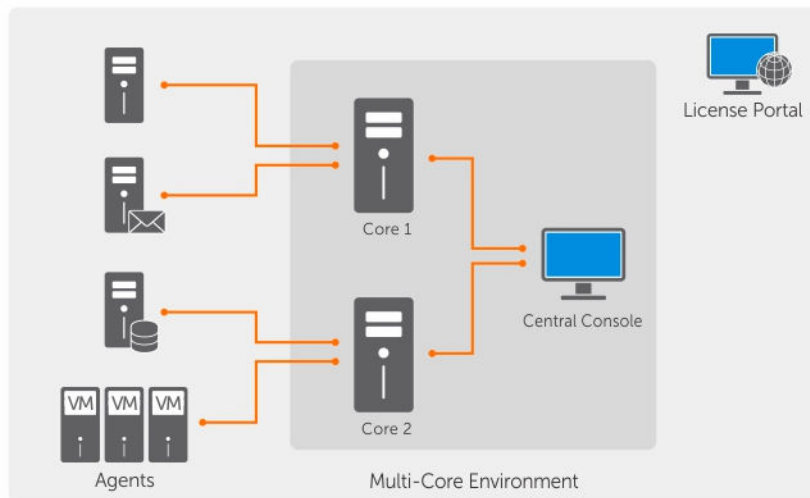


図 2. 複数コアの導入アーキテクチャ

Smart Agent

Smart Agent は、ディスクボリューム上の変更されたブロックを追跡して、事前に定義された保護間隔で変更されたブロックのイメージのスナップショットをとります。永続的に増分するブロックレベルのスナップショットのアプローチにより、保護対象マシンから Core に同じデータのコピーが繰り返し行われるのを回避します。Rapid Recovery Smart Agent は、Rapid Recovery（迅速な回復）コアにより保護されるマシンにインストールされます。

Smart Agent は、アプリケーションウェアであり、インストールされているアプリケーションのタイプとデータの場所も検出します。Smart Agent は、効果的な保護と迅速なリカバリを実現するためにデータベースなどの依存関係を持つデータボリュームを自動的にグループ化し、それらをまとめてログに記録します。Rapid Recovery（迅速な回復）エージェントソフトウェアは、設定完了後に高性能テクノロジーを使用して、保護対象ディスクボリューム上の変更されたブロックを追跡します。スナップショットの準備が整うと、そのスナップショットはインテリジェントなマルチスレッドのソケットベース接続を使用してコアへ速やかに転送されます。保護対象マシン上での CPU 帯域幅とメモリの消費を抑えるために、Smart Agent はソース側でデータの暗号化や重複排除を実行せず、保護対象マシンは保護のために Core とペアリングされます。

DL アプライアンスのコア

Core は、導入アーキテクチャの中心的なコンポーネントです。すべてのマシンバックアップを保存および管理し、バックアップ、リカバリ、保持、レプリケーション、アーカイブ、および管理のためにコアサービスを提供します。Core は 64 ビットの Microsoft Windows オペレーティングシステムが実行されている自己完結型のネットワークアドレス対応コンピュータです。アプライアンスは、保護対象マシンから受信したデータのターゲットベースのインライン圧縮、暗号化、および重複排除を実行します。Core は、ストレージエリアネットワーク（SAN）やダイレクトアタッチストレージ（DAS）などのリポジトリにスナップショットバックアップを保存します。

リポジトリは、Core 内の内部ストレージにも常駐させることができます。Core は、ウェブブラウザから **<https://CORENAME:8006/apprecovery/admin>** にアクセスすることによって管理されます。内部的には、すべてのコアサービスは、REST API を介してアクセスできます。コアサービスには、コア内からアクセスすることも、HTTP/HTTPS リクエストの送信と HTTP/HTTPS レスポンスの受信が可能な任意のアプリケーションからインターネット経由で直接アクセスすることもできます。すべての API 操作は、SSL を使用して実行され、X.509 v3 証明書で相互認証されます。

Core は、レプリケーションのために他の Core とペアになります。

スナップショットプロセス

ベースイメージが保護対象マシンから Core へ転送されると、スナップショットが作成されます。スナップショットは、データを生成するアプリケーションが引き続き使用中である際、特定の時点におけるディスクボリュームの状態をキャプチャし、保存します。Rapid Recovery（迅速な回復）では、スナップショットの一時停止、リポジトリの現在のリカバリポイントのリスト表示、および必要に応じた削除を強制することができます。リカバリポイントは、保護対象マシンをリストアしたり、ローカルファイルシステムにマウントするために使用します。Rapid Recovery（迅速な回復）によってキャプチャされるスナップショットは、ブロックレベルで行われ、アプリケーションに認識されます。これは、すべての未処理トランザクションと進行中トランザクションのログが、Snapshot の作成前に完了され、キャッシュがディスクにフラッシュされることを意味します。

Rapid Recovery（迅速な回復）は、低レベルのボリュームフィルタドライバを使用します。このドライバは、マウントされているボリュームにアタッチされ、次のスナップショットのためにブロックレベルの変更をすべて追跡します。アプリケーションクラッシュ整合なスナップショットの促進には Microsoft Volume Shadow Services（VSS）が使用されます。

災害復旧サイトまたはサービスプロバイダのレプリケーション

レプリケーションプロセスには、2つのコア間でのソースとターゲットのペアの関係が必要です。ソースコアは保護対象マシンのリカバリポイントをコピーし、それらをリモート災害復旧サイトにあるターゲットコアに非同期的かつ継続的に送信します。このオフサイトの場所は、会社が所有するデータセンター（自己管理コア）または第三者のマネージドサービスプロバイダ（MSP）の場所にすることも、クラウド環境にすることもできます。MSP に複製する場合、接続を要求し、自動のフィードバック通知を受け取ることを可能にするビルトインワークフローを使用できます。最初のデータ転送には、データシーディングの実行に外部メディアを使用できます。これは、データが大量にある場合やサイト間のリンクが低速の場合に便利です。

深刻な機能の停止が発生した場合、アプライアンスはレプリケーション環境でのフェールオーバーとフェールバックをサポートします。広範囲にわたって機能の停止が発生した場合、セカンダリサイト内のターゲットコアは、複製された保護対象マシンからインスタンスを回復し、フェールオーバーマシン上で保護をただちに開始できます。プライマリサイトの復旧後、複製されたコアは、回復されたインスタンスからプライマリサイトの保護対象マシンにデータをフェールバックできます。

リカバリ

リカバリは、ローカルサイトまたはレプリケーとされたリモートサイトで実行できます。導入がローカル保護およびオプションのレプリケーションで安定した状態になると、DL1000 Core では、Recovery Assure、Universal Recovery、または Live Recovery を使用したリカバリの実行が可能になります。

製品の特徴

次の機能と機能性を使用して、重要なデータの保護とリカバリを管理できます。

- ・ リポジトリ
- ・ Rapid Recovery の重複排除
- ・ 暗号化
- ・ レプリケーション
- ・ 保持とアーカイブ
- ・ 仮想化とクラウド
- ・ アラートとイベント管理
- ・ ライセンスポータル
- ・ ウェブコンソール

リポジトリの理解

リポジトリは、保護対象ワークステーションおよびサーバーからキャプチャされたバックアップのスナップショットデータが保存され、管理される中心的場所です。データは、リカバリポイントの形式でリポジトリに保存されます。

リポジトリは、ストレージエリアネットワーク (SAN)、ダイレクトアタッチトストレージ (DAS)、またはネットワーク接続ストレージ (NAS) などの異なるストレージテクノロジーで存在することができます。

① **メモ: Rapid Recovery コアのリポジトリをプライマリストレージデバイスに保存します。**ストレージボリュームの速度は最も重要な要素です。**Data Domain** などのアーカイブ用のストレージデバイスはパフォーマンス制限によりサポートされていません。同様に、クラウドに階層化される **NAS** ファイラ上のリポジトリも保存されません。これらのデバイスが、プライマリストレージとして使用される場合に、パフォーマンス制限がある傾向があるからです。

DAS は最高のデータ帯域幅と高速のアクセスレートを提供し、実装が容易です。最適な結果を得るには、RAID 6 のストレージの冗長アレイで DAS を使用します。詳細については、[Dell Knowledge Base article 118153 \(Dell Knowledge Base 記事 118153\)](#)、"Repository Options: Direct Attached Storage, Storage Area Network or Network Attached Storage (リポジトリのオプション: ダイレクトアタッチトストレージ (DAS)、ストレージエリアネットワーク (SAN) またはネットワーク接続ストレージ (NAS))"を参照してください。

リポジトリのストレージ場所は、常に指定するサブディレクトリないに確保する必要があります (たとえば、**E:\Repository** など)。ボリュームのルートに確保することはできません (たとえば、**E:**など)。

Rapid Recovery (迅速な回復) リポジトリ形式は、重複排除ボリュームマネージャ (DVM) を使用します。DVM リポジトリは、複数のボリュームを、単一の Core で最大 255 のリポジトリまでエクステンツを使用してサポートします。DVM リポジトリの作成は Windows オペレーティングシステムのみのマシンで行えます。新規の Rapid Recovery インストールを使用する際に、このリポジトリタイプとを使用できます。DVM リポジトリは作成時にサイズを指定できます。エクステンツは後で追加できます。

DVM Repository (DVM リポジトリ) 機能と属性には次のものが含まれます。

- ・ Rapid Recovery 6.X のアーカイブとリカバリポイントからのリカバリをサポートします。
- ・ Windows OS のみのストレージの場所をサポートします。リポジトリボリュームは、ローカル (Core サーバーに接続されたストレージ)、または共通インターネットファイルシステム (CIFS) 共有ロケーションのストレージの場所に指定できます。
- ・ サポートされるストレージタイプには、ストレージエリアネットワーク (SAN)、ダイレクトアタッチトストレージ (DAS)、またはネットワーク接続ストレージ (NAS) が含まれます
- ・ 8 GB の RAM が必須で、ECC メモリの使用を推奨します。
- ・ Core マシンでクアッドコアプロセッサが必須です (この長期にわたる要件は現在施行されています)。
- ・ ホスト単位で複数の DVM リポジトリをサポートします。
- ・ 追加のサービスが不要です。DVM リポジトリは、Core との通信、ならびにイベントを追跡するための通信のために、リポジトリのネイティブの Core サービスを使用します。
- ・ 各 DVM リポジトリは最大 4096 のリポジトリエクステンツ (ストレージの場所とも呼ばれます) をサポートします。
- ・ 固定のサイズです。DVM リポジトリでは、ボリュームのリポジトリサイズを指定する必要があります。指定するサイズは、ボリュームのサイズを超えることはできません。ストレージの場所として定義する各ボリュームでは、最小でも 1 GB の空き領域が利用可能である必要があります。
- ・ リポジトリのストレージ場所は、最も重要な要因である速度に応じて、シンプルなもの、またはダイナミックディスクを利用するものから選択できます。
- ・ コアコンソール (Core ベースの暗号化) で作成され、管理される標準の暗号化キーを使用できます。
- ・ リポジトリ全体にわたって (暗号化キーが使用されている場合は各リポジトリ内で暗号化ドメインにわたって) データの重複排除
- ・ サイズ変更可能な専用の重複排除キャッシュを使用します。Core 設定で設定可能なストレージの場所を使用します。
- ・ Core ローカルでリポジトリにデータの書き込んだり、スナップショットのデータを保存したりするために最適化されています。データはすべて、Core によって処理されます。

- ・ 作成後に名前を変更できません。
- ・ このタイプの新しいリポジトリを REST API (Rapid Recovery Command Line Management Utility (cmdutil.exe) または Windows PowerShell® cmdlet) を使用して作成できます。

DVM のリポジトリを作成する場合は、Rapid Recovery コアは、指定された場所にあるデータおよびメタデータに必要なストレージ容量を事前に割り当てます。最小 DVM リポジトリサイズは 1GB です。これはテスト以外の実用の目的には一般的には小さすぎるサイズです。

DVM 重複排除はプライマリおよびセカンダリのキャッシュが必要なため、重複排除キャッシュサイズの 2 倍のストレージ容量を必ず予約してください。たとえば Core で DVM 重複排除キャッシュ設定に 1.5 GB 予約した場合は、キャッシュボリュームで 3 GB 予約します。キャッシュのデフォルトのインストールパスは、C ドライブです。詳細については、[重複排除キャッシュと保存場所について](#) を参照してください。

単一の Core に関連付けられている複数の独立したリポジトリを 255 DVM リポジトリまで作成できます。リポジトリは、異なるストレージテクノロジーにまたがることが可能です。

新しいファイルエクステンションまたは仕様を追加することによって、DVM リポジトリのサイズをさらに増やすことができます。拡張リポジトリには、異なるストレージテクノロジーにまたがる最高 4096 のエクステンションを含むことができます。

DVM リポジトリの操作の詳細については、[DVM リポジトリの管理](#) を参照してください。

Rapid Recovery の重複排除

重複排除は、ストレージ要件とネットワーク負荷の両方を削減することができるデータ圧縮方法です。このプロセスでは、データの固有ブロックが物理的に 1 回だけディスク上に保存されます。Rapid Recovery では、リポジトリ内で固有のデータブロックが再び発生すると、そのデータをもう一度保存する代わりに、そのデータへの仮想参照が保存されます。

重複排除は、Rapid Recovery Core によってキャプチャされたバックアップスナップショットで実行されます。バックアップ情報は単一のリポジトリ内で重複排除されます。複数のリポジトリ間で重複排除することはできません。

Rapid Recovery リリース 6.0.2 では、すべて DVM リポジトリに対してターゲットベースの重複排除が使用されます。このモデルでは、情報が DVM リポジトリ (ターゲット) に転送され、その後、リポジトリから重複排除されます。

ほとんどの場合、重複排除はインラインで (バックアップ情報の転送中に) 実行されます。

最大限の効果が得られるように、Rapid Recovery では現在もプロセス後に実行される重複排除機能が提供されています。プロセス後の重複排除は、パススルー重複排除と呼ばれることもあります。このモデルを使用して、リポジトリ内のデータを DVM データキャッシュ内の参照と比較します。リポジトリ内のデータブロックが既に保存されている場合、データの追加オカレンスはそのデータへのポインタまたは参照にそれぞれ置き換えられます。

このプロセス後の重複排除では、リポジトリストレージボリュームの容量を節約できます。特に、重複排除キャッシュが入力されて、さらに重複排除を利用できるように後からキャッシュが追加された場合に有効です。リポジトリの最適化ジョブの実行中は、このタイプの重複排除が実行されます。これは DVM リポジトリに固有の機能で、重複排除ブロックの再利用とも呼ばれます。

リポジトリの最適化ジョブの詳細については、「[リポジトリ最適化ジョブについて](#)」を参照してください。このタスク実行の詳細については、「[DVM リポジトリの最適化](#)」を参照してください。

つまり、Rapid Recovery では、ここに記載されているターゲットベースの重複排除、インライン重複排除、およびプロセス後の重複排除というすべてのタイプの重複排除が利用されます。

固有ブロックへの参照が保存される DVM リポジトリの場所については、「[重複排除キャッシュと保存場所について](#)」を参照してください。

暗号化キーの理解

Rapid Recovery コアは、暗号化キーを使用するリポジトリのすべてのボリュームに対してスナップショットを暗号化します。この際、コアコンソールから定義し管理する暗号化キーを使用します。

リポジトリ全体を暗号化する代わりに Rapid Recovery では単一の Rapid Recovery コアで保護される 1 つまたは複数のマシンのために暗号化キーを指定できます。それぞれのアクティブな暗号化キーが暗号化ドメインを作成します。暗号化キーを Core 上に作成する数には制限はありません。

マルチテナント環境では、(単一の Core が複数の暗号化ドメインをホストしている場合、) データは、各暗号化ドメイン内でパーティション化および重複排除処理が行われます。結果として、保護対象マシンのセットで重複排除の利点を最大化する場合には、Dell は複数の保護対象マシンに対して単一の暗号化キーを使用することを推奨します。

3 つの方法のいずれかを使用して Core の間で暗号化キーを共有することもできます。1 つ目の方法は、暗号化キーを 1 つの Rapid Recovery コアからのファイルとしてエクスポートし、別の Core へインポートします。2 番目の方法は、暗号化キーで保護されたデータをアーカイブし、そのアーカイブを別の Rapid Recovery コアへインポートします。3 番目の方法は、暗号化キーを使用して、保護対象マシンからリカバリポイントをレプリケーションします。保護対象マシンをレプリケーションすると、ソース Core に使用された暗号化キーが、ターゲット Core の暗号化キーとしてレプリケーションされたことが表示されます。

すべての場合、インポートした後は、任意の暗号化キーは、コア内にはロックされた状態で表示されます。ロックされた暗号化キーからデータにアクセスするには、ロックを解除する必要があります。暗号化キーのインポート、エクスポート、ロック、ロック解除については、トピック [暗号化キーの管理](#) を参照してください。

キーセキュリティには以下の概念と考慮事項があります。

- ・ 暗号化は、SHA-3 と互換性のある暗号ブロック連鎖 (CBC) モードで 256 ビット Advanced Encryption Standard (AES) を使用して実行されます。
- ・ 重複排除は、機密性を確実にするために暗号化ドメイン内で実行されます。
- ・ 暗号化はパフォーマンスに影響することなく実行されます。
- ・ 任意の数の保護対象マシンに対して、単一の暗号化キーを適用できますが、保護対象マシンは一度に 1 つの暗号化キーしか適用できません。
- ・ Rapid Recovery コア上で設定された暗号化キーの追加、除去、インポート、エクスポート、変更、および削除を実行できます。

 **注意:** Rapid Recovery は、保護されるマシンに暗号化キーを適用すると、新しいスナップショットを取得します。保護対象マシンの暗号化キーの関連付けを解除した後に、新しいスナップショットもトリガーされます

Rapid Recovery コアから生成される暗号化キーは、テキストファイルです。次の表の説明に従ってパラメータを 4 つ含みます。

表 1. 暗号化キーのコンポーネント

コンポーネント	説明
Name (名前)	この値は、Rapid Recovery コアコンソールにキーを追加するときに与えられるキーの名前と同等です。
キー	このパラメータは、107 のランダムに生成されるアルファベット、数字および算術演算子文字から構成されます。
ID	キー ID は、26 のランダムに生成される大文字と小文字の英語の文字で構成されます。
Comment (コメント)	コメントにはキーの作成時に入力したキーの説明のテキストが含まれます。

Rapid Recovery でのレプリケーション

本項では、Rapid Recovery でのレプリケーションの概念と設定の手順について説明します。

レプリケーションは、1つの Rapid Recovery Core からリカバリポイントをコピーし、ディザスタリカバリ目的で別の Rapid Recovery Core に送信するプロセスです。このプロセスには、2つ以上の Core 間でのソースとターゲットのペアの関係が必要です。

ソース Core は選択された保護対象マシンのリカバリポイントをコピーした後、非同期的かつ継続的にそのスナップショットデータをターゲット Core に転送します。

レプリケーションのスケジュールを設定してデフォルトの動作を変更しない限り、すべてのバックアップスナップショット、チェックサムチェック、アタッチ可否チェック、夜間ジョブが完了するとすぐに、Core はレプリケーションジョブを開始します。詳細については、「[レプリケーションのスケジュール](#)」を参照してください。

最適なデータセキュリティを確保するために、管理者は通常、ターゲット Core をリモートディザスタリカバリサイトで使用します。アウトバウンドレプリケーションは、会社が所有するデータセンターやリモートディザスタリカバリサイト（つまり「自己管理型」ターゲット Core）に対して設定することができます。または、オフサイトバックアップおよびディザスタリカバリサービスをホストするサードパーティマネージドサービスプロバイダ (MSP) またはクラウドプロバイダに対して設定することができます。サードパーティのターゲット Core へレプリケートを行う場合は、組み込みのワークフローを使用して接続をリクエストしたり、自動フィードバック通知を受け取ったりすることができます。

レプリケーションは保護対象マシンごとに管理されます。ソース Core で保護またはレプリケートされる任意のマシン（またはすべてのマシン）をターゲット Core にレプリケートするように設定できます。

次のようなレプリケーションのシナリオが考えられます。

- ・ **ローカル場所へのレプリケーション。** ターゲット Core がローカルデータセンターまたはオンサイトの場所にあり、レプリケーションは常に維持されます。この設定では、Core がなくなってもリカバリは妨げられません。
- ・ **オフサイトの場所へのレプリケーション。** ターゲット Core は、損失が発生した場合のリカバリのため、オフサイトのディザスタリカバリ施設にあります。
- ・ **相互レプリケーション。** 2つの場所にある2つのデータセンターのどちらにも Core があり、マシンを保護していて、お互いにオフサイトディザスタリカバリバックアップとして動作しています。このシナリオでは、それぞれの Core がもう一方のデータセンターにある Core に保護対象マシンをレプリケートします。
- ・ **ホストされているレプリケーションおよびクラウドレプリケーション。** Rapid Recovery MSP パートナーは、データセンターまたはパブリッククラウドで複数のターゲット Core を維持しています。これらの各 Core で、MSP パートナーにより、1つ、または複数の顧客が、リカバリポイントを顧客のサイトにあるソース Core から MSP のターゲット Core に有料でレプリケートすることができます。

① | **メモ:** このシナリオでは、顧客は自分のデータにだけアクセスできます。

次のようなレプリケーションの設定が考えられます。

- ・ **Point-to-Point レプリケーション。** 1つ、または複数の保護対象マシンを1つのソース Core から1つのターゲット Core にレプリケートします。

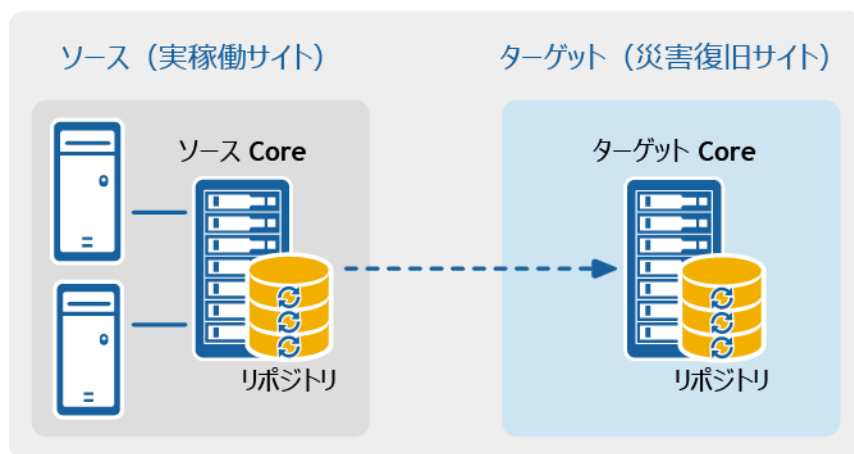


図 3. Point-to-Point レプリケーションの設定

- ・ **Multipoint-to-Point** レプリケーション。複数のソース Core から 1 つのターゲット Core に保護対象マシンをレプリケートします。

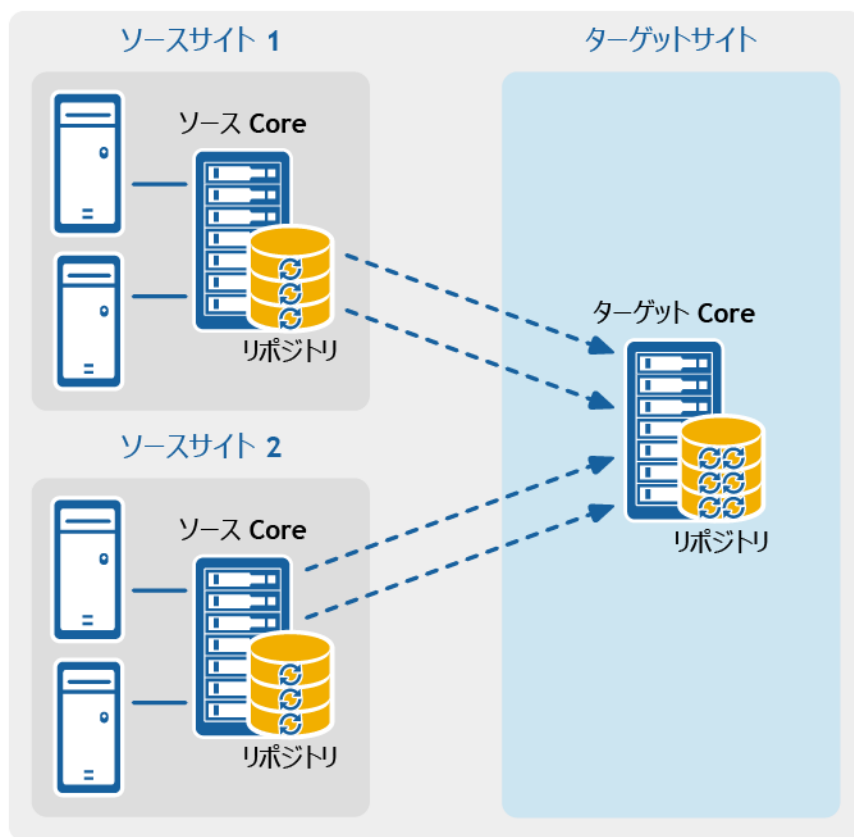


図 4. Multipoint-to-Point レプリケーションの設定

- ・ **Point-to-Multipoint** レプリケーション。1 つ、または複数の保護対象マシンを 1 つのソース Core から複数のターゲット Core にレプリケートします。

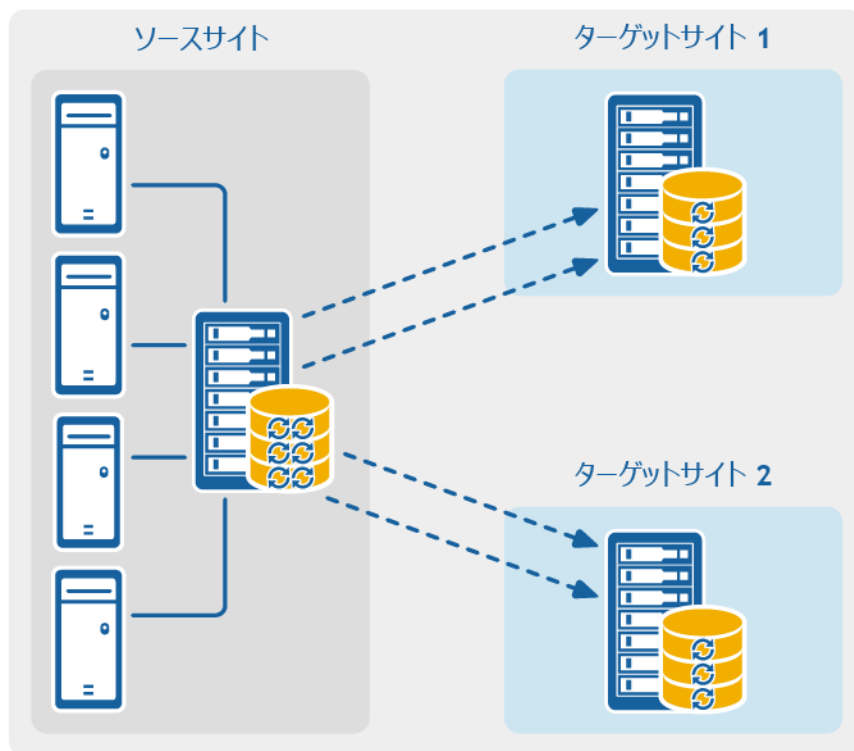


図 5. Point-to-Multipoint レプリケーションの設定

- ・ マルチホップレプリケーション。1つ、または複数の保護対象マシンを1つのターゲット Core から他のターゲット Core にレプリケートして、レプリケートした Core で追加のフェイルオーバーオプションまたはリカバリオプションを生成します。

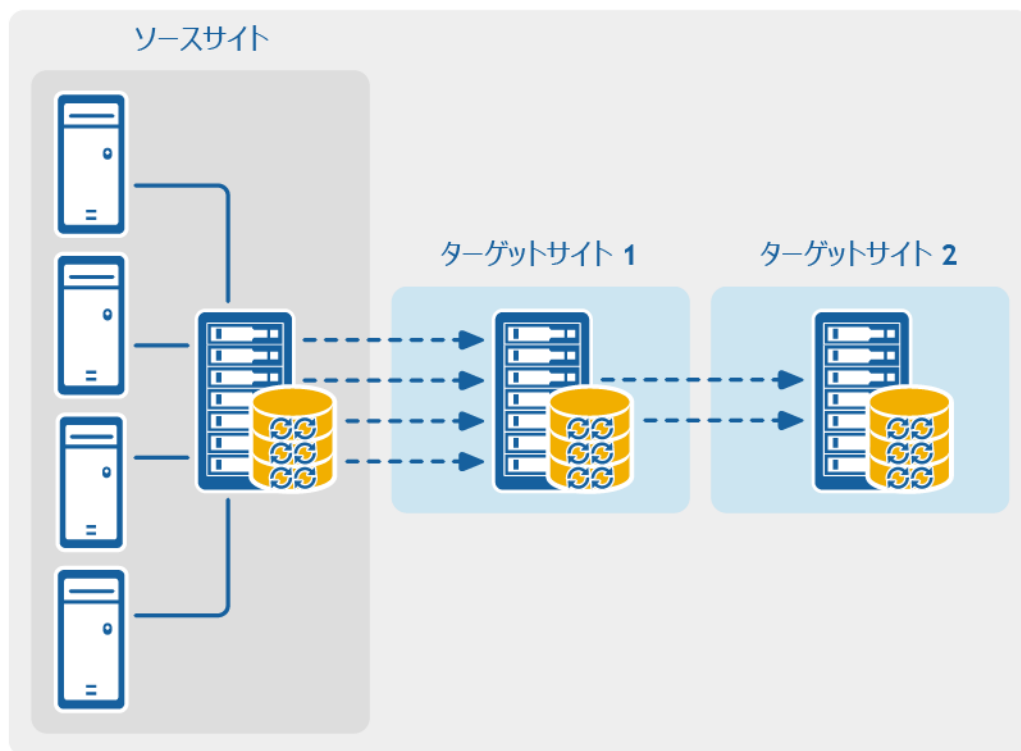


図 6. マルチホップレプリケーションの設定

DL1x00 または DL4x00 シリーズなどの Dell Data Protection バックアップアプライアンスを使用している場合は、レプリケートするターゲット Core に有効なソフトウェアライセンスが設定されている必要があります。これらのハードウェアアプライアンスには購入したレプリケーションターゲットライセンスが含まれます。アプライアンスを購入した際に受信した、ようこそメールメッセージのライセンスキーを確認してください。サポートが必要な場合は、ライセンスアシスタンスウェブサイト (<https://support.software.dell.com/ja-jp/licensing-assistance>) にアクセスするか、license@software.dell.com までメールでお問い合わせください。

保持とアーカイブ

アプライアンスでは、バックアップおよび保持ポリシーは柔軟であるため、設定が容易です。組織のニーズに合わせて保持ポリシーを調整する機能は、コンプライアンス要件を満たすために役立つだけでなく、そのために RTO を損なうことはありません。

バックアップが短期（高速かつ高価な）メディアに保存される期間は保持ポリシーによって決定されます。特定のビジネス要件と技術要件によっては、これらのバックアップ保持期間の延長が必要になる場合がありますが、高速ストレージの使用はコストが高く現実的ではありません。したがって、このような要件により、長期（低速かつ安価な）ストレージが必要になります。ビジネスでは、準拠データと非準拠データの両方のアーカイブに長期ストレージがよく使用されます。アーカイブ機能は、準拠データと非準拠データの長期的な保持をサポートするほか、レプリケーションデータをターゲットコアにシーディングするためにも使用されます。

Custom Retention Policy

☒ Enable Roll-up

Keep all Recovery Points for ...

☒ ...and then keep one Recovery Point per hour for ...

☒ ...and then keep one Recovery Point per day for ...

☒ ...and then keep one Recovery Point per week for ...

☒ ...and then keep one Recovery Point per month for ...

☒ ...and then keep one Recovery Point per year for ...

Newest Recovery Point:

Resulting Retention Period

5/13/2012 | 5/10/2012 | 5/8/2012 | 4/10/2012 | 1/11/2012 | 1/11/2011

Oldest Recovery Point will be 1 year, 4 months, 6 days old

図 7. カスタム保持ポリシー

アプライアンスでは、保持ポリシーをカスタマイズして、バックアップリカバリポイントが維持される期間を指定することができます。リカバリポイントの有効期間が保持期間の終了に近づき、リカバリポイントの有効期間が期限切れになると、そのリカバリポイントは保持プールから削除されます。通常、このプロセスはデータの量と保持期間が急速に増加し始めると効率が悪くなり、最終的には失敗します。アプライアンスは、複雑な保持ポリシーで大量データの保持を管理し、効率的なメタデータ操作を使用して古いデータのロールアップを実行することにより、大規模データの問題を解決します。

バックアップは数分間隔で実行することができます。これらのバックアップが日、月、年の単位で古くなるにつれ、保持ポリシーは、古いバックアップのエージングと削除を管理します。エージングプロセスは、単純なウォーターフォール方法によって定義されます。ウォーターフォール内のレベルは、分、時、日、週、月、年の単位で定義されます。保持ポリシーは、夜間のロールアッププロセスで適用されます。

長期アーカイブのために、アプライアンスには、リムーバブルメディア上にソースコアまたはターゲットコアのアーカイブを作成する機能が備わっています。アーカイブは内部で最適化され、アーカイブ内のすべてのデータは圧縮、暗号化、および重複排除されます。アーカイブの合計サイズがリムーバブルメディアで使用できる容量よりも大きい場合、アーカイブはメディア上の空き容量に基づいて複数のデバイスにまたがって保存されます。また、アーカイブはパスフレーズでロックすることができます。アーカイブからのリカバリに新しいコアは必要ありません。管理者がパスフレーズと暗号化キーを持っていれば、任意のコアでアーカイブを取り込み、データを回復できます。

仮想化とクラウド

Core はクラウドに対応で、クラウドのコンピューティング能力をリカバリに活用できます。

アプライアンスは、任意の保護対象またはレプリケーション対象マシンをライセンスバージョンの VMware や Hyper-V などの仮想マシンにエクスポートできます。一回のみの仮想エクスポートを実行するか、または継続的な仮想エクスポートを確立することによって、仮想スタンバイ VM を確立することもできます。継続的なエクスポートでは、スナップショットが実行されるたびに仮想マシンが増分アップデートされます。増分アップデートは非常に高速であり、ボタンをクリックするだけで電源投入できる準備が整ったスタンバイクローンを提供します。サポートされている仮想マシンのエクスポートタイプは、フォルダ上の VMware Workstation または VMware Server、vSphere/VMware ESX (i) ホストへの直接エクスポート、Oracle VirtualBox へのエクスポート、Windows Server 2008 (x64)、2008 R2、2012 (x64) および 2012 R2 上の Microsoft Hyper-V Serve へのエクスポート (Hyper-V 第 2 世代 VM のサポートも含む) です。

さらに Microsoft Azure、Amazon S3、Rackspace Cloud Block Storage、またはその他の OpenStack ベースのクラウドサービスを使用して、リポジトリデータをアーカイブすることができるようになりました。

アラートとイベント管理

アプライアンスには、HTTP REST APIに加え、電子メール、Syslog、Windows イベントログを使用してイベントの記録および通知を行う豊富な機能セットも含まれます。電子メールによる通知は、アラートに応じたさまざまなイベントの状態またはステータスをユーザーやグループに警告するために使用できます。Syslog および Windows イベントログメソッドは、複数のオペレーティングシステムがある環境のリポジトリへの一元化されたロギングを行うために使用され、Windows のみの環境では、Windows イベントログだけが使用されます。

ライセンスポータル

ライセンスポータルには、ライセンス権利を管理するための使い勝手のよいツールが用意されています。ライセンスキーのダウンロード、アクティブ化、表示、および管理を行ったり、会社のプロファイルを作成してライセンス資産を追跡したりすることができます。また、サービスプロバイダやリセラーはこのポータルを利用して、顧客のライセンスを追跡し、管理することができます。

ウェブコンソール

アプライアンスは、分散されたコアを一元的に管理する、新しいウェブベースの中央コンソールを備えています。複数の分散型コアを持つ MSP および企業カスタマーは、一元管理のために統合されたビューを得るために、中央コンソールを導入できます。中央コンソールは、管理対象コアを階層的な組織単位で分類する機能を提供します。これらの組織単位は、事業部門、所在地、または役割ベースのアクセス権を持つ MSP の顧客などにすることができます。中央コンソールは、管理対象コア全体のレポートを実行することもできます。

サービス管理 API

お使いのアプライアンスにはサービス管理 API がバンドルされており、Central Management Console から利用可能なすべての機能に対するプログラムからのアクセスを提供します。サービス管理 API は REST API です。すべての API 操作は SSL 経由で実行され、X.509 v3 証明書で相互認証されます。管理サービスには、環境内からアクセスすることも、HTTPS リクエストとレスポンスを送受信可能な任意のアプリケーションからインターネット経由で直接アクセスすることもできます。このアプローチにより、Relationship Management Methodology (RMM) ツールや請求システムなどのウェブアプリケーションとの統合が容易になります。また、アプライアンスには、PowerShell スクリプティング用の SDK クライアントもバンドルされています。

DL アプライアンス コア の操作

Rapid Recovery Core Console について

本項では、Rapid Recovery Core Console ユーザーインターフェースのさまざまなエレメントについて説明します。

Rapid Recovery Core Console へのアクセス

Rapid Recovery Core Console にアクセスするには、次の手順を実行します。

- ・ Rapid Recovery Core Console にアクセスするには、次のいずれかの手順を実行します。
 - a Rapid Recovery Core サーバにローカルでログインして、Core Console アイコンをダブルクリックします。
 - b または、ウェブブラウザで次のいずれかの URL を入力します。
 - ・ `https://<yourCoreServerName>:8006/apprecovery/admin/` または
 - ・ `https://<yourCoreServerIPaddress>:8006/apprecovery/admin/`

① メモ: Rapid Recovery Core Console の UI は JavaScript に依存しているため、Core Console へのアクセスに使用するウェブブラウザで JavaScript が有効になっている必要があります。

Rapid Recovery サービスのデフォルトポートを変更している場合は、前述の URL のポートを適宜アップデートします。

クイックスタートガイドについて

クイックスタートガイドは、Rapid Recovery Core を設定または使用するための推奨されるタスクフローを紹介する機能です。

クイックスタートガイドは、Rapid Recovery Core を初めてアップグレードまたはインストールして Core Console に移動すると、自動的に表示されます。ガイドの **ようこそ** ページで **スタートガイド** をクリックすると、さまざまな推奨設定タスクが表示されます。**ステップをスキップ** オプションと **戻る** オプションを使用して、ガイド内を移動します。最後の推奨タスクが表示されたら、**終了** をクリックしてガイドを閉じます。

『クイックスタートガイド』は、Core Console の ヘルプ メニューからいつでも再度起動することができます。クイックスタートガイドの **ようこそ** ページを非表示にすることもできます。

非表示にしなければ、Rapid Recovery Core Console にログインして、**ホーム** ページにアクセスするたびに、クイックスタートガイドが再表示されます。詳細については、「[クイックスタートガイドの非表示設定](#)」を参照してください。

ガイドによって推奨されているステップを実行する必要はありません。推奨タスクを単に表示し、**ステップをスキップ** オプションと **戻る** オプションを使用してそれらを移動できます。必要に応じて、いつでも **ガイドを終了** をクリックするとガイドを非表示にすることができます。

「クイックスタートガイド」で推奨されている設定タスクを実行する場合は、ガイドのステップで示されているプロンプトに従うと、該当するウィザードまたはユーザーインターフェース内の関連エリアが表示されます。次の表は、クイックスタートガイドが推奨する各手順について説明しています。

① **メモ:** 「クイックスタートガイド」が推奨しているすべての設定タスクが、すべてのユーザーに必要であるというわけではありません。特定のニーズに合わせて、実行する必要のあるタスクを把握する必要があります。

「クイックスタートガイド」により、次の設定タスクを実行できます。

表 2. 「クイックスタートガイド」の設定タスク

機能	簡単な説明	タスクの選択結果、手順へのリンク
保護	単一マシンの保護、サーバクラスターの保護、または一括保護を使用した複数のマシンの保護	保護 をクリックするか、ドロップダウンメニューから 保護されるマシン を選択し、マシンの保護 ウィザードを開きます。マシン保護 ウィザードを完了する方法については、「マシンの保護」を参照してください。 ドロップダウンメニューから クラスターの保護 を選択し、クラスターに接続ダイアログボックスを開きます。クラスターの保護の詳細については、「クラスターの保護」を参照してください。 ドロップダウンメニューから 一括保護 を選択し、複数のマシンの保護 ウィザードを開きます。複数のマシンの保護 ウィザードを完了する方法については、「複数のマシンの保護について」を参照してください。
レプリケーション	プライマリ（ソース）Core からセカンダリ（ターゲット）Core にレプリケーションを設定する	レプリケーション をクリックし、レプリケーション ページを開きます。レプリケーション ウィザードを使用してターゲット Core を追加するように、プロンプトが表示されます。レプリケーション ウィザードを使用して自己管理 Core でレプリケーションを設定する方法については、「自己管理ターゲット Core へのレプリケーション」を参照してください。レプリケーションの一般的な情報については、「レプリケーションの設定」を参照してください。
仮想エクスポート	保護対象マシンから仮想マシンに 1 回限りのエクスポートを実行するか、連続エクスポートを設定する	エクスポート をクリックして、保護対象マシンから仮想マシンにデータのエクスポートを実行します。1 回限りのエクスポートを実行するか、仮想マシンに継続してエクスポートを行うために Virtual Standby を設定することができます。仮想エクスポートについては、「Rapid Recovery を使用した仮想マシンへのエクスポートについて」を参照してください。
設定	Rapid Recovery Core の追加設定をセットアップできます。	より多い をクリックして、設定または管理することができるその他の機能を参照してください。機能には、アーカイブ、マウント、起動 CD、リポジトリ、暗号キー、クラウドアカウント、ファイル検索、保持ポリシー、通知、レポート、ログなどがあります。
設定： 暗号化	1 台または複数の保護マシンに使用できる暗号化キーの追加またはインポート	暗号化キー をクリックして、暗号化キーを追加またはインポートすることによって保護対象データのセキュリティを管理します。暗号化キーを 1 台または複数の保護対象マシンに適用できます。暗号化については、「暗号化キーの理解」のトピックで説明されています。
設定： 通知	イベント、警告、およびアラートの通知を設定します。	イベント をクリックして、イベント、警告、およびアラートの通知グループを指定します。これらを電子メールで送信するには、SMTP サーバーの設定も行う必要があります。イベントの管理の詳細については、「イベント」のトピック、さらに「通知グループの設定」と「電子メールサーバーの設定」のトピックも参照してください。
設定： 保持	Core のデフォルト保持ポリシーの表示または変更	保持ポリシー をクリックして、Core の 保持ポリシー ページを開きます。ここから、ロールアップする前にリカバリポイントを保持する期間を定義できます。保持ポリシーの概念については、「過去のデータ管理」のトピックを参照してください。手順については、「保持ポリシーの管理」を参照してください。
リストア	Core 上のリカバリポイントからデータをリストアします。	リストア をクリックして、マシンのリストア ウィザードを開きます。データのリストアの詳細については、「リカバリポイントからのボリュームの復元」のトピックを参照してください。

クイックスタートガイドの非表示設定

『クイックスタートガイド』は、Rapid Recovery Core を初めてアップグレードまたはインストールするときに、自動的に表示されます。

これは ヘルプ ドロップダウンメニューから クイックスタートガイド を選択したときにも表示されます。また、Core Console の ホーム ページにアクセスするたびに表示されます。

「クイックスタートガイド」を非表示に設定するには、次の手順を実行します。

- ・ Rapid Recovery Core Console で『クイックスタートガイド』の ようこそ ページが表示されている場合、次の手順を実行します。
 - ・ 『クイックスタートガイド』の ようこそ ページを非表示にするには、**次回から表示しない**を選択します。

① メモ: このオプションを設定すると、**Rapid Recovery Core** をアップグレードするまで、スタートガイドを開くたびに ようこそ ページが開くことはなくなります。
このページを非表示にして、後で詳細設定オプションにアクセスする場合、ウィザードの **戻る** を選択して、非表示にされたこのページを表示します。

- ・ このセッションの「クイックスタートガイド」を非表示にするには、**閉じる**をクリックします。
「クイックスタートガイド」が閉じます。Core Console の ホーム ページに次にアクセスしたときに、『クイックスタートガイド』は表示されます。

ヘルプ メニューから「クイックスタートガイド」を開くこともできます。

- ・ 「クイックスタートガイド」の任意のページで、**ガイドを終了**をクリックします。
「クイックスタートガイド」が閉じます。このオプションを選択しても、ヘルプ メニューから『クイックスタートガイド』を開くことができます。

Rapid Recovery Core Console での移動

Core Console にログインして **ホーム**  をクリックすると、**ホーム** ページが表示されます。**ホーム** ページには、Rapid Recovery Core を表示する 2 つのオプションが用意されています。メインビューの領域では、デフォルトの内容が新しい Core ダッシュボードに表示されます。ここには、お使いのシステムの一連のリアルタイムレポートが示されます。デフォルトのダッシュボードレポートには、最近の転送ジョブのステータス、マシンごとの転送、リポジトリの概要と、保護対象マシン、レプリケート済みマシン、およびリカバリポイントのみのマシンの接続状態が含まれます。また、従来のサマリテーブルビューに切り替えることもできます。このビューでは、Rapid Recovery Core の表示名がページのタイトルに示され、保護対象マシン、リポジトリ、最近のアラートが表示されるサマリテーブルを確認できます。詳細については、「[ホーム ページ \(サマリテーブルビュー\) について](#)」と「[Core ダッシュボードについて](#)」をそれぞれ参照してください。

ホーム ページ（および Core Console のすべてページ）で、左側のナビゲーションエリアには Core で保護されているアイテムが表示されます。これらの UI でその他のページに移動するには、次のいずれかの操作を実行します。

- ・ 左側のナビゲーションエリアのアイコンの中から、対応するアイコンをクリックします。アイコンバー（レプリケーション、イベント、設定、詳細）からオプションにアクセスできます。
- ・ アイコンバーの （より多い）メニューを展開し、移動先を選択します。
- ・ ボタンバーのボタンまたはメニューオプションをクリックします。保護、リストア、アーカイブ、およびレプリケートのボタンがあります。

左側のナビゲーションエリアからアイテムを選択すると、Core Console のフォーカスが切り替わり、そのアイテムに関するサマリ情報が表示されます。たとえば、保護対象マシンの名前をクリックすると、Core Console には Core ではなくそのマシンに関する情報のみが表示されます。この例では、保護対象マシンの表示名がページのタイトルとして表示されます。サブメニューが右側に表示され、保護対象マシンに関する特定の情報が表示されるようになります。メニューオプションには、サマリ、リカバリポイント、イベント、設定、レポート、および詳細が含まれています。

もう一度 Core に関する情報（ダッシュボードのレポート、または複数の保護対象マシンまたはレプリケートされたマシンのサマリビューを含む）を表示するには、UI の左上にある **ホーム**  アイコンをクリックします。**ホーム** ページでは、ページ右上の赤いリンクをクリックして、ダッシュボードと サマリ ページのビューを切り替えることができます。

Core Console の一番上にあるタイトルには、現在 Core に表示されている情報のコンテキストが示されます。たとえば、次のとおりです。

- Core の表示名または IP アドレスは、Core に関するサマリ情報を表示しながら、いつでもページタイトルで確認できます。
- タイトルが **ダッシュボード** の場合は、Core **ダッシュボード** が表示されます。
- 保護対象マシンの表示名または IP アドレスが表示されているか、ページの最上部に サマリ ペインが表示されている場合は、Core で保護またはレプリケートされている単一のマシンに関する情報が表示されます。
- 保護対象マシンのタイトルが表示されている場合は、Rapid Recovery Core. で保護されているすべてのマシンに関する情報が示されます。
- ... からレプリケートされたマシンのタイトルが表示されている場合は、Rapid Recovery Core. でレプリケートされたすべてのマシンに関する情報が示されます。
- リカバリポイントのみのページタイトルが表示されている場合は、その Core 上のリカバリポイントのみのマシンすべてに関する情報が示されます。

各ページで利用できる機能については、次の該当する項を参照してください。

保護対象マシンの表示の詳細については、「[保護対象マシン メニューの表示](#)」を参照してください。保護対象マシンの管理の詳細については、「[保護対象マシンの管理](#)」を参照してください。

レプリケートされたマシンの表示の詳細については、「[入力方向および出力方向のレプリケーションの表示](#)」を参照してください。

リカバリポイントのみのマシンの表示については、以下を参照してください。 [「リカバリポイントのみ」メニューの表示](#)

左側のナビゲーションエリアについて

Core Console の左側にあるナビゲーションエリアは、ユーザーインターフェースの左側に表示されます。このナビゲーションエリアの内容は、Rapid Recovery Core で保護されているオブジェクトのタイプに応じて異なる場合があります。

左側のナビゲーションエリアには常に次の要素が含まれます。

- **アイコンバー**。Core Console のメインページ間を移動します。
- **テキストフィルタ**。テキストフィルタは、その下の各メニューに表示される項目をフィルタできるテキストフィールドです。テキストフィルタの右側にある矢印をクリックすると、その下に表示される各メニューを展開したり折りたたむことができます。

これらの要素に続いて、左側のナビゲーションエリアには通常、Core で保護されているオブジェクトを移動、フィルタ、表示できるメニューが表示されます。これには保護対象マシン、レプリケートされたマシンなどが含まれています。

各メニューは文脈依存です。つまり、各メニューは関連する場合にのみ Core Console に表示されます。たとえば、1 つ以上のマシンを保護している場合は、保護されているマシンメニューが表示されます。

詳細については、「[Core Console ユーザーインターフェースの表示](#)」で左のナビゲーションエリアのテーブルを参照してください。

Rapid Recovery Core Console の ホーム ページの表示

Rapid Recovery Core Console にログインするたびに、またはアイコンバーで **ホーム**  アイコンをクリックするたびに、**ホーム** ページが表示されます。

Core Console の **ホーム** ページでは、新しい **ダッシュボード** ビューが導入され、使い慣れた **サマリ表** ビューも表示できます。ダッシュボードがデフォルトのビューです。

ホーム ページの右上にある赤いリンクをクリックして、**ホーム** ページのビューを切り替えることができます。

ホーム ページ、および Core Console のその他の全ページでは、左のナビゲーション領域を使用して、目的の機能に移動することができます。

詳細については、次のトピックを参照してください。

- ・ [左側のナビゲーションエリアについて](#)
- ・ [Core ダッシュボードについて](#)
- ・ [ホーム ページ \(サマリテーブルビュー\) について](#)

ホーム ページ (サマリテーブルビュー) について

ホーム ページは Core にのみ適用されます。ダッシュボードビューには、リアルタイムのグラフィックレポートが表示されます。サマリテーブルビューに切り替えると、ホーム ページには Core で保護またはレプリケートされるすべてのマシン、お使いの Core に関連付けられているリポジトリ、およびその Core 上のマシンのアラートが表示されます。

ホーム ページの各ペインのビューは、展開したり折り畳んだりすることができます。たとえば、保護対象マシン ペインの右側にある  (ビューの折り畳み) アイコンをクリックすると、保護対象マシンのビューが折り畳まれて、そのペインの名前だけが表示されます。ビューを展開してすべての保護対象マシンを再度表示するには、 (ビューの展開) アイコンをクリックします。

次の表では、サマリテーブルビューの ホーム ページ上のさまざまな要素について説明します。

表 3. ホーム ページのオプション

UI エlement	説明
保護対象マシン	保護対象マシン ペインには、この Core で保護されているマシンがリストされます。このペインは、マシンが保護対象として Core に追加されているかどうかに関係なく表示されます。 このセクションには、各保護対象マシンの次の情報が表示されます。 ・ マシンタイプ。アイコンによって、物理マシン、仮想マシン、または保護されたクラスタのどのマシンであるのかが示されます。 ・ ステータス：ステータス 行の色付きの円では、その保護対象マシンがアクセス可能、一時停止、またはオフラインおよび到達不能のどの状態であるのかが示されます。 ・ 表示名。保護対象マシンの表示名または IP アドレス。 ・ リポジトリ名：そのマシンのリカバリポイントを保存するリポジトリの名前。 ・ 最新のスナップショット：Rapid Recovery が、そのマシンの最新のリカバリポイントスナップショットを取得した日付と時刻。 ・ リカバリポイント：リポジトリに保存されているリカバリポイントの数と、各保護対象マシンの使用容量。 ・ バージョン。そのマシンにインストールされている Rapid Recovery Agent ソフトウェアのバージョン。 このペインに表示される特定のマシン名をクリックすると、サマリ ページが表示されます。ここには、選択したマシンのサマリ情報が示されます。サマリ ページで実行できる操作の詳細については、「保護対象マシンのサマリ情報の表示」を参照してください。
レプリケートされたマシン	レプリケートされたマシン ペインには、別の Core からこの Core にレプリケートされたマシンがすべてリストされます。別の Core から現在の Core にマシンがレプリケートされない限り、このペインは表示されません。 このセクションには、レプリケートされた各マシンの次の情報が表示されます。 ・ マシンタイプ。アイコンによって、物理マシン、仮想マシン、または保護されたクラスタのどのマシンであるのかが示されます。 ・ ステータス：ステータス 行の色付きの円では、そのレプリケート済みマシンがアクセス可能、一時停止、またはオフラインおよび到達不能のどの状態であるのかが示されます。 ・ 表示名。レプリケートされたマシンの表示名または IP アドレス。

- ・ **レプリケーション名**。現在のターゲット Core 上にマシンをレプリケートする元のソース Core の表示名。この名前には、レプリケーションをセットアップするときに定義できます。
- ・ **リポジトリ名**：そのマシンのリカバリポイントを保存するリポジトリの名前。
- ・ **最後にレプリケートされたスナップショット**。Rapid Recovery が、元の保護対象マシンの最新のレプリカを取得した日付と時刻。
- ・ **リカバリポイント**：リポジトリに保存されているリカバリポイントの数と、レプリケートされた各マシンの使用容量。
- ・ **バージョン**。そのマシンにインストールされている Rapid Recovery Agent ソフトウェアのバージョン。

このペインに表示される特定のマシン名をクリックすると、サマリ ページが表示されます。ここには、そのレプリケート済みマシンのサマリ情報が示されます。

リカバリポイントのみのマシン

リカバリポイントのみマシン ペインには、リカバリポイントが保持されている場合に、保護またはレプリケーションの対象から削除されたマシンのリストが表示されます。これらのマシンは、ファイルレベルのリカバリには使用できますが、ベアメタル復元、ボリューム全体のリストア、またはスナップショットデータの追加には使用できません。このペインは、この定義に一致するマシンがない限り、表示されません。

このセクションには、リカバリポイントのみの各マシンの次の情報が表示されます。

- ・ **マシンタイプ**。アイコンによって、物理マシン、仮想マシン、または保護されたクラスタのどのマシンであるのかが示されます。
- ・ **ステータス**：ステータス 行の色付きの円では、そのリカバリポイントのみのマシンがアクセス可能、一時停止、またはオフラインおよび到達不能のどの状態であるのかが示されます。
- ・ **表示名**。リカバリポイントを保持するマシンの表示名または IP アドレス。
- ・ **リポジトリ名**：そのマシンのリカバリポイントをそのまま保存するリポジトリの名前。
- ・ **リカバリポイント**：リポジトリに保存されているリカバリポイントの数と、リカバリポイントのみの各マシンの使用容量。

このペインに表示される特定のマシン名をクリックすると、サマリ ページが表示されます。ここには、そのリカバリポイントのみのマシンの情報が示されます。

DVM リポジトリ

このペインには、DVM リポジトリが作成されているかどうかに関係なく、DL 1000 の情報が表示されます。このペインは、Core に 1 つまたは複数の DVM リポジトリが存在する場合にのみ表示されます。

このセクションには、各 DVM リポジトリの次の情報が表示されます。

- ・ **タイプ**：アイコンによってリポジトリが示されます。
- ・ **ステータス**：ステータス 行の色付きの円では、リポジトリがマウントされていて、リカバリポイント転送を受け入れることができるか、到達不能であるか、またはエラー状態であるかどうかを示されます。
- ・ **リポジトリ名**：リポジトリの表示名。
- ・ **使用容量**。そのリポジトリで使用されている合計容量と、ストレージボリュームまたは拡張のサイズ。
- ・ **保護対象データ**：リポジトリの使用容量。
- ・ **マシン**。そのリポジトリにリカバリポイントが保存されているマシンの数。
- ・ **リカバリポイント**：リポジトリに保存されているリカバリポイントの数。
- ・ **圧縮率**：容量を節約するためにリポジトリで保護対象データを圧縮する比率。
詳細については、「[リポジトリの理解](#)」を参照してください。

アラート

このセクションには、Core の重要なアラートと Core で保護している各マシンがリストされます。このセクションには、次の情報が表示されます。

- ・ **アイコン**：アイコンの列には、アラートの特徴が表示されます。これらには、情報メッセージとエラーが含まれます。
- ・ Rapid Recovery がアラートを発行した日時が表示されます。
- ・ **メッセージ**：アラートの説明が表示されます。
Core の イベント ページでもこれらの詳細を確認できます。詳細については、「[タスク、アラート、およびジャーナルを使用したイベントの表示](#)」を参照してください。

Core ダッシュボードについて

Core ダッシュボードには、Core と保護対象マシンに関連するデータを示す、リアルタイムのグラフィックスレポートのセットが表示されます。このダッシュボードには次のレポートが含まれます。

- ・ **転送ジョブ**。このレポートには、過去 24 時間以内に完了したスナップショットのデータ転送（ベースイメージと増分スナップショットを含む）がすべて表示されます。スナップショットには、ベースイメージと増分スナップショットが含まれます。このダッシュボードレポートは円グラフとして表示されます。
- ・ **マシンごとの転送ジョブ**。このジョブでは、保護対象マシンごとに、過去 24 時間以内に成功および失敗した転送ジョブの数を示します。このダッシュボードレポートは線グラフとして表示されます。
- ・ **リポジットリ**。このレポートには、Core に関連付けられたリポジットリが表示されます。リポジットリの数、各リポジットリで保護されているマシンの数、リカバリポイントの数、圧縮または重複排除されている割合が表示されます。このレポートは毎分ごとに更新されます。
- ・ **マシンの接続性**。このレポートには、Core 上で保護され、複製されているマシンの接続状態が表示されます。また、**リカバリポイントのみのマシン** 上のデータの接続状態も表示されます。

ダッシュボード上のレポートのビューを展開または縮小するには、レポートのヘッダーで上下矢印をクリックします。一部のダッシュボードのレポート（マシンの接続性とリポジットリ）には矢印の横にプラス記号があり、別の保護対象マシンまたは別のリポジットリをそれぞれ追加するために利用できます。

いずれかのレポートをドラッグアンドドロップすると、レポートをダッシュボード上の別の場所に移動でき、使用するうえで最も効果的な方法でレポートを整理できます。

保護対象マシン メニューの表示

「保護対象マシン」メニューは、Rapid Recovery ユーザーインターフェースの左側にあるナビゲーションエリアに表示されます。ナビゲーションエリアにあるすべてのメニューラベルと同様に、このメニューのラベルもすべて大文字で表示されます。デフォルトでは、このメニューは完全に展開されていて、この Core で保護されているマシンのリストが表示されます。保護されているサーバークラスタがある場合、このリストに表示されます。

Core の保護対象マシンおよび保護対象サーバークラスタのビューを縮小表示または展開するには、このメニューの左側にある矢印をクリックします。

「保護対象マシン」メニューの右側にはドロップダウンメニューがあり、これにはすべての保護対象マシンで実行できる機能がリストされます。**保護対象マシン** の右側にある矢印をクリックすると、メニューが表示され、次の操作を実行できます。

- ・ すべてのマシンに対する増分スナップショットの強制実行
- ・ すべてのマシンに対するベースイメージの強制実行
- ・ すべてのマシンに対する保護の一時停止（保護がアクティブな場合）
- ・ すべてのマシンに対する保護の再開（保護が一時停止されている場合）
- ・ すべての保護対象マシンのメタデータの更新
- ・ すべてのマシンを Core の保護対象から削除する

「保護されたマシン」メニューの下にリストされる各マシンにはドロップダウンメニューも含まれており、これを使用して、各種機能をそのマシンのみに制御できます。マシンのドロップダウンメニューからも、次を実行できます。

- ・ 選択したマシンに対する増分スナップショットの強制実行
- ・ 選択したマシンに対する保護を一時停止する（保護がアクティブな場合）
- ・ 保護を再開する（保護が一時停止されている場合）
- ・ メタデータを更新する
- ・ 選択したマシンを Core の保護対象から削除する
- ・ 選択したマシンの サマリ ページに移動する
- ・ 選択したマシンの リカバリポイント ページに移動する

- ・ 選択したマシンの イベント ページに移動する
- ・ 選択したマシンの 設定 ページに移動する
- ・ マシン固有のレポートを生成する
- ・ システム情報、マウント、保持ポリシー、通知、またはマシン固有のログなど、選択したマシンに固有の機能へアクセスする
- ・ 「保護対象マシン」リストに表示されるカスタムラベルを作成する

Rapid Recovery Core からサーバクラスタを管理している場合、そのクラスタは左側にあるナビゲーションメニューにも表示されます。クラスタのドロップダウンメニューからも、次を実行できます。

- ・ 選択したクラスタの **保護対象ノード** ページに移動する

「保護対象マシン」メニューの左側にある矢印をクリックすると、保護対象マシンおよび保護対象サーバークラスタの契約のリストが表示されますが、マシンはリストされません。もう一度この矢印をクリックすると、マシンのリストが再度展開表示されます。

保護対象マシン メニューでいずれかのマシン名をクリックすると、そのマシンの サマリ ページが開きます。サマリ ページで実行できる操作の詳細については、「[保護対象マシンのサマリ情報の表示](#)」を参照してください。

最後に、**保護対象マシン** メニューを直接クリックすると、**保護対象マシン** ページがメインコンテンツ領域に表示され、この Core で保護されているマシンが単一のペインに示されます。保護対象マシン ページの **保護対象マシン** ペインで実行可能な操作の詳細については、「[Protected Machines \(保護されたマシン\) ペインの表示](#)」を参照してください。

① **メモ:** 保護対象マシン ページから、アイコンバーの ホーム アイコンをクリックすると、**Core** 側のビューに戻ることができます。

保護対象マシンのサマリ情報の表示

Core Console で保護対象マシンの名前をクリックすると、**サマリ** ページが表示されます。このページには、少なくとも、**サマリ** ペインと **ボリューム** ペインがあります。マシンがレプリケーションに追加されている場合は、**レプリケーション** ペインも表示されます。

保護対象の Exchange Server が1つまたは複数存在する場合は、保護対象の Exchange Server に関する情報を含んだ **Exchange Server 情報** ペインも表示されます。

保護対象の SQL Server が1つまたは複数存在する場合は、保護対象の SQL Server に関する情報を含んだ **SQL Server 情報** ペインも表示されます。

ページの一番上にあるアクションのメニューは、保護対象マシンで実行することができます。その下には、少なくとも、サマリ ペインと ボリューム ペインがあります。マシンがレプリケーションに追加されている場合は、レプリケーション ペインも表示されます。

保護対象マシンの情報を表示すると（サマリ ページとその他すべてのビューで）、ページの一番上にあるメニューにはユーザーが実行できる機能が示されます。このメニューは、保護対象マシンの名前のすぐ下に表示されます。

関連するリンク

[「サマリ」ペインの表示](#)

[保護対象マシンでのボリュームの表示](#)

[レプリケーション情報の表示](#)

[Exchange Server 情報 ペインの表示](#)

[SQL Server 情報 ペインの表示](#)

「サマリ」 ペインの表示

サマリ ペインには、ホスト名、最新のスナップショットが作成された日時、次回スナップショットがスケジュールされている日時、暗号化キー情報、Rapid Recovery エージェントソフトウェアのバージョン情報など、保護対象マシンに関するサマリ情報が表示されます。マシンの詳細な システム情報 ページへのリンクもあります。

保護対象マシンでのボリュームの表示

任意の保護対象マシンの場合、サマリ ページの ボリューム ペインで、リストされている任意のボリュームに次のアクションを実行できます。

- ・ 選択したボリュームの保護スケジュールの設定または変更。保護スケジュールは、通常、マシンを最初に保護するときに設定されます。保護スケジュールの変更の詳細については、「[保護スケジュールの変更](#)」を参照してください。
- ・ ベースイメージまたはスナップショットの強制実行。スナップショットは、通常、保護スケジュールに基づいて実行されます。ただし、選択したボリュームのベースイメージまたは増分スナップショットは、いつでも強制実行することができます。詳細については、「[スナップショットの強制](#)」を参照してください。

レプリケーション情報の表示

レプリケーション ペインには、レプリケーション名、レプリケーションの状態、進捗状況、使用可能な容量など、レプリケートされたマシンのサマリ情報が表示されます。

Exchange Server 情報 ペインの表示

Exchange Server 情報 ペインは、保護対象マシンが Exchange Server である場合にのみ表示されます。

このペインには、インストールされている Microsoft Exchange のバージョン、Exchange のインストール先のパス、Exchange のメールボックスデータを定義するパスなど、保護対象の Exchange Server に関するサマリ情報が示されます。

メールストア グリッドには、Exchange データベース (EDB) 名、EDB ファイルのパス、ログファイルの保存先のパス、ログのプレフィックス、システムのパス、データベース可用性グループ (DAG)、およびメールストアのタイプが示されます。

SQL Server 情報 ペインの表示

SQL Server 情報 ペインは、SQL Server である保護対象マシンに対してのみ表示されます。

このペインには保護対象 SQL Server のサマリ情報が表示されます。データベースの情報を展開し、データベースの各テーブルの詳細を確認できます。データベースまたはテーブル名とデータベースのパスを表示することもできます。

マシンのリカバリポイントの表示

リカバリポイント ページには、その保護対象マシンで収集されたリカバリポイントのリスト、および関連するマシンとリポジトリデータが表示されます。このページでは、特定のリカバリポイントのマウント、エクスポート、リストア、およびリカバリポイントの削除を実行できます。

このページは、リカバリポイントのサマリ と リカバリポイント の 2 つのペインに分かれています。サマリ ペインには、アクション可能なリンクは含まれていません。マシンに関する次のデータが表示されます。

表 4. リカバリポイントのサマリ ペインのデータ

UI エlement	説明
合計リカバリポイント	この特定の保護対象マシンに対して収集されたリカバリポイントの数。
保護データの合計	リポジトリに保存されている保護対象マシンのデータ量。
リポジトリ	Rapid Recovery でこの保護対象マシンのリカバリポイントを保存するリポジトリの名前。
リポジトリのステータス	進捗状況バーに、リポジトリの合計使用容量がパーセントで表示されます。リポジトリの使用データ量と合計サイズが進捗状況バーの下に表示されます。

詳細については、「[Protected Machines（保護されたマシン） ペインの表示](#)」を参照してください。

保護対象マシンのイベントの表示

イベントページには、選択した保護対象マシンに対する実行済みまたは進行中のジョブが表示されます。ページの上部にあるボタンを使用すると、アクティビティの3つの各カテゴリのジョブのリストに移動できます。

- ・ **タスク**：正常に操作するために Rapid Recovery で実行する必要があるジョブ。
- ・ **アラート**。エラーや警告など、タスクまたはイベントに関連する通知。
- ・ **ジャーナル**。すべての保護対象マシンのタスクとアラートの複合。

次の表は、イベント ページの各要素を説明しています。

表 5. イベント ページの要素

UI エlement	説明
検索キーワード	各カテゴリ内の特定のアイテムを検索できます。タスクでのみ使用可能です。
送信者	検索を開始する日付を入力して、結果を絞り込むことができます。タスクでのみ使用可能です。
宛先	検索を終了する日付を入力して、結果を絞り込むことができます。タスクでのみ使用可能です。
ステータスアイコン	各アイコンは、さまざまなジョブステータスを表しています。アラートとタスクの場合は、いずれかのアイコンをクリックすると、そのステータスでリストをフィルタでき、実質的にレポートが生成されます。アイコンを2回クリックすると、そのステータスのフィルタは削除されます。複数のステータスでフィルタすることができます。次のようなステータスがあります。 ・ アクティブ。進行中のジョブ。 ・ キューに登録済み：開始できるようになるまで別のジョブの完了を待機しているジョブ。 ・ 待機しています。シードドライブなど、承認または完了を待機しているジョブ（シードドライブの詳細については、「レプリケーション」を参照してください）。 ・ 完了しました。正常に完了したジョブ。 ・ 失敗しました：失敗して完了できなかったジョブ。
サービスアイコン	このボタンを使用すると、サービスジョブがジョブのリストに追加されます。このアイコンをクリックすると、各ステータスアイコン上に小さなサービスアイコンが表示され、それらのステータスを持つサービスジョブでフィルタできるようになります（サービスジョブが存在する場合）。サービスジョブの例として、インデックスファイルの削除や保護からのマシンの削除などが挙げられます。
エクスポートタイプ ドロップダウンリスト	ドロップダウンリストには、イベントレポートをエクスポートできる形式が表示されます。タスクでのみ使用可能です。次のような形式があります。 ・ PDF

UI エlement	説明
	- HTML - CSV - XLS - XLSX
 (エクスポートアイコン)	選択した形式にイベントレポートを変換します。タスクでのみ使用可能です。
ページ選択	イベントレポートには、複数のページにわたって数個のジョブを含めることができます。イベント ページの下部にある番号や矢印を使用して、レポートの他のページに移動できます。

イベント ページでは、すべてのイベントが1つの表に表示されます。次の表は、項目 ごとに表示される情報のリストです。

表 6. イベントのサマリ表の詳細情報

UI エlement	説明
ステータス	タスク、アラート、またはジャーナルのアイテムのステータスが表示されます。アラートまたはジャーナルのアイテムで使用可能です。ヘッダーをクリックすると、ステータスで結果がフィルタされます。
名前	名前はタスクにのみ使用できます。このテキストフィールドには、この保護対象マシンの完了したタスクタイプのリストが表示されます。例としては、ボリュームの転送、リポジトリの維持、ロールアップ、実行マウント可否チェック、チェックサムチェックなどがあります。
開始時刻	タスク、アラート、およびジャーナルのアイテムで使用可能です。ジョブまたはタスクが開始された日付と時刻を表示します。
終了時刻	タスクでのみ使用可能です。タスクが完了した日付と時刻を表示します。
 ジョブの詳細	タスクでのみ使用可能です。 アクティブなタスクをモニタ ダイアログボックスが開き、特定のジョブまたはタスクの詳細を表示することができます。これらの詳細には、ジョブの ID、Core がデータを転送したレート（該当する場合）、ジョブの完了までの経過時間、ギガバイト単位での作業の合計、およびジョブに関連付けられている子タスクが含まれます。
Message (メッセージ)	アラートおよびジャーナルのアイテムで使用可能です。このテキストフィールドには、アラートまたはジャーナルのアイテムを説明するメッセージが表示されます。

保護対象マシンのレポートの表示

レポート  ドロップダウンメニューでは、必要に応じて、選択した保護対象マシンのレポートを生成できます。

このジョブのレポートでは、選択したマシンで正常に実行されたジョブと失敗したジョブのステータスに関するレポートが提供されます。失敗したジョブについては、失敗レポートに詳細を表示できます。このレポートタイプの詳細については、「[ジョブレポートについて](#)」を参照してください。

失敗に関するレポートでは、指定したマシンで失敗してキャンセルされた Core ジョブについての情報が報告されます。このレポートタイプの詳細については、「[失敗レポートについて](#)」を参照してください。

これらのレポートの生成については、「[オンデマンドでの Core レポートの生成](#)」を参照してください。

ナビゲーションメニューからのレプリケートされたマシンの表示

Core が別の Rapid Recovery Core からマシンをレプリケートする場合、ソース Core の表示名は折りたたみ可能なメニューとして Core Console の左のナビゲーションに表示されます。ナビゲーションエリアにあるすべてのメニューラベルの場合と同様に、このレプリケートされたマシンメニュー名は、保護されているマシンメニューの下にすべて大文字で表示されます。デフォルトでは、レプリケートされたマシンメニューは完全に展開され、そのソース Core から送信され、ターゲット Core にレプリケートされるすべてのマシンが一覧表示されます。

このメニューの左側にある矢印をクリックして、ソース Core からレプリケートされたマシンの表示を折りたたんだり展開したりできます。

レプリケートされたマシンメニューの右側にはそれぞれドロップダウンメニューが含まれており、これには Core から送信されるすべてのレプリケートされたマシンで同時に実行できる機能がリストされます。レプリケートされたマシンメニューの右側にある矢印をクリックすると、実行できる機能のドロップダウンリストが表示されます。次のような機能を実行できます。

- ・ レプリケーションを一時停止します。レプリケーションが現在アクティブな場合は、ユーザーが再開するまでレプリケーションを停止します。
- ・ レプリケーションを再開します。レプリケーションが一時停止されている場合は、再度レプリケーションが再開します。
- ・ レプリケーションを強制実行する。スケジュールされた時刻ではなく、必要な時にレプリケーションが実行されます。
- ・ レプリケーションを削除する。ソース Core とターゲット Core 間のレプリケーション関係を削除します。必要に応じて、この Core に保存されているリカバリポイントを削除できます。詳細については、「[レプリケーションの削除](#)」を参照してください。

ナビゲーションメニューでソース Core の名前を直接クリックすると、**[ソース Core 名] からレプリケートされたマシン** ページがメインコンテンツエリアに表示されます。このページで実行できる操作の詳細については、「[入力方向および出力方向のレプリケーションの表示](#)」を参照してください。

関連するリンク

- [レプリケーションの一時停止と再開](#)
- [レプリケーションの強制実行](#)
- [レプリケーションの削除](#)

「リカバリポイントのみ」メニューの表示

次のいずれかの条件が当てはまる場合、リカバリポイントのみメニューが左側のナビゲーションエリアに表示されます。

- ・ Rapid Recovery Core が以前保護されていたマシンから一部のリカバリポイントを保持している
- ・ レプリケーションを削除しても、リカバリポイントは保持している

ナビゲーションエリアにあるすべてのメニューラベルの場合と同様に、このメニューのラベルもすべて大文字で表示されます。

このメニューの左側にある矢印をクリックして、リカバリポイントのみのマシンの表示を折りたたんだり展開したりできます。

このメニューの右側にはドロップダウンメニューが含まれており、これにはすべてのリカバリポイントのみのマシンで同時に実行できる機能がリストされます。この場合は、Core からリカバリポイントを削除する機能のみを実行できます。

△ 注意: このアクションでは、**Rapid Recovery Core** にあるすべてのリカバリポイントのみのマシンが完全に削除され、この Core からそれらのリカバリポイントの情報をリストアップできなくなります。

カスタムグループ メニューの表示

カスタムグループ メニューは、1つ以上のカスタムグループを定義している場合にのみ、左側にあるナビゲーションエリアに表示されます。ナビゲーションエリアにあるすべてのメニューラベルと同様に、このメニューのラベルもすべて大文字で表示されます。

このメニューの左側にある矢印をクリックして、メニュー内のアイテムの表示を折りたたんだり展開したりできます。

カスタムグループ メニューの右側にはドロップダウンメニューが含まれており、これにはそのグループ内のすべての類似するアイテムで同時に実行できる機能がリストされます。

詳細については、「[カスタムグループについて](#)」を参照してください。

「エラー」 ダイアログボックスの使用

無効なパラメータを入力しようとするなど、Rapid RecoveryRapid Recovery Core Console ユーザーインターフェイスでエラーが発生すると、エラー ダイアログボックスが表示されます。通常、このダイアログボックスには、エラーの原因、エラーに関する詳細を提供するリンク、および「閉じる」ボタンが表示されます。続行するには「エラー」ダイアログボックスを閉じる必要がありますが、エラーに関する詳細を表示することもできます。

「エラー」ダイアログボックスで、次のオプションを選択します。

ユーザーインターフェイスエラーが原因でエラー ダイアログボックスが表示された場合、そのエラーは単に検証エラーまたはデータ入力エラーであるため、Rapid Recovery の イベント タブでは追跡されません。ただし、エラーの「ナレッジベースを検索」オプションをクリックすると、そのエラーの URL リンクが CoreAppRecovery.log ファイルに記録されます。ログでテキスト文字列「KB article url generated」を検索し、ブラウザで表示した各エラーの URL を確認できます。Core エラーログのダウンロードまたは表示の詳細については、「[Core ログファイルのダウンロードと表示](#)」または「[Core ログへのアクセス](#)」のトピックをそれぞれ参照してください。

Core 設定

本項では、 設定 アイコンから Rapid Recovery Core の設定を管理および変更する方法について説明します。

Rapid Recovery Core の設定

Rapid Recovery Core の設定は、デフォルトでほとんどのユーザーに最適なパフォーマンスを提供するように設定されています。これらの設定は Rapid Recovery Core のパフォーマンスに影響し、場合によっては Rapid Recovery Core Console の情報の表示に影響し

ます。アイコンバーで、 (設定) をクリックして Core の設定に移動します。すべての Core 設定のリストが左側に表示されます。このリストの設定のタイトルをクリックして、右側の詳細な設定にジャンプします。または、右側ですべての Core 設定を下にスクロールして、すべての設定オプションを確認することもできます。詳細については、「[Rapid Recovery Core の設定](#)」を参照してください。

また、システム情報のサマリの表示や Core ログファイルのダウンロードなど、Core のツールにアクセスすることもできます。詳細については、「[Core レベルのツール](#)」を参照してください。

構成可能な Rapid Recovery Core 設定の包括的なセットを次の表に示します。

表 7. Rapid Recovery Core の構成可能な設定

構成設定	説明
Core 設定をバックアップ / Core 設定をリストア	Rapid Recovery では、Core 設定を XML ファイルにバックアップできます。バックアップファイルがある場合は、それを使用して Core 設定をリストアまたは移行できます。 Core 設定のバックアップと復元の詳細については、「Core 設定のバックアップとリストア」を参照してください。
一般	一般設定には、Web サーバおよび Rapid Recovery サービスの表示オプションとポートなど、Rapid Recovery Core に一般的に適用される設定オプションが含まれています。 これらの設定の構成方法など、Rapid Recovery Core の一般設定の詳細については、「Core 一般設定の構成」を参照してください。
アップデート	アップデート設定は、Rapid Recovery ソフトウェアのアップデートバージョンをチェックする自動アップデート機能をコントロールします。 これらの設定の構成方法など、Rapid Recovery Core のアップデート設定の詳細については、「アップデート設定の構成」を参照してください。
夜間ジョブ	夜間ジョブ設定は、Core で毎日実行される自動化タスクです。ジョブの開始時刻および実行するジョブを設定できます。Dell ジョブのスケジュールは通常の営業時間外に設定し、リソースの需要が高い時間のシステムの負荷を軽減することをお勧めします。 詳細については、「夜間ジョブの理解」、「Core の夜間ジョブの設定」、および「保護対象マシンの夜間ジョブのカスタマイズ」を参照してください。
転送キュー	転送キュー設定は、リソースを使用できないためにジョブが失敗した場合に、転送操作を試行する回数をコントロールします。最大同時転送数およびデータ転送の最大試行回数を設定できます。 転送キュー設定の詳細については、「転送キュー設定の変更」を参照してください。
クライアントのタイムアウト	クライアントのタイムアウト設定では、特定の接続リクエストまたは読み取りおよび書き込み操作の試行がタイムアウトするまでの時間を決定します。 クライアントのタイムアウト設定の詳細については、「クライアントタイムアウト設定の調整」を参照してください。
DVM 重複排除キャッシュ	重複排除によって、情報の一意のブロックがリポジトリに1回のみ保存され、繰り返されるデータブロックへの参照が作成されます。この参照は重複排除キャッシュに保存されます。暗号化キーが使用されている場合、重複排除は各暗号化ドメイン内で行われます。 DVM 重複排除のキャッシュ設定では、キャッシュのサイズを設定し、プライマリキャッシュとセカンダリキャッシュの場所およびメタデータキャッシュの場所を指定できます。 重複排除キャッシュの詳細については、「重複排除キャッシュと保存場所について」を参照してください。設定の調整の詳細については、「重複排除キャッシュ設定の構成」を参照してください。
Replay エンジン	Replay エンジンの設定は、IP アドレスやタイムアウト設定などの、Replay エンジン用の通信チャンネルに関する情報を制御し、お使いのネットワークのニーズに合わせてパフォーマンスを調整するのに役立ちます。 Rapid Recovery のエンジン設定の詳細については、「Replay エンジン設定の構成」を参照してください。
導入	展開設定では、Core から保護対象マシンに Rapid Recovery Agent ソフトウェアを展開するオプションを設定できます。 展開設定の構成については、「導入設定の構成」を参照してください。
データベース接続	Rapid Recovery は、デフォルトで Core マシンのローカルにインストールされる MongoDB サービスデータベースにトランザクション情報を保存します。これらの設定を構成して、データベースに情報が保持される期

構成設定	説明
	間を変更したり、許可される同時接続数を増減するために接続プールサイズを変更したりすることができます。 サービスデータベースのデータベース接続の設定を確立または変更する方法については、「データベース接続の設定の構成」を参照してください。
ローカルデータベース	Rapid Recovery の イベント ページには、Core のタスク、イベント、およびアラートに関する情報が表示されます。Rapid Recovery は、このトランザクション情報を Rapid Recovery Core と同じマシンのローカルにインストールされる MongoDB サービスデータベースに保存します。 ローカルデータベース設定を使用して、ローカル Mongo サービスデータベースの資格情報（ユーザー名とパスワード）を構成できます。ローカルデータベースの設定を調整する方法については、「ローカルデータベースの接続設定の変更」を参照してください。
SMTP サーバー	Core で SMTP サーバ設定を構成すると、Core のイベント情報を電子メールで送信することもできます。SMTP 電子メールサーバーの設定の詳細については、「電子メールサーバーの設定」を参照してください。 ① メモ: イベント情報を電子メールで送信するには、通知グループ設定も構成する必要があります。電子メールアラートを受信するためのイベントの指定方法については、「通知グループの設定」を参照してください。
クラウド設定	クラウド設定 では、サポート対象のクラウドストレージのアカウントの構成設定を指定できます。これらの設定ではクラウドアカウントは作成されません。代わりに、既存のクラウドストレージアカウントを Rapid Recovery Core に関連付けて、Rapid Recovery 情報のアーカイブなどの操作を簡単に実行できるようにすることが可能です。 Rapid Recovery Core のクラウドストレージアカウント情報を管理する方法については、「クラウドアカウントの管理」を参照してください。
レポート	レポート設定には、Rapid Recovery Core からレポートを生成するときに使用されるフォントを選択できる 1 つの設定パラメーターがあります。 レポート設定を変更する方法については、「レポート設定の管理」を参照してください。
アタッチ可否	アタッチ可否の設定では、保護対象マシンで SQL アタッチ可否チェックを実行するかどうか、または Core で SQL Server インスタンスを使用するかどうかを指定できます。Core で SQL を指定する場合は、資格情報を指定する必要があります。 Core での SQL アタッチ可否 設定の管理については、「Core の SQL アタッチ可否設定の管理」を参照してください。
ジョブ	レプリケーションなどの操作を開始すると、Core ジョブが自動的に作成されます。ジョブ の Core 設定では、各ジョブの設定を指定できます。 一度に実行するジョブの数を設定できます。ネットワークまたは他の通信エラーにより初回のジョブに失敗した場合のジョブの試行回数を設定できます。 Core ジョブ、使用可能なジョブ、およびそれらの設定方法の詳細については、「Core ジョブの設定」を参照してください。
ライセンス	Core Console では、Rapid Recovery を使用して、Core に関連付けられたライセンスの変更、日常のスナップショット数の制限、ライセンスプール情報の表示、ライセンスサーバへの接続を行うことができます。 Core からのライセンス管理の詳細については、「ライセンスの管理」を参照してください。 ライセンス管理の詳細については、Dell Data Protection Rapid Recovery ライセンスポータルガイドを参照してください。 ① メモ: Dell Data Protection Rapid Recovery ライセンスポータルのリリースサイクルは、Rapid Recovery ソフトウェアとは異なります。最新の製品ドキュメントについては、Dell Technical Documentation Web サイトを参照してください。

構成設定	説明
SNMP 設定	簡易ネットワーク管理プロトコル（SNMP）は、IP ネットワーク上のデバイスを管理するためのプロトコルです。Rapid Recovery Core は SNMP エージェントとして設定できます。この設定後、Core はアラート、リポジトリのステータス、保護対象マシンなどの情報をレポートできます。 Rapid Recovery で SNMP を使用方法については、「SNMP 設定について」を参照してください。
vSphere	vSphere Core の設定は、仮想マシンのエージェントレス保護のユーザーにのみ適用されます。vSphere ホストを使用している場合、これらの設定には VM に適用される設定が含まれています。 VMware または ESXi エージェントレス保護に関する vSphere 設定の詳細については、「vSphere 設定の構成」を参照してください。
ログのアップロード	このオプションを はい に設定すると、Rapid Recovery Core は全体的な製品品質を改善する持続的努力の一環として、解析用のログファイルを Dell にアップロードします。この設定はオプションです。

Core 一般設定の構成

Rapid Recovery Core の一般設定には、Core 表示名、Web サーバ、サーバポート、およびロケール（Core Console 表示言語）があります。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、（設定）をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**一般**をクリックします。
 - ・ 設定 ページの右側で、一般 の見出しが表示されるまで下にスクロールします。
一般 の Core 設定が表示されます。
- 3 変更する一般設定をクリックします。
選択した設定は、テキストフィールドまたはドロップダウンメニューとして編集できるようになります。
- 4 次の表の説明に従って、設定情報を入力します。

表 8. 一般設定情報

テキストボックス	説明
表示名	Core の新しい表示名を入力します。これは、Rapid Recovery Core Console に表示される名前です。64 文字まで入力できます。
Web サーバーポート	Web サーバーのポート番号を入力します。デフォルトポートは 8006 です。
サービスポート	Rapid Recovery Core サービスのポート番号を入力します。デフォルトポートは 8006 です。
ロケール	ロケール ドロップダウンリストから、表示する言語を選択します。 英語、フランス語、ドイツ語、日本語、韓国語、ポルトガル語、簡体字中国語、およびスペイン語から選択できます。

① メモ: 言語を変更した場合は、**Rapid Recovery Core** サービスを再起動する必要があることを示すメッセージを確認すると、アップデートした言語が **Core Console** に表示されるようになります。**Windows** タスクマネージャからこのサービスを再開できます。

- 5 希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。

アップデート設定の構成

Rapid Recovery には、自動アップデートの機能が含まれています。Rapid Recovery Core をインストールするときに、新しいアップデートを利用できる場合に Rapid Recovery Core ソフトウェアを自動的にアップデートできるかどうかと、アップデートのチェック頻度を選択できます。

Rapid Recovery リリース番号は、通常、小数点で区切られる 4 つの情報のまとまりから構成されます。4 つの情報とは、メジャーリリース番号、マイナリリース番号、リビジョン、およびビルド番号です。たとえば、リニューアルした Rapid Recovery の最初のリリースは 6.0.1.609 です。次のリリースは、6.0.2.142 です。

自動アップデート機能では、リリース番号に含まれるすべての数字を比較します。自動アップデートが有効な場合、メジャーリリース番号およびマイナリリース番号が同一の時のみ Core ソフトウェアは外部からの介入なしでアップデートされます。たとえば、Core のバージョンが 6.0.1.609 から 6.0.2.142 (両方 6.0 ではじまっています) になる場合は、自動アップデートが行われます。同じマシン上でも、Core のバージョンが 6.0.2.142 から 6.1.1.XXX になる場合は、はじめの小数点の後の桁が同じではないため、自動アップデートは行われません。代わりに、Core ソフトウェアのアップデートが入手可能になった旨の通知が (Core Console の上部にあるバナーに) 行われます。この通知は、リリースノートを確認し、最新の Core バージョンへのアップデートがニーズに対して適切かどうかを判断するよい機会になります。

① **メモ:** Rapid Recovery Core ソフトウェアのインストールについては、**Dell Data Protection | Rapid Recovery** の『インストールおよびアップグレードガイド』を参照してください。

アップデートのチェックで使用される設定をいつでも表示、変更することができます。

△ **注意:** レプリケーションを使用している場合、アップデートを自動的にインストールするようにシステムを設定すると、ターゲット Core の前にソース Core がアップグレードされ、レプリケーションに失敗したり、Core 間で新しいレプリケーションを設定できなくなったりする可能性があります。レプリケーション機能を使用するユーザーの場合は、Dell 管理者がターゲット Core にのみ自動アップグレードを適用した後に、手動でソース Core をアップグレードし、最後に保護対象マシンをアップグレードすることをお勧めします。

アップデート設定を行うには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (設定) をクリックしてから、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**アップデート** をクリックします。
 - ・ 設定 ページの右側で、アップデート の見出しが表示されるまでスクロールダウンします。アップデート の Core 設定が表示されます。
- 3 変更する設定をクリックします。
選択した設定が編集可能になります。
- 4 次の表の説明に従って、設定情報を入力します。

表 9. アップデートの設定情報

テキストボックス	説明
新規アップデートのチェック	Rapid Recovery がアップデートをチェックしてインストールする頻度を選択しします。次のいずれかのオプションを選択できます。 ・ 確認しない ・ 日次 ・ 週次 ・ 月次

テキストボックス 説明

自動アップデートを選択すると、選択したしきい値の期間が経過した後で使用可能なアップデートがある場合は、夜間ジョブの完了後にそれがインストールされます。

アップデートをインストール	利用可能なアップデートの処理方法を、次のいずれかのオプションから指定します。 ・ 「アップデートを確認しない」 ・ 「アップデートの通知は受けるが、自動的にアップデートをインストールしない」 ・ アップデートを自動的にインストール
ステータス	このステータスは、新しいアップデートが使用可能かどうかを示します。
最後のチェック	最後のチェック フィールドには、システムがアップデートを最後にチェックした日付と時刻が示されます。 ソフトウェアアップデートを利用可能であるかどうか直ちに検証する場合は、今すぐチェック をクリックします。このチェックは、設定した頻度とは無関係に実行されます。

- 5 各設定の変更が完了したら、 をクリックして変更内容を保存して編集モードを終了します。または、 をクリックして変更内容を保存せずに編集モードを終了します。

夜間ジョブの理解

夜間ジョブは通常の営業時間外の所定の時間に発生する毎日の自動タスクです。これらのジョブは、大量のメモリを使用し、さまざまな整合性チェックとデータの統合タスクを含みます。これらのタスクは、Rapid Recovery (迅速な回復) コアがあまりアクティブでないときに実行されるのが最善です。

すべての夜間ジョブ、およびそれらが適用されている範囲は、次の表で説明します。夜間ジョブは (Core で保護されるすべてのマシンに適用される) Core レベルで管理されます。特定の保護されたマシンリストにも適用されるこれらの夜間ジョブは、「保護されたマシン」として範囲がリストされます。

表 10. 夜間ジョブ情報

ジョブ名	範囲	説明
 変更	該当なし	このコントロールは、Nightly Jobs (夜間ジョブ) ダイアログボックスを開きます。このダイアログボックスでは、各夜間ジョブを有効または無効にしたり、設定を変更したりすることができます。
Nightly jobs time (夜間ジョブ時刻)	すべて	この設定は実行を開始する予定の夜間ジョブの時刻を示します。Dell は、アクティビティがあまり行われていない時刻に夜間ジョブを実行するように Core を設定することをお勧めします。 デフォルトの時刻は 12:00 AM です。
Rollup (ロールアップ)	Core or protected machine (Core または保護されたマシン)	ポリシーで規定されているスケジュールでリカバリポイントを組み合わせるか、「ロールアップ」することでバックアップデータへ保持ポリシーを適用します。Core でポリシーをカスタマイズでき、これはデフォルトですべての保護マシンに適用されます。デフォルトでは、ロールアップジョブが Core 全体に対して実行されます。またはを  どの保護対象マシンに Core ポリシーを使用してロールアップを実行させるかを定義します。 Core に設定されているデフォルトのポリシーとは異なり、保護対象マシンで保持ポリシーを使用する方法の詳細については、保護対象マシンの保持ポリシー設定のカスタマイズを参照してください。

ジョブ名	範囲	説明
Check attachability of SQL databases (SQL データベースのアタッチ可否チェック)	Protected Machine (保護されたマシン)	SQL データベースを含むリカバリポイントの整合性をチェックします。プロセス: - データベースを含む保護グループの最新のリカバリポイントをマウントします。 - SQL Server からデータベースに接続します。 - データベースを開きます。 - データベースを閉じます。 - リカバリポイントをマウント解除します。 この夜間チェックを有効にするには、保護対象マシンの SQL Server データベースでアタッチ可否チェックを実行するために、SQL Server インスタンスを指定し、使用します。 ① メモ: このオプションは、Core の SQL Server を保護していない場合には表示されません。
Download logs from protected machines (保護されたマシンからログをダウンロード)	Core (コア)	保護対象マシンから Core に対してログをダウンロードし、ログサーバーに送信されるようにします。
Consolidate VMware snapshots for protected virtual machines (保護された仮想マシン用に VMware スナップショットを統合)	Core or protected machine (Core または保護されたマシン)	ネイティブ VMware API を使用して、Rapid Recovery (迅速な回復) エージェントソフトウェアなしにマシンを保護する場合には、この夜間ジョブは関連します。 VMware スナップショットを定期的に統合する必要があります。この夜間ジョブを有効にすると、これらの統合が毎日実行されます。この夜間ジョブには、Maximum simultaneous consolidations (最大同時統合) という 1 つのパラメータが含まれていて、これは 1 から 100 までの数に設定する必要があります。
Check integrity of recovery points (リカバリポイントの整合性をチェック)	Core or protected machine (Core または保護されたマシン)	各保護対象マシンのリカバリポイントの整合性を確認します。デフォルトでは、Check integrity of recovery points オプションは有効になっていません。 プロセス: - 各保護グループの最新のリカバリポイントをマウントします。 - 各ボリュームのファイルとフォルダを列挙します。 - リカバリポイントを調べ、それらが有効であることを確認します。 - リカバリポイントをマウント解除します。
Check checksum of Exchange databases (Exchange データベースのチェックサムを確認)	Protected Machine (保護されたマシン)	Exchange Database (EDB) ファイルを含むリカバリポイントの整合性を確認します。 ① メモ: このオプションは、Core で Exchange Server を保護していない場合には表示されません。
Truncate SQL logs (simple recovery model only) (SQL ログの切り捨て (単純なリカバリモデルのみ))	Protected Machine (保護されたマシン)	データベーストランザクションのログを切り捨てて、最後のリカバリポイントに一致させることで、SQL Server ログのサイズを保持します。 ① メモ: このオプションは、Core の SQL Server を保護していない場合には表示されません。

ジョブ名	範囲	説明
Truncate Exchange logs (Exchange ログの切り捨て)	Protected Machine (保護されたマシン)	Exchange データベースのトランザクションログを切り捨て、最後のリカバリポイントに一致させることで、Exchange ログのサイズを保持します。 ① メモ: このオプションは、Core で Exchange サーバーを保護していない場合には表示されません。
Log repository statistics (ログリポジトリの統計)	Core (コア)	リポジトリの統計をログサーバーに送信します。
Delete old events and jobs (古いイベントおよびジョブの削除)	Core (コア)	古いイベントを削除して、イベントデータベースのスケールを保持します。日数は設定可能です。デフォルトは 30 日です。

Core の夜間ジョブの設定

Rapid Recovery Core で夜間ジョブが有効になっている場合、選択したジョブは Core によって保護されているすべてのマシンで指定された時間に、毎日 1 回実行されます。逆に、Core レベルで夜間ジョブを無効にすると、Core によって保護されているすべてのマシンでジョブが実行されなくなります。

① メモ: 夜間ジョブの範囲（「[夜間ジョブの理解](#)」のトピックを参照）に保護対象マシンが含まれている場合は、1 つまたは複数の特定の保護対象マシンにのみ、個別にその夜間ジョブを適用できます。保護対象マシン固有の夜間ジョブ設定の適用の詳細については、「[保護対象マシンの夜間ジョブのカスタマイズ](#)」を参照してください。

夜間ジョブはメモリ集中型であるため、Dell 負荷の低い時間帯にジョブを実行するように Core を設定することをお勧めします。夜間ジョブを実行するデフォルトのスケジュールは 12:00 AM です。別の時間の方が適切な場合は、次の手順を実行して夜間ジョブの時間フィールドでこの設定を変更します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、（設定）をクリックしてから、次のいずれかを実行します。
 - ・ **設定** ページの左側にある Core 設定のリストから、**夜間ジョブ** をクリックします。
 - ・ **設定** ページの右側で、夜間ジョブの見出しが表示されるまでスクロールダウンします。
夜間ジョブの Core 設定が表示されます。
- 3 夜間ジョブを変更するか、または夜間ジョブの実行を開始する時間を変更する場合は、 **変更** をクリックします。
夜間ジョブ ダイアログボックスが表示されます。
- 4 夜間ジョブを実行する時間を変更する場合は、**夜間ジョブの時間** テキストボックスに新しい時間を入力します。
- 5 最初の行で、Core に設定する各夜間ジョブのオプションをクリックして選択します。選択したオプションのいずれかをクリックすると、そのオプションはオフになります。
- 6 **OK** をクリックします。
夜間ジョブ ダイアログボックスが閉じ、お使いの夜間ジョブの Core 設定が保存されます。

転送キュー設定の変更

転送キュー設定は、データを転送するための最大同時転送数と最大再試行回数を決定するコアレベルの設定です。

転送キュー設定を変更するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで （設定）をクリックし、次のいずれかを実行します。

- ・ 設定 ページの左側にある Core 設定のリストから、**転送キュー** をクリックします。
 - ・ 設定 ページの右側で、転送キュー の見出しが表示されるまでスクロールダウンします。
転送キュー の Core 設定が表示されます。
- 3 変更する設定をクリックします。
選択した設定が編集可能になります。
 - 4 次の表の説明に従って、設定情報を入力します。

表 11. 転送キューの設定情報

テキストボックス	説明
最大同時転送数	同時転送数をアップデートする値を入力します。 1～60 の数値を設定します。数値が小さいほど、ネットワークおよびその他のシステムリソースにかかる負荷も小さくなります。処理される Agent の数が増えるにつれて、システムにかかる負荷も大きくなります。
Maximum Retries (最大再試行回数)	転送操作をキャンセルするまでの最大試行回数を設定する値を入力します。 1～60 の数値を設定します。

- 5 希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。

クライアントタイムアウト設定の調整

クライアントのタイムアウト設定は、さまざまな操作の試行がタイムアウトするまでの時間を制御します。

- ① **メモ:** Dell ご使用の環境で特定の問題が発生している場合や、Dell サポート担当者から設定の変更を指示されている場合を除き、タイムアウト設定はデフォルトのままにすることをお勧めします。

クライアントタイムアウト設定を調整するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (設定) をクリックしてから、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**クライアントのタイムアウト** をクリックします。
 - ・ 設定 ページの右側で、クライアントのタイムアウト の見出しが表示されるまでスクロールダウンします。
クライアントのタイムアウト の Core 設定が表示されます。
- 3 変更する設定をクリックします。
選択した設定が編集可能になります。
- 4 次の表の説明に従って、設定情報を入力します。
- 5

表 12. クライアントのタイムアウト の設定情報

設定	説明
接続タイムアウト	ハイパーテキスト転送プロトコル (http) を介してデータを送信する場合の、Core と保護対象マシン間の接続タイムアウトを制御します。 接続がタイムアウトするまでの経過時間を入力します。HH:MM:SS の形式を使用します。

① | **メモ:** デフォルト設定は **0:05:00**、つまり **5 分間**です。

読み取り / 書き込みタイムアウト http を介してストリームデータを読み取りまたは書き込みする場合の、Core と保護対象マシン間の接続タイムアウトを制御します。例として、増分スナップショットの実行で、保護対象マシンから Core への変更データブロックの送信する場合などです。
読み取り / 書き込みイベントの最中にタイムアウトが発生するまでの経過時間を入力します。HH:MM:SS の形式を使用します。

① | **メモ:** デフォルト設定は **0:05:00**、つまり **5 分間**です。

接続 UI タイムアウト http を介したグラフィックユーザーインターフェースと Rapid Recovery Core サービス間の接続のタイムアウトを制御します。
UI 接続がタイムアウトするまでの経過時間を入力します。HH:MM:SS の形式を使用します。

① | **メモ:** デフォルト設定は **0:05:00**、つまり **5 分間**です。

読み取り / 書き込み UI タイムアウト http を介したグラフィックユーザーインターフェースと Rapid Recovery Core サービス間のデータ読み取り / 書き込みのタイムアウトを制御します。
読み取り / 書き込みイベントの最中にタイムアウトが発生するまでの経過時間を入力します。HH:MM:SS の形式を使用します。

① | **メモ:** デフォルト設定は **0:05:00**、つまり **5 分間**です。

- 6 各設定の変更が完了したら、 をクリックして変更を保存して編集モードを終了します。または、 をクリックして変更内容を保存せずに編集モードを終了します。

重複排除キャッシュと保存場所について

グローバル重複排除により、Core のバックアップデータに必要なディスクストレージ容量が削減されます。各リポジトリは重複排除されます。つまり、それぞれの一意のブロックを一度物理的にディスクに保存し、後続のバックアップでそれらのブロックへの仮想参照またはポインタを使用します。重複ブロックを識別するため、Rapid Recovery には重複排除ボリュームマネージャ (DVM) リポジトリの重複排除キャッシュが含まれています。このキャッシュは、固有ブロックへの参照を保持します。

デフォルトで、DVM リポジトリ用の重複排除キャッシュは 1.5 GB です。これは、多くのリポジトリに適切なサイズです。このキャッシュ容量を超えるまで、データはリポジトリ全体で重複排除されます。冗長な情報の量が多く重複排除キャッシュが満杯になると、リポジトリでは、新しく追加されたデータに対して、それ以降の重複排除を行うことができなくなります。重複排除キャッシュが満杯になるまでリポジトリに保存できるデータの容量は、バックアップ対象のデータのタイプに応じて異なり、また、すべてのユーザーで異なります。

Rapid Recovery Core では、重複排除キャッシュ設定を変更することで、DVM 重複排除キャッシュのサイズを増やすことができます。キャッシュサイズを増やす方法については、「[重複排除キャッシュ設定の構成](#)」のトピックを参照してください。

DVM 重複排除キャッシュのサイズを増やす場合は、ディスク容量と RAM の使用量という 2 つの要因について考慮する必要があります。

ディスク容量。 ディスクには、DVM 重複排除キャッシュの 2 つのコピー、つまりプライマリキャッシュと、パラレルコピーであるセカンダリキャッシュが保存されます。したがって、DVM リポジトリのデフォルトのキャッシュサイズ 1.5 GB を使用している場合は、3 GB のディスクストレージがシステムで使用されます。キャッシュサイズを増加するときは、使用ディスク容量は、常にキャッシュサイズの 2 倍になります。適切かつ耐障害性のあるパフォーマンスを実現するため、Core ではプライマリキャッシュとセカンダリキャッシュの優先順位を動的に変更します。両方とも必須のキャッシュです。唯一の違いは、プライマリとして設定されているキャッシュに先にデータが保存されるということです。

RAM の使用量。Rapid Recovery Core を起動すると、RAM に重複排除キャッシュがロードされます。このため、キャッシュのサイズはお使いのシステムのメモリ使用量に影響します。Core が使用する RAM の合計容量は、多くの要因に依存します。これらの要因には、実行中の操作、ユーザーの数、保護対象マシンの数、および重複排除キャッシュのサイズが含まれます。Core が実行するそれぞれの操作（転送、レプリケーション、ロールアップなど）はさらに多くの RAM を消費します。操作が完了すると、それに応じて、メモリ消費量も減ります。ただし、管理者は、効率的な操作を実現するため、RAM の最大負荷要件を考慮する必要があります。

Rapid Recovery Core の場所のデフォルト設定は、AppRecovery ディレクトリ内の DVM リポジトリのプライマリキャッシュ、セカンダリキャッシュ、およびメタデータキャッシュに保存されます。このフォルダは Core マシンにインストールされます。

❶ **メモ:** 設定によっては、AppRecovery ディレクトリが Rapid Recovery Core で表示されないようになっている場合があります。このディレクトリを表示するには、非表示のファイル、フォルダ、およびドライブを表示するように、コントロールパネルのフォルダ表示 オプションの設定を変更する必要があります。

Rapid Recovery Core が C ドライブにインストールされているとすると、これらの場所は、通常、次のようになります。

表 13. DVM 重複排除キャッシュ設定のデフォルトの保存先

設定	デフォルトの保存先
プライマリキャッシュの場所	C:\ProgramData\AppRecovery\Repository\MetaData\PrimaryCache
セカンダリキャッシュの場所	C:\ProgramData\AppRecovery\Repository\MetaData\SecondaryCache
メタデータキャッシュの場所	C:\ProgramData\AppRecovery\Repository\MetaData\CacheMetadata

これらのキャッシュの保存を変更することができます。たとえば、フォールトトレランスを向上させるためには、セカンダリキャッシュの場所をプライマリキャッシュとは異なる物理ドライブに変更できます。この際、Rapid Recovery Core がそのドライブにアクセスできることが前提となります。

これらの設定のいずれかで保存先を変更する方法については、「[重複排除キャッシュ設定の構成](#)」のトピックを参照してください。

Dell 重複排除ストレージは別々にすることをお勧めします。重複排除は単一のリポジトリでのみ発生します（複数のリポジトリにまたがることはありません）。重複排除で Core ベースの暗号化を使用している場合、セキュリティを確保するために各キーは単一の暗号化ドメインを提供するので、重複排除は単一のキーによって保護されるデータに制限されます。

重複排除の詳細については、「[Rapid Recovery の重複排除](#)」を参照してください。

重複排除キャッシュ設定の構成

DVM リポジトリの重複排除キャッシュ設定を構成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで （設定）をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**DVM 重複排除キャッシュ** をクリックします。この設定は、Core に 1 つまたは複数の DVM リポジトリが存在する場合にのみ表示されます。
 - ・ 設定 ページの右側で、DVM 重複排除キャッシュ の見出しが表示されるまでスクロールダウンします。
DVM 重複排除キャッシュ の Core 設定が表示されます。
- 3 任意のタイミングで DVM 重複排除キャッシュのデフォルト設定を復元する場合は、次の手順を実行します。
 - a 重複排除キャッシュの設定領域の一番上にある **デフォルトにリストア** をクリックします。
デフォルトにリストア ダイアログボックスが表示されます。
 - b **はい** をクリックして復元を確認します。
- 4 変更する設定をクリックします。

選択した設定が編集可能になります。

- 5 個々の重複排除キャッシュ設定を変更する場合は、次の表の説明に従って情報を入力します。

表 14. DVM 重複排除キャッシュの設定情報

設定	説明
 デフォルトにリストア	このコントロールは、DVM キャッシュの場所をシステムのデフォルトの場所にリセットします。各設定については、以下の説明を参照してください。
プライマリキャッシュの場所	DVM リポジトリの一次キャッシュの場所を変更する場合は、一次キャッシュの場所 テキストボックスで Core からアクセスできる保存先へのパスを入力します。 デフォルトの場所は次のとおりです。 C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache 一次キャッシュと二次キャッシュは同じサイズであるため、これら 2 つのキャッシュをまとめたストレージには、重複排除キャッシュサイズに割り当てられている容量の 2 倍の容量が必要です。たとえば、重複排除キャッシュサイズにデフォルトの容量の 1.5 GB を指定する場合は、2 つの保存先のそれぞれに少なくとも 1.5 GB が必要です。特に、両方の場所が同じドライブ (C ドライブなど) に属している場合、少なくとも 3.0GB の空きディスク容量が必要です。
セカンダリキャッシュの場所	DVM リポジトリの二次キャッシュの場所を変更する場合は、二次キャッシュの場所 テキストボックスで Core からアクセスできる保存先へのパスを入力します。 デフォルトの場所は次のとおりです。 C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
キャッシュメタデータの場所	DVM リポジトリのキャッシュメタデータの場所を変更する場合は、キャッシュメタデータの場所 テキストボックスで Core からアクセスできる保存先へのパスを入力します。 デフォルトの場所は次のとおりです。 C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata
重複排除キャッシュサイズ (GB)	DVM リポジトリの重複排除キャッシュサイズを変更する場合は、重複排除キャッシュサイズ テキストボックスに、新しい容量を入力します (GB 単位)。 デフォルトの場所は次のとおりです。 C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache 最小キャッシュサイズ設定は、1.5GB です。また、キャッシュサイズはインストールされている RAM の 50% を超えることはできません。

- 6 希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。

Replay エンジン設定の構成

Rapid Recovery の通信チャネルである Replay エンジンに関する情報を設定できます。これらの設定によって、効果的な通信を提供する Core 設定が決まります。

通常は Dell デフォルト設定を使用することをお勧めします。場合によっては、Dell サポートからご使用のネットワークのニーズに固有のパフォーマンスを調整するために、これらの設定の変更が指示されることがあります。

Replay エンジン設定を構成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (設定) をクリックしてから、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**Replay エンジン** をクリックします。
 - ・ 設定 ページの右側で、Replay エンジンの見出しが表示されるまでスクロールダウンします。
Replay エンジンの Core 設定が表示されます。
- 3 変更する設定をクリックします。
選択した設定が編集可能になります。
- 4 次の表の説明に従って、設定情報を入力します。

表 15. Replay エンジンの設定情報

テキストボックス	説明
IP アドレス	リカバリポイントのマウントおよび復元を実行するとき、Core はこの IP アドレスを使用して保護対象マシンと Core 間のフィードバックを許可します。 Replay エンジンの IP アドレスには、Core マシンの IP アドレスが自動的に入力されます。サーバの IP アドレスを手動で入力すると、保護対象マシンが自動的に提供された IP アドレスを解決できない場合に、この値が使用されます。 保護対象マシンで不具合が発生せず、Core と通信できる限り、この値を手動で設定する必要はありません
優先ポート	ポート番号を入力するか、デフォルト設定を使用します。デフォルトポートは 8007 です。 ポートは、Replay エンジンの通信チャネルを指定するために使用されます。
使用中のポート	Replay エンジン設定で使用中のポートを示します。
ポートの自動割当てを許可	TCP ポートの自動割当てを行う場合は、クリックします。
管理者グループ	管理者グループの新しい名前を入力します。デフォルト名は BUILTIN\Administrators です。
非同期 I/O 最小長	値を入力するか、デフォルト設定を選択します。非同期入出力の最小長を示します。 デフォルト設定は 65536 です。
読み取りタイムアウト	読み取りタイムアウト値を入力するか、デフォルト設定を選択します。デフォルト設定は 0:05:00 です。
書き込みタイムアウト	書き込みタイムアウト値を入力するか、デフォルト設定を選択します。デフォルト設定は 0:05:00 です。
受信バッファサイズ	受信バッファサイズを入力するか、デフォルト設定を受け入れます。デフォルト設定は 8192 です。
送信バッファサイズ	送信バッファサイズを入力するか、デフォルト設定を受け入れます。デフォルト設定は 8192 です。
遅延なし	このチェックボックスはオフのままにすることをお勧めします。オンにするとネットワーク効率に影響します。この設定を変更する必要がある場合は、Dell サポートまでお問い合わせの上、手順をご確認ください。

5 各設定の変更が完了したら、 をクリックして変更を保存して編集モードを終了します。または、 をクリックして変更内容を保存せずに編集モードを終了します。

導入設定の構成

Rapid Recovery では、Rapid Recovery Core から保護対象マシンにインストーラをダウンロードできます。

Core から保護対象マシンへの Rapid Recovery Agent ソフトウェアの展開に関する設定を構成できます。

導入設定を構成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (設定) をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**展開** をクリックします。
 - ・ 設定 ページの右側で、展開 の見出しが表示されるまでスクロールダウンします。
展開 の Core 設定が表示されます。
- 3 変更する設定をクリックします。
選択した設定が編集可能になります。
- 4 次の表の説明に従って、設定情報を入力します。

表 16. 展開の設定情報

テキストボックス	説明
Agent インストーラ名	デフォルトのファイル名は Agent-Web.exe です。何らかの理由でこのファイル名を変更したい場合は、この設定を使用して Core Web インストーラの実行可能ファイルに新しい名前を指定することができます。このファイルは最新バージョンの Rapid Recovery Core インストーラをストリーム方式でダウンロードします。このダウンロード処理は、Web から直接実行され、必要に応じて、処理を一時停止および再開できます。
Core アドレス	Core サーバーのアドレスを入力します。このアドレスは、通常はプロトコル、Core Server の名前とポート、および Core ファイルが置かれているディレクトリで構成されます。 たとえば、サーバー名が Sample の場合、この設定は https://sample:8006/apprecovery/admin/Core となります。
受信タイムアウトによる失敗	Agent ソフトウェアの導入の試行がタイムアウトするまでの時間。 デフォルト設定は 00:25:00、つまり 25 分間です。この設定を変更する場合は、読み取りまたは書き込みイベント中にタイムアウトが発生するまで、Agent ソフトウェアの展開をシステムに試行する時間の長さを入力します。HH:MM:SS の形式を使用します。
最大パラレルインストール	この設定は、一度に Core の Agent ソフトウェア導入を試行できる最大数を制御します。 デフォルト設定は 100 です。

- 5 希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。

データベース接続の設定の構成

Rapid Recovery の イベント ページには、Core のタスク、イベント、およびアラートに関する情報が表示されます。Rapid Recovery は、デフォルトでこのトランザクション情報を Core マシンのローカルにインストールされる MongoDB サービスデータベースに保存します。これらの設定を構成して、データベースに情報が保持される期間を変更したり、許可される同時接続数を増減するために接続プールサイズを変更したりすることができます。

2 番目の Rapid Recovery Core を使用している場合は、1 番目の Core のデータベース接続の設定で 2 番目の Core マシンを参照するように構成できます。こうすることで、両方の Core のイベントデータが 2 番目の Core の MongoDB に保存されるようになります。

または、Core のデータベース接続の設定で、ネットワーク経由で Rapid Recovery Core にアクセスできる MongoDB が個別にインストールされている、別のマシンを参照するように構成できます。この場合は Core のイベントトランザクションデータがローカルではなくそのサービスデータベースに保存されます。サービスデータベースのデータベース接続の設定を確立または変更する方法については、「[データベース接続の設定の構成](#)」を参照してください。

① **メモ:** Rapid Recovery Core のイベント情報を表示する方法については、「[タスク、アラート、およびジャーナルを使用したイベントの表示](#)」を参照してください。

ユーザーは、ネットワークを介して Rapid Recovery Core にアクセスできる別のマシンに MongoDB サービスデータベースをインストールするように指定できます。ご使用の Rapid Recovery Core のサービスデータベースが Rapid Recovery Core をホストするマシン以外のマシンにインストールされている場合は、これらの設定でデータベース資格情報（ユーザー名とパスワード）を指定する必要があります。

Rapid Recovery Core で使用されるサービスデータベースのデータベース接続の設定を変更するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、（設定）をクリックしてから、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**データベース接続** をクリックします。
 - ・ 設定 ページの右側で、データベース接続の見出しが表示されるまでスクロールダウンします。
データベース接続 の Core 設定が表示されます。
- 3 データベース接続 領域の一番上から、以下の操作を実行できます。
 - ・ **接続テスト** をクリックして、設定を検証します。
データベース接続の設定を変更した場合は、必ず接続をテストすることをお勧めします。
 - ・ **デフォルトにリストア** をクリックし、データベース接続のデフォルト設定をすべて復元します。
このアクションを確認するように求めるプロンプトが表示され、カスタマイズされたデータベース接続の設定がすべて破棄されます。
- 4 変更する設定をクリックします。
選択した設定が編集可能になります。
- 5 次の表の説明に従って、設定情報を入力します。

表 17. データベース接続 の設定情報

テキストボックス	説明
ホスト名	データベース接続のホスト名を入力します。 ① メモ: localhost がホストとして指定されたパラメータである場合、MongoDB は Core をホストするマシンのローカルにインストールされます。
ポート	データベース接続のポート番号を入力します。 ① メモ: デフォルト設定は 27017 です。
ユーザー名	MongoDB サービスデータベースに対する管理者権限を持つユーザーの名前を入力します。 ① メモ: ホスト名パラメータが localhost である場合、このフィールドは不要です。
パスワード	指定したユーザー名に関連付けられているパスワードを入力します。 ① メモ: ホスト名パラメータが localhost である場合、このフィールドは不要です。

テキストボックス	説明
保存期間（日）	サービスデータベースのイベントとジョブ履歴を保持する日数を入力します。
最大接続プールサイズ	動的に再利用できるキャッシュされたデータベース接続の最大数を設定します。 ① メモ: デフォルト設定は 100 です。
最小接続プールサイズ	動的に再利用できるキャッシュされたデータベース接続の最小数を設定します。 ① メモ: デフォルト設定は 0 です。

- 6 各設定の変更が完了したら、 をクリックして変更を保存して編集モードを終了します。または、 をクリックして変更内容を保存せずに編集モードを終了します。

ローカルデータベースの接続設定の変更

イベント ページには、Rapid Recovery Core に関連するシステムイベントが表示されます。Rapid Recovery Core は、MongoDB サービスデータベースにこのトランザクション情報を保存します。デフォルトで、このデータベースが Core マシン上にローカルインストールされ、データベース接続設定の詳細に含まれるデフォルトのホスト名は localhost になります。この場合、ループバックインタフェースがローカルネットワークインタフェースハードウェアをバイパスするので、データベース認証情報が不要になります。

必要に応じてセキュリティを強化するため、Rapid Recovery Core によって使用される MongoDB データベースの認証情報（ユーザー名とパスワード）を明示的に指定することができます。

- ① | **メモ:** **Rapid Recovery Core** のイベント情報を表示する方法については、「[タスク、アラート、およびジャーナルを使用したイベントの表示](#)」を参照してください。データベース接続設定の詳細については、「[データベース接続の設定の構成](#)」を参照してください。

データベース認証情報を指定してローカルデータベースの接続設定を変更するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで （設定）をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**ローカルデータベースの設定** をクリックします。
 - ・ 設定 ページの右側で、ローカルデータベースの設定 の見出しが表示されるまでスクロールダウンします。
ローカルデータベースの Core 設定が表示されます。
- 3 変更する設定をクリックします。
選択した設定が編集可能になります。
- 4 次の表の説明に従って、サービスデータベースに接続するための適切な認証情報を入力します。

表 18. ローカルデータベースの設定情報

テキストボックス	説明
ユーザー名	MongoDB サービスデータベースに対する管理者権限を持つユーザーの名前を入力します。
パスワード	指定したユーザー名に関連付けられているパスワードを入力します。

- 5 希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。

SMTP サーバ設定の管理

Core に簡易メール転送プロトコル (SMTP) サーバ設定を構成すると、タスク、イベント、およびアラート通知を電子メールで送信できるようになります。

SMTP 電子メールサーバの設定の詳細については、「[電子メールサーバーの設定](#)」のトピックに記載されています。

① **メモ:** イベント情報を電子メールで送信するには、通知グループ設定も構成する必要があります。電子メールアラートを受信するためのイベントの指定方法については、「[通知グループの設定](#)」を参照してください。

クラウド設定の管理

Rapid Recovery では、クラウドストレージプロバイダを使用するストレージアカウントを Rapid Recovery Core に関連付けることができます。これによって、データが古くなったときに保護対象マシンの情報をアーカイブできるようになります。

Rapid Recovery は、OpenStack オープンソーステクノロジーを使用して、Amazon™ S3、Microsoft Azure、および管理対象のクラウドプロバイダと統合されます。

Rapid Recovery Core のクラウドストレージアカウント情報を管理する方法については、「[クラウドアカウントの管理](#)」を参照してください。

レポート設定の管理

Rapid Recovery Core または保護対象マシンのレポートを生成することができます。生成可能なレポートについては、「[レポートの生成と表示](#)」を参照してください。

Core レポートのレポート設定を管理するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (設定) をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**レポート** をクリックします。
 - ・ 設定 ページの右側で、レポート の見出しが表示されるまでスクロールダウンします。
レポート の Core 設定が表示されます。次の表では、レポートの設定について説明しています。

オプション 説明

デフォルトの復元	このオプションは、すべてのレポートの設定をデフォルト設定に復元します。デフォルト値は、各設定の下にリストされます。

フォント	このオプションは、レポートで使用されるデフォルトのフォントを制御します。デフォルト値は Trebuchet MS 書体です。このフォントを、使用可能な任意の書体に変更することができます。

用紙サイズ	このオプションは、レポートを印刷する場合のデフォルトの用紙サイズを制御します。デフォルト値は A4 です。次のいずれかの用紙サイズを選択できます。

- ・ レター
- ・ タブロイド
- ・ 総勘定元帳
- ・ リーガル
- ・ A3
- ・ A4

オプション 説明

- ・ エグゼクティブ
- ・ B4
- ・ C3 封筒
- ・ C4 封筒

ページの向き このオプションは、エクスポートされたレポートのページの向きを制御します。デフォルトの向きは 縦 です。次のいずれかのレイアウトオプションを選択できます。

- ・ 縦
- ・ 横

- 3 レポートのいずれかの設定を変更する場合は、適切な設定フィールド内をクリックします。目的の設定フィールドが、設定可能なドロップダウンメニューとして表示されます。
- 4 ドロップダウンメニューをクリックし、使用可能ないずれかの値を選択します。たとえば、フォント フィールドで **Times New Roman** をクリックします。
- 5 希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。選択したオプションは、選択したレポートのパラメータに新しい設定として直ちに表示されます。

Core の SQL アタッチ可否設定の管理

SQL アタッチ可否検証は、Rapid Recovery の夜間ジョブの一部として実行されます。ライセンスコストを低減するため、Rapid Recovery には、アタッチの可否を検証する 2 種類のオプションが用意されています。これらは、Rapid Recovery Core マシンにインストールされている SQL Server のライセンスが付与されたインスタンスを使用する方法と、保護対象マシンに既にインストールされている SQL Server のインスタンスを使用する方法です。デフォルトで、この 2 番目のオプションが設定されています。ただし、夜間ジョブの発生時に保護対象マシンが既に稼働している場合は、Core 上の SQL Server インスタンスを使用して検証することを検討してください。

Core SQL のアタッチ可否の設定を管理するプロセスでは、大別すると、次のタスクを行います。

- ・ データベースを含む保護グループの最新のリカバリポイントをマウントします。
 - ・ SQL Server からデータベースに接続します。
 - ・ データベースを開きます。
 - ・ データベースを閉じます。
 - ・ リカバリポイントをマウント解除します。
- この夜間チェックを有効にするには、保護対象マシン上の SQL Server データベースに対するアタッチ可否チェックの実行に使用する、SQL Server インスタンスを指定します。

① **メモ:** Core で SQL Server を保護していない場合、このオプションは表示されません。

Core で SQL のアタッチ可否チェックを夜間ジョブの一部として実行するには、次の手順を実行します。

① **メモ:** 保護対象マシンにインストールされた SQL Server インスタンスを使用するオプションを選択すると、その SQL Server インスタンスは、保護されているすべての SQL マシンの SQL アタッチ可否を管理します。この設定を保護されているすべての SQL マシンに適用しない場合は、Core 上の SQL Server を使用します。Core 上でアタッチ可否検証を実行するには、Core マシン上でライセンスが付与されたバージョンの SQL Server をインストールまたは使用する必要があります。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (設定) をクリックしてから、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**アタッチの可否** をクリックします。

- ・ 設定 ページの右側で、アタッチの可否 の見出しが表示されるまでスクロールダウンします。
- 3 保護されている SQL Server マシンにインストールされた SQL Server インスタンスを使用するには、'**保護対象マシンで SQL Server を使用**' を選択します。これは、デフォルトのオプションです。
 - 4 Rapid Recovery Core にインストールされた SQL Server インスタンスを使用するには、**Core で SQL Server を使用** を選択し、次の表の説明に従って認証情報を入力します。

表 19. SQL Server の認証情報

テキストボックス	説明
SQL Server	SQL Server ドロップダウンメニューで、Core サーバーからの適切な SQL Server インスタンスを選択します。
資格情報タイプ	認証情報の適切な認証方法を、次のオプションの中から選択します。 ・ Windows ・ SQL
ユーザー名	選択した認証情報のタイプに基づいて、Core 上の SQL Server にアクセスするためのユーザー名を指定します。
パスワード	選択した認証情報のタイプに基づいて、Core 上の SQL Server にアクセスするためのパスワードを指定します。

- 5 **接続テスト** をクリックします。

① **メモ:** 認証情報を誤って入力すると、認証情報のテストに失敗したことを警告するメッセージが表示されます。認証情報を訂正して、接続をもう一度テストしてください。

- 6 希望する変更を加えたら、**適用** をクリックします。

Core ジョブについて

Core ジョブとは、リカバリポイントへのバックアップ、データのレプリケート、データの VM へのエクスポート、リポジトリのメンテナンスなどの操作のサポートを Rapid Recovery Core が実行するプロセスです。また、Core ジョブは、確立されたスケジュールによるレプリケーションやアーカイブなど、一部の操作を自動的に開始します。Core Console 上のさまざまな要素から、必要に応じて一部のジョブを起動することもできます。

- ・ Core ジョブ設定を表示または編集する際、各 Core ジョブには、最大同時実行ジョブ数と試行回数という 2 つのパラメータが含まれています。
 - ・ 最大同時実行ジョブ数パラメータは、同時に実行することができそのタイプのジョブの数を決定します。
 - ・ 試行回数パラメータは、ネットワークまたはその他の通信エラーが原因で最初にジョブが失敗した場合に、ジョブを破棄する前に行うジョブの試行回数を決定します。
- ・ Core ジョブ テーブルの 設定 行には、リストされているジョブがデフォルトで Core ジョブ設定に含まれているのか、または明示的に追加されて含まれているのかが示されます。

次の表では、使用可能なプライマリ Core ジョブと、それらの機能について説明しています。

表 20. Core ジョブ

ジョブ名	説明	最大同時実行ジョブ数	試行回数	設定
スナップショットの SQL データベースのアタッチ可否チェック	Core が SQL データベースの一貫性をチェックし、バックアップスナップショットで使用可能な MDF (データ) および LDF (ログ) ファイルがすべてサポートされているかどうか確認されます。プロセス:	1	0	デフォルト

ジョブ名	説明	最大同時実行ジョブ数	試行回数	設定
	- SQL データベースを含む保護対象グループの最新のリカバリポイントをマウントします。 - データベースをマウントします。保護された SQL Server からアタッチ可否チェックを実行している場合は、UNC パスを使用してマウントします。 - SQL Server からデータベースに接続します。 - アタッチ可否チェックを実行します。 - クリーンアップ操作を実行します。 - データベースを閉じます。 - データベースをマウント解除します。 - リカバリポイントをマウント解除します。			
Exchange データベースのチェックサムチェック	Exchange データベースを含むリカバリポイントの整合性をチェックします。プロセス： - SQL データベースを含む保護対象グループの最新のリカバリポイントをマウントします。 - SQL Server からデータベースに接続します。 - データベースを開きます。 - データベースを閉じます。 - リカバリポイントをマウント解除します。	1	0	デフォルト
Exchange データベースのマウント可否チェック	Exchange データベースがマウント可能であることをチェックします。	1	0	デフォルト
リモートソースからの保護対象マシンのデータのレプリケート	保護対象マシンのリカバリポイントをソース Core からターゲット Core に転送します。このジョブは、レプリケートされたリカバリポイントを受信したターゲット Core 上で実行されます。	3	0	デフォルト
リモートターゲットへの保護対象マシンのデータのレプリケート	保護対象マシンのリカバリポイントを、ソース Core（初めに保存した場所）からターゲット Core に転送します。このジョブは、ソース Core 上で実行され、送信レプリケーションを制御します。	1	3	デフォルト
リカバリポイントのロールアップ	保持ポリシーで定義されたスケジュールに含まれるリカバリポイントを組み合わせるか、「ロールアップ」して、バックアップデータに保持ポリシー保持ポリシーを適用します。	1	0	デフォルト
リカバリポイントのチェック	リカバリポイントの整合性をチェックします。	1	0	追加
すべてのリカバリポイントの削除	保護対象マシンから、リカバリポイントの完全なセットが削除されます。	1	0	追加
リカバリポイントのチェーンの削除	保護対象マシンから、完全なリカバリポイントチェーンが削除されます。	1	0	追加
リカバリポイントの範囲の削除	リカバリポイントの識別子または日付の範囲別に、保護対象マシンからリカバリポイントのセットが削除されます。	1	0	追加
マシンへの Agent ソフトウェアの展開	指定したマシン（複数可）に Rapid Recovery Agent ソフトウェアを展開します。	1	0	追加

ジョブ名	説明	最大同時実行ジョブ数	試行回数	設定
Exchange ライブラリのダウンロード	Microsoft Exchange ライブラリを、C:\ProgramData \AppRecovery\exchangelibraries のパスを使用して、保護対象マシンから Core マシンにダウンロードします。	1	0	追加
アーカイブへのエクスポート	選択したリカバリポイントのアーカイブを使用して指定したパスにバックアップが作成されます。プロセス： - リカバリポイントをマウントする。 - バックアップにデータを書き込みます。 - リカバリポイントをマウント解除します。	1	0	追加
仮想マシンへのエクスポート	保護対象マシンの指定したリカバリポイントのデータを、宛先のパスに仮想マシンとしてエクスポートします。プロセス： - リカバリポイントをマウント - リカバリポイントデータから宛先のパスに仮想マシンを作成します。 - リカバリポイントをマウント解除します。	1	0	追加
アーカイブのインポート	以前に作成された Core アーカイブで指定されたバックアップから、リカバリポイントをインポートします。	1	0	追加
リポジトリの維持	リポジトリのチェックを実行します。プロセス： - リポジトリのファイルシステムをチェックします。 - リカバリポイントをマウント - リポジトリの重複排除キャッシュを再計算します。 - リポジトリからリカバリポイントをロードします。	1	0	追加
リカバリポイントのスナップショットのマウント	指定したパスへのリカバリポイントのマウントを実行します。	1	0	追加
ESX® 仮想マシンをの保護	指定したすべての仮想マシンをエージェントレス保護に追加します。 複数のマシンの保護ウィザードを使用して、1つまたは複数の VM のエージェントレス保護を Core に追加した直後に、ジョブが実行されます。 ジョブによって指定した各 VM の ID 番号が設定され、Core に関する情報が設定ファイルに書き込まれて、そのファイルからメタデータが取得されます。	1	0	追加
リカバリポイントからのリストア	リカバリポイントから指定したターゲットマシンへの復元を実行します。プロセス： - リカバリポイントをマウント - リカバリポイントから指定したターゲットマシンに、すべてのデータを書き込みます。 - リカバリポイントをマウント解除します。	1	0	追加

ジョブ名	説明	最大同時実行ジョブ数	試行回数	設定
ログのアップロード	指定したサーバーにログをアップロードします。	1	0	追加

一部の Core ジョブは設定に含まれています。ジョブ設定では、Core で同時に実行できる同じタイプのジョブ数と、最初の試行が失敗した場合の再試行回数を指定できます。

これらの設定の詳細については、「[Core ジョブの設定](#)」を参照してください。

Core 設定にジョブを追加する方法については、「[Core ジョブの設定への追加](#)」を参照してください。

設定 リストのジョブの設定を編集する方法については、「[Core ジョブ設定の編集](#)」を参照してください。

Core ジョブの設定

アイコンバーで  (設定) を選択すると、一部の Core ジョブの設定にアクセスできます。Core 設定ページの **ジョブ** 領域では、リストに示されているジョブタイプごとに 2 種類の設定を指定します。

- 1 そのタイプの Core ジョブを一度に試行できる最大数。これは、1～50 までの値に設定する必要があります。
- 2 ネットワークまたはその他の通信エラーが原因で最初にジョブが失敗した場合に、試行されるジョブの回数。これは、0～10 までの値に設定する必要があります。

一部のジョブは、自動的に Core 設定に含まれます。これらのジョブには、設定 行の デフォルト の値が含まれます（「[Core ジョブについて](#)」のトピックを参照）。

設定にその他のジョブを追加して、これらの設定を構成し、ジョブの最大数やその機能の再試行回数を制御することができます。これらのジョブには、設定 行の 追加 の値が含まれます。設定 テーブルにこれらのジョブを追加する方法については、「[Core ジョブの設定への追加](#)」を参照してください。

設定 で使用不可になっている Core ジョブでは、これら 2 種類のパラメータを設定することはできません。

設定にリストされているジョブについては、既存の設定を編集できます。これにより、2 種類のパラメータをカスタマイズしたり、ジョブの設定リストからジョブタイプを削除したり、デフォルト設定を復元したりします。詳細については、「[Core ジョブ設定の編集](#)」のトピックを参照してください。

Core ジョブの設定への追加

Core ジョブ設定では、Core で一度に試行する最大ジョブ数と、最初の試行が失敗した場合の再試行回数をジョブタイプごとに定義することができます。

Core ジョブのタイプごとに、これら 2 種類のパラメータのデフォルト値が存在します（「[Core ジョブの設定](#)」のトピックを参照）。このリストには、デフォルトで Core 設定に含まれているジョブタイプも示されます。

Core ジョブを設定に追加すると、追加するジョブタイプのこれらのパラメータを変更することができます。

Core 設定にジョブを追加するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (設定) をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**ジョブ** をクリックします。
 - ・ 設定 ページの右側で、ジョブ の見出しが表示されるまでスクロールダウンします。ジョブ の Core 設定が表示されます。
- 3 Core の 設定 ページで、ジョブ の下にある **+** **追加** をクリックします。

「ジョブ設定」ダイアログボックスが表示されます。

- 4 **ジョブ設定** ダイアログボックスの **ジョブ** フィールドから、Core 設定に追加するジョブの名前を選択します。
これらのジョブの説明については、「[Core ジョブの設定](#)」のトピックを参照してください。
- 5 Core で一度に試行する最大ジョブ数を設定するには、**最大同時実行ジョブ数** テキストボックスに 1～50 までの新しい値を入力します。
- 6 ジョブを破棄する前に行う Core の試行回数を設定するには、**試行回数** テキストボックスに 0～10 までの新しい値を入力します。
- 7 「**保存**」をクリックします。
「ジョブ設定」ダイアログボックスが閉じ、新しいジョブ設定が適用されます。

Core ジョブ設定の編集

Core ジョブ設定では、Core で一度に試行する最大ジョブ数と、最初の試行が失敗した場合の再試行回数をジョブタイプごとに定義することができます。

Core ジョブのタイプごとに、これら 2 種類のパラメータのデフォルト値が存在します（「[Core ジョブについて](#)」のトピックを参照）。このリストには、デフォルトで Core 設定に含まれているジョブタイプも示されます。Core ジョブ設定を編集すると、次の目的を達成することができます。

- ・ 各 Core ジョブタイプの設定をカスタマイズする。
 - ・ Core 設定のリストから、ジョブタイプを削除する。デフォルトで設定に含まれているジョブタイプについては、この機能を使用できません。
- ① **メモ:** Core 設定からジョブを削除すると、単純にこのリストから該当するジョブタイプが削除されます。今後、同じジョブタイプの Core 設定をもう一度編集したい場合は、リストに追加することができます（「[Core ジョブの設定への追加](#)」のトピックを参照）。
- ・ 任意のジョブタイプの設定をデフォルト設定に復元することができます。
- ① **メモ:** デフォルトで Core 設定に含まれているジョブタイプについては、この機能のみを使用できますが、リストから削除して再び追加することで、その他のジョブタイプをデフォルトに設定することができます。

ジョブの設定を編集するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで （設定）をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**ジョブ** をクリックします。
 - ・ 設定 ページの右側で、ジョブ の見出しが表示されるまでスクロールダウンします。
ジョブ の Core 設定が表示されます。
- 3 ジョブ グリッドで、リストから削除するジョブを選択します。そのジョブの  ドロップダウンメニューから、**削除** を選択します。
ジョブがリストから削除されます。
- 4 ジョブ グリッドで、リストから設定をリセットするジョブを選択します。そのジョブの  ドロップダウンメニューから、**デフォルトにリセット** を選択します。
対象ジョブのジョブ設定が、デフォルト設定にリセットされます。
- 5 ジョブ グリッドで、変更するジョブを選択します。そのジョブの  ドロップダウンメニューから、**編集** を選択します。
- 6 「ジョブ設定: [ジョブ名]」ダイアログボックスが開きます。
- 7 Core で一度に試行する最大ジョブ数を変更するには、「最大同時ジョブ」テキストボックスに 1～50 で新しい値を入力します。
- 8 ジョブを破棄する前に行う Core の追加試行回数の設定を変更するには、試行回数 テキストボックスに 0～10 までの新しい値を入力します。
- 9 「**保存**」をクリックします。

「ジョブ設定」ダイアログボックスが閉じ、新しいジョブ設定が適用されます。

ライセンスの管理

多くの Rapid Recovery Core ユーザーは、機能に制限がある試用版ライセンスから開始します。試用版ライセンスは 14 日間有効ですが、グループ管理者は 1 回に限りライセンスの試用期間を 28 日に延長できます。試用期間が切れると、有効な非試用版ライセンスを取得して登録するまで、Rapid Recovery Core はスナップショットの作成を停止します。

① **メモ:** ライセンスキーまたはファイル情報の入力（試用版ライセンスを有効な長期ライセンスにアップデートまたは変更するなど）については、「[ライセンスのアップデートまたは変更](#)」を参照してください。

ライセンスは、ライセンスファイルまたはライセンスキーを使用して検証されます。

ライセンスファイルは、ファイル拡張子が **.lic** のテキストファイルです。次に、ライセンスファイルの例を示します。

- ・ ライセンスファイルは、3 グループから成る 9 文字のアラビア数字で表されます。各グループはハイフンで区切られます。たとえば、123-456-789.lic となります。
- ・ ソフトウェアベースのライセンスは、カスタマ名またはアカウントの後にグループ名を付けた Software-<グループ名>.lic の形式で表されます。たとえば、Software-YourCompany.lic となります。
- ・ Dell アブライアンスのライセンスは、カスタマ名またはアカウントの後にグループ名を付けた <アブライアンスシリーズ>-<グループ名> の形式で表されます。たとえば、DL4X00 Series-YourCompany.lic となります。

ライセンスキーは、6 グループから成る 30 文字の英数字で表されます。各グループはハイフンで区切られます。たとえば、ライセンスキー形式のサンプルは ABC12-DEF3G-H45IJ-6K78L-9MN10-OPQ11 です。

Rapid Recovery では、ライセンスを管理したり、Core Console からライセンスサーバに直接アクセスしたりすることができます。

この操作を行うには、アイコンバーの （設定）を選択し、**ライセンスの付与** をクリックします。

ライセンスの付与 の設定には、次の情報が含まれています。

ライセンスの詳細：

- ・  **ライセンスを変更。** ライセンスファイルをアップロードするか、ライセンスキーを入力して、Core に関連付けられている既存のライセンスを変更できます。
- ・  **ライセンスの追加。** このオプションは、Dell バックアップアブライアンスでのみ使用可能です。ライセンスファイルをアップロードするか、ライセンスキーを入力します。
- ・  **ライセンスポータルグループ。** このオプションは、グループ管理用のライセンスポータルを開きます。
- ・ **ライセンスタイプ。** ライセンスタイプには、試用版、サブスクリプション、エンタープライズがあります。詳細については、Dell Data Protection | Rapid Recovery ライセンスポータルの『ユーザーガイド』で、Dell Data Protection | Rapid Recovery ライセンスポータルのソフトウェアライセンスタイプに関するトピックを参照してください。
- ・ **ライセンスステータス。** ライセンスのステータスを示します。アクティブなステータスでは、スケジュールどおりにスナップショットを続行できます。ライセンスがブロック済み / 期限切れの場合、または Core が猶予期間を過ぎた Dell Data Protection | Rapid Recovery ライセンスポータルと通信できない場合、ライセンスステータスが修正されるまでスナップショットは一時停止されます。

ライセンスの制限：

- ・ **1 日あたりの最大スナップショット数。** 特定のライセンスによって制限されているバックアップの数を示します。

ライセンスプール：

- ・ **プールサイズ。** ライセンスプールとは、Dell Data Protection | Rapid Recovery ライセンスポータルのグループとサブグループに割り当て可能な非試用版ライセンスの数です。プールのサイズによって、割り当て可能なライセンス数が決まります。詳細については、Dell Data Protection | Rapid Recovery ライセンスポータルの『ユーザーガイド』で、「Understanding License Pools」（ライセンスプールについて）のトピックを参照してください。”

- ・ **この Core によって保護。**この Core によって保護されているライセンスプールのマシンの数を示します。
- ・ **グループ内の合計保護対象。**この Core と同じライセンスグループ内で保護されているマシンの合計数を示します。

ライセンスサーバー。これらの設定は、標準 (Phone Home) ライセンスに適用されます。アプライアンスや他の Phone Home 以外のライセンスには適用されません。

- ・ **ライセンスサーバーのアドレス。**この Core に関連付けられたライセンスサーバーのアクティブ URL が表示されます。
- ・ **ライセンスサーバーからの最後の応答。**ライセンスサーバーポータルとの最後の通信の試行が成功したかどうかを示します。
- ・ **ライセンスサーバーとの最後の接続。**ライセンスサーバーと最後に正常に接続した日時を表示します。
- ・ **ライセンスサーバーへの次の接続。**ライセンスサーバーとの次の通信予定の日時を示します。
- ・ **今すぐ接続。**必要に応じて、このボタンを使用してライセンスサーバにアクセスします。お使いのライセンス設定を変更した後、このオプションを使用すると、スケジュールされた次の試行を待たずに今すぐ変更内容を登録できます。

ライセンスの詳細については、*Dell Data Protection | Rapid Recovery* ライセンスポータルの『ユーザーガイド』を参照してください。

ライセンスキーまたはファイルの追加 / 変更の詳細については、「[ライセンスのアップデートまたは変更](#)」を参照してください。

ライセンスポータルサーバへのアクセスの詳細については、以下を参照してください。[Dell Data Protection | Rapid Recovery ライセンスポータルサーバへのアクセス](#)

保護対象の1つのマシンのライセンス情報も表示できます。詳細については、「[マシンのライセンス情報の表示](#)」を参照してください。

ライセンスのアップデートまたは変更

Rapid Recovery の長期ライセンスをアップグレードするか、購入すると、ライセンスファイルまたはライセンスキーのいずれかを電子メールで受信します。

この手順を完了して、試用版ライセンスをアップグレードするか、既存のライセンスを変更し、Rapid Recovery Core Console に関連付けます。

- ① **メモ:** Dell バックアップアプライアンスのユーザーは、必要に応じて **Core** にライセンスを追加することもできます。詳細については、「[ライセンスの追加](#)」を参照してください。

ライセンスキーの取得について、またはライセンスポータルを使用したソフトウェアのダウンロード、アプライアンスの登録、ライセンスサブスクリプションとライセンスグループの管理、およびライセンスポータルレポートの生成の詳細については、*Dell Data Protection | Rapid Recovery* ライセンスポータルの『ユーザーズガイド』を参照してください。

新しい Core をインストールして、ライセンスファイルまたはライセンスキーを選択するように求められただけである場合は、「[手順 5](#)」に進んでください。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (設定) をクリックします。
- 3 **設定** ページの右側で、ライセンスの付与の見出しが表示されるまでスクロールダウンします。
ライセンスの Core 設定が表示されます。
- 4 既存のライセンスをアップデートまたは変更してお使いの Core と関連付けるには、ライセンスの詳細の Core 設定領域の一番上にある  **ライセンスを変更** をクリックします。
Change License (ライセンスの変更) ダイアログボックスが表示されます。
- 5 ライセンスキーを入力するか、ライセンスファイルをアップロードするには、次のいずれかを実行します。
 - a ライセンスキーを手動入力する場合は、ライセンスを変更 ダイアログボックスで慎重にキーを入力し、**続行** をクリックします。
ダイアログボックスが閉じて選択したライセンスファイルが認証され、そのライセンスがお使いの Core に関連付けられます。

- b ライセンスファイルをアップロードする場合は、ライセンスを変更 ダイアログボックスで **ファイルを選択** をクリックします。
ファイルアップロード ダイアログボックスで、ファイルシステムを移動して使用する新しいライセンスファイルを探します。たとえば、Software-YourCompany.lic を探します。
 - c 目的のライセンスファイルをクリックし、**開く** をクリックします。
ファイルアップロード ダイアログボックスが閉じます。ライセンスを変更 ダイアログボックスに、選択したライセンスファイルが表示されます。
 - d **ライセンスを変更** ダイアログボックスで、**続行** をクリックします。
ライセンスを変更 ダイアログボックスが閉じて選択したライセンスファイルが認証され、そのライセンスがお使いの Core に関連付けられます。
- 6 設定 ページの右側で、ライセンスサーバー の見出しが表示されるまでスクロールダウンします。
 ライセンスの付与 の Core 設定が表示されます。
- 7 ライセンスサーバー 領域で、**今すぐ接続** をクリックします。
 ライセンスサーバーにライセンスが適用されると、すべての関連する保護対象マシンが新しいライセンスで自動的にアップデートされます。

ライセンスの追加

Dell バックアップアプライアンスの所有者は、Rapid Recovery Core Console に1つまたは複数のライセンスを追加できます。

Rapid Recovery ライセンスをアップグレードするか、購入すると、ライセンスファイルまたはライセンスキーのいずれかを電子メールで受信します。

また、Core Console で既存のライセンスをアップデートまたは変更することもできます。詳細については、「[ライセンスのアップデートまたは変更](#)」を参照してください。

① **メモ:** アプライアンスの追加 ボタンが表示されるのは、Dell バックアップアプライアンスのユーザーだけです。

① **メモ:** ライセンスキーの取得については、**Dell Data Protection | Rapid Recovery** ライセンスポータルの『ユーザーガイド』を参照してください。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (設定) をクリックします。
- 3 設定 ページの右側で、ライセンスの付与 の見出しが表示されるまでスクロールダウンします。
 ライセンスの Core 設定が表示されます。
- 4 ライセンスを追加してお使いの Core と関連付けるには、ライセンスの詳細 の Core 設定領域の一番上にある **ライセンスの追加** をクリックします。**ライセンスの追加** ダイアログボックスで、次のいずれかを実行します。
 - a ライセンスキーを手動入力する場合は、ライセンスを変更 ダイアログボックスで慎重にキーを入力し、**続行** をクリックします。
ライセンスを変更 ダイアログボックスが閉じて選択したライセンスファイルが認証され、そのライセンスがお使いの Core に関連付けられます。
 - b ライセンスファイルをアップロードする場合は、ライセンスを変更 ダイアログボックスで **ファイルを選択** をクリックします。
ファイルアップロード ダイアログボックスで、ファイルシステムを移動して使用する新しいライセンスファイルを探します。たとえば、Software-YourCompany.lic を探します。
 - c 目的のライセンスファイルをクリックし、**開く** をクリックします。
ファイルアップロード ダイアログボックスが閉じます。ライセンスを変更 ダイアログボックスに、選択したライセンスファイルが表示されます。
 - d **ライセンスを変更** ダイアログボックスで、**続行** をクリックします。
ライセンスを変更 ダイアログボックスが閉じて選択したライセンスファイルが認証され、そのライセンスがお使いの Core に関連付けられます。
- 5 設定 ページの右側で、ライセンスサーバー の見出しが表示されるまでスクロールダウンします。

ライセンスの付与の Core 設定が表示されます。

- 6 ライセンスサーバー 領域で、**今すぐ接続** をクリックします。

ライセンスサーバーにライセンスが適用されると、すべての関連する保護対象マシンが新しいライセンスで自動的にアップデートされます。

Dell Data Protection | Rapid Recovery ライセンスポータルサーバへのアクセス

Rapid Recovery Core Console は頻繁にポータルサーバにアクセスし、Dell Data Protection | Rapid Recovery ライセンスポータルで行った変更を反映した最新の状態を維持します。

試用版以外のライセンスの場合、Rapid Recovery Core は1時間ごとにライセンスポータルにアクセスします。10 日間の猶予期間が経過しても Core からライセンスポータルにアクセスできない場合、その Core はスナップショットの作成を停止します。

通常、ライセンスポータルサーバとの通信は、指定された間隔で自動的に行われますが、必要に応じて通信を開始することができます。

ライセンスポータルサーバにアクセスするには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで **設定** をクリックし、**設定** ページの右側で ライセンスサーバー の見出しが表示されるまでスクロールダウンします。
- 3 ライセンスサーバー 領域で、**今すぐ接続** をクリックします。

SNMP 設定について

簡易ネットワーク管理プロトコル (SNMP) は、IP ネットワーク上のデバイスを管理するためのプロトコルです。SNMP は主に、ネットワーク上にある注意が必要な状態のデバイスを監視するために使用されます。このプロトコルは、ソフトウェアコンポーネント (Agent) を使用して管理コンピュータ (マネージャ) に情報をレポートします。SNMP エージェントはマネージャのリクエストを処理し、特定のパラメータを取得または設定します。また、SNMP エージェントは、マネージャにトラップ (特定のイベントに関する通知) を送信することもできます。

SNMP エージェントが管理するデータオブジェクトは、オブジェクト識別子 (OID) を含む管理情報ベース (MIB) ファイルに組み込まれます。各 OID は、SNMP を使用して読み取りまたは設定できる変数を識別します。

Rapid Recovery は、SNMP バージョン 1.0 をサポートします。

Rapid Recovery Core を SNMP エージェントとして設定ですることがきます。この設定後、Core はアラート、リポジトリのステータス、保護対象マシンなどの情報をレポートできます。SNMP ホストは、SNMP ブラウザと呼ばれるスタンドアロンアプリケーションを使用して、この情報を読み取ることができます。SNMP ブラウザは、ネットワーク経由で Rapid Recovery Core にアクセス可能な任意のマシンにインストールできます。

SNMP ブラウザで受信可能な Core の SNMP イベント通知を確認するには、通知グループの通知オプションが SNMP トラップによって通知されるよう適切に設定されていることを検証します。

① | メモ: デフォルトのグループを使用するか、カスタム通知グループを作成することができます。このプロセスは同じです。

通知グループを開いて **通知オプション** タブを選択し、**SNMP トラップで通知** オプションが有効になっていることを確認します。通知グループは、デフォルトでトラップ番号1を指定します。必要に応じてトラップ番号を変更し、SNMP ブラウザが要求する設定と一致させることができます。

通知オプション設定の詳細と特例については、「[通知グループの設定](#)」を参照してください。

また、MIB ファイルを Rapid Recovery Core からダウンロードすることも可能です。このファイルは、Core から直接受信するデータよりもわかりやすく、SNMP ブラウザで読み取ることができます。

本項は、次のトピックで構成されています。

- ・ [SNMP の設定](#)
- ・ [SNMP MIB ファイルのダウンロード](#)

SNMP の設定

SNMP 設定を使用して、Core と SNMP ブラウザ間の通信を制御します。これには、SNMP ポート、トラップ受信ポート、およびトラップ受信に使用するホスト名が含まれています。

Core の SNMP 設定を構成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (設定) をクリックし、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**SNMP 設定** をクリックします。
 - ・ 設定 ページの右側で、SNMP 設定 の見出しが表示されるまでスクロールダウンします。
SNMP 設定が表示されます。
- 3 次の表の説明に従って、SNMP 設定を変更します。

表 21. SNMP 接続の設定情報

テキストボックス	説明
着信ポート	SNMP 接続のポート番号を入力します。  メモ: デフォルト設定は 8161 です。
トラップ受信ポート	トラップ受信に使用するポート番号を入力します。 デフォルト設定は 162 です。
トラップ受信ホスト名	SNMP 接続のホスト名を入力します。  メモ: デフォルトのホスト名は localhost です。

- 4 希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。

SNMP MIB ファイルのダウンロード

簡易ネットワーク管理プロトコルは、ネットワーク上にある注意が必要な状態のデバイスを監視するために使用されます。Rapid Recovery Core は SNMP エージェントとして設定されると、アラート、リポジットリステータス、保護対象マシンなどの情報をレポートします。この情報は、SNMP ブラウザと呼ばれるスタンドアロンアプリケーションを使用して SNMP ホストによって読み取られます。

SNMP エージェントが管理するデータオブジェクトは、オブジェクト識別子 (OID) を含む管理情報ベース (MIB) ファイルに組み込まれます。各 OID は、SNMP を使用して読み取りまたは設定できる変数を識別します。

また、MIB ファイルを Rapid Recovery Core からダウンロードできます。このファイルは dell-aa-core.mib という名前で、Core から直接受信するデータよりもわかりやすく、SNMP ブラウザで読み取ることができます。

SNMP MIB ファイルを Rapid Recovery Core からダウンロードするには、次の手順を使用します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (詳細) をクリックし、**ダウンロード** をクリックします。

ダウンロード ページが表示されます。

- 3 その他のファイル ペインをスクロールダウンします。
- 4 MIB ファイルをダウンロードするには、**SNMP MIB ファイル** のダウンロードリンクをクリックします。
SNMP 設定が表示されます。
- 5 **dell-aa-core.mib** を開く ダイアログボックスで、次のいずれかを実行します。
 - ・ ログファイルを開くには、開く を選択してテキストベースの MIB ファイルを表示する SNMP ブラウザアプリケーションを選択し、最後に **OK** をクリックします。
選択したアプリケーションで dell-aa-core.mib ファイルを開きます。
 - ・ ファイルをローカルに保存するには、**ファイルを保存** を選択して **OK** をクリックします。
dell-aa-core.mib ファイルが ダウンロード フォルダに保存されます。これは、SNMP ブラウザやテキストディタを使用して開くことができます。

vSphere 設定の構成

VMware vSphere は、ESXi または vCenter Server 仮想マシンを管理できる一連の仮想化ソフトウェアです。vSphere を使用すると、Rapid Recovery Agent ソフトウェアを個々の VM にロードしてを保護する必要がなくなります。これはエージェントレス保護機能と呼ばれ、仮想マシンにのみ適用されます。

Core の vSphere 設定を構成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (設定) をクリックしてから、次のいずれかを実行します。
 - ・ 設定 ページの左側にある Core 設定のリストから、**vSphere** をクリックします。
 - ・ 設定 ページの右側で、vSphere の見出しが表示されるまでスクロールダウンします。
vSphere の設定が表示されます。
- 3 次の表の説明に従って、vSphere 設定を変更します。

表 22. vSphere の Core 設定情報

UI エlement	UI の種類	説明
接続の有効期間	スピンボックス	ESXi サーバとの接続がタイムアウトするまでの時間を設定します。HH:MM:SS の形式を使用します。 ① メモ: デフォルト設定は 00:10:00 つまり 10 分 です。
最大同時統合数	テキストフィールド	保護されている仮想マシンを同時に統合できる最大数を設定します。 ① メモ: デフォルト設定は 0 です。
最大再試行回数	テキストフィールド	タイムアウトするまでの仮想ディスクへの接続の試行または読み取り / 書き込み操作の最大数を設定します。 ① メモ: デフォルト設定は 10 です。
パラレルリストアを許可	ブール (チェックボックス)	このオプションをオンにすると、エージェントレス仮想マシンのパラレルリストアが有効になります。 このオプションをオフにすると、この機能は無効になります。 ① メモ: デフォルト設定は いいえ (オフ) です。

- 4 希望する変更を各設定に加えたら、チェックマークをクリックして変更を保存し、編集モードを終了します。または、**X** をクリックし、保存せずに編集モードを終了します。

Core 設定のバックアップとリストア

Core 設定情報をファイルにバックアップし、Core マシンで問題が生じた場合や、設定を別のマシンに移行する場合に、これらの設定を後から復元することができます。バックアップされる情報には、リポジトリメタデータ（リポジトリ名、データパス、メタデータパスなど）、Core で保護されるマシン、レプリケーション関係（ターゲットとソース）、仮想スタンバイ用に設定されるマシン、暗号化キーに関する情報があります。

このプロセスでは、構成設定のみリストアされます。データはリストアされません。セキュリティ情報（認証情報など）は設定ファイルには格納されません。Core 設定ファイルを保存してもセキュリティ上のリスクは発生しません。

① **メモ:** このプロセスを使用して **Core** 設定を復元する前に、まず **Core** 設定情報をバックアップする必要があります。

Core 設定をバックアップおよび復元するには、次の手順を実行します。

1 Rapid Recovery Core Console に移動します。

2 アイコンバーで、（設定）をクリックします。

Settings（設定）ページが表示されます。設定 ペインの一番上（設定カテゴリの上）に、バックアップ設定 と リストア設定 の 2 つのボタンが表示されます。

3 Core の設定をバックアップする場合は、**手順 4** に進みます。Core の設定を復元する場合は、**手順 6** に進みます。

4 XML ファイルで現在の設定をバックアップするには、設定 ページの一番上で **バックアップ設定** をクリックします。

Core 設定のバックアップ ダイアログボックスが表示されます。

5 ローカルパス テキストボックスに、Core 設定を XML ファイルとして保存する Core マシンにローカルアクセスできるディレクトリパスを入力してから、**バックアップ** をクリックします。

たとえば、C:\Users\Your_User_Name\Documents\AA5CoreSettings と入力して **バックアップ** をクリックします。

AppRecoveryCoreConfigurationBackup.xml という名前のファイルが、指定したローカル宛先に保存されます。

6 この方法を使用して以前に保存されたバックアップ XML ファイルから Core 設定をリストアするには、次の手順を実行します。

① **メモ:** Core 構成設定を復元すると、**Rapid Recovery Core** サービスが再起動します。

a 設定 ページの一番で **リストア** をクリックします。

Core 設定をリストア ダイアログボックスが表示されます。

b ローカルパス テキストボックスに、Core 構成設定を保存した場所のローカルパスを入力します。

たとえば、C:\Users\Your_User_Name\Documents\AA5CoreSettings を入力します。

c リポジトリの情報を復元しない場合は、**手順 g** に進みます。

d 必要に応じて、バックアップファイルで設定されているリポジトリ情報を復元する場合は、**リポジトリをリストア** を選択し、**リストア** をクリックします。

リポジトリをリストア ダイアログボックスが表示されます。

バックアップされた設定データからのリポジトリ情報のリストアを選択すると、Core 設定の保存時に設定されたすべてのリポジトリが検証用に表示されます。デフォルトでは、既存の各リポジトリが選択されます。

e リストアするリポジトリ情報を確認します。検証リストに複数のリポジトリが表示され、その一部の情報のみを復元する場合は、復元しない各リポジトリの選択をクリアします。

f 復元するリポジトリの選択に問題がないことを確認したら、**保存** をクリックします。

リポジトリをリストア ダイアログボックスが閉じられます。

g **リポジトリをリストア** ダイアログボックスで **リストア** をクリックします。

リポジトリをリストア ダイアログボックスが閉じられ、復元プロセスが開始されます。リポジトリサービス設定が変更されたことを示すアラートが表示されます。

h 構成設定をリストアできない場合は、エラーメッセージが表示されます。エラーの詳細を確認して、対応措置が必要かどうかを判断します。詳細については、「**タスク、アラート、およびジャーナルを使用したイベントの表示**」を参照してください。続行するには、**閉じる** をクリックしてエラーダイアログボックスをクリアします。

- i 設定を復元した後、次の内容を確認します。
 - ・ すべての暗号化キーをロック解除します。詳細については、「[暗号化キーのロック解除](#)」を参照してください。
 - ・ ネットワーク上の宛先へ VM を継続的にアップデートするように Virtual Standby が設定されている場合、正常な同期を実現するには、Virtual Standby の設定にネットワーク認証情報を指定する必要があります。詳細については、「[VM エクスポート](#)」を参照してください。
 - ・ クラウドストレージアカウントにアーカイブするようにスケジュールアーカイブが設定されている場合、Core がクラウドアカウントに接続できるように、認証情報を指定する必要があります。Core とクラウドストレージアカウントをリンクする方法の詳細については、「[クラウドアカウントの追加](#)」を参照してください。
 - ・ レプリケーションが設定され、ターゲット Core に復元する場合は、ターゲット Core の設定（特にホスト）をソース Core で確認します。独自の Core を管理している場合、詳細については「[自己管理ターゲット Core へのレプリケーション](#)」を参照してください。第三者が管理する Core にレプリケートする場合は、「[サードパーティのターゲット Core へのレプリケート](#)」を参照してください。
 - ・ SQL アタッチ可否検証が設定されており、チェックを実行する SQL Server インスタンスが Core マシンに配置されている場合、アタッチの可否 設定に SQL 認証情報を指定します。詳細については、「[Core の SQL アタッチ可否設定の管理](#)」を参照してください。

Replay Engine の設定が復元されたことを確認し、この設定で有効な通信が維持されない場合は、設定をアップデートします。詳細については、「[Replay エンジン設定の構成](#)」を参照してください。

Core レベルのツール

Core 設定を構成するだけで、Core レベルのツールを使用することもできます（次の表の説明を参照）。

表 23. 他の Core レベルのツール

UI エlement	説明
システム情報	Rapid Recovery では、システム情報、ローカルおよびマウントされたボリューム、Replay エンジンの接続など、Rapid Recovery Core についての情報を表示できます。 システム情報 ページに表示される情報の詳細については Core のシステム情報について」を参照してください。 システム情報データを表示する方法については、「Core のシステム情報の表示」を参照してください。
Core ログファイルのダウンロード	Rapid Recovery Core のさまざまなアクティビティに関する情報は、Core ログファイルに保存されます。発生する可能性のある不具合を診断するために、Rapid Recovery Core のログをダウンロードして表示することができます。Core Console ログのアクセスおよび表示の詳細については、「Core ログへのアクセス」を参照してください。 各保護対象マシンも、アクティビティのログを保存します。夜間ジョブと呼ばれる保護対象マシンからのログのダウンロードを選択すると、このログを Core にアップロードすることができます。夜間ジョブの詳細については、「夜間ジョブの理解」を参照してください。Core で夜間ジョブの設定を構成する方法については、「Core の夜間ジョブの設定」を参照してください。特定の保護対象マシンに対する夜間ジョブの設定については、「保護対象マシンの夜間ジョブのカスタマイズ」を参照してください。

Core のシステム情報について

Rapid Recovery では、Rapid Recovery Core についての情報を表示することができます。表示できるのは、一般的な情報、ローカルボリュームに関する情報、およびマウントされたボリュームに関する情報です。

一般 ペインでは、次の表に記載されている情報を確認できます。

表 24. システム情報

UI エlement	説明
ホスト名	Rapid Recovery Core のマシン名。
OS バージョン	Rapid Recovery Core にインストールされているオペレーティングシステムのバージョン。
OS アーキテクチャ	Rapid Recovery Core をホストしているマシンの基盤となる構造と設計がリストされます。チップセットが含まれ、64 ビットシステムがリストされる可能性もあります。Rapid Recovery Core は、64 ビットシステムのみをサポートします。
メモリ (物理)	Core マシンにインストールされているランダムアクセスメモリ量がリストされます。
表示名	設定可能な Core の表示名が表示されます (「 Core 一般設定の構成 」を参照)。
完全修飾ドメイン名	Core マシンの完全修飾ドメイン名が表示されます。
メタデータキャッシュの場所	メタデータキャッシュの場所のパスが表示されます。 詳細については、「 重複排除キャッシュと保存場所について 」を参照してください。
プライマリキャッシュの場所	プライマリ重複排除キャッシュの場所のパスが表示されます。 詳細については、「 重複排除キャッシュと保存場所について 」を参照してください。
セカンダリキャッシュの場所	セカンダリ重複排除キャッシュの場所のパスが表示されます。 詳細については、「 重複排除キャッシュと保存場所について 」を参照してください。

ボリューム ペインには、Core マシンのストレージボリュームに関する情報 (名前、デバイス ID、ファイルシステム、Raw 容量、フォーマット済み容量、使用容量、およびマウントポイント) が表示されます。

Replay エンジンの接続 ペインには、現在マウントされているリカバリポイントの詳細情報が表示されます。ローカルエンドポイント、リモートエンドポイント、マウントされたイメージの Agent ID、マウントされたイメージの ID、およびマウントされたイメージの表示名を確認できます。マウントが書き込み可能かどうかを確認し、認証済みユーザー、読み取りバイト数、および書き込みバイト数を表示できます。

マウント ページから、Core でローカルにマウントされているリカバリポイントをマウント解除できます。リカバリポイントのマウント解除の詳細については、「[リカバリポイントのマウント解除](#)」を参照してください。

詳細については、「[Core のシステム情報の表示](#)」を参照してください。

Core のシステム情報の表示

Core のシステム情報には、一般的な情報、ローカルボリュームの情報、Core のマウントボリュームの情報が含まれています。このページに表示される情報の詳細については、「[Core のシステム情報について](#)」を参照してください。

Core に関するシステム情報を表示するには、次の手順を実行します。

① **メモ:** 保護対象マシンのシステム情報も表示できます。詳細については、「[保護対象マシンのシステム情報の表示](#)」を参照してください。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (詳細) をクリックし、 **システム情報** をクリックします。
システム情報 ページが表示されます。

Core ログへのアクセス

Rapid Recovery Core のさまざまなアクティビティに関する情報は、Core ログファイルに保存されます。このファイル AppRecovery.log は、デフォルトで C:\ProgramData\AppRecovery\Logs のパスに保存されます。

- ① **メモ:** 設定によっては、AppRecovery ディレクトリが Rapid Recovery Core で表示されないようになっている場合があります。このディレクトリを表示するには、非表示のファイル、フォルダ、およびドライブを表示するように、コントロールパネルの「フォルダ表示」オプションの設定を変更する必要があります。これらの設定にファイルの拡張子を表示しないオプションが含まれている場合、Core ログファイルが .log 拡張子を持たない AppRecovery として表示されることがあります。

Core ログには、完了した Core ジョブ、接続障害、Core がライセンスポータルにアクセスする際の試行結果、およびその他の情報が含まれます。Core ログファイルに保存されている各ステートメントの前には、INFO、DEBUG、ERROR、WARN の 4 つのうち、いずれかの修飾子が付きます。これらの修飾子は、不具合が診断された場合のログに保存される情報の性質を分類するために役立ちます。

- ① **メモ:** 同様に、ログファイルは、Core との通信に関する試行の情報を含む各保護対象マシンにも保存されます。マシンログの詳細については、「[保護対象マシンの診断情報へのアクセス](#)」を参照してください。

ログにアクセスする機能は、不具合をトラブルシューティングしたり、Dell Rapid Recovery のサポートとやり取りしたりする場合に便利です。ログにアクセスするには、次の手順を参照してください。

- [Core ログファイルのダウンロードと表示](#)
- [保護対象マシンのログファイルのダウンロードと表示](#)

Core ログファイルのダウンロードと表示

Core でエラーまたは不具合が発生した場合は、Core のログをダウンロードして表示するか、Dell サポートの担当者と Core ログを共有できます。

- 1 Rapid Recovery Core Console のアイコンバーで、 (より多い) をクリックして、 **Core ログ** をクリックします。
- 2 **Core ログのダウンロード** ページで、 **ダウンロードを開始するには、ここをクリックしてください** をクリックします。
- 3 CoreAppRecovery.log ファイルを開く、または保存するように指示するプロンプトが表示された場合、**保存** をクリックします。
- 4 **CoreAppRecovery.log を開いています** ダイアログボックスが表示されている場合、次のいずれかを実行します。
 - ログファイルを開くには、**プログラムから開く** を選択し、テキストベースのログファイルを表示するアプリケーション (メモ帳など) を選択して、**OK** をクリックします。
CoreAppRecovery.log ファイルが、選択したアプリケーションで開きます。
 - ファイルをローカルに保存するには、**ファイルの保存** を選択して、**OK** をクリックします。
CoreAppRecovery.log ファイルが **ダウンロード** フォルダに保存されます。ファイルは、任意のテキストエディタを使用して開くことができます。

関連するリンク

[Core ログファイルのダウンロードと表示](#)

[保護対象マシンのログファイルのダウンロードと表示](#)

Core を設定するためのロードマップ

設定には、バックアップスナップショットを保存するリポジトリの作成および設定、保護対象データを保護するための暗号化キーの定義、通知とアラートの設定などのタスクが含まれます。Core の設定が完了したら、エージェントの保護およびリカバリの実行が可能になります。

Core の設定には、特定の概念と以下の初期操作の実行について理解する必要があります。

- ・ リポジトリの作成
- ・ 暗号化キーの設定
- ・ イベント通知の設定
- ・ 保持ポリシーの設定
- ・ SQL アタッチ可否の設定

リポジトリ

本項では、リポジトリの操作方法について説明します。重複排除ボリュームマネージャリポジトリ、その機能、および属性について説明します。Rapid Recovery で使用される重複排除のタイプ、およびアプリケーション全体での重複排除の使用方法について説明します。次に本項では、リポジトリの作成、詳細情報の表示と編集、リポジトリの削除など、DVM リポジトリの管理方法について説明します。特定の Core のリポジトリを、別の Core で開く方法について学習できます。最後に、本項では、リポジトリ間でリカバリポイントを手動で移行する方法について説明します。

DVM リポジトリの管理

Rapid Recovery を使用する前に、Rapid Recovery Core で1つ、または複数のリポジトリをセットアップする必要があります。リポジトリは、保護対象データ、具体的には、お使いの環境内の保護対象マシンからキャプチャされたスナップショットを保存します。

DVM リポジトリを管理するには、次の操作を実行します。

- 1 **DVM リポジトリの作成。** リポジトリを作成する前に、適切なテクノロジータイプを検討してください。
リポジトリの詳細については、「[リポジトリの理解](#)」を参照してください。

DVM リポジトリの作成の詳細については、「[DVM リポジトリの作成](#)」を参照してください。
- 2 **新しいストレージ場所の追加。** DVM リポジトリに新しいストレージの場所を追加する方法の詳細については、「[既存 DVM リポジトリへのストレージ場所の追加](#)」を参照してください。
- 3 **リポジトリ設定の変更。** リポジトリのリポジトリ設定を変更する方法の詳細については、を参照してください。 [リポジトリの詳細の表示または変更](#)
- 4 **リポジトリのチェック。** リポジトリのチェックの詳細については、「[リポジトリのチェック](#)」を参照してください。
- 5 **リポジトリ最適化ジョブの実行** リポジトリ最適化ジョブの詳細については、「[リポジトリ最適化ジョブについて](#)」を参照してください。既存の DVM リポジトリを最適化する手順については、「[DVM リポジトリの最適化](#)」を参照してください。
- 6 **リポジトリの削除。** リポジトリの削除の詳細については、「[リポジトリの削除](#)」を参照してください。

DVM リポジトリの作成

このプロセスは、重複除外ボリュームマネージャ（DVM）リポジトリのテクノロジーを使用して Core 上にリポジトリを作成する方法を説明します。

- ・ DVM のリポジトリを作成するマシンに対して管理者のアクセス権限を保有している必要があります。
- ・ このリポジトリタイプは、ストレージの場所として定義するボリューム上で最小 150 GB のストレージ容量を必要とします。
- ・ DVM リポジトリのストレージ場所は、Core サーバーにアタッチされているローカルドライブ上である必要があります。
- ・ Core サーバーは、システム要件を満たしている DL シリーズアプライアンス（DL1000 を含む）、またはソフトウェアベースの Windows サーバーを利用できます。

① **メモ:** リポジトリの作成には、**Appliance**（アプライアンス）タブの使用をお奨めします。詳細については、[ストレージのプロビジョニング](#) 項を参照してください。

DVM リポジトリを作成するには、以下の手順を完了します。

- 1 Rapid Recovery コアコンソールへ移動します。
- 2 アイコンバーで、 (More (詳細)) をクリックして、**Repositories** (リポジトリ) を選択します。
Repositories (リポジトリ) ページが表示されます。

Repositories (リポジトリ) ページで、DVM Repositories (DVM リポジトリ) ペインが表示されます。

- 3 ページの上部で、**Add New DVM Repository** (新しい DVM リポジトリを追加) をクリックします。
Add New Repository (新規リポジトリを追加) ダイアログボックスが表示されます。
- 4 次の表の説明に従って、情報を入力します。

表 25. 新しいリポジトリ設定の追加

テキストボックス	説明
Repository Name (リポジトリ名)	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは Repository (リポジトリ) という単語と、この Core のリポジトリの番号に対応する番号で構成されます。たとえば、最初のリポジトリの場合、デフォルト名は Repository 1 です。必要に応じて名前を変更します。 リポジトリ名にはスペースを含む 1 文字から 40 文字の英数字を含める必要があります。使用禁止文字または 禁止語 を使用しないでください。
Concurrent Operations (同時操作)	レポジトリで対応する同時要求の数を定義します。デフォルトの値は 64 です。
Comments (コメント)	オプションで、このリポジトリの説明を入力します。最大 254 文字を入力できます。たとえば、 DVM Repository 2 と入力します。

- 5 **Add Storage Location** (ストレージの場所を追加) をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。

△ **注意:** リポジトリ用のストレージの場所のルート内の専用のフォルダを定義します。ルートの場所は指定しません。たとえば、E:\ではなく E:\Repository\ を使用します。この手順で作成するリポジトリが後で削除された場合、リポジトリのストレージの場所にあるすべてのファイルが削除されます。ルートでお使いのストレージの場所を定義する場合は、ボリューム内のその他のすべてのファイル (たとえば、E:\) が削除され、致命的なデータ損失が発生する可能性があります。

Add Storage Location (ストレージの場所の追加) ダイアログボックスが表示されます。

- 6 **Add Storage Location** (ストレージの場所を追加) をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。
- 7 **Storage Location** (ストレージの場所) 領域には、ストレージの場所にファイルを追加する方法を指定します。ローカルに接続されているストレージ (DAS、SAN、NAS など) を追加することを選択できます。共通インターネットファイルシステム (CIFS) の共有場所にストレージボリュームを指定することもできます。
 - **Add the file on local disk** (ローカルディスクにファイルを追加) を選択して、ローカルマシンを指定し、以下の表に記載されているとおりに情報を入力します。

表 26. ローカルディスクの設定

テキストボックス	説明
Data Path (データパス)	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Data と入力します。

テキストボックス 説明

パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。

Metadata Path (メタデータパス) 保護されたメタデータを保存するための場所を入力します。
たとえば、X:\Repository\Metadata と入力します。

パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。

または、**Add file on CIFS share (CIFS 共有にファイルを追加)** を選択して、ネットワーク共有の場所を指定し、以下の表に記載されているとおりに情報を入力します。

表 27. CIFS 共有の資格情報

テキストボックス 説明

UNC Path (UNC パス) ネットワーク共有の場所のパスを入力します。
この場所がルートにある場合は、専用のフォルダ名（たとえば、Repository）を定義します。

パスの開始部分には \\ を使用する必要があります。パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。英字 a~z は大文字と小文字が区別されません。スペースは使用しないでください。その他の記号および句読点は使用できません。

ユーザー名 ネットワーク共有の場所にアクセスするためのユーザー名を指定します。

パスワード ネットワーク共有の場所にアクセスするためのパスワードを指定します。

8 **Storage Configuration (ストレージの設定)** 領域で、**More Details (詳細)** をクリックし、次の表の説明に従ってストレージの場所の詳細を入力します。

表 28. ストレージ構成の詳細

テキストボックス 説明

サイズ ストレージの場所のサイズまたは容量を設定します。最小サイズは 1 GB です。デフォルトは 250 GB です。次から選択できます。

- GB
- TB

① | メモ: 指定するサイズは、ボリュームのサイズを超えることはできません。

ストレージの場所が Windows XP または Windows 7 を使用した New Technology File System (NTFS) ボリュームの場合、ファイルサイズの上限は 16 TB です。

ストレージの場所が Windows 8 と 8.1、Windows 10、または Windows Server 2012 と 2012 R2 を使用した NTFS ボリュームの場合、ファイルサイズの制限は 256 TB です。

① | メモ: **Rapid Recovery** からオペレーティングシステムを検証する場合は、**Windows Management Instrumentation (WMI)** が対象のストレージの場所にインストールされている必要があります。

Write Caching Policy (ライトキャッシングポリシー) ライトキャッシングポリシーは、リポジトリでの Windows Cache Manager の使用を制御し、さまざまな構成で最適なパフォーマンスを得られるようにリポジトリを調整します。
次のいずれかの値に設定します。

- 点灯
- オフ
- 同期

デフォルトのまま On (オン) に設定すると、Windows がキャッシングを制御します。これは、Windows 10、および Windows Server 2012 以降のバージョンに対して適切です。

① **メモ:** ライトキャッシングポリシーを On (オン) に設定すると、パフォーマンスを高速化できます。Windows Server 2008 SP2 または Windows Server 2008 R2 SP2 を使用している場合、推奨の設定は Off (オフ) です。

Off (オフ) に設定すると、Rapid Recovery がキャッシングを制御します。

Sync (同期) に設定すると、Windows が同期入出力に加えてキャッシングも制御します。

セクタあたりのバイト 各セクタに包含するバイト数を指定します。デフォルト値は 512 です。

Average Bytes per Record (レコードあたりの平均バイト数) レコードあたりの平均バイト数を指定します。デフォルト値は 8192 です。

9 **Save (保存)** をクリックします。

Add Storage Location (ストレージの場所の追加) ダイアログボックスが閉じて、設定が保存されます。**Add New Repository (新規リポジトリを追加)** ダイアログボックスが、新しいストレージの場所を示します。

10 オプションで、手順 6 から 手順 9 を繰り返して、リポジトリ用の追加のストレージの場所を追加します。

11 この時点でリポジトリ用に作成したいすべてのストレージロケーションを定義したら、**Add New Repository (新しいリポジトリを追加)** ダイアログボックスで、**Create (作成)** をクリックしてください。

Add New Repository (新規リポジトリを追加) ダイアログボックスが閉じ、変更が適用されます。**Repositories (リポジトリ)** ページが表示され、DVM Repositories (DVM リポジトリ) サマリテーブルで新しく追加されたリポジトリが表示されます。

リポジトリの拡張

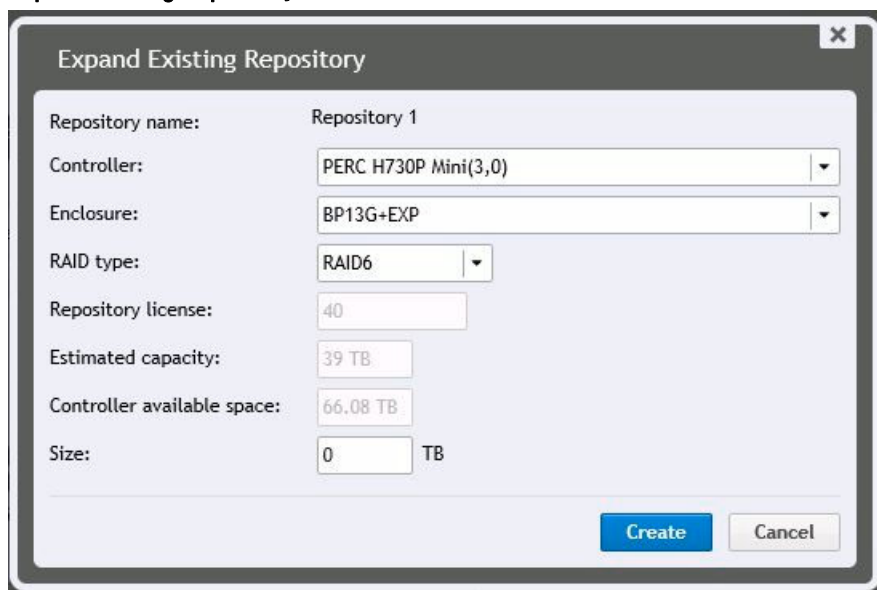
Expand Repository (リポジトリの拡張) 機能が DL 1000 以外のすべての DL モデル (1300、4300、4000 など) で利用できます。適用されたライセンスのタイプは、リポジトリのサイズを制限します。外部エンクロージャ上の未使用の内部ストレージとストレージを使用してリポジトリを拡張するには、ライセンスを更新します。ライセンスキーを変更する場合は、[ライセンスのアップデートまたは変更](#) セクションを参照してください。既存のリポジトリを拡張するには、次の操作を実行します。

1 **Appliance > Provisioning** (アプライアンスプロビジョニング) をクリックします。



2 **Repositories** セクションで、**Expand Existing Repository (既存のリポジトリを拡張)** をクリックします。

Expand Existing Repository（既存のリポジトリを拡張）ダイアログボックスが表示されます。

A screenshot of the 'Expand Existing Repository' dialog box. The dialog has a title bar with a close button. Inside, there are several fields: 'Repository name' with the value 'Repository 1'; 'Controller' with a dropdown menu showing 'PERC H730P Mini(3,0)'; 'Enclosure' with a dropdown menu showing 'BP13G+EXP'; 'RAID type' with a dropdown menu showing 'RAID6'; 'Repository license' with a text input field containing '40'; 'Estimated capacity' with a text input field containing '39 TB'; 'Controller available space' with a text input field containing '66.08 TB'; and 'Size' with a text input field containing '0' and a 'TB' unit label. At the bottom right, there are two buttons: 'Create' (blue) and 'Cancel' (gray).

- 3 **Expand Existing Repository**（既存のリポジトリを拡張）ボックスに、次の情報を指定します。

表 29. 既存リポジトリの拡張

テキストボックス	説明
Repository Name（リポジトリ名）	拡張するリポジトリの名前が表示されます。
コントローラ	内部ストレージまたは DAS エンクロージャのどちらかにリポジトリを作成するのかに応じて、適切なストレージコントローラを選択します。
Enclosure	適切なストレージエンクロージャを選択します。
RAID type（RAID の種類）	適切な RAID 構成を選択します。RAID 構成 1、5、または 6 の次の次のオプションがあります。
Repository license（リポジトリのライセンス）	リポジトリのライセンスが表示されます。
Estimated capacity（推定容量）	リポジトリの作成に使用可能な推定容量を表示します。
Controller available space（コントローラの使用可能なスペース）	コントローラ上の使用可能な容量が表示されます。
サイズ	作成するリポジトリのサイズを入力します。

- 4 **作成** をクリックします

新しいストレージの場所が既存リポジトリに追加されます。

リポジトリが指定したサイズに拡張されます。

リポジトリの詳細の表示または変更

- 1 Rapid Recovery（迅速な回復）コアコンソールへ移動します。

- 2 アイコンバーで、（More（詳細））をクリックして、**Repositories**（リポジトリ）を選択します。

Repositories（リポジトリ）ページが表示されます。

DVM Repositories (DVM リポジトリ) ペインが表示されます。

- 3 **Repositories** (リポジトリ) ページメニューから、次の一般的なアクションを実行できます。

オプション	説明
Add New DVM Repository (新しい DVM リポジトリを追加します。)	リポジトリの追加
Open Existing DVM Repository (既存の DVM リポジトリを開く)	別の Core から既存の DVM リポジトリを開きます。これにより、リポジトリの所有権がこの Core に変更されます。 詳細については、「 既存の DVM リポジトリを開く 」を参照してください。
更新	リポジトリのリストを表示または更新します。

- 4 **DVM Repositories** (DVM リポジトリ) ペインで、 ドロップダウンメニューから、次の追加のアクションを実行できます。

オプション	説明
Add Storage Location (ストレージの場所を追加することにより、既存のリポジトリを拡張します。)	① メモ: DVM リポジトリボリュームを拡張する場合は、最初に保護を一時停止します。次にボリュームを拡張し、最後に保護を再開します。このアクションは、特定の転送フェーズでボリュームを同時に拡張する場合にのみ発生することが稀な間違いを防止できます。
チェック	リポジトリのチェックを実行
設定	リポジトリ設定を表示または変更します。これらの設定は次のとおりです。 - リポジトリ名の表示 - 最大同時操作の表示または変更 - リポジトリの説明の表示または変更 - 重複排除の有効化または無効化 - リポジトリに保存されたデータに対して圧縮を有効化または無効化
Perform Optimization Job (ジョブの最適化を実行)	リポジトリ最適化のジョブを実行します。
削除	リポジトリを削除します。

- ① **メモ:** DVM リポジトリボリュームを拡張する場合は、最初に保護を一時停止します。次にボリュームを拡張し、最後に保護を再開します。このアクションは、特定の転送フェーズで拡張する場合に発生することが稀な間違いを防止できます。

Repositories (リポジトリ) ページでは、次の一般的なアクションを実行できます。

- リポジトリのリストを表示または更新します。
- 新しいリポジトリを追加します。
- このリポジトリの所有権を変更する別の Core コアから既存のリポジトリを開きます。

既存 DVM リポジトリへのストレージ場所の追加

- ① **メモ:** アプライアンス タブでリポジトリを展開することが推奨されます。詳細については、次を参照してください。 [リポジトリの拡張](#)

ストレージ場所を DVM リポジトリに追加すると、リポジトリまたはボリュームを保存する場所を定義できます。

リポジトリまたはボリュームのストレージの場所を指定するには、次の手順を実行します。

- Rapid Recovery Core Console に移動します。
- アイコンバーで、 (より多い) をクリックして、**レポジトリ** を選択します。
Repositories (リポジトリ) ページが表示されます。

DVM リポジトリ ペインが表示されます。

- 3 リポジトリのサマリ表で、そのストレージ場所を追加する DVM リポジトリを表す行から、**設定** をクリックし、**ストレージ場所の追加** を選択します。

ストレージ場所の追加 ダイアログボックスが表示されます。

- 4 ストレージ場所でファイルを追加する方法を指定します。ローカルディスクまたは CIFS 共有にファイルを追加することもできます。
- ・ **ローカルディスクにファイルを追加** を選択して、ローカルマシンを指定してから、次の表の説明に従って、情報を入力します。

表 30. ローカルディスクの設定

テキストボックス	説明
データパス	保護対象データを保存する場所を入力します。 たとえば、「X:\Repository\Data」を入力します。 パスと同じ制限が適用されます。英数字、ハイフン、ピリオドのみを使用し、スペースまたは特殊文字は使用できません。
メタデータパス	保護対象メタデータを保存する場所を入力します。 たとえば、「X:\Repository\Metadata」を入力します。 パスを指定する場合には、英数字、ハイフン、ピリオド（ホスト名とドメインを区切るため）のみを使用できます。a から z までの文字では、大文字と小文字は区別されません。スペースは使用できません。他の記号または句読点文字は無効です。

- ・ または、**CIFS 共有にファイルを追加** を選択してネットワーク共有の場所を指定してから、次の表の説明に従って、情報を入力します。

表 31. CIFS 共有資格情報

テキストボックス	説明
UNC パス	ネットワーク共有の場所のパスを入力します。 この場所がルートにある場合は、専用フォルダ名（Repository など）を定義します。 パスは「\\」で開始する必要があります。パスを指定する場合には、英数字、ハイフン、ピリオド（ホスト名とドメインを区切るため）のみを使用できます。a から z までの文字では、大文字と小文字は区別されません。スペースは使用できません。他の記号または句読点文字は無効です。
ユーザー名	ネットワーク共有の場所にアクセスするためのユーザー名を指定します。
パスワード	ネットワーク共有の場所にアクセスするためのパスワードを指定します。

- 5 ストレージ設定 ペインで、**詳細表示** をクリックして、次の表の説明に従って、ストレージの場所の詳細を入力します。

表 32. ストレージの場所の詳細

テキストボックス	説明
サイズ	ストレージの場所のサイズまたは容量を設定します。デフォルトサイズは 250 GB です。次から選択できます。 ・ GB ・ TB  メモ: 最小サイズは 1 GB です。指定するサイズは、ボリュームのサイズを超えることはできません。 ストレージの場所が、Windows XP または Windows 7 を使用する New Technology File System (NTFS) ボリュームの場合は、ファイルサイズが 16 TB に制限されます。 ストレージの場所が、Windows 8、8.1、Windows Server 2012、2012 R2 を使用する NTFS ボリュームの場合は、ファイルサイズが 256 TB に制限されます。

① **メモ:** Rapid Recovery からオペレーティングシステムを検証する場合は、**Windows Management Instrumentation (WMI)** が対象のストレージ場所にインストールされている必要があります。

ライトキャッシングポリシー ライトキャッシングポリシーは、リポジトリで Windows Cache Manager がどのように使用されるかを制御し、さまざまな設定でパフォーマンスが最適になるようにリポジトリを調整するのに役立ちます。次のいずれかの値を指定します。

- ・ オン
- ・ オフ
- ・ 同期化

デフォルト値である「オン」に設定すると、Windows がキャッシングを制御します。これは、Windows 10、および Windows Server 2012 以降の各バージョンに適しています。

① **メモ:** ライトキャッシングポリシーを「オン」に設定すると、パフォーマンスを向上できます。**Windows Server 2008 SP2** または **Windows Server 2008 R2 SP2** を使用している場合、推奨される設定は **オフ** です。

オフに設定すると、Rapid Recovery がキャッシングを制御します。

「同期化」に設定すると、Windows が同期入出力とキャッシングを制御します。

セクタあたりのバイト数 各セクタに含めるバイト数を指定します。デフォルト値は 512 です。

レコードあたり平均バイト数 1レコードの平均バイト数を指定します。デフォルト値は 8192 です。

- 6 必要に応じて、選択したリポジトリでリポジトリ最適化ジョブを実行する場合は、**【リポジトリ名】に対してリポジトリ最適化ジョブを実行します**を選択します。

Dell では、既存のリポジトリにストレージ場所を追加するときは、リポジトリ最適化ジョブを実行することをお勧めします。このジョブでは、リポジトリに保存されているデータに重複排除を適用して空き容量を最適化します。

リポジトリのサイズ、リポジトリ内のデータの量、使用可能なネットワーク帯域幅、システムの既存の入出力負荷などの要因に基づいて、リポジトリ最適化ジョブの実行には、長時間かかる場合や、環境内で広い帯域幅を要する場合があります。

リポジトリ最適化ジョブの詳細については、「[リポジトリ最適化ジョブについて](#)」を参照してください。

- 7 **保存** をクリックします。

ダイアログボックスが閉じ、ストレージ場所が保存されます。リポジトリのサマリ表でリポジトリの詳細を展開すると、作成したストレージ場所が表示されます。

DVM リポジトリの整合性チェックについて

Rapid Recovery（迅速な回復）コアのユーザーはソースコアとターゲット Core 間の異なる保持ポリシーを設定することができます。レプリケーションを異なる保持ポリシーで正しく動作させるには、ターゲット Core にソース Core と同じバージョン（かそれ以降）のソフトウェアが必要です。

① **メモ:** Core のリリース番号で同じ **3** 桁を共有する必要があります（たとえば、両方の頭に **6.0.1.xxxx** または **5.4.3.xxxx** を使用します。）。ビルド番号（xxxx によって表される）は、ターゲット Core が新しい場合のみ別のものにすることができます。

管理者はソース Core とは異なるレートでターゲット Core のロールアップを設定できるようになりました。同様に、レプリケートされた任意のマシンにカスタム保持ポリシーを定義できます。たとえば、高速レートでターゲット Core にリカバリポイントをロールアップできます。その際、ソース Core でより低い粒度で、容量を節約することができます。または選択した任意のレプリケーションされたマシンのリカバリポイントをターゲット Core で低い速度でロールアップできます。この際より高い粒度を保持することができます。これはコンプライアンスのために役立つ可能性があります。Core でのデフォルトとは異なる保持ポリシーの使用についての詳細は、[保護対象マシンの保持ポリシー設定のカスタマイズ](#)を参照してください。

Core が AppAssure 5.3.x からの任意のポイントでアップグレードされていて、レプリケーションを使用した場合には、ソース Core およびターゲット Core の間で異なる保持ポリシーを設定する前、あるいはレプリケーションされたマシンでカスタム保持ポリシーを設定する前に、このジョブを実行する必要があります。

1つまたは複数の適切なリポジトリ（5.4.x より前に作成され、まだ実行されていないもの）を作成しない限り、このジョブを表示したり、実行したりできません。

このジョブを実行すると、指定したリポジトリに保存されたすべてのデータの整合性が検証され、各スナップショットまたはベースイメージからデータを確実に回復できます。整合性チェックがリポジトリ内のデータに問題を検出した場合は、ジョブがすぐに停止します。Core のジョブのイベントの詳細により、Dell Support に連絡するように表示され、サポート担当者と作業を行うように時間をスケジュールし、追加手順を実行し、データの不整合を特定し、修正することができます。

△ 注意: このジョブを実行するには、延長時間がかかることが予想されます。リポジトリのデータの量とタイプ、基礎となるストレージシステムにより時間は異なります。ジョブの実行中はそのリポジトリ内で、転送、夜間ジョブなどを含む他のトランザクション（スナップショットおよびベースイメージバックアップ、およびレプリケーション）を実行することはできません。

このジョブの実行中は、他のリポジトリ内のその他の操作を実行できます。

① メモ: このジョブにはリポジトリ内のすべてのコンテンツの整合性をチェックします。Integrity Check（整合性チェック）ジョブは、リポジトリを確実にマウント可能かつ使用可能にするために使用できます。これに関する情報については、[リポジトリのチェック](#)を参照してください。

リポジトリのチェック

Rapid Recovery では、エラーが発生したときに DVM リポジトリボリュームの診断チェックを実行できます。不適切なシャットダウン、ハードウェア障害、または Rapid Recovery の機能が影響を受ける可能性のあるその他の環境レベルの下位 IP スタック要因などにより、Core でエラーが引き起こされる場合があります。

① メモ: この手順は、診断目的でのみ使用する必要があります。たとえば、ハードウェア障害、Core の不適切なシャットダウン、またはリポジトリのインポート時の障害が発生した場合に、このチェックを実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで （詳細）をクリックし、**リポジトリ** を選択します。
Repositories（リポジトリ）ページが表示されます。

DVM リポジトリ ペインが表示されます。
- 3 DVM リポジトリをチェックするには、**DVM リポジトリ** ペインで、DVM リポジトリを表すサマリ表のいずれかの行の  をクリックし、**チェック** を選択します。
Check Repository（リポジトリのチェック）ダイアログボックスが表示されます。
- 4 **リポジトリの確認** ダイアログボックスで、このリポジトリに関連付けられているアクティブなタスクのすべてがキャンセルされることを理解した上で続行する確認操作が行われます。
アクティブなジョブがキャンセルされ、リポジトリの確認ジョブが開始されます。
- 5 必要に応じて、ボタンバーの **実行中のタスク** ドロップダウンメニューをクリックし、リポジトリ維持ジョブを選択することで、ジョブのステータスを追跡することもできます。

リポジトリ最適化ジョブについて

DVM リポジトリを使用している場合、各スナップショットでキャプチャされるデータでは、重複が排除されます。スナップショットがリポジトリに保存されると、この重複排除が漸次実行されます。情報の各ストリングの1回の発生が、リポジトリに保存されます。情報のストリングが複製される場合、重複排除キャッシュ内の元のストリングへの参照が使用されるため、リポジトリ内のストレージ容量が節約されます。

DVM 重複排除キャッシュが容量不足になると、キャッシュ内ですでに参照されているスナップショットデータのみが重複排除されます。重複排除が実行されると、キャッシュは引き続き新しい固有の値でアップデートされ、キャッシュ内の最も古い値が上書きされます。この結果、最適な重複排除よりも少なくなります。

重複排除の詳細については、「[重複排除キャッシュと保存場所について](#)」を参照してください。

容量不足になる前に DVM 重複排除キャッシュのサイズを増やしておく、引き続きそのリポジトリでデータの最適な重複排除を確実に実行させることができます。詳細については、「[重複排除キャッシュ設定の構成](#)」を参照してください。

また容量不足になった後でも、重複排除キャッシュのサイズを増やすことができます。キャッシュのサイズを増やした後、リポジトリ内の容量を再利用する場合、リポジトリを最適化できます。このアクションでは、スナップショット内のデータと重複排除キャッシュ内の情報が強制的に比較されます。リポジトリ内で繰り返しのストリングが見つかり、そのデータはデータへの参照に置き換えられるため、リポジトリ内のストレージ容量が節約されます。この重複排除プロセスは、スナップショットデータの転送にともなって漸次実行されるのではなく、リクエストに基づいて実行されるため、オフライン重複排除と呼ばれることもあります。

プロセッサにとっては、最適化は大きな負荷になるプロセスです。このジョブの実行時間は、いくつかの要因によって変わります。これらの要因とは、リポジトリのサイズ、リポジトリにあるデータの量、使用可能なネットワーク帯域幅、システムの入出力にかかっている既存の負荷などです。リポジトリにあるデータが多くなると、このジョブの実行時間も長くなります。

リポジトリ最適化ジョブが開始されると、次のアクションは代替されるか、キャンセルされます。

- ・ リカバリポイントの削除ジョブ
- ・ リポジトリの維持ジョブ
- ・ リポジトリ整合性のチェックジョブ

最適化ジョブが開始されると、次のアクションは代替されるか、キャンセルされます。

- ・ すべてのリカバリポイントの削除ジョブ
- ・ リカバリポイントチェーンの削除ジョブ
- ・ リポジトリの維持ジョブ
- ・ リカバリポイントの削除ジョブベース
- ・ リポジトリ整合性のチェックジョブ

既存の DVM リポジトリを最適化する手順については、「[DVM リポジトリの最適化](#)」を参照してください。

限られた時間のために、必要に応じてリポジトリ最適化ジョブを中断できます。詳細については、「[リポジトリ最適化ジョブの中断または再開](#)」を参照してください。

DVM リポジトリの最適化

この手順を実行するには、お使いの Core に DVM リポジトリがある必要があります。

既存の DVM リポジトリに保存されたデータの重複排除をオフラインで実行することができます。これは、リポジトリ最適化ジョブを起動して実行します。

① **メモ:** Dell では、重複排除キャッシュのサイズを増やした後でのみ、リポジトリ最適化ジョブを実行することを推奨します。このアクションにより、リポジトリの容量を再利用し、DVM 重複排除キャッシュをより効果的に使用することができます。

DVM リポジトリを最適化するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (より多い) をクリックして、**リポジトリ** を選択します。
Repositories (リポジトリ) ページが表示されます。
- 3 DVM リポジトリ ペインで、最適化するリポジトリを表す行から  をクリックし、**最適化ジョブを実行** を選択します。
最適化の確認を求める警告プロンプトが表示されます。

- 4 クリックして最適化を確認します。

最適化ジョブは、他のほとんどのジョブよりも優先されます。必要な場合は、進行中の最適化ジョブを中断することができます。このジョブの中断または再開の詳細については、「[リポジトリ最適化ジョブの中断または再開](#)」を参照してください。

リポジトリ最適化ジョブの中断または再開

リポジトリ最適化ジョブを開始すると、選択した DVM リポジトリが重複排除されます。この重複排除の最適化は、リポジトリ内の容量を節約するための、プロセッサ負荷の高いジョブです。詳細については、「[リポジトリ最適化ジョブについて](#)」を参照してください。

このジョブが開始された後、次の手順を使用してジョブを中断させることができます。これにより重複排除が一時停止します。すでに最適化を中断している場合は、次の手順を使用してプロセスを再開できます。

① **メモ:** この手順は、DVM リポジトリにのみ、リポジトリ最適化ジョブが開始されている場合にのみ適用されます。

リポジトリ最適化ジョブを中断または再開するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (詳細) をクリックし、**リポジトリ** を選択します。
Repositories (リポジトリ) ページが表示されます。

DVM リポジトリ ペインが表示されます。
- 3 最適化ジョブを中断するには、次の手順を実行します。
 - a リポジトリのサマリ表で、適切なリポジトリを表す行の  をクリックし、**最適化ジョブを中断** を選択します。
中断の確認を求める警告プロンプトが表示されます。
 - b クリックして最適化を確認します。
- 4 中断した最適化ジョブを再開するには、次の手順を実行します。
 - a リポジトリのサマリ表で、適切なリポジトリを表す行の  をクリックし、**最適化ジョブを続行** を選択します。
中断の確認を求める警告プロンプトが表示されます。
 - b ダイアログボックスで **中断した時点からジョブを続行する** オプションを選択し、**はい** をクリックします。
ダイアログボックスが閉じ、リポジトリ最適化ジョブが、最後に中断された時点から再開されます。

既存の DVM リポジトリを開く

Rapid Recovery のプライマリリポジトリのテクノロジーとして、DVM リポジトリには、特定の Rapid Recovery Core で保護されているマシンからのスナップショットデータが (リカバリポイントの形式で) 含まれています。既存のリポジトリを、2 つ目の Core (Core B) 上にある 1 つの Core (たとえば Core A) から開くことができます。

① **メモ:** 別の **Core** からリポジトリを開くと、コアリポジトリの所有権が変更されます。そのため、既存のリポジトリを開くとき、情報は 2 つ目の **Core** にのみアクセスできます。

DVM リポジトリの場合、元の Core (Core A) は現在使用中でない必要があります。たとえば、マシンがオフになっているか、ネットワークにアクセス不可であるか、Core サービスが停止している必要があります。

リポジトリは共有ネットワーク上の場所にするか、または 2 つ目の Core にアクセス可能なストレージデバイスにすることができます。

既存リポジトリを開くには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (より多い) をクリックして、**レポジトリ** を選択します。
Repositories (リポジトリ) ページが表示されます。

DVM リポジトリ ペインも表示されます。

- 既存の DVM リポジトリを開くには、ページの上にある、**既存の DVM リポジトリを開く** をクリックします。
既存の DVM リポジトリを開く ダイアログボックスが表示されます。
- 既存の DVM リポジトリを開く** ダイアログボックスで、開くレポジトリに関する次の情報を入力し、**開く** をクリックします。

表 33. 既存の DVM リポジトリを開く オプション

テキストボックス	説明
パス	リポジトリのパス（たとえば、ローカルパスの場合は D:\work\machine、IP アドレスによる場合は \10.10.99.155\repositories、ネットワークパスの場合は \\servername\sharename）。
ユーザー名	リポジトリにネットワークパスが含まれる場合は、ネットワーク共有にログインするためのユーザー名を入力します。
パスワード	リポジトリにネットワークパスが含まれる場合は、ネットワーク共有にログインするためのパスワードを入力します。

ダイアログボックスが閉じ、選択したリポジトリが現在の Core に追加されます。

リポジトリの削除

リポジトリを削除するには、次の手順を実行します。

- Rapid Recovery Core Console に移動します。
- アイコンバーで、（詳細）をクリックし、**レポジトリ** を選択します。
Repositories（リポジトリ）ページが表示されます。

リポジトリ ページに、DVM リポジトリ ペインが表示されます。
- リポジトリサマリ表内の、削除するリポジトリを表す行から、 をクリックしてドロップダウンメニューを展開し、**削除** を選択します。
削除を確認する警告メッセージが表示されます。
- 「はい」をクリックして、リポジトリの削除を確認します。

 **注意:** リポジトリが削除されると、リポジトリに含まれるデータは破棄され、リカバリできなくなります。

DVM リポジトリでのリポジトリの確認ジョブの実行

この手順は、DVM リポジトリ全体の整合性をチェックするために実行します。AppAssure 5.3.x からリリース 5.4 にアップグレードする場合、レプリケートされたターゲット Core にこの手順を実行することをお勧めします。整合性チェックには時間がかかる場合がありますが、実行中はリポジトリ内で他のアクションは実行できません。

ターゲット Core に複数の DVM リポジトリがある場合、この処理をリポジトリ毎に 1 回ずつ実行します。

- ① **メモ:** ターゲット Core 上にすでに整合性チェックジョブが完了したリポジトリがある場合や、このターゲット Core に新しいリポジトリを追加で作成した場合には、指定した DVM リポジトリで整合性チェックジョブを実行中、そのセカンダリリポジトリでの操作は実行できます。

- Rapid Recovery Core Console に移動します。
- アイコンバーで、 より多い をクリックし、**リポジトリ** を選択します。
Repositories（リポジトリ）ページが表示されます。

DVM リポジトリ ペインが表示されます。

- 3 リポジトリサマリ表内のチェックするリポジトリを表す行で、 をクリックし、ドロップダウンメニューから、**リポジトリの確認ジョブ**を選択します。
- 確認メッセージが表示されます。

△ 注意: ジョブを実行することを確認する前に、必要な時間について慎重に検討する必要があります。ジョブの実行中は、そのリポジトリでは転送（スナップショットやベースイメージのバックアップ、およびレプリケーション）や夜間ジョブなど、他のトランザクションを実行することはできません。

- 4 整合性チェックを実行するには、**リポジトリの確認ジョブ** ダイアログボックスで、**はい** をクリックします。
- ダイアログボックスが閉じます。キューに登録済みのジョブや進行中のジョブはすべてキャンセルされ、整合性チェックジョブが開始します。
- 5 リポジトリの確認ジョブの進捗状況を監視し、チェック後に追加手順が必要になるかどうかを判断するには、アイコンバーで、 イベント をクリックします。

- 6 イベント ページで、 **ジョブの詳細** をクリックし、ジョブのステータスに関する詳細情報を表示します。
- このジョブの子タスクにエラーが表示された場合には、そのエラーについての情報を Dell のテクニカルサポート担当者に提供してください。
 - リポジトリの確認ジョブのすべての子タスクが正常に完了すると、このリポジトリにカスタム保持ポリシーを設定できるようになります。

セキュリティの管理

Core は、リポジトリ内の保護対象マシンスナップショットデータを暗号化できます。リポジトリ全体を暗号化する代わりに、リポジトリ内のマシンを保護する間に暗号化キーを指定することができ、これによって異なる保護対象マシンに対してこのキーを再使用することが可能になります。アクティブな各暗号化キーはそれぞれ暗号化ドメインを作成するので、暗号化がパフォーマンスに影響することはなく、単一のコアが複数の暗号化ドメインをホストすることによってマルチテナントをサポートすることが可能になります。マルチテナント環境では、データは暗号化ドメイン内でパーティション化され、重複排除されます。ユーザーが暗号化キーを管理することから、ボリュームの損失でキーが漏出することはありません。キーのセキュリティには、以下の概念と考慮事項があります。

- 暗号化は、SHA-3 に準拠した暗号ブロック連鎖（CBC）モードで 256 ビット AES を使用して実行されます。
- 重複排除は、機密性を確実にするために暗号化ドメイン内で実行されます。
- 暗号化はパフォーマンスに影響することなく実行されます。
- Core 上で設定された暗号化キーの追加、除去、インポート、エクスポート、変更、および削除を実行できます。
- コア上に作成できる暗号化キーの数に制限はありません。

保護対象マシンに対する暗号化の適用または削除

暗号化キーを定義し、それをリポジトリ内の 1 つ以上の保護対象マシンに適用することによって、Core で保護されるデータをいつでもセキュリティ保護することができます。1 つの暗号化キーは任意の数の保護対象マシンに適用できますが、保護対象マシンで一度に使用できるのは 1 つの暗号化キーのみです。

Rapid Recovery における重複排除の範囲は、同じレポジトリおよび暗号化キーを使用する保護対象マシンに限定されます。そのため、重複排除の利点を最大限に活用するには、実際に役立つできるだけ多くの保護対象マシンに 1 つの暗号化キーを適用することをお勧めします。ただし、Core 上に作成できる暗号化キーの数に制限はありません。したがって、法的コンプライアンス、セキュリティルール、プライバシーポリシー、その他に必要なであれば、暗号化キーをいくつでも追加および管理できます。その場合、1 つの保護対象マシンのみまたはリポジトリ内の任意の数のマシンに各キーを適用できます。

暗号化キーを保護対象マシンに適用するか、保護対象マシンから暗号化キーの関連付けを解除すると、スケジュールされた次のスナップショット作成時または強制的なスナップショット作成時に Rapid Recovery によりそのマシンの新しいベースイメージが

取得されます。そのベースイメージ（および暗号化キーの適用中に取得される以降のすべての増分スナップショット）に保存されたデータは、256 ビットの高度暗号化標準により保護されます。この暗号化方法を損なう既知の方法はありません。

保護対象マシンに現在使用されている既存の暗号化キーの名前またはパスフレーズを変更すると、スケジュールされた次のスナップショットまたは強制的なスナップショットの作成時に Rapid Recovery Core はそのキーの更新されたプロパティをキャプチャし、反映します。そのイメージ（および暗号化キーの適用中に取得される以降のすべての増分スナップショット）に保存されたデータは、256 ビットの高度暗号化標準により保護されます。この暗号化方法を損なう既知の方法はありません。

暗号化キーが作成され、保護対象マシンに適用された後、暗号化を削除する場合には 2 つの概念が関係します。1 つ目の概念は、保護対象マシンからキーの関連付けを解除することです。すべての保護対象マシンから暗号化キーの関連付けが解除されたら、必要に応じて Rapid Recovery Core から削除できます。

本項は、次のトピックで構成されています。

- ・ [暗号化キーの保護対象マシンとの関連付け](#)
- ・ [保護対象マシンページからの暗号化キーの適用](#)
- ・ [暗号化キーの関連付けを保護対象マシンから解除](#)

暗号化キーの保護対象マシンとの関連付け

次のいずれかの方法を使用して、暗号化キーを保護対象マシンに適用できます。

- ・ **マシンの保護の一環として：**この方法では、暗号化を 1 つまたは複数のマシンに同時に適用できます。この方法を使用すると、選択された 1 つ以上のマシンに、新しい暗号化キーを追加したり、既存のキーを適用したりできます。
マシンに対して保護を初めて定義するときに暗号化を使用するには、関連する「マシンの保護」ウィザードで詳細設定オプションを選択する必要があります。この選択を行うと、ウィザードのワークフローに「暗号化」ページが追加されます。このページで、「[暗号化の有効化](#)」を選択してから、既存の暗号化キーを選択するか、新しいキーのパラメータを指定します。詳細については、「[マシンの保護](#)」または「[複数のマシンの保護について](#)」をそれぞれ参照してください。
- ・ **マシンの構成設定を変更する：**この方法では、暗号化キーが一度に 1 つの保護対象マシンに適用されます。Rapid Recovery UI でマシンの構成設定を変更するには、次の 2 通りの方法があります。
 - ・ 保護対象マシンの構成設定を変更します。このアプローチで使用する暗号化キーは、Rapid Recovery Core にすでに存在していること、キータイプがユニバーサルであること、ロックされていないことが利用条件になります。暗号化は、一般設定の一部です。詳細については、「[保護対象マシンの設定の表示と変更](#)」を参照してください。
 - ・  **暗号化されていないアイコン**を保護対象マシンページでクリックします。この方法では、新しい暗号化キーを作成および適用したり、指定された保護対象マシンに既存のロック解除ユニバーサルキーを割り当てたりできます。詳細については、「[保護対象マシンページからの暗号化キーの適用](#)」を参照してください。

保護対象マシンページからの暗号化キーの適用

暗号化キーが Rapid Recovery Core に追加されたら、任意の数の保護対象マシンに使用できます。

1 つ以上のマシンを最初に保護するときに暗号化キーを選択すると、そのウィザードを使用して保護するすべてのマシンにそのキーが自動的に適用されます。この場合、次の手順は必要ありません。

次の手順を実行します。

- ・ Core の保護対象マシンのいずれかに、ロックされていない既存のユニバーサル暗号化キーを適用する場合。
- ・ トピック「[暗号化キーの追加](#)」で説明されているプロセスを使用して、新しい暗号化キーを追加済みで、そのキーを保護されたマシンに適用する場合。
- ・ Core の保護対象マシンに暗号化を適用済みでも、Core で使用可能なロックされていない別のユニバーサルキーにキーを変更する場合。

△ **注意:** 暗号化キーを保護対象マシンに適用すると、スケジュールされた次のスナップショット、または強制的なスナップショットの作成時に **Rapid Recovery** により新しいベースイメージが取得されます。

- 1 Rapid Recovery Core に移動し、**保護対象マシン** をクリックします。
保護対象マシン ページが表示され、この Core で保護されるすべてのマシンのリストが示されます。暗号化キーが適用されていないマシンには、開いた錠  が表示されます。閉じた錠  は、保護対象マシンに暗号化が適用されていることを示します。
- 2 保護対象マシン ペインで、設定する保護対象マシンのロックアイコンをクリックします。
暗号化の設定 ダイアログボックスが表示されます。
- 3 次の手順のいずれかを実行します。
 - ・ このマシンに既存の暗号化キーを適用する場合は、**Core** ベースの暗号化を使用して既存のキーでデータを暗号化 を選択し、ドロップダウンメニューから適切なキーを選択します。**OK** をクリックして確認します。
 - ・ 既存の暗号化キーを、ロックされていない別のユニバーサルキーに変更する場合は、**Core** ベースの暗号化を使用して新しいキーでデータを暗号化 を選択し、ドロップダウンメニューから適切なキーを選択します。**OK** をクリックして確認します。
 - ・ 新しい暗号化キーを作成し、この保護対象マシンに適用する場合は、**Core** ベースの暗号化を使用して新しいキーでデータを暗号化 を選択します。次の表の説明に従って、キーの詳細を入力します。

表 34. 新しい暗号化キーの詳細

テキストボックス	説明
名前	暗号化キーの名前を入力します。 暗号化キーの名前には、1～64 文字の英数字を入力する必要があります。 禁止されている文字 と 禁止されている語句 は、使用できません。
説明	暗号化キーの説明コメントを入力します。この情報は、Rapid Recovery Core Console から暗号化キーを表示するときに 説明 フィールドに表示されます。説明には 254 文字まで入力できます。 禁止されている文字 と 禁止されている語句 を使用しないことをお勧めします。
パスフレーズ	アクセスを制御するために使用されるパスフレーズを入力します。 禁止されている文字 を使用しないことをお勧めします。 パスフレーズは安全な場所に保管してください。Dell サポートでは、パスフレーズをリカバリすることはできません。暗号化キーを作成して 1 つ以上の保護対象マシンに適用した後でパスフレーズを損失した場合は、データをリカバリできません。
パスフレーズの確認	パスフレーズを再入力します。パスフレーズの入力を確認するために使用されます。

- 4 **OK** をクリックします。
ダイアログボックスが閉じます。指定した暗号化キーが、この保護対象マシンの今後のバックアップに適用されたので、閉じたロックが表示されます。

暗号化キーをただちに適用する場合は、必要に応じてスナップショット作成を強制実行します。詳細については、「[スナップショット作成の強制実行](#)」を参照してください。

△ **注意:** **Rapid Recovery** は、256 ビットキーを持つ CBC (Cipher Block Chaining、暗号文ブロック連鎖) モードの AES 256 ビット暗号化を採用しています。暗号化の使用は任意ですが、**Dell** 暗号化キーを設定し、定義したパスフレーズを保護することをお勧めします。パスフレーズはデータのリカバリに欠かせない重要なものであるため、安全な場所に保存してください。パスフレーズがない場合は、データをリカバリできません。

暗号化キーの関連付けを保護対象マシンから解除

暗号化キーが保護対象マシンに適用されると、Rapid Recovery Core に保存される以降のすべてのスナップショットデータが暗号化されます。

暗号化キーの関連付けは、保護対象マシンから解除できます。この操作では、既存のバックアップデータが復号化されるのではなく、スケジュールされた次のスナップショット作成時またはスナップショット作成の強制実行時に、そのマシンの新しいベースイメージが作成されます。

① **メモ:** 暗号化キーを **Core** から削除する場合は、**暗号化キーの削除**のトピックの説明に従って、その暗号化キーの関連付けをすべての保護対象マシンからまず解除する必要があります。

暗号化キーの関連付けを特定の保護対象マシンから解除するには、次の手順を実行します。

- 1 Rapid Recovery Core に移動し、**保護対象マシン** をクリックします。
保護対象マシン ページが表示され、この Core で保護されるすべてのマシンのリストが示されます。暗号化キーが適用されていないマシンには、開いた錠  が表示されます。閉じた錠  は、保護対象マシンに暗号化が適用されていることを示します。
- 2 保護対象マシン ペインで、設定する保護対象マシンの  **暗号化済み** アイコンをクリックします。
暗号化の設定 ダイアログボックスが表示されます。
- 3 **既存のキーで Core ベースの暗号化を使用してデータを暗号化する** を選択し、ドロップダウンメニューから **(なし)** を選択して、**OK** をクリックします。
- 4 この暗号化キーを Rapid Recovery Core から削除する場合は、このキーを使用するすべての保護対象マシンに対してまずこの手順を繰り返します。次に、**暗号化キーの削除**のトピックに記載されている手順を実行します。

暗号化キーの管理

Rapid Recovery Core の暗号化キーを管理するには、アイコンバーで  (詳細) をクリックし、次に **暗号化キー** を選択します。**暗号化キー** ページが表示されます。Rapid Recovery Core に追加された各暗号化キー (定義済みの場合) について、次の表に示す情報が表示されます。

表 35. 各暗号化キーの情報

UI エLEMENT	説明
アイテムを選択	表の上にあるメニューオプションリストからアクションを実行するために、各暗号化キーのチェックボックスを選択できます。
名前	暗号化キーに関連付けられた名前。
サンプリント	このパラメータは、各暗号化キーを一意に特定するのに役立つ、ランダムに生成された 26 文字の大文字と小文字の文字列です。
タイプ	タイプは、暗号化キーの始点とその適用性を示します。暗号化キーには、次のいずれかのタイプを指定できます。 ユニバーサル : ユニバーサル タイプは、暗号化キーを作成するときのデフォルトの状態です。ユニバーサル タイプのキーは、ロック解除 状態と組み合わせて、保護対象マシンにキーを適用できることを示します。ユニバーサル キータイプを手動でロックすることはできません。代わりに、「暗号化キーのタイプを変更」の手順に従って、まずタイプを変更する必要があります。 レプリケーション : ソース Core の保護対象マシンで暗号化が有効になっており、そのマシンのリカバリポイントがターゲット Core でレプリケートされると、ソースで使用されるすべての暗号化キーは、レプリケート タイプでターゲット Core に自動的に表示されます。レプリケートされたキーの受信後のデフォルト状態は「ロック」です。パスフレーズを指定すると、レプリケート タイプの暗号化キーをロック解除できます。キーが ロック解除 タイプの場合は、手動でロックできます。詳細については、「暗号化キーのロック解除」のトピックを参照してください。
州	状態は、暗号化キーを使用できるかどうかを示します。次の 2 つの状態が有効です。

- ・ **ロック解除**。「ロック解除」状態は、キーをただちに使用できることを示します。たとえば、保護対象マシンのスナップショットを暗号化したり、ターゲット Core のレプリケートされたリカバリポイントからデータリカバリを実行したりできます。
- ・ **ロック**。「ロック」状態は、パスフレーズを指定してロック解除するまで、キーを使用できないことを示します。「ロック」は、新しくインポートまたはレプリケートされた暗号化キーのデフォルトの状態です。

暗号化キーが ロック 状態の場合は、使用する前にロック解除する必要があります。

ロックされた暗号化キーを以前にロック解除しており、ロック解除の保持期間が終了すると、状態が ロック 解除 から ロック に変更されます。自動的にロックされたキーを使用するには、再びロック解除する必要があります。詳細については、「[暗号化キーのロック解除](#)」のトピックを参照してください。

説明	説明は、使用目的やパスフレーズのヒントなど、暗号化キーに関する便利な情報を提供するために推奨される省略可能なフィールドです。

暗号化キー ペインの上部で、暗号化キーを追加したり、別の Rapid Recovery Core からエクスポートされたファイルを使用してキーをインポートしたりできます。サマリ表で選択したキーを削除することもできます。

Core に暗号化キーが存在する場合は、名前または説明プロパティの編集、パスフレーズの変更、ロックされた暗号化キーのロック解除、Rapid Recovery Core からのキーの削除などを行って、既存のキーを管理できます。また、キーをファイルにエクスポートすることもできます。このファイルは、別の Rapid Recovery Core にインポートできます。

暗号化キー ページから暗号化キーを追加すると、キーは暗号化キーのリストには表示されますが、特定の保護対象マシンには適用されません。**暗号化キー** ペインから作成した暗号化キーを適用する方法、および Rapid Recovery Core からキー全体を削除する方法については、「[保護対象マシンに対する暗号化の適用または削除](#)」を参照してください。

暗号化キー ペインから次の手順を実行すると、リポジトリ内の任意の保護対象マシンに対して、Core に保存されたバックアップデータのセキュリティを管理できます。

- ・ [暗号化キーの追加](#)
- ・ [暗号化キーのインポート](#)
- ・ [暗号化キーのロック解除](#)
- ・ [暗号化キーの編集](#)
- ・ [暗号化キーのパスフレーズの変更](#)
- ・ [暗号化キーのエクスポート](#)
- ・ [暗号化キーの削除](#)
- ・ [暗号化キーのタイプを変更](#)

暗号化キーの追加

Rapid Recovery は、256 ビットキーを持つ CBC (Cipher Block Chaining、暗号文ブロック連鎖) モードの AES 256 ビット暗号化を採用しています。暗号化の使用は任意ですが、Dell 暗号化キーを設定し、定義したパスフレーズを保護することをお勧めします。

△ 注意: パスフレーズは安全な場所に保管してください。パスフレーズがないと、暗号化されたリカバリポイントからデータをリカバリすることはできません。

暗号化キーが定義されたら、それを使用してデータを保護できます。暗号化キーを使用できる保護対象マシンの数に制限はありません。

次の手順では、Rapid Recovery Core Console から暗号化キーを追加する方法を説明します。この手順では、Core で現在保護されているマシンにキーを適用しません。マシンの保護プロセス中に、暗号化キーを追加することもできます。1 台のマシンの保護の一環として暗号化を追加する場合は、「[マシンの保護](#)」を参照してください。複数のマシンを初めて保護するときに暗号化を追加する場合は、「[複数のマシンの保護について](#)」を参照してください。

暗号化キーを追加するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (より多い) をクリックして、**暗号化キー** を選択します。
暗号化キー ページが表示されます。
- 3 **暗号化キーを追加** をクリックします。
暗号化キーを作成 ダイアログボックスが表示されます。
- 4 **暗号化キーを作成** ダイアログボックスで、次の表の説明に従って、キーの詳細を入力します。

表 36. 暗号化キーの詳細の作成

テキストボックス	説明
名前	暗号化キーの名前を入力します。 暗号化キーの名前には、1～64 文字の英数字を入力する必要があります。 禁止されている文字と禁止されている語句 は、使用できません。
説明	暗号化キーのコメントを入力します。 この情報は、Core Console から暗号化キーを表示するときに 説明 フィールドに表示されます。254 文字まで入力できます。 禁止されている文字と禁止されている語句 を使用しないことをお勧めします。
パスフレーズ	アクセスを制御するために使用されるパスフレーズを入力します。 禁止されている文字 を使用しないことをお勧めします。  注意: パスフレーズは安全な場所に保管してください。Dell サポートでは、パスフレーズをリカバリできません。暗号化キーを作成して 1 つ以上の保護対象マシンに適用した後でパスフレーズを損失した場合は、データをリカバリできません。
パスフレーズの確認	パスフレーズを再入力します。パスフレーズの入力を確認するために使用されます。

- 5 **OK** をクリックします。
ダイアログボックスが閉じて、作成した暗号化キーが **暗号化キー** ページに表示されます。
- 6 暗号化キーを保護対象マシンに適用する場合は、「**保護対象マシンページからの暗号化キーの適用**」を参照してください。

暗号化キーのインポート

暗号化キーを別の Rapid Recovery Core からインポートし、そのキーを使用して Core 内の保護対象マシンのデータを暗号化できます。キーをインポートするには、ローカルまたはネットワーク経由で Core マシンからデータにアクセスする必要があります。暗号化キーのパスフレーズも知る必要があります。

暗号化キーをインポートするには、次の手順を実行します。

- ① **メモ:** 次の手順では、保護対象マシンにキーを適用しません。キーの適用の詳細については、「**保護対象マシンページからの暗号化キーの適用**」を参照してください。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで、 (詳細) をクリックし、**暗号化キー** を選択します。
暗号化キー ページが表示されます。
- 3  **インポート** をクリックします。

ファイルのアップロード ダイアログボックスが表示されます。

- 4 **ファイルのアップロード** ダイアログボックスで、インポートする暗号化キーが含まれているネットワークまたはローカルのディレクトリに移動します。

たとえば、ログインユーザーの **ダウンロード** フォルダに移動します。

キーのファイル名は「EncryptionKey」で始まり、その後にキー ID が続き、ファイル拡張子 .key で終わります。たとえば、暗号化キーの名前は EncryptionKey-RandomAlphabeticCharacters.key のようになります。

- 5 インポートするキーを選択し、「**開く**」をクリックします。
- 6 **キーをインポート** ダイアログボックスで、**OK** をクリックします。

ダイアログボックスが閉じて、インポートした暗号化キーが **暗号化キー** ページに表示されます。暗号化キーがエクスポートされる前にボリュームの保護に使用されている場合は、キーが「ロック」状態になります。

暗号化キーのロック解除

暗号化キーは、ロック解除またはロックの状態になることがあります。ロック解除された暗号化キーは、保護対象マシンに適用して、リポジトリに保存されたそのマシンのバックアップデータをセキュリティ保護することができます。ロック解除された暗号化キーを Rapid Recovery Core から使用して、リカバリポイントからデータをリカバリすることもできます。

暗号化キーを Rapid Recovery Core にインポートすると、デフォルトにより「ロック」状態になります。キーを明示的にインポートしたかどうか、あるいは暗号化された保護対象マシンのレプリケーションまたは暗号化されたリカバリポイントのアーカイブのインポートのいずれかを行うことによって暗号化キーが Rapid Recovery Core に追加されたかどうかに関係なく、この状態になります。

暗号化キーがレプリケーションによって Rapid Recovery Core に追加された場合にのみ、キーをロック解除するときに、暗号化キーのロック解除の保持期間（時間、日、月単位）を指定できます。1日は24時間を基にしており、ロック解除リクエストが Rapid Recovery Core に保存された時刻から開始します。たとえば、キーを火曜日の午前11時24分にロック解除し、保持期間に2日を選択した場合は、木曜日の午前11時24分にキーが自動的にロックされます。

① メモ: ロックされた暗号化キーを使用して、データをリカバリしたり、保護対象マシンに適用したりすることはできません。まず、パスフレーズを指定して、キーをロック解除する必要があります。

また、ロック解除された暗号化キーをロックして、ロック解除されるまで保護対象マシンに適用できないようにすることもできます。ユニバーサルステータスの暗号化キーをロックするには、まずタイプを **レプリケート** に変更する必要があります。

Core のマシンを保護するためにロック解除された暗号化キーが現在使用中の場合は、まずその暗号化キーの関連付けを保護対象マシンから解除してから、ロックする必要があります。

ロックされた暗号化キーをロック解除するには、次の手順を実行します。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで、より多いをクリックし、**暗号化キー** を選択します。
暗号化キー ページが表示されます。「状態」列に、どの暗号化キーがロックされているかが示されます。
- 3 ロック解除する暗号化キーを見つけ、ドロップダウンメニュー  をクリックし、**ロック解除** を選択します。
暗号化キーをロック解除 ダイアログボックスが表示されます。
- 4 ダイアログボックスのパスフレーズフィールドに、このキーをロック解除するためのパスフレーズを入力します。
- 5 キーのロック解除の保持期間を指定するには、「期間」オプションで次のいずれかを実行します。
 - ・ 明示的にロックするまでキーのロック解除を保持するには、Rapid Recovery で **手動でロックするまで** を選択します。
 - ・ 時間、日、月単位で設定した期間はキーをロックしておくように指定するには、次の手順を実行します。
 - ・ 番号フィールドを選択し、1～999の間の値を入力します。
 - ・ 時間、日数、月数の期間をそれぞれ選択します。
 - ・ 次に、「**OK**」をクリックします。

このオプションは、レプリケーションによって追加された暗号化キーに使用できます。

ダイアログボックスが閉じて、選択した暗号化キーが「暗号化キー」ページに表示されます。

- ・ 指定した日付と時刻までキーをロックしておくように指定するには、次の手順を実行します。
 - ・ **終了日** オプションを選択します。
 - ・ テキストフィールドまたはカレンダーか時計ウィジェットを使用して、暗号化キーをロックする日付と時刻を明示的に指定します。
 - ・ 次に、「OK」をクリックします。
- このオプションは、レプリケーションによって追加された暗号化キーに使用できます。

ダイアログボックスが閉じて、選択した暗号化キーが「暗号化キー」ページに表示されます。

暗号化キーのロック

暗号化キーの状態がロックであると、ロック解除するまで保護対象マシンに適用することはできません。「ユニバーサル」タイプの暗号化キーをロックするには、まず「レプリケート」タイプに変更する必要があります。

暗号化キーをロックするには、次の手順を実行します。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで、（詳細）をクリックし、**暗号化キー**を選択します。
暗号化キー ページが表示されます。状態 列に、どの暗号化キーがロック解除されているかが示され、各キーのタイプが表示されます。
- 3 ロックする暗号化キーを見つけます。タイプがユニバーサルの場合は、ドロップダウンメニューで  をクリックし、**タイプをレプリケートに変更**を選択します。
暗号化キーのタイプを変更 ダイアログボックスが表示されます。
- 4 ダイアログボックスで、キータイプを **レプリケート** に変更することを確認します。
- 5 暗号化キーのステータスがレプリケートに正常に変更されたら、ドロップダウンメニュー  をクリックし、**ロック**を選択します。
暗号化キーをロック ダイアログボックスが表示されます。
- 6 ダイアログボックスで、キーをロックすることを確認します。
ダイアログボックスが閉じて、選択した暗号化キーの状態が「ロック」になります。

① | **メモ:** このオプションは、レプリケーションによって追加された暗号化キーに使用できます。

暗号化キーの編集

暗号化キーが定義されたら、暗号化キーの名前や説明を編集できます。これらのプロパティは、「暗号化キー」ペインに暗号化キーのリストを表示するときに表示されます。

既存のロック解除された暗号化キーの名前または説明を編集するには、次の手順を実行します。

△ | **注意:** 1つ以上のマシンの保護に使用される暗号化キーの名前または説明を編集すると、**Rapid Recovery** で新しいベースイメージが取得されます。スケジュールされた次のスナップショット作成時またはスナップショット作成の強制実行時に、そのマシンのベースイメージのスナップショットが作成されます。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで、（詳細）をクリックし、**暗号化キー**を選択します。
暗号化キー ページが表示されます。
- 3 編集する暗号化キーを見つけ、次の手順を実行します。
 - ・ キーがロックされている場合は、最初にロックを解除する必要があります。参照先 [暗号化キーのロック解除](#)

- ・ キーがロック解除されている場合は、次のように操作を続けます。

- 4 ドロップダウンメニューで  をクリックし、**編集** を選択します。
Edit Encryption Key (暗号化キーを変更) ダイアログボックスが表示されます。
- 5 ダイアログボックスで、暗号化キーの名前や説明を編集して、**OK** をクリックします。
ダイアログボックスが閉じて、選択した暗号化キーが **暗号化キー** ページに表示されます。

暗号化キーのパスフレーズの変更

セキュリティを最大限に保持するため、既存の暗号化キーのパスフレーズを変更できます。暗号化キーのパスフレーズを変更するには、次の手順を実行します。

△ **注意:** 1つ以上のマシンの保護に使用される暗号化キーのパスフレーズを編集すると、スケジュールされた次のスナップショット作成時またはスナップショット作成の強制実行時に、**Rapid Recovery Core** によってそのマシンの増分スナップショットが取得されます。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで、 (より多い) をクリックして、**暗号化キー** を選択します。
暗号化キー ページが表示されます。
- 3 アップデートする暗号化キーを見つけ、ドロップダウンメニュー  をクリックして、**パスフレーズを変更** を選択します。
Change Passphrase (パスフレーズの変更) ダイアログボックスが表示されます。
- 4 ダイアログボックスで、**パスフレーズ** フィールドに暗号化用の新しいパスフレーズを入力します。
- 5 **パスフレーズの確認** フィールドに、同一のパスフレーズを再入力します。
- 6 **OK** をクリックします。
ダイアログボックスが閉じて、パスフレーズがアップデートされます。
- 7 必要に応じて、説明 フィールドにヒントを使用している場合、暗号化キーを編集してヒントを更新します。詳細については、「**暗号化キーの編集**」を参照してください。

△ **注意:** **Rapid Recovery** は、**256 ビット** キーを持つ **CBC (Cipher Block Chaining、暗号文ブロック連鎖)** モードの **AES 256** ビット暗号化を採用しています。**Dell** パスフレーズは、安全な場所に保管し、最新の状態にしておくことをお勧めします。**Dell** サポートでは、パスフレーズをリカバリすることはできません。パスフレーズがないと、暗号化されたリカバリポイントから情報をリカバリすることはできません。

暗号化キーのエクスポート

暗号化キーを任意の Rapid Recovery Core からエクスポートして、別の Core で使用できます。次の手順を実行すると、アクティブな Windows ユーザーアカウントの **ダウンロード** フォルダにキーが保存されます。

暗号化キーをエクスポートするには、次の手順を実行します。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで、 (詳細) をクリックし、**暗号化キー** を選択します。
暗号化キー ページが表示されます。
- 3 エクスポートする暗号化キーを見つけ、ドロップダウンメニューで  をクリックし、**エクスポート** を選択します。
EncryptionKey-[name.key] を開く ダイアログボックスが表示されます。
- 4 ダイアログボックスで **ファイルを保存** を選択して、暗号化キーを安全な場所に保存し、**OK** をクリックします。
暗号化キーはデフォルトの場所 (アクティブな Windows ユーザーアカウントの **ダウンロード** フォルダなど) にテキストファイルとしてダウンロードされます。

- 5 必要に応じて、別の Core にこのキーをインポートする場合は、その Core からアクセス可能な場所にファイルをコピーします。

暗号化キーの削除

暗号化キーページで暗号化キーを削除すると、Rapid Recovery Core からキーが削除されます。

- ① **メモ:** 暗号化キーを削除しても、キーを使用してすでに保存されているリカバリポイントは復号化されません。既存の暗号化済みリカバリポイントのデータをリカバリする場合でも、パスフレーズを保持し、入力する必要があります。

保護対象マシンに既に関連付けられている暗号化キーは削除できません。まず、キーを使用している保護対象マシンごとに暗号化設定を表示し、削除する暗号化キーの関連付けを解除する必要があります。詳細については、「[暗号化キーの関連付けを保護対象マシンから解除](#)」のトピックを参照してください。

暗号化キーを削除するには、次の手順を実行します。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで  (詳細) をクリックし、**暗号化キー** を選択します。
暗号化キー ページが表示されます。
- 3 削除する暗号化キーを見つけます。そのドロップダウンメニュー  をクリックし、**削除** を選択します。
暗号化キーを削除 ダイアログボックスが表示されます。暗号化キーを削除するアクションを確認するメッセージが表示されます。
- 4 ダイアログボックスで、暗号化キーを削除することを確認します。

- ① **メモ:** 暗号化キーを削除しても、キーを使用してすでに保存されているリカバリポイントは復号化されません。既存の暗号化済みリカバリポイントのデータをリカバリする場合でも、キーを保持し、入力する必要があります。

ダイアログボックスが閉じ、削除した暗号化キーが **暗号化キー** ページに表示されなくなります。

暗号化キーのタイプを変更

「暗号化キー」ペインには、暗号化キーに有効な「ユニバーサル」または「レプリケート」のいずれかのタイプが表示されます。タイプは、暗号化キーの始点を示し、詳細またはパスフレーズを変更できるかどうかが決まります。これらの属性は、「ユニバーサル」タイプの場合にのみ変更できます。これらの属性を「レプリケート」タイプのキーで変更する必要がある場合は、次の手順を実行してタイプを「ユニバーサル」に変更する必要があります。暗号化キーのタイプを「ユニバーサル」に変更すると、暗号化キーが手動でロック解除され、他の保護対象マシンの暗号化に使用できます。

- ① **メモ:** タイプを「レプリケート」から「ユニバーサル」に変更するには、パスフレーズが必要です。

また、暗号化キーには、「ロック」および「ロック解除」という 2 つの有効な状態もあります。状態は、暗号化キーを保護対象マシンに適用できるかどうか、または暗号化のリカバリポイントからデータをリストアできるかどうかを制御します。暗号化キーのタイプは、「ロック解除」状態の場合にのみ手動で変更できます。

暗号化キーを初めて作成した時点では、タイプは「ユニバーサル」、状態は「ロック解除」になります。このようなキーはただちに使用できます (保護対象マシンのバックアップを暗号化するなど)。ただし、ユニバーサルキーのタイプを手動でロックすることはできません。「ユニバーサル」タイプのキーを手動でロックするには、次の手順を実行してタイプを「レプリケート」に変更する必要があります。

暗号化キーのタイプが 1 つ、または複数の保護対象マシンのリカバリポイントの暗号化にすでに使用中である場合は、それを変更することはできません。

暗号化キータイプを変更するには、次の手順に従います。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンバーで、（詳細） をクリックし、**暗号化キー** を選択します。
暗号化キー ページが表示されます。Core に関連付けられている暗号化キーがサマリ表に表示されます。各暗号化キーには、「ユニバーサル」または「レプリケート」のいずれかのタイプが表示されます。
- 3 アップデートする暗号化キーを選択します。
- 4 「ユニバーサル」暗号化キーを「レプリケート」に変更する場合は、次のいずれかを実行します。
 - a ドロップダウンメニューで  をクリックし、**タイプをレプリケートに変更** を選択します。
暗号化キーのタイプを変更 ダイアログボックスが表示されます。タイプをレプリケートに変更することを確認するメッセージが表示されます。
 - ・ ダイアログボックスで、タイプをレプリケートに変更することを確認します。ダイアログボックスが閉じ、暗号化キーのタイプがレプリケートにアップデートされます。
- 5 「レプリケート」暗号化キーを「ユニバーサル」に変更する場合は、次のいずれかを実行します。
 - a ドロップダウンメニューで  をクリックし、**タイプをユニバーサルに変更** を選択します。
暗号化キーのタイプを変更 ダイアログボックスが表示されます。タイプをユニバーサルに変更することを確認するメッセージが表示されます。
 - ・ ダイアログボックスの **パスフレーズ** フィールドにパスフレーズを入力し、**OK** をクリックしてタイプをユニバーサルに変更することを確認します。ダイアログボックスが閉じ、暗号化キーのタイプがユニバーサルにアップデートされます。

クラウドアカウントの管理

本項では、既存のクラウドストレージプロバイダアカウントへのリンクを定義する方法、および Rapid Recovery で使用するためにそれらのクラウドアカウントを管理する方法について説明します。たとえば、Rapid Recovery のデータをクラウドにアーカイブしたり、クラウドからアーカイブ済みデータをインポートしたりできます。

クラウドアカウントについて

Rapid Recovery を使用すると、多岐にわたるクラウドプロバイダにデータをアーカイブしたり、クラウドアカウントに保存されているアーカイブ済みデータをインポートしたりできます。互換性のあるクラウドには、Microsoft Azure、Amazon™、Rackspace、および OpenStack ベースのすべてのプロバイダが含まれます。

Rapid Recovery Core Console には既存のクラウドアカウントを追加できます。アカウントを追加したら、情報の編集、アカウント接続オプションの設定、Rapid Recovery からのアカウントの削除を実行できます。

クラウドアカウントの追加

クラウドアカウントと Core の間のどちらの方向であっても、データを移動する前には、クラウドプロバイダのアカウント情報を Rapid Recovery Core Console に追加する必要があります。この情報は、接続情報を安全な方法でキャッシュしている間に、Core Console のクラウドアカウントを識別します。このプロセスでは、次に Rapid Recovery Core をクラウドアカウントに接続させて、指定した操作を実行します。

クラウドアカウントを追加するには、次の手順を実行します。

- 1 Rapid Recovery Core Console アイコンバーをクリックし、 **より多い** アイコンをクリックして **クラウドアカウント** を選択します。

クラウドアカウント ページが表示されます。

- 2 クラウドアカウント ページで **新しいアカウントを追加** をクリックします。
新規アカウントの追加 ダイアログボックスが開きます。
- 3 クラウドタイプ ドロップダウンリストから互換性のあるクラウドプロバイダを選択します。
- 4 手順3 で選択したクラウドタイプに基づいて、次の表に説明されている詳細を入力します。

表 37. クラウドアカウントの詳細

クラウドタイプ	テキストボックス	説明
Microsoft Azure	ストレージアカウント名	Microsoft Azure ストレージアカウントの名前を入力します。 ① メモ: アカウントの名前は、 Azure のストレージアカウント名と完全に一致する必要があります。使用できるのは小文字の英字と数字のみで、 3 ~ 24 文字にする必要があります。
	アクセスキー	ご使用のアカウントのアクセスキーを入力します。 ① メモ: プライマリまたはセカンダリのキーを入力できます。 Azure アカウントのアクセスキーを取得するには、設定のキーを確認します。
	HTTPS プロトコルを使用する	標準的な HTTP プロトコルの代わりに HTTPS プロトコルを使用するには、このオプションを選択します。
	表示名	Rapid Recovery Core コンソールに表示する、このクラウドアカウントの表示名を入力します。たとえば、Microsoft Azure 1 などとします。
Amazon™ S3	アクセスキー	ご使用の Amazon™ クラウドアカウントのアクセスキーを入力します。
	秘密キー	このアカウントの秘密キーを入力します。
	表示名	Rapid Recovery Core コンソールに表示する、このクラウドアカウントの表示名を入力します。たとえば、Amazon 1 などとします。
OpenStack ベースのクラウド	地域	クラウドアカウントの領域を入力します。
	ユーザー名	OpenStack ベースのクラウドアカウントのユーザー名を入力します。
	パスワードまたは API キー	パスワードまたは API キーを使用するかどうかを選択し、このアカウントでの選択を入力します。
	テナント ID	このアカウントのテナント ID を入力します。
	認証 URL	このアカウントの認証 URL を入力します。
Rackspace クラウドファイル	表示名	Rapid Recovery Core Console に表示する、このクラウドアカウントの表示名を入力します。たとえば、OpenStack 1 などとします。
	地域	ドロップダウンリストを使用してアカウント用の領域を選択します。
	ユーザー名	Rackspace クラウドアカウントのユーザー名を入力します。
	パスワードまたは API キー	パスワードまたは API キーを使用するかどうかを選択し、このアカウントでの選択を入力します。
	テナント ID	このアカウントのテナント ID を入力します。
	認証 URL	このアカウントの認証 URL を入力します。

表示名	Rapid Recovery Core コンソールに表示する、このクラウドアカウントの表示名を入力します。たとえば、Rackspace 1 などとします。

- 5 **保存** をクリックします。
ダイアログボックスが閉じて、アカウントが Core Console の **クラウドアカウント** ページに表示されます。

クラウドアカウントの編集

パスワードのアップデートや、表示名の編集など、クラウドアカウントに接続するための情報を変更する必要がある場合は、Rapid Recovery Core Console の **クラウドアカウント** ページで変更できます。クラウドアカウントを編集するには、次の手順を実行します。

- 1 Rapid Recovery Core Console アイコンバーをクリックし、 **より多い** アイコンをクリックして **クラウドアカウント** を選択します。
クラウドアカウント ページが表示されます。
- 2 編集するクラウドアカウントの横にあるドロップダウンメニューをクリックして、**編集** をクリックします。
アカウントを編集 ウィンドウが開きます。
- 3 必要に応じて、詳細を編集し、**保存** をクリックします。

① | **メモ:** クラウドタイプは編集できません。

クラウドアカウント設定の構成

クラウド設定を指定すると、Rapid Recovery がクラウドアカウントに接続を試みてからタイムアウトするまでの時間を特定できます。クラウドアカウントの接続設定を構成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のアイコンバーで  **設定** をクリックします。
「設定」ページが表示されます。
- 2 左側のメニューで **クラウドアカウント** をクリックします。
- 3 クラウドアカウントの表で、設定するクラウドアカウントの横にあるドロップダウンメニューをクリックし、次のアクションのいずれかを実行します。
 - ・ クラウドアカウントの接続設定を変更するには、**編集** をクリックします。
 - 1 クラウド設定 ダイアログボックスで、次の手順のいずれかを実行します。
 - ・ **リクエストタイムアウト** では、上下の矢印を使用して、遅延が生じた場合に、Rapid Recovery がクラウドアカウントに 1 回の接続試行で費やす時間を、分と秒の単位で指定します。接続試行は入力された時間が経過すると停止します。
 - ・ **書き込みバッファサイズ** では、アーカイブデータのクラウドへの書き込み用に予約するバッファのサイズを入力します。
 - ・ **読み取りバッファサイズ** では、アーカイブデータのクラウドからの読み取り用に予約するブロックのサイズを入力します。
 - 2 「**OK**」をクリックします。
 - ・ クラウド設定をデフォルト設定に戻すには、**リセット** をクリックします。
 - ・ **リクエストタイムアウト** : 01:30 (分と秒)
 - ・ **書き込みバッファサイズ** : 8388608 (バイト)
 - ・ **読み取りバッファサイズ** : 8388608 (バイト)

クラウドアカウントの削除

クラウドサービスを切断したり、特定の Core でクラウドサービスの使用を停止する場合は、Core Console からクラウドアカウントを削除できます。クラウドアカウントを削除するには、次の手順を実行します。

- 1 Rapid Recovery Core Console アイコンバーをクリックし、 より多いアイコンをクリックして **クラウドアカウント** を選択します。
クラウドアカウント ページが表示されます。
- 2 編集するクラウドアカウントの横にあるドロップダウンメニューをクリックして、**削除** をクリックします。
- 3 **アカウントを削除** ダイアログボックスで **はい** をクリックして、アカウントの削除を確認します。
- 4 クラウドアカウントが現在使用中の場合は、2 番目のダイアログボックスが表示され、本当に削除するかどうかを確認されます。**はい** をクリックして確認します。

① **メモ:** 現在使用されているアカウントを削除すると、そのアカウントでスケジュール設定されているすべてのアーカイブジョブが失敗します。

アーカイブあーかいぶ

このセクションでは、アーカイブ作成のビジネスケース、Rapid Recovery を使用したアーカイブ作成方法、アーカイブの保存場所について説明します。

アーカイブについて

保持ポリシーは、短期間（高速で高価な）メディアにバックアップを保存する期間を適用します。特定の事業および技術要件によって、これらのバックアップの延長保持が必要となることがありますが、高速ストレージの使用は非常に高額です。したがって、この要件では、長期間（遅くて安い）ストレージが必要になります。企業では、準拠および非準拠データの両方のアーカイブに長期ストレージを使用することがよくあります。Rapid Recovery のアーカイブ機能は、準拠および非準拠データの延長保持をサポートします。レプリケーションデータをリモートレプリカ Core にシーディングするときにも使用されます。

アーカイブが作成されると、次の方法で使用できるようになります。

- ・ 単純なファイルまたはフォルダをリカバリするファイルシステムとしてマウントする。
- ・ Bare Metal Restore のソースとして使用する。
- ・ リポジトリにインポートする。

アーカイブの作成

この手順を使用して、1 回限りの、またはスケジュール設定されたアーカイブを作成することができます。

クラウドの場所にアーカイブを作成しようとしている場合は、最初にクラウドアカウントを Rapid Recovery Core Console に追加します。詳細については、「[クラウドアカウントの追加](#)」を参照してください。

1 回限りのアーカイブとは、指定されたマシンに対してオンデマンドで作成されるアーカイブです。スケジュール設定されたアーカイブとは、ウィザードで指定した日付と時間に自動的に繰り返し作成されるアーカイブです。スケジュール設定によりアーカイブ

ブを繰り返し作成できる機能により、アーカイブを手動で作成するという手間をかけずに、マシンのアーカイブを頻繁に保存することが必要な状況に対応できます。



- 1 Rapid Recovery Core Console のボタンバーで **アーカイブ** をクリックします。
アーカイブウィザードが開きます。
- 2 ウィザードの **アーカイブタイプ** ページで、次のいずれかのオプションを選択します。
 - ・ 1回限りのアーカイブ
 - ・ 継続アーカイブ（スケジュール使用）
- 3 「次へ」をクリックします。
- 4 **場所** ページで **場所のタイプ** ドロップダウンリストからオプションを選択し、次の表の説明に従って情報を入力します。

表 38. アーカイブの場所のタイプのオプション

オプション	テキストボックス	説明
ローカル	場所	出力の場所を入力します。d:\work\archive などアーカイブを格納する場所のパスの定義のために使用されます。
ネットワーク	場所	出力の場所を入力します。\\servername\sharename などアーカイブを格納する場所のパスの定義のために使用されます。
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
クラウド	アカウント	ドロップダウンリストからアカウントを選択します。
ⓘ メモ: クラウドアカウントを選択するには、先に、 Core Console にクラウドアカウントが追加されている必要があります。詳細については、「 クラウドアカウントの追加 」を参照してください。		
	コンテナ	ドロップダウンメニューからアカウントに関連付けられているコンテナを選択します。
	フォルダ名	アーカイブデータの保存先のフォルダ名を入力します。

- 5 「次へ」をクリックします。
- 6 ウィザードの **マシン** ページで、アーカイブする保護対象マシンを 1 台または複数選択します。
- 7 「次へ」をクリックします。
- 8 次の手順のいずれかを実行します。
 - ・ 1回限りのアーカイブを作成する場合は、[手順 15](#) に進みます。
 - ・ スケジュール設定されたアーカイブを作成する場合は、[手順 9](#) に進みます。
- 9 **スケジュール** ページで、**データを送信** ドロップダウンリストから、次のいずれかのオプションを選択します。
 - ・ 日次
 - ・ 週次
 - ・ 月次
- 10 [手順 9](#) での選択内容に基づき、次の表に従って、情報を入力します。

表 39. データ送信のオプション

オプション	テキストボックス	説明
日次	時間	日次アーカイブを作成する時間を選択します。
週次	曜日	アーカイブを自動的に作成する曜日を選択します。
	時間	アーカイブを作成する時刻を選択します。
月次	日付	アーカイブを自動的に作成する日付を選択します。
	時間	アーカイブを作成する時刻を選択します。

- 11 ウィザードの完了後に次のスケジュール時刻にアーカイブジョブを開始しない場合は、**最初のアーカイブを一時停止**を選択することもできます。

① **メモ:** アーカイブを再開する前にターゲットの場所を準備する時間が必要な場合は、スケジュールされたアーカイブを一時停止することをお勧めします。このオプションを選択しない場合は、スケジュールされた時間にアーカイブが開始されます。

- 12 「次へ」をクリックします。

- 13 継続アーカイブの **オプション** ページで、次の表に説明されているリサイクルアクションのいずれかを選択します。

表 40. 継続アーカイブのリサイクルのオプション

テキストボックス	説明
Incremental (増分)	既存のアーカイブにリカバリポイントを追加できます。リカバリポイントを比較して、アーカイブに既に存在するデータの重複を回避します。
この Core を置換	この Core に関連する既存のアーカイブを上書きしますが、他の Core のデータはそのまま残します。
完全に消去	新しいアーカイブへの書き込みの前にディレクトリからすべてのアーカイブデータを消去します。

- 14 必要に応じて、**リカバリポイントチェーンを作成 (オフエンの修正)** を選択し、**手順 18** に進みます。

- 15 1 回限りのアーカイブの **オプション** ページで、次の表に説明されている情報を入力します。

表 41. 1 回限りのアーカイブのオプション

テキストボックス	説明
最大サイズ	容量の大きいデータアーカイブは、複数のセグメントに分割できます。次のいずれかを実行して、アーカイブを作成するために確保する必要がある最大領域サイズを選択します。 - ターゲット全体を選択して、手順 4 で入力した宛先で指定したパスの使用可能なすべての領域を予約します。(たとえば、場所が D:\work\archive である場合は、D: ドライブ上のすべての使用可能な領域が確保されます)。 - 空白のテキストボックスを選択して、上矢印と下矢印を使用して数量を入力し、ドロップダウンリストから単位を選択して、確保する最大領域をカスタマイズします。 ① メモ: Amazon™ クラウドアーカイブは、自動的に 50 GB のセグメントに分割されます。Microsoft Azure クラウドアーカイブは、自動的に 200 GB のセグメントに分割されます。
リサイクルアクション	次のリサイクルアクションオプションのいずれかを選択します。 - 再使用不可。この場所から既存のアーカイブデータを上書きまたはクリアしません。場所が空でない場合は、Rapid Recovery で別の場所を選択することができます。 - この Core を交換。この Core に関連する既存のアーカイブを上書きしますが、他の Core のデータはそのまま残します。 - 完全に消去。新しいアーカイブへの書き込みの前にディレクトリからすべてのアーカイブデータを消去します。

テキストボックス 説明

- ・ 増分。既存のアーカイブにリカバリポイントを追加できます。リカバリポイントを比較して、アーカイブに既に存在するデータの重複を回避します。

コメント	アーカイブをキャプチャするために必要な追加情報を入力します。後でアーカイブをインポートする場合にコメントが表示されます。

リカバリポイントチェーンの修正)	このオプションを選択すると、リカバリポイントチェーン全体をアーカイブできます。このオプションは、デフォルトで、選択されています。

- 16 「次へ」をクリックします。
- 17 **日付範囲** ページで、アーカイブするリカバリポイントの開始日と終了日を手動で入力するか、カレンダーウィンドウの下でカレンダーアイコン、時計アイコンの順にクリックして日時を選択します。
- 18 「終了」をクリックします。
ウィザードが閉じます。

クラウドへのアーカイブ

データの保存期間の終了が近づいたときに、古いデータのアーカイブを作成し、保存を延長することができます。データのアーカイブでは、常に、保存する場所が問題になります。Rapid Recovery では、多岐にわたるクラウドプロバイダにアーカイブを Core Console から直接アップロードできます。互換性のあるクラウドには、Microsoft Azure、Amazon™、Rackspace、および OpenStack ベースのすべてのプロバイダが含まれます。

Rapid Recovery を使用してアーカイブをクラウドにエクスポートするには、次の手順を実行します。

- ・ Rapid Recovery Core Console にクラウドアカウントを追加します。詳細については、「[クラウドアカウントの追加](#)」を参照してください。
- ・ データをアーカイブして、クラウドアカウントにエクスポートします。詳細については、「[アーカイブの作成](#)」を参照してください。
- ・ クラウドの場所にアーカイブされたデータをインポートして、取得します。詳細については、「[アーカイブのインポート](#)」を参照してください。

スケジュール設定されたアーカイブの編集

Rapid Recovery では、スケジュール設定されたアーカイブの詳細を変更できます。スケジュール設定されたアーカイブを編集するには、次の手順を実行します。

- 1 Rapid Recovery Core Console で、アイコンバーの  **詳細** ドロップダウンメニューをクリックし、**アーカイブ** を選択します。
- 2 アーカイブページで、変更するアーカイブの横にあるドロップダウンメニューをクリックし、**編集** をクリックします。
アーカイブを追加ウィザード が開きます。
- 3 アーカイブを追加ウィザードの **場所** ページで、**場所タイプ** ドロップダウンリストから、次のいずれかのオプションを選択します。
 - ・ ローカル
 - ・ ネットワーク
 - ・ クラウド
- 4 **手順 3** で選択した場所のタイプに基づき、次の表の説明に従ってアーカイブの詳細を入力します。

表 42. アーカイブの詳細

オプション	テキストボックス	説明
ローカル	場所	出力の場所を入力します。d:\work\archive などアーカイブを格納する場所のパスの定義のために使用されます。
ネットワーク	場所	出力の場所を入力します。\\servername\sharename などアーカイブを格納する場所のパスの定義のために使用されます。
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
クラウド	アカウント	ドロップダウンリストからアカウントを選択します。
		① メモ: クラウドアカウントを選択するには、先に、 Core Console にクラウドアカウントが追加されている必要があります。詳細については、「 クラウドアカウントの追加 」を参照してください。
	コンテナ	ドロップダウンメニューからアカウントに関連付けられているコンテナを選択します。
	フォルダ名	Rapid-Recovery-Archive-[作成日]-[作成時間] など、アーカイブデータを保存するフォルダ名を入力します。

- 5 「次へ」をクリックします。
- 6 ウィザードの **マシン** ページで、アーカイブするリカバリポイントが格納されている保護対象マシンを選択します。アーカイブしないマシンは、選択を解除します。
- 7 「次へ」をクリックします。
- 8 アーカイブを追加ウィザードの **スケジュール** ページで、**データを送信** ドロップダウンリストから、次のいずれかのオプションを選択します。
 - ・ 日次
 - ・ 週次
 - ・ 月次
- 9 **手順 8** での選択内容に基づき、次の表に従って、情報を入力します。

表 43. データ送信のオプション

オプション	テキストボックス	説明
日次	時間	日次アーカイブを作成する時間を選択します。
週次	曜日	アーカイブを自動的に作成する曜日を選択します。
	時間	日次アーカイブを作成する時間を選択します。
月次	日付	アーカイブを自動的に作成する日付を選択します。
	時間	日次アーカイブを作成する時間を選択します。

- 10 必要に応じて、アーカイブを延期して後で再開するには、**最初のアーカイブを一時停止** を選択します。
- ① **メモ:** アーカイブを再開する前にターゲットの場所を準備する時間が必要な場合は、スケジュールされたアーカイブを一時停止することをお勧めします。このオプションを選択しない場合は、スケジュールされた時間にアーカイブが開始されます。
- 11 「次へ」をクリックします。
- 12 **オプション** ページで、**リサイクルアクション** ドロップダウンリストを使用して、次の表で説明しているオプションのいずれかを選択します。

表 44. アーカイブリサイクルのオプション

テキストボックス	説明
Incremental (増分)	既存のアーカイブにリカバリポイントを追加できます。リカバリポイントを比較して、アーカイブに既に存在するデータの重複を回避します。
この Core を置換	この Core に関連する既存のアーカイブを上書きしますが、他の Core のデータはそのまま残します。
完全に消去	新しいアーカイブへの書き込みの前にディレクトリからすべてのアーカイブデータを消去します。

13 必要に応じて、**リカバリポイントチェーンの作成 (オフエンの修正)** を選択します。

14 「終了」をクリックします。

Rapid Recovery によりアーカイブに変更が適用されます。

スケジュール設定されたアーカイブの一時停止または再開

定期的に繰り返し実行されるアーカイブジョブがある場合は、必要に応じて、これを一時停止または再開することができます。

対象のアーカイブの場所の変更が必要になるなど、スケジュール設定されたアーカイブジョブの一時停止が必要になる場合があります。また、**アーカイブの作成**手順を実行したときに最初にアーカイブを一時停止するようにした場合は、その後、スケジュール設定されたアーカイブの再開が必要になります。スケジュール設定されたアーカイブを一時停止または再開するには、次の手順を実行します。

- 1 Rapid Recovery Core Console で、アイコンバーの  **詳細** メニューをクリックし、**アーカイブ** をクリックします。
- 2 **アーカイブ** ページのスケジュールされたアーカイブで、次のいずれかを実行します。
 - ・ 目的のアーカイブを選択して、必要に応じて、次のいずれかのアクションをクリックします。
 - ・ Pause
 - ・ Resume
 - ・ 目的のアーカイブの横にあるドロップダウンメニューをクリックし、必要に応じて、次のいずれかのアクションをクリックします。
 - ・ Pause
 - ・ Resume

アーカイブのステータスが「スケジュール」列に表示されます。

アーカイブジョブの強制実行

この手順を使用して、Rapid Recovery ではスケジュールされたアーカイブ上のアーカイブジョブをいつでも強制的に実行することができます。

アーカイブジョブを強制的に実行するには、Core 上にスケジュールされたアーカイブが必要です。

- 1 Rapid Recovery Core Console のアイコンバーで  **詳細** ドロップダウンをクリックし、**アーカイブ** を選択します。
 - 2 **アーカイブ** ページのスケジュールされたアーカイブで、強制的に実行するアーカイブの横にあるドロップダウンメニューをクリックし、**強制** をクリックします。
- Rapid Recovery は設定済みのアーカイブのスケジュールに関係なく、そのアーカイブに対して選択された設定に基づいてリカバリポイントをアーカイブします。

アーカイブのチェック

アーカイブをチェックすると、アーカイブとその内容が正常で、リカバリ可能であるかどうかを検証します。

アーカイブチェックを実行して、アーカイブ構造、データセグメント、インデックスファイルの整合性をスキャンすることができます。アーカイブチェックにより、アーカイブ内に必要なファイルがすべて存在することと、それらのファイルが正常であることを検証します。アーカイブのチェックを実行するには、次の手順を実行します。

- 
- Rapid Recovery Core Console で、アイコンバーの **詳細** ドロップダウンメニューをクリックし、**アーカイブ** を選択します。
 - アーカイブ** ページで **チェック** をクリックします。
Check Archive (アーカイブのチェック) ダイアログボックスが表示されます。
 - Location Type** (場所のタイプ) には、ドロップダウンリストから次のオプションのいずれかを選択します。
 - ローカル
 - ネットワーク
 - クラウド
 - 手順 3** で選択した場所のタイプに基づいて、次の表の説明に従ってアーカイブの詳細を入力します。

表 45. アーカイブの詳細

オプション	テキストボックス	説明
ローカル	場所	アーカイブのパスを入力します。
ネットワーク	場所	アーカイブのパスを入力します。
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
クラウド	アカウント	ドロップダウンリストからアカウントを選択します。
		① メモ: クラウドアカウントを選択するには、先に、Core Console にクラウドアカウントが追加されている必要があります。詳細については、「クラウドアカウントの追加」を参照してください。
	コンテナ	ドロップダウンメニューからアカウントに関連付けられているコンテナを選択します。
	フォルダ名	Rapid Recovery -5-Archive-[作成日]-[作成時間] など、アーカイブデータが保存されているフォルダを選択します。

- 5 次の表の説明に従って、チェックボックスをオンまたはオフにします。デフォルトでは、すべてがオンです。

① **メモ:** チェックボックスをすべてオフにはしないでください。少なくとも 1 つはオンにする必要があります。

オプション	説明
インデックスファイルのマッピングオフセット	このオプションでは、アーカイブの内部構造にあるデータがすべて、正しいロケーションにあるかどうかをチェックします。
構造整合性	このオプションでは、特定の内部ファイルの存在とアーカイブのフォルダ構造を検証します。いずれかのファイルまたはフォルダが存在しない場合は、チェックが失敗します。
チェックサム整合性	このオプションでは、アーカイブ内のデータセグメントの整合性をチェックし、セグメントが正常であることを確認します。

6 ファイルのチェック をクリックします。

Rapid Recovery が、選択したオプションに従ってアーカイブをチェックします。

アーカイブのアタッチ

アーカイブをアタッチすると、そのアーカイブからリカバリポイントを参照することができます。

この手順を完了するには、Rapid Recovery Core 6.0.1 以降で作成されたアーカイブが存在する必要があります。詳細については、「[アーカイブの作成](#)」を参照してください。

アーカイブをアタッチすると、指定したアーカイブ名が Core Console の左側のナビゲーションメニューにアーカイブメニューとして表示されます。そのアーカイブに含まれているリカバリポイントを持つ保護対象マシンが、それぞれアーカイブメニューの下にリストに個別に表示されます。アーカイブに含まれる任意のマシン名をクリックして、それらのリカバリポイントを参照することができます。また、お使いの Core に現在表示されているその他のリカバリポイントについても、同様のアクションを実行できます。

アーカイブをアタッチすると、その情報にアクセスするための資格情報もキャッシュされます。アタッチされているアーカイブ定義を削除するまで、簡単にアーカイブを再アタッチおよびデタッチして、そのリカバリポイントにアクセスしやすくなります。

アーカイブをアタッチするには、次の手順を実行します。

- 1 Rapid Recovery Core Console で  **アーカイブ** ▼ ドロップダウンメニューをクリックし、 **アーカイブのアタッチ** を選択します。

アーカイブのアタッチ ダイアログボックスが表示されます。

- 2 **名前** テキストボックスにアタッチするアーカイブの名前を入力します。
このフィールドに入力した値は、左側のナビゲーションメニューにアーカイブメニュー名として表示されます。

次の表示名のベストプラクティスに従って、アーカイブ名には 1～64 文字の英数字（スペースを含む）を指定します。「[禁止されている文字](#)」や「[禁止語](#)」は使用しないでください。

- 3 **場所のタイプ** ドロップダウンリストで、アーカイブの場所のタイプを次のオプションの中から選択します。
 - ・ ローカル
 - ・ ネットワーク
 - ・ クラウド
- 4 「[手順 3](#)」で選択した場所のタイプに基づき、次の表の説明に従ってアーカイブの詳細を入力します。

表 46. 場所のタイプの詳細

オプション	テキストボックス	説明
ローカル	場所	D:\Work\Archive など、アーカイブへのパスを入力します。
ネットワー ク	場所	\\servername\sharename など、アーカイブへのパスを入力します。
	ユーザー名	ネットワーク共有にログインするためのユーザー名を入力します。
	パスワード	ネットワーク共有にログインするためのパスワードを入力します。
クラウド	アカウント	ドロップダウンリストからアカウントを選択します。

① **メモ:** クラウドアカウントを選択するには、先に、**Core Console** にクラウドアカウントが追加されている必要があります。詳細については、「[クラウドアカウントの追加](#)」を参照してください。

オプション	テキストボックス	説明
	コンテナ	アカウントに関連付けられているアーカイブのコンテナをドロップダウンメニューから選択します。
	フォルダ名	Rapid-Recovery-Archive-[作成日]-[作成時間] など、アーカイブデータのフォルダ名を入力します。

5 **Attach** (連結) をクリックします。

アーカイブがこの Core にアタッチされて、コンテンツがファイルシステムとしてマウントされます。

アーカイブのインポート

この手順を使用して、アーカイブを一度にインポートするか、アーカイブを反復してをインポートするようにスケジュールできます。

アーカイブされたデータをリカバリするには、アーカイブ全体を指定の場所にインポートします。

△ 注意: 慎重に考慮した後にのみ、この手順を実行します。アーカイブのインポートは、アーカイブのコンテンツでリポジトリをリカバリし、アーカイブのキャプチャ以降に加えられた新しいデータを交換します。

アーカイブするには、次の手順のステップを完了します。

- 1 Rapid Recovery コアコンソールのメニューバーで、 **Archive (アーカイブ)** ドロップダウンメニューをクリックしてから **Import Archive (インポートアーカイブ)** を選択します。
Import Archive (アーカイブのインポート) ウィザードが開きます。
- 2 ウィザードの **Import Type (インポートの種類)** ページで、次のオプションのいずれかを選択します。
 - ・ One-time import (1 回のインポート)
 - ・ Continuous import (by schedule) ((スケジュールによる) 連続的インポート)
- 3 **次へ** をクリックします。
- 4 **Location (場所)** ページで、ドロップダウンリストからインポートするアーカイブの場所を選択し、次の表の説明に従って情報を入力します。

表 47. インポートしたアーカイブの場所のタイプのオプション

オプション	テキストボックス	説明
ローカル	場所	出力先を入力します。これは、アーカイブを格納する場所のパスを定義するために使用されます。たとえば、d:\work\archive などです。
ネットワーク	場所	出力先を入力します。これは、アーカイブを格納する場所のパスを定義するために使用されます。たとえば、\\servername\sharename などです。
	ユーザー名	ユーザー名を入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
クラウド	Account (アカウント)	ドロップダウンリストからアカウントを選択します。
	① メモ: クラウドアカウントを選択するには、最初にコアコンソールに追加しておく必要があります。詳細については、 クラウドアカウントの追加 を参照してください。	

オプション	テキストボックス	説明

Container (コンテナ)	ドロップダウンメニューからお使いのアカウント関連づけられているコンテナを選択します。

Folder Name (フォルダ名)	アーカイブされたデータを保存するフォルダの名前を入力します。

- 5 次へ をクリックします。
- 6 ウィザードの **Archive Information (アーカイブ情報)** ページで、アーカイブに含まれる各マシンをインポートする場合は、**Import all machines (すべてのマシンをインポート)** を選択します。
- 7 選択した内容に基づいて、次のオプションのいずれかを完了します。
 - ・ 手順 2 で **One-time import (1 回のインポート)** を選択し、ステップ 6 で **Import all machines (すべてのマシンのインポート)** を選択し、すべてのマシンが Core に保護され、レプリケートされたもの、あるいはリカバリポイントのみのマシンとして存在する場合、手順 12 に進みます。
 - ・ 手順 2 で **Continuous import (by schedule) ((スケジュールによる) 連続的インポート)** を選択し、手順 6 で **Import all machines (すべてのマシンのインポート)** を選択し、Core に少なくとも 1 つのマシンが存在せず、保護され、レプリケートされたもの、あるいはリカバリポイントのみのマシンとして存在しない場合、**Next (次へ)** をクリックしてから手順 9 に進みます。
 - ・ 手順 6 ですべてのマシンをインポートしなかった場合は、**Next (次へ)** をクリックして、手順 8 に進みます。
- 8 **Machines (マシン)** ページで、アーカイブからインポートするマシンを選択します。
 - ・ 手順 2 で **One-time import (1 回のインポート)** を選択し、Core に少なくとも 1 つのマシンが存在せず、保護された、レプリケートされたもの、またはリカバリポイントのみのマシンとして存在しない場合、ドロップダウンリストを使用して、インポートするマシンごとにリポジトリを選択して、手順 12 に進みます。
 - ・ Core にすべてのマシンがすでに存在し、保護され、レプリケートされたもの、またはリカバリポイントのみのマシンとして存在する場合、手順 12 へ進みます。
- 9 次へ をクリックします。
- 10 **Repository (リポジトリ)** ページで、次のオプションのいずれかを完了します。
 - ・ リポジトリが Core と関連付けられている場合、次の表のいずれかのオプションを選択します。

表 48. リポジトリオプション

オプション	説明
Use an existing Repository (既存のリポジトリを使用)	ドロップダウンリストから、このコアに現在関連付けられているリポジトリを選択します。
Create a Repository (リポジトリの作成)	Server (サーバ) テキストボックスに、たとえば、servername または localhost というように、新しいリポジトリに保存するサーバーの名前を入力してから、 DVM リポジトリの作成 を参照します。
Core に関連付けられているリポジトリがない場合は、たとえば、servername または localhost というように、新しいリポジトリに保存するサーバーの名前を入力してから、 DVM リポジトリの作成 を参照します。	

- 11 手順 2 で、**Continuous import (by schedule) ((スケジュールによる) 連続的インポート)** を選択した場合、**Schedule (スケジュール)** ページで、次の表で説明するオプションを選択します。

表 49. スケジュールインポートオプション

オプション	説明
毎日	時計のアイコンをクリックし、アーカイブジョブを開始する時間を上向きと下向きの矢印を使用して選択します。 12 時間システムを使用している場合は AM または PM ボタンをクリックして時刻を指定します。
毎週	アーカイブジョブを開始する曜日を選択してから、時刻を選択します。 12 時間システムを使用している場合は AM または PM ボタンをクリックして時刻を指定します。

オプション 説明

毎月	アーカイブジョブを開始する日付と時刻を選択します。 12 時間システムを使用している場合は AM または PM ボタンをクリックして時刻を指定します。
初期のインポートの一時停止	ウィザードを完了した後に、インポートジョブを次のスケジュール時間に開始したくない場合は、このオプションを選択します。 ① メモ: インポートを再開する前にターゲットの場所を準備する時間が必要な場合は、スケジュール済みのインポートを一時停止することができます。このオプションを選択しない場合は、スケジュールされた時間にインポートが開始されます。

12 **終了** をクリックします。

イベント

Rapid Recovery Core には、事前定義されたイベントセットが含まれます。これらのイベントは、管理者に対して Core の重大な不具合、またはバックアップ、仮想エクスポート、レプリケーションなどに関連するジョブの不具合を通知するために使用できます。

本項では、Rapid Recovery Core Console に表示されるイベントを確認する方法について説明します。また、電子メールによる通知の設定を含む、通知の方法や設定についても学習できます。最終的には、通知の設定でイベントログが保持される時間を変更したり、重複するイベント通知を減らしたりすることができます。

Rapid Recovery イベント

Rapid Recovery コアには、保護対象マシンの Core またはバックアップジョブでの重要な問題について管理者に通知するために使用できる事前定義されたイベントセットが含まれています。

- アラートをトリガーするイベントのタイプ、これらの通知（メール、トーストアラートなど）に対してシステムが使用する方法も、通知グループを設定することにより定義します。詳細については、[通知グループの設定](#) を参照してください。
- 管理者に電子メールを使用して通知を受信させる場合は、通知グループを設定するだけでなく、メールサーバーを設定し、電子メール通知テンプレートを設定する必要があります。詳細については、[電子メールサーバーの設定](#) および [電子メール通知テンプレートの設定](#) をそれぞれ参照してください。
- 繰り返しの削減機能を使用して、Events（イベント）ページに表示される同じタイプと範囲のイベントの数を減らすことができます。繰り返しの削減機能はデフォルトで有効です。この機能を無効にすることができます。イベントログにおける単一の表示と組み合わせられるイベントの時間をコントロールできます。詳細については、[繰り返し回数の削減の設定について](#) を参照してください。
- 長いイベントおよびジョブの履歴情報が、コアコンソールの Events（イベント）ページに保持される方法をコントロールできます。詳細については、[イベントの保持の設定](#) を参照してください。

タスク、アラート、およびジャーナルを使用したイベントの表示

Core Console からは、Core のイベントを表示でき、特定の保護対象マシンまたはレプリケートされたマシンのイベントを表示できます。

Core Console の **イベント** ページには、Rapid Recovery Core に関連するすべてのシステムイベントのログが表示されます。Core の

イベントにアクセスし、表示するには （イベント）をクリックします。

特定の保護対象マシンまたはレプリケートされたマシンの **イベント** ページには、特定のマシンに関連するイベントのログが表示されます。選択されたマシンのイベントにアクセスして表示するには、保護対象マシン メニューのマシン名をクリックし、マシンの **サマリ** ページから、**イベント** メニューをクリックします。

(Core または指定されたマシンの) イベント ページの内容は、タスク、アラート、およびジャーナルの 3 つのセクションに分かれています。これらの表示によって、さまざまなイベントについての詳細を適宜フィルタリングできます。

通知グループを設定することで、さまざまなイベントの通知方法を定義できます。詳細については、「[通知グループの設定](#)」を参照してください。

タスク、アラート、すべてのイベントのジャーナルをそれぞれ表示するには、次の手順を実行します。

- ・ [タスクの表示](#)
- ・ [アラートの表示](#)
- ・ [すべてのイベントの表示](#)

タスクの表示

タスクとは、定期的にスケジュールされたバックアップでのデータの転送、リカバリポイントからのリストアの実行など、Rapid Recovery Core で実行する必要があるジョブのことです。

実行中のタスクは、Core Console 上部の **実行中のタスク** ドロップダウンメニューに表示されます。実行中のタスクをクリックすると、アクティブタスクの監視 ダイアログボックスが表示されます。

また、Rapid Recovery Core のすべてのタスク、または特定のマシンに関連付けられたすべてのタスクを表示することもできます。

- 1 Rapid Recovery Core のすべてのタスクを表示するには、アイコンバーで  **イベント** をクリックします。
特定の保護対象マシンのタスクを表示する場合は、指定したマシンの **サマリ** ページに移動し、**イベント** メニューをクリックします。
- 2 タスクのみを表示するには、ページの左上隅で「**タスク**」をクリックします。これがデフォルトの表示です。
イベントのリストは、Core または選択したマシンのタスクのみを表示するようにフィルタされます。
- 3 必要に応じて、キーワード、開始日時、終了日時、またはその組み合わせでタスクのリストをフィルタするには、次の操作を実行します。
 - a キーワードでフィルタするには、**検索キーワード** テキストボックスにキーワードを入力します。
たとえば、「ロールアップ」、「アーカイブ」、または「転送」などのキーワードでフィルタできます。
 - b 開始日時でフィルタするには、次のいずれかのオプションを使用して、開始日時を入力します。
 - ・ **開始日時** テキストボックスに、MM/DD/YYYY HH:MM AM/PM の形式で日時を入力します。たとえば、2016 年 1 月 1 日午前 8 時から検索するには、1/1/2016 08:00 AM と入力します。
 - ・ 現在の日時を選択するには、 **カレンダー** ウィジェットを **開始日時** テキストボックスでクリックし、現在の日付をクリックします。現在の時刻が自動的に表示されます。
 - ・  **カレンダー** ウィジェットをクリックし、日付を選択したら、 **クロック** ウィジェットをクリックし、コントロールを使用して目的の時間を選択します。カレンダーから離れてクリックし、選択した変更を確定します。
 - c 同じ形式で終了日時も定義すると、表示されたタスクリストをさらに調整できます。
タスクリストは、選択した基準に基づいて直ちにフィルタされます。
- 4 必要に応じて、リストに表示されるタスクを次のようにフィルタできます。

オプション 説明



アクティブなタスクのみを表示するには、**アクティブなタスク** アイコンをクリックします。



実行用にキューに登録済みのタスクのみを表示するには、**キューに登録済みタスク** アイコンをクリックします。

オプション 説明



実行待ちのタスクのみを表示するには、**待機中のタスク** アイコンをクリックします。



完了済みのタスクのみを表示するには、**完了済みのタスク** アイコンをクリックします。

失敗したタスクのみを表示するには、**失敗したタスク** アイコンをクリックします。

- 5 タスクリストをエクスポートするには、リストから形式を選択し、 **エクスポート** をクリックします。結果のダイアログボックスでエクスポートを確認し、**OK** をクリックします。
次の形式を使用してエクスポートできます。

表 50. エクスポート形式

形式	説明
PDF	ポータブルドキュメントフォーマット（デフォルトのエクスポート形式）
HTML	Web ページ形式
CSV	カンマ区切り値
XLS	Microsoft Excel® 1997 ~ 2003 Workbook
XLSX	Excel Workbook

選択したタイプのファイルが Core サーバのデフォルトの場所にダウンロードされます。

- 6 任意のタスクの  **ジョブの詳細** アイコンをクリックすると、新しいウィンドウが開き、次の情報を含むタスクの詳細が表示されます。
- ・ ステータス
 - ・ 作業合計（サイズまたは完了率）
 - ・ 開始日時
 - ・ 終了日時
 - ・ レート
 - ・ 経過時間
 - ・ フェーズ（子タスクの場合）

アラートの表示

アラートとは、タスクまたはイベントに関係する通知のことです。アラートタイプには、エラー、警告、情報があります。

Rapid Recovery Core の重要なアラートのジャーナルを表示したり、特定のマシンに関連付けられた重要なアラートを表示したりすることができます。

- 1 Rapid Recovery Core のアラートを表示するには、アイコンバーで （イベント）をクリックし、**アラート** をクリックします。
特定の保護対象マシンで発生するアラートを表示するには、そのマシンの **サマリ** ページに移動し、**イベント** メニューをクリックして **アラート** をクリックします。

イベントのリストは、Core または選択したマシンの重要なアラートのみを表示するようにフィルタされます。

- 2 必要に応じて、開始日、終了日、アラートメッセージの説明、または任意の組み合わせで重要なアラートのリストをフィルタするには、次の手順を実行します。

- a 開始日時でフィルタするには、次のいずれかのオプションを使用して、開始日時を入力します。
 - ・ **開始日時** テキストボックスに、MM/DD/YYYY HH:MM AM/PM の形式で日時を入力します。たとえば、2016 年 1 月 1 日午前 8 時から検索するには、1/1/2016 08:00 AM と入力します。
 - ・ 現在の日時を選択するには、 **カレンダー** ウィジェット（**開始日時** テキストボックスにある）をクリックし、現在の日付をクリックします。現在の時刻は自動的に表示されます。
 - ・  **カレンダー** ウィジェットをクリックして日付を選択し、 **クロック** ウィジェットをクリックしてコントロールで目的の時間を選択します。カレンダーの外側をクリックし、選択した変更を受け入れます。
 - b アラートメッセージの説明でフィルタするには、**メッセージの検索** テキストボックスに説明を入力します。
たとえば、エージェントに関連したアラートのみを表示するには「エージェント」、転送に関連したアラートを表示するには「転送」、というように入力します。
 - c 表示されるアラートのリストをさらに絞り込むために、同じ形式で終了日時も定義できます。
アラートのリストは、選択した基準に基づいて直ちにフィルタされます。
- 3 必要に応じて、すべてのアラートを削除する場合は、「**すべて破棄**」を選択します。

すべてのイベントの表示

Rapid Recovery Core のすべてのイベントを表示したり、特定のマシンに関連付けられたすべてのイベントを表示したりすることができます。

- 1 Rapid Recovery Core のすべてのイベントのジャーナルを表示するには、アイコンバーで （イベント）をクリックして **ジャーナル** をクリックします。Rapid Recovery Core で発生するすべてのイベントを表示するには、Rapid Recovery Core の ホーム ページに移動し、（イベント）をクリックします。
特定の保護対象マシンで発生するすべてのイベントのジャーナルを表示するには、そのマシンの **サマリ** ページに移動し、**イベント** メニュー、**ジャーナル** を順にクリックします。
- 2 必要に応じて、開始日、終了日、アラートメッセージの説明、または任意の組み合わせですべてのイベントのリストをフィルタするには、次の手順を実行します。
 - a 開始日時でフィルタするには、次のいずれかのオプションを使用して、開始日時を入力します。
 - ・ **開始日時** テキストボックスに、MM/DD/YYYY HH:MM AM/PM の形式で日時を入力します。たとえば、2016 年 1 月 1 日午前 8 時から検索するには、1/1/2016 08:00 AM と入力します。
 - ・ 現在の日時を選択するには、 **カレンダー** ウィジェット（**開始日時** テキストボックスにある）をクリックし、現在の日付をクリックします。現在の時刻が自動的に表示されます。
 - ・  **カレンダー** ウィジェットをクリックして日付を選択し、 **クロック** ウィジェットをクリックしてコントロールで目的の時間を選択します。カレンダーの外側をクリックし、選択した変更を受け入れます。
 - b アラートメッセージの説明でフィルタするには、**メッセージの検索** テキストボックスに説明を入力します。
たとえば、エージェントに関連したアラートのみを表示するには「agent」、転送に関連したアラートを表示するには「transfer」、というように入力します。
 - c 表示されるイベントのリストをさらに絞り込むために、同じ形式で終了日時も定義できます。
イベントのリストは、選択した基準に基づいて直ちにフィルタされます。

電子メール通知を理解する

セットアップの Rapid Recovery コアを設定し、指定した電子メールアドレスに電子メールメッセージを送信することで、特定のイベントの通知を受信します。アラートをトリガーするイベントが他の通知方法として通知グループで定義されます。

- ① **メモ:** 通知方法として電子メールを使用しているかどうかに関係なく通知グループを確立する必要があります。詳細については、[通知グループの設定](#) を参照してください。

通知オプションのいずれかとして電子メールを選択した場合、メールの SMTP サーバーを設定する必要もあります。Rapid Recovery コアは、定義するサーバーを使用して、通知グループのパラメータに基づいてアラートを送信します。

さらに、電子メール通知テンプレートを定義する必要もあります。Core は、このテンプレートを使用して、それぞれのアラートの電子メールの件名と電子メールメッセージ本文のコンテンツを定義します。テンプレートにはデフォルト設定があります。デフォルトをそのまま使用することもできますが、テストして、必要に応じて修正を加えることもできます。

本項には以下のトピックがあります。

- ・ [電子メールサーバーの設定](#)
- ・ [電子メール通知テンプレートの設定](#)

電子メールサーバーの設定

電子メールサーバーを設定するには、次の手順を実行します。

- ① **メモ:** また、電子メールアラートメッセージが送信されるためには、電子メールで通知 オプションの有効化など、通知グループの設定を行う必要があります。電子メールアラートを受信するためのイベントの指定方法の詳細については、「[通知グループの設定](#)」を参照してください。

- 1 Rapid Recovery Core Console に移動します。

- 2 アイコンバーで  (設定) をクリックし、次のいずれかの操作を行います。
- ・ 設定ページの左側にある Core 設定のリストで **SMTP サーバ** をクリックします。
 - ・ 設定 ページの右側で、**SMTP サーバ** 見出しが表示されるまで下にスクロールします。

SMTP サーバの Core 設定が表示されます。

- 3 変更する設定をクリックします。
選択した設定が編集可能になります。
- 4 次の表の説明に従って、設定情報を入力します。

オプション 説明

SMTP サーバ	電子メール通知テンプレートで使用する電子メールサーバー名を入力します。命名規則にはホスト名、ドメイン、および接尾辞が含まれます (例: smtp.gmail.com)。
送信者	返信先の電子メールアドレスを入力します。電子メール通知テンプレートの返信先電子メールアドレスを指定するために使用されます (例: noreply@localhost.com)。
ユーザー名	電子メールサーバーのユーザー名を入力します。
パスワード	電子メールサーバーへのアクセスに必要なユーザー名に関連付けられているパスワードを入力します。
ポート	ポート番号を入力します。電子メールサーバーのポートの識別に使用します。例えば Gmail にはポート 587 です。 デフォルトは 25 です。
タイムアウト (秒)	電子メールサーバーへの接続を試行する時間を指定する整数値を入力します。これは、タイムアウトが発生する前の時間 (秒) を確立するために使用されます。 デフォルトは 60 秒です。
TLS	メールサーバーでセキュアな接続 (Transport Layer Security (TLS) や Secure Sockets Layer (SSL)) を使用する場合は、このオプションを選択します。

- 5 各設定の変更を完了したら、 をクリックして変更を保存し、編集モードを終了するか、 をクリックして、保存せずに編集モードを終了します。

△ | 注意: それぞれの変更を確認しなければ、設定は変更されません。

- 6 **テスト電子メールを送信** をクリックし、次の手順を実行します。
- a **テスト電子メールを送信** ダイアログボックスで、テストメッセージの宛先電子メールアドレスを入力し、**送信** をクリックします。

- b テストメッセージが正常に送信されない場合は、エラーダイアログボックスと **テスト電子メールを送信** ダイアログボックスを閉じ、電子メールサーバの設定を修正します。そして、テストメッセージをもう一度送信します。
- c テストメッセージに成功したら、「OK」をクリックして、成功した操作を確認します。
- d テストメールメッセージを送信した電子メールアカウントをチェックします。

電子メール通知テンプレートの設定

Rapid Recovery イベントのメールでの通知を有効にすると、デフォルトテンプレートがデフォルトで作成されます。Core 用に定義された SMTP 電子メールサーバがこのテンプレートを使用し、Rapid Recovery イベントに関する通知を電子メールで送信します。

このトピックでは、デフォルトの電子メール通知テンプレートの設定やコンテンツをカスタマイズするプロセスについて説明します。Restore Default（リストアデフォルト）オプションを使用して、いつでもデフォルトの通知テンプレートの変更をリストアできます。

注意: テンプレートは、ご自身の責任で変更してください。ユーザーは、テンプレートに加えられる修正をテストする責任があります。デフォルトのテンプレートのみがサポートされます。

電子メール通知テンプレートを設定するには、以下の手順を行います。

メモ: 電子メールサーバと、通知グループ設定を設定する必要もあります。これには、電子メールアラートメッセージが送信される前に、**Notify by email**（電子メールによる通知）オプションを有効化することも含まれます。アラートを送信するために電子メールサーバを設定する際の詳細情報については、[電子メールサーバの設定](#)を参照してください。電子メールアラートを受信するイベントを指定する際の詳細については、[通知グループの設定](#)を参照してください。

- 1 Rapid Recovery コアコンソールへ移動します。
- 2 アイコンバーで、（More（詳細））をクリックして、 **Notifications（通知）**を選択します。
Notifications（通知） ページが表示されます。
- 3 Email Settings（電子メール設定）ペインで、 **Change（変更）**をクリックします。
Edit Email Notification Configuration（電子メール通知設定の編集） ダイアログボックスが表示されます。
- 4 **E-メール通知を有効にする**を選択します。
電子メールテンプレートが有効で、表示されています。デフォルトの電子メールテンプレートの値は、次の手順で説明します。
- 5 Edit Email Notification Configuration（電子メール通知設定の編集）ダイアログボックスで、コンテンツを確認し、デフォルトのコンテンツがユーザーのニーズに合っているかを判断します。

オプション 説明

電子メールを有効にする この設定は、電子メール通知テンプレートを有効または無効に設定します。

- ・ 電子メール通知を有効にするには、このオプションを選択します。
- ・ 電子メール通知を無効にするには、このオプションをオフにします。

Email Subject（電子メールの件名） このテキストフィールドのコンテンツは、システムイベントの通知として送信される電子メールメッセージの件名をコントロールします。デフォルトの電子メールの件名の行は次のとおりです。

```
<hostName> <level>: <name> for <agentName>
```

Email（電子メール） このテキスト領域のコンテンツは、システムイベントの通知として送信される電子メールメッセージの本文をコントロールします。デフォルトの電子メール本文メッセージは次のとおりです。

```
<shortCompanyName> <coreProductName> on <hostName> has reported the <level> event "<name>"
```

```
Date/Time: <localTimestamp>
```

```
<message>
```

オプション 説明

```
<if(details.errorDetails)>
<details.ErrorDetails.Message>

<details.ErrorDetails.Details>
<endif>
---
```

About this event: <description>

<coreAdminUrl>

Send Test Email (テスト電子メールの送信)	このボタンをクリックすると、テスト電子メールメッセージが、 Send Test Email (テスト電子メールの送信) ダイアログボックスの結果指定される電子メールアドレスに送信されます。
Restore Defaults	このボタンをクリックすると、カスタマイズされたすべての変更が電子メールテンプレートから削除され、このテーブルに記載されるデフォルトコンテンツを使用して電子メールの件名および電子メールのフィールドがリストアされます。
OK	このボタンをクリックすると、Edit Email Notification Configuration (電子メール通知設定) ダイアログボックスの設定が確認され、保存されます。
キャンセル	このボタンをクリックすると、Edit Email Notification Configuration (電子メール通知設定) ダイアログボックスに加えられた変更がキャンセルされます。

- 6 電子メールテンプレートをカスタマイズするには、前述の手順で説明するテキストまたは変数を変更します。デフォルトで使われている変数を、次の表で説明します。

オプション	説明
hostName	Core no ホスト名
details	特定のイベントの詳細オブジェクトです。
agentName	イベントに単一の保護対象マシンの範囲がある場合は、このイベントに関連付けられた保護対象マシンの名前。
repositoryName	イベントにリポジトリの範囲がある場合は、このイベントに関連付けられたリポジトリの名前。
jobSummary	このイベントにジョブの範囲がある場合は、このイベントに関連付けられたジョブのサマリー。
remoteSlaveCoreName	イベントにターゲットコアの範囲がある場合は、このイベントに関連付けられたリモートターゲットコアの名前。
remoteMasterCoreName	イベントにソースコアの範囲がある場合は、このイベントに関連付けられたリモートソースコアの名前。
productName	Rapid Recovery コアという製品の名前。この製品名は、ブランディングの目的のためにホワイトラベルを使用して変更できます。
companyName	製品を販売する会社の名前。

- 7 **Email Subject (電子メールの件名)** テキストボックスには、電子メールテンプレートの件名を入力します。Email Subject (電子メールの件名) は、電子メール通知テンプレートの件名を定義するために使用されます。たとえば、<hostname> - <level> <name>といったようにです。
- 8 **Email (電子メール)** テキストボックスに、発生時にイベントを説明するテンプレートの本文の情報を入力し、重要度も入力します。
- 9 **Send Test Email (テスト電子メールの送信)** をクリックしてから、次の操作を行います
- Send Test Email (テスト電子メールの送信) ダイアログボックスで、テストメッセージ用の宛先電子メールアドレスを入力して **Send (送信)** をクリックします。
 - テストメッセージが失敗した場合は、エラーダイアログボックスと Send Test Email (テスト電子メールの送信) ダイアログボックスを終了して、**[OK]** をクリックして、現在の電子メールテンプレート設定を保存します。次に、手順 [電子メールサーバーの設定](#) に従ってお使いの電子メールサーバーの設定を変更します。そのメールアドレスのパスワードを再入力するようにします。これらの設定を保存し、この手順に戻ります。
 - テストメッセージが成功したら、**[OK]** をクリックし、正常に操作が行われたことを確認します。
 - テスト電子メールメッセージを送信するメールアドレスをチェックします。

テストの結果に満足したら、Edit Email Notification Configuration (電子メール通知設定の編集) ダイアログボックスに戻り、**OK** をクリックし、ダイアログボックスを閉じ、設定を保存します。

システムイベントの通知グループは、SMTP の設定、通知テンプレート

通知グループにより、ユーザーに警告を与える特定のイベントセットを定義し、通知がどのように行われるかを定義できます。通知グループを設定または編集する場合には、[通知グループの設定](#) を参照してください。

アラートを電子メールメッセージとして送信する場合は、簡易メール転送プロトコル (SMTP) サーバーも設定する必要があります。メールサーバーの設定方法の詳細については、[電子メールサーバーの設定](#) を参照してください。

イベントの通知を送信する場合、システムは電子メール通知を使用します。このテンプレートをカスタマイズすることができます。電子メール通知テンプレートの設定またはカスタマイズの詳細については、[電子メール通知テンプレートの設定](#) を参照してください。

通知グループの設定

① **メモ:** また、電子メールメッセージとしてアラートを送信する場合は、次の手順に従って、**SMTP (Simple Mail Transfer Protocol)** サーバーも設定する必要があります。**SMTP** サーバ設定の設定方法の詳細については、「[電子メールサーバーの設定](#)」を参照してください。

通知グループを使用すると、ユーザーにアラートを送信する特定のイベントセットや、通知方法を定義できます。送信されるアラートは、次の方法で設定できます。

- ・ 電子メール
- ・ Windows イベントログ
- ・ syslogd
- ・ トーストアラート
- ・ アラート
- ・ SNMP トラップ

異なる通知パラメーターを使用して複数の通知グループを設定することができます。

通知グループは、Core レベルまたは保護対象マシンレベルごとに管理できます。

アラートの通知グループを設定するには、次の手順を実行します。

1 次の手順のいずれかを実行します。

- ・ Core レベルで通知を設定するには、アイコンバーで  (詳細) をクリックし、**通知** を選択します。**通知** ページが表示されます。
- ・ 特定の保護対象マシンの通知を設定するには、次の操作を行います。
 - 1 保護対象マシンメニューで、通知を指定するマシンをクリックします。**カスタム通知グループ** ページが表示されます。
 - 2 保護対象マシンの サマリ ページの 詳細 ドロップダウンメニューで **通知** を選択します。**カスタム通知グループ** ページが表示されます。

2  **グループを追加** をクリックします。**通知グループを追加** ダイアログボックスが表示されます。

通知グループを使用すると、ユーザーにアラートを送信する特定のイベントセットや、通知方法を定義できます。送信されるアラートは、次の方法で設定できます。

通知グループを追加 ダイアログボックスには、一般的な説明の領域と 2 つのタブがあります。

- ・ アラートを有効化
- ・ 通知オプション

3 一般的な説明の領域で、次の表の説明に従って、通知グループの基本情報を入力します。

オプション	説明

名前	イベント通知グループの名前を入力します。この情報は必須です。

 **注意:** 通知グループ名として入力した値は、後で変更することができません。

説明	イベント通知グループの目的を明確に示す説明を入力します。この情報は任意です。

4 **アラートを有効化** タブで、次のように一連のシステムイベントを定義します。これらのイベントについて、ログが記録され、レポートが作成され、アラートが通知されます。

オプション	説明

すべてのアラート	すべてのイベントでアラートを作成するには、 All Alerts (すべてのアラート) を選択します。

エラー	エラーのアラートを作成するには、 タイプを選択 メニューで エラー をクリックします。これは、赤色の X で表されます。 

警告	警告のアラートを作成するには、 タイプを選択 メニューで 警告 をクリックします。これは、黄色の感嘆符アイコンで表されます。 

情報	情報メッセージのアラートを作成するには、 タイプを選択 メニューで 情報 をクリックします。これは、青色の i で表されます。 

デフォルトの復元	デフォルトのアラートタイプに戻すには、 タイプを選択 メニューで デフォルトにリストア をクリックします。これは、濃い青色の左矢印で表されます。 

5 特定のイベントタイプ (エラー、警告、または情報メッセージ) のアラートを作成するには、次の手順を実行します。

- すべてのアラート** オプションにアラートグループが表示されない場合は、すべてのアラートラベルの前の右山括弧 > 記号をクリックします。この記号が下矢印に変化し、ビューが展開されてグループが表示されます。
- 次に、特定のアラートグループの横にある右山括弧 > 記号をクリックし、グループ内の関連イベントを表示します。イベントグループのカテゴリには次のものがあります。

- ・ Archive
- ・ 自動レポート
- ・ アタッチ可否
- ・ 自動アップデート
- ・ バックアップリポジトリ
- ・ ブート CD
- ・ クラウド
- ・ クラスタ
- ・ Core サービス
- ・ データベース保持
- ・ 重複排除キャッシュ
- ・ DVM リポジトリ
- ・ Exchange
- ・ エクスポート
- ・ ジョブ
- ・ ライセンス
- ・ ローカルマウント
- ・ ログの切り捨て

- ・ メタデータ
 - ・ 夜間ジョブ
 - ・ 通知
 - ・ Core 状態の保持
 - ・ PowerShell Scripting
 - ・ 保護
 - ・ プッシュインストール
 - ・ リカバリポイントチェック
 - ・ リモートマウント
 - ・ リポジトリ共通
 - ・ レプリケーション
 - ・ リストア
 - ・ ロールアップ
 - ・ スケジュール設定されたアーカイブ
 - ・ セキュリティ
 - ・ サーバーログ
 - ・ vSphere
- ・ すべてのグループ内のすべてのイベントのアラートを定義するには、**すべてのアラート**のチェックボックスをオンにします。
 - ・ いずれかのグループ内のすべてのイベントのアラートを定義するには、そのグループの横にあるチェックボックスをオンにします。
 - ・ アラートグループ内の一部のアラートタイプのみを選択するには、グループを展開し、ログ、レポート、およびアラート設定の対象とする特定のイベントのみを選択します。

6 **通知オプション**タブをクリックします。

7 **通知オプション**タブで、通知プロセスの処理方法を指定します。

オプション	説明
電子メールで通知	電子メール通知の受信者を指定します。複数の電子メールアドレスや BCC や CC を指定できます。次を選択できます。 ・ To: ・ CC: ・ BCC:
Windows イベントログで通知	Windows イベントログを通してアラートを通知したい場合はこのオプションを選択します。
syslogd で通知	syslogd を通してアラートを通知したい場合はこのオプションを選択します。次のテキストボックスに syslogd の詳細を指定します。 ・ ホスト: ・ ポート:
トーストアラートで通知	画面の右下隅にポップアップとしてアラートを表示する場合は、このオプションを選択します。
アラートで通知	Core Console の右下隅にポップアップウィンドウとしてアラートを表示する場合は、このオプションを選択します。
SNMP トラップで通知	Rapid Recovery Core は、SNMP エージェントとして動作し、SNMP マネージャにトラップ（特定のイベントに関する通知）を送信します。その結果、アラート、リポジトリステータス、保護対象マシンなど、Core 情報が報告されます。このオプションは、Core イベントを SNMP トラップで通知する場合に選択します。また、トラップ番号も指定する必要があります。たとえば、Rapid Recovery Core で使用されるデフォルトのトラップ番号は 162 です。

8 「OK」をクリックします。

グループの作成後は、定義した通知グループ名を変更できないことを示すメッセージが表示されます。通知グループのその他のプロパティはいつでも変更できます。

- ・ グループ名が確定したら、このメッセージを確認して作業を保存します。
- ・ グループ名を変更する場合は、「いいえ」をクリックして、「通知グループを作成」ウィンドウに戻り、グループ名とその他の通知グループ設定をアップデートして、作業を保存します。

通知グループがサマリ表に表示されます。任意のパラメーターセットを使用して、さまざまな通知グループを作成することができます。

繰り返し回数の削減の設定について

重大な特定のイベントが発生した場合に管理者にアラートを送信する機能です。ただし、状況によっては、認識しているイベント通知を繰り返し受信することが不適切な場合もあります。環境障害のためにただちに把握する必要があるアラートが生成される場合でも、同じエラー状況によって膨大な量のイベントがイベントログに生成される可能性があります。イベントログでの繰り返しを削減し、Core Console の同じイベントに対して電子メール通知を繰り返し受信する不都合を軽減するため、Rapid Recovery には繰り返し回数の削減設定が含まれています。この設定は、デフォルトで有効になっており、5 分に設定されています。この設定を1分や60分に設定することができます。また、設定全体を無効にすることもできます。

繰り返し回数の削減が無効になっていると、タイプと範囲が同じイベントが発生するたびに、データベースにログ記録されます。そのイベントが以前に発生してから経過時間に関係なく、新しいイベントはすべて「イベント」タブの「アラート」部分に表示されます。

繰り返し回数の削減を有効にすると（例：デフォルトの5分を使用）、特定のイベントが初めて発生した時点でイベントデータベースにログ記録され、アラートログに表示されます。同じタイプと範囲の以降のイベントが、設定された時間のしきい値内で再びログ記録されると、しきい値内での繰り返しごとに、データベース内のイベント件数が1だけ増えます。ログにはイベントページのアラート部分が表示されます。ただし、イベントは直近の発生日時とともに一度だけ表示されます。初回発生時からの時間のしきい値が切れるまで、イベントログは同じイベントではアップデートされません。たとえば、5分に設定した場合にイベントが6分後にもう一度発生すると、イベントはログに表示され、別の電子メールを受信します。

繰り返し回数の削減の設定

イベントの繰り返しの削減を設定するには、以下の手順を行います。

- 1 Rapid Recovery Core Console に移動します。アイコンバーで、（詳細）をクリックし、**通知** を選択します。**通知** ページが表示されます。
- 2 繰り返しの削減 ペインで、既存の設定を表示します。
- 3 保存されたイベントしきい値の時間を有効化、無効化、または変更するには、 **変更** をクリックします。**繰り返しの削減の編集** ダイアログボックスが表示されます。
- 4 次の手順のいずれかを実行します。
 - ・ 繰り返し回数を無効にするには、**繰り返し回数を有効にする** オプションをクリアします。
 - ・ 繰り返し回数を有効にするには、**繰り返し回数を有効にする** オプションを選択します。
 - ・ 同一イベントの繰り返しの無視する時間しきい値（分単位）を変更するには、**__ 分** テキストボックスで、1~60 の範囲の数値を入力します。
- ① **メモ:** この値を変更するには、**繰り返し回数を有効にする** オプションが選択されている必要があります。
- 5 **OK** をクリックして設定を保存し、ダイアログボックスを閉じます。

イベントの保持の設定

Core 上で追跡されたイベントとジョブは、指定された期間だけ保存されます。デフォルト設定は 30 日です。この数字は、0 日から 3652 日（約 10 年間）までの範囲内で設定できます。

イベントの保持を設定するには、このプロセスの手順を完了してください。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで （設定）をクリックし、次のいずれかの操作を行います。
 - ・ 設定ページの左側にある Core 設定のリストで **データベース接続** をクリックします。
 - ・ 設定ページの右側で、**データベース接続** 見出しが表示されるまで下にスクロールします。データベース接続の設定が表示されます。
- 3 イベント情報がデータベースに保存される日数を変更するには、**保持期間（日）** テキストフィールドをクリックし、0~3652 のいずれかの値を入力して、 をクリックして変更を保存します。
イベントの保持期間が、指定したとおりに調整されます。

Rapid Appliance Self Recovery

Rapid Appliance Self Recovery（RASR）は、お使いのアプライアンスを動作状態に素早く復元できる、ベアメタルの復元プロセスです。

RASR は 2 つの復元のオプションを提供します。

- ・ 工場出荷時設定の復元
- ・ 障害発生時直前の状態にお使いのアプライアンスを回復（OS、構成、設定を復元）

RASR USB キーの作成

RASR USB キーを作成するには、次の手順を実行します。

- 1 **Appliance（アプライアンス）** タブへ移動します。
- 2 左ペインのナビゲーションを使用して **Appliance（アプライアンス） > Backup（バックアップ）** と選択します。
Create RASR USB Drive（RASR USB ドライブの作成） ウィンドウが表示されます。
- 3  **メモ:** 16 GB 以上の USB キーを挿入してから、RASR キーを作成します。
- 3 16 GB またはそれ以上の USB キーを挿入した後、**Create RASR USB Drive now（RASR USB ドライブを今すぐ作成）** をクリックします。
Prerequisite Check（前提条件チェック） メッセージが表示されます。
前提条件チェックの完了後、**Create the RASR USB Drive（RASR USB ドライブの作成）** ウィンドウに USB ドライブの作成に必要な最低限のサイズと **List of Possible target paths（可能なターゲットパスのリスト）** が表示されます。
- 4 ターゲットを選択し、**Create（作成）** をクリックします。
警告ダイアログボックスが表示されます。
- 5 **Yes（はい）** をクリックします。
RASR USB ドライブキーが作成されます。
- 6  **メモ:** USB キーの取り外し準備には、**Windows** のドライブ取り出し機能を使用するようにしてください。使用しなければ、USB キー内のコンテンツが破損する、または USB キーが期待通りに動作しない可能性があります。

各 DL アプライアンス、ラベル用に作成した RASR USB キーを取り外し、今後の使用のために保管します。

RASR の実行

① **メモ:** デルでは、アプライアンスをセットアップした後で RASR USB キーを作成することをお勧めします。RASR USB キーの作成については、「**RASR USB キーの作成**」の項を参照してください。

① **メモ:** RUU が最新でお使いのアプライアンスに到達可能であることを確認します。

① **メモ:** RASR を使用してシステムリカバリを実行するには、Dell.com/support/home で「*Recovering a Dell™ DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR)*」(*Rapid Appliance Self Recovery (RASR)* を使用した Dell™ DL Backup and Recovery Appliance のリカバリ) マニュアルを参照してください。

工場出荷時の状態にリセットするには、次の手順を実行します。

- 1 作成した RASR USB キーを挿入します。
- 2 アプライアンスを再起動して、**Boot Manager (F11)** (ブートマネージャ (F11)) を選択します。
- 3 **Boot Manager Main Menu** (ブートマネージャメインメニュー) で **One-shot BIOS Boot Menu** (ワンショット BIOS 起動メニュー) を選択します。
- 4 **Boot Manager Boot Menu** (ブートマネージャ起動メニュー) で、接続されている USB ドライブを選択します。
- 5 キーボードのレイアウトを選択します。
- 6 **Troubleshoot** (トラブルシューティング) > **Rapid Appliance Self Recovery** とクリックします。
- 7 ターゲットのオペレーティングシステム (OS) を選択します。
RASR が起動され、**welcome** (ようこそ) 画面が表示されます。
- 8 **Next** (次へ) をクリックします。
Prerequisites (前提条件) のチェック画面が表示されます。

① **メモ:** RASR を実行する前にすべてのハードウェア、およびその他の前提条件が満たされていることを確認します。

- 9 **Next** (次へ) をクリックします。
Recovery Mode Selection (リカバリモード選択) 画面に 3 つのオプションが表示されます。
 - ・ **System Recovery** (システムリカバリ)
 - ・ **Windows Recovery Wizard** (Windows リカバリウィザード)
 - ・ **Factory Reset** (工場出荷時の状態にリセット)
- 10 **Factory Reset** (工場出荷時の状態にリセット) オプションを選択します。
このオプションでは、工場出荷時のイメージからオペレーティングシステムのディスクを回復します。
- 11 **Next** (次へ) をクリックします。
This operation will recover the operating system. All OS disk data will be overwritten という警告メッセージがダイアログボックスに表示されます。
- 12 **Yes** (はい) をクリックします。
オペレーティングシステムのディスクの工場出荷時のリセット状態への復元が開始されます。
- 13 リカバリ処理が完了したら、**RASR Completed** (RASR が完了しました) ページが表示されます。**Finish** (終了) をクリックします。
- 14 復元後にシステムを起動します。
- 15 ① **メモ:** AppAssure アプライアンス設定ウィザードが表示された場合のみさらに続行します。それ以外は、手順 17 に進みます。
AppAssure アプライアンス設定ウィザードのロードを待ってから閉じる必要があります。Windows タスクマネージャを使用してウィザードを閉じます。
- 16 RUU パッケージの **launchRUU.exe** ファイルを実行します。指示に従ってオプションを選択し、RUU のインストールを続行して完了させます。

17 DL アプライアンス設定ウィザードが起動し、復元プロセスの残りの手順を案内します。

これでお使いのアプライアンスが正常に動作します。

Local Mount Utility

本項では、Windows ベースの Rapid Recovery Local Mount Utility (LMU) を使用して、リカバリポイントをマウントし、Rapid Recovery Core をホストしていないマシンを使用してファイルレベルからコンテンツを検索する方法について説明します。

Local Mount Utility について

LMU は、ダウンロード可能な Windows ベースのアプリケーションで、任意の Windows マシン上で 3 つの使用可能なモードのいずれかを使用して Rapid Recovery リカバリポイントをマウントできます。この軽量のユーティリティは、32 ビットおよび 64 ビットの Windows オペレーティングシステムにインストールすることができ、rapidrecovery-vdisk (以前の aavdisk) と aavstor ドライバを含んでいますが、サービスとして実行されません。ユーティリティをインストールすると、デフォルトで **C:\Program Files\AppRecovery\Local Mount Utility** ディレクトリにインストールされ、ショートカットがマシンのデスクトップに作成されます。

LMU は Rapid Recovery Core マシンへのリモートアクセス用に設計されたものですが、Rapid Recovery Core と同じマシン上に LMU をインストールすることもできます。Core 上で LMU を実行すると、Rapid Recovery Core Console から実行されたマウントを含む、その Core のすべてのマウントが認識され表示されます。同様に、LMU で実行されたマウントも Core Console 内に表示されます。

LMU が Mailbox Restore と同じマシン上にインストールされているときには、Exchange データベースを開いたときに LMU が Mailbox Restore を自動的に起動します。Mailbox Restore は、Microsoft Exchange データストアとアイテムをリストアするために使用される Dell Rapid Recovery アプリケーションです。Mailbox Restore は、LMU または Rapid Recovery Core のインストール時にインストールすることができます。Mailbox Restore の詳細については、『*Dell Data Protection | Rapid Recovery Mailbox Restore for Microsoft Exchange ユーザーガイド*』を参照してください。

① **メモ:** Linux マシンは、コマンドラインユーティリティ **local_mount** を使用して、保護対象マシンの **Core** およびそれに対応するリカバリポイントを照会します。同様に、このツールを使用すると、ユーザーが、リモートからのリカバリポイントボリュームのマウント、ファイルレベルでのボリュームコンテンツの検索、リカバリポイントからの個別のファイルまたはボリューム全体（システムボリュームの **BMR** を含む）のリストアを実行できます。詳細については、それぞれ「**Linux マシンでのリカバリポイントボリュームのマウント**」、「**コマンドラインを使用した Linux マシンのボリュームのリストア**」、および「**Linux マシンでの Bare Metal Restore の実行**」を参照してください。

Local Mount Utility での Rapid Recovery Core マシンの操作

Local Mount Utility (LMU) を使用すると、制限のない数の Core マシンをローカルまたはリモートで操作できます。LMU を Rapid Recovery Core マシンにインストールする場合、そのマシンは LMU で自動的にローカルホストとして表示されます。すべての追加のリモート Core は、それらを追加したときに入力した情報に応じてマシン名または IP アドレスとして表示されます。LMU を使用して、Core マシンを追加、編集および削除できます。詳細については、次の手順を参照してください。

関連するリンク

- [Local Mount Utility への Core マシンの追加](#)
- [Local Mount Utility オプションの変更](#)
- [Local Mount Utility での Core の接続設定の編集](#)
- [Core への再接続](#)
- [Local Mount Utility からの Rapid Recovery Core マシンの削除](#)

Local Mount Utility への Core マシンの追加

リカバリポイントをマウントするには、LMU に Core マシンを追加する必要があります。追加可能な Core の数に制限はありません。

Core を追加して LMU をセットアップするには、次の手順を実行します。

- 1 LMU がインストールされているマシンから、デスクトップアイコンをダブルクリックして LMU を起動します。
- 2 次の手順のいずれかを実行します。
 - ・ Local Mount Utility メニューの左上隅で、**Core の追加** をクリックします。
 - ・ 左側のパネルでブランクスペースを右クリックし、**Core の追加** をクリックします。

フォルダの追加 ダイアログボックスが表示されます。

- 3 **Core の追加** ダイアログボックスで、次の表の説明に従って、要求された資格情報を入力します。

表 51. Rapid Recovery Core の資格情報

オプション	説明
ホスト名	リカバリポイントのマウント元である Core の名前または IP アドレス。 ① メモ: Rapid Recovery Core マシンに LMU をインストールしている場合、LMU は自動的に localhost マシンを追加します。
ポート	Core と通信するために使用されるポート番号。 デフォルトポート番号は 8006 です。
自分の Windows ユーザー資格情報を使用します	Core にアクセスするために使用する資格情報が Windows 資格情報と同じである場合は、このオプションを選択します。
特定の資格情報を使用してください	Core にアクセスするために使用する資格情報が Windows 資格情報と異なる場合は、このオプションを選択します。
ユーザー名	Core マシンにアクセスするために使用するユーザー名。 ① メモ: 特定の資格情報を使用することを選択した場合のみ、このオプションを使用できます。
パスワード	Core マシンにアクセスするために使用するパスワード。 ① メモ: 特定の資格情報を使用することを選択した場合のみ、このオプションを使用できます。

- 4 「**接続**」をクリックします。
- 5 複数の Core を追加する場合は、必要に応じて手順を繰り返します。

Local Mount Utility オプションの変更

LMU に接続されているすべての Rapid Recovery Core のオプションを変更するには、以下の手順を実行します。

- 1 Local Mount Utility ユーザーインターフェースで、**オプション** をクリックします。
- 2 **オプション** ダイアログボックスで、次の表の説明に従って設定を変更できます。

表 52. Core 設定

オプション	説明
デフォルトのマウントポイントリポジトリ	参照 ボタンを使用するか、またはリカバリポイントのマウントに使用する場所へのパスを入力します。
自分の Windows ユーザーアカウント資格情報を使用します	Core にログインしたときに、Windows 資格情報をデフォルトで常に使用するには、このオプションを選択します。
特定の資格情報を使用してください	接続されている各 Core に以下の資格情報を使用するには、このオプションを選択します。 ・ ユーザー名：すべての Core を使用するユーザー名を入力します。 ・ パスワード：すべての Core で使用するパスワードを入力します。
Core 接続タイムアウト (秒)	接続がタイムアウトになる前に、LMU が Core に接続するための試行を続行する時間の長さを入力します (分：秒：ミリ秒の形式)。
言語	LMU を表示する言語を選択します。次のいずれかのオプションを選択できます。 ・ English (英語) ・ フランス語 ・ ドイツ語 ・ ポルトガル語 ・ スペイン語 ・ 簡体字中国語 ・ 日本語 ・ Korean (韓国語)

Local Mount Utility での Core の接続設定の編集

Core を LMU に追加した際に確立した設定を編集するには、次の手順を実行します。

① **メモ**: この手順は **localhost Core** には適用されません。リモート **Core** のマシンにのみ適用されます。

- 1 Local Mount Utility のユーザーインターフェースで、設定を編集する Core を右クリックし、**Core の編集** をクリックします。
- 2 **Core の編集** ダイアログ ボックスで、次の表に説明されている設定を変更できます。

表 53. Core 設定

オプション	説明
ホスト名	リカバリポイントのマウント元である Core の名前。
	① メモ : Rapid Recovery Core マシンに LMU をインストールしている場合、LMU は自動的に localhost マシンを追加します。
ポート	Core と通信するために使用されるポート番号。 デフォルトポート番号は 8006 です。
自分の Windows ユーザー資格情報を使用します	Core にアクセスするために使用する資格情報が Windows 資格情報と同じである場合は、このオプションを選択します。

オプション	説明
特定の資格情報を使用してください	Core にアクセスするために使用する資格情報が Windows 資格情報と異なる場合は、このオプションを選択します。
ユーザー名	Core マシンにアクセスするために使用するユーザー名。  メモ: 特定の資格情報を使用することを選択した場合のみ、このオプションを使用できます。
パスワード	Core マシンにアクセスするために使用するパスワード。  メモ: 特定の資格情報を使用することを選択した場合のみ、このオプションを使用できます。

3 変更を行った後、**OK** をクリックします。

Core への再接続

Rapid Recovery Core マシンへの接続が切断された場合は、次の手順を実行して接続を更新することができます。

Local Mount Utility のユーザーインターフェースで、次のいずれかの操作を行います。

- Core がオフラインになっている場合は、接続を再確立する Core をダブルクリックします。
LMU が Core との接続の再確立を試みます。
- Core がオンラインになっている場合は、Core を右クリックし、Core への再接続をクリックします。
LMU で接続が更新されます。

Local Mount Utility からの Rapid Recovery Core マシンの削除

LMU から Core を削除するには、次の手順を実行します。

 **メモ:** このオプションは、**localhost** に配置され、**localhost** とラベル付けされている **Rapid Recovery Core** では使用できません。

- Local Mount Utility のユーザーインターフェースで、削除する Core を右クリックし、**Core の削除** をクリックします。
- コマンドを確認するには、ダイアログボックスで **はい** をクリックします。
LMU によって Core とその保護対象マシンがナビゲーションツリーから削除されます。

Local Mount Utility での保護対象マシンの操作

Local Mount Utility (LMU) を使用して、マシンに関連付けられている Rapid Recovery Core Console にログインせずに、保護対象マシンのリカバリポイントをマウントおよび参照できます。詳細については、次の手順を参照してください。

- Local Mount Utility を使用したリカバリポイントのマウント
- Local Mount Utility を使用したマウント済みリカバリポイントの検索
- リカバリポイントの更新
- Local Mount Utility を使用した個々のリカバリポイントのマウント解除
- 1 つの Rapid Recovery Core または保護対象マシンからのすべてのリカバリポイントのマウント解除
- Local Mount Utility を使用したすべてのマウント済みリカバリポイントのマウント解除

Local Mount Utility を使用したリカバリポイントのマウント

LMU では、保護対象マシン、レプリケートされたマシン、およびリカバリポイントのみのマシンなど、接続されている Core マシンに関連付けられたリカバリポイントをマウントすることができます。

リカバリポイントをマウントする前に、リカバリポイントが保存されている Core に Local Mount Utility (LMU) を接続する必要があります。手順 [Local Mount Utility への Core マシンの追加](#) に記載されているとおり、LMU に追加できる Core の数は無制限ですが、アプリケーションが一度に接続できる Core は1つのみです。たとえば、1つの Core によって保護されているマシンのリカバリポイントをマウントしたあとに、別の Core に保護されているマシンのリカバリポイントをマウントする場合、LMU は最初の Core との接続を自動的に切断し、2 つ目の Core との接続を確立します。

- 1 Local Mount Utility ユーザーインターフェースから、ナビゲーションツリーで Core を展開して、保護対象マシンを表示します。
- 2 ナビゲーションツリーから、リカバリポイントのマウント元であるマシンを選択します。
リカバリポイントがメインフレーム内に表示されます。
- 3 必要に応じて、マウントするリカバリポイントを展開して、個々のディスクのボリュームまたはデータベースを表示します。
- 4 マウントするリカバリポイントを右クリックして、次のいずれかを選択します。

オプション	説明
マウント	このオプションを使用すると、読み取り専用としてリカバリポイントをマウントすることができます。
書き込み可能でマウント	このオプションを使用すると、マウントされたリカバリポイントを変更することができます。
以前の書き込みとともに読み取り専用でマウント	このオプションでは、リカバリポイントを読み取り専用としてマウントし、以前に行われた変更が含まれます。
高度なマウント...	このオプションでは、高度なマウント ダイアログボックスが開きます。

- 5 高度なマウント を選択した場合は、次の表に説明されているオプションを完了します。

表 54. 「高度なマウント」のオプション

オプション	説明
マウントポイントのパス	参照 をクリックして、デフォルトマウントポイントのパス以外のリカバリポイントのパスを選択するか、または手動で優先パスを入力します。
マウントタイプ	次のオプションのいずれかを選択します。 ・ 読み取り専用でマウント ・ 書き込み可能でマウント ・ 以前の書き込みとともに読み取り専用でマウント 各オプションの説明については、 手順 4 を参照してください。

- ・ 「マウント」をクリックします。
マウントされたリカバリポイントを含むフォルダを自動的に開きます。

① **メモ:** 既にマウントされているリカバリポイントを選択すると、マウント中 ダイアログボックスでリカバリポイントをマウント解除するかどうかを尋ねるプロンプトが表示されます。

Local Mount Utility を使用したマウント済みリカバリポイントの検索

リカバリポイントを検索すると、Windows エクスプローラ ウィンドウでバックアップされたデータが開き、リカバリ対象のアイテム（複数可）のボリュームとフォルダを検索できます。

Windows エクスプローラなどのファイルマネージャーを使用して（またはプログラムによっては Windows API を使用して）優先場所にコピーすることでアイテムを回復することができます。現在マウントされているリカバリポイントを検索するには、次の手順を実行します。

① **メモ:** リカバリポイントをマウントした後すぐに検索する場合、マウント手順が完了したときにリカバリポイントを含むフォルダが自動的に開くため、この手順は必要ありません。

- 1 Local Mount Utility ユーザーインターフェースで、**アクティブなマウント** をクリックします。
「アクティブなマウント」ウィンドウが開き、マウントされたすべてのリカバリポイントが表示されます。
- 2 ナビゲーションツリーを展開すると、各マシンにマウントされたリカバリポイントとそのボリュームが表示されます。

- 3 検索するボリュームの横にある **エクスプローラ** をクリックします。

リカバリポイントの更新

LUM は、Core および保護対象マシンからリアルタイムで更新を受信しません。保護対象マシンを更新し、最新のリカバリポイントを表示するには、次の手順を実行します。

Local Mount Utility のユーザーインターフェースから、更新する保護対象マシンを右クリックし、リカバリポイントを更新します。

Local Mount Utility を使用した個々のリカバリポイントのマウント解除

LMU を使用してリモート Core 上のリカバリポイントをマウント解除するには、次の手順を実行します。

- 1 Local Mount Utility ユーザーインターフェースで、**アクティブなマウント** をクリックします。
アクティブなマウント ウィンドウが開き、マウントされたすべてのリカバリポイントが表示されます。
- 2 **アクティブなマウント** ウィンドウで、オプションとして、プラスアイコンまたはマイナスアイコンをクリックして、マウントされたリカバリポイントごとにボリュームの表示を展開または折りたたむことができます。
- 3 **アクティブなマウント** ウィンドウで、マウント解除する各リカバリポイントまたはボリュームの横にある **マウント解除** をクリックします。
選択したリカバリポイントがマウント解除されると、進行状況ウィンドウが表示されます。
- 4 **アクティブなマウント** ウィンドウの右上部にある **x** をクリックし、ウィンドウを閉じて LMU に戻ります。

1 つの Rapid Recovery Core または保護対象マシンからのすべてのリカバリポイントのマウント解除

1 つの Core または保護対象マシンからマウントされているリカバリポイントのみをマウント解除するには、次の手順を実行します。

- 1 Local Mount Utility ユーザーインターフェースで、次のいずれかの手順を実行します。
 - ・ すべてのリカバリポイントをマウント解除する Core を右クリックします。
 - ・ すべてのリカバリポイントをマウント解除する保護対象マシンを右クリックします。
- 2 **[machine_name] のすべてをマウント解除** をクリックします。
- 3 コマンドを確認するには、ダイアログボックスで、**はい** をクリックします。

① **メモ:** 既存のマウントを使用しているアクティブなタスクがある場合は、それらのマウントをマウント解除するとタスクが失敗します。

選択した項目のすべてのマウントされているリカバリポイントがマウント解除されます。

Local Mount Utility を使用したすべてのマウント済みリカバリポイントのマウント解除

LMU ですべてのリカバリポイントを同時にマウント解除する主な方法が 2 つあります。どのリカバリポイントが現在マウントされているかを表示せずに、すべてのリカバリポイントをマウント解除することができます。または現在マウントされているすべてのリカバリポイントを表示してから、それらをすべてマウント解除することができます。それぞれの関連する手順を参照してください。

すべてのマウントを解除ボタンを使用したすべてのリカバリポイントのマウント解除

次の手順を実行して、マウントされているすべてのリカバリポイントを一度にマウント解除します。

- 1 ローカルマウントユーティリティメニューで、**すべてのマウントを解除**をクリックします。
- 2 コマンドを確認するには、ダイアログボックスで、**はい**をクリックします。

① **メモ:** 既存のマウントを使用しているアクティブなタスクがある場合は、それらのマウントをマウント解除するとタスクが失敗します。

アクティブなマウント ウィンドウを使用したすべてのリカバリポイントのマウント解除

アクティブなマウント ウィンドウからすべてのマウントされているリカバリポイントを1回のみマウント解除するには、次の手順を実行します。

- 1 Local Mount Utility ユーザーインターフェースで、**アクティブなマウント**をクリックします。
- 2 **アクティブなマウント ウィンドウ**で、**すべてをマウント解除**をクリックします。
- 3 コマンドを確認するには、ウィンドウで、**はい**をクリックします。
- 4 **アクティブなマウント ウィンドウ**で、**閉じる**をクリックします。

Local Mount Utility のトレイメニューの使用

LMU トレイメニューはデスクトップのタスクバーにあります。アイコンを右クリックして、次の表で説明されているオプションを表示します。

表 55. トレイメニューオプション

オプション	説明
リカバリポイントの参照	LMU メインウィンドウを開きます。
アクティブなマウント	LMU メインウィンドウの上部で「アクティブなマウント」ダイアログボックスを開きます。
オプション	LMU メインウィンドウの上部で「オプション」ダイアログボックスを開きます。オプション ダイアログボックスでは、LMU ユーザーインターフェースのデフォルトのマウントポイントディレクトリとデフォルトの Core 資格情報を変更できます。
バージョン情報	Local Mount Utility のライセンス情報を表示します。
終了	LMU アプリケーションを閉じます。

アプライアンスの管理

Core Console には **Appliance** (アプライアンス) タブがあります。このタブを使用して、容量のプロビジョニング、アプライアンスの状態の監視、および管理ツールへのアクセスを行うことができます。

トピック：

- ・ アプライアンスのステータスの監視
- ・ Windows のバックアップ
- ・ ストレージのプロビジョニング
- ・ 仮想ディスク用の容量割り当ての削除
- ・ Recovery and Update Utility

アプライアンスのステータスの監視

アプライアンスサブシステムのステータスは、**Appliance > Health** (アプライアンス正常性) ページを使用して監視できます。**Health (正常性)** ページには、ステータスライト (各サブシステムの横にある) とサブシステムの正常性を示すステータスの説明が表示されます。

Health (正常性) ページには、ツールへのリンクも提供され、ドリルダウンすると各サブシステムの詳細が表示されます。これらは警告またはエラーのトラブルシューティングを行う際に役立つことがあります。**Provisioning Status (プロビジョニングステータス)** リンクは、Storage Provisioning サブシステムで利用できるもので、**Provisioning (プロビジョニング)** 画面が開き、サブシステムのプロビジョニングステータスを表示します。**Rapid Appliance Self Recovery (アプライアンスの迅速なセルフ回復)** リンクは、Rapid Appliance Self Recovery サブシステムで利用できるもので、**Backup (バックアップ)** ページを開き、そこで RASR USB キーを作成し、Windows バックアップステータスを監視し、Windows のバックアップポリシーを設定できます。VM Management (VM 管理) リンクは、**Virtual Standby (仮想スタンバイ)** ページを開き、そこで仮想マシンを管理することができます。**Server Administrator (サーバー管理者)** リンクは、Storage Hardware サブシステムで利用できるもので、正常性ページを開き、そこでコントローラ、エンクロージャ、物理ドライブなどの正常性を分析できます。**Controllers (コントローラ)** リンクは、Appliance Hardware で利用できるもので、**Controllers (コントローラ)** ページを開き、コントローラに関連付けられるコントローラと物理ドライブの詳細を表示します。

Windows のバックアップ

Windows のバックアップ機能は DL 1000 以外のすべての DL フレーバで使用できます。**Appliance > Backup** (アプライアンスバックアップ) タブにより、Windows のバックアップポリシーを設定し、最後のバックアップのステータスを表示し、以前にバックアップしたアイテムも表示することができます。この Windows バックアップ機能を使用するには、Windows バックアップ仮想ディスクが存在している必要があります。

- ・ お使いのアプライアンスを最新の RUU (3.0.x) でアップグレードした後、(AppAssure 環境で作成された) Windows バックアップ仮想ディスクが存在しない場合は、DL Appliance Configuration (DL アプライアンス構成) ウィザードを完了した後に、Windows Backup 仮想ディスクが作成されます。Windows バックアップ仮想ディスクが存在しない場合は、**Windows Backup Policy (Windows のバックアップポリシー)** セクションの **Backup (バックアップ)** ページの下にある **+ Create WinBackups VD (+ WinBackups VD の作成)** をクリックします。DL 4000 および DL 4300 では 295 GB のサイズの仮想ディスクが作成され、DL1300

では 210 GB のサイズの仮想ディスクが作成されます。



- ・ 最新の RUU でアプライアンスをアップグレードした後、AppAssure 環境で作成した Windows バックアップ仮想ディスクが存在する場合、次の手順を実行し、RR 環境で Windows バックアップ仮想ディスクを作成します。
 - a **ApplianceProvisioningConfiguration.xml** を編集します（このファイルは各ボリュームのルートにあるため、一度だけ編集し、必要に応じてコピーすることができます）。
 - △ | **注意:** 既存の Windows バックアップ仮想ディスクを削除しないでください。
 - 1 <BackupVolumes> タグの間のテキストをすべて削除します。
 - 2 </BackupVolumes> タグを削除します。
 - 3 <BackupVolumes> タグを <Backupvolume/> になるように編集します。
 - 4 保存して閉じます。
 - b コアコンソールに移動します。
 - c をクリックして **Appliance > RASR**（アプライアンス RASR）タブをクリックします。
 - d **Create Windows Backup volume（Windows バックアップボリュームを作成）** ボタンをクリックします。
 - e 空き領域が充分にある場合は、Windows バックアップ仮想ディスクが作成されます。

① **メモ:** Windows バックアップは、任意の場所に Windows Server バックアップ機能およびストアバックアップを使用して設定することもできますが、この場合は、RASR ページにエラーが表示されます。RASR を使用してリストアを一貫して実行する場合、バックアップが制御できず、保証されないからです。

バックアップステータス

Microsoft Windows バックアップステータスは、**Last Backup（最後のバックアップ）** タブ下に表示されます。バックアップが現在実行されている場合、その情報は、**Current Backup（現在のバックアップ）** タブ下に表示されます。最後のバックアップを表示するには、次の手順を実行します。

- 1 コアコンソールで、**Appliance（アプライアンス） > Backup（バックアップ）** タブに移動します。
- 2 **Status（ステータス）** ボタンの横の矢印をクリックして、バックアップのステータスを表示します。
- 3 **Last Backup（最後のバックアップ）** ペインに、次の情報が表示されます。
 - ・ ステータス
 - ・ State（状態）
 - ・ Backup Location（バックアップの場所）
 - ・ 開始時刻
 - ・ 終了時刻
 - ・ Error Description（エラーの内容）
 - ・ Items that were backed up（バックアップされたアイテム）

① **メモ:** 上記の情報は、Windows のバックアップポリシーが実行されたかどうかに関係なく表示されます。

Backup Status	
Last Backup	
Status:	● (Completed successfully)
Backup Location:	F:
Start Time:	8/16/2016 7:34:00 PM
End Time:	8/16/2016 7:39:00 PM
Error Description:	
Error Action:	
Items Backed Up	
State	Name
1	VolumeList
1	SystemState
1	BareMetalRecovery

バックアップが実行されている場合は、**Current Backup Progress**（現在のバックアップ進捗状況）と **Start Time**（開始時間）に関する情報が表示されます。

Windows バックアップポリシー

Windows バックアップポリシーを設定するには、次の手順を実行します。

- 1 コアコンソールで、**Appliance > Backup**（アプライアンス > バックアップ）に移動します。
- 2 **Configure Policy**（ポリシーの設定）ボタンをクリックします。

Windows Backup Policy（Windows バックアップポリシー）ウィンドウが表示されます。

- 3 以下に示すようにパラメータを入力します。

テキストボックス 説明

- 以下のアイテムがバックアップされます。
- ・ OS ボリューム
 - ・ リカバリパーティション
 - ・ ベアメタルリカバリのバイナリ

上記のすべてのアイテムがデフォルトで選択されます。

Perform backup（バックアップを実行します） Winbackup が実行される頻度を選択します。毎日、毎週、毎月のオプションがあります。

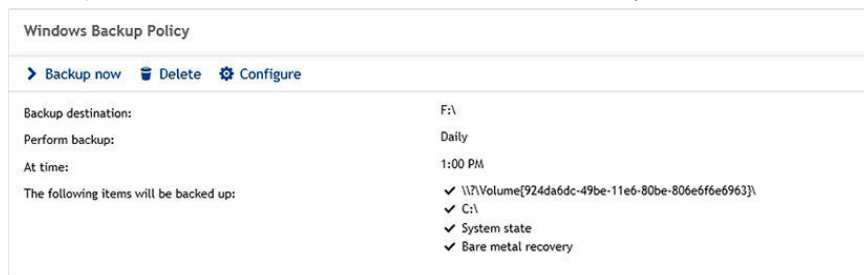
テキストボックス 説明

バックアップをスケジュールする時間をスケジュールする時間を選択してください。

4 **Configure** (設定) をクリックします。

Winbackup ポリシーが設定され、詳細が **Windows Backup Policy (Windows のバックアップポリシー)** セクションに表示されます。

設定されたら、**Backup now (今すぐバックアップ)** オプションを使用し、任意のインスタントで選択したアイテムをバックアップを行う選択を行い、**Windows Backup Policy (Windows のバックアップポリシー)** セクションの **Delete policy (ポリシーの削除)** を使用し、バックアップポリシーを削除する選択を行えます。



Windows Backup Policy

Backup destination: F:\

Perform backup: Daily

At time: 1:00 PM

The following items will be backed up:

- ✓ \\?\Volume{924da6dc-49be-11e6-80be-806e6f6e6963}\
- ✓ C:\
- ✓ System state
- ✓ Bare metal recovery

ストレージのプロビジョニング

アプライアンスは、使用可能な内部ストレージ、および接続されている対応外部ストレージエンクロージャのすべてを次のために設定します。

- ・ リポジトリ
- ・ スタンバイ VM、またはその他の目的のためのディスクボリューム

ディスク上でストレージのプロビジョニングを開始する前に、スタンバイ仮想マシンに割り当てるストレージの容量を決定します。スタンバイ仮想マシンをホストするために、Rapid Recovery リポジトリの作成後に残っている使用可能な容量から、任意の割合の容量を割り当てることができます。たとえば、Storage Resource Management (SRM) を使用している場合、Rapid Recovery リポジトリの作成後に残っている容量のうち最大 100 パーセントまでを割り当てることができます。スタンバイ VM に容量を割り当てることができるのは、仮想マシンをホストするためにプロビジョニングされたアプライアンスのみです。アプライアンスで保護されているサーバに障害が発生した場合、Rapid Recovery のライブリカバリ機能を使用して、それらのサーバを仮想マシンに素早く置き換えることができます。

スタンバイ仮想マシンを必要としない中規模の環境では、すべてのストレージを使用してかなりの数のエージェントをバックアップすることができます。一方、スタンバイ仮想マシン用に追加のリソースを必要とし、より少ない数のエージェントマシンをバックアップする場合は、より大きな VM 用により多くのリソースを割り当てることができます。

Appliance (アプライアンス) > Provisioning (プロビジョニング) タブを選択すると、Rapid Recovery アプライアンスソフトウェアは、システム内のサポートされているすべてのコントローラに対して使用可能なストレージ容量の場所を特定し、ハードウェアが要件を満たしていることを検証します。

使用可能なすべてのストレージのディスクプロビジョニングを完了するには、次の手順を実行します。

- 1 **Appliance (アプライアンス) > Provisioning (プロビジョニング)** をクリックします。
Provisioning (プロビジョニング) 画面リポジトリとストレージボリュームの項が表示されます。

△ **注意:** 作業を進める前に、本手順の手順 2 〜 手順 4 が実施されていることを確認します。

- 2 以下の作成に利用可能なストレージのプロビジョニング
 - ・ リポジトリ

- ・ スタンバイ VM、またはその他の目的のためのディスクボリューム
- 3 リポジトリを作成するには、次の手順を実行します。
 - a **provisioning (プロビジョニング)** ページのリポジトリセクションで、**Add New Repository (新規リポジトリを追加)** をクリックします。
 - Add New Repository (新規リポジトリを追加)** ダイアログボックスが表示されます。
 - b 次の表の説明に従って、情報を入力します。

表 56. ストレージのプロビジョニング

テキストボックス	説明
リポジトリ名	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは「リポジトリ」という単語と、この Core のリポジトリ番号に対応する番号で構成されます。たとえば、これが 2 番目のリポジトリである場合、デフォルトの名前はリポジトリ 2 です。必要に応じて名前を変更します。 リポジトリの名前には、1～40 文字の英数字（スペースを含む）を入力する必要があります。「禁止文字」または「禁止語句」は使用できません。詳細については、『 <i>Dell Data Protection Rapid Recovery 6.0 ユーザーガイド</i> 』の「禁止文字」および「禁止語句」のトピックを参照してください。
コントローラ	リポジトリを内部ストレージ、またはダイレクトアタッチドストレージエンクロージャのどちらで作成しているかによって、適切なストレージコントローラを選択します。
エンクロージャ	適切なストレージエンクロージャを選択します。
RAID のタイプ	適切な RAID レベルを選択します。RAID 構成のオプションは次のとおりです。1、5、または 6
容量見積もり	リポジトリの作成に使用可能な容量の見積もりを表示します。
コントローラの空き領域	コントローラ上の空き領域が表示されます。
サイズ	リポジトリのサイズを入力します。

① メモ: お使いのシステムでは、ストレージが構成され工場以外で利用可能な RAID レベルでのみリポジトリを作成できます。希望する RAID 構成でリポジトリを作成するには、希望の RAID レベルで、ストレージを設定する必要があります。希望の RAID レベルでストレージを設定するには、www.dell.com/support/home で **Dell アダプタマニュアル** を参照してください。

- c **Creat (作成)** をクリックします。
新しいリポジトリが作成されます。
- 4 スタンバイ VM、またはその他の目的のためのディスクボリュームを作成するには、次の手順を実行します。
 - a **ストレージボリューム** セクションで **Creat Volume (ボリュームの作成)** をクリックします。
 - b **Creat Volume (ボリュームの作成)** ダイアログボックスで、新しいディスクボリュームの次の情報を指定します。ボリューム名、コントローラ、エンクロージャ、RAID タイプ、およびサイズ
コントローラの空き領域がデフォルトで表示されます。次の RAID 構成のいずれかを選択できます。1、5、または 6
 - c **Creat (作成)** をクリックします。
新しいストレージボリュームが作成されます。

仮想ディスク用の容量割り当ての削除

プロビジョニングの構成を変更する必要がある場合は、テクニカルサポートにお問い合わせください。詳細については、**Contacting Dell (Dell へのお問い合わせ)** を参照してください。

Recovery and Update Utility

Recovery and Update Utility (RUU) は、DL アプライアンス (DL1000、DL1300、DL4000 および DL4300) のソフトウェアを回復してアップデートする、オールインワンのインストーラです。これには、Rapid Recovery Core ソフトウェアおよびアプライアンス固有のコンポーネントが含まれています。

RUU は、Windows Server の役割と機能、.Net 4.5.2、LSI Provider、DL アプリケーション、OpenManage Server Administrator および Rapid Recovery Core ソフトウェアの、アップデートされたバージョンで構成されています。また、Recovery and Update Utility は、Rapid Appliance Self Recovery (RASR) コンテンツもアップデートします。

① **メモ:** 現在 AppAssure Core バージョン、Rapid Recovery Core バージョン 6.0.2.144 以前のいずれかを使用している場合、RUU はペイロードで利用可能な最新バージョンへのアップデートを強制します。アップデートをスキップすることはできません。またこのアップデートは復帰不可能です。Core ソフトウェアをアップグレードしない場合は、RUU を実行しないでください。

アプライアンスのアップグレード

アプライアンスをアップグレードするには、次の手順を実行します。

- 1 Download (ダウンロード) セクションの下に License Portal (ライセンスポータル) に移動します。または、**support.dell.com** に移動し、RUU インストーラをダウンロードします。
- 2 そのユーティリティをアプライアンスのデスクトップにコピーし、ファイルを解凍します。
- 3 **launchRUU** アイコンをダブルクリックします。
- 4 プロンプトが表示されたら、リストされているいずれのプロセスも実行していないことを確認して **Yes (はい)** をクリックします。
- 5 **Recovery and Update Utility** 画面が表示されたら、**Start (開始)** をクリックします。
- 6 再起動のプロンプトが表示されたら、**OK** をクリックします。

Windows Server の役割と機能、.Net 4.5.2、LSI Provider、DL Applications、OpenManage Server Administrator、および Rapid Recovery (迅速な回復) コアソフトウェアのアップデートされたバージョンが Recovery and Update Utility の一部としてインストールされます。Recovery and Update Utility は、これらに加えて RASR コンテンツもアップデートします。

① **メモ:** AppAssure Core、Rapid Recovery Core version 6.0.2.144 以前の任意のバージョンを現在使用している場合は、RUU は **Payload (ペイロード)** で利用可能な最新バージョンへのアップデートを強制します。アップデートを省略することはできず、この更新を取り消すことはできません。Core ソフトウェアをアップグレードしない場合は、RUU を実行しないでください。

- 7 プロンプトが表示されたら、システムを再起動します。
- 8 すべてのサービスとアプリケーションのインストールが完了したら、**Proceed (続行)** をクリックします。Core Console が起動します。

アプライアンスの修復

アプライアンスを修復するには、次の手順を実行します。

- 1 Download (ダウンロード) セクションの下に License Portal (ライセンスポータル) に移動します。または、**support.dell.com** に移動し、RUU インストーラをダウンロードします。
- 2 そのユーティリティをアプライアンスのデスクトップにコピーし、ファイルを解凍します。
- 3 **launchRUU** アイコンをダブルクリックします。
- 4 プロンプトが表示されたら、リストされているいずれのプロセスも実行していないことを確認して **Yes (はい)** をクリックします。
- 5 Recovery and Update Utility 画面が表示されたら、**Start (開始)** をクリックします。
- 6 再起動のプロンプトが表示されたら、**OK** をクリックします。

Windows Server の役割と機能、.Net 4.5.2、LSI Provider、DL Applications、OpenManage Server Administrator、および Rapid Recovery（迅速な回復）コアソフトウェアの最新バージョンが Recovery and Update Utility の一部としてインストールされます。

- 7 ユーティリティにバンドルされているバージョンがインストール済みのバージョンと同じ場合、Recovery and Update Utility は、修復インストールを実行することを確認するプロンプトを表示します。Rapid Recovery（迅速な回復）コアの修復インストールが不要な場合は、この手順を省略できます。
- 8 ユーティリティにバンドルされているバージョンがインストール済みのバージョンよりも上の場合、Recovery and Update Utility は、Rapid Recovery コアソフトウェアをアップグレードすることを確認するプロンプトを表示します。

① | **メモ:** Rapid Recovery（迅速な回復）コアソフトウェアのダウングレードはサポートされません。

- 9 プロンプトが表示されたら、システムを再起動します。
- 10 すべてのサービスとアプリケーションのインストールが完了したら、**Proceed（続行）**をクリックします。
修復後にシステムを再設定する必要がある場合は、DL アプライアンス設定ウィザードが起動されます。それ以外の場合は、コアコンソールが起動されます。

ワークステーションとサーバーの保護

マシンの保護

本項では、Rapid Recovery 環境内の保護対象マシンを保護、設定、および管理する方法について説明します。

Rapid Recovery によるマシンの保護について

Rapid Recovery を使用してデータを保護するには、Rapid Recovery Core Console でワークステーションおよびサーバ（お使いの Exchange Server、SQL Server、Linux サーバなど）を追加する必要があります。

Core で保護するすべての物理マシンまたは仮想マシンに、Rapid Recovery エージェントソフトウェアをインストールする必要があります。

① **メモ:** このルールの例外は、**VMware** または **ESXi** ホストで仮想マシンを保護する場合、エージェントレスの保護を使用できるということです。エージェントレスの保護の制限事項など、詳細については、「[仮想の高速スナップに対する理解](#)」を参照してください。

Rapid Recovery Core Console で、いずれかのマシン保護ウィザードを使用する場合、保護するマシンを指定できます。次の操作が可能です。

- ・ ネットワークホスト名または IP アドレスを使用しているマシンに接続すると、マシン保護ウィザードを使用して、その 1 台のマシンを保護することができます。1 台のマシンを保護する方法の詳細については、「[マシンの保護](#)」を参照してください。
- ・ ネットワークホスト名または IP アドレスを使用しているクラスタまたはノードに接続すると、クラスタを保護 機能を使用して、ネットワーククラスタを保護することができます。
- ・ Microsoft Active Directory® を使用するマシンに接続すると、または vCenter あるいは ESXi ホストに接続すると、複数のマシンの保護ウィザードを使用して、同時に複数のマシンを保護できます。また、手動で入力するマシンリストに、ネットワークホスト名または IP アドレスを指定できます。

① **メモ:** 保護操作を失敗させるリソース不足を未然に回避するため、デルは同時に保護するマシンの台数を 50 以下に制限するように推奨しています。

ウィザードで 1 台のマシンの保護要件を識別するとき、保護するボリュームを指定できます。複数のマシンを保護する場合、すべてのボリュームがデフォルトで保護されます（この指定はマシンごとに後から変更できます）。

またウィザードでは、保護に対して、カスタマイズされたスケジュールを定義できます（または既存のスケジュールを再利用できます）。

詳細設定 オプションを使用すると、保護するマシンのバックアップに暗号化キーを指定または適用して、セキュリティ対策を追加することができます。

最後に、リポジトリがまだ存在していない場合は、ウィザードを使用してリポジトリを定義できます。

エージェントソフトウェアをインストールしたら、インストール後の再起動をマシンごとに実行する必要があります。

ワークステーションとサーバを保護する方法の詳細については、「[マシンの保護](#)」を参照してください。

△ **注意:** **Rapid Recovery** は、**ext2** ブートパーティションを使用している **Linux** マシンの **Bare Metal Restore (BMR)** をサポートしていません。**EXT2** パーティションが存在するマシンで **BMR** を実行すると、そのマシンが起動しなくなります。**ext2** ブートパーティションがある **Linux** マシンで **BMR** を実行できるようにする場合は、マシンの保護とバックアップを開始する前に、**ext2** ブートパーティションを **ext3** または **ext4** に変換する必要があります。

Rapid Recovery を使用した Linux マシンの保護について

Rapid Recovery エージェントソフトウェアは複数の Linux ベースのオペレーティングシステム（詳細については、『*Rapid Recovery インストールおよびアップグレードガイド*』または『*Rapid Recovery リリースノート*』に含まれているシステム要件を参照してください）。Rapid Recovery Core は、Windows マシンとのみ互換性があります。保護対象 Linux マシンは Rapid Recovery Core Console から管理できますが、Linux マシンの管理手順には、Windows マシンと異なる個所がいくつかあります。また、一部のアクションは、`local_mount` コマンドラインユーティリティを使用して、保護対象 Linux マシン上で直接実行できます。

① **メモ:** `local_mount` ユーティリティは、以前のマニュアルで `aamount` と呼ばれていました。

Rapid Recovery Core での Exchange Server および SQL Server の管理について

Exchange Server および SQL Server に固有のオプションが Rapid Recovery Core Console に表示されるのは、このソフトウェアのインスタンスおよび関連するファイルが保護対象サーバで検出された場合のみです。この場合、Core Console で保護対象マシンを選択すると、追加のオプションが使用可能になります。

たとえば、左側のナビゲーションメニューで保護対象 Exchange Server を選択すると、その保護対象マシンに対して表示されるメニューオプションに **Exchange** ドロップダウンメニューオプションが含まれます。

左側のナビゲーションメニューで保護対象 SQL Server を選択すると、その保護対象マシンに対して表示されるメニューオプションに **SQL** ドロップダウンメニューが含まれます。

これらのオプションの機能は異なりますが、共通点もあります。保護対象 Exchange Server および SQL Server に対して実行可能な機能は次のとおりです（他の保護対象マシンに対しては実行されません）。

- ・ **サーバーログの切り捨ての強制実行。** SQL Server および Exchange Server の両方にサーバーログが含まれています。SQL ログの切り捨てプロセスでは、サーバの空き容量を特定します。Exchange Server のログを切り捨てる場合は、空き容量の特定だけでなく、このプロセスにより、サーバの領域が解放され、空き容量が増えます。
- ・ **関連サーバーの資格情報の設定** Exchange Server では、保護対象サーバの サマリ ページで保護対象マシンの資格情報を設定できます。SQL Server では、1つの保護対象 SQL Server の資格情報を設定したり、すべての保護対象 SQL Server のデフォルトの資格情報を設定したりできます。
- ・ **Exchange Server または SQL Server からのリカバリポイントのチェックステータスの表示** 保護対象 SQL Server または Exchange Server からキャプチャされたリカバリポイントには対応する色のステータスインジケータがあります。これらの色は SQL Server または Exchange Server に関連するさまざまなチェックの成功または失敗を示します。

本項は、Exchange Server または SQL Server を使用する保護対象マシンの管理に関連するトピックで構成されています。

- ・ [リカバリポイントステータスインジケータについて](#)
- ・ [保護対象 Exchange Server の設定と機能](#)
- ・ [保護対象 SQL Server の設定と機能](#)

サーバクラスタの保護について

Rapid Recovery では、サーバクラスタ保護は、個々のクラスタノード（つまり、クラスタ内の個々のマシン）にインストールされている Rapid Recovery 保護対象マシンと Rapid Recovery Core に関連付けられています。この関連付けにより、これらのマシンは1台の複合マシンとして保護されます。

Rapid Recovery Core では、クラスタの保護および管理のための設定が簡単に行えます。Core Console では、クラスタは別個のエントリとして編成されており、関連するノードを含む「コンテナ」として機能します。たとえば、左側にあるナビゲーションエ

リアの **保護対象マシン** メニューには、保護されるクラスタが表示されます。各クラスタのすぐ下には、関連付けられている個々のノードまたは Agent マシンが表示されます。これらはそれぞれ、Rapid Recovery エージェントソフトウェアがインストールされている保護対象マシンです。クラスタをクリックすると、Core Console にクラスタの **サマリ** ページが表示されます。

Core レベルとクラスタレベルで、関連するノードと共有ボリュームのリストなど、クラスタについての情報を表示できます。Core Console でクラスタの情報を表示する場合は、上部のナビゲーションメニューで **保護対象ノード** をクリックし、クラスタ内の個々のノードについてサマリ表を表示することができます。各ノードのサマリ表では、さまざまな機能を実行できます。たとえば、スナップショットの強制実行、1回限りのエクスポートの実行、Virtual Standby の設定、リカバリポイントのマウントまたは表示、リカバリポイントからの復元、クラスタノードから独自の保護対象マシンへの変換、保護からのノードの削除などです。ノードが Exchange または SQL Server である場合、ログを切り捨てるオプションも表示されます。

クラスタレベルでは、クラスタ内のノードに対応する Exchange および SQL クラスタメタデータも表示できます。クラスタ全体の設定、およびそのクラスタ内の共有ボリュームの設定を指定できます。

左側のナビゲーションメニューでクラスタ内の任意のノードをクリックすると、クラスタ内のそのノードの情報が Core Console に表示されます。ここでは、そのノードの情報を表示したり、そのノードの設定を指定したりできます。

クラスタ共有ボリュームのサポート

Rapid Recovery リリース 6.x では、クラスタ共有ボリューム (CSV) のサポートが Windows Server 2008 R2 を実行している CSV のネイティブバックアップに限定されます。Windows Server 2008 R2 を実行している CSV ボリュームをリカバリポイントからリストアすることも、Windows Server 2008 R2 を実行する Hyper-V CSV に対して仮想エクスポートを実行することもできます。クラスタ共有ボリュームの仮想エクスポートは実行できません。Rapid Recovery リリース 6.0.1 以降の新機能に、Windows Server 2012 または Windows Server 2012 R2 を実行している Hyper-V CSV に対して仮想エクスポートを実行する機能があります。

① **メモ: Hyper-V のエージェントレスの機能は、Windows Server 2012 R2 以降に対してのみ互換性があります。**

その他のオペレーティングシステムの場合は、Rapid Recovery エージェントサービスをクラスタ内のすべてのノード上で実行でき、クラスタを Rapid Recovery コア内のクラスターとして保護できます。ただし、CSV はコアコンソールを表示せず、保護のために使用できません。(オペレーティングシステムボリュームなどの) すべてのローカルディスクは、保護に使用できます。

次の表は、クラスタ共有ボリュームに対する Rapid Recovery コアの現在のサポート状況を説明します。

表 57. クラスタ共有ボリュームの Rapid Recovery のサポート

Rapid Recovery のクラスタ共有ボリュームのサポート	保護、レプリケーション、ロールアップ、マウント、アーカイブ	CSV ボリュームのリストア	Hyper-V CSV に対する仮想エクスポート
Rapid Recovery	6.0	6.0	6.0.x
Windows Server 2008 R2	有	有	有
Windows Server 2012	無	無	有
Windows Server 2012 R2	無	無	有

¹ Hyper-V のエージェントレスの機能を除外します。この機能は Windows Server 2012 R2 以降に対してのみ互換性があります。

Rapid Recovery はクラスタ共有ボリュームの他の一部のオペレーティングシステムを保護しますが、これはあくまでもお客様の責任で行われます。上の表の構成のみが Dell でサポートされます。

ダイナミックボリュームとベーシックボリュームのサポート

Rapid Recovery では、すべてのダイナミックボリュームとベーシックボリュームのスナップショットを作成できます。また、Rapid Recovery では、1つの物理ディスク上にあるシンプルダイナミックボリュームのエクスポートも可能です。その名前が示すように、シンプルダイナミックボリュームとはストライプボリューム、ミラーボリューム、スパンボリュームのいずれでもありません。

ダイナミックディスクの仮想エクスポートは、エクスポートするボリュームが Rapid Recovery Agent ソフトウェアによって保護されているか、VM がエージェントレス保護の機能を使用しているかによって動作が異なります。これは、シンプルではないダイナミックボリュームまたは複雑なダイナミックボリュームは、Rapid Recovery からは完全には認識できない恣意的なディスクジオメトリであるためです。

Rapid Recovery Agent ソフトウェアを使用して、マシンから複雑なダイナミックディスクをエクスポートしようとする、エクスポート機能はシンプルなダイナミックボリュームに制限されるという内容の注意がユーザーインターフェースに表示されます。また、Rapid Recovery Agent を使用してシンプルなダイナミックボリューム以外のものをエクスポートしようとする、エクスポートのジョブは失敗します。

これとは対照的に、エージェントレスで保護している VM のダイナミックボリュームは、保護、仮想エクスポート、データの復元、および BMR をサポートします。また、リポジトリストレージもいくつかの重要な制限事項付きでサポート対象となります。たとえば、次のとおりです。

- ・ **保護**：ダイナミックボリュームが複数のディスクにまたがる場合、ボリュームの完全性を維持するために、それらのディスクをまとめて保護する必要があります。
- ・ **仮想エクスポート**：エージェントレス保護を使用している ESXi ホストから、ストライプボリューム、ミラーボリューム、スパンボリューム、または RAID ボリュームなどの複雑なダイナミックボリュームをエクスポートすることができます。
ただし、ボリュームはディスクレベルでエクスポートされますが、ボリューム解析はされません。たとえば、2 つのディスクにまたがるダイナミックボリュームをエクスポートする場合、2 つのディスクボリュームが個別にエクスポート対象となります。

△ 注意：複数のディスクにまたがるダイナミックボリュームをエクスポートする場合は、ディスクタイプを保持するために、元々のシステムボリュームとともにダイナミックディスクをエクスポートする必要があります。

- ・ **データの復元**：複数のディスクにまたがるダイナミックボリュームを復元する場合、ディスクタイプを保持するために、元々のシステムボリュームとともに、ダイナミックボリュームを復元する必要があります。1 つのディスクだけを復元すると、ディスク設定が壊れてしまいます。

リポジトリストレージ：さらに、Rapid Recovery は、複雑なダイナミックボリューム（ストライプボリューム、ミラーボリューム、スパンボリューム、または RAID ボリューム）上でのリポジトリの作成をサポートしています。リポジトリが設定されたマシンのファイルシステムは NTFS または ReFS である必要があります。

Rapid Recovery Agent ソフトウェアのインストーラについて

Rapid Recovery では、Rapid Recovery Core からインストーラをダウンロードすることができます。**ダウンロード** ページから、Agent のインストーラ、Local Mount Utility (LMU)、または SNMP MIB ファイルのいずれかを選択してダウンロードできます。LMU の詳細については、「[Local Mount Utility](#)」を参照してください。SNMP の詳細については、「[SNMP 設定について](#)」を参照してください。

- ① **メモ**：Agent のインストーラへのアクセスについては、「[Rapid Recovery エージェントインストーラのダウンロード](#)」を参照してください。Agent のインストーラの展開の詳細については、**Dell Data Protection | Rapid Recovery** の『インストールおよびアップグレードガイド』を参照してください。

Agent のインストーラは、Rapid Recovery Core で保護される予定のマシン上に Rapid Recovery Agent アプリケーションをインストールするために使用します。Agent のインストーラが必要なマシンがある場合は、Rapid Recovery Core Console の **ダウンロード** ページから、Web インストーラをダウンロードできます。

- ① **メモ**：Core のダウンロードは、**Dell Data Protection | Rapid Recovery** ライセンスポータルから実行されます。**Rapid Recovery Core** のインストーラをダウンロードする場合は、「<https://licenseportal.com>」にアクセスしてください。詳細については、**Dell Data Protection | Rapid Recovery** ライセンスポータルの『ユーザーガイド』を参照してください。

Rapid Recovery エージェントインストーラのダウンロード

Rapid Recovery エージェントインストーラをダウンロードして、Rapid Recovery Core 上で保護する任意のマシンに配備します。本プロセスの手順に従って、Web Installer をダウンロードします。

- 1 エージェント Web インストーラを、保護するマシンから直接ダウンロードするには、次の操作を実行します。
 - a Web ブラウザで、Dell Data Protection | Rapid Recovery ライセンスポータル (<https://licenseportal.com>) を開きます。

- b 左側のナビゲーションメニューで、「ダウンロード」をクリックします。
 - c **Windows ベースのアプリケーション** ペインから、**Windows エージェント** の行へ下にスクロールして、適切なインストーラ（32 ビットまたは 64 ビットシステム）の **ダウンロード** をクリックします。
- インストーラファイル、たとえば Agent-X64-6.0.1.xxxx.exe がダウンロード先フォルダに保存されます。

- 2 Core から Web インストーラをダウンロードするには、Core Console アイコンバーで、 **詳細** アイコンをクリックし、**ダウンロード** を選択します。
 - 3 **ダウンロード** ページの **エージェント** ペインで、**Web インストーラをダウンロード** をクリックします。
 - 4 **Agent-Web.exe** を開いています ウィンドウで、**ファイルの保存** をクリックします。
- インストーラファイル、たとえば Agent-X64-6.0.1.xxxx.exe がダウンロード先フォルダに保存されます。
- 5 インストーラを適切なマシンに移動し、Rapid Recovery エージェントソフトウェアをインストールします。
- Rapid Recovery エージェントソフトウェアのインストールの詳細については、『*Rapid Recovery インストールおよびアップグレードガイド*』を参照してください。

Agent をコアコンソールから複数のマシンへ同時に導入

Rapid Recovery エージェントソフトウェアを複数の Windows マシンに同時に導入できます。マシンは Active Directory ドメインあるいは vCenter または ESX 仮想ホストの一部とすることができます。または、Rapid Recovery エージェントソフトウェアをアップグレードする場合のように、ローカルの RRapid Recovery コアによりすでに保護されているマシンとすることもできます。特定のドメインまたはホストに必ずしも関連付けられていないマシンに、ソフトウェアを手動で導入することもできます。

することができます手動で導入された Rapid Recovery エージェントソフトウェアを、コアコンソールから1つまたは複数の Linux マシンに、手動で導入することもできます。

△ 注意: Rapid Recovery エージェントのインストール前に **AppAssure** エージェントが **Linux** マシンに以前にインストールされている場合には、シェルスクリプトを使用して **AppAssure** エージェントをマシンから削除します。Linux マシンからエージェントの削除の詳細については、トピックを [Uninstalling the AppAssure Agent software from a Linux machine \(Linux マシンから AppAssure エージェントソフトウェアをアンインストール\)](#) を参照してください。エージェントソフトウェアを Linux マシンに正常に導入するには、トピック [About installing the Agent software on Linux machines \(Linux マシンにエージェントソフトウェアをインストール\)](#) の必要条件を参照してください。これらのトピックは *Dell Data Protection | Rapid Recovery (デルデータ保護 | 迅速な回復) インストール/アップグレードガイド* にあります。

Rapid Recovery エージェントソフトウェアを導入しても、マシンが自動的に保護されるわけではありません。導入後、コアコンソールのボタンバーから **Protect Multiple Machines (複数のマシンの保護)** オプションを選択する必要があります。

① メモ: この機能は複数のマシンに同時に導入されており、以前は“**bulk deploy (一括導入)**”と呼ばれていました。この機能は複数のマシンを保護しており、以前“**bulk protect (一括保護)**”と呼ばれていました。

複数のマシンを導入して保護するには、次のタスクを実行します。

- ・ Rapid Recovery) エージェントを複数のマシンに導入します。 [Rapid Recovery Agent ソフトウェアの1つまたは複数のマシンへの展開](#) を参照してください。
- ・ 導入を監視します。 [複数マシンへの導入の確認](#) を参照してください。
- ・ 複数のマシンを保護します。 [複数のマシンの保護について](#) を参照してください。

① メモ: 導入時に **Protect Machine After Install (インストール後にマシンを保護)** オプションを選択した場合、このタスクを省略します。

- ・ 一括保護のアクティビティを監視します。 [複数マシンの保護の監視](#) を参照してください。

Rapid Recovery Agent ソフトウェアの1つまたは複数のマシンへの展開

Rapid Recovery Agent ソフトウェアを1つまたは複数の Windows マシンに展開するタスクは、マシンへの Agent ソフトウェアの展開 ウィザードを使用して簡略化することができます。

① **メモ:** これまで、この機能は「一括展開」と呼ばれていました。

マシンへの Agent ソフトウェアの展開 ウィザードを使用すると、Rapid Recovery はホスト上のマシンを自動的に検知することができます。ユーザーは展開するマシンを選択できます。Active Directory、vCenter、ESX (i) 以外のドメインまたはホスト上のマシンは、IP アドレスと適切な認証情報を使用して個々のマシンに手動で接続することができます。また、ローカルの Rapid Recovery Core マシンに既に保護されているマシンに、ソフトウェアのアップグレードをプッシュすることもできます。

Core Console から、次のいずれかの操作を実行できます。

- ・ [Active Directory ドメイン上のマシンへの導入](#)
- ・ [VMware vCenter/ESX \(i\) 仮想ホスト上のマシンへの導入](#)
- ・ [Rapid Recovery エージェントソフトウェアのアップグレードを保護対象マシンに導入する](#)
- ・ [手動によるマシンへの導入](#)

① **メモ:** 同時に展開できるマシンの数を 50 以下に制限して、展開操作が失敗する原因となる可能性があるリソースの制約が起きないようにすることをお勧めします。

① **メモ:** ターゲットマシンには、ビットをダウンロードしてインストールするためのインターネットアクセスが必要です。これは、**Rapid Recovery** が **Rapid Recovery Agent** インストーラの **Web** バージョンを使用してインストールコンポーネントを展開するからです。インターネットアクセスが使用できない場合は、**Core Console** を使用して **USB ドライブ**などのメディアにインストーラをダウンロードし、保護するマシン上にソフトウェアを物理的にインストールします。詳細については、「[Rapid Recovery エージェントインストーラのダウンロード](#)」を参照してください。

Active Directory ドメイン上のマシンへの導入

Rapid Recovery エージェントのソフトウェアを1つまたは複数の Active Directory ドメイン上のマシンに同時に導入するには、次の手順を実行します。

この手順を開始する前に、Active Directory サーバのドメイン情報とログオン資格情報を入手しておく必要があります。

- 1 Rapid Recovery Core Console で、**保護** ドロップダウンメニューをクリックし、**エージェントソフトウェアの導入** をクリックします。
エージェントソフトウェアの導入 ウィザードが開きます。
- 2 ウィザードの **接続** ページで、**ソース** ドロップダウンリストから **Active Directory** を選択します。
- 3 次の表の説明に従って、ドメイン情報とログオン認証情報を入力します。

表 58. ドメイン情報と資格情報

テキストボックス	説明
ホスト	Active Directory ドメインのホスト名または IP アドレス。
ユーザー名	ドメインへの接続に使用するユーザー名（例、Administrator（マシンがドメイン内にある場合は [ドメイン名]\Administrator））。
パスワード	ドメインへの接続に使用するパスワード。

- 4 「**次へ**」をクリックします。
- 5 **マシン** ページで、Rapid Recovery のエージェントソフトウェアを導入するマシンを選択します。
- 6 エージェントがインストールされた後に、必要に応じて自動的に保護対象マシンを再起動するには、**エージェントのインストール後に、マシンを自動的に再起動します（推奨）** を選択します。
- 7 「**終了**」をクリックします。
システムは選択されている各マシンを自動的に検証します。
Rapid Recovery が自動検証中に問題点を検出した場合は、ウィザードが **警告** ページに進み、このページでマシンを選択対象からクリアして手動で選択済みのマシンを検証することができます。追加したマシンが自動検証に合格した場合は、マシンへのエージェントの導入 ペインに表示されます。
- 8 **警告** ページが表示されたが選択が適切である場合は、**完了** をもう一度クリックします。

Rapid Recovery エージェントソフトウェアが指定されたマシンに導入されます。マシンはまだ保護されていません。保護は「[Active Directory ドメインの複数のマシンを保護](#)」の完了後に開始されます。

VMware vCenter/ESX (i) 仮想ホスト上のマシンへの導入

Rapid Recovery エージェントのソフトウェアを1つまたは複数の VMware vCenter/ESX (i) 仮想ホスト上のマシンに同時に導入するには、次の手順を実行します。
この手順を開始する前に、次のような情報を入手している必要があります。

- ・ VMware vCenter/ESX (i) 仮想ホストのためのログオン資格情報。
- ・ ホストの場所。
- ・ 保護する各マシンのログオン資格情報。

① **メモ:** すべての仮想マシンには **VMware** ツールがインストールされている必要があります。インストールされていない場合、**Rapid Recovery** は導入先の仮想マシンのホスト名を検出できません。**Rapid Recovery** は、ホスト名の代わりに仮想マシン名を使用するため、ホスト名と仮想マシン名が異なっている場合、問題が発生する可能性があります。

- 1 Rapid Recovery Core Console で、**保護** ドロップダウンメニューをクリックし、**エージェントソフトウェアの導入** をクリックします。
エージェントソフトウェアの導入 ウィザードが開きます。
- 2 ウィザードの **接続** ページで、**ソース** ドロップダウンリストから **vCenter / ESX (i)** を選択します。
- 3 次の表の説明に従って、ホスト情報とログオン認証情報を入力します。

表 59. vCenter/ESX (i) の接続設定

テキストボックス	説明
ホスト	VMware vCenter Server/ESX (i) 仮想ホストの名前または IP アドレス。
ポート	仮想ホストへの接続に使用するポート。 デフォルト設定は 443 です。
ユーザー名	仮想ホストへの接続に使用するユーザー名 (例、Administrator (マシンがドメイン内にある場合は [ドメイン名]\Administrator))。
パスワード	この仮想ホストへの接続に使用するセキュアなパスワード。

- 4 「**次へ**」をクリックします。
- 5 ウィザードの **マシン** ページで、ドロップダウンメニューから次のオプションのうち1つを選択します。
 - ・ 「ホストとクラスタ」
 - ・ VM およびテンプレート
- 6 マシンのリストを展開し、ソフトウェアを導入する VM を選択します。
Rapid Recovery によりマシンがオフラインであるか VMware Tools がインストールされていないことが検出された場合は、通知が表示されます。
- 7 展開後に自動的にマシンを再起動する場合は、**エージェントのインストール後に、マシンを自動的に再起動します (推奨)** を選択します。
- 8 「**次へ**」をクリックします。
Rapid Recovery は選択された各マシンを自動的に検証します。
- 9 ウィザードの **調整** ページに、各マシンの資格情報を次の形式で入力します。hostname::username::password。

① **メモ:** 各行に 1 台のマシンを入力してください。

- 10 「**終了**」をクリックします。
システムは選択されている各マシンを自動的に検証します。
Rapid Recovery が自動検証中に問題点を検出した場合は、ウィザードが **警告** ページに進み、このページでマシンを選択対象からクリアして手動で選択済みのマシンを検証することができます。追加したマシンが自動検証に合格した場合は、マシンへのエージェントの導入 ペインに表示されます。
- 11 警告 ページが表示されたが選択が適切である場合は、**完了** をもう一度クリックします。

Rapid Recovery エージェントソフトウェアが指定されたマシンに導入されます。マシンはまだ保護されていません。保護は「[Vcenter/ESX\(i\) 仮想ホスト上の複数マシンの保護](#)」の完了後に開始されます。

Rapid Recovery エージェントソフトウェアのアップグレードを保護対象マシンに導入する

エージェントソフトウェアの導入 ウィザードを使用して、ローカルの Rapid Recovery Core によってすでに保護されているマシンに Rapid Recovery エージェントソフトウェアのアップグレードをプッシュすることができます。

- 1 Rapid Recovery Core Console で、**保護** ドロップダウンメニューをクリックし、**エージェントソフトウェアの導入** をクリックします。
エージェントソフトウェアの導入 ウィザードが開きます。
- 2 ウィザードの **接続** ページで、**ソース** ドロップダウンリストから **ローカル Core** を選択します。
- 3 「**次へ**」をクリックします。
- 4 ウィザードの **マシン** ページで、Rapid Recovery のエージェントソフトウェアのアップグレードを導入する保護対象マシンを選択します。
- 5 「**終了**」をクリックします。
システムは選択されている各マシンを自動的に検証します。
Rapid Recovery が自動検証中に問題点を検出した場合は、ウィザードが **警告** ページに進み、このページでマシンを選択対象からクリアして手動で選択済みのマシンを検証することができます。追加したマシンが自動検証に合格した場合は、**マシンへのエージェントの導入** ペインに表示されます。
- 6 **警告** ページが表示されたが選択が適切である場合は、**終了** をもう一度クリックします。

手動によるマシンへの導入

Rapid Recovery エージェントをローカル Core、Active Directory、または vCenter/ESXi 以外の任意のタイプのホスト上にある複数マシンに導入するには、次の手順に従います。

- 1 Rapid Recovery Core Console で、**保護** ドロップダウンメニューをクリックし、**エージェントソフトウェアの導入** を選択します。
エージェントソフトウェアの導入 ウィザードが開きます。
- 2 ウィザードの **接続** ページで、**ソース** ドロップダウンリストから **手動** を選択します。
- 3 「**次へ**」をクリックします。
- 4 ウィザードの **マシン** ページで、ダイアログボックスにマシンの詳細を次の形式で入力します。
hostname::username::password::port。例には次の内容が含まれます。
10.255.255.255::administrator::&11@yYz90z::8006
abc-host-00-1::administrator::99!zU\$083r::168
- 5 展開後に自動的にマシンを再起動する場合は、**エージェントのインストール後に、マシンを自動的に再起動します（推奨）** を選択します。
- 6 「**終了**」をクリックします。
システムは選択されている各マシンを自動的に検証します。
Rapid Recovery が自動検証中に問題点を検出した場合は、ウィザードが **警告** ページに進み、このページでマシンを選択対象からクリアして手動で選択済みのマシンを検証することができます。追加したマシンが自動検証に合格した場合は、**マシンへのエージェントの導入** ペインに表示されます。
- 7 **警告** ページが表示されたが選択が適切である場合は、**終了** をもう一度クリックします。

Rapid Recovery エージェントソフトウェアが指定されたマシンに導入されます。マシンはまだ保護されていません。保護は「[手動での複数マシンの保護](#)」の完了後に開始されます。

複数マシンへの導入の確認

Rapid Recovery エージェントソフトウェアを複数のマシンに同時に展開したら、保護対象マシン メニューにリストされる各マシンを参照し、導入が成功したかどうかを確認できます。

イベント ページから一括展開プロセスに関する情報を表示することもできます。導入を確認するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動し、 (イベント) をクリックして、**アラート** をクリックします。
アラートイベントがリストに表示され、イベントの開始時間とメッセージが表示されます。Agent ソフトウェアが正常に導入されるたびに、保護対象マシンが追加されたことを示すアラートが表示されます。
- 2 必要に応じて、保護対象マシンのリンクをクリックします。
選択したマシンの **サマリ** ページが表示され、次を含む関連情報を表示します。
 - ・ 保護対象マシンのホスト名
 - ・ 最新のスナップショット (該当する場合)
 - ・ 選択したマシンの保護スケジュールに基づいた、次のスケジュール済みスナップショットの時間
 - ・ この保護対象マシンに使用される暗号化キー (存在する場合)
 - ・ Agent ソフトウェアのバージョン

導入設定の変更

導入設定を変更するには、次の手順を実行します。

- 1 Rapid Recovery Core Console から、 (設定) をクリックします。
- 2 **設定** ページの左の欄で、**導入** をクリックして 導入 セクションに移動します。
- 3 以下のオプションのどれかを変更するには、変更する設定をクリックし、テキストボックスまたはドロップダウンリストとして編集可能にして、 をクリックして設定を保存します。

表 60. 導入オプション

オプション	説明
Agent Installer Name (エージェン トインストーラ名)	エージェント実行可能ファイルの名前を入力します。デフォルトは Agent-web.exe です。
Core Address (Core アドレス)	Core のアドレスを入力します。
受信タイムアウト による失敗	アクティビティのない状態でタイムアウトまで待機する分数を入力します。
最大パラレルイン ストール	同時にインストールする、インストール最大数を入力します。デフォルト値と制限値は 100 です。
インストール後の 自動再起動	はい の場合はチェックボックスを選択し、いいえ の場合はクリアします。
導入後に保護	はい の場合はチェックボックスを選択し、いいえ の場合はクリアします。

保護スケジュールについて

保護スケジュールは保護対象のエージェントマシンから Rapid Recovery Core にいつバックアップを転送するかを定義します。

Core に保存される最初のバックアップ転送は、ベースイメージスナップショットと呼ばれます。指定した全ボリュームの全データ (オペレーティングシステム、アプリケーション、設定を含む) が、Core に保存されます。この処理では、転送されるデータの量によっては、非常に長い時間がかかる可能性があります。以降は、増分スナップショット (前回のバックアップ以降に保護対象マシンで変更されたデータのみで構成される小さなバックアップ) が、定義した間隔 (60 分ごとなど) に基づいて定期的に Core に

保存されます。このバックアップに含まれるデータは、ベースイメージのデータより少ないため、転送にかかる時間は短くなります。

保護スケジュールは、まず「マシンの保護」ウィザードまたは「複数のマシンの保護」ウィザードを使用して定義します。ウィザードで（期間または毎日の保護時刻のいずれかを選択して）保護スケジュールをカスタマイズして、業務上のニーズに対応できます。特定の保護対象マシンのサマリ ページで、保護スケジュール ダイアログボックスを表示すると、いつでも既存のスケジュールを変更したり、新しいスケジュールを作成したりできます。

Rapid Recovery にはデフォルトの保護スケジュールが用意されています。このスケジュールは、すべての曜日にまたがる単一の期間で、1つの期間（12:00 AM ～ 11:59 PM）が定義されています。デフォルトの間隔（スナップショット間隔）は 60 分です。保護を初めて有効にするときに、スケジュールもアクティブにすることができます。そのため、デフォルト設定を使用すると、現在の時刻に関係なく、毎時（12:00 AM、1:00 AM、2:00 AM など）に最初のバックアップが発生します。

期間を選択した場合、デフォルトの保護スケジュールを表示して、必要に応じて調整できます。毎日の保護時間を選択すると、Rapid Recovery Core によって、指定した保護対象マシンが 1 日 1 回指定の時間にバックアップされます。

平日と週末の使用可能な時間を使ってスケジュールをカスタマイズすると、ピークとオフピークの時間帯を定義できます。たとえば、平日に、保護対象マシンがほとんど使用状態になっている場合、平日の間隔を 20 分に減らすと、1 時間に 3 つのスナップショットが生成されることになります。または、週末の期間の間隔を 60 分から 180 分に延長して、トラフィックが少ないときに 3 時間ごとにスナップショットが取得されるようになります。

あるいは、ピーク時間とオフピーク時間を毎日定義するようにデフォルトのスケジュールを変更することもできます。これを行うには、デフォルトの開始時刻と終了時刻をより小さい時間範囲（0:00 AM ～ 4:59 PM など）に変更し、適切な間隔（20 分など）を設定します。これは、ピーク期間には頻繁にバックアップを行うことを表しています。次に、残りの期間のために週末の時間帯（5:00 PM ～ 11:59 PM）を追加して、適切な（通常はより大きな）間隔（180 分など）を設定することができます。この設定は、オフピーク期間として、毎日 5:00 PM から夜の 12 時までを定義します。このカスタマイズにより、5:00 PM から 11:59 PM までは 3 時間ごとに、12:00 AM から 4:59 PM までは 20 分ごとにスナップショットが作成されるようになります。

Rapid Recovery で 保護スケジュール ダイアログボックスを使用して保護スケジュールの変更または作成を行う場合、他の保護対象マシンに適用できる再使用可能なテンプレートとしてスケジュールを保存するオプションが表示されます。

保護ウィザードのその他のオプションには、毎日の保護時間の設定などがあります。これにより、定義した時間（デフォルト設定は 12:00 PM）で 1 日 1 回バックアップが実行されます。

ウィザードを使用して 1 台以上のマシンを保護する場合、最初に保護を一時停止することで、マシンを保護せずに保護スケジュールを定義できます。確立された保護スケジュールでマシンの保護を開始する準備が整ったら、明示的に保護を再開する必要があります。保護の再開の詳細については、「[保護の一時停止と再開](#)」を参照してください。マシンをすぐに保護する必要がある場合、スナップショットを強制実行できます。詳細については、「[スナップショット作成の強制実行](#)」を参照してください。

マシンの保護

Rapid Recovery エージェントソフトウェアが保護するマシンにすでにインストールされていて、まだ再起動していない場合は、すぐにマシンを再起動します。

このトピックでは、Protect Machine（マシンの保護）ウィザードを使用して、指定の単一のマシンでデータ保護を開始する方法を、説明します。

- ① **メモ: VMware ESXi ホストでエージェントレスの保護を使用しない限り、保護するマシンに Rapid Recovery エージェントソフトウェアをインストールして、そのマシンを保護する必要があります。この手順を行う前にエージェントソフトウェアをインストールする選択を行えます。または、Protect Machine (マシンの保護) ウィザードを完了する手順の一部としてソフトウェアをターゲットマシンに導入することができます。**

エージェントレスの保護と制限事項の詳細については、[仮想の高速スナップに対する理解](#)を参照してください。

エージェントソフトウェアのインストールの詳細については、「Rapid Recovery エージェントソフトウェアのインストール」を参照してください。Dell Data Protection | Rapid Recovery ライセンスポータル *Installation and Upgrade Guide* (Dell データ保護 | Rapid Recovery ライセンスポータルインストール/アップグレードガイド)。エージェントソフトウェアがマシンの保護の前にインストールされていない場合、このウィザードの一部として保護のための特定のボリュームを選択することはできません。この場合、デフォルトでは、エージェントマシン上のすべてのボリュームが保護のために含まれます。Rapid Recovery は、EISA パーティションで構成されるマシンのリカバリの保護をサポートします。サポートは、Windows 回復環境 (Windows RE) を使用する Windows 8 と 8.1、Windows 2012 および Windows 2012 R2 のマシンにも拡張されます。

1つのプロセスを同時に使用する複数のマシンを保護する場合は、[複数のマシンの保護について](#)を参照してください。

保護を追加する場合には、IP アドレスやポートなどの接続情報を定義し、保護するマシンの資格情報を提供する必要があります。オプションで、IP アドレスの代わりにコアコンソールに表示名が表示されるようにすることもできます。これを変更すると、コアコンソールで詳細を表示する際に、保護されたマシンの IP アドレスが表示されません。マシンの保護スケジュールも定義します。

詳細設定を選択すると、保護プロセスでオプションの手順にアクセスできるようになります。詳細オプションには、リポジトリの機能と暗号化が含まれます。たとえば、既存の Rapid Recovery リポジトリを指定して、スナップショットを保存するように指定したり、新規のリポジトリを作成したりすることができます。既存の暗号化キーを指定 (または新しい暗号化キーを追加) し、このマシンに対して Core に保存されているデータを適用することもできます。暗号化キーの詳細については、[暗号化キーの理解](#)を参照してください。

保護ウィザードのワークフローが環境に若干異なる場合があります。たとえば、Rapid Recovery エージェントソフトウェアが保護するマシンにインストールされている場合、ウィザードからそれをインストールするように要求されません。同様に、リポジトリが Core にすでに存在する場合も、作成するように要求されません。

- △ **注意: Rapid Recovery は、ext2 ブートパーティションのある Linux マシンのベアメタルリストア (BMR) をサポートしません。このパーティションタイプのあるマシンで BMR が実行されると、マシンが起動しなくなります。将来的に、このマシンで BMR を実行できるようにする場合は、マシンの保護とバックアップを開始する前に、ext2 パーティションを ext4 または ext3 に変換する必要があります。**

- 1 次の手順のいずれか1つを実行します。
 - ・ Protect Machine (マシンの保護) ウィザードから開始する場合は、[手順 2](#)に進んでください。
 - ・ Rapid Recovery コアコンソールから開始する場合は、ボタンバーで **Protect (保護)** をクリックしてください。

Protect Machine (マシンの保護) ウィザードが表示されます。

- 2 **Welcome (ようこそ)** ページで、適切なインストールオプションを選択します。
 - ・ リポジトリの定義または暗号化の確立が必要ない場合は、**Typical (標準)** を選択します。
 - ・ 選択したマシン用に、リポジトリを作成するか、バックアップのために別のリポジトリを定義する必要がある場合、あるいはウィザードを使用して暗号化を確立する場合は、**Advanced (show optional steps) (詳細 (オプションの手順を表示))** を選択します。
 - ・ 今後 Protect Machine (マシンの保護) ウィザードの **Welcome (ようこそ)** ページを表示したくない場合は、**Skip this Welcome page the next time the wizard opens (次回ウィザードを開く際に Welcome (ようこそ) ページをスキップする)** オプションを選択します。
- 3 Welcome (ようこそ) ページで、選択内容を設定し終わったら **Next (次へ)** をクリックします。

Connection (接続) ページが表示されます。
- 4 **Connection (接続)** ページで、次の表に説明されているとおり、接続先のマシンに関する情報を入力し、**Next (次へ)** をクリックします。

表 61. マシンの接続設定

テキストボックス	説明
Host (ホスト)	保護するマシンのホスト名または IP アドレス。
ポート	Rapid Recovery コアがマシン上のエージェントと通信するときに使用するポートの番号。 デフォルトポート番号は 8006 です。
ユーザー名	このマシンへの接続に使用するユーザー名。たとえば、Administrator (または、マシンがドメイン内にある場合は、[domain name]\Administrator)。
パスワード	このマシンに接続するために使用するパスワード。

Install Agent (エージェントのインストール) ページが Protect Machine (マシンの保護) ウィザードの横に表示されます。これは、Rapid Recovery が Rapid Recovery エージェントをマシンで検出せず、ソフトウェアの現在のバージョンをインストールすることを意味します。手順 7 に進みます。

Upgrade Agent (エージェントのアップグレード) ページがウィザードの横に表示されます。これは、保護するマシン上にエージェントのソフトウェアの古いバージョンが存在することを意味します。

① **メモ:** エージェントソフトウェアを保護するマシンにインストールする必要があります。また、**Core** へのバックアップを実行する前に、そのマシンを再起動する必要があります。インストーラで保護されたマシンを再起動するには、オプション **After installation, restart the machine automatically (recommended)** (インストールした後にマシンを自動的に再起動する (推奨)) を選択し、**Next** (次へ) をクリックします。

- 5 **Upgrade Agent (エージェントのアップグレード)** ページで、次のいずれかを実行します。
 - ・ エージェントソフトウェアの新しいバージョン (Rapid Recovery コアのバージョンと一致するもの) を導入するには、**Upgrade the Agent to the latest version of the software** (エージェントをソフトウェアの最新バージョンにアップグレード) を選択します。
 - ・ エージェントソフトウェアバージョンを更新せずにマシンを引き続き保護するには、オプション **Upgrade the Agent to the latest version of the software** (エージェントをソフトウェアの最新バージョンにアップグレード) をオフにしてください。
- 6 **次へ** をクリックします。
- 7 オプションとして、**Protection (保護)** ページで、Rapid Recovery コアコンソールで IP アドレス以外の名前をこの保護対象マシンに対して表示する場合は、**Display Name (表示名)** フィールドでダイアログボックスに名前を入力します。
最大 64 文字を入力できます。トピック **使用禁止文字** で説明されている特殊文字を使用しないでください。また、トピック **禁止語** で説明されている文字の組み合わせを表示名の開始部分に使用しないでください。
- 8 次の説明に従って、適切な保護スケジュールを選択します。
 - ・ デフォルトの保護スケジュールを使用するには、Schedule Settings (スケジュール設定) オプションで、を選択します **Default protection (デフォルトの保護)** を選択してください。

デフォルトの保護スケジュールを使用すると、Core では、保護対象マシン上のすべてのボリュームのスナップショットを 1 時間ごとに 1 回作成します。どのボリュームを保護するかを選択することも含めて、ウィザードを閉じた後に任意のタイミングで保護設定を変更するには、特定の保護対象マシンの Summary (サマリ) ページに移動します。

- ・ 別の保護スケジュールを定義するには、**Custom protection (カスタム保護)** を選択します。

- 9 次のように設定を行います。
 - ・ Protect Machine (マシンの保護) ウィザードで Typical (標準) を選択し、デフォルトの保護設定を指定した場合、**Finish (終了)** をクリックして選択内容を確定し、ウィザードを閉じると、指定したマシンが保護されます。
マシンに対してはじめて保護が追加されると、保護を当初一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ (保護対象ボリューム内の全データのスナップショット) が Rapid Recovery コア上のリポジトリに転送されます。
 - ・ Protect Machine (マシンの保護) ウィザードで Typical (標準) 設定を選択し、カスタム保護を指定した場合、**Next (次へ)** をクリックしてカスタム保護スケジュールをセットアップします。保護スケジュールのカスタマイズの詳細については、**カスタム保護スケジュールの作成** 参照してください。
 - ・ Protect Machine (マシンの保護) ウィザードの詳細設定と、デフォルトの保護を選択した場合は、**Next (次へ)** をクリックして **手順 14** に進み、リポジトリと暗号化のオプションを設定します。

- Protect Machine (マシンの保護) ウィザードの Advanced (詳細) 設定を選択し、カスタム保護を指定した場合は、**Next (次へ)** をクリックして **手順 11** に進み、保護するボリュームを選択します。
- 10 **Protection Volumes (保護ボリューム)** ページで、保護したいボリュームを指定します。保護の対象にしたくないボリュームがリストにある場合、Check (チェック) 列をクリックして選択を解除します。その後、**Next (次へ)** をクリックします。
- ① **メモ:** 一般には、少なくとも、システム予約済みボリュームとオペレーティングシステムのボリューム (通常は C ドライブ) を保護することが慣例です。
- 11 **Protection Schedule (保護スケジュール)** ページで、カスタム保護スケジュールを定義し、**Next (次へ)** をクリックします。カスタム保護スケジュールを定義に関する詳細は、[カスタム保護スケジュールの作成](#) を参照してください。
- すでに設定されているリポジトリ情報があり、手順 1 で Advanced (詳細) オプションを選択した場合は、暗号化ページが表示されます。 **手順 13** に進みます。
- 12 **Repository (リポジトリ)** ページでは、次の内容を実行します。
- リポジトリがすでにあり、既存のリポジトリで保護するためにこのマシンからデータを保存するには、次の手順を実行します。
 - Use an existing repository (既存のリポジトリを使用)** を選択します。
 - リストから既存のリポジトリを選択します。
 - 次へ** をクリックします。
- Encryption (暗号化)** ページが表示されます。 **手順 13** に進み、暗号化をオプションで定義します。
- リポジトリを作成する場合は、 **Repository (リポジトリ)** を選択してから、次の手順を完了します。
 - Repository (リポジトリ)** で、次の表の情報を入力します。

表 62. 新しいリポジトリ設定の追加

テキストボックス 説明	
Repository Name (リポジトリ名)	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは Repository (リポジトリ) という単語と、この Core のリポジトリの番号に対応する番号で構成されます。たとえば、最初のリポジトリの場合、デフォルト名は Repository 1 です。必要に応じて名前を変更します。 リポジトリ名にはスペースを含む 1 文字から 40 文字の英数字を含める必要があります。 使用禁止文字 または 禁止語 を使用しないでください。
Concurrent Operations (同時操作)	レポジトリで対応する同時要求の数を定義します。デフォルトの値は 64 です。
Comments (コメント)	オプションで、このリポジトリの説明を入力します。最大 254 文字を入力できます。たとえば、DVM Repository 2 と入力します。

- 2 **Add Storage Location (ストレージの場所を追加)** をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。

△ **注意:** リポジトリ用のストレージの場所のルート内の専用のフォルダを定義します。ルート場所は指定しません。たとえば、E:\ではなく **E:\Repository** を使用します。この手順で作成するリポジトリが後で削除された場合、リポジトリのストレージの場所にあるすべてのファイルが削除されます。ルートで使いのストレージの場所を定義する場合は、ボリューム内のその他のすべてのファイル (たとえば、E:\) が削除され、致命的なデータ損失が発生する可能性があります。

Add Storage Location (ストレージの場所の追加) ダイアログボックスが表示されます。

- Add Storage Location (ストレージの場所を追加)** をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。
- Storage Location (ストレージの場所)** 領域には、ストレージの場所にファイルを追加する方法を指定します。ローカルに接続されているストレージ (DAS、SAN、NAS など) を追加することを選択できます。共通インターネットファイルシステム (CIFS) の共有場所にストレージボリュームを指定することもできます。
- Add the file on local disk (ローカルディスクにファイルを追加)** を選択して、ローカルマシンを指定し、以下の表に記載されているとおりに情報を入力します。

表 63. ローカルディスクの設定

テキストボックス	説明
Data Path (データパス)	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Data と入力します。 パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。
Metadata Path (メタデータパス)	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Metadata と入力します。 パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。

または、**Add file on CIFS share (CIFS 共有にファイルを追加)** を選択して、ネットワーク共有の場所を指定し、以下の表に記載されているとおりに情報を入力します。

表 64. CIFS 共有の資格情報

テキストボックス	説明
UNC Path (UNCパス)	ネットワーク共有の場所のパスを入力します。 この場所がルートにある場合は、専用のフォルダ名（たとえば、Repository）を定義します。 パスの開始部分には \\ を使用する必要があります。パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。英字 a~z は大文字と小文字が区別されません。スペースは使用しないでください。その他の記号および句読点は使用できません。
ユーザー名	ネットワーク共有の場所にアクセスするためのユーザー名を指定します。
パスワード	ネットワーク共有の場所にアクセスするためのパスワードを指定します。

- 5 **Storage Configuration (ストレージの設定)** 領域で、**More Details (詳細)** をクリックし、次の表の説明に従ってストレージの場所の詳細を入力します。

表 65. ストレージ構成の詳細

テキストボックス	説明
サイズ	ストレージの場所のサイズまたは容量を設定します。最小サイズは 1 GB です。デフォルトは 250 GB です。次から選択できます。 - GB - TB ① メモ: 指定するサイズは、ボリュームのサイズを超えることはできません。 ストレージの場所が Windows XP または Windows 7 を使用した New Technology File System (NTFS) ボリュームの場合、ファイルサイズの上限は 16 TB です。 ストレージの場所が Windows 8 と 8.1、Windows 10、または Windows Server 2012 と 2012 R2 を使用した NTFS ボリュームの場合、ファイルサイズの制限は 256 TB です。

- ① **メモ:** **Rapid Recovery** からオペレーティングシステムを検証する場合は、**Windows Management Instrumentation (WMI)** が対象のストレージの場所にインストールされている必要があります。

Write caching policy (ライトキャッシングポリシー) ライトキャッシングポリシーは、リポジトリでの Windows Cache Manager の使用を制御し、さまざまな構成で最適なパフォーマンスを得られるようにリポジトリを調整します。次のいずれかの値に設定します。

- ・ 点灯
- ・ オフ
- ・ 同期

デフォルトのまま On (オン) に設定すると、Windows がキャッシングを制御します。これは、Windows 10、および Windows Server 2012 以降のバージョンに対して適切です。

- ① **メモ:** ライトキャッシングポリシーを On (オン) に設定すると、パフォーマンスを高速化できます。**Windows Server 2008 SP2** または **Windows Server 2008 R2 SP2** を使用している場合、推奨の設定は Off (オフ) です。

Off (オフ) に設定すると、Rapid Recovery がキャッシングを制御します。

Sync (同期) に設定すると、Windows が同期入出力に加えてキャッシングも制御します。

セクタあたりのバイト 各セクタに包含するバイト数を指定します。デフォルト値は 512 です。

Average bytes per record (レコードあたりの平均バイト数) レコードあたりの平均バイト数を指定します。デフォルト値は 8192 です。

6 次へ をクリックします。

手順 1 で **Advanced (詳細)** オプションを選択すると、**Encryption (暗号化)** ページが表示されます。

- 13 オプションで、**Encryption (暗号化)** ページで、暗号化を有効にし、**Enable Encryption (暗号化を有効化)** を選択します。Encryption key (暗号化キー) フィールドが **Encryption (暗号化)** ページに表示されます。

- ① **メモ:** 暗号化を有効にする場合は、このマシンの保護されたすべてのボリュームのデータに適用されます。暗号化設定を後で、**Rapid Recovery** コアコンソールから変更できます。暗号化についての詳細は、トピック [暗号化キーの理解](#) を参照してください。

- △ **注意:** **Rapid Recovery** は、256 ビットキーの暗号ブロック連鎖 (CBC) モードで AES 256 ビット暗号化を使用します。暗号化はオプションですが、暗号化キーを設定し、定義したパスフレーズを保護することを強くお勧めします。データの回復に非常に重要であることから、パスフレーズを安全な場所に保管してください。パスフレーズがないとデータは回復できません。

- 14 **Encryption (暗号化)** ページで、次のオプションのいずれかを選択します。

- ・ Rapid Recovery コアで既に定義されている暗号化キーを使用してこの保護対象マシンを暗号化するには、**Encrypt data using an existing Encryption key (既存の暗号化キーを使用してデータを暗号化)** を選択してから、ドロップダウンメニューから適切なキーを選択します。[次の手順](#)に進みます。
- ・ Core に新しい暗号化キーを追加し、そのキーをこの保護対象マシンに適用する場合は、次の表の説明に従って情報を入力します。

表 66. 暗号化キーの設定

テキストボックス 説明

Name (名前) 暗号化キーの名前を入力します。

テキストボックス 説明

	暗号化キーの名前には、1~130 文字の英数字文字を含める必要があります。バックスラッシュ、スラッシュ、パイプ、コロン、アスタリスク、引用符、疑問符、開くまたは閉じる括弧、アンパサンドまたはハッシュなどの特殊文字は使用できません。
説明	暗号化キーのコメントを入力します。 この情報は、コアコンソールからの暗号化キーを表示する際に、Description（説明）フィールドに表示されます。
Passphrase（パスフレーズ）	アクセスの制御に使用するパスフレーズを入力します。 上記にリストされている特殊文字を避けるのが慣例です。 安全な場所にパスフレーズを記録します。Dell Support はパスフレーズを復元できません。いったん暗号化キーを作成し、1つまたは複数の保護対象マシンにそれを適用した場合、パスフレーズを失うとデータを復元できません。
パスフレーズの確認	テキストボックスに先ほど入力したパスフレーズを再度入力します。

15 **Finish（終了）** をクリックして、設定を保存し適用します。

マシンに対してはじめて保護が追加されると、保護を当初一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ（保護対象ボリューム内の全データのスナップショット）が Rapid Recovery コア上のリポジトリに転送されます。

クラスタの保護

このトピックでは、Rapid Recovery でクラスタを追加して保護する方法について説明します。保護するクラスタを追加する場合は、クラスタのホスト名または IP アドレス、クラスタアプリケーション、または Rapid Recovery Agent ソフトウェアが含まれるクラスタノードまたはマシンの1つを指定する必要があります。

- ① **メモ:** リポジトリは、保護されたノードからキャプチャされたデータのスナップショットを保存するために使用します。クラスタ内のデータの保護を開始する前に、お使いの **Rapid Recovery Core** に関連付けられているリポジトリを少なくとも1つ設定しておく必要があります。

リポジトリのセットアップの詳細については、「[リポジトリの理解](#)」を参照してください。

- 1 Rapid Recovery Core Console で、**保護** ボタンドロップダウンメニューをクリックし、**クラスタの保護** をクリックします。
- 2 クラスタに接続 ダイアログボックスで、次の情報を入力します。

表 67. 「クラスタに接続」の設定

テキストボックス	説明
ホスト	クラスタ、クラスタアプリケーション、またはいずれかのクラスタノードのホスト名または IP アドレス。
ポート	Rapid Recovery Core がエージェントと通信するマシン上のポート番号。 デフォルトポートは 8006 です。
ユーザー名	このマシンに接続するために使用するドメイン管理者のユーザー名（たとえば、domain_name \administrator）。
① メモ: ドメイン名は必須です。ローカル管理者のユーザー名では、クラスタに接続できません。	
パスワード	このマシンに接続するために使用するパスワード。

- 3 **接続** をクリックします。
- 4 クラスタを保護 ダイアログボックスで、このクラスタのリポジトリを選択します。
- 5 Core ベースの暗号化を使用してこのクラスタのリカバリポイントを保護するには、暗号化キーを選択します。

- 6 この手順を完了した後即座に保護を開始しない場合は、**最初に保護を一時停止** を選択します。
 - 7 デフォルト設定に基づいてクラスタを保護するには、デフォルト保護のノードを選択して、**手順 10** に進みます。
- ① **メモ:** デフォルトの設定では、すべてのボリュームのスナップショットを **60 分ごと** にスケジュール設定します。
- 8 クラスタのカスタム設定を入力するには（たとえば、共有ボリュームの保護スケジュールをカスタマイズする）、次のいずれかを行い、「**カスタム保護スケジュールの作成**」を参照します。
 - ・ 個々のノードの設定をカスタマイズするには、カスタマイズするノードの横にある、**設定** をクリックし、関連するボリュームの横にある **機能** をクリックします。
 - ・ クラスタの設定をカスタマイズするには、ダイアログボックスの下にある設定ボタンをクリックし、関連するボリュームの横にある **機能** をクリックします。
- ノードのカスタマイズの詳細については、「**クラスタ内のノードの保護**」を参照してください。
- 9 すべての必要な変更を行ったら、**保存** をクリックします。
 - 10 クラスタを保護 ダイアログボックスで、**保護** をクリックします。

クラスタノード設定の変更

クラスタノードに保護を追加したら、これらのマシンまたはノードの基本設定（表示名、ホスト名など）、保護設定（マシン上のローカルボリュームの保護スケジュールの変更、ボリュームの追加または削除、保護の一時停止）などを簡単に変更できます。

クラスタノード設定を変更するには、次のタスクを実行してください。

- ・ Rapid Recovery コアコンソールで、変更したいノードを含むクラスタに移動し、変更するマシンまたはノードを選択します。
- ・ 設定を変更および表示するには、「**通知グループの設定**」を参照してください。
- ・ システムイベントの通知グループを設定するには、「**保護対象マシンの設定の表示と変更**」を参照してください。
- ・ 保持ポリシー設定をカスタマイズするには、「**保護対象マシンの保持ポリシー設定のカスタマイズ**」を参照してください。
- ・ 保護スケジュールを変更するには、「**保護スケジュールの変更**」を参照してください。
- ・ 転送設定を変更するには、「**転送設定の変更について**」を参照してください。

クラスタ内のノードの保護

このタスクでは、最初にクラスタを保護する必要があります。詳細については、「**クラスタの保護**」を参照してください。

このトピックでは、Rapid Recovery Agent がインストールされているクラスタノードまたはマシンでデータを保護する方法について説明します。この手順を実行すると、クラスタを保護した際に省略された可能性のある個々のノードを保護に追加することができます。

- 1 Rapid Recovery Core Console で保護対象マシンの下にある、保護するノードを含むクラスタをクリックします。
- 2 クラスタのサマリ ページで **保護対象ノード** をクリックします。
- 3 保護対象ノード ページで **クラスタノードを保護** をクリックします。
- 4 クラスタノードを保護 ダイアログボックスで、必要に応じて、次の情報を選択または入力します。

表 68. 「クラスタノードを保護」の設定

テキストボックス	説明
ホスト	クラスタ内の保護可能なノードのドロップダウンリスト。
ポート	Rapid Recovery Core がノード上の Agent と通信するために使用するポート番号。
ユーザー名	このノードに接続するために使用するドメイン管理者のユーザー名（たとえば、example_domain\administrator または administrator@example_domain.com）。
パスワード	このマシンに接続するために使用するパスワード。

- 5 ノードを追加するには、**接続** をクリックします。

- 6 デフォルト保護設定でこのノードの保護を開始するには、[手順 13](#)に進みます。

④ **メモ:** デフォルト設定では、マシン上のすべてのボリュームが **60 分**ごとのスケジュールで保護されます。

- 7 デフォルト以外のリポジトリを使用する場合は、[ノード名]を保護ダイアログボックスでドロップダウンリストからリポジトリを選択します。
- 8 Core ベースの暗号化を使用して、このクラスタのリカバリポイントを保護する場合は、ドロップダウンリストで暗号化キーを選択します。
- 9 この手順を完了した後即座に保護を開始しない場合は、「**最初に保護を一時停止**」を選択します。
- 10 カスタム設定（共有ボリュームの保護スケジュールのカスタマイズなど）を入力するには、次の手順を実行します。
- a 個々のボリュームの設定をカスタマイズするには、カスタマイズするボリュームの横の **関数** をクリックします。
 - b 「[カスタム保護スケジュールの作成](#)」を参照してください。
- 11 **Protect**（保護）をクリックします。

カスタム保護スケジュールの作成

ウィザードを使用して保護を定義する場合、保護対象マシン上のデータを保護するカスタムスケジュールを作成するには、次の手順を実行します。

- 1 保護ウィザードの **保護** ページ（マシンを保護、複数のマシンを保護、クラスタを保護）で、**カスタム保護** を選択します。
- 2 「**次へ**」をクリックします。
- 3 **保護対象ボリューム** ページで、保護するボリュームを選択し、**次へ** をクリックします。
- 4 **保護スケジュール** ページで任意の期間のスケジュール間隔を変更するには、次の操作を実行します。
 - a 「**複数の期間**」を選択します。
既存の期間が表示され、変更することができます。各期間の開始時刻、終了時刻、および間隔（X 分ごと）などのフィールドを編集できます。
 - b 各期間について **間隔** テキストボックスをクリックし、適切な間隔を分単位で入力します。
たとえば、デフォルトの間隔の 60 をハイライト表示して、その値を 20 に置き換え、この期間中 20 分ごとにスナップショットが実行されるようにします。
- 5 ピーク期間およびオフピーク期間を作成するには、平日期間の時間範囲を 24 時間より小さい範囲に変更して、ピーク範囲の適切な間隔を設定し、**残りの時間のスナップショットを取得** を選択して、オフピーク間隔を設定します。これを行うには、次の手順を実行します。
 - a 「**複数の期間**」を選択します。
既存の期間が表示され、変更することができます。
 - b **開始時刻** ボックス内をクリックするか、時計のアイコンを使用して、この期間の開始時刻を変更します。
 - c **終了時刻** ボックス内をクリックするか、時計のアイコンを使用して、この期間の終了時刻を変更します。
 - d **間隔** テキストボックス内をクリックして、適切な間隔を分単位で入力します。
たとえば、デフォルトの間隔の 60 をハイライト表示して、その値を 20 に置き換え、この期間に選択した時間範囲中 20 分ごとにスナップショットが実行されるようにします。
 - e **残された時間にスナップショットを取得** を選択し、間隔を分単位で入力します。
- 6 1 日 1 回バックアップが発生するように 1 つの時刻を設定するには、「**毎日の保護時刻**」を選択して、HH:MM AM 形式で時刻を入力します。たとえば、毎日 9:00 PM にバックアップを行うには、「09:00 PM」と入力します。
- 7 バックアップを開始せずにスケジュールを定義するには、「**最初に保護を一時停止**」を選択します。
ウィザードから保護を一時停止すると、明示的に保護を再開するまで一時停止し続けます。保護を再開すると、確立したスケジュールに基づいてバックアップが発生します。保護の再開の詳細については、「[保護の一時停止と再開](#)」を参照してください。
- 8 保護スケジュールの変更内容に問題がなければ、必要に応じて「**終了**」または「**次へ**」をクリックします。残りの要件を完了できるように、該当のウィザードの手順に戻ります。

保護スケジュールの変更

保護スケジュールは保護対象のエージェントマシンから Rapid Recovery Core にいつバックアップを転送するかを定義します。保護スケジュールは、まず「マシンの保護」ウィザードまたは「複数のマシンの保護」ウィザードを使用して定義します。

特定の Agent マシンの「サマリ」タブでいつでも既存の保護スケジュールを変更できます。

- ① **メモ:** 保護スケジュールの概念については、「[保護スケジュールについて](#)」を参照してください。1 台のマシンの保護については、「[マシンの保護](#)」を参照してください。一括保護（複数マシンの保護）については、「[複数のマシンの保護について](#)」を参照してください。これらのいずれかのウィザードを使用してエージェントを保護する場合の保護期間のカスタマイズについては、「[カスタム保護スケジュールの作成](#)」を参照してください。既存の保護スケジュールの変更については、「[保護スケジュールの変更](#)」を参照してください。

保護対象マシン上のボリュームに対する既存の保護スケジュールを変更するには、次の手順を実行します。

- 1 Core Console に表示された保護対象マシンのリストで、保護スケジュールを変更する保護対象マシンをクリックします。
- 2 選択したマシンのページ上で目的のボリュームを選択し、**スケジュールを設定** をクリックします。
一度にすべてのボリュームを選択するには、ヘッダ行のチェックボックスをオンにします。最初は、すべてのボリュームで同じ保護スケジュールを共有しています。

- ① **メモ:** 通常、少なくともシステムで予約されているボリュームとオペレーティングシステムのボリューム（通常は C ドライブ）を保護することをお勧めします。

「保護スケジュール」ダイアログボックスが表示されます。

- 3 保護スケジュール ダイアログボックスで、次のいずれかを実行します。
 - ・ 以前に保護スケジュールテンプレートを作成したことがあり、そのテンプレートをこの保護対象マシンに適用する場合は、ドロップダウンリストからそのテンプレートを選択して、[手順 7](#)に進みます。
 - ・ スケジュールから既存の期間を削除する場合、各期間のオプションの横にあるチェックボックスをオフにして、[手順 7](#)に進みます。次のようなオプションがあります。
 - ・ 月 - 金：(月曜日～金曜日) この時間の範囲は、一般的な週休 2 日制を意味します。
 - ・ 土 - 日：(土曜日～日曜日) この時間の範囲は、一般的な週末を意味します。
 - ・ 新しい保護スケジュールをテンプレートとして保存する場合、[手順 4](#)に進みます。
 - 4 平日の開始時刻と終了時刻が 12:00 AM ~ 11:59 PM になっている場合、1 つの期間が存在することになります。定義された期間の開始時刻または終了時刻を変更するには、次の手順を実行します。
 - a 適切な期間を選択します。
 - b この期間の開始時刻を変更するには、**開始時刻** の下にあるクロックアイコンを使用します。
たとえば、矢印を使用して、08:00 AM の時間を表示します。
 - c この期間の終了時刻を変更するには、**終了時刻** の下にあるクロックアイコンを使用します。
たとえば、矢印を使用して、18:00 AM の時間を表示します。
 - d 要件に応じて間隔を変更します。たとえば、ピーク期間を定義する場合です。間隔を 60 分から 20 分に変更して、1 時間に 3 回スナップショットを取得するようにします。
 - 5 [手順 7](#)で 12:00 AM ~ 11:59 PM 以外の時間を定義して、残り時間範囲内でバックアップを発生させるには、次の手順を行って、保護を定義する追加期間を追加します。
 - a 目的のカテゴリの下で **期間を追加** をクリックします。
 - b クロックアイコンをクリックし、必要に応じて目的の開始時刻と終了時刻を選択します。
たとえば、開始時刻に 12:00 AM、終了時刻に 07:59 AM を設定します。
 - c 要件に応じて間隔を変更します。たとえば、オフピーク期間を定義する場合です。間隔を 60 分から 120 分に変更して、2 時間おきにスナップショットを取得するようにします。
 - 6 必要に応じて、引き続き追加の期間を作成し、開始時刻と終了時刻および間隔を設定します。
- ① **メモ:** 追加した期間を削除する場合、その期間の右端にあるごみ箱アイコンをクリックし、次には **はい** をクリックして削除を確認します。
- 7 設定するスケジュールからテンプレートを作成するには、**テンプレートとして保存** をクリックします。
 - 8 テンプレートを保存 ダイアログボックスで、テンプレート名を入力し、**保存** をクリックします。
 - 9 必要な保護スケジュールが設定できたら、**Apply** (適用) をクリックします。
「保護スケジュール」ダイアログボックスが閉じます。

保護の一時停止と再開

保護を一時停止するときは、選択したマシンから Rapid Recovery Core へのすべてのデータの転送を一時的に停止します。保護を再開すると、Rapid Recovery Core は、保護スケジュールの要件に従い、そのスケジュールに基づいてデータを定期的にバックアップします。

次の場所で、Rapid Recovery の保護対象マシンの保護を一時停止することができます。

- ・ 「マシンの保護」ウィザードまたは「複数のマシンの保護」ウィザード（保護の確立時）
- ・ Rapid Recovery Core の左側にあるナビゲーションエリアの 保護対象マシン メニュー（すべての保護対象マシンの保護の一時停止）
- ・ 「保護対象マシン」ページ（「保護対象マシン」メニューをクリックしてアクセスできる）
- ・ 保護対象マシン ドロップダウンメニューの特定の保護マシン
- ・ 特定の保護対象マシンの各ページの最上部

「マシンの保護」ウィザードまたは「複数のマシンの保護」ウィザードを使用して保護を一時停止する場合、明示的に再開するまで保護は一時停止します。

ウィザード以外で保護を一時停止する場合、再開するまで保護を一時停止するのか、指定（日、時、分の任意の組み合わせで指定）した期間だけ保護を一時停止するかを選択できます。一定期間一時停止する場合、その期間が終了すると、保護スケジュールに基づいてシステムによって自動的に保護が再開されます。

次の場所で、一時停止されている Rapid Recovery の保護対象マシンの保護を再開することができます。

- ・ Rapid Recovery Core の左側にあるナビゲーションエリアの 保護対象マシン メニュー（すべての保護対象マシンの保護の再開）
- ・ 保護対象マシン ドロップダウンメニューの特定の保護マシン
- ・ 「保護対象マシン」ページ（「保護対象マシン」メニューをクリックしてアクセスできる）
- ・ 特定の保護対象マシンの各ページの最上部

必要に応じて、保護を一時停止または再開するには、次の手順を実行します。

- 1 Rapid Recovery Core Console で、すべてのマシンの保護を一時停止するには、左側にあるナビゲーションエリアの 保護対象マシン ドロップダウンメニューから次の操作を行います。
 - a 「**保護を一時停止**」を選択します。
「保護を一時停止」ダイアログボックスが表示されます。
 - b 次のいずれかのオプションを使用して適切な設定を選択し、「**OK**」をクリックします。
 - ・ 明示的に再開するまで保護を一時停止するには、「**再開まで一時停止**」を選択します。
 - ・ 指定した期間保護を一時停止するには、「**次の期間で一時停止**」を選択し、「日」、「時」、「分」コントロールで、必要に応じて適切な一時停止期間を入力または選択します。
- 2 すべてのマシンの保護を再開するには、次の操作を行います。
 - a 「**保護を再開**」を選択します。
「保護を再開」ダイアログボックスが表示されます。
 - b 「保護を再開」ダイアログボックスで、「**はい**」をクリックします。
「保護を再開」ダイアログボックスが閉じて、すべてのマシンの保護が再開されます。
- 3 単一のマシンの保護を一時停止するには、左側のナビゲーションエリアで、該当のマシンの右側にあるドロップダウンメニューをクリックして、次の操作を行います。
 - a 「**保護を一時停止**」を選択します。
「保護を一時停止」ダイアログボックスが表示されます。
 - b 次のいずれかのオプションを使用して適切な設定を選択し、「**OK**」をクリックします。
 - ・ 明示的に再開するまで保護を一時停止するには、「**再開まで一時停止**」を選択します。
 - ・ 指定した期間保護を一時停止するには、「**次の期間で一時停止**」を選択し、「日」、「時」、「分」コントロールで、必要に応じて適切な一時停止期間を入力または選択します。
- 4 単一のマシンの保護を再開するには、次の操作を行います。

- a 「保護を再開」を選択します。
「保護を再開」ダイアログボックスが表示されます。
 - b 「保護を再開」ダイアログボックスで、「はい」をクリックします。
「保護を再開」ダイアログボックスが閉じて、選択したマシンの保護が再開されます。
- 5 マシンのページから1つのマシンの保護を一時停止するには、該当のマシンに移動します。
選択したマシンの サマリ ページが表示されます。
- a ページ最上部で **一時停止** をクリックします。
「保護を一時停止」ダイアログボックスが表示されます。
 - b 次のいずれかのオプションを使用して適切な設定を選択し、「OK」をクリックします。
 - ・ 明示的に再開するまで保護を一時停止するには、「再開まで一時停止」を選択します。
 - ・ 指定した期間保護を一時停止するには、「次の期間で一時停止」を選択し、「日」、「時」、「分」コントロールで、必要に応じて適切な一時停止期間を入力または選択します。
- 6 保護を再開するには、次の手順を実行します。
- a ページ最上部で **再開** をクリックします。
 - b 保護を再開 ダイアログボックスで、**はい** をクリックします。
保護を再開 ダイアログボックスが閉じて、選択したマシンの保護が再開されます。

保護対象マシンの管理

本項では、Rapid Recovery 環境内の保護対象マシンを表示、設定、および管理する方法について説明します。

保護対象マシンの管理について

保護対象マシンを管理するためのタスクは、以下のカテゴリに分類されます。

- ・ 「Rapid Recovery」に記載されているオプションを使用して、[Rapid Recovery Core](#) に含まれている保護対象マシンを表示することができます。
- ・ マシン設定の構成、システム情報の参照、特定のマシンに関するイベント通知の設定。詳細については、「[マシンの設定](#)」を参照してください。
- ・ 保護対象マシンの診断情報へのアクセス。詳細については、「[保護対象マシンのログファイルのダウンロードと表示](#)」を参照してください。
- ・ マシンの保護対象からの削除、現在の操作のキャンセル、保護対象マシンのライセンス情報の表示。詳細については、「[マシンの管理](#)」を参照してください。
- ・ Core に保存されたデータの表示と管理。詳細については、「[スナップショットとリカバリポイントの管理](#)」を参照してください。

保護対象マシンの表示

Rapid Recovery Core Console の **ホーム** ページでは、サマリテーブルを表示しているときに、保護対象マシン ペインで Core によって保護されているマシンのサマリ情報を確認できます。

- ① **メモ:** ソフトウェアエージェントは、ユーザーに代わって個々のアクションを実行します。保護対象マシンは、**Rapid Recovery Core** 上でデータのバックアップとレプリケーションを容易に行えるように **Rapid Recovery Agent** ソフトウェアを実行するので、**Agent** と呼ばれることがあります。

「ホーム」タブでは、ステータス、各マシンの表示名、使用リポジトリ、最新スナップショットの作成日時、マシンのリポジトリに存在するリカバリポイントの数、スナップショットがリポジトリ内で使用しているストレージ領域の合計を確認できます。

保護対象マシンのさまざまな側面を管理するには、まず、表示、設定、または管理するマシンに移動します。ホーム ページから保護対象マシンに移動するには、次の3つの方法があります。

- ・ 保護対象マシン ペインから保護されているマシンの IP アドレスまたは表示名をクリックすることができます。これにより、選択した保護対象マシンの サマリ ページに移動します。
- ・ 左側のナビゲーションエリアで、**保護対象マシン** メニューのタイトルをクリックすることができます。Protected Machines (保護マシン) ページが表示されます。保護対象マシン ページで、各マシンのサマリ情報を表示することができます。このページの詳細については、「[保護対象マシンのサマリ情報の表示](#)」を参照してください。
- ・ 左側にあるナビゲーションエリアの 保護対象マシン メニューで、保護対象マシンの IP アドレスまたは表示名をクリックすることができます。これにより、選択した保護対象マシンの サマリ ページに移動します。このページの詳細については、[保護対象マシンのサマリ情報の表示](#)を参照してください。

クラスタのサマリ情報の表示

クラスタの関連するクォーラムについての情報を含むクラスタのサマリ情報を表示するには、次の手順を実行します。

- 1 Rapid Recovery Core Console の保護対象マシンで、表示するクラスタをクリックします。
マシンの サマリ ページが表示されます。
- 2 サマリ ページで、クラスタ名、クラスタタイプ、クォーラムタイプ (該当する場合)、およびクォーラムパス (該当する場合) などの情報を確認できます。このページには、サイズや保護スケジュールを含む、このクラスタ内のボリュームについての概要情報も表示されます。また、異なるクラスタの SQL Server または Exchange Server の情報を表示することもできます (該当する場合)。
- 3 最近の情報を表示するには、**更新** をクリックします。

クラスタ内の個々のマシンまたはノードのサマリ情報とステータス情報を表示する方法については、「[保護対象マシンの表示](#)」を参照してください。

マシンの設定

いったん Rapid Recovery (迅速な回復) で保護するマシンを追加すると、保護されたマシンの動作を制御する設定を簡単に表示および変更することができます。特定のマシンの設定を変更すると、それらの設定は Core レベルで設定した動作より優先されます。

Rapid Recovery (迅速な回復) コアコンソールで次のマシンの設定を表示し、構成できます。

- ・ **General (一般)**。一般的なマシン構成設定には、表示名、ホスト名、ポート、暗号化キー、およびリポジトリが含まれます。マシンの一般設定の構成に関する詳細については、[保護対象マシンの設定の表示と変更](#)を参照してください。
- ・ **Nightly jobs (夜間ジョブ)**。特定の保護されたマシンに対して表示される Core の夜間ジョブ設定のサブセットを利用すると、Core レベルで設定された夜間ジョブの設定よりも優先される設定を行うことができます。これには、ロールアップが含まれ、保持ポリシーを管理できます。一部の設定は、保護されているマシンのタイプにより異なる場合があります。
- ・ **Transfer settings (転送設定)**。選択された保護対象マシンのデータ転送プロセスを管理する上で特有の設定です。これらの設定によって影響を受けるデータ転送のタイプについては、[転送設定の変更について](#)を参照してください。
- ・ **Excluded writers** 除外されているライター。これらの設定を利用すると、ライターを除外することができます。ライターは特有の API が公開された my Microsoft で、これを利用すると他のソフトウェアコンポーネントが Microsoft ボリュームシャドウコピーサービス (VSS) を使用して参加することができます。ボリュームのスナップショットに参加する Rapid Recovery (迅速な回復) の各ライターは、Excluded Writers (除外されているライター) 設定にリストされます。ライターがまたはに成功したバックアップの転送に干渉しているか、阻止している場合、これらの1つずつ無効にできます。Dell のサポート担当者によって指示された場合を除き、これらの設定をそのままにしておくことを Dell は推奨します。
- ・ **License details (ライセンスの詳細)**。これらは、特定の保護されたマシンのライセンスについての詳細です。これらの設定は、Core と Dell Data Protection | Rapid Recovery ライセンスポータル (Dell データ保護 | 迅速な回復ライセンスポータル) からの情報をレポートします。これらの設定は読み取り専用です。これらの設定を変更するには、Core とライセンスポータルの間のライセンス情報をアップデートします。詳細については、ライセンス管理者を参照します。詳細については、[Dell Data Protection | Rapid Recovery ライセンスポータル User Guide \(Dell データ保護 | 迅速な回復ライセンスポータル ユーザーガイド\)](#)を参照してください。

マシンレベルの設定を表示または変更する手順は一般的な除外されたライターとライセンス詳細については同一です。詳細については、[保護対象マシンの設定の表示と変更](#)を参照してください。

マシンの夜間ジョブを変更する手順は異なります。マシンの夜間ジョブ設定の構成方法については、[保護対象マシンの夜間ジョブのカスタマイズ](#)を参照してください。

場合によっては、保護対象マシンのデータ転送レートを調整することができます。詳細については、[転送設定の変更について](#) を参照してください。

保護対象マシンの設定の表示と変更

マシン設定は、Core で保護されるマシンの動作を決定する際に役立ちます。特定マシンの設定を変更した場合、それらの設定は Core レベルで設定されている動作よりも優先されます。

保護対象マシンの一般設定、転送設定、除外されるライターの設定、およびライセンス設定を表示および変更するには、次の手順を実行します。

① **メモ:** 夜間ジョブの設定を表示および変更する場合は、「[保護対象マシンの夜間ジョブのカスタマイズ](#)」を参照してください。

このタスクは、「[クラスタノード設定の変更](#)」の手順でもあります。

- 1 Rapid Recovery Core Console の 保護対象マシン メニューで、設定を表示または変更するマシンの IP アドレスまたはマシン名をクリックします。
選択したマシンの **サマリ** ページが表示されます。
- 2 **設定** メニューをクリックします。
設定 ページが開き、選択したマシンの設定が表示されます。必要に応じて、ページ上のどこからでも設定カテゴリを表示するには、ページの左側にある該当するハイパーリンクをクリックします。

変更する設定をクリックすると、その設定は編集可能なテキストフィールドまたはドロップダウンメニューになります。

希望する変更を各設定に加えたら、 をクリックして変更を保存し、編集モードを終了します。または、 をクリックし、保存せずに編集モードを終了します。

- 3 保護対象マシンの一般設定を変更する場合は、適切な設定をクリックし、次の表の説明に従って設定情報を入力します。

表 69. 保護対象マシンの一般設定

テキストボックス	説明
表示名	マシンの表示名を入力します。 これは、Rapid Recovery Core Console で保護対象マシンに対して表示される名前です。64 文字まで入力できます。これは、デフォルトでマシンのホスト名になります。必要に応じて、わかりやすい名前に変更できます。「 使用禁止文字 」または「 禁止語 」は使用できません。
ホスト名	マシンのホスト名を入力します。
ポート	マシンのポート番号を入力します。 このポートは、マシンと通信するために Rapid Recovery Core サービスが使用します。デフォルトポートは 8006 です。
暗号化キー	この Rapid Recovery Core に既に定義してある暗号化を、この保護対象マシンのすべてのボリュームのデータに適用する場合は、ここに暗号化キーを指定します。キーはアンロックする必要があります。暗号化キーが存在しない場合は追加できます。暗号化キーの管理の詳細については、「 暗号化キーの管理 」を参照してください。 この保護対象マシンのボリュームが暗号化されている場合は、暗号化キーを変更できます。また、 暗号化キー ドロップダウンメニューで (なし) を選択し、暗号化キーの関連付けを解除することもできます。
① メモ: 保護対象マシンで暗号化キーの適用、暗号化キーの変更、暗号化キーの関連付け解除を行うと、 Rapid Recovery によって、次のスケジュール済みスナップショットまたは強制スナップショットの実行時に新しいベースイメージが取得されます。	
リポジトリ	リカバリポイント用のリポジトリを選択します。

テキストボックス 説明

このマシンのデータを保存する、Rapid Recovery Core に設定されたリポジトリを表示します。

リポジトリボリュームはローカル（Core サーバに接続されているストレージ上）に設定するか、または CIFS 共有の場所にあるボリューム上に設定することができます。

① メモ: このページの リポジトリ 設定を変更できるのは、リカバリポイントがない場合、または前回のリポジトリが失われた場合だけです。

- 4 保護対象マシンの夜間ジョブ設定を変更する場合は、「[保護対象マシンの夜間ジョブのカスタマイズ](#)」を参照してください。
- 5 保護されている Exchange Server の Exchange 設定を変更するには、Exchange Server の設定 セクションで **マウント可否の自動チェックを有効にする** をクリックし、次の手順を実行します。

- ・ マウント可否の自動チェックを有効にするには、チェックボックスをオンにして  をクリックします。
- ・ マウント可否の自動チェックを無効にするには、チェックボックスをオフにして  をクリックします。

マウント可否の自動チェックの詳細については、「[Exchange データベースのマウント可否チェックについて](#)」を参照してください

- 6 保護対象マシンの転送設定を変更する場合は、適切な設定をクリックし、次の表の説明に従って設定情報を入力します。

① メモ: 転送設定の概念については、「[転送設定の変更について](#)」を参照してください。

表 70. 保護対象マシンの転送設定

テキストボックス 説明

 デフォルトにリストア	このコントロールは、すべての転送設定をシステムのデフォルト設定に復元します。
優先度	保護されたマシン間に転送の優先順位を設定します。他の保護対象マシンと比較して優先度を割り当てることができます。1～10（1が最も優先度が高い）の数値を選択します。デフォルトでは、優先度5が設定されます。
① メモ: 優先度はキューに入っている転送に適用されます。	
最大同時ストリーム	Core に送信される TCP リンクの保護対象マシン（DVM リポジトリで保護されているマシン）ごとの同時最大処理数を設定します。
① メモ: この値は 8 に設定することをお勧めします。パケットが破棄される場合は、この設定を増やしてください。	
最大同時書き込み	保護対象マシンに対する接続ごとの最大同時ディスク書き込みアクション数を設定します。
① メモ: 「最大同時ストリーム」に選択した値と同じ値に設定することをお勧めします。パケット損失が発生する場合は、若干少ない値に設定します。たとえば、「最大同時ストリーム」が 8 の場合は、この値を 7 に設定します。	
Core のデフォルト最大試行回数を使用する	このオプションを選択すると、操作の一部が完了しなかった場合に、各保護対象マシンのデフォルトの再試行回数を使用されます。
最大セグメントサイズ	コンピュータが1つの TCP セグメントに受信できる最大データ量（バイト単位）を指定します。デフォルト設定は 4194304 です。 Dell のサポート担当者からの指示がないかぎり、この設定をデフォルトから変更しないでください。

テキストボックス 説明

転送キューの最大深さ	同時に送信できるコマンド数を指定します。デフォルト設定は 64 です。 システムの同時入力/出力操作数が多くなる場合、この値を高い数値に調整できます。
1 ストリームあたりの未処理の読み取り	バックエンドで保存される、キューに登録済みの読み取り操作数を指定します。この設定は、保護対象マシンのキューイングを制御するのに役立ちます。デフォルト設定は 0 です。
データ転送サーバーポート	転送用のポートを設定します。デフォルト設定は 8009 です。
転送タイムアウト	パケット未転送許容時間（分と秒）を指定します。
スナップショットタイムアウト	スナップショットの取得の最大待機時間（分と秒）を指定します。
スナップショットクリーニングタイムアウト	保護対象マシンの VSS スナップショットを削除するプロセスの最大時間を分と秒で指定します。
ネットワークの読み取りタイムアウト	読み取り接続の最大待機時間（分と秒）を指定します。その時間でネットワーク読み取りを実行できない場合、操作が再試行されます。
ネットワークの書き込みタイムアウト	書き込み接続を待機する最大秒数を指定します。その時間でネットワーク書き込みを実行できない場合、操作が再試行されます。

- 7 除外されるライターの設定を変更する場合は、適切な設定をクリックし、次の表の説明に従って設定情報を入力します。

表 71. 保護対象マシンの除外されるライター設定

テキストボックス 説明

除外されるライター	除外するライターを選択します。設定するマシンに固有であるライターがリストに表示されるため、すべてのライターがリストに表示されるわけではありません。たとえば、次のようなライターが表示されます。 - ASR ライター - COM+ REGDB ライター - パフォーマンスカウンタライター - レジストリライター - シャドウコピー最適化ライター - SQL サーバーライター - システムライター - タスクスケジューラライター - VSS メタデータストアライター - WMI ライター

- 8 保護対象マシンのライセンスの詳細は、読み取り専用です。ライセンスの詳細情報については、次の表を参照してください。

表 72. 保護体操マシンのライセンスの詳細

テキストボックス	説明
有効期限日	選択した保護対象マシンのライセンスの有効期限の日付を示します。
ライセンスステータス	選択した保護対象マシンのライセンスの現在のステータスを示します。
ライセンスタイプ	選択した保護対象マシンのライセンスのタイプを示します。
Agent タイプ	現在の保護対象マシンが、物理エージェントまたは仮想エージェントであるかどうかを示します。

Hyper-V ホストまたはノードの設定の変更

この手順は、仮想マシン（VM）を保護するために Rapid Recovery 高速スナップ仮想用（エージェントレスの保護）を使用する Hyper-V のホストまたはノードに適用されます。

VM を保護するために高速スナップ仮想用（エージェントレスの保護を使用している Hyper-V ホストが、左のナビゲーション領域にホストアイコンで表示されます。  エージェントレスに保護される VM のある Hyper-V ホストの設定は、通常の保護対象マシンと同じではありません。ホストの設定に加えられるすべての変更は、そのホストの VM に適用されます。

- 1 コアコンソールの左のナビゲーション領域にある Protected Machines（保護されたマシン）で、設定を変更する Hyper-v ホストをクリックします。
ホストの **Summary（サマリ）** ページが開きます。
- 2 ホスト用のメニューバーで、**Settings（設定）** をクリックします。
Settings（設定） ページが開きます。
- 3 **General（一般）** の下で、変更したい設定をクリックします。
選択した設定が、テキストフィールドまたはドロップダウンメニューで編集可能になります。
- 4 以下の表に記載されているとおりに設定情報を入力します。

表 73. 一般設定情報

テキストボックス	説明
表示名	Rapid Recovery コアコンソールの保護対象マシンの表示名。最大 64 文字を入力できます。デフォルトでは、マシンのホスト名です。表示名を、必要に応じて、ユーザーフレンドリーな名前に変更することができます。 使用禁止文字 または 禁止語 を使用しないでください。
ホスト名	マシンのメタデータ内に表示される保護対象マシンの名前です。

- ① **メモ:** この設定を変更しないでください。変更すると、保護対象マシンと **Core** の間の接続が切断される場合があります。

- 5 **Transfer Queue（転送キュー）** の下で、ホスト上で 1 回に処理する転送ジョブの数を変更するには、**Maximum concurrent transfers（最大同時転送数）** の設定をクリックします。
① **メモ:** 最適なパフォーマンスのためには、Hyper-v ホストまたはノードの最大同時転送数をデフォルトのまま 1 に設定することをお勧めします。
- 6 **Nightly Jobs（夜間ジョブ）** の下で、利用可能な夜間ジョブの設定を変更するには、**Change（変更）** をクリックしてください。
Nightly Jobs（夜間ジョブ） ウィンドウが表示されます。
- 7 以下の表に記載されているとおりに設定情報を入力します。

表 74. Nightly Jobs（夜間ジョブ）の設定情報

テキストボックス	説明
Clear orphaned registry keys on protected Hyper-V host（保護されている Hyper-V ホストで孤立したレジストリキーをクリア）	データ転送中に仮想ディスクを接続したり、切断したりすると、結果としてレジストリから不要なファイルが削除されます。
Check integrity of recovery points（リカバリポイントの整合性をチェック）	Hyper-v ホスト上の仮想マシン用に作成された各リカバリポイントの整合性チェックを実行します。

8 **OK** をクリックします。

9 **Auto Protection（自動保護）** の下で、新しい仮想マシンが Hyper-V ホストに追加されたときにそれらを自動的に保護するかを確認するために、**Auto protect new virtual machines（新しい仮想マシンを自動保護）** の設定をクリックします。

Hyper-V の保護対象仮想マシンの設定変更

この手順は、Rapid Recovery Rapid Snap for Virtual（エージェントレス保護）を使用して保護している Hyper-V の仮想マシン（VM）に適用されます。

Rapid Snap for Virtual（エージェントレス保護）を使用して保護している Hyper-V の VM は、左のナビゲーションエリアにホストアイコン  で示されます。Hyper-V のエージェントレス VM の設定は、**設定** ページの一番下にある Hyper-V セクションの例外も含めて一般的な保護対象マシンと同じです。次のタスクでは、**Hyper-V** セクションの設定のみに適用される手順を示します。その他のすべての保護対象マシンの設定については、「[保護対象マシンの設定の表示と変更](#)」を参照してください。

- 1 Core Console の左側のナビゲーションエリアにある **保護対象マシン** で、設定を変更したい Hyper-V の VM をクリックします。VM の **サマリ** ページが表示されます。
- 2 ホストのメニューバーで、**設定** をクリックします。**設定** ページが表示されます。
- 3 左側の一覧で、**Hyper-V** をクリックします。選択した設定は、テキストフィールドまたはドロップダウンメニューとして編集できるようになります。
- 4 **Hyper-V のスナップショットの設定** をクリックします。選択した設定は、編集可能なドロップダウンメニューになります。
- 5 このドロップダウンメニューから、次の表で説明されているオプションのいずれかを選択します。

表 75. Hyper-V の設定情報

テキストボックス	説明
最初に転送中に VSS スナップショットの作成を試みて、それに失敗した場合は、チェックポイントを作成します	VSS スナップショットの作成が成功した場合、そのリカバリポイントは、アプリケーションに整合性がある状態になります。VSS スナップショットの作成に失敗してチェックポイントを作成した場合は、そのリカバリポイントは、クラッシュ整合性のある状態になります。
転送中に VSS スナップショットを作成しません	クラッシュ整合性がある状態でリカバリポイントを生成します。
転送中には、VSS スナップショットのみを使用します。VSS スナップショットの作成に失敗した場合は、全体の転送処理に失敗します	アプリケーション整合性があるリカバリポイントのみを生成します。VSS スナップショットが失敗した場合は、リカバリポイントは生成されません。

VMware 保護対象仮想マシンの vSphere 設定の変更

この手順は、Rapid Recovery Rapid Snap for Virtual によって保護（エージェントレス保護）される VMware ESXi または Workstation の仮想マシン（VM）に適用されます。

エージェントレスで保護される VMware VM の設定には、一般的な保護対象マシンと同じ設定が含まれますが、1つだけ例外があります。設定 ページの **vSphere** セクションには、エージェントレスで保護される VMware VM のみに適用される設定があります。次のタスクでは、設定 ページの **vSphere** セクションのみに使用される手順を示します。その他のすべての保護対象マシンの設定については、「[保護対象マシンの設定の表示と変更](#)」を参照してください。

- 1 Core Console の左のナビゲーションエリアの 保護対象マシン で、設定を変更する Hyper-V ホストをクリックします。
ホストの **サマリ** ページが表示されます。
- 2 ホストのメニューバーで、**設定** をクリックします。
設定 ページが表示されます。
- 3 リスト内の左側で、**vSphere** をクリックします。
選択した設定は、テキストフィールドまたはドロップダウンメニューとして編集できるようになります。
- 4 **vSphere** で、変更したい設定をクリックします。
選択した設定は、テキストフィールドまたはドロップダウンメニューとして編集できるようになります。
- 5 次の表の説明に従って、設定情報を入力します。

表 76. vSphere の設定情報

テキストボックス	説明
ユーザーが作成した VMware スナップショットの Rapid Recovery による削除を許可	デフォルト設定はいいえ です。
使用容量が不正なボリュームの転送を許可	デフォルト設定は はい です。
静止スナップショットを許可	デフォルト設定は はい です。

転送設定の変更について

Rapid Recovery では、保護対象マシンのデータ転送プロセスを管理する設定を変更できます。本項で説明する転送設定は、保護対象マシンレベルで設定されます。Core レベルでの転送を設定するには、[転送キュー設定の変更](#) を参照してください。

Rapid Recovery は、ベースおよび増分だけでなく、リストア、ベアメタルリストア、仮想マシンエクスポートを含む通常の転送を、Windows 8 および Windows Server 2012 でサポートします。

Rapid Recovery には、次の 3 つの転送タイプがあります。

- ・ **スナップショット**。保護対象マシン上のデータをバックアップします。2 種類のスナップショットが可能です。保護されたすべてのデータのベースイメージ、それから最後のスナップショット以降に更新されたデータの増分スナップショットです。この転送タイプは、Core に関連付けられているリポジトリに保存されるリカバリポイントを作成します。詳細については、[スナップショットとリカバリポイントの管理](#) を参照してください。
- ・ **Virtual Machine Export（仮想マシンのエクスポート）**。リカバリポイントからの仮想マシン（VM）を作成します。保護対象マシンのバックアップからのデータのすべてのほか、オペレーティングシステムおよびドライバ、ならびに関連付けられているデータが含まれ、VM が必ず起動できるようにします。詳細については、[VM エクスポート](#) を参照してください。
- ・ **Restore（リストア）**。保護対象マシンのバックアップ情報をリストアします。詳細については、[リカバリポイントからのボリュームの復元](#) を参照してください。

❗ **メモ:** ボリューム全体は、EFI システムパーティションを使用した **Windows** システムのリストア中に常にかき換えられます。

Rapid Recovery でのデータ転送には、保護対象マシンから Core までの、ネットワーク経由での大量のデータ転送が伴います。レプリケーションの場合、送信元またはソース Core からターゲット Core までの転送も発生します。

データ転送は、一部のパフォーマンスオプション設定を使用して、お使いのシステムに合わせた最適化を行うことができます。これらの設定により、保護対象マシンのバックアップ中、VM エクスポートの実行中、またはリストアの実行中でのデータ帯域幅の使用量が制御されます。データ転送のパフォーマンスに影響する要因には次のものがあります。

- ・ 同時エージェントデータ転送数
- ・ 同時データストリーム数
- ・ ディスク上のデータ変更量
- ・ 使用可能なネットワーク帯域幅
- ・ リポジットリディスクサブシステムのパフォーマンス
- ・ データバッファリングに使用可能なメモリ量

ビジネスニーズへの最適な対応とお使いの環境に基づいたパフォーマンスの微調整を行うために、これらのパフォーマンスオプションを調整できます。詳細については、[転送速度のスロットル](#)を参照してください。

転送速度のスロットル

バックアップデータ、またはネットワーク経由で保護対象マシンと Core 間でレプリケート済みのリカバリポイントを転送するときは、意図的に転送速度を下げるすることができます。このプロセスは、スロットルと呼ばれています。

転送速度をスロットルすると、Rapid Recovery からのファイル転送のみに使用される、ネットワーク帯域幅の量が制限されます。レプリケーションをセットアップするとき、スロットルを使用すると、レプリケートされた Core に以前のリカバリポイントを転送してネットワーク帯域幅のすべてを消費するような可能性を軽減できます。

△ 注意: 転送速度のスロットルは、必ずしも必要であったり、推奨されたりするわけではありません。この情報は、お使いの **Rapid Recovery** 環境でパフォーマンスの不具合が発生した場合に参考として使用できる、解決策の1つです。たとえば、保護対象またはレプリケートされた **Core** のデータを大量に転送したために繰り返し発生する転送障害やネットワークの速度低下に関する不具合は、スロットルによって解決されることがあります。

スロットルに最適なアプローチを特定するための要因は複数存在します。保護されているマシンのタイプは、重要な要因です。たとえば、ビジー状態の Microsoft Exchange Server の変更レートは、あまり使用されないレガシー Web サーバーよりも大幅に高くなります。

保護対象マシン上のストレージボリュームの入出力機能も、効率に大きな影響を及ぼす場合があります。

また、ネットワーク速度は、さまざまな可変要素を含む別の重要な要素です。所定のネットワークバックボーン (1GbE または 10GbE など)、アーキテクチャ、設定、意図的な NIC チューニングの使用や、使用されるケーブルのタイプさえも、すべてネットワーク転送速度に影響します。お使いの環境が低速のワイドエリアネットワークである場合、およびバックアップまたはレプリケーションの転送ジョブが失敗した場合は、これらの設定の一部を使用して転送速度をスロットルすることを検討します。

最終的に、ネットワークのスロットルプロセスでは試行錯誤が付きものです。Dell 転送設定は調整およびテストして、これらの設定がニーズを満たしているか定期的に何度も確認することをお勧めします。

転送速度の調整は、マシン単位で個別に行う必要があります。Core Console で特定のマシンに移動し、設定 を選択して転送速度を調整します。これらの設定の表示および変更に関する具体的な情報については、「[保護対象マシンの設定の表示と変更](#)」を参照してください。このトピックでは、転送のスロットルに使用される各設定に関する説明も記載しています。これらの説明は、最初に試す設定を決定する際に役立つ場合があります。

次の表では、転送速度のスロットルに関連する 4 つの主な設定について説明します。

表 77. 転送速度のスロットルに使用される、保護対象マシンの設定

Machine-Level 設定	デフォルト設定	提案されるスロットル設定
最大同時ストリーム	8	4
最大同時書き込み	8	4
最大セグメントサイズ	4194304	2097152

Dellサポートの担当者から指示されないかぎり、1 ストリームあたりの未処理の読み取りのデフォルト設定を変更する前に、他の設定を調整およびテストすることをお勧めします。この設定を調整およびテストする場合は、24 の値から開始します。

保護対象マシンの転送パラメータに制限を指定すると、ジョブごとにその制限も適用されます。2 つの転送ジョブが同時に発生したり、重複したりすると、2 倍の帯域幅が使用されます。ネットワークで 4 つの転送ジョブが重複した場合は 4 倍の帯域幅が使用され、同様に使用される帯域幅の量は増加していきます。

保護対象マシンの夜間ジョブのカスタマイズ

夜間ジョブは、Core レベルと適切な Configuration (構成) タブでのマシンレベルで設定できます。夜間とジョブの設定が Core レベルで設定され、変更内容は、その Core によって保護されているすべての関連するマシンに適用されます。マシンレベルで夜間ジョブに加えられた変更は、Core レベルでに加えられた変更より優先されます。指定されたマシンにのみ有効です。

それぞれに対して利用可能な説明と範囲を含めて、すべての夜間ジョブのリストについては、トピック [夜間ジョブの理解](#) を参照してください。

次の手順のステップを完了し、単一の保護されたマシンの夜間ジョブを変更します。

- 1 Rapid Recovery コアコンソールの Protected Machines (保護されたマシン) メニューで、夜間ジョブをカスタマイズするマシンの IP アドレスまたはマシン名をクリックします。
選択したマシンの **Summary (サマリ)** ページが表示されます。
- 2 **Settings (設定)** メニューをクリックします。
Settings (設定) ページが表示され、選択したマシンの設定が表示されます。
- 3 オプションで、**Nightly Jobs (夜間ジョブ)** リンクをクリックして、Settings (設定) ページをスクロールダウンし、夜間ジョブ設定を表示します。

- 4 Nightly Jobs (夜間ジョブ) 見出しの下で、 **Change (変更)** をクリックします。
Nightly Jobs (夜間ジョブ) ダイアログボックスが表示されます。

① **メモ:** カスタム保持ポリシーの設定を含む **Rollup (ロールアップ)** 設定については、[保護対象マシンの保持ポリシー設定のカスタマイズ](#) を参照してください。

- 5 **Nightly Jobs (夜間ジョブ)** ダイアログボックスでは、夜間に実行するジョブを選択するか、このマシンを省略するオプションをクリアします。

① **メモ:** オプションはマシンによって異なる場合があります。たとえば、**Exchange Server** を使用する保護対象マシンは、**Exchange** データベースのチェックサムを含み、**Exchange** ログを切り捨てる場合があります。

- 6 **OK** をクリックします。

① **メモ:** この手順の結果は、選択した保護対象マシンだけに適用されます。他のマシンに適用する場合には、カスタマイズするマシンごとに手順を繰り返します。**Core** に保護されるマシンすべての夜間ジョブ設定を変更するには、[Core の夜間ジョブの設定](#) を参照してください。

保護対象マシンのシステム情報の表示

Rapid Recovery Core Console では、Core で保護されているマシンに関するシステム情報に簡単にアクセスできます。

一般 ペインには、Core マシンと環境に関する一般的な情報が表示されます。**ボリューム** ペインには、Core マシンのストレージボリュームに関する情報がリストされます。**Replay エンジン** の接続 ペインでは、保護されているすべてのマシンのボリュームが表示されます。

保護対象マシンに関する詳細システム情報を表示するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動し、左側にあるナビゲーションエリアにある保護対象マシンのメニューから、保護対象マシン名をクリックします。

選択した保護対象マシンの **サマリ** ページが表示されます。

- 2 **サマリ** ページで、**サマリ** ペインの下部にある、 **システム情報** をクリックします。
- 3 **システム情報** ページでは、選択した保護対象マシンに関する次の詳細情報を表示することができます。
 - ・ **システム情報**。これには、ホスト名、OS バージョン、OS アーキテクチャ、メモリ（物理）、表示名、完全修飾ドメイン名、キャッシュメタデータの場所、一次キャッシュの場所、二次キャッシュの場所、および仮想マシンのタイプ（該当する場合）が含まれます。
 - ・ **ボリューム**。これには、ボリューム名、デバイス ID、ファイルシステム、フォーマット済み容量、使用容量、およびマウントポイントが含まれます。
 - ・ **プロセッサ**。これには、Core のアーキテクチャと番号が含まれます。
 - ・ **ネットワークアダプタ**。これには、アダプタのタイプと速度が含まれます。
 - ・ **IP アドレス**。これには、IP アドレスとシリーズが含まれます。

マシンの管理

本項では、マシンを管理する際に実行するさまざまなタスクについて説明します。次のトピックで構成されています。

- ・ [マシンの削除](#)
- ・ [保護からのクラスタの削除](#)
- ・ [マシンのライセンス情報の表示](#)
- ・ [保護対象マシンのログファイルのダウンロードと表示](#)
- ・ [保護対象クラスタノードの保護対象マシンへの変換](#)

マシンの削除

マシンを Rapid Recovery Core の保護対象から削除する際には、それまでに RR に保存されたリカバリポイントを保持するのか、リカバリポイントを削除するのかを尋ねる 2 つのオプションが提示されます。保護対象からのマシンの削除後リカバリポイントを保持する場合、そのマシンは「リカバリポイントのみ」のマシンになります。こうした現在の保護対象から削除されたマシンのリカバリポイントは、以降も引き続きマシンのリストアに使用できますが、リカバリ可能範囲は保存されたリカバリポイントで取得されている状態までに限定されます。

リカバリポイントを削除する場合は、この削除アクションによって、Rapid Recovery Core からそれまでの保護対象マシンのスナップショットデータがすべて削除されます。

△ | 注意: リカバリポイントを削除すると、そのマシンのデータをリストアできなくなります。

Rapid Recovery 環境の保護対象からマシンを削除するには、次の手順を実行します。

- 1 Rapid Recovery Core Console の左側にあるナビゲーションエリアの **保護対象マシン** で、削除するマシンをクリックします。
- 2 関連するマシンの **サマリ** ページで、**マシンを削除** をクリックします。
- 3 リポジトリからこのマシンのすべてのリカバリポイントも削除する場合は、ダイアログボックスで **リカバリポイントを含むマシンを削除** を選択します。
- 4 マシンの削除を選択したことを確認し、**はい** をクリックします。
Rapid Recovery で保護対象からそのマシンが削除され、そのマシンのアクティブなタスクがすべてキャンセルされます。

保護からのクラスタの削除

保護からクラスタを削除するには、次の手順を実行します。

- 1 Rapid Recovery Core Console の **保護対象マシン** の下にある、削除するクラスタをクリックします。
- 2 クラスタの **サマリ** ページで **クラスタを削除** をクリックします。
- 3 必要に応じて、このクラスタの、現在保存されているリカバリポイントをすべてリポジトリから削除するには、ダイアログボックスで **リカバリポイントを含むマシンを削除** を選択します。
- 4 ダイアログボックスで **はい** をクリックして確認します。

保護からのクラスタノードの削除

保護からクラスタノードを削除するには、次の手順を実行します。

クラスタからノードだけを削除したい場合は、「[保護対象クラスタノードの保護対象マシンへの変換](#)」を参照してください。

- 1 Rapid Recovery Core Console の保護対象マシンで、削除するクラスタノードをクリックします。
- 2 ノードのサマリページで **マシンを削除** をクリックします。
ノードを削除 ダイアログボックスが表示されます。
- 3 必要に応じて、このダイアログボックスで、現在このクラスタに保存されているすべてのリカバリポイントをこのリポジトリから削除するには、**リカバリポイントを含むマシンを削除** を選択します。
- 4 ダイアログボックスで、**はい** をクリックして確定します。

クラスタ内のすべてのノードの保護からの削除

クラスタ内のすべてのノードを保護から削除するには、次の手順を実行します。

△ | 注意: すべてのクラスタノードを削除すると、このクラスタも削除されます。

- 1 Rapid Recovery Core Console の保護対象マシンで、ノードを削除するクラスタをクリックします。
- 2 クラスタの サマリ ページで **保護対象ノード** をクリックします。
- 3 保護対象ノード ページで、すべてのノードを選択します。
- 4 **マシンの削除** ドロップダウンメニューをクリックし、次の表で説明されているオプションのいずれかを選択します。

表 78. 「ノードを削除」のオプション

オプション	説明
削除してリカバリポイントを維持	現在保存されているこのクラスタのすべてのリカバリポイントを維持します。
リカバリポイントを削除	現在保存されているこのクラスタのすべてのリカバリポイントをリポジトリから削除します。

- 5 ノードを削除 ダイアログボックスで、**はい** をクリックして削除を確認します。

マシンのライセンス情報の表示

保護対象マシンにインストールされた Rapid Recovery Agent ソフトウェアの現在のライセンスステータス情報を表示できます。

- 1 Rapid Recovery Core Console の 保護対象マシン の下で、変更するマシンをクリックします。
選択したマシンの **サマリ** ページが表示されます。
- 2 **設定** メニューをクリックします。
設定 ページが表示され、選択したマシンの設定が表示されます。
- 3 設定 ページで **ライセンスの付与** リンクをクリックし、スクロールダウンすると、マシン固有のライセンス設定が表示されます。
ステータス 画面が表示され、製品ライセンスの詳細が表示されます。

保護対象マシンのログファイルのダウンロードと表示

保護対象マシンでエラーまたは不具合が発生した場合は、マシンログをダウンロードして表示するか、デルサポートの担当者と Core ログを共有できます。

- 1 Core Console の左側にあるナビゲーション領域で、保護対象マシン メニューの下の矢印をクリックすると、関連する保護対象マシンの文脈依存メニューが展開されます。**より多い** までスクロールダウンしてメニューを展開し、 **Agent ログ** を選択します。
Agent ログのダウンロード ページが表示されます。
- 2 **Agent ログのダウンロード** ページ、 **ダウンロードを開始するには、ここをクリックしてください** をクリックします。

3 **AgentAppRecovery.log** を開いています ダイアログボックスで、次のいずれかを実行します。

- ・ ログファイルを開くには、**プログラムから開く** を選択し、テキストベースのログファイルを表示するアプリケーション（メモ帳など）を選択して、**OK** をクリックします。
AgentAppRecovery.log ファイルが、選択したアプリケーションで開きます。
- ・ ファイルをローカルに保存するには、**ファイルの保存** を選択して、次に **OK** をクリックします。
AgentAppRecovery.log ファイルが ダウンロード フォルダに保存されます。ファイルは、任意のテキストエディタを使用して開くことができます。

関連するリンク

[Core ログファイルのダウンロードと表示](#)

保護対象クラスタノードの保護対象マシンへの変換

Rapid Recovery では、保護対象クラスタノードを保護対象マシンに変換できます。変換後のマシンは、引き続き Core で管理されますが、クラスタの一部ではなくなります。これは、クラスタからクラスタノードを削除する必要があるが引き続き保護しておきたい場合などに便利です。

- 1 Rapid Recovery Core Console で、変換するマシンが属するクラスタに移動し、**保護対象ノード** をクリックします。
- 2 **保護対象ノード** ページで、変換する特定のノードのアクション ドロップダウンメニューをクリックし、**Agent に変換** を選択します。
- 3 マシンをクラスタに追加し直すには、マシンを選択し、アクション メニューの サマリ ページで**クラスタノードに変換** を選択して、**はい** をクリックしてアクションを確認します。

カスタムグループについて

Rapid Recovery Core Console では、左側にあるナビゲーションエリアに 保護対象マシン メニューが表示されます。ここには、Rapid Recovery Core の保護対象として追加されたすべてのマシンまたはサーバークラスタが表示されます。その下には、Core 内に対象オブジェクトが含まれているかどうかに基づいて、その他のメニューが表示される場合があります。同じ方法でカスタムグループを作成し、左側にあるナビゲーションエリアの一番下にメニュータイプとして表示することができます。

カスタムグループの主な特長は、Core オブジェクトを論理コンテナ内で一緒にグループ化できることです。これは、特定の目的（組織、コストセンター、部門、地理的地域など）で Core オブジェクトを編成および管理する場合に役立ちます。

グループを作成すると、常に1つのグループメンバー（保護対象マシンまたはサーバークラスタ、レプリケートされたマシン、またはリカバリポイントのみのマシンなど）が新しいカスタムグループに追加されます。追加されるオブジェクトは、そのグループを作成した基準点によって決定されます。また、グループにメンバーをさらに追加することもできます。その後、「[グループアクションの実行](#)」で説明されているように、そのカスタムグループの類似したすべてのメンバーに適用されるグループアクションを実行できます。

カスタムグループには、保護対象マシン、サーバークラスタ、レプリケートされたマシン、およびリカバリポイントのみのマシンを含めることができます。サーバークラスタは保護対象マシンと同じように動作しますが、サーバークラスタとそのノードは1つのエンティティのように動作する点が異なります。サーバークラスタに含まれているノードをグループに追加しようとすると、そのクラスタ全体が追加されます。

カスタムグループには類似するメンバーを含めることも、類似しないメンバーを含めることもできます。類似するメンバーでグループを作成すると、すべてのグループアクションがそのグループのすべてのメンバーに適用されます。たとえば、保護対象マシンのカスタムグループのスナップショットを強制的に作成すると、各マシンがバックアップされます。類似しないメンバーでグループを作成した場合は（保護対象マシンとレプリケートされたマシンなど）、レプリケーションの強制などのグループアクションを適用すると、そのアクションはレプリケートされたマシンにのみ適用されます。

1つ以上のグループを作成できます。1台の保護対象マシンまたはレプリケートされたマシンを、1つまたは複数のグループに組み込むことができます。このようにして、選択した任意の方法で Core 上のマシンをグループ化し、その特定のグループに対してアクションを実行できます。

各カスタムグループは、ユーザーが指定したラベル付きで左ナビゲーションエリアに表示されます。カスタムグループでは、標準的な保護対象マシンを持つグループが最初に表示されます。必要に応じて、レプリケートされたマシンが保護対象マシンの下に表示されます。リカバリポイントのみのマシンがある場合は、レプリケートされたマシンの下にリストされます。

左側にあるナビゲーションエリアに、Core で保護されている各オブジェクトが独自のメニューとして表示されます。これらのメニューの最後にはカスタムグループが表示されます。

グループにマシンを含めても、元の場所からそれが削除されることはありません。たとえば、Agent1、Agent2、および Agent3 と呼ばれる 3 台の保護対象マシンがある場合に、Agent1 を CustomGroup1 に追加すると、Agent1 は両方の場所に表示されます。

詳細については、次のトピックを参照してください。

- ・ [カスタムグループ名の変更](#)
- ・ [カスタムグループの削除](#)
- ・ [グループアクションの実行](#)
- ・ [カスタムグループ内のすべてのマシンを 1 ページに表示](#)

カスタムグループの作成

「保護されたマシン」または「レプリケートされたマシン」メニューでスクロールして、いずれかのマシンの名前の上にカーソルを合わせると矢印が表示され、ドロップダウンメニューが開きます。このメニューから、カスタムラベルを作成できます。

カスタムグループを作成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 保護対象マシン、レプリケートされたマシン、またはリカバリポイント専用メニューで、次のいずれかを実行します。
 - a メニューでマシンの上にカーソルを置きます。
 - b そのマシンのドロップダウンメニューをクリックします。
 - c 下にスクロールして「次としてラベル付け」を選択し、「新規ラベル」をクリックします。

ラベルの作成ダイアログボックスが表示されます。

- 3 **名前** フィールドで、カスタムグループの適切なラベルを入力します
そのグループの目的が伝わるように、わかりやすい名前を使用してください。たとえば、保護対象マシン、レプリケートされたマシン、およびリカバリポイントのみのマシンを部門別にグループ化するには、「Accounting Department」と入力します。このグループ名は、後で変更できます。

① **メモ:** ラベルは、50 文字以下にしてください。単語の間に単一スペースを入れることができます。カスタムグループのラベルを指定する必要があります。

- 4 ラベル名を確認したら、**OK** をクリックします。
ダイアログボックスが閉じ、カスタムグループが左側ナビゲーション領域の最後の要素として表示されます。
- 5 必要に応じて、このグループに他の保護対象マシン、レプリケートされたマシン、またはリカバリポイントのみのマシンを追加することができます。該当するメニューでマシン名に移動し、ドロップダウンメニューをクリックして下にスクロールし、**次としてラベル付け** を選択して、カスタムグループの名前をクリックします。
これで、そのグループに対してグループアクションを実行できるようになります。詳細については、「[グループアクションの実行](#)」を参照してください。

カスタムグループ名の変更

カスタムグループの名前を変更すると、ラベルのみが変更されます。マシン名は変わりません。

カスタムグループ名を変更するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 「保護されたマシン」メニューで、変更するカスタムグループまでスクロールしてカーソルを合わせます。
- 3 そのグループのドロップダウンメニューをクリックし、「編集」をクリックします。
ラベルの編集 ダイアログボックスが表示されたら、カスタムグループの名前を編集できるようになります。

- 名前フィールドで、テキストを更新するか、既存のラベルを削除して新しいラベルをまたはカスタムグループを入力します。そのグループの目的が伝わるように、わかりやすい名前を使用してください。たとえば、保護対象マシン、レプリケートされたマシン、およびリカバリポイントのみのマシンを地域別にグループ化するには、「Tokyo」と入力します。このグループ名は、後で変更できます。

① **メモ:** ラベルは、**50 文字以下**にしてください。単語の間に単一スペースを入れることができます。カスタムグループのラベルを指定する必要があります。

- ラベル名を確認したら、**OK** をクリックします。
ダイアログボックスが閉じ、更新されたカスタムグループが左側ナビゲーション領域の最後の要素として表示されます。
- 必要に応じて、このグループに他の保護対象マシン、レプリケートされたマシン、またはリカバリポイントのみのマシンを追加することができます。該当するメニューでマシン名に移動し、ドロップダウンメニューをクリックして下にスクロールし、**次としてラベル付け**を選択して、カスタムグループの名前をクリックします。

カスタムグループの削除

カスタムグループを削除するときは、「保護されたマシン」メニューからそのグループを削除します。そのグループに含まれていたマシンは削除されず、該当する標準メニューには表示されたままになります。

カスタムグループを削除するには、次の手順を実行します。

- Rapid Recovery Core Console に移動します。
- 「保護されたマシン」メニューで、削除するカスタムグループまでスクロールしてカーソルを合わせます。
- そのグループのドロップダウンメニューをクリックし、「**ラベルを削除**」をクリックします。
グループの削除を確定するかを尋ねるメッセージが表示されます。
- カスタムグループの削除を確認します。
ダイアログボックスが閉じ、ナビゲーションエリアからカスタムグループが削除されます。

グループアクションの実行

Rapid Recovery Core Console の左ナビゲーションエリアに表示されているどのグループに対しても、グループアクションを実行できます。グループに類似しないメンバーが含まれている場合（たとえば、レプリケートされたマシンとリカバリポイントのみのマシンなど）、ユーザーによって要求されたアクションは関連するグループメンバーに対してのみ実行されます。

カスタムグループに対してグループアクションを実行するには、次の手順を実行します。

- Rapid Recovery Core Console に移動します。
- 「保護されたマシン」メニューで、グループアクションを実行するカスタムグループまでスクロールしてカーソルを合わせます。
- そのグループのドロップダウンメニューをクリックし、次のようにアクションを選択します。
 - グループ内のすべての保護対象マシンに対して増分スナップショットまたはベースイメージを強制的に作成するには、必要に応じて、**強制的にスナップショットを作成** または **強制的にベースイメージを作成** をクリックします。詳細については、「[スナップショット作成の強制実行](#)」を参照してください。
 - グループ内のすべての保護対象マシンに対する保護を一時停止するには、**保護の一時停止** をクリックし、再開パラメータを指定します。詳細については、[レプリケーションの一時停止と再開](#)を参照してください。
 - 保護が一時停止されたグループ内の保護対象マシンの保護を再開するには、**保護を再開** をクリックし、再開を確定します。詳細については、[レプリケーションの一時停止と再開](#)を参照してください。
 - グループ内のすべてのオブジェクトの情報を更新するには、**メタデータを更新** をクリックします。
 - このグループ内のすべてのレプリケートされたマシンのレプリケーションを一時停止するには、**一時停止** をクリックします。詳細については、[レプリケーションの一時停止と再開](#)を参照してください。
 - レプリケーションが一時停止されたグループ内のすべてのレプリケートされたマシンのレプリケーションを再開するには、レプリケーションの下にある **再開** をクリックします。詳細については、次を参照してください。[レプリケーションの一時停止と再開](#)
 - グループ内のすべてのレプリケートされたマシンのレプリケーションを強制的に実行するには、**強制的に実行** をクリックします。詳細については、[レプリケーションの強制実行](#)を参照してください。
 - グループ内のすべてのレプリケートされたマシンのレプリケーションを削除するには、**削除** をクリックします。詳細については、[ターゲット Core からの入力方向のレプリケーションの削除](#)を参照してください。

- ・ この Core からリカバリポイントのみのマシンを削除し、リカバリポイントを破棄するには、リカバリポイントのみの下に
ある **リカバリポイントを削除** をクリックします。
- ・ (カスタムグループの場合のみ) カスタムグループのラベルを変更するには、「**編集**」を選択します。詳細については、[カスタムグループ名の変更](#)を参照してください。
- ・ (カスタムグループの場合のみ) ナビゲーションメニューからカスタムグループを削除するには、**ラベルを削除** を選択します。詳細については、[カスタムグループの削除](#)を参照してください。

カスタムグループ内のすべてのマシンを1ページに表示

カスタムグループの名前をクリックすると マシン ページに移動し、そのカスタムグループに含まれているすべてのマシンが一覧で表示されます。次に、アクション メニューからすべてのマシンに対していくつかの機能を実行したり、個々のマシンからコマンドを選択して、個別に機能を実行したりすることができます。

複数のマシンの保護について

複数のマシンの保護ウィザードを使用して、Rapid Recovery Core 上の複数の保護対象 Windows マシンを同時に追加できます。Rapid Recovery を使用してデータを保護するには、Rapid Recovery Core Console でワークステーションおよびサーバ（お使いの Exchange Server、SQL Server、Linux サーバなど）を追加する必要があります。

個々のマシンを保護する場合と同様に、複数のマシンを同時に保護する場合は、保護する各マシンに Rapid Recovery エージェントソフトウェアをインストールする必要があります。

① **メモ:** このルールの例外は、**VMware** または **ESXi** ホストで仮想マシンを保護する場合、エージェントレスの保護を使用できるということです。エージェントレスの保護の制限事項など、詳細については、「[仮想の高速スナップに対する理解](#)」を参照してください。

保護対象マシンには、リモートインストールが行えるようにセキュリティポリシーを設定しておく必要があります。

マシンに接続する場合、マシンは電源が入っており、アクセス可能な状態になっている必要があります。

Agent ソフトウェアを複数のマシンに同時に導入する方法は複数あります。たとえば、次のとおりです。

- ・ エージェントソフトウェア展開ウィザードを使用して、複数のマシンに Rapid Recovery エージェントソフトウェアをインストールできます。詳細については、「[Rapid Recovery Agent ソフトウェアの1つまたは複数のマシンへの展開](#)」を参照してください。
- ・ 複数のマシンの保護ウィザードの一部として、Rapid Recovery エージェントソフトウェアを展開できます。

複数のマシンを保護するプロセスには、詳細設定を選択した場合に実行できる省略可能な手順があります。高度なオプションとして、リポジトリ機能と暗号化があります。たとえば、既存の Rapid Recovery リポジトリを指定してスナップショットを保存したり、新しいリポジトリを作成したりできます。既存の暗号化キーを指定して（または、新しい暗号化キーを追加して）、保護しているマシンの Core に保存されるデータに適用することもできます。

環境によっては、「複数のマシンの保護」ウィザードのワークフローが若干異なる場合もあります。たとえば、保護するマシンに Rapid Recovery エージェントソフトウェアがインストールされている場合、ウィザードでエージェントソフトウェアをインストールするように求められることはありません。同様に、Core にリポジトリがすでに存在している場合、リポジトリを作成するように求められることはありません。

複数のマシンを保護する場合、設定に基づいて適切な手順に従ってください。複数のマシンを保護するために、次のオプションを参照してください。

- ・ [Active Directory ドメインの複数のマシンを保護](#)
- ・ [Vmware Vcenter/ESX\(i\) 仮想ホスト上の複数マシンの保護](#)
- ・ [手動での複数マシンの保護](#)

Active Directory ドメインの複数のマシンを保護

この手順を使用して、Active Directory ドメインの1つまたは複数のマシンを同時に保護します。

- 1 Rapid Recovery コアコンソールで、**Protect (保護)** ドロップダウンメニューをクリックし、**Protect Multiple Machines (複数のマシンの保護)** をクリックします。
Protect Multiple Machines (複数のマシンの保護) ウィザードが開きます。
- 2 ウィザードの **Welcome (ようこそ)** ページで、次のオプションのいずれかを選択します。
 - ・ 標準
 - ・ Advanced (show optional steps) (詳細 (オプションの手順を表示))
- 3 **次へ** をクリックします。
- 4 ウィザードの **Connection (接続)** ページで、**Source (ソース)** ドロップダウンリストから **Active Directory** を選択します。
- 5 次の表の説明に従ってドメイン情報とログオン資格情報を入力します。

表 79. ドメイン情報と資格情報

テキストボックス	説明
Host (ホスト)	Active Directory ドメインのホスト名または IP アドレス。
ユーザー名	ドメインへの接続に使用するユーザー名。たとえば、Administrator。または、マシンがドメイン内にある場合は、[domain name]\Administrator。
パスワード	このドメインへの接続に使用するセキュアなパスワード。

- 6 **次へ** をクリックします。
 - 7 ウィザードの **Select Machines (マシンの選択)** ページで、保護するマシンを選択します。
システムが選択した各マシンを自動的に検証します。
 - 8 **次へ** をクリックします。
Protection (保護) ページが Protect Multiple Machines (複数マシンの保護) ウィザードの横に表示された場合は、手順 11 に進みます。
エージェントソフトウェアが保護するマシンに導入されていない場合、または指定のマシンを別の理由により保護できない場合、Warnings (警告) ページに選択したマシンが表示されます。
 - 9 オプションとして、ウィザードの **Warnings (警告)** ページで、マシンを選択して、ツールバーの **Verify (確認)** をクリックすることで、任意のマシンを確認できます。
 - 10 オプションとして、**Warnings (警告)** ページで、**After Agent installation, restart the machines automatically (エージェントのインストール後にマシンを再起動)** を選択します。
- ① **メモ:** Dell は、このオプションの使用をお勧めします。保護する前に、エージェントマシンを再起動する必要があります。
- 11 ステータスがマシンが到達可能であることを表示している場合には、**Next (次へ)** をクリックして、Rapid Recovery エージェントソフトウェアをインストールします。
Protection (保護) ページが表示されます。
 - 12 ウィザードの **Protection (保護)** ページで、以下で説明する適切な保護スケジュールを選択します。
 - ・ デフォルトの保護スケジュールを使用するには、Schedule Settings (スケジュール設定) オプションで **Default protection (hourly snapshots of all volumes) (デフォルト保護 (全ボリュームの1時間ごとのスナップショット))** を選択します。
 - ・ 別の保護スケジュールを定義する場合は、Schedule Settings (スケジュール設定) オプションで、**Custom protection (カスタム保護)** を選択します。
 - 13 次のように設定を行います。
 - ・ Protect Machine (マシンの保護) ウィザードで Typical (標準) を選択し、デフォルトの保護設定を指定した場合、**Finish (終了)** をクリックして選択内容を確認し、ウィザードを閉じると、指定したマシンが保護されます。
マシンに対してはじめて保護が追加されると、保護を当初一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ (保護対象ボリューム内の全データのスナップショット) が Rapid Recovery コア上のリポジトリに転送されます。
 - ・ Protect Machine (マシンの保護) ウィザードで Typical (標準) 設定を選択し、カスタム保護を指定した場合は、**Next (次へ)** をクリックします。[カスタム保護スケジュールの作成](#) を参照してください。

- Protect Machine (マシンの保護) ウィザードの Advanced (詳細) 設定と、デフォルトの保護を選択した場合は、**Next (次へ)** をクリックして [手順 15](#) に進み、リポジトリと暗号化のオプションを設定します。
- Protect Machine (マシンの保護) ウィザードで Advanced (詳細) 設定を選択し、カスタム保護を指定した場合、**Next (次へ)** をクリックしてカスタム保護スケジュールをセットアップします。保護スケジュールのカスタマイズの詳細については、[カスタム保護スケジュールの作成](#) を参照してください。

14 **次へ** をクリックします。

15 ウィザードの **Repository (リポジトリ)** ページで、次のいずれかの操作を行います。

- リポジトリがすでにあり、既存のリポジトリで保護するためにこのマシンからデータを保存するには、次の手順を実行します。
 - Use an existing repository (既存のリポジトリを使用)** を選択します。
 - リストから既存のリポジトリを選択します。
 - 次へ** をクリックします。

Encryption (暗号化) ページが表示されます。手順 19 に進み、暗号化をオプションで定義します。

- リポジトリを作成する場合は、**Create a Repository (リポジトリを作成)** を選択してから、次の手順を完了します。
 - Repository (リポジトリ)** で、次の表の情報を入力します。

表 80. 新しいリポジトリ設定の追加

テキストボックス 説明	
Repository Name (リポジトリ名)	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは Repository (リポジトリ) という単語と、この Core のリポジトリの番号に対応する番号で構成されます。たとえば、最初のリポジトリの場合、デフォルト名は Repository 1 です。必要に応じて名前を変更します。 リポジトリ名にはスペースを含む 1 文字から 40 文字の英数字を含める必要があります。 使用禁止文字 または 禁止語 を使用しないでください。
Concurrent Operations (同時操作)	レポジトリで対応する同時要求の数を定義します。デフォルトの値は 64 です。
Comments (コメント)	オプションで、このリポジトリの説明を入力します。最大 254 文字を入力できます。たとえば、 DVM Repository 2 と入力します。

- Add Storage Location (ストレージの場所を追加)** をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。

△ 注意: リポジトリ用のストレージの場所のルート内の専用のフォルダを定義します。ルートの場所は指定しません。たとえば、**E:\.**ではなく **E:\Repository** を使用します。この手順で作成するリポジトリが後で削除された場合、リポジトリのストレージの場所にあるすべてのファイルが削除されます。ルートでお使いのストレージの場所を定義する場合は、ボリューム内のその他のすべてのファイル (たとえば、**E:**) が削除され、致命的なデータ損失が発生する可能性があります。

Add Storage Location (ストレージの場所の追加) ダイアログボックスが表示されます。

- Add Storage Location (ストレージの場所を追加)** をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。
- Storage Location (ストレージの場所)** 領域には、ストレージの場所にファイルを追加する方法を指定します。ローカルに接続されているストレージ (DAS、SAN、NAS など) を追加することを選択できます。共通インターネットファイルシステム (CIFS) の共有場所にストレージボリュームを指定することもできます。
 - Add the file on local disk (ローカルディスクにファイルを追加)** を選択して、ローカルマシンを指定し、以下の表に記載されているとおりに情報を入力します。

表 81. ローカルディスクの設定

テキストボックス	説明
Data Path (データパス)	保護されたメタデータを保存するための場所を入力します。

テキストボックス	説明

	たとえば、X:\Repository\Data と入力します。 パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。
Metadata Path (メタデータパス)	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Metadata と入力します。 パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。

または、**Add file on CIFS share (CIFS 共有にファイルを追加)** を選択して、ネットワーク共有の場所を指定し、以下の表に記載されているとおりに情報を入力します。

表 82. CIFS 共有の資格情報

テキストボックス	説明

UNC Path (UNC パス)	ネットワーク共有の場所のパスを入力します。 この場所がルートにある場合は、専用のフォルダ名（たとえば、Repository）を定義します。 パスの開始部分には \\ を使用する必要があります。パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。英字 a~z は大文字と小文字が区別されません。スペースは使用しないでください。その他の記号および句読点は使用できません。
ユーザー名	ネットワーク共有の場所にアクセスするためのユーザー名を指定します。
パスワード	ネットワーク共有の場所にアクセスするためのパスワードを指定します。

- 5 **Storage Configuration (ストレージの設定)** 領域で、**More Details (詳細)** をクリックし、次の表の説明に従ってストレージの場所の詳細を入力します。

表 83. ストレージ構成の詳細

テキストボックス	説明

サイズ	ストレージの場所のサイズまたは容量を設定します。最小サイズは 1 GB です。デフォルトは 250 GB です。次から選択できます。 - GB - TB ① メモ: 指定するサイズは、ボリュームのサイズを超えることはできません。 ストレージの場所が Windows XP または Windows 7 を使用した New Technology File System (NTFS) ボリュームの場合、ファイルサイズの上限は 16 TB です。 ストレージの場所が Windows 8 と 8.1、Windows 10、または Windows Server 2012 と 2012 R2 を使用した NTFS ボリュームの場合、ファイルサイズの制限は 256 TB です。 ① メモ: Rapid Recovery からオペレーティングシステムを検証する場合は、Windows Management Instrumentation (WMI) が対象のストレージの場所にインストールされている必要があります。
Write caching policy (ライトキャ ッシングポリシ ー)	ライトキャッシングポリシーは、リポジトリでの Windows Cache Manager の使用を制御し、さまざまな構成で最適なパフォーマンスを得られるようにリポジトリを調整します。

テキストボックス 説明

次のいずれかの値に設定します。

- ・ 点灯
- ・ オフ
- ・ 同期

デフォルトのまま On (オン) に設定すると、Windows がキャッシングを制御します。これは、Windows 10、および Windows Server 2012 以降のバージョンに対して適切です。

① **メモ:** ライトキャッシングポリシーを On (オン) に設定すると、パフォーマンスを高速化できます。Windows Server 2008 SP2 または Windows Server 2008 R2 SP2 を使用している場合、推奨の設定は Off (オフ) です。

Off (オフ) に設定すると、Rapid Recovery がキャッシングを制御します。

Sync (同期) に設定すると、Windows が同期入出力に加えてキャッシングも制御します。

セクタあたりのバイト 各セクタに包含するバイト数を指定します。デフォルト値は 512 です。

Average bytes per record (レコードあたりの平均バイト数) レコードあたりの平均バイト数を指定します。デフォルト値は 8192 です。

6 次へ をクリックします。

手順 1 で **Advanced (詳細)** オプションを選択すると、**Encryption (暗号化)** ページが表示されます。

- 16 オプションで、ウィザードの **Encryption (暗号化)** ページで、暗号化を有効にし、**Enable Encryption (暗号化を有効化)** を選択します。

Encryption key (暗号化キー) フィールドが Encryption (暗号化) ページに表示されます。

① **メモ:** 暗号化を有効にする場合は、このマシンの保護されたすべてのボリュームのデータに適用されます。設定を後で、**Rapid Recovery** コアコンソールの **Encryption Keys (暗号化キー)** ページから変更できます。暗号化についての詳細は、トピック [暗号化キーの理解](#) を参照してください。

△ **注意:** **Rapid Recovery** は、**256 ビット** キーの暗号ブロック連鎖 (**CBC**) モードで **AES 256 ビット** 暗号化を使用します。暗号化はオプションですが、暗号化キーを設定し、定義したパスフレーズを保護することを強くお勧めします。データの回復に非常に重要であることから、パスフレーズを安全な場所に保管してください。パスフレーズがないとデータは回復できません。

- 17 **Rapid Recovery** コアで既に定義されている暗号化キーを使用してこれらの保護対象マシンを暗号化するには、**Encrypt data using an existing Encryption key (既存の暗号化キーを使用してデータを暗号化)** を選択し、ドロップダウンメニューから適切なキーを選択します。

手順 19 に進みます。

- 18 Core に新しい暗号化キーを追加し、そのキーをこれらの保護対象マシンに適用する場合は、次の表の説明に従って情報を入力します。

表 84. 暗号化キーの設定

テキストボックス 説明

Name (名前)	暗号化キーの名前を入力します。 暗号化キーの名前には、1~130 文字の英数字文字を含める必要があります。バックスラッシュ、スラッシュ、パイプ、コロン、アスタリスク、引用符、疑問符、開くまたは閉じる括弧、アンパサンドまたはハッシュなどの特殊文字は使用できません。
説明	暗号化キーのコメントを入力します。

テキストボックス 説明

この情報は、コアコンソールからの暗号化キーを表示する際に、Description（説明）フィールドに表示されます。

Passphrase（パスフレーズ） アクセスの制御に使用するパスフレーズを入力します。
上記にリストされている特殊文字を避けるのが慣例です。

安全な場所にパスフレーズを記録します。Dell Support はパスフレーズを復元できません。いったん暗号化キーを作成し、1つまたは複数の保護対象マシンにそれを適用した場合、パスフレーズを失うとデータを復元できません。

パスフレーズの確認 テキストボックスに先ほど入力したパスフレーズを再度入力します。

19 **Finish（終了）** をクリックして、設定を保存し適用します。

ウィザードが閉じます。

20 **Warning（警告）** ページが表示され、選択した内容に満足したら、**Finish（完了）** を再度クリックします。

Rapid Recovery エージェントソフトウェアが必要に応じて指定したマシンに導入され、マシンが Core 上の保護に追加されます。

Vmware Vcenter/ESX(i) 仮想ホスト上の複数マシンの保護

VMware vCenter/ESX(i) 仮想ホスト上で1つまたは複数のマシンを同時に保護するために、この手順を使用します。

△ **注意:** エージェントレスの保護を使用する場合、Dell は保護を一度に 200 台という少ない仮想マシンに制限することをお勧めします。たとえば、**Protect Multiple Machines（複数のマシンの保護）** ウィザードを使用する際には 200 台より多くの VM を選択しないでください。200 台より多くの VM を保護すると、パフォーマンスが低下します。時間を置いた場合には Core がエージェントレスに保護できる VM の台数には制限がありません。たとえば、今日 200 台の VM を保護し、その翌日に別の 200 台の VM を保護することができます。

1 Rapid Recovery コアコンソールでは、**Protect（保護）** ドロップダウンメニューをクリックし、**Protect Multiple Machines（複数のマシンの保護）** をクリックします。

Protect Multiple Machines（複数のマシンの保護）ウィザードが開きます。

2 Welcome（ようこそ）ページで、次のオプションのいずれかを選択します。

- ・ 標準
- ・ Advanced（詳細）（オプションの手順を表示します）

3 次へをクリックします。

4 ウィザードの Connection（接続）ページでは、**Source（ソース）** ドロップダウンリストから **vCenter / Esx(i)** を選択します。

5 次の表の説明に従って、ホスト情報とログオン資格情報を入力します。

表 85. vCenter/ESX(i) 接続設定

テキストボックス	説明
Host（ホスト）	VMware vCenter Server/ESX(i) 仮想ホストの名前または IP アドレスを入力します。
ポート	仮想ホストへの接続に使用するポート。 デフォルト設定は 443 です。
ユーザー名	Administrator など仮想ホストへの接続に使用されるユーザー名、またはマシンが [domain name] \Administrator というドメインにある場合のユーザー名。
パスワード	この仮想ホストへの接続に使用するセキュアなパスワード。

- ・ エージェントレスの保護を使用するには、**Protect selected VMs Agentlessly（選択された VM をエージェントレスに保護）** を選択し、**vCenter/ESXi 仮想マシンを Rapid Recovery（迅速な回復）エージェントなしで保護**を参照してください。

6 Select Machines（マシンの選択）ページで、ドロップダウンメニューから次のオプションのいずれかを選択します。

- ・ 「ホストとクラスタ」
 - ・ VM およびテンプレート
- 7 マシンのリストを展開し、保護する VM を選択します。
Rapid Recovery がマシンがオフラインか VMware Tools がインストールされていないことを検出すると、通知が表示されます。
- 8 次へをクリックします。
- 9 Adjustment (調整) ページで、各マシンに対して次の形式の資格情報を入力してください。
hostname::username::password

① | **メモ:** それぞれの行に 1 つのマシンを入力します。

- 10 次へをクリックします。
Protection (保護) ページが Protect Multiple Machines (複数のマシンの保護) ウィザードの隣に表示された場合は、[手順 14](#) に進みます。
Agent ソフトウェアが保護するマシンにまだ展開されていない場合、あるいは指定のマシンのいずれかが別の理由で保護できない場合、選択されたマシンが Warning (警告) ページに表示されます。
- 11 オプションで、Warning (警告) ページで、マシンを選択してから、ツールバーの **Verify (確認)** をクリックすることで、任意のマシンを確認できます。
- 12 オプションで、Warnings (警告) ページで、**Agent のインストール後にマシンを自動的に再起動**を選択します。

① | **メモ:** Dell は、このオプションをお勧めします。保護される前に、エージェントマシンを再起動する必要があります。

- 13 ステータスが、マシンが到達可能であることを示している場合、**Next (次へ)** をクリックし、エージェントソフトウェアをインストールします。
Protection (保護) ページが表示されます。
- 14 Protection (保護) ページで、以下で説明する適切な保護スケジュールを選択します。
- ・ デフォルトの保護スケジュールを使用するには、Schedule Settings (スケジュール設定) オプションで **Default protection (hourly snapshots of all volumes) (デフォルト保護 (全ボリュームの 1 時間ごとのスナップショット))** を選択します。
 - ・ 別の保護スケジュールを定義する場合は、Schedule Settings (スケジュール設定) オプションで、**Custom protection (カスタム保護)** を選択します。
- 15 次のように設定を行います。
- ・ Protect Machine (マシンの保護) ウィザードで Typical (標準) 構成を選択し、デフォルトの保護設定を指定した場合、**Finish (終了)** をクリックして選択内容を確定し、ウィザードを閉じると、指定したマシンが保護されます。
マシンに対してはじめて保護が追加されると、保護を当初一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ (保護対象ボリューム内の全データのスナップショット) が Rapid Recovery コア上のリポジトリに転送されます。
 - ・ Protect Machine (マシンの保護) ウィザードで Typical (標準) 設定を選択し、カスタム保護を指定した場合、**Next (次へ)** をクリックしてカスタム保護スケジュールをセットアップします。保護スケジュールのカスタマイズの詳細については、[カスタム保護スケジュールの作成](#) を参照してください。
 - ・ Protect Machine (マシンの保護) ウィザードの Advanced (詳細) 設定と、デフォルトの保護を選択した場合は、**Next (次へ)** をクリックして [手順 17](#) に進み、リポジトリと暗号化のオプションを確認します。
 - ・ Protect Machine (マシンの保護) ウィザードで Advanced (詳細) 設定を選択し、カスタム保護を指定した場合、**Next (次へ)** をクリックしてカスタム保護スケジュールをセットアップします。保護スケジュールのカスタマイズの詳細については、[カスタム保護スケジュールの作成](#) を参照してください。
- 16 次へをクリックします。
- 17 **Repository (リポジトリ)** ページで、次のいずれかを実行します。
- ・ リポジトリがすでにある場合は、既存のリポジトリでの保護のため、このマシンからのデータを保存するには、次の手順を実行します。
 - 1 **Use an existing repository (既存のリポジトリを使用)** を選択します。
 - 2 リストから既存のリポジトリを選択します。
 - 3 次へをクリックします。
- Encryption (暗号化)** ページが表示されます。 [手順 18](#) へ進み、暗号化をオプションで定義します。
- ・ リポジトリを作成する場合には、**Create a Repository (リポジトリの作成)** を選択してから、次の手順を完了します。
 - 1 **Repository (リポジトリ)** で、次の表の情報を入力します。

表 86. 新しいリポジトリ設定の追加

テキストボックス 説明	
Repository Name (リポジトリ名)	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは Repository (リポジトリ) という単語と、この Core のレポジトリの数に対応する番号で構成されます。たとえば、これが最初にリポジトリの場合、デフォルト名は Repository 1 です。必要に応じて名前を変更します。 リポジトリ名はスペースを含めて 1 文字から 40 文字の英数字を含む必要があります。使用禁止文字 または 禁止語 を使用しないでください。
Concurrent Operations (同時操作)	レポジトリで対応する同時要求の数を定義します。デフォルトの値は 64 です。
Comments (コメント)	オプションで、このリポジトリの説明を入力します。最大 254 文字を入力できます。たとえば、 DVM Repository 2 と入力します。
2	Add Storage Location (ストレージの場所を追加) をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。 △ 注意: リポジトリ用のストレージの場所のルート内の専用のフォルダを定義します。ルートの場所を指定しません。たとえば、E:\ ではなく E:\Repository\ を使用します。この手順で作成しているリポジトリが後で削除された場合は、リポジトリのストレージの場所にあるすべてのファイルが削除されます。ルートでお使いのストレージの場所を定義する場合は、ボリューム内のその他のすべてのファイル (たとえば、E:\) が削除され、致命的なデータ損失が発生する可能性があります。 Add Storage Location (ストレージの場所の追加) ダイアログボックスが表示されます。
3	Add Storage Location (ストレージの場所を追加) をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。
4	Storage Location (ストレージの場所) 領域では、ストレージの場所にファイルを追加する方法を指定します。ローカルに接続されたストレージボリューム (たとえば、DAS、SAN、または NAS) を追加することを選択できます。共通インターネットファイルシステム (CIFS) 共有場所のストレージボリュームを指定することもできます。 Add the file on local disk (ローカルディスクにファイルを追加) を選択して、ローカルマシンを指定し、以下の表に記載されているとおりに情報を入力します。

表 87. ローカルディスクの設定

テキストボックス 説明	
Data Path (データパス)	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Data と入力します。 パスを指定するときは、英数字、ハイフン、およびピリオド (ホスト名とドメインを区切る場合のみ) のみを使用します。バックスラッシュ文字は、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号および句読点は使用できません。
メタデータパス	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Metadata と入力してください。 パスを指定するときは、英数字、ハイフン、およびピリオド (ホスト名とドメインを区切る場合のみ) のみを使用します。バックスラッシュ文字は、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号および句読点は使用できません。
・	または、Add file on CIFS share (CIFS 共有にファイルを追加) を選択して、ネットワーク共有の場所を指定し、以下の表に記載されているとおりに情報を入力します。

表 88. CIFS 共有の資格情報

テキストボックス	説明
UNC パス	ネットワーク共有の場所のパスを入力します。 この場所がルートにある場合は、専用のフォルダ名（たとえば、Repository）を定義します。 パスの頭に \\ を使用する必要があります。パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。英字 a~z は大文字と小文字が区別されません。スペースは使用しないでください。その他の記号および句読点は使用できません。
ユーザー名	ネットワーク共有の場所にアクセスするためのユーザー名を指定します。
パスワード	ネットワーク共有の場所にアクセスするためのパスワードを指定します。

- 5 **Storage Configuration（ストレージの設定）** 領域で、**More Details（詳細）** をクリックし、次の表の説明に従ってストレージの場所の詳細を入力します。

表 89. ストレージ構成の詳細

テキストボックス	説明
サイズ	ストレージの場所のサイズまたは容量を設定します。最小サイズは 1 GB です。デフォルトは 250 GB です。以下から選択できます。 - GB - TB ① メモ: 指定するサイズは、ボリュームのサイズを超えることはできません。 ストレージの場所が Windows XP または Windows 7 を使用した New Technology File System (NTFS) ボリュームの場合、ファイルサイズの上限は 16 TB です。 ストレージの場所が Windows 8、8.1、Windows 10、または Windows Server 2012、2012 R2 を使用した NTFS ボリュームの場合、ファイルサイズの制限は 256 TB です。 ① メモ: Rapid Recovery でオペレーティングシステムを検証する場合は、Windows Management Instrumentation (WMI) が対象のストレージの場所にインストールされている必要があります。
ライトキャッシングポリシー	ライトキャッシングポリシーは、リポジトリでの Windows Cache Manager の使用を制御し、さまざまな構成で最適なパフォーマンスを得られるようにリポジトリを調整します。 次のいずれかの値に設定します。 - 点灯 - オフ - 同期 デフォルトのに設定のまま On（オン）が設定されると、Windows がキャッシングを制御します。これは、Windows 10、および Windows Server 2012 以降のバージョンに対して適切です。 ① メモ: ライトキャッシングポリシーを On（オン）に設定すると、パフォーマンスを高速化できます。Windows Server 2008 SP2 または Windows Server 2008 R2 SP2 を使用している場合は、推奨の設定は Off（オフ）です。 Off（オフ）に設定すると、Rapid Recovery がキャッシングを制御します。 Sync（同期）に設定すると、Windows が同期入出力に加えてキャッシングも制御します。
セクタあたりのバイト	各セクタに包含するバイト数を指定します。デフォルト値は 512 です。

テキストボックス 説明

レコードあたりの レコードあたりの平均バイト数を指定します。デフォルト値は 8192 です。
平均バイト数

6 次へをクリックします。

手順 1 で **Advanced (詳細)** オプションを選択すると、**Encryption (暗号化)** ページが表示されます。

- 18 オプションで、Encryption (暗号化) ページで、暗号化を有効にするには、**Enable Encryption (暗号化を有効)** を選択します。Encryption key (暗号化キー) フィールドが Encryption (暗号化) ページに表示されます。

メモ: 暗号化を有効にする場合、このエージェントマシン上の保護対象ボリュームのデータに適用されます。**Rapid Recovery** コアコンソールの **Configuration (設定)** タブで、設定を後から変更できます。暗号化についての詳細は、トピック **暗号化キーの理解** を参照してください。

注意: **Rapid Recovery** は、**256 ビット** キーの暗号ブロック連鎖 (**CBC**) モードで **AES 256 ビット** 暗号化を使用します。暗号化はオプションですが、暗号化キーを設定し、定義したパスフレーズを保護することを強くお勧めします。データの回復に非常に重要であることから、パスフレーズを安全な場所に保管してください。パスフレーズがないとデータは回復できません。

- 19 この Rapid Recovery コアで既に定義されている暗号化キーを使用するこれらの保護されたマシンを暗号化するには、**Encrypt data using an existing Encryption key (既存の暗号化キーを使用してデータを暗号化)** を選択し、ドロップダウンメニューから適切なキーを選択します。

手順 21 に進みます。

- 20 Core に新しい暗号化キーを追加し、このキーをこれらの保護マシンに適用する場合、次の表の説明に従って情報を入力します。

表 90. 暗号化キーの設定

テキストボックス	説明
Name (名前)	暗号化キーの名前を入力します。 暗号化キーの名前には、1~130 文字の英数字文字を含める必要があります。バックスラッシュ、スラッシュ、パイプ、コロン、アスタリスク、クォーテーションマーク、クエスチョンマーク、始め括弧または閉じる括弧、アンパサンドまたはハッシュなどの特殊文字を含めることはできません。
説明	暗号化キーのコメントを入力します。 この情報は、コアコンソールから暗号化キーを表示する際に、Description (説明) フィールドに表示されます。
Passphrase (パスフレーズ)	アクセスの制御に使用するパスフレーズを入力します。 ベストプラクティスでは、上記にリストされている特殊文字が避けられます。 安全な場所ではパスフレーズを記録します。Dell Support は、パスフレーズを回復できません。いったん暗号化キーを作成し、1つまたは複数の保護対象マシンにそれを適用すると、パスフレーズを失った場合にデータを回復することはできません。
パスフレーズの確認	テキストボックスに先ほど入力したパスフレーズを再度入力します。

- 21 **Finish (終了)** をクリックして、設定を保存し適用します。

- 22 Warning (警告) ページが表示され、結果に満足の場合、**Finish (終了)** を再度クリックします。

Rapid RecoveryAgent ソフトウェアが必要に応じて指定したマシンに展開され、Core の保護にマシンが追加されます。

手動での複数マシンの保護

次の手順に従って、保護する各マシンを手動で入力します。これは、Linux マシンを保護する時などに使用されます。

- 1 Rapid Recovery Core Console で **保護** ドロップダウンメニューをクリックし、**複数のマシンを保護** をクリックします。

複数のマシンの保護ウィザードが開きます。

- 2 **ようこそ** ページで、次のいずれかのオプションを選択します。
 - ・ 標準
 - ・ 詳細 (任意指定のステップを表示)
- 3 **次へ** をクリックします。
- 4 ウィザードの **接続** ページで、**ソース** ドロップダウンリストから **手動** を選択します。
- 5 **次へ** をクリックします。
- 6 **マシンを選択** ページのダイアログボックスで、マシンの詳細情報を `hostname::username::password::port` の形式で入力します。ポート設定はオプションです。例：
`10.255.255.255::administrator::&l1@yYz90z::8006`
`abc-host-00-1::administrator::99!zU$o83r::168`
- 7 **次へ** をクリックします。

複数のマシンの保護ウィザードで、次に **保護** ページが表示された場合、**手順 11** にスキップします。

保護するマシンに Agent ソフトウェアがまだ導入されていない場合、または指定したマシンのいずれかを別の理由で保護できない場合、選択したマシンが **警告** ページに表示されます。
- 8 必要に応じて、**マシンの警告** ページで、マシンを選択してツールバーの **検証** をクリックすることでマシンを検証できます。
- 9 必要に応じて、**マシンの警告** ページで、**Agent のインストール後にマシンを自動的に再起動する** を選択します。

① **メモ:** Dell は、このオプションの選択を推奨しています。保護する前に、**Agent** マシンを再起動する必要があります。再起動すると、エージェントサービスが確実に実行され、該当する場合はマシンを保護するために適切なカーネルモジュールが使用されます。

- 10 マシンが到達可能であることがステータスで示されている場合、**次へ** をクリックして Agent ソフトウェアをインストールします。

保護 ページが表示されます。
- 11 **保護** ページで、次の説明に従って、適切な保護スケジュールを選択します。
 - ・ デフォルトの保護スケジュールを使用するには、スケジュール設定 オプションで、**デフォルト保護 (すべてのボリュームの毎時スナップショット)** を選択します。
 - ・ 別の保護スケジュールを定義するには、スケジュール設定 オプションで、**カスタム保護** を選択します。
- 12 次のように設定を続けます。
 - ・ マシンの保護 ウィザードで **一般** を選択して、デフォルトの保護を指定した場合、**終了** をクリックして選択内容を確認します。次に、ウィザードを閉じて、指定したマシンを保護します。

マシンに対してはじめて保護が追加されると、最初に保護を一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ (保護対象ボリューム内の全データのスナップショット) が Rapid Recovery Core 上のリポジトリに転送されます。
 - ・ マシン保護ウィザードで **一般** を選択して、カスタム保護を指定した場合、**次へ** をクリックします。「**カスタム保護スケジュールの作成**」を参照してください。
 - ・ マシン保護ウィザードの詳細設定と、デフォルト保護を選択した場合は、**次へ** をクリックして**手順 14** に進み、リポジトリと暗号化のオプションを設定します。
 - ・ マシン保護ウィザードで **詳細設定** を選択して、カスタム保護を指定した場合、**次へ** をクリックしてカスタム保護スケジュールを設定します。カスタム保護スケジュールの定義の詳細については、「**カスタム保護スケジュールの作成**」を参照してください。
- 13 **リポジトリ** ページで、次のいずれかを実行します。
 - ・ すでにリポジトリがあり、このマシンのデータを既存のリポジトリに保護のために格納する場合、次のいずれかの操作を実行します。
 - 1 **既存のリポジトリを使用** を選択します。
 - 2 リストから既存のリポジトリを選択します。
 - 3 **次へ** をクリックします。

暗号化 ページが表示されます。**手順 19** にスキップし、必要に応じて暗号化を定義します。
 - ・ リポジトリを作成する場合、**リポジトリを作成** を選択して、次の手順を実行します。
 - 1 **リポジトリ** で、次の表の情報を入力します。

表 91. 「新しいリポジトリを追加」の設定

テキストボックス 説明	
リポジトリ名	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは「リポジトリ」という単語と、この Core のリポジトリ番号に対応する番号で構成されます。たとえば、これが最初のリポジトリである場合、デフォルトの名前はリポジトリ 1 です。必要に応じて名前を変更します。 リポジトリの名前には、1～40 文字の英数字（スペースを含む）を入力する必要があります。「使用禁止文字」または「禁止語」は適用できません。
同時動作	レポジトリで対応する同時要求の数を定義します。デフォルト値は 64 です。
コメント	必要に応じて、このリポジトリの説明を入力します。254 文字まで入力できます。たとえば、 DVM リポジトリ 2 を入力します。

- 2 ストレージ場所の追加 をクリックして、特定のストレージの場所またはリポジトリのボリュームを定義します。このボリュームは、プライマリのストレージ場所にする必要があります。

△ **注意:** リポジトリのために、ストレージ場所のルート内に専用フォルダを定義します。ルートの場所を指定しないでください。たとえば、**E:** ではなく、**E:\Repository** を使用します。この手順で作成しているリポジトリを後で削除すると、リポジトリの保管場所にあるすべてのファイルが削除されます。ルート内にストレージ場所を定義すると、ボリューム（例：E:\）内のその他のすべてのファイルが削除され、致命的なデータロスが発生する可能性があります。

Add Storage Location（ストレージの場所の追加）ダイアログボックスが表示されます。

- 3 ストレージ場所の追加 をクリックして、特定のストレージの場所またはリポジトリのボリュームを定義します。このボリュームは、プライマリのストレージ場所にする必要があります。
 - 4 ストレージ場所 エリアでは、ストレージの場所にファイルを追加する方法を指定します。ローカルにアタッチされているストレージボリューム（直接アタッチストレージ、ストレージエリアネットワーク、またはネットワークアタッチストレージなど）を追加することができます。また CIFS（Common Internet File System）の共有の場所にあるストレージボリュームも指定できます。
- ・ **ローカルディスクにファイルを追加** を選択して、次の表の説明に従って、情報を入力します。

表 92. ローカルディスクの設定

テキストボックス 説明	
データパス	保護対象データを保存する場所を入力します。 たとえば、「X:\Repository\Data」を入力します。 パスを指定する場合には、英数字、ハイフン、ピリオド（ホスト名とドメインを区切るため）のみを使用できます。バックスラッシュ文字のみを使用して、パスでレベルを定義できます。スペースは使用できません。他の記号または句読点文字は無効です。
メタデータパス	保護対象メタデータを保存する場所を入力します。 たとえば、「X:\Repository\Metadata」を入力します。 パスを指定する場合には、英数字、ハイフン、ピリオド（ホスト名とドメインを区切るため）のみを使用できます。バックスラッシュ文字のみを使用して、パスでレベルを定義できます。スペースは使用できません。他の記号または句読点文字は無効です。

- ・ または、**CIFS 共有にファイルを追加** を選択して、次の表の説明に従って、情報を入力します。

表 93. CIFS 共有資格情報

テキストボックス 説明	
UNC パス	ネットワーク共有の場所のパスを入力します。

テキストボックス 説明

この場所がルートにある場合は、専用フォルダ名（Repository など）を定義します。

パスは「\」で開始する必要があります。パスを指定する場合には、英数字、ハイフン、ピリオド（ホスト名とドメインを区切るため）のみを使用できます。a から z までの文字では、大文字と小文字は区別されません。スペースは使用できません。他の記号または句読点文字は無効です。

ユーザー名 ネットワーク共有の場所にアクセスするためのユーザー名を指定します。

パスワード ネットワーク共有の場所にアクセスするためのパスワードを指定します。

- 5 ストレージ設定 エリアで、**詳細表示** をクリックして、次の表の説明に従って、ストレージの場所の詳細を入力します。

表 94. ストレージ設定の詳細

テキストボックス 説明

サイズ	ストレージの場所のサイズまたは容量を設定します。最小サイズは 1 GB です。デフォルトは 250 GB です。次から選択できます。 - GB - TB ① メモ: 指定するサイズは、ボリュームのサイズを超えることはできません。 ストレージの場所が、Windows XP または Windows 7 を使用する New Technology File System (NTFS) ボリュームの場合は、ファイルサイズが 16 TB に制限されます。 ストレージの場所が、Windows 8、8.1、Windows 10、Windows Server 2012、2012 R2 を使用する NTFS ボリュームの場合は、ファイルサイズが 256 TB に制限されます。 ① メモ: Rapid Recovery からオペレーティングシステムを検証する場合は、Windows Management Instrumentation (WMI) が対象のストレージの場所にインストールされている必要があります。
ライトキャッシングポリシー	ライトキャッシングポリシーは、リポジトリで Windows Cache Manager がどのように使用されるかを制御し、さまざまな設定でパフォーマンスが最適になるようにリポジトリを調整するのに役立ちます。 次のいずれかの値を指定します。 - オン - オフ - 同期化 デフォルト値である「オン」に設定すると、Windows がキャッシングを制御します。これは、Windows 10 および Windows Server 2012 以降のバージョンに適しています。 ① メモ: ライトキャッシングポリシーを「オン」に設定すると、パフォーマンスを向上できます。Windows Server 2008 SP2 または Windows Server 2008 R2 SP2 を使用している場合、推奨される設定はオフです。 オフ に設定すると、Rapid Recovery がキャッシングを制御します。 「同期化」に設定すると、Windows が同期入出力とキャッシングを制御します。
セクタあたりのバイト	各セクタに含めるバイト数を指定します。デフォルト値は 512 です。
レコードあたりの平均バイト数	1 レコードの平均バイト数を指定します。デフォルト値は 8192 です。

- 6 **次へ** をクリックします。

手順 1 で **詳細設定** オプションを選択した場合、**暗号化** ページが表示されます。

- 14 暗号化を有効にするには、**暗号化** ページで必要に応じて **暗号化の有効化** を選択します。
暗号化キー フィールドが **暗号化** ページに表示されます。

① **メモ:** 暗号化を有効にすると、このマシンのすべての保護対象ボリュームのデータに適用されます。この設定は、後で **Rapid Recovery Core Console** の **暗号化キー** ページから変更できます。暗号化の詳細については、「**暗号化キーの理解**」を参照してください。

△ **注意:** **Rapid Recovery** は、**256 ビット** キーを持つ **CBC (Cipher Block Chaining、暗号文ブロック連鎖)** モードの **AES 256 ビット** 暗号化を採用しています。暗号化の使用は任意ですが、**Dell** 暗号化キーを設定し、定義したパスフレーズを保護することを強くお勧めします。パスフレーズはデータのリカバリに欠かせない重要なものであるため、安全な場所に保存してください。パスフレーズがない場合は、データをリカバリできません。

- 15 これらの保護対象マシンを **Rapid Recovery Core** にすでに定義されている暗号化キーを使用して暗号化する場合は、**既存の暗号化キーを使用してデータを暗号化** を選択して、ドロップダウンメニューから適切なキーを選択します。

手順 17 に進みます。

- 16 **Core** に新しい暗号化キーを追加して、そのキーをこれらの保護対象マシンに適用する場合は、次の表の説明に従って情報を入力します。

表 95. 暗号化キーの設定

テキストボックス	説明
名前	暗号化キーの名前を入力します。 暗号化キーの名前には、1～130 文字の英数字を入力する必要があります。逆スラッシュ、順スラッシュ、パイプ、コロン、アスタリスク、引用符、疑問符、開き/閉じ括弧、アンパサンド、ナンバー記号などの特殊文字を含めることはできません。
説明	暗号化キーのコメントを入力します。 この情報は、 Core Console から暗号化キーを表示するときに 説明 フィールドに表示されます。
パスフレーズ	アクセスを制御するために使用されるパスフレーズを入力します。 ベストプラクティスは、上記の特殊文字を使用しないことです。 パスフレーズは安全な場所に保管してください。デルサポートでは、パスフレーズをリカバリできません。暗号化キーを作成して1つ以上の保護対象マシンに適用した後でパスフレーズを損失した場合は、データをリカバリできません。
パスフレーズの確認	直前のテキストボックスに入力したパスフレーズを再度入力します。

- 17 **終了** をクリックし、設定を保存して適用します。
ウィザードが閉じます。

- 18 **警告** ページが表示され、それでも選択に問題がない場合、**完了** をもう一度クリックします。

Rapid Recovery Agent ソフトウェアが指定したマシンに導入されます。必要に応じて、マシンは **Core** の保護対象に追加されます。

複数マシンの保護の監視

Rapid Recovery がマシンに対して保護ポリシーおよびスケジュールを適用する進捗状況を監視することができます。

Rapid Recovery Core Console で、**Rapid Recovery** の ホーム ページに移動し、 (イベント) をクリックします。

タスク、アラート、およびイベントで分類された **イベント** ページが表示されます。ボリュームの転送に応じて、ステータス、開始時刻および終了時刻が [タスク] ペインに表示されます。

ステータス (アクティブ、待機中、完了済み、キューに登録済み、失敗) でタスクをフィルタすることもできます。詳細については、「**タスクの表示**」を参照してください。

① | **メモ:** 実行を待機しているタスクのみを表示するには、待機中のタスクアイコンを選択します。

各保護対象マシンの追加中、操作が正常に行われたか、またはエラーがログされたかをリストするアラートがログされます。詳細については、「[アラートの表示](#)」を参照してください。

すべてのイベントの表示については、「[すべてのイベントの表示](#)」を参照してください。

保護対象 Exchange Server の設定と機能

Microsoft Exchange Server を Core 内で保護している場合、Rapid Recovery Core Console に追加できる設定と、実行できる追加の機能があります。

単一設定である **自動マウント可否チェックを有効にする** は、Exchange Server に関連する Core Console で使用できます。有効にすると、Exchange Server のマウント可否チェックは自動的に実行されます。この設定は、保護対象マシンのステータスが緑色（アクティブ）または黄色（一時停止）の場合に使用できます。

詳細については、「[Exchange データベースのマウント可否チェックについて](#)」を参照してください。

保護対象 Exchange Server マシンの リカバリポイント ペインから、オンデマンドでマウント可否チェックを実行することもできます。詳細については、「[Exchange データベースのマウント可否チェックの強制実行](#)」を参照してください。

Core によって保護されている Exchange Server で実行可能な機能は次のとおりです。

- **Exchange Server 資格情報の指定。** Rapid Recovery Core では、Core で Exchange Server を認証し、情報を取得できるように資格情報を設定できます。

Exchange Server の資格情報設定の詳細については、「[Exchange Server マシンの認証情報の設定](#)」を参照してください。

- **Exchange ログを切り捨て。** Exchange Server のログの切り捨てを強制実行すると、このプロセスによって使用可能な容量が特定され、保護対象 Exchange Server で容量が再利用されます。

オンデマンドでの Exchange Server ログの切り捨てに関する詳細については、「[Exchange マシンのログの切り捨ての強制実行](#)」を参照してください。このプロセスは夜間ジョブの一部として実行することもできます。

- **Exchange データベースのマウント可否チェックの強制実行。** この機能は、Exchange Server 上のすべてのデータが正常にリカバリされるように、Exchange データベースがマウント可能かどうかをチェックし、破損を検出して管理者に警告します。オンデマンドでのマウント可否チェックの強制実行の詳細については、「[Exchange データベースのマウント可否チェックの強制実行](#)」を参照してください。

スナップショットを作成するたびに自動的に実行されるように、マウント可否チェックを強制実行することもできます。マウント可否チェックの詳細については、「[Exchange データベースのマウント可否チェックについて](#)」を参照してください。

- **Exchange Server リカバリポイントのチェックサムチェックの強制実行。** この機能は Exchange データベースファイルが含まれるリカバリポイントの整合性をチェックします。

オンデマンドでのチェックサムチェックの強制実行の詳細については、「[Exchange データベースファイルのチェックサムチェックの強制実行](#)」を参照してください。

Exchange ログを切り捨て、夜間ジョブの一部としてチェックサムチェックを強制実行できます。夜間ジョブとしてスケジュール設定できるタスクの詳細については、「[夜間ジョブの理解](#)」を参照してください。夜間ジョブの設定の詳細については、「[Core の夜間ジョブの設定](#)」を参照してください。

Exchange Server マシンの認証情報の設定

ログイン認証情報を設定するためには、保護されたボリュームに Exchange Server が存在する必要があります。Rapid Recovery によって Exchange Server の存在が検知されない場合は、認証情報を設定の機能が Core Console に表示されません。

Microsoft Exchange Server 上のデータを保護すると、Rapid Recovery Core Console でログイン認証情報を設定できるようになります。

Exchange Server ごとに認証情報を設定するには、次の手順を実行します。

- 1 Rapid Recovery Core Console の左側にあるナビゲーションエリアで、認証情報を設定する保護された Exchange Server マシンを選択します。
その保護された Exchange Server の **サマリ** ページが表示されます。
- 2 ページの一番上にあるリンクから **サマリ** ページを開き、Exchange メニューの右側に表示される下向き矢印 ▼ をクリックして、表示されるドロップダウンメニューから **認証情報を設定** を選択します。
その保護された Exchange Server の **Exchange 認証情報を編集** ダイアログボックスが表示されます。
- 3 **Exchange 認証情報を編集** ダイアログボックスで、次のように認証情報を入力します。
 - a **ユーザー名** テキストフィールドで、その Exchange Server に対する権限を持つユーザーの名前を入力します。たとえば、Administrator (マシンがドメイン内にある場合は [ドメイン名]\Administrator) となります。
 - b **パスワード** テキストフィールドで、Exchange Server に接続するために指定したユーザー名に関連付けられているパスワードを入力します。
 - c 「**OK**」をクリックして、設定を確認し、ダイアログボックスを閉じます。

Exchange マシンのログの切り捨ての強制実行

ログの切り捨てを強制実行する機能を表示するには、保護対象ボリュームに Exchange データベースが存在している必要があります。Rapid Recovery によりデータベースの存在が検出されない場合は、ログの切り捨てチェックは Core Console に表示されません。

保護対象 Exchange サーバにログの切り捨てを強制実行すると、ログのサイズが縮小されます。オンデマンドでログの切り捨てを強制実行するには、次の手順を完了します。

- 1 Rapid Recovery Core コンソールの左側にあるナビゲーションエリアで、ログの切り捨てを強制する対象となる保護された Exchange サーバを選択し、次の手順を実行します。
保護対象マシンの **サマリ** タブが表示されます。
- 2 ページの一番上にある **Exchange** ドロップダウンメニューをクリックし、**ログの切り捨てを強制** を選択します。
- 3 表示されるダイアログでクリックし、ログの切り捨ての強制を実行することを確認します。
ダイアログボックスが閉じます。システムでは Exchange Server のログの切り捨てが開始されます。Toast アラートがこのタイプのイベントに対して有効になっている場合は、ログの切り捨てのプロセスが開始されているというメッセージが表示されます。

Exchange データベースのマウント可否チェックについて

Microsoft Exchange Server のバックアップをとるために Rapid Recovery を使用している場合、各スナップショットの後にすべての Exchange データベースでマウント可否チェックを実行できます。この破損検出機能は、管理者に潜在的な障害を通知し、障害が発生した場合に Exchange サーバー上のすべてのデータが正常にリカバリされるようにします。

この機能を有効または無効にするには、保護対象マシンの **設定** メニューに移動し、**自動マウント可否チェックを有効にする** オプションを はい または いいえ にそれぞれ設定します。保護対象マシンの設定の変更に関する詳細については、「[保護対象マシンの設定の表示と変更](#)」を参照してください。

マウント可否チェックは夜間設定の一部ではありません。ただし、自動マウント可否チェックを有効にした場合に、Exchange ログを切り捨ての夜間ジョブが有効になっている場合、マウント可否チェックはログの切り捨てが完了した後にトリガされます。

保護対象 Exchange Server マシンの **リカバリポイント** ペインから、オンデマンドでマウント可否チェックを実行することもできます。詳細については、「[Exchange データベースのマウント可否チェックの強制実行](#)」を参照してください。

① **メモ:** マウント可否チェックは、**Microsoft Exchange 2007、2010、および 2013** にのみ適用されます。さらに、**Rapid Recovery Agent** サービスアカウントに **Exchange** の組織の管理者役割が割り当てられている必要があります。

Exchange データベースのマウント可否チェックの強制実行

マウント可否チェックを強制実行するには、保護対象ボリュームに Exchange データベースが存在している必要があります。Rapid Recovery によりデータベースの存在が検出されない場合は、マウント可否チェック機能が Core Console に表示されません。

特定の Exchange Server リカバリポイントに対してマウント可否チェックをオンデマンドでシステムに強制実行させるには、次の手順を実行します。

- 1 Rapid Recovery Core Console の左のナビゲーション領域で、マウント可否チェックの強制実行先となる保護対象 Exchange Server マシンを選択し、**リカバリポイント** メニューをクリックします。
- 2 **リカバリポイント** ペインまで下にスクロールします。
- 3 リカバリポイント間を移動して、目的のリカバリポイントを見つけます。必要に応じて、リスト内のリカバリポイントの右側にある  の矢印をクリックしてビューを展開します。
展開されたリカバリポイント情報で、リカバリポイントに含まれている各ボリュームを確認することができます。
- 4 **リカバリポイント** ペインで、適切なリカバリポイントを表す行にある  をクリックし、ドロップダウンメニューで **マウント可否チェックを強制** を選択します。
- 5 表示されるダイアログボックスでクリックして、マウント可否チェックを強制実行することを確認します。
ダイアログボックスが閉じます。システムがマウント可否チェックを実行します。このタイプのイベントに対するトーストアラートが有効になっている場合は、マウント可否チェックの開始を示すメッセージが表示されます。

マウント可否チェックのステータスを表示する手順については、「[タスク、アラート、およびジャーナルを使用したイベントの表示](#)」を参照してください。

Exchange データベースファイルのチェックサムチェックの強制実行

チェックサムチェックを強制実行するには、保護対象ボリュームに Exchange データベースが存在している必要があります。Rapid Recovery によりデータベースの存在が検出されない場合は、チェックサムチェック機能は Core Console に表示されません。

特定の Exchange Server リカバリポイントに対してチェックサムチェックをシステムに強制実行させるには、以下の手順を行います。

- 1 Rapid Recovery Core Console の左のナビゲーション領域で、チェックサムチェックを強制実行する保護対象 Exchange Server を選択して、**リカバリポイント** メニューをクリックします。
保護対象 Exchange Server の **リカバリポイント** ページが表示されます。
- 2 **リカバリポイント** ペインにスクロールダウンします。
- 3 リカバリポイント内を移動し、目的のリカバリポイントを見つけます。必要に応じて、リスト内のリカバリポイントの右にある  矢印をクリックして表示を展開します。
展開されたリカバリポイントの情報の中に、リカバリポイントに含まれているボリュームが表示されます。
- 4 **リカバリポイント** ペインで、適切なリカバリポイントを表す行から、 をクリックし、ドロップダウンメニューから **チェックサムチェックを強制** を選択します。
- 5 表示されるダイアログでクリックし、チェックサムチェックの強制を実行することを確認します。
ダイアログボックスが閉じます。システムがチェックサムチェックを実行します。Toast アラートがこのタイプのイベントに対して有効になっている場合は、チェックサムチェックが開始されているというメッセージが表示されます。

チェックサムチェックのステータスを表示する手順に関しては、「[タスク、アラート、およびジャーナルを使用したイベントの表示](#)」を参照してください。

保護対象 SQL Server の設定と機能

Microsoft SQL Server を Core 内で保護している場合、Rapid Recovery Core Console に追加できる設定と、実行できる追加の機能があります。

単一設定 **アタッチの可否** は、SQL Server に関連する Core Console で使用できます。

Rapid Recovery Core では、SQL アタッチ可否チェックを実行して SQL データベースが含まれているリカバリポイントの整合性を確認できます。このアクションは、SQL データベースの整合性をチェックし、サポートしているすべての MDF（データ）と LDF（ログ）ファイルがバックアップスナップショットで使用できることを確認します。

以前のリリースでは、SQL アタッチ可否チェックには Core マシンに SQL Server のライセンス版が従来から必要でした。Rapid Recovery Core では、Core 上の SQL Server インスタンスまたは保護対象 SQL Server マシンのライセンス版から、SQL アタッチ可否チェックを実行できるようになりました。

アタッチ可否設定では、このチェックで使用する SQL Server のライセンス版を指定できます。アタッチの可否設定の詳細については、「[Core の SQL アタッチ可否設定の管理](#)」を参照してください。

SQL アタッチ可否の詳細については、「[SQL アタッチ可否について](#)」を参照してください。

Core によって保護された SQL Server で実行可能な機能は次のとおりです。

- ・ **SQL Server 資格情報の指定。** Rapid Recovery Core では、Core で SQL Server を認証し、情報を取得できるように資格情報を設定できます。1つの保護対象 SQL Server マシンの資格情報を設定したり、すべての保護対象 SQL Server のデフォルトの資格情報を設定したりできます。

SQL Server の資格情報設定の詳細については、「[SQL Server マシンの資格情報の設定](#)」を参照してください。

- ・ **SQL ログの切り捨て。** SQL Server のログの切り捨てを強制実行すると、このプロセスによって保護対象サーバの使用可能な容量が特定されます。このプロセスは容量を再利用しません。
オンデマンドでの SQL Server ログの切り捨てに関する詳細については、「[SQL マシンのログの切り捨ての強制実行](#)」を参照してください。

- ・ **SQL Server のアタッチ可否チェックの強制実行。** この機能は、SQL データベースの整合性をチェックし、サポートしているすべての MDF（データ）と LDF（ログ）ファイルがバックアップスナップショットで使用できることを確認します。

SQL Server のアタッチ可否チェックをオンデマンドで強制実行する方法の詳細については、「[SQL Server のアタッチ可否チェックの強制実行](#)」を参照してください。

資格情報を指定する機能の他に、前のリストに記載した各機能をオンデマンドで実行でき、Core に実行される夜間ジョブの一部として発生するように設定することもできます。夜間ジョブとしてスケジュール設定できるタスクの詳細については、「[夜間ジョブの理解](#)」を参照してください。夜間ジョブの設定の詳細については、「[Core の夜間ジョブの設定](#)」を参照してください。

SQL Server マシンの資格情報の設定

この手順を実行する前に、Rapid Recovery Core の保護対象に SQL Server マシンを追加する必要があります。保護対象マシンの詳細については、「[マシンの保護](#)」を参照してください。

Microsoft SQL Server マシン上にデータを保護すると、Rapid Recovery Core Console で単一のインスタンスまたはすべての SQL Server 用にログイン認証情報を設定できるようになります。

SQL Server ごとに認証情報を設定するには、次の手順を実行します。

- 1 Rapid Recovery Core Console の左側にあるナビゲーションエリアで、認証情報を設定する保護された SQL Server マシンを選択します。
その保護された SQL Server の **サマリ** ページが表示されます。
- 2 ページの一番上にあるリンクから **サマリ** ページを開き、SQL メニューの右側に表示される下向き矢印 ▼ をクリックして、表示されるドロップダウンメニューから次のいずれかを実行します。

- すべての SQL Server データベースインスタンスのデフォルトの認証情報を設定する場合は、**すべてのインスタンスにデフォルト認証情報を設定** をクリックして、**デフォルト認証情報を編集** ダイアログボックスで、次の手順を実行します。
 - ユーザー名** テキストフィールドで、関連付けられているすべての SQL Server に対する権限を持つユーザーの名前を入力します。たとえば、Administrator (マシンがドメイン内にある場合は [ドメイン名]\Administrator) となります。
 - パスワード** テキストフィールドで、SQL Server に接続するために指定したユーザー名に関連付けられているパスワードを入力します。
 - 「OK」** をクリックして、設定を確認し、ダイアログボックスを閉じます。
- 1つの SQL Server データベースインスタンスの認証情報を設定する場合は、保護されている SQL Server マシンの表示名をクリックし、**インスタンス認証情報の編集** ダイアログボックスで、次の手順を実行します。
 - 資格情報のタイプ (デフォルト、Windows、または SQL) を選択します
 - ユーザー名** テキストフィールドで、その SQL Server に対する権限を持つユーザーの名前を入力します。たとえば、Administrator (マシンがドメイン内にある場合は [ドメイン名]\Administrator) となります。
 - パスワード** テキストフィールドで、SQL Server に接続するために指定したユーザー名に関連付けられているパスワードを入力します。
 - 「OK」** をクリックして、設定を確認し、ダイアログボックスを閉じます。

SQL マシンのログの切り捨ての強制実行

ログの切り捨ては、SQL Server を使用するマシンで使用できます。ログの切り捨てを強制実行するには、次の手順を完了します。

① **メモ:** SQL マシンで実行する場合は、切り捨てによりディスク上の空き容量が特定されますが、ログのサイズは縮小されません。

- Rapid Recovery Core Console の左側にあるナビゲーションエリアで、ログの切り捨てを強制する対象となるマシンを選択します。
保護対象マシンの **サマリ** ページが表示されます。
- サマリ** ページ (またはこの保護対象マシンの任意のページ) から、ページの一番上にある **SQL** ドロップダウンメニューをクリックし、**ログの切り捨てを強制** を選択します。
- 「はい」** をクリックして、ログの切り捨てを強制することを確定します。

SQL アタッチ可否について

SQL アタッチ可否機能を使用すると、Rapid Recovery Core で SQL マスターデータベースファイル (.MDF ファイル) およびログデータベースファイル (.LDF ファイル) を保護対象 SQL Server のスナップショットに添付できます。スナップショットは Microsoft SQL Server のローカルインスタンスを使用してキャプチャされます。

SQL Server マシンを保護する Rapid Recovery ユーザーに関連する問題には、アタッチ可否を実行する SQL Server のインスタンス、SQL アタッチ可否の実行方法 (オンデマンドまたは夜間ジョブの一部として) などがあります。

アタッチ可否チェックにより、Core が SQL データベースの一貫性を検証でき、すべての MDF および LDF ファイルがバックアップスナップショット内に確実に存在するようになります。

アタッチ可否チェックは、必要に応じて、または夜間ジョブの一部として、特定のリカバリポイントで実行できます。

必要に応じて SQL アタッチ可否チェックを実行する場合は、「[SQL Server のアタッチ可否チェックの強制実行](#)」を参照してください。SQL アタッチ可否を、夜間ジョブ操作の指定時刻に毎日 1 回実行するには、夜間ジョブの **SQL データベースのアタッチ可否チェック** を有効にします。Core の夜間ジョブ設定の詳細については、「[Core の夜間ジョブの設定](#)」を参照してください。特定のマシンの夜間ジョブ設定の詳細については (この場合は、保護対象 SQL Server)、「[保護対象マシンの夜間ジョブのカスタマイズ](#)」を参照してください。

以前のバージョンでは、SQL アタッチ可否を使用するには、Core マシン上に Microsoft SQL Server のローカルインスタンスがインストールされ、設定されている必要がありました。Rapid Recovery Core では、Core 上の SQL Server インスタンスまたは保護対象 SQL Server マシンの SQL Server インスタンスからアタッチ可否チェックを実行できるようになりました。選択するインスタンスは、Microsoft または正規販売店から取得した完全ライセンス版の SQL Server である必要があります。Microsoft では、パッシブ SQL ライセンスの使用を認めてはいません。

指定した SQL Server インスタンスがどれであっても、すべてのアタッチ可否チェックで使用されます。アタッチ可否は Core 設定と夜間ジョブの間で同期されます。たとえば、夜間ジョブに SQL Server の Core インスタンスの使用を指定すると、オンデマンドのアタッチ可否チェックでも Core が使用されます。逆に、特定の保護対象マシン上で SQL Server インスタンスの使用を指定すると、すべてのオンデマンドと夜間のアタッチ可否チェックで保護対象マシン上のローカルインスタンスが使用されるようになります。

グローバル Core 設定の一部として使用する SQL Server インスタンスを選択します。詳細については、「[Core の SQL アタッチ可否設定の管理](#)」を参照してください。

① **メモ:** 保護対象 SQL Server マシンでアタッチ可否チェックを実行するには、**Rapid Recovery Agent** ソフトウェアがそのサーバーにインストールされている必要があります。エージェントレス保護は SQL アタッチ可否でサポートされていません。

Rapid Recovery Core でのアタッチ可否機能は、SQL Server 2005、2008、2008 R2、2012 および 2014 でサポートされています。テストの実行に使用されるアカウントは、SQL Server インスタンス上の sysadmin 役割を付与されている必要があります。

SQL Server のディスク上のストレージフォーマットは、64 ビットおよび 32 ビットの両方の環境で同じであり、アタッチ可否はどちらのバージョンでも機能します。ある環境で実行されているサーバーインスタンスからデタッチされるデータベースは、別の環境で実行されるサーバーインスタンスでアタッチできます。

① **メモ:** Core 上の SQL Server のバージョンは、SQL Server がインストールされているすべての保護対象マシンの SQL Server バージョンと同じ、またはそれ以降のバージョンである必要があります。

SQL Server のアタッチ可否チェックの強制実行

アタッチ可否検証を強制実行するには、保護対象ボリュームに SQL データベースが存在する必要があります。Rapid Recovery によりデータベースの存在が検出されない場合は、アタッチ可否検証機能が Core Console に表示されません。

特定の SQL Server リカバリポイントに対してアタッチ可否チェックをシステムに強制実行させるには、次の手順を実行します。

- 1 Rapid Recovery Core Console の左のナビゲーション領域で、アタッチ可否検証の強制実行先となる保護対象 SQL Server マシンを選択し、**リカバリポイント** メニューをクリックします。
- 2 **リカバリポイント** ペインまで下にスクロールします。
- 3 リカバリポイント間を移動して、目的のリカバリポイントを見つけます。必要に応じて、リスト内のリカバリポイントの右側にある  の矢印をクリックしてビューを展開します。
展開されたリカバリポイント情報で、リカバリポイントに含まれている各ボリュームを確認することができます。
- 4 **リカバリポイント** ペインで、適切なリカバリポイントを表す行にある  をクリックし、ドロップダウンメニューで **アタッチの可否チェックを強制** を選択します。
- 5 表示されるダイアログボックスでクリックして、アタッチ可否検証を強制実行することを確認します。
ダイアログボックスが閉じます。システムがアタッチ可否チェックを実行します。

アタッチ可否検証のステータスを表示する手順については、「[タスク、アラート、およびジャーナルを使用したイベントの表示](#)」を参照してください。

仮想の高速スナップに対する理解

Rapid Recovery エージェントソフトウェアをインストールすることにより、Rapid Recovery コア上の物理マシンまたは仮想マシンを保護できます。サポートされるオペレーティングシステムは、トピック“Rapid Recovery Agent software requirements (迅速な回復エージェントソフトウェアの要件)”に示されています。

Rapid Recovery は、マシンの保護のための現時点での別のアプローチを提供します。

Rapid Recovery の Rapid Snap for Virtual 機能は、エージェントレスな保護としても知られています。この機能を利用すると、VM ごとに Rapid Recovery エージェントをインストールせずに、VMware ESXi 上の仮想マシン (VM) または Hyper-V ホストを保護できます。

注意: Dell は保護を一度に 200 台という少ない仮想マシンに制限することをお勧めします。たとえば、**Protect Multiple Machines** (複数のマシンの保護) ウィザードを使用する際には 200 台より多くの VM を選択しないでください。200 台より多くの VM を保護すると、パフォーマンスが低下します。時間を置いた場合には **Core** がエージェントレスに保護できる VM の台数には制限がありません。たとえば、今日 200 台の VM を保護し、その翌日に別の 200 台の VM を保護することができます。

vCenter/ESXi VM の保護

Rapid Recovery を利用すると、Rapid Recovery エージェントを VM または ESXi のホストにインストールせずに、vCenter/ESXi VM を保護し、エージェントレスな保護を受けることができます。ESXi 環境を保護するために、Rapid Recovery コアは、VMware にネイティブなスナップショットテクノロジーと連携します。

Rapid Recovery のエージェントレスな保護は、ESXi クライアントと既存のアプリケーションプログラムインタフェース (API) を使用し、Rapid Recovery エージェントソフトウェアをインストールせずに、単一のホスト上の選択された VM を保護します。次に、Rapid Recovery コアが、保護対象ボリュームの必要な詳細情報を確認するために仮想マシンディスク (VMDK) と通信します。Rapid Recovery が VMDK ではなくボリュームに基づいてリカバリポイントを作成するため、各ボリュームを個別にマウントし、リストアし、エクスポートすることができます。

メモ: Rapid Recovery は、VMware Tools を vSphere または ESXi ホストで保護する仮想マシン (VM) 上にインストールすることをお勧めします。Windows オペレーティングシステム (OS) を使用して VMware Tools を VM にインストールすると、Rapid Recovery コアがキャプチャするバックアップが、Microsoft Volume Shadow Services (VSS) を使用します。または、VMware Tools がある場合、ない場合のエージェントレスの VM の動作の詳細については、[エージェントレス保護のために VMware ツールをインストールする利点](#) を参照してください。

エージェントレスの保護は、VMware Changed Block Tracking (CBT) も使用し、増分スナップショットに必要な時間を削減します。CBT は、VMDK ファイル内のどのブロックが変更されるかを決定し、Rapid Recovery が最後のスナップショット以降に変更されたディスクの部分のみをバックアップするようにします。このバックアップ方法により、バックアップオペレーションが短縮化され、ネットワークとストレージのエLEMENTのリソース消費が削減されることがよくあります。

エージェントレスの保護の利用には複数の利点があります。最も便利な属性には、次の特性が含まれます。

- ・ ホストマシン上に追加のソフトウェアは必要ありません。
- ・ エージェントレスの保護を利用すると、ESXi ホストに追加される新しい VM を自動的に保護することを選択できます。
- ・ 再起動は、保護プロセス中に必要はありません。
- ・ 資格情報は、それぞれの VM に必要はありません。
- ・ エージェントレスの保護を利用すると、電源がオフの場合でも、VM を保護できます。
- ・ エージェントレスの保護を利用すると、ディスクにリストアを行うことができます。
- ・ エージェントレスの保護は、転送中にボリュームの空き領域は必要ありません。
- ・ エージェントレスの保護は、すべてのゲストオペレーティングシステムをサポートします。
- ・ エージェントレスの保護を利用すると、ダイナミックディスクまたはボリュームをエクスポートできます。

メモ: ダイナミックボリュームが複雑 (ストライピング、ミラーリング、スパニング、または RAID) な場合、それらはディスクイメージとしてエクスポートされ、エクスポート操作がエクスポートされた VM で完了した後にボリュームに解析されません。

ESXi の VM のためにエージェントレスの保護を使用するか理由は多数ありますが、お使いの環境およびビジネスニーズに最適な保護方法を選択してください。エージェントレスの保護を選択する際には、前述の利点に加えて、次の点にも留意してください。

- ・ エージェントレスの保護は、ボリュームレベルでのダイナミックボリューム (たとえば、スパニング、ストライピング、ミラーリング、または RAID ボリューム) の保護をサポートしません。ディスクレベルでそれらを保護します。
- ・ エージェントレスの保護は Live Recovery (ライブリカバリ) をサポートしません。この機能の詳細については、[Live Recovery について](#) を参照してください。
- ・ 保護対象 VM への単一ボリュームのリストアをそれぞれ行った後、仮想マシンを再起動する必要があります。

- ・ エージェントレスの保護は Microsoft SQL や Microsoft Exchange のメタデータを収集しません。
- ・ エージェントレスの保護対象マシンでキャプチャされたリカバリポイントでは、SQL アタッチ可否チェック、ログの切り捨て、マウント可否チェックを実行できません。
- ・ エージェントレスの保護は、ボリュームラベルまたはドライブ文字を収集せず、表示もしません。
- ・ エージェントレスの保護は、仮想ディスクの種類がシックプロビジョン Eager Zeroed 場合、VM で使用される実際の容量を表示しません。

お使いの ESXi の VM のためにエージェントレスの保護の使用を選択した場合は、エージェントレスの保護のために次の最小要件を正常に満たしている必要があります。

- ・ ホストマシンが、ESXi バージョン 5.0.0 ビルド 623860 またはそれ以降を実行している必要があります。
- ・ ホストマシンは、*Rapid Recovery* インストールおよびアップグレードガイドに記載されている最小システム要件を満たす必要があります。
- ・ ボリュームレベルの保護の場合は、VMDK がマスターブートレコード (MBR) パーティションテーブルまたは GUID パーティションテーブル (GPT) を含める必要があります。これらのパーティションテーブルなしの VMDK は個々のボリュームではなくディスク全体として保護されます。
- ・ 各 VMware 仮想マシンには VMware Tools をインストールし、スナップショット整合性を確保する必要があります。

Hyper-V サーバーおよびクラスタの保護

Hyper-V サーバーをエージェントレスに保護するために、Rapid Recovery エージェントを VM にインストールする必要はありません。ホストマシンまたはクラスタノードにインストールする必要があるだけです。エージェントはホスト上の仮想ハードディスクを保護し、ファイルシステムに応じてハードディスクファイルへ加えられた変更をボリュームイメージまたはディスクイメージへ変換します。新しいドライバは、ホストとクラスタ共有ボリューム (CSV) の VM に対するファイルレベルのサポートを提供します。

❶ **メモ:** Rapid Recovery は、VHDx ディスクファイル形式をサポートしています。VHD 形式はサポートしていません。

CSV の VM を保護するには、Rapid Recovery エージェントとドライバーを、Protect Multiple Machines (複数のマシンの保護) ウィザードの自動導入機能を使用して、各クラスターノードにインストールする必要があります。ノードから、エージェントは CSV で動作しているすべての VM を、各ファイルの変更の 2 つのタイプを作成することにより保護できます。変更の最初のタイプは、スナップショットまたはクリーンなシステムの再起動の前または後にのみ保存されます。変更の 2 番目のタイプは、ディスク上のもので、電源障害またはダーティシャットダウンがある場合でも増分スナップショットが利用可能です。ノードにインストールされているエージェントは、データを転送する前に変更のすべてを 1 つにマージします。

ホストまたはノードが実行中の場合、Rapid Recovery はアプリケーションの一貫性があるバックアップを作成します。ホストが実行していない場合は、バックアップは作成できません。しかし、ノードの 1 つが実行されていない場合、Rapid Recovery がクラスタ上の VM のスナップショットを取り続けることができます。

❶ **メモ:** 最適なパフォーマンスのためには、Hyper-V ホストまたはノードの最大同時転送数を 1 に設定することをお勧めします。これがデフォルトの設定です。

エージェントレスの Hyper-V の保護には、従来の保護機能と同等の機能があります。この機能では、各 VM にエージェントがインストールされていて、次のものが含まれます。

- ・ アーカイブ作成
- ・ リカバリポイントの整合性をチェック
- ・ マウントリカバリポイント
- ・ 新しい仮想マシンの自動検出 (エージェントレスの保護に一意)
- ・ レプリケーション
- ・ VM のリストア
- ・ CSV のリストア
- ・ VHDx 形式を使用する CIFS のリストア
- ・ ゲスト VHDx 形式でのファイルのリストア
- ・ Rollup (ロールアップ)

- ・ Hyper-v VM および他のハイパーバイザーへの仮想エクスポート。ESXi、VMware Workstation、および VirtualBox も含まれます。

ただし、エージェントレスの Hyper-V の保護を選択する際に考慮しなければならない制限事項があります。実行されない機能には次のものが含まれます。

- ・ Exchange のマウント整合性チェック
- ・ SQL のアタッチ可否チェック
- ・ Live Recovery
- ・ VHD 形式を使用した CIFS の VM のリストア
- ・ ゲスト VHD 形式のファイルのリストア

① **メモ:** アプリケーションの一貫スナップショットの場合、各 VM に SCSI コントローラをインストールする必要があります。このコントローラがないと、結果は常に、クラッシュコンシステントのスナップショットになります。

エージェントレス保護のために VMware ツールをインストールする利点

Rapid Recovery Agent を使用せずに仮想マシン (VM) を保護する場合、Dell では vSphere または ESXi ホスト上で保護対象 VM に VMware ツールをインストールし、Microsoft Volume Shadow Services (VSS) 機能をフル活用することをお勧めします。

エージェントレス保護は VMware にネイティブのスナップショットテクノロジーを使用して保護対象データをバックアップします。VMware ツールが Windows オペレーティングシステム (OS) 搭載の VM にインストールされると、Rapid Recovery Core でキャプチャされるバックアップは VSS も使用できます。VMware ツールがインストールされていない場合でも Rapid Recovery はスナップショットを収集しますが、VMware ツールがないと保護対象 VM 上のデータの状態に悪影響を及ぼす場合があります。

可能なデータの状態には次の 2 つがあります。

- ・ **クラッシュの整合性:** VM OS は起動し、ファイルシステムを読み込んで認識できます。
- ・ **アプリケーション整合性:** VM OS は起動し、ファイルシステムを読み込んで認識できます。また、トランザクションアプリケーションのファイルは整合性がとれた状態です。たとえば、SQL Server ではログがデータベースファイルと一致し、迅速かつ容易にデータベースが表示されます。

クラッシュ整合性状態からトランザクションアプリケーションをリカバリすると、データベースは最後に有効であった状態に戻ります。この場合の最新の有効な状態は、クラッシュ時、またはクラッシュより前の時点の状態です。状態が前の時点の場合、ログにある情報とデータファイルが一致するように、データベースで一部の作業をロールフォワードする必要があります。データベースを初めて表示する際は、この処理にしばらく時間がかかり、マシンの起動時に遅延が発生します。

次の条件は、VMware ツールがインストールされているかどうか、VM の電源がオンの状態かどうかに基づいて適用されます。

表 96. VM のバックアップタイプの条件

VMware ツール	VM の電源オン	Backup Type (バックアップのタイプ)
未インストール	はい	クラッシュ整合性
未インストール	いいえ (ダーティシャットダウン)	クラッシュ整合性
未インストール	いいえ (クリーンシャットダウン)	アプリケーション整合性
取り付け済み	はい	アプリケーション整合性
取り付け済み	いいえ (ダーティシャットダウン)	クラッシュ整合性
取り付け済み	いいえ (クリーンシャットダウン)	アプリケーション整合性

vCenter/ESXi 仮想マシンを Rapid Recovery (迅速な回復) エージェントなしで保護

次の手順を完了して ESXi 仮想マシンをエージェントレスに保護します。

① **メモ:** **Rapid Recovery** (迅速な回復) は、**VMware Tools** を **vSphere** または **ESXi** ホストで保護する仮想マシン (VM) にインストールすることをお勧めします。**Windows** オペレーティングシステム (OS) を使用して **VMware Tools** が VM にインストールされると、**Rapid Recovery** (迅速な回復) コアがキャプチャするバックアップが、**Microsoft** ボリュームシャドウコピーサービス (VSS) を使用します。**VMware Tools** のあるまたはないエージェントレス VM の動作の詳細については、[エージェントレス保護のために VMware ツールをインストールする利点](#) を参照してください。

△ **注意:** **Dell** は、エージェントレスの保護を一度に 200 以下の VM に制限することをお勧めします。たとえば、**Protect Multiple Machines** (複数のマシンの保護) ウィザードを使用している場合に 200 以上の VM を選択しないでください。200 より多くの VM を保護すると、結果としてパフォーマンスが低下する場合があります。時間を置いた場合、**Core** がエージェントレスに保護できる VM の数には制限がありません。たとえば、200 の VM は今日保護して、別の 200 の VM を次の日に保護することができます。

- 1 **Rapid Recovery** (迅速な回復) コアコンソールで、**Protect (保護)** ドロップダウンメニューをクリックし、**Protect Multiple Machines** (複数のマシンの保護) をクリックします。
Protect Multiple Machines (複数のマシンの保護) ウィザードが開きます。
- 2 **Welcome** (ようこそ) ページで、次のオプションのいずれかを選択します。
 - ・ 標準
 - ・ Advanced (show optional steps) (詳細 (オプションの手順を表示))
- 3 **次へ** をクリックします。
- 4 ウィザードの **Connection** (接続) ページで、**Source** (ソース) ドロップダウンリストから **vCenter / ESX(i)** を選択します。
- 5 次の表の説明に従ってホスト情報とログオン資格情報を入力します。

表 97. vCenter/ESX(i) 接続設定

テキストボックス	説明
Host (ホスト)	VMware vCenter Server/ESX(i) 仮想ホストの名前または IP アドレス。
ポート	仮想ホストへの接続に使用するポート。 デフォルト設定は 443 です。
ユーザー名	仮想ホストへの接続に使用するユーザー名。たとえば、Administrator。または、マシンがドメイン内にある場合は、[domain name]\Administrator。
パスワード	この仮想ホストへの接続に使用するセキュアなパスワード。

- 6 **Protect selected VMs Agentlessly** (選択された VM をエージェントレスに保護) が選択されていることを確認します。(このオプションはデフォルトで選択されます)。
- 7 **Select Machines** (マシンの選択) ページで、保護する VM を選択します。ドロップダウンメニューを使用して、ホストおよびクラスタのリストを表示するか、VM およびテンプレートのリストを表示できます。

① **メモ:** **VMware Changed Block Tracking (CBT)** (VMware がブロック追跡を変更 (CBT)) を保護する各 VM で有効にする必要があります。これが有効でない場合は、**Rapid Recovery** (迅速な回復) が自動的に CBT を有効にし、確実に保護を行います。

- 8 新しい VM を自動的に保護する場合は、ホストにこれらを追加する際に、**Auto protect new machines** (新しいマシンの自動保護) を選択し、次の手順を完了します。
 - a **次へ** をクリックします。
 - b **Auto Protection** (自動保護) ページで、新しいマシンを追加する任意のコンテナを選択します。
- 9 **次へ** をクリックします。
- 10 **Protection** (保護) ページで、次の保護スケジュールのいずれかを適切なものとして選択します。
 - ・ デフォルトの保護スケジュールを使用するには、Schedule Settings (スケジュール設定) オプションで **Default protection (hourly snapshots of all volumes)** (デフォルト保護 (全ボリュームの 1 時間ごとのスナップショット)) を選択します。
 - ・ 別の保護スケジュールを定義する場合は、Schedule Settings (スケジュール設定) オプションで、**Custom protection (カスタム保護)** を選択します。
- 11 次のように設定を行います。
 - ・ Typical (標準) を選択し、デフォルトの保護設定を指定した場合、**Finish** (終了) をクリックして選択内容を確定し、ウィザードを閉じると、指定したマシンが保護されます。

マシンに対してはじめて保護が追加されると、保護を当初一時停止するように指定していない限り、定義したスケジュールに従ってベースイメージ（保護対象ボリューム内の全データのスナップショット）が Rapid Recovery（迅速な回復）コア上のリポジトリに転送されます。

- Typical（標準）設定を選択し、カスタム保護を指定した場合、**Next（次へ）** をクリックしてカスタム保護スケジュールをセットアップします。保護スケジュールのカスタマイズの詳細については、[カスタム保護スケジュールの作成](#) 参照してください。
- Protect Machine（マシンの保護）ウィザードの Advanced（詳細）設定と、デフォルトの保護を選択した場合は、**Next（次へ）** をクリックして [手順 13](#) に進み、リポジトリと暗号化のオプションを設定します。
- Protect Machine（マシンの保護）ウィザードで Advanced（詳細）設定を選択し、カスタム保護を指定した場合、**Next（次へ）** をクリックしてカスタム保護スケジュールをセットアップします。保護スケジュールのカスタマイズの詳細については、[カスタム保護スケジュールの作成](#) を参照してください。

12 **次へ** をクリックします。

13 **Repository**（リポジトリ）ページでは、次の内容を実行します。

- リポジトリがすでにあり、既存のリポジトリで保護するためにこのマシンからデータを保存するには、次の手順を実行します。
 - 1 **Use an existing repository**（既存のリポジトリを使用）を選択します。
 - 2 リストから既存のリポジトリを選択します。
 - 3 **次へ** をクリックします。

Encryption（暗号化）ページが表示されます。[手順 19](#) に進み、暗号化をオプションで定義します。

- リポジトリを作成する場合は、**Repository**（リポジトリ）を選択してから、次の手順を完了します。
 - 1 **Repository**（リポジトリ）で、次の表の情報を入力します。

表 98. 新しいリポジトリ設定の追加

テキストボックス 説明	
Repository Name (リポジトリ名)	リポジトリの表示名を入力します。 デフォルトでは、このテキストボックスは Repository（リポジトリ）という単語と、この Core のリポジトリの番号に対応する番号で構成されます。たとえば、最初のリポジトリの場合、デフォルト名は Repository 1 です。必要に応じて名前を変更します。 リポジトリ名にはスペースを含む 1 文字から 40 文字の英数字を含める必要があります。 使用禁止文字 または 禁止語 を使用しないでください。
Concurrent Operations (同時操作)	レポジトリで対応する同時要求の数を定義します。デフォルトの値は 64 です。
Comments (コメント)	オプションで、このリポジトリの説明を入力します。最大 254 文字を入力できます。たとえば、 DVM Repository 2 と入力します。

- 2 **Add Storage Location**（ストレージの場所を追加）をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。

△ 注意: リポジトリ用のストレージの場所のルート内の専用のフォルダを定義します。ルート場所は指定しません。たとえば、E:\ではなく **E:\Repository** を使用します。この手順で作成するリポジトリが後で削除された場合、リポジトリのストレージの場所にあるすべてのファイルが削除されます。ルートでお使いのストレージの場所を定義する場合は、ボリューム内のその他のすべてのファイル（たとえば、E:\）が削除され、致命的なデータ損失が発生する可能性があります。

Add Storage Location（ストレージの場所の追加）ダイアログボックスが表示されます。

- 3 **Add Storage Location**（ストレージの場所を追加）をクリックして、リポジトリ用の特定のストレージの場所またはボリュームを定義します。このボリュームはプライマリのストレージの場所にする必要があります。
- 4 **Storage Location**（ストレージの場所）領域には、ストレージの場所にファイルを追加する方法を指定します。ローカルに接続されているストレージ（DAS、SAN、NAS など）を追加することを選択できます。共通インターネットファイルシステム（CIFS）の共有場所にストレージボリュームを指定することもできます。
 - **Add the file on local disk**（ローカルディスクにファイルを追加）を選択して、ローカルマシンを指定し、以下の表に記載されているとおりに情報を入力します。

表 99. ローカルディスクの設定

テキストボックス	説明
Data Path (データパス)	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Data と入力します。 パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。
Metadata Path (メタデータパス)	保護されたメタデータを保存するための場所を入力します。 たとえば、X:\Repository\Metadata と入力します。 パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。バックスラッシュは、パスのレベルを定義する場合のみ使用できます。スペースは使用しないでください。他の記号または句読点は許可されていません。

または、**Add file on CIFS share (CIFS 共有にファイルを追加)** を選択して、ネットワーク共有の場所を指定し、以下の表に記載されているとおりに情報を入力します。

表 100. CIFS 共有の資格情報

テキストボックス	説明
UNC Path (UNCパス)	ネットワーク共有の場所のパスを入力します。 この場所がルートにある場合は、専用のフォルダ名（たとえば、Repository）を定義します。 パスの開始部分には \\ を使用する必要があります。パスを指定するとき、英数字、ハイフン、およびピリオド（ホスト名とドメインを区切る場合のみ）のみを使用します。英字 a~z は大文字と小文字が区別されません。スペースは使用しないでください。その他の記号および句読点は使用できません。
ユーザー名	ネットワーク共有の場所にアクセスするためのユーザー名を指定します。
パスワード	ネットワーク共有の場所にアクセスするためのパスワードを指定します。

- 5 **Storage Configuration (ストレージの設定)** 領域で、**More Details (詳細)** をクリックし、次の表の説明に従ってストレージの場所の詳細を入力します。

表 101. ストレージ構成の詳細

テキストボックス	説明
サイズ	ストレージの場所のサイズまたは容量を設定します。最小サイズは 1 GB です。デフォルトは 250 GB です。次から選択できます。 - GB - TB ① メモ: 指定するサイズは、ボリュームのサイズを超えることはできません。 ストレージの場所が Windows XP または Windows 7 を使用した New Technology File System (NTFS) ボリュームの場合、ファイルサイズの上限は 16 TB です。 ストレージの場所が Windows 8 と 8.1、Windows 10、または Windows Server 2012 と 2012 R2 を使用した NTFS ボリュームの場合、ファイルサイズの制限は 256 TB です。

- ① **メモ:** **Rapid Recovery** (迅速な回復) からオペレーティングシステムを検証する場合は、**Windows Management Instrumentation (WMI)** が対象のストレージの場所にインストールされている必要があります。

Write caching policy (ライトキャッシングポリシー)
ライトキャッシングポリシーは、リポジトリでの Windows Cache Manager の使用を制御し、さまざまな構成で最適なパフォーマンスを得られるようにリポジトリを調整します。次のいずれかの値に設定します。

- ・ 点灯
- ・ オフ
- ・ 同期

デフォルトのまま On (オン) に設定すると、Windows がキャッシングを制御します。これは、Windows 10、および Windows Server 2012 以降のバージョンに対して適切です。

- ① **メモ:** ライトキャッシングポリシーを On (オン) に設定すると、パフォーマンスを高速化できます。**Windows Server 2008 SP2** または **Windows Server 2008 R2 SP2** を使用している場合、推奨の設定は Off (オフ) です。

Off (オフ) に設定すると、Rapid Recovery (迅速な回復) がキャッシングを制御します。

Sync (同期) に設定すると、Windows が同期入出力に加えてキャッシングも制御します。

セクタあたりのバイト
各セクタに包含するバイト数を指定します。デフォルト値は 512 です。

Average bytes per record (レコードあたりの平均バイト数)
レコードあたりの平均バイト数を指定します。デフォルト値は 8192 です。

6 次へをクリックします。

手順 1 で **Advanced** (詳細) オプションを選択すると、**Encryption** (暗号化) ページが表示されます。

- 14 オプションで、Encryption (暗号化) ページで、暗号化を有効にし、**Enable Encryption** (暗号化を有効化) を選択します。Encryption key (暗号化キー) フィールドが Encryption (暗号化) ページに表示されます。

- ① **メモ:** 暗号化を有効にする場合は、このマシンの保護されたすべてのボリュームのデータに適用されます。設定を後で、**Rapid Recovery** (迅速な回復) コアコンソールの **Configuration** (設定) タブから変更できます。暗号化についての詳細は、トピック **暗号化キーの理解** を参照してください。

- △ **注意:** **Rapid Recovery** (迅速な回復) は、**256 ビット** キーの暗号ブロック連鎖 (CBC) モードで **AES 256 ビット** 暗号化を使用します。暗号化はオプションですが、暗号化キーを設定し、定義したパスフレーズを保護することを強くお勧めします。データの回復に非常に重要であることから、パスフレーズを安全な場所に保管してください。パスフレーズがないとデータは回復できません。

- 15 **Rapid Recovery** (迅速な回復) コアで既に定義されている暗号化キーを使用してこれらの保護対象マシンを暗号化するには、**Encrypt data using an existing Encryption key** (既存の暗号化キーを使用してデータを暗号化) を選択し、ドロップダウンメニューから適切なキーを選択します。

手順 17 に進みます。

- 16 Core に暗号化キーを追加し、そのキーをこれらの保護対象マシンに適用する場合は、次の表の説明に従って情報を入力します。

表 102. 暗号化キーの設定

テキストボックス 説明

Name (名前) 暗号化キーの名前を入力します。

テキストボックス 説明

暗号化キーの名前には、1~130 文字の英数字文字を含める必要があります。バックスラッシュ、スラッシュ、パイプ、コロン、アスタリスク、引用符、疑問符、開くまたは閉じる括弧、アンパサンドまたはハッシュなどの特殊文字は使用できません。

説明

暗号化キーのコメントを入力します。

この情報は、コアコンソールからの暗号化キーを表示する際に、Description（説明）フィールドに表示されます。

Passphrase（パスフレーズ）

アクセスの制御に使用するパスフレーズを入力します。

この表の Name（名前）説明に特殊文字をリストするのを避けるが通例です。

安全な場所にパスフレーズを記録します。Dell Support はパスフレーズを復元できません。いったん暗号化キーを作成し、1つまたは複数の保護対象マシンにそれを適用した場合、パスフレーズを失うとデータを復元できません。

パスフレーズの確認

テキストボックスに先ほど入力したパスフレーズを再度入力します。

17 終了をクリックします。

Rapid Recovery（迅速な回復）は、選択した VM とそのホストを保護されたマシンのリストに追加します。

保護対象マシンの診断情報へのアクセス

Rapid Recovery では、各保護対象マシンの診断情報をダウンロードして表示できます。また、Rapid Recovery では、Core のログデータをダウンロードして表示することもできます。

ログにアクセスするには、次の手順を参照してください。

- [Core ログファイルのダウンロードと表示](#)
- [保護対象マシンのログファイルのダウンロードと表示](#)

保護対象マシンのログファイルのダウンロードと表示

保護対象マシンでエラーまたは不具合が発生した場合は、マシンログをダウンロードして表示するか、デルサポートの担当者と Core ログを共有できます。

1 Core Console の左側にあるナビゲーション領域で、保護対象マシン メニューの下に矢印をクリックすると、関連する保護対象

マシンの文脈依存メニューが展開されます。**詳細** までスクロールダウンしてメニューを展開し、 **エージェントログ** を選択します。

エージェントログのダウンロード ページが表示されます。

2 エージェントログのダウンロード ページで **ダウンロードを開始するには、ここをクリックしてください** をクリックします。

3 **AgentAppRecovery.log** を開いています ダイアログボックスで、次のいずれかを実行します。

- ログファイルを開くには、**プログラムから開く** を選択し、テキストベースのログファイルを表示するアプリケーション（メモ帳など）を選択して、**OK** をクリックします。

AgentAppRecovery.log ファイルが、選択したアプリケーションで開きます。

- ファイルをローカルに保存するには、**ファイルの保存** を選択して、次に **OK** をクリックします。

AgentAppRecovery.log ファイルがダウンロードフォルダに保存されます。ファイルは、任意のテキストエディタを使用して開くことができます。

保護対象マシンのログファイルのダウンロードと表示

保護対象マシンでエラーまたは不具合が発生した場合は、マシンログをダウンロードして表示するか、デルサポートの担当者と Core ログを共有できます。

- 1 Core Console の左側にあるナビゲーション領域で、保護対象マシン メニューの下の方の矢印をクリックすると、関連する保護対象マシンの文脈依存メニューが展開されます。**より多い**までスクロールダウンしてメニューを展開し、 **Agent ログ** を選択します。
Agent ログのダウンロード ページが表示されます。
- 2 **Agent ログのダウンロード** ページ、 **ダウンロードを開始するには、ここをクリックしてください** をクリックします。
- 3 **AgentAppRecovery.log を開いています** ダイアログボックスで、次のいずれかを実行します。
 - ・ ログファイルを開くには、**プログラムから開く** を選択し、テキストベースのログファイルを表示するアプリケーション（メモ帳など）を選択して、**OK** をクリックします。
AgentAppRecovery.log ファイルが、選択したアプリケーションで開きます。
 - ・ ファイルをローカルに保存するには、**ファイルの保存** を選択して、次に **OK** をクリックします。
AgentAppRecovery.log ファイルがダウンロードフォルダに保存されます。ファイルは、任意のテキストエディタを使用して開くことができます。

関連するリンク

[Core ログファイルのダウンロードと表示](#)

マシンのステータスおよびその他詳細の表示

マシンのステータスやその他詳細を表示するには、次の手順を完了します。

Rapid Recovery コアコンソールで、表示する保護対象マシンに移動します。

マシンの情報が Summary（サマリ）ページに表示されます。表示される詳細には、次の情報が含まれます。

- ・ ホスト名
 - ・ 最後に取得したスナップショット
 - ・ 次に予定されているスナップショット
 - ・ 暗号化ステータス
 - ・ バージョン番号
- Exchange Server がマシンにインストールされている場合、サーバーの詳細情報も表示されます。これには、次の情報が含まれます。
- ・ 最後に正常に実行されたマウント可否チェック
 - ・ 最後に正常に実行されたチェックサムチェック
 - ・ 最後に実行されたログ切り捨て
- このマシンに含まれるボリュームについても詳細情報が表示されます。次の情報が含まれます。
- ・ ボリューム名
 - ・ スケジュール
 - ・ 現在のスケジュール
 - ・ 次回スナップショット
 - ・ ファイルシステムタイプ
 - ・ 全体サイズのうちのスペース使用状況
- SQL Server がマシンにインストールされている場合、サーバーの詳細情報も表示されます。これには、次の情報が含まれます。

オンライン状態

- ・ Name (名前)
- ・ インストールパス
- ・ バージョン

Exchange Server がマシンにインストールされている場合、サーバーとメールストアの詳細情報も表示されます。これには、次の情報が含まれます。

- ・ バージョン
- ・ インストールパス
- ・ Data Path (データパス)
- ・ データベース名
- ・ Exchange データベースのパス
- ・ ログファイルのパス
- ・ ログプレフィックス
- ・ システムパス
- ・ メールストアタイプ

マシンの管理

本項では、マシンを管理する際に実行するさまざまなタスクについて説明します。次のトピックで構成されています。

- ・ マシンの削除
- ・ 保護からのクラスタの削除
- ・ マシンのライセンス情報の表示
- ・ 保護対象マシンのログファイルのダウンロードと表示
- ・ 保護対象クラスタノードの保護対象マシンへの変換

マシンの削除

マシンを Rapid Recovery Core の保護対象から削除する際には、それまでに RR に保存されたリカバリポイントを保持するのか、リカバリポイントを削除するのかを尋ねる 2 つのオプションが提示されます。保護対象からのマシンの削除後リカバリポイントを保持する場合、そのマシンは「リカバリポイントのみ」のマシンになります。こうした現在の保護対象から削除されたマシンのリカバリポイントは、以降も引き続きマシンのリストアに使用できますが、リカバリ可能範囲は保存されたリカバリポイントで取得されている状態までに限定されます。

リカバリポイントを削除する場合は、この削除アクションによって、Rapid Recovery Core からそれまでの保護対象マシンのスナップショットデータがすべて削除されます。

△ | 注意: リカバリポイントを削除すると、そのマシンのデータをリストアできなくなります。

Rapid Recovery 環境の保護対象からマシンを削除するには、次の手順を実行します。

- 1 Rapid Recovery Core Console の左側にあるナビゲーションエリアの 保護対象マシン で、削除するマシンをクリックします。
- 2 関連するマシンの サマリ ページで、**マシンを削除** をクリックします。
- 3 リボジトリからこのマシンのすべてのリカバリポイントも削除する場合は、ダイアログボックスで **リカバリポイントを含むマシンを削除** を選択します。
- 4 マシンの削除を選択したことを確認し、**はい** をクリックします。
Rapid Recovery で保護対象からそのマシンが削除され、そのマシンのアクティブなタスクがすべてキャンセルされます。

マシン上の操作のキャンセル

マシンで現在実行している操作をキャンセルすることができます。現在のスナップショットだけをキャンセルすることも、現在のすべての操作（エクスポート、レプリケーションなど）をキャンセルすることもできます。

- 1 Rapid Recovery Core Console を開き、左側のナビゲーション領域にある 保護対象マシン の下で、操作をキャンセルするマシンをクリックします。
- 2 イベント をクリックします。
- 3 進行中のイベントまたはキャンセルする操作の右端で、ジョブの詳細 アイコンをクリックします。
- 4 アクティブなタスクをモニタ ダイアログボックスで **キャンセル** をクリックします。

マシンのライセンス情報の表示

保護対象マシンにインストールされた Rapid Recovery Agent ソフトウェアの現在のライセンスステータス情報を表示できます。

- 1 Rapid Recovery Core Console の 保護対象マシン の下で、変更するマシンをクリックします。
選択したマシンの **サマリ** ページが表示されます。
- 2 **設定** メニューをクリックします。
設定 ページが表示され、選択したマシンの設定が表示されます。
- 3 設定 ページで **ライセンスの付与** リンクをクリックし、スクロールダウンすると、マシン固有のライセンス設定が表示されます。
ステータス 画面が表示され、製品ライセンスの詳細が表示されます。

VM エクスポート

本項では、リカバリポイントをエクスポートして仮想マシンを作成する方法について説明します。

Rapid Recovery を使用した仮想マシンへのエクスポートについて

Rapid Recovery Core を使用して、リポジトリから仮想マシンにリカバリポイントをエクスポートすることができます。このプロセスは仮想エクスポートと呼ばれることもあり、リカバリポイントから仮想マシンを作成する、物理から仮想への（P2V）プロセスです。VM は保護対象マシンの起動可能なクローンです。

① **メモ:** 使用されるリカバリポイントは、完全なリカバリポイントチェーンの一部である必要があります。リカバリポイントチェーンの詳細については、「[リカバリポイントチェーンとオフライン](#)」のトピックを参照してください。

Core Console の Virtual Standby ページから仮想エクスポートを実行することができます。または、**VM のエクスポート**（ボタンバ

ーの  **復元** ドロップダウンメニューにある）を選択します。

Rapid Recovery Core から仮想エクスポートを実行する場合は、次の 2 種類の方法があります。

- ・ **1 回限りの仮想エクスポート**を実行できます。この方法では、所定の時点におけるリカバリポイント情報からの単一のスナップショットが示されます。
- ・ **Virtual Sandby**を作成できます。Virtual Standby を使用すると、ソースマシンからスケジュール済みのスナップショットまたは強制的に作成されたスナップショットがキャプチャされるたびに、選択したリカバリポイントから作成した VM スナップショットが Core によって継続的にアップデートされます。これによって、データリカバリ用の可用性の高いリソースが作成されま

す。保護対象マシンに障害が発生した場合は、仮想マシンを起動して一時的にすばやく置き換えて、大幅なダウンタイムを発生させることなく元の保護対象マシンを復元する時間が得られるようにすることができます。

次の図に、仮想マシンにデータをエクスポートする場合の一般的な導入を示します。

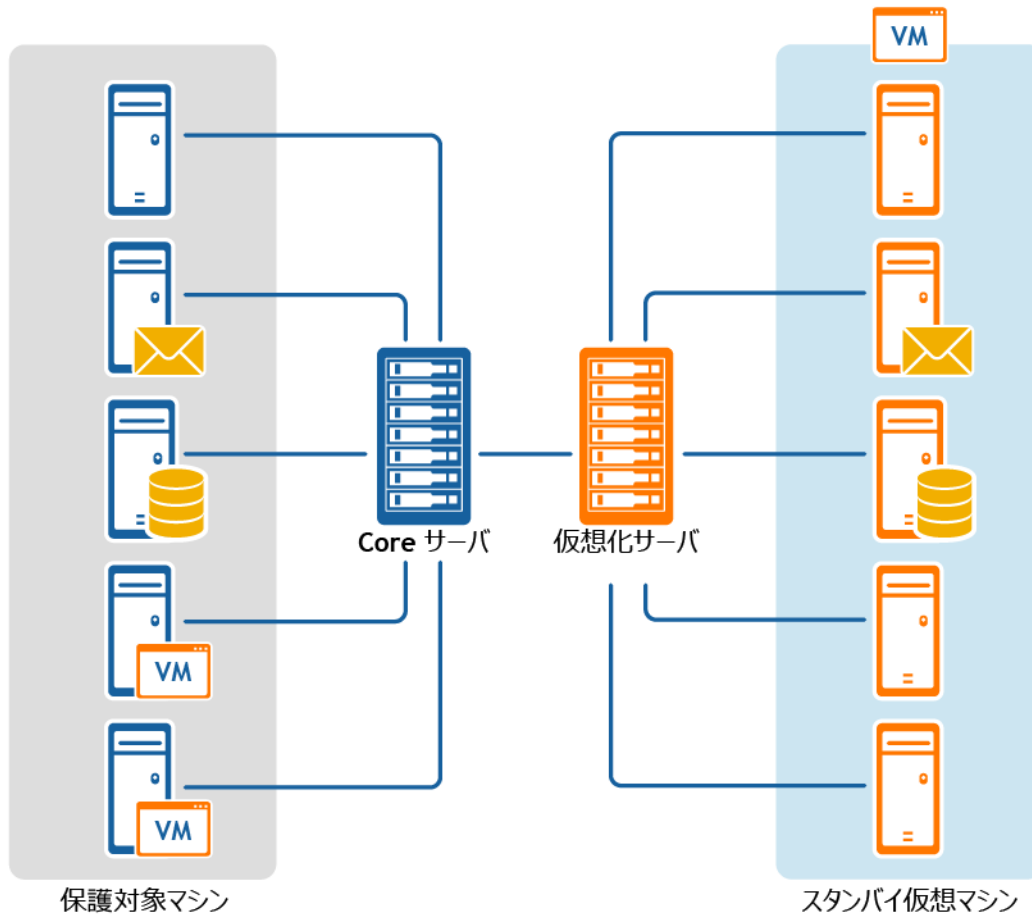


図 8. Virtual Standby の導入

① **メモ:** レプリケーションを含む設定では、ターゲット **Core** を表す **Core** が表示されます。

仮想マシンにエクスポートする際は、次の情報がエクスポートされます。

- ・ リカバリポイントからのすべてのバックアップデータ
- ・ 元の保護対象マシンからのオペレーティングシステムと設定

保護対象 Windows または Linux マシンのリカバリポイントの VMware、ESXi、Hyper-V、および VirtualBox への仮想エクスポートを実行できます。

① **メモ:** ESXi、VMware Workstation、または Hyper-V の場合は、仮想マシンのバージョンが試用版や無料版ではなく、ライセンスが付与されているバージョンである必要があります。

レプリケーションが 2 つの Core（ソースとターゲット）間で設定されている場合は、初回のレプリケーションの完了後にターゲット Core からのみデータをエクスポートできます。

1 回限りの ESXi エクスポートの実行

ESXi に対して 1 回限りのエクスポートを実行するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のボタンバーで、**リストア** ドロップダウンメニューをクリックし、**VM のエクスポート** をクリックします。
- 2 仮想マシンのエクスポートウィザードで **1 回限りのエクスポート** を選択します。
- 3 「次へ」をクリックします。
- 4 マシン ページで、エクスポートする保護対象マシンを選択します。
- 5 「次へ」をクリックします。
- 6 リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 7 「次へ」をクリックします。
- 8 「エクスポート」ウィザードの「宛先」ページにある「仮想マシンにリカバリ」ドロップダウンメニューで、「**ESX(i)**」を選択します。
- 9 次の表の説明に従って、仮想マシンにアクセスするためのパラメータを入力し、「次へ」をクリックします。

表 103. 仮想マシンパラメータ

オプション	説明
ホスト名	ホストマシンの名を入力します。
ポート	ホストマシンのポートを入力します。デフォルトは 443 です。
ユーザー名	ホストマシンのログオンユーザー名を入力します。
パスワード	ホストマシンのログオンパスワードを入力します。

- 10 「仮想マシンのオプション」ページで、次の表で説明されている情報を入力します。

表 104. 仮想マシンオプション

オプション	説明
リソースプール	ドロップダウンリストからリソースプールを選択します。
VM 設定の場所	ドロップダウンリストからデータストアを選択します。
仮想マシン名	仮想マシンの名前を入力します。
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
プロセッサ数	エクスポートされた仮想マシンで使用するプロセッサ (CPU) 数。最小値は 1 です。
プロセッサあたりの Core 数	各プロセッサを構成する Core の数。最小値は 1 です。
ディスクのプロビジョニング	次のオプションから、ディスクプロビジョニングのタイプを選択します。 ・ シン。シンプロビジョニングでは、ボリューム全体のサイズではなく、元のボリュームの使用容量のサイズに合わせて仮想ディスクが作成されます。たとえば、元のボリュームが 1 TB であり、使用容量が 2 GB のみである場合、Rapid Recovery では、2 GB の仮想ディスクが作成されます。 ・ シック。元のボリュームの一部のみが使用されている場合でも、シックプロビジョニングでは、元のボリュームと同じサイズの新しいディスクまたはボリュームが保護サーバから作成されます。た

オプション	説明
	たとえば、ボリュームが 1TB であり、使用容量が 2 GB のみである場合、Rapid Recovery では、1TB の仮想ディスクが作成されます。
ディスクのマッピング	次のオプションから、ディスクマッピングのタイプを選択します。 ・ 自動 ・ 手動 ・ VM を使用
バージョン	仮想マシンの作成に使用する ESXi のバージョンを、ドロップダウンリストから選択します。

- 11 「次へ」をクリックします。
- 12 「ボリューム」ページで、エクスポートするボリュームを選択し、「次へ」をクリックします。
- 13 「サマリ」ページで「完了」をクリックしてウィザードを完了し、エクスポートを開始します。

① **メモ:** Virtual Standby または イベント ページを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

連続 (Virtual Standby) ESXi エクスポートの実行

Rapid Recovery を使用して ESXi 仮想マシン (VM) への連続エクスポートを実行するには、次の手順を完了します。

- 1 Rapid Recovery Core Console で、次のいずれかを実行します。

- ・ Core Console から、ボタンバーで  **復元** ドロップダウンメニューをクリックし、**VM エクスポート** を選択します。
 - 1 仮想マシンのエクスポートウィザードで、**連続 (Virtual Standby)** を選択します。
 - 2 **次へ** をクリックします。

- ・ Core Console から、アイコンバーで  (仮想スタンバイ) をクリックします。
 - ・ **Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。
- 2 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。
 - 3 「次へ」をクリックします。
 - 4 **リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。
 - 5 「次へ」をクリックします。
 - 6 エクスポート ウィザードの **宛先** ページにある 仮想マシンにリカバリ ドロップダウンメニューで、**ESXi** を選択します。
 - 7 次の表の説明に従って、仮想マシンにアクセスするための情報を入力し、「次へ」をクリックします。

表 105. ESXi 資格情報

オプション	説明
ホスト名	ホストマシンの名を入力します。
ポート	ホストマシンのポートを入力します。デフォルトは 443 です。
ユーザー名	ホストマシンのログオン資格情報を入力します。
パスワード	ホストマシンのログオン資格情報を入力します。

- 8 **Virtual Machine Options** (仮想マシンオプション) ページで、次の表で説明されている情報を入力します。

表 106. 仮想マシンオプション

オプション	説明
リソースプール	ドロップダウンリストからリソースプールを選択します。
データストア	ドロップダウンリストからデータストアを選択します。
仮想マシン名	仮想マシンの名前を入力します。
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
プロセッサ数	エクスポートされた仮想マシンに実装するプロセッサ（CPU）の数です。最小値は 1 です。
プロセッサあたりの Core 数	プロセッサごとに実装する Core 数です。最小値は 1 です。
ディスクプロビジョニング	次のオプションからディスクのプロビジョニングのタイプを選択します。 ・ シン。シンプロビジョニングでは、ボリュームサイズ全体ではなく、元のボリュームの使用容量のサイズで仮想ディスクが作成されます。たとえば、元のボリュームが 1 TB で、使用容量が 2 GB しか含まれていない場合、Rapid Recovery は 2 GB の仮想ディスクを作成します。 ・ シック。シックプロビジョニングでは、元のボリュームの一部のみが使用されている場合でも、保護対象サーバからの元のボリュームと同じサイズで新しいディスクまたはボリュームが作成されます。たとえば、ボリュームが 1 TB の大きさで、2 GB の使用容量を含む場合、Rapid Recovery は 1 TB の仮想ディスクを作成します。
ディスクマッピング	必要に応じて、ディスクマッピングのタイプ（「自動」、「手動」、または「VM を使用」）を指定します。
バージョン	仮想マシンのバージョンを選択します。
初回の 1 回限りのエクスポートの実行	スケジュールされた次のスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行するには、これを選択します（省略可能）。

9 「次へ」をクリックします。

10 ボリューム ページで、エクスポートするボリュームを選択して 次へ をクリックします。

11 サマリ ページで 終了 をクリックしてウィザードを完了し、エクスポートを開始します。

④ | **メモ:** Virtual Standby ページまたは イベント ページを表示すると、エクスポートのステータスと進捗状況を監視できます。

1 回限りの VMware Workstation エクスポートの実行

VMware Workstation へ 1 回限りのエクスポートを実行するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のボタンバーで、リストア ドロップダウンメニューをクリックし、**VM エクスポート** をクリックします。
- 2 仮想マシンのエクスポートウィザードで、**1 回限りのエクスポート** を選択します。
- 3 「次へ」をクリックします。
- 4 マシン ページで、エクスポートする保護対象マシンを選択します。
- 5 「次へ」をクリックします。
- 6 リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 7 「次へ」をクリックします。

- 8 「エクスポート」ウィザードの「宛先」ページにある「仮想マシンにリカバリ」ドロップダウンメニューで、「**VMware Workstation**」を選択し、「**次へ**」をクリックします。
- 9 「仮想マシンのオプション」ページで、次の表の説明に従って、仮想マシンにアクセスするためのパラメータを入力します。

表 107. 仮想マシンパラメータ

オプション	説明
VM Machine Location (VM マシンの場所) ①	仮想マシンを作成するローカルフォルダまたはネットワーク共有のパスを指定します。 ❗ メモ: ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なログオン資格情報を入力する必要があります。アカウントにはネットワーク共有に対する読み取りおよび書き込み権限がある必要があります。
ユーザー名	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なユーザー名を入力する必要があります。 - ローカルパスを入力した場合は、ユーザー名は必要ありません。
パスワード	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なパスワードを入力する必要があります。 - ローカルパスを入力した場合は、パスワードは必要ありません。
VM 名	作成される仮想マシンの名前（例：VM-0A1B2C3D4）を入力します。 ① メモ: デフォルト名は、ソースマシンの名前です。
バージョン	仮想マシンの VMware Workstation のバージョンを指定します。次から選択できます。 - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
RAM 容量 (MB)	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 - ソースマシンと同じ容量の RAM を使用 - 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
プロセッサ数	エクスポートされた仮想マシンに使用するプロセッサ (CPU) の数です。最小値は 1 です。
プロセッサあたりの Core 数	各プロセッサに使用する Core 数です。最小値は 1 です。

- 10 「**次へ**」をクリックします。
- 11 「ボリューム」ページで、エクスポートするボリューム (C:\ および D:\ など) を選択し、「**次へ**」をクリックします。
- 12 「サマリ」ページで「**完了**」をクリックしてウィザードを完了し、エクスポートを開始します。

① **メモ:** 「**Virtual Standby**」または「**イベント**」タブを表示すると、エクスポートのステータスと進捗状況を監視できます。

連続 (Virtual Standby) VMware Workstation エクスポートの実行

Rapid Recovery を使用して VMware Workstation 仮想マシン (VM) への継続的なエクスポートを実行するには、次の手順を完了します。

1 Rapid Recovery Core Console で、次のいずれかを実行します。

- Core Console から、ボタンバーで  **復元** ドロップダウンメニューをクリックし、**VM エクスポート** を選択します。

- 仮想マシンのエクスポートウィザードで、**連続 (Virtual Standby)** を選択します。
- 次へ** をクリックします。

- Core Console から、アイコンバーで  (仮想スタンバイ) をクリックします。
 - Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。

- 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。
- 「次へ」** をクリックします。
- リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。
- 「次へ」** をクリックします。
- 仮想マシンのエクスポートウィザードの **宛先** ページにある 仮想マシンにリカバリ ドロップダウンメニューで、**VMWare Workstation** を選択し、**次へ** をクリックします。
- Virtual Machine Options** (仮想マシンオプション) ページで、次の表の説明どおりに仮想マシンにアクセスするためのパラメータを入力します。

表 108. 仮想マシンパラメータ

オプション	説明
ターゲットパス	仮想マシンを作成するローカルフォルダまたはネットワーク共有のパスを指定します。 ① メモ: ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なログオン資格情報を入力する必要があります。アカウントにはネットワーク共有に対する読み取りおよび書き込み権限がある必要があります。
ユーザー名	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なユーザー名を入力する必要があります。 - ローカルパスを入力した場合は、ユーザー名は必要ありません。
パスワード	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なパスワードを入力する必要があります。 - ローカルパスを入力した場合は、パスワードは必要ありません。
仮想マシン	作成される仮想マシンの名前 (例: VM-0A1B2C3D4) を入力します。 ① メモ: デフォルト名は、ソースマシンの名前です。
バージョン	仮想マシンの VMware Workstation のバージョンを指定します。次から選択できます。 - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0

オプション	説明
	- VMware Workstation 11.0 - VMware Workstation 12.0
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 - ソースマシンと同じ容量の RAM を使用 - 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
プロセッサ数	エクスポートされた仮想マシンに実装するプロセッサ (CPU) の数です。最小値は 1 です。
プロセッサあたり の Core 数	プロセッサごとに実装する Core 数です。最小値は 1 です。
8	「初回の 1 回限りのエクスポートを実施」を選択して、スケジュールされた次のスケジュール済みスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行します。
9	「次へ」をクリックします。
10	ボリューム ページで、エクスポートするボリューム (C:\ および D:\ など) を選択し、次へをクリックします。
11	サマリ ページで 終了 をクリックしてウィザードを完了し、エクスポートを開始します。

① | **メモ:** Virtual Standby ページまたは イベント ページを表示すると、エクスポートのステータスと進捗状況を監視できます。

1 回限りの Hyper-V エクスポートの実行

Hyper-V に対して 1 回限りのエクスポートを実行するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のボタンバーで、**復元** ドロップダウンメニューをクリックし、**VM エクスポート** をクリックします。
- 2 仮想マシンのエクスポート ウィザードで、**1 回限りのエクスポート** を選択します。
- 3 「次へ」をクリックします。
- 4 マシン ページで、エクスポートする保護対象マシンを選択します。
- 5 「次へ」をクリックします。
- 6 リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 7 「次へ」をクリックします。
- 8 宛先 ページにある 仮想マシンへのエクスポート ドロップダウンメニューで、**Hyper-V** を選択します。
- 9 Hyper-V 役割が割り当てられたローカルマシンにエクスポートするには、「**ローカルマシンを使用**」をクリックします。
- 10 Hyper-V サーバがリモートマシンに存在することを示すには、**リモートホスト** をクリックし、次の表の説明に従って、リモートホストの情報を入力します。

表 109. リモートホスト情報

テキストボックス	説明
ホスト名	Hyper-V サーバーの IP アドレスまたはホスト名を入力します。リモート Hyper-V サーバーの IP アドレスまたはホスト名を示します。
ポート	マシンのポート番号を入力します。Core がこのマシンと通信するときに使用するポートを示します。
ユーザー名	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーのユーザー名を入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。

テキストボックス 説明

パスワード	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーアカウントのパスワードを入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。

11 「次へ」をクリックします。

12 仮想マシンオプション ページの **VM マシンの場所** テキストボックスに、仮想マシンのパス（D:\export など）を入力します。これは、仮想マシンの場所を識別するために使用されます。

① **メモ:** 仮想マシンの場所は、ローカルおよびリモートの両方の Hyper-V サーバーで指定する必要があります。このパスは Hyper-V サーバーの有効なローカルパスであるようにしてください。存在しないディレクトリが自動的に作成されます。手動で作成しようとししないでください。共有フォルダ（例えば \\data\share）へのエクスポートは許可されません。

13 仮想マシン名 テキストボックスに仮想マシンの名前を入力します。

入力する名前は、Hyper-V Manager Console の仮想マシンリストに表示されます。

14 メモリの使用容量を指定するには、次のいずれかをクリックします。

- ・ **ソースマシンと同容量の RAM を使用** 仮想マシンとソースマシン間の RAM 使用量が同じであることを指定する場合は、このオプションを選択します。
- ・ **指定の RAM 容量を使用する** RAM の容量を MB 単位で指定する場合は、このオプションを選択します。
最低量は 1024 MB、アプリケーションで許可される最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。

15 ディスクフォーマットを指定するには、「ディスクフォーマット」の横にある次のいずれかをクリックします。

- ・ VHDX
- ・ VHD

① **メモ:** ターゲットマシンで Windows 8 (Windows Server 2012) 以降が実行されている場合、Hyper-V エクスポートでは VHDX ディスクフォーマットがサポートされます。お使いの環境で VHDX がサポートされていない場合、このオプションは無効になります。

Hyper-V generation 2 にエクスポートする場合は、VHDX ディスクフォーマットのみがサポートされます。

16 エクスポートに使用する Hyper-V の世代を指定するには、次のいずれかをクリックします。

- ・ Generation 1
- ・ Generation 2

① **メモ:** セキュアブートオプションをサポートしているのは、**Generation 2** のみです。

17 エクスポートされた VM の適切なネットワークアダプタを指定します。

18 **Volumes** (ボリューム) ページで、エクスポートするボリューム (複数可) (例: C:\) を選択します。

① **メモ:** 選択されたボリュームが次に示すアプリケーションがサポートする適切な最大割り当てを超えているか、使用可能領域の容量を超えている場合は、エラーが表示されます。

- ・ VHDX ディスクフォーマットでは、選択したボリュームは 64 TB を超えることはできません。
- ・ VHD ディスクフォーマットでは、選択したボリュームは 2040 GB を超えることはできません。

19 ボリューム ページで **終了** をクリックしてウィザードを完了し、エクスポートを開始します。

① **メモ:** **Virtual Standby** ページまたは **イベント** ページを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

連続 (Virtual Standby) Hyper-V エクスポートの実行

Rapid Recovery を使用して Hyper-V 仮想マシン (VM) に対して連続エクスポートを実行するには、この説明の各手順を実行します。

1 Rapid Recovery Core Console で、次のいずれかを実行します。

- ・ Core Console のボタンバーで  **リストア** ドロップダウンメニューをクリックし、**VM のエクスポート** を選択します。

1 仮想マシンのエクスポートウィザードで **連続 (Virtual Standby)** を選択します。

2 **次へ** をクリックします。

- Core Console のアイコンバーで  (Virtual Standby) をクリックします。
 - Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。
- 2 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。
- 3 「**次へ**」 をクリックします。
- 4 **リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。
- 5 「**次へ**」 をクリックします。
- 6 **宛先** ページの 仮想マシンへエクスポート ドロップダウンメニューで **Hyper-V** を選択し、次のいずれかの手順を実行します。
- Hyper-V 役割が割り当てられたローカルマシンにエクスポートするには、「**ローカルマシンを使用**」 をクリックします。
 - Hyper-V サーバがリモートマシンに存在することを示すには、**リモートホスト** をクリックし、次の表の説明に従って、リモートホストのパラメータを入力します。

表 110. リモートホスト情報

テキストボックス	説明
ホスト名	Hyper-V サーバーの IP アドレスまたはホスト名を入力します。リモート Hyper-V サーバーの IP アドレスまたはホスト名を示します。
ポート	マシンのポート番号を入力します。Core がこのマシンと通信するときに使用するポートを示します。
ユーザー名	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーのユーザー名を入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。
パスワード	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーアカウントのパスワードを入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。

- 7 「**次へ**」 をクリックします。
- 8 **仮想マシンオプション** ページの **VM マシンの場所** テキストボックスに、仮想マシンのパス (D:\export など) を入力します。これは、仮想マシンの場所を識別するために使用されます。

① **メモ:** 仮想マシンの場所は、ローカルおよびリモートの両方の **Hyper-V** サーバーで指定する必要があります。このパスは **Hyper-V** サーバーの有効なローカルパスであるようにしてください。存在しないディレクトリが自動的に作成されます。手動で作成しようとししないでください。共有フォルダ (例えば \\data\share) へのエクスポートは許可されません。

- 9 **仮想マシン名** テキストボックスに、仮想マシンの名前を入力します。
入力する名前は、Hyper-V Manager Console の仮想マシンリストに表示されます。
- 10 メモリの使用容量を指定するには、次のいずれかをクリックします。
- ソースマシンと同容量の RAM を使用。** 仮想マシンとソースマシンの間で RAM の使用量が同じであることを示す場合、このオプションを選択します。
 - 指定の RAM 容量を使用する。** RAM の容量を MB を単位として指定する場合、このオプションを選択します。
アプリケーションで許可される最低量は 1,024 MB で、最大量は 65,536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
- 11 ディスクフォーマットを指定するには、「ディスクフォーマット」の横にある次のいずれかをクリックします。
- VHDX
 - VHD

① **メモ:** ターゲットマシンで **Windows 8 (Windows Server 2012)** 以降が実行されている場合、**Hyper-V** エクスポートでは **VHDX** ディスクフォーマットがサポートされます。お使いの環境で **VHDX** がサポートされていない場合、このオプションは無効になります。

Hyper-V generation 2 にエクスポートする場合は、VHDX ディスクフォーマットのみがサポートされます。

- 12 エクスポートに使用する Hyper-V の世代を指定するには、次のいずれかをクリックします。
- Generation 1
 - Generation 2

① **メモ:** セキュアブートオプションをサポートしているのは、**Generation 2** のみです。

13 エクスポートされた VM の適切なネットワークアダプタを指定します。

14 **Volumes** (ボリューム) ページで、エクスポートするボリューム (複数可) (例 : C:\) を選択します。

① **メモ:** 選択されたボリュームが次に示すアプリケーションがサポートする適切な最大割り当てを超えているか、使用可能領域の容量を超えている場合は、エラーが表示されます。

- ・ VHDX ディスクフォーマットでは、選択したボリュームは 64 TB を超えることはできません。
- ・ VHD ディスクフォーマットでは、選択したボリュームは 2040 GB を超えることはできません。

15 「初回の**1回限りのエクスポートを実施**」を選択して、スケジュールされた次のスケジュール済みスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行します。

16 ボリューム ページで、**完了** をクリックしてウィザードを完了し、エクスポートを開始します。

① **メモ:** **Virtual Standby** または **イベント** ページを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

1 回限りの VirtualBox エクスポートの実行

VirtualBox に対して 1 回限りのエクスポートを実行するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のボタンバーで、**リストア** ドロップダウンメニューをクリックし、**VM エクスポート** をクリックします。
- 2 仮想マシンのエクスポート ウィザードで、**1 回限りのエクスポート** を選択します。
- 3 「**次へ**」をクリックします。
- 4 マシン ページで、エクスポートする保護対象マシンを選択します。
- 5 「**次へ**」をクリックします。
- 6 リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 7 「**次へ**」をクリックします。
- 8 「エクスポート」ウィザードの「宛先」ページにある「仮想マシンにリカバリ」ドロップダウンメニューで、「**VirtualBox**」を選択し、「**次へ**」をクリックします。
- 9 「仮想マシンオプション」 ページで、「**Windows マシンを使用**」を選択します。
- 10 次の表の説明に従って、仮想マシンにアクセスするためのパラメータを入力します。

表 111. 仮想マシンパラメータ

オプション	説明
仮想マシン名	作成している仮想マシンの名前を入力します。 ① メモ: デフォルト名は、ソースマシンの名前です。
ターゲットパス	仮想マシンを作成するための、ローカルまたはリモートのターゲットパスを指定します。 ① メモ: ターゲットパスには、ルートディレクトリを指定しないでください。ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウント用に有効なログオン資格情報 (ユーザー名とパスワード) を入力する必要があります。アカウントにはネットワーク共有に対する読み取りおよび書き込み権限がある必要があります。
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定

アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。

- 11 仮想マシンのユーザーアカウントを指定するには、「**エクスポートされる仮想マシンのユーザーアカウントを指定します**」を選択し、次の情報を入力します。これは、仮想マシンに複数のユーザーアカウントが存在する場合に、仮想マシンを登録する特定のユーザーアカウントを指します。このユーザーアカウントにログオンすると、VirtualBox マネージャでこの仮想マシンがこのユーザーに対してのみ表示されます。アカウントが指定されていないと、VirtualBox がインストールされている Windows マシンの既存のすべてのユーザーに対して仮想マシンが登録されます。
 - ・ ユーザー名 - 仮想マシンが登録されるユーザー名を入力します。
 - ・ パスワード - このユーザーアカウントのパスワードを入力します。
- 12 「**次へ**」をクリックします。
- 13 「**ボリューム**」ページで、エクスポートするボリューム (C:\ および D:\ など) を選択し、「**次へ**」をクリックします。
- 14 「**サマリ**」ページで「**完了**」をクリックしてウィザードを完了し、エクスポートを開始します。

① | **メモ:** 「**Virtual Standby**」または「**イベント**」タブを表示すると、エクスポートのステータスと進捗状況を監視できます。

連続 (Virtual Standby) VirtualBox エクスポートの実行

この手順を実行するには、VirtualBox が Core マシンにインストールされている必要があります。

Rapid Recovery を使用して VirtualBox 仮想マシン (VM) への連続エクスポートを実行するには、次の手順を完了します。

- 1 Rapid Recovery Core Console で、次のいずれかを実行します。

- ・ Core Console から、ボタンバーで  **復元** ドロップダウンメニューをクリックし、**VM エクスポート** を選択します。
 - 1 仮想マシンのエクスポートウィザードで、**連続 (Virtual Standby)** を選択します。
 - 2 **次へ** をクリックします。

- ・ Core Console から、アイコンバーで  (仮想スタンバイ) をクリックします。
 - ・ **Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。
- 2 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。
 - 3 「**次へ**」をクリックします。
 - 4 **リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。
 - 5 「**次へ**」をクリックします。
 - 6 エクスポート ウィザードの **宛先** ページにある **仮想マシンにリカバリ** ドロップダウンメニューで、**VirtualBox** を選択します。
 - 7 **Virtual Machine Options** (仮想マシンオプション) ページで **Remote Linux Machine** (リモート Linux マシン) を選択します。
 - 8 次の表の説明に従って、仮想マシンに関する情報を入力します。

表 112. リモート Linux マシンの設定

オプション	説明
VirtualBox ホスト名	VirtualBox サーバーの IP アドレスまたはホスト名を入力します。このフィールドは、リモート VirtualBox サーバーの IP アドレスまたはホスト名を表します。
ポート	マシンのポート番号を入力します。この数値は、Core がこのマシンと通信するときに使用するポートを表します。
仮想マシン名	作成している仮想マシンの名前を入力します。

① | **メモ:** デフォルト名は、ソースマシンの名前です。

オプション	説明
ターゲットパス	仮想マシンを作成するためのターゲットパスを指定します。
	① メモ: 仮想マシンがルートから実行されるようにするため、ルートフォルダをルートから作成することをお勧めします。ルートを使用しないと、エクスポートを設定する前に、ターゲットマシン上に宛先フォルダを手動で作成する必要があります。また、エクスポート後に仮想マシンを手動でアタッチまたはロードする必要もあります。
ユーザー名	ターゲットマシンにあるアカウントのユーザー名（root など）です。
パスワード	ターゲットマシンにあるアカウントのパスワードです。
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。

9 「初回の 1 回限りのエクスポートを実施」を選択して、スケジュールされた次のスケジュール済みスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行します。

10 「次へ」をクリックします。

11 ボリューム ページで、エクスポートするデータのボリュームを選択して 次へ をクリックします。

12 サマリ ページで 終了 をクリックしてウィザードを完了し、エクスポートを開始します。

① メモ: Virtual Standby ページまたは イベント ページを表示すると、エクスポートのステータスと進捗状況を監視できます。

エクスポートの管理

Core に仮想エクスポートが確立されている場合は、各仮想エクスポートの設定パラメーターが **仮想スタンバイ** ページの行として表示されます。ここで、現在設定されているエクスポートのステータスを表示し、仮想スタンバイマシンを管理することができます。仮想スタンバイを追加し、エクスポートを強制し、仮想スタンバイを一時停止または再開し、継続的なエクスポートの要件を削除することができます。

1 回限りのエクスポート処理が行われると、ジョブは **仮想スタンバイ** ページのエクスポートキューに一覧表示されます。この時間中に、エクスポート操作を一時停止、再開、またはキャンセルすることができます。

① メモ: Rapid Recovery では、Window 8、Window 8.1、Windows Server 2012 および 2012 R2 への Hyper-V エクスポートがサポートされています。

VM の電源が入っている場合は、仮想スタンバイ VM への仮想エクスポートは発生しません。

仮想エクスポートを管理するには、次の手順を実行します。

- 1 Core Console のアイコンバーで、（仮想スタンバイ）をクリックします。
仮想スタンバイ ページが表示されます。ここでは 2 つのテーブルに、保存済みのエクスポート設定が表示されます。次の表に示された情報が含まれます。

表 113. 仮想スタンバイ情報

列	説明
項目選択	サマリテーブルの行ごとに、テーブルの前のメニューオプションリストからアクションを実行するためのチェックボックスを選択できます。
ステータスインジケータ	ステータス列の色付きの球は仮想スタンバイのステータスを表示します。色付きの円にカーソルを合わせると、ステータス状態が表示されます。 ・ 緑色。仮想スタンバイが正常に設定され、アクティブであり、一時停止していません。次のエクスポートは次のスナップショットの完了直後に実行されます。 ・ 黄色。仮想スタンバイは一時停止していますが、パラメーターがまだ Core に定義され、保存されています。ただし、新しい転送の後、エクスポートジョブは自動的に開始せず、ステータスが変更されるまで、この保護対象マシンに対して新しいエクスポートは行われません。
マシン名	ソースマシンの名前。
宛先	データをエクスポートしている仮想マシンとそのパス。
エクスポートタイプ	ESXi、VMware、Hyper-V、VirtualBox など、エクスポート用の仮想マシンプラットフォームのタイプ。
最終エクスポート	最後のエクスポートの日時。 エクスポートが追加されてもまだ完了していない場合は、エクスポートが実行されていないことを示すメッセージが表示されます。エクスポートが失敗またはキャンセルされた場合は、該当するメッセージも表示されます。
設定	 ドロップダウンメニューを使用すると、次の機能を実行できます。 ・ 編集。仮想スタンバイの設定を編集することができます。 ・ 強制。仮想エクスポートを強制します。 ・ 一時停止。仮想エクスポートを一時停止します。ステータスがアクティブの場合だけ使用できます。 ・ 再開。仮想エクスポートを再開します。ステータスが一時停止の場合にのみ使用できます。 ・ 削除。継続的なエクスポートの要件を削除します。最新のエクスポートされた VM は削除されません。

表 114. エクスポートキュー情報

列	説明
項目選択	サマリテーブルの行ごとに、テーブルの前のメニューオプションリストからアクションを実行するためのチェックボックスを選択できます。
宛先	データをエクスポートしている仮想マシンとそのパス。
エクスポートタイプ	ESXi、VMware、Hyper-V、VirtualBox など、エクスポート用の仮想マシンプラットフォームのタイプ。
スケジュールタイプ	エクスポートタイプ（「1 回限り」または「連続」のいずれか）。
ステータス	進捗状況バーにパーセントで表示される、エクスポートの進捗状況。

- 2 保存されたエクスポート設定を管理するには、エクスポートを選択し、次のいずれかをクリックします。
 - ・ **編集**。仮想マシンのエクスポートウィザードを開き、**VM オプション** ページに進みます。ここでは、エクスポートされた VM の場所を変更し、VM タイプのバージョンを変更し、エクスポート対象の RAM またはプロセッサを指定することができます。VM のエクスポートをただちに開始するには、**最初の 1 回限りのエクスポートを実施** を選択します。

- ・ **強制**。強制的に、新しいエクスポートを行います。このオプションは、Virtual Standby が一時停止後に再開された場合に便利です。つまり、エクスポートジョブは、新しい転送の後でのみ再開されます。新しい転送を待機しない場合は、エクスポートを強制できます。
 - ・ **一時停止**。アクティブなエクスポートを一時停止します。
 - ・ **再開**。次のスケジュール済みスナップショットまたは強制スナップショットの際に、継続的なエクスポートの要件を再開します。
- 3 エクスポートをシステムから削除するには、エクスポートを選択し、**削除** をクリックします。
エクスポート構成は、システムから恒久的に削除されます。仮想スタンバイ設定の削除を実行しても、設定の結果としてエクスポートされた仮想マシンは削除されません。
 - 4 同時実行できるエクスポート数を管理するには、次の手順を実行します。
 - ・ エクスポートキューで、**設定** をクリックします。
 - ・ **最大同時エクスポート数** ダイアログボックスに、同時に実行されるようにするエクスポートの数を入力します。デフォルトの数は 5 です。
 - ・ 「**保存**」 をクリックします。
 - 5 エクスポートキューに現在リストされている 1 回限りのエクスポートまたは継続的なエクスポートをキャンセルするには、エクスポートを選択し、**キャンセル** をクリックします。
 - 6 新しい Virtual Standby エクスポートを追加するには、「**追加**」 をクリックして「エクスポート」ウィザードを起動します。特定の仮想マシンの Virtual Standby の設定の詳細については、次のいずれかのトピックを参照してください。
 - ・ [ESXi 仮想マシンへのデータのエクスポート](#)
 - ・ [VMware Workstation 仮想マシンへのデータのエクスポート](#)
 - ・ [Hyper-V 仮想マシンへのデータのエクスポート](#)
 - ・ [VirtualBox 仮想マシンへのデータのエクスポート](#)

ESXi 仮想マシンへのデータのエクスポート

Rapid Recovery では、1 回限りのエクスポートを実行するか、または連続エクスポート（Virtual Standby の場合）を設定して、データを ESXi にエクスポートできます。エクスポートタイプに合わせて、次の手順を実行します。

1 回限りの ESXi エクスポートの実行

ESXi に対して 1 回限りのエクスポートを実行するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のボタンバーで、**リストア** ドロップダウンメニューをクリックし、**VM のエクスポート** をクリックします。
- 2 仮想マシンのエクスポートウィザードで **1 回限りのエクスポート** を選択します。
- 3 「**次へ**」 をクリックします。
- 4 マシン ページで、エクスポートする保護対象マシンを選択します。
- 5 「**次へ**」 をクリックします。
- 6 リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 7 「**次へ**」 をクリックします。
- 8 「エクスポート」ウィザードの「宛先」ページにある「仮想マシンにリカバリ」ドロップダウンメニューで、「**ESX(i)**」を選択します。
- 9 次の表の説明に従って、仮想マシンにアクセスするためのパラメータを入力し、「**次へ**」 をクリックします。

表 115. 仮想マシンパラメータ

オプション	説明
ホスト名	ホストマシンの名を入力します。
ポート	ホストマシンのポートを入力します。デフォルトは 443 です。

オプション	説明
ユーザー名	ホストマシンのログオンユーザー名を入力します。
パスワード	ホストマシンのログオンパスワードを入力します。

10 「仮想マシンのオプション」 ページで、次の表で説明されている情報を入力します。

表 116. 仮想マシンオプション

オプション	説明
リソースプール	ドロップダウンリストからリソースプールを選択します。
VM 設定の場所	ドロップダウンリストからデータストアを選択します。
仮想マシン名	仮想マシンの名前を入力します。
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
プロセッサ数	エクスポートされた仮想マシンで使用するプロセッサ（CPU）数。最小値は 1 です。
プロセッサあたりの Core 数	各プロセッサを構成する Core の数。最小値は 1 です。
ディスクのプロビジョニング	次のオプションから、ディスクプロビジョニングのタイプを選択します。 ・ シン。シンプロビジョニングでは、ボリューム全体のサイズではなく、元のボリュームの使用容量のサイズに合わせて仮想ディスクが作成されます。たとえば、元のボリュームが 1 TB であり、使用容量が 2 GB のみである場合、Rapid Recovery では、2 GB の仮想ディスクが作成されます。 ・ シック。元のボリュームの一部のみが使用されている場合でも、シックプロビジョニングでは、元のボリュームと同じサイズの新しいディスクまたはボリュームが保護サーバから作成されます。たとえば、ボリュームが 1 TB であり、使用容量が 2 GB のみである場合、Rapid Recovery では、1 TB の仮想ディスクが作成されます。
ディスクのマッピング	次のオプションから、ディスクマッピングのタイプを選択します。 ・ 自動 ・ 手動 ・ VM を使用
バージョン	仮想マシンの作成に使用する ESXi のバージョンを、ドロップダウンリストから選択します。

11 「次へ」をクリックします。

12 「ボリューム」 ページで、エクスポートするボリュームを選択し、「次へ」をクリックします。

13 「サマリ」 ページで「完了」をクリックしてウィザードを完了し、エクスポートを開始します。

④ **メモ:** Virtual Standby または イベント ページを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

連続（Virtual Standby）ESXi エクスポートの実行

Rapid Recovery を使用して ESXi 仮想マシン（VM）への連続エクスポートを実行するには、次の手順を完了します。

1 Rapid Recovery Core Console で、次のいずれかを実行します。

- ・ Core Console から、ボタンバーで  復元 ドロップダウンメニューをクリックし、**VM エクスポート** を選択します。

1 仮想マシンのエクスポートウィザードで、**連続 (Virtual Standby)** を選択します。

2 **次へ** をクリックします。

・ Core Console から、アイコンバーで  (仮想スタンバイ) をクリックします。

・ **Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。

2 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。

3 「**次へ**」 をクリックします。

4 **リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。

5 「**次へ**」 をクリックします。

6 エクスポート ウィザードの **宛先** ページにある 仮想マシンにリカバリ ドロップダウンメニューで、**ESXi** を選択します。

7 次の表の説明に従って、仮想マシンにアクセスするための情報を入力し、「**次へ**」 をクリックします。

表 117. ESXi 資格情報

オプション	説明
ホスト名	ホストマシンの名を入力します。
ポート	ホストマシンのポートを入力します。デフォルトは 443 です。
ユーザー名	ホストマシンのログオン資格情報を入力します。
パスワード	ホストマシンのログオン資格情報を入力します。

8 **Virtual Machine Options** (仮想マシンオプション) ページで、次の表で説明されている情報を入力します。

表 118. 仮想マシンオプション

オプション	説明
リソースプール	ドロップダウンリストからリソースプールを選択します。
データストア	ドロップダウンリストからデータストアを選択します。
仮想マシン名	仮想マシンの名前を入力します。
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
プロセッサ数	エクスポートされた仮想マシンに実装するプロセッサ (CPU) の数です。最小値は 1 です。
プロセッサあたりの Core 数	プロセッサごとに実装する Core 数です。最小値は 1 です。
ディスクプロビジョニング	次のオプションからディスクのプロビジョニングのタイプを選択します。 ・ シン。シンプロビジョニングでは、ボリュームサイズ全体ではなく、元のボリュームの使用容量のサイズで仮想ディスクが作成されます。たとえば、元のボリュームが 1 TB で、使用容量が 2 GB しか含まれていない場合、Rapid Recovery は 2 GB の仮想ディスクを作成します。 ・ シック。シックプロビジョニングでは、元のボリュームの一部のみが使用されている場合でも、保護対象サーバからの元のボリュームと同じサイズで新しいディスクまたはボリュームが作成されます。たとえば、ボリュームが 1 TB の大きさで、2 GB の使用容量を含む場合、Rapid Recovery は 1 TB の仮想ディスクを作成します。
ディスクマッピング	必要に応じて、ディスクマッピングのタイプ (「自動」、「手動」、または「VM を使用」) を指定します。
バージョン	仮想マシンのバージョンを選択します。

オプション	説明
初回の1回限りのエクスポートの実行	スケジュールされた次のスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行するには、これを選択します（省略可能）。

- 「次へ」をクリックします。
- ボリューム ページで、エクスポートするボリュームを選択して 次へ をクリックします。
- サマリ ページで 終了 をクリックしてウィザードを完了し、エクスポートを開始します。

① | **メモ:** Virtual Standby ページまたは イベント ページを表示すると、エクスポートのステータスと進捗状況を監視できます。

VirtualBox 仮想マシンへのデータのエクスポート

Rapid Recovery では、1 回限りのエクスポートを実行するか、または連続エクスポート（Virtual Standby の場合）を設定して、データを VirtualBox エクスポートにエクスポートできます。

① | **メモ:** Windows 10 の保護されたマシンの VirtualBox エクスポートは、現在サポートされていません。

エクスポートタイプに合わせて、次の手順を実行します。

① | **メモ:** このタイプのエクスポートを実行するには、Core マシンに VirtualBox がインストールされている必要があります。Windows ホストでは、Virtual Box Version 4.2.18 以降がサポートされています。

1 回限りの VirtualBox エクスポートの実行

VirtualBox に対して 1 回限りのエクスポートを実行するには、次の手順を実行します。

- Rapid Recovery Core Console のボタンバーで、リストア ドロップダウンメニューをクリックし、**VM エクスポート** をクリックします。
- 仮想マシンのエクスポート ウィザードで、**1 回限りのエクスポート** を選択します。
- 「次へ」をクリックします。
- マシン ページで、エクスポートする保護対象マシンを選択します。
- 「次へ」をクリックします。
- リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 「次へ」をクリックします。
- 「エクスポート」ウィザードの「宛先」ページにある「仮想マシンにリカバリ」ドロップダウンメニューで、「**VirtualBox**」を選択し、「次へ」をクリックします。
- 「仮想マシンオプション」 ページで、「**Windows マシンを使用**」を選択します。
- 次の表の説明に従って、仮想マシンにアクセスするためのパラメータを入力します。

表 119. 仮想マシンパラメータ

オプション	説明
仮想マシン名	作成している仮想マシンの名前を入力します。 ① メモ: デフォルト名は、ソースマシンの名前です。
ターゲットパス	仮想マシンを作成するための、ローカルまたはリモートのターゲットパスを指定します。 ① メモ: ターゲットパスには、ルートディレクトリを指定しないでください。ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウント用に有効なログオン資格情報（ユーザー名とパスワード）を入力する必要があります。アカウントにはネットワーク共有に対する読み取りおよび書き込み権限がある必要があります。

オプション	説明
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
11	仮想マシンのユーザーアカウントを指定するには、「 エクスポートされる仮想マシンのユーザーアカウントを指定します 」を選択し、次の情報を入力します。これは、仮想マシンに複数のユーザーアカウントが存在する場合に、仮想マシンを登録する特定のユーザーアカウントを指します。このユーザーアカウントにログオンすると、VirtualBox マネージャでこの仮想マシンがこのユーザーに対してのみ表示されます。アカウントが指定されていないと、VirtualBox がインストールされている Windows マシンの既存のすべてのユーザーに対して仮想マシンが登録されます。 ・ ユーザー名 - 仮想マシンが登録されるユーザー名を入力します。 ・ パスワード - このユーザーアカウントのパスワードを入力します。
12	「 次へ 」をクリックします。
13	「ボリューム」ページで、エクスポートするボリューム（C:\ および D:\ など）を選択し、「 次へ 」をクリックします。
14	「サマリ」ページで「 完了 」をクリックしてウィザードを完了し、エクスポートを開始します。

① | **メモ:** 「Virtual Standby」または「イベント」タブを表示すると、エクスポートのステータスと進捗状況を監視できます。

連続 (Virtual Standby) VirtualBox エクスポートの実行

この手順を実行するには、VirtualBox が Core マシンにインストールされている必要があります。

Rapid Recovery を使用して VirtualBox 仮想マシン (VM) への連続エクスポートを実行するには、次の手順を完了します。

- 1 Rapid Recovery Core Console で、次のいずれかを実行します。

- ・ Core Console から、ボタンバーで  **復元** ドロップダウンメニューをクリックし、**VM エクスポート** を選択します。
 - 1 仮想マシンのエクスポートウィザードで、**連続 (Virtual Standby)** を選択します。
 - 2 **次へ** をクリックします。

- ・ Core Console から、アイコンバーで  (仮想スタンバイ) をクリックします。
 - ・ **Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。
- 2 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。
 - 3 「**次へ**」をクリックします。
 - 4 **リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。
 - 5 「**次へ**」をクリックします。
 - 6 エクスポート ウィザードの **宛先** ページにある **仮想マシンにリカバリ** ドロップダウンメニューで、**VirtualBox** を選択します。
 - 7 **Virtual Machine Options** (仮想マシンオプション) ページで **Remote Linux Machine** (リモート Linux マシン) を選択します。
 - 8 次の表の説明に従って、仮想マシンに関する情報を入力します。

表 120. リモート Linux マシンの設定

オプション	説明
VirtualBox ホスト名	VirtualBox サーバーの IP アドレスまたはホスト名を入力します。このフィールドは、リモート VirtualBox サーバーの IP アドレスまたはホスト名を表します。
ポート	マシンのポート番号を入力します。この数値は、Core がこのマシンと通信するときに使用するポートを表します。

オプション	説明
仮想マシン名	作成している仮想マシンの名前を入力します。 ① メモ: デフォルト名は、ソースマシンの名前です。
ターゲットパス	仮想マシンを作成するためのターゲットパスを指定します。 ① メモ: 仮想マシンがルートから実行されるようにするため、ルートフォルダをルートから作成することをお勧めします。ルートを使用しないと、エクスポートを設定する前に、ターゲットマシン上に宛先フォルダを手動で作成する必要があります。また、エクスポート後に仮想マシンを手動でアタッチまたはロードする必要もあります。
ユーザー名	ターゲットマシンにあるアカウントのユーザー名 (root など) です。
パスワード	ターゲットマシンにあるアカウントのパスワードです。
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 ・ ソースマシンと同じ容量の RAM を使用 ・ 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。

9 「初回の1回限りのエクスポートを実施」を選択して、スケジュールされた次回のスケジュール済みスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行します。

10 「次へ」をクリックします。

11 ボリューム ページで、エクスポートするデータのボリュームを選択して 次へ をクリックします。

12 サマリ ページで 終了 をクリックしてウィザードを完了し、エクスポートを開始します。

① | メモ: Virtual Standby ページまたは イベント ページを表示すると、エクスポートのステータスと進捗状況を監視できます。

VMware Workstation 仮想マシンへのデータのエクスポート

Rapid Recovery では、1回限りのエクスポートを実行するか、または連続エクスポート (Virtual Standby の場合) を設定して、データを VMware Workstation にエクスポートできます。エクスポートタイプに合わせて、次の手順を実行します。

1回限りの VMware Workstation エクスポートの実行

VMware Workstation へ 1回限りのエクスポートを実行するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のボタンバーで、**リストア** ドロップダウンメニューをクリックし、**VM エクスポート** をクリックします。
- 2 仮想マシンのエクスポートウィザードで、**1回限りのエクスポート** を選択します。
- 3 「次へ」をクリックします。
- 4 マシン ページで、エクスポートする保護対象マシンを選択します。
- 5 「次へ」をクリックします。
- 6 リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 7 「次へ」をクリックします。
- 8 「エクスポート」ウィザードの「宛先」ページにある「仮想マシンにリカバリ」ドロップダウンメニューで、「**VMware Workstation**」を選択し、「次へ」をクリックします。
- 9 「仮想マシンのオプション」ページで、次の表の説明に従って、仮想マシンにアクセスするためのパラメータを入力します。

表 121. 仮想マシンパラメータ

オプション	説明
VM Machine Location (VM マシンの場所)	仮想マシンを作成するローカルフォルダまたはネットワーク共有のパスを指定します。 メモ: ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なログオン資格情報を入力する必要があります。アカウントにはネットワーク共有に対する読み取りおよび書き込み権限がある必要があります。
ユーザー名	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なユーザー名を入力する必要があります。 - ローカルパスを入力した場合は、ユーザー名は必要ありません。
パスワード	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なパスワードを入力する必要があります。 - ローカルパスを入力した場合は、パスワードは必要ありません。
VM 名	作成される仮想マシンの名前（例：VM-0A1B2C3D4）を入力します。 メモ: デフォルト名は、ソースマシンの名前です。
バージョン	仮想マシンの VMware Workstation のバージョンを指定します。次から選択できます。 - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
RAM 容量 (MB)	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 - ソースマシンと同じ容量の RAM を使用 - 特定容量の RAM を使用し、MB 単位で指定 アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
プロセッサ数	エクスポートされた仮想マシンに使用するプロセッサ (CPU) の数です。最小値は 1 です。
プロセッサあたりの Core 数	各プロセッサに使用する Core 数です。最小値は 1 です。

10 「次へ」をクリックします。

11 「ボリューム」ページで、エクスポートするボリューム (C:\ および D:\ など) を選択し、「次へ」をクリックします。

12 「サマリ」ページで「完了」をクリックしてウィザードを完了し、エクスポートを開始します。

メモ: 「Virtual Standby」または「イベント」タブを表示すると、エクスポートのステータスと進捗状況を監視できます。

連続 (Virtual Standby) VMware Workstation エクスポートの実行

Rapid Recovery を使用して VMware Workstation 仮想マシン (VM) への継続的なエクスポートを実行するには、次の手順を完了します。

1 Rapid Recovery Core Console で、次のいずれかを実行します。

- Core Console から、ボタンバーで  **復元** ドロップダウンメニューをクリックし、**VM エクスポート** を選択します。

- 1 仮想マシンのエクスポートウィザードで、**連続 (Virtual Standby)** を選択します。
- 2 **次へ** をクリックします。

- Core Console から、アイコンバーで  (仮想スタンバイ) をクリックします。

- Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。

- 2 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。
- 3 「**次へ**」をクリックします。
- 4 **リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。
- 5 「**次へ**」をクリックします。
- 6 仮想マシンのエクスポートウィザードの **宛先** ページにある 仮想マシンにリカバリ ドロップダウンメニューで、**VMWare Workstation** を選択し、**次へ** をクリックします。
- 7 **Virtual Machine Options** (仮想マシンオプション) ページで、次の表の説明どおりに仮想マシンにアクセスするためのパラメータを入力します。

表 122. 仮想マシンパラメータ

オプション	説明
ターゲットパス	仮想マシンを作成するローカルフォルダまたはネットワーク共有のパスを指定します。 ① メモ: ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なログオン資格情報を入力する必要があります。アカウントにはネットワーク共有に対する読み取りおよび書き込み権限がある必要があります。
ユーザー名	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なユーザー名を入力する必要があります。 - ローカルパスを入力した場合は、ユーザー名は必要ありません。
パスワード	エクスポート用のネットワークの場所のログオン資格情報を入力します。 - ネットワーク共有パスを指定した場合、ターゲットマシンに登録されたアカウントの有効なパスワードを入力する必要があります。 - ローカルパスを入力した場合は、パスワードは必要ありません。
仮想マシン	作成される仮想マシンの名前 (例: VM-0A1B2C3D4) を入力します。 ① メモ: デフォルト名は、ソースマシンの名前です。
バージョン	仮想マシンの VMware Workstation のバージョンを指定します。次から選択できます。 - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
メモリ	次のいずれかをクリックして、仮想マシンのメモリの使用容量を指定します。 - ソースマシンと同じ容量の RAM を使用 - 特定容量の RAM を使用し、MB 単位で指定

アプリケーションで許可される最低量は 1024 MB で、最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。

プロセッサ数 エクスポートされた仮想マシンに実装するプロセッサ（CPU）の数です。最小値は 1 です。

プロセッサあたり
の Core 数 プロセッサごとに実装する Core 数です。最小値は 1 です。

- 8 「初回の 1 回限りのエクスポートを実施」を選択して、スケジュールされた次のスケジュール済みスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行します。
- 9 「次へ」をクリックします。
- 10 ボリューム ページで、エクスポートするボリューム（C:\ および D:\ など）を選択し、次へをクリックします。
- 11 サマリ ページで 終了 をクリックしてウィザードを完了し、エクスポートを開始します。

① | **メモ:** Virtual Standby ページまたは イベント ページを表示すると、エクスポートのステータスと進捗状況を監視できます。

Hyper-V 仮想マシンへのデータのエクスポート

Rapid Recovery では、1 回限りのエクスポートを実行するか、または連続エクスポート（Virtual Standby の場合）を設定して、データを Hyper-V にエクスポートできます。

Rapid Recovery では、次のホストに対する第 1 世代の Hyper-V エクスポートをサポートしています。

- ・ Windows 8
- ・ Windows 8.1
- ・ Windows Server 2008
- ・ Windows Server 2008 R2
- ・ Windows Server 2012
- ・ Windows Server 2012 R2

Rapid Recovery では、次のホストに対する第 2 世代の Hyper-V エクスポートをサポートしています。

- ・ Windows 8.1
- ・ Windows Server 2012 R2

① | **メモ:** すべての保護対象マシンを Hyper-V generation 2 のホストにエクスポートできるわけではありません。

次の Unified Extensible Firmware Interface (UEFI) オペレーティングシステムを使用している保護対象マシンのみが Hyper-V generation 2 のホストへの仮想エクスポートをサポートしています。

- ・ Windows 8 (UEFI)
- ・ Windows 8.1 (UEFI)
- ・ Windows Server 2012 (UEFI)
- ・ Windows Server 2012 R2 (UEFI)

① | **メモ:** Hyper-V ホストで、エクスポートを実行するために割り当てられている RAM が十分でない場合は、Hyper-V generation 2 の VM への Hyper-V エクスポートは失敗する可能性があります。

エクスポートタイプに合わせて、次の手順を実行します。

1 回限りの Hyper-V エクスポートの実行

Hyper-V に対して 1 回限りのエクスポートを実行するには、次の手順を実行します。

- 1 Rapid Recovery Core Console のボタンバーで、**復元** ドロップダウンメニューをクリックし、**VM エクスポート** をクリックします。
- 2 仮想マシンのエクスポート ウィザードで、**1 回限りのエクスポート** を選択します。
- 3 「次へ」をクリックします。
- 4 マシン ページで、エクスポートする保護対象マシンを選択します。
- 5 「次へ」をクリックします。
- 6 リカバリポイント ページで、エクスポートに使用するリカバリポイントを選択します。
- 7 「次へ」をクリックします。
- 8 宛先 ページにある 仮想マシンへのエクスポート ドロップダウンメニューで、**Hyper-V** を選択します。
- 9 Hyper-V 役割が割り当てられたローカルマシンにエクスポートするには、「**ローカルマシンを使用**」をクリックします。
- 10 Hyper-V サーバがリモートマシンに存在することを示すには、**リモートホスト** をクリックし、次の表の説明に従って、リモートホストの情報を入力します。

表 123. リモートホスト情報

テキストボックス	説明
ホスト名	Hyper-V サーバーの IP アドレスまたはホスト名を入力します。リモート Hyper-V サーバーの IP アドレスまたはホスト名を示します。
ポート	マシンのポート番号を入力します。Core がこのマシンと通信するときに使用するポートを示します。
ユーザー名	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーのユーザー名を入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。
パスワード	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーアカウントのパスワードを入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。

- 11 「次へ」をクリックします。
- 12 仮想マシンオプション ページの **VM マシンの場所** テキストボックスに、仮想マシンのパス（D:\export など）を入力します。これは、仮想マシンの場所を識別するために使用されます。
① メモ: 仮想マシンの場所は、ローカルおよびリモートの両方の **Hyper-V** サーバーで指定する必要があります。このパスは **Hyper-V** サーバーの有効なローカルパスであるようにしてください。存在しないディレクトリが自動的に作成されます。手動で作成しようとししないでください。共有フォルダ（例えば \\data\share）へのエクスポートは許可されません。
- 13 仮想マシン名 テキストボックスに仮想マシンの名前を入力します。
入力する名前は、Hyper-V Manager Console の仮想マシンリストに表示されます。
- 14 メモリの使用容量を指定するには、次のいずれかをクリックします。
 - ・ **ソースマシンと同容量の RAM を使用** 仮想マシンとソースマシン間の RAM 使用量が同じであることを指定する場合は、このオプションを選択します。
 - ・ **指定の RAM 容量を使用する** RAM の容量を MB 単位で指定する場合は、このオプションを選択します。
最低量は 1024 MB、アプリケーションで許可される最大量は 65536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
- 15 ディスクフォーマットを指定するには、「ディスクフォーマット」の横にある次のいずれかをクリックします。
 - ・ VHDX
 - ・ VHD

① **メモ:** ターゲットマシンで **Windows 8 (Windows Server 2012)** 以降が実行されている場合、**Hyper-V** エクスポートでは **VHDX** ディスクフォーマットがサポートされます。お使いの環境で **VHDX** がサポートされていない場合、このオプションは無効になります。

Hyper-V generation 2 にエクスポートする場合は、VHDX ディスクフォーマットのみがサポートされます。

16 エクスポートに使用する Hyper-V の世代を指定するには、次のいずれかをクリックします。

- Generation 1
- Generation 2

① **メモ:** セキュアブートオプションをサポートしているのは、**Generation 2** のみです。

17 エクスポートされた VM の適切なネットワークアダプタを指定します。

18 **Volumes** (ボリューム) ページで、エクスポートするボリューム (複数可) (例: C:\) を選択します。

① **メモ:** 選択されたボリュームが次に示すアプリケーションがサポートする適切な最大割り当てを超えているか、使用可能領域の容量を超えている場合は、エラーが表示されます。

- VHDX ディスクフォーマットでは、選択したボリュームは 64 TB を超えることはできません。
- VHD ディスクフォーマットでは、選択したボリュームは 2040 GB を超えることはできません。

19 ボリューム ページで **終了** をクリックしてウィザードを完了し、エクスポートを開始します。

① **メモ:** **Virtual Standby** ページまたは **イベント** ページを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

連続 (Virtual Standby) Hyper-V エクスポートの実行

Rapid Recovery を使用して Hyper-V 仮想マシン (VM) に対して連続エクスポートを実行するには、この説明の各手順を実行します。

1 Rapid Recovery Core Console で、次のいずれかを実行します。

- Core Console のボタンバーで  **リストア** ドロップダウンメニューをクリックし、**VM のエクスポート** を選択します。
 - 1 仮想マシンのエクスポートウィザードで **連続 (Virtual Standby)** を選択します。
 - 2 **次へ** をクリックします。

- Core Console のアイコンバーで  (Virtual Standby) をクリックします。
 - **Virtual Standby** ページで **追加** をクリックして、仮想マシンのエクスポートウィザードを起動します。

2 仮想マシンのエクスポートウィザードの **マシン** ページで、エクスポートする保護対象マシンを選択します。

3 「**次へ**」をクリックします。

4 **リカバリポイント** ページで、エクスポートに使用するリカバリポイントを選択します。

5 「**次へ**」をクリックします。

6 **宛先** ページの 仮想マシンへエクスポート ドロップダウンメニューで **Hyper-V** を選択し、次のいずれかの手順を実行します。

- Hyper-V 役割が割り当てられたローカルマシンにエクスポートするには、「**ローカルマシンを使用**」をクリックします。
- Hyper-V サーバがリモートマシンに存在することを示すには、**リモートホスト** をクリックし、次の表の説明に従って、リモートホストのパラメータを入力します。

表 124. リモートホスト情報

テキストボックス	説明
ホスト名	Hyper-V サーバーの IP アドレスまたはホスト名を入力します。リモート Hyper-V サーバーの IP アドレスまたはホスト名を示します。
ポート	マシンのポート番号を入力します。Core がこのマシンと通信するときに使用するポートを示します。

テキストボックス 説明

ユーザー名	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーのユーザー名を入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。
パスワード	Hyper-V サーバーを備えたワークステーションに対する管理者権限を持つユーザーアカウントのパスワードを入力します。これは、仮想マシンのログオン資格情報の指定に使用されます。

- 7 「次へ」をクリックします。
- 8 仮想マシンオプション ページの **VM マシンの場所** テキストボックスに、仮想マシンのパス（D:\export など）を入力します。これは、仮想マシンの場所を識別するために使用されます。
 - ① **メモ:** 仮想マシンの場所は、ローカルおよびリモートの両方の **Hyper-V** サーバーで指定する必要があります。このパスは **Hyper-V** サーバーの有効なローカルパスであるようにしてください。存在しないディレクトリが自動的に作成されます。手動で作成しようとししないでください。共有フォルダ（例えば \\data\share）へのエクスポートは許可されません。
- 9 仮想マシン名 テキストボックスに、仮想マシンの名前を入力します。
入力する名前は、Hyper-V Manager Console の仮想マシンリストに表示されます。
- 10 メモリの使用容量を指定するには、次のいずれかをクリックします。
 - ・ **ソースマシンと同容量の RAM を使用。** 仮想マシンとソースマシンの間で RAM の使用量が同じであることを示す場合、このオプションを選択します。
 - ・ **指定の RAM 容量を使用する。** RAM の容量を MB を単位として指定する場合、このオプションを選択します。
アプリケーションで許可される最低量は 1,024 MB で、最大量は 65,536 MB です。メモリの使用容量の最大値はホストマシンが使用できる RAM 容量によって制限されます。
- 11 ディスクフォーマットを指定するには、「ディスクフォーマット」の横にある次のいずれかをクリックします。
 - ・ VHDX
 - ・ VHD
 - ① **メモ:** ターゲットマシンで **Windows 8 (Windows Server 2012)** 以降が実行されている場合、**Hyper-V** エクスポートでは **VHDX** ディスクフォーマットがサポートされます。お使いの環境で **VHDX** がサポートされていない場合、このオプションは無効になります。
Hyper-V generation 2 にエクスポートする場合は、**VHDX** ディスクフォーマットのみがサポートされます。
- 12 エクスポートに使用する Hyper-V の世代を指定するには、次のいずれかをクリックします。
 - ・ Generation 1
 - ・ Generation 2
 - ① **メモ:** セキュアブートオプションをサポートしているのは、**Generation 2** のみです。
- 13 エクスポートされた VM の適切なネットワークアダプタを指定します。
- 14 **Volumes** (ボリューム) ページで、エクスポートするボリューム（複数可）（例：C:\）を選択します。
 - ① **メモ:** 選択されたボリュームが次に示すアプリケーションがサポートする適切な最大割り当てを超えているか、使用可能領域の容量を超えている場合は、エラーが表示されます。
 - ・ VHDX ディスクフォーマットでは、選択したボリュームは 64 TB を超えることはできません。
 - ・ VHD ディスクフォーマットでは、選択したボリュームは 2040 GB を超えることはできません。
- 15 「初回の 1 回限りのエクスポートを実施」を選択して、スケジュールされた次のスケジュール済みスナップショットの後ではなく、直ちに仮想マシンのエクスポートを実行します。
- 16 ボリューム ページで、完了 をクリックしてウィザードを完了し、エクスポートを開始します。
 - ① **メモ:** **Virtual Standby** または **イベント** ページを表示して、エクスポートのステータスおよび進捗状況を監視することができます。

過去のデータ管理

本項では、リポジトリに保存された過去のスナップショットデータを管理する方法について説明します。説明には、リポジトリ内のリカバリポイントの保持、保持ポリシー、容量を節約するためのリカバリポイントをロールアップした結果行われる処理などが

含まれます。リポジトリから Dell の DR バックアップおよび重複排除アプライアンスに、リカバリポイントを再配置する新しい機能について説明します。

また、本項では、ロールアップの対象とはならない長期ストレージのデータをアーカイブする方法と、アーカイブされたリカバリポイントへのアクセス方法について説明します。

Rapid Recovery のデータ保持とアーカイブについて

Core がスナップショットをキャプチャするたびに、そのデータはリカバリポイントとしてリポジトリに保存されます。リカバリポイントは時間の経過に伴い自然に蓄積されます。Core は保持ポリシーを使用して、スナップショットデータがリポジトリに保持される期間を指定します。夜間ジョブのロールアップ期間中、Core は保持ポリシーを適用して、消費されるストレージ容量を低減します。ロールアップ中に各リカバリポイントの日付は最新のリカバリポイントの日付と比較されます。Core は古いリカバリポイントを結合するか「ロールアップ」します。時間の経過に伴い、最も古いリカバリポイントが最も古い保持期間を経過すると「期限切れ」になり、古いリカバリポイントは新しいポイントと最終的に置き換わります。

結合されて最終的に削除されてしまうリカバリポイントを保持するために、Core Console からアーカイブを作成できます。アーカイブとは、Core で保護されているマシンのリカバリポイントが作成された時点の完全なセットを含むファイルです。

アーカイブはファイルシステムまたはクラウド内のストレージアカウントに保存できます。

リカバリポイント内のデータにアクセスする必要がある場合は、後でアーカイブを添付（Rapid Recovery 6.x 以降の場合）またはインポートして、これらのリカバリポイントをリポジトリにリストアできます。現在 Core にある他のリカバリポイントと同様に、そのデータで同じ操作を行うことができます。

① **メモ:** Core はアーカイブでリカバリポイントの元の日付を認識するため、インポートされたリカバリポイントはもう一度ロールアップされるか、次の夜間ジョブの期間中に削除されます。古いリカバリポイントを保持する場合は、関連するマシンのロールアップを無効にするか、保持期間を延長できます。

保持ポリシーの管理

保持ポリシーは、ロールアップの開始前にリカバリポイントを保持するために、Core の時間の長さを指定する規則です。保持ポリシーは時間、日、週、月、年に基づいてロールアップできるように設定できます。最大 6 つの規則を設定できます（デフォルトのポリシーは 5 つ規則を設定します）。

5 分ごとなど頻繁にバックアップを行うことができますので、保持ポリシーの最初の規則はすべてのリカバリポイントを保持する期間を通常に設定します。たとえば、マシンを 15 分ごとにバックアップする場合、ロールアップが開始されるまで 1 日ごとに 96 のリカバリポイントをリポジトリに保存されます。保持ポリシーを管理しないと、データ量によりリポジトリがすぐに一杯になります。

① **メモ:** 管理者は、頻繁にバックアップを行うと、ネットワークトラフィックに影響が出ることに注意する必要があります。ネットワークトラフィックに影響を与える他の要因には、他の転送（レプリケーションなど）、データの変更率、ならびにネットワークのハードウェア、ケーブル、およびスイッチが含まれます。

Core のデフォルト保持ポリシーがあらかじめ設定されています。デフォルトのポリシー機能は以下のものを保持します。

- ・ 3 日間のすべてのリカバリポイント
- ・ 2 日間の 1 時間あたりの 1 つのリカバリポイント
- ・ 4 日間の 1 日あたりの 1 つのリカバリポイント
- ・ 3 週間の週ごとの 1 つのリカバリポイント
- ・ 2 ヶ月の 1 ヶ月あたりの 1 つのリカバリポイント
- ・ X 年間の 1 年あたりの 1 つのリカバリポイント（デフォルトポリシーでは無効）。

このデフォルトのポリシーに従う場合、最も古いリカバリポイントは通常は 92 日前のものです。デフォルトポリシーのその作成日時を過ぎているデータは削除されます。

Core レベルで自動的に保持ポリシーを設定すると、Core によって保護されるマシンのすべてにそれが適用されます。デフォルトポリシーを必要に応じて変更できます。

任意のマシンでは、カスタム保持ポリシーを作成することもできます。マシンレベルでポリシーを設定すると、デフォルトの Core ポリシーとは異なる保持ポリシーを指定できます。保持ポリシーの設定の詳細については、[デフォルト保持ポリシーの設定](#) および [保護対象マシンの保持ポリシー設定のカスタマイズ](#) を参照してください。

デフォルト保持ポリシーの設定

Core の保持ポリシーは、保護対象マシンのリカバリポイントがリポジトリ内に保存される期間を指定します。

Core の保持ポリシーが、夜間ジョブの実行のいずれかのコンポーネントとして実行されるロールアップ処理によって実施されます。次に、保持ポリシーで指定された経過時間を越えたりリカバリポイントが、大まかな期間をカバーする少数のリカバリポイントに「ロールアップ」され（組み合わせられ）ます。保持ポリシーを毎晩適用すると、古いバックアップのロールアップが続行して行われます。この結果、その保持ポリシーに指定されている要件に基づいて最も古いリカバリポイントが削除されます。

別の保持設定を、ソースおよびターゲット Core 用に指定することができます。

① **メモ:** このトピックは、**Rapid Recovery** コアの保持ポリシー設定のカスタマイズに特有のものです。**Core** 上でカスタマイズされた保持ポリシー設定を保存すると、デフォルト保持ポリシー設定が確立され、この設定内容をこの **Core** によって保護されているすべてのマシンに適用できます。個々の保護対象マシンに対する保持ポリシー設定のカスタマイズの詳細については、[保護対象マシンの保持ポリシー設定のカスタマイズ](#) を参照してください。

- 1 Rapid Recovery コアコンソールへ移動します。
- 2 アイコンバーで、 (Settings (設定)) をクリックしてから、次のいずれかを実行します。
 - ・ Setting (設定) ページの左側にある Core 設定のリストから、**Nightly Jobs (夜間ジョブ)** ををクリックします。
 - ・ Settings (設定) ページの右側にスクロールダウンして、**Nightly Jobs (夜間ジョブ)** 見出しを表示します。Nightly Jobs (夜間ジョブ) 設定を表示します。
- 3 **Nightly Jobs (夜間ジョブ)** の下で、 **Change (変更)** をクリックします。**Nightly Jobs (夜間ジョブ)** ダイアログボックスが表示されます。
- 4 必要に応じてバックアップデータを保持する時間間隔を指定するには、Nightly Jobs (夜間ジョブ) ペインで、**Rollup (ロールアップ)** を選択して、**Settings (設定)** をクリックします。
Core のデフォルト保持ポリシーのための **Configuration (設定)** ダイアログボックスが表示されます。
- 5 Core の保持ポリシー設定をデフォルト値に任意のタイミングでリストアするには、Configuration (設定) ダイアログボックスの下で、**Restore Defaults (デフォルトの復元)** をクリックし、**Yes (はい)** をクリックして、確定します。
すべての設定が、[手順 6](#) の表で説明されているデフォルトの値へリストアされます。
- 6 保持ポリシーを定義するには、まず初期バックアップのスナップショットが保持される期間を決定するプライマリ設定を指定します。次に、リカバリポイントをロールアップする間隔を決定するロールアップ要件のカスケードセットの定義に進みます。
次の表では、保持ポリシーの各オプションについて説明します。

表 125. デフォルトの保持ポリシーのスケジュールオプション

テキストボックス	説明
Keep all recovery points for n [retention time period]	リカバリポイントの保持期間を指定します。 (すべて 保持期間を示す数字を入力し、期間を選択します。デフォルトは 3 日間です。)

テキストボックス	説明
のリカバリポイントを n [保持期間] 保持)	日、週、月、または年から選択できます。
...and then keep one recovery point per hour for n [retention time period] (...さらに、1 時間につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとしてプライマリ設定と共に使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 日間です。 日、週、月、または年から選択できます。
...and then keep one recovery point per day for n [retention time period] (...さらに、1 日につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 4 日間です。 日、週、月、または年から選択できます。
...and then keep one recovery point per week for n [retention time period] (...さらに、1 週につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 3 週間です。 週、月、または年から選択できます。
...and then keep one recovery point per month for n [retention time period] (...さらに、1 ヶ月につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 ヶ月間です。 月または年から選択できます。
...and then keep one recovery point per year for n [retention time period] (...さらに、1 年につき 1 つのリカバリポイントを n [保持期間] 保持)	保持期間を示す数字を入力し、期間を選択します。 年から選択できます。

最も古いリカバリポイントは、保持ポリシー設定によって判断されます。

次に、保持期間の計算方法の例を示します。

すべてのリカバリポイントを 3 日間保持します。

...さらに、1 時間ごとに 1 つのリカバリポイントを 3 日間保持

...さらに、1 日ごとに 1 つのリカバリポイントを 4 日間保持

...さらに、1 週ごとに 1 つのリカバリポイントを 3 週間保持

...さらに、1 ヶ月ごとに 1 つのリカバリポイントを 2 ヶ月間保持

...さらに、1 ヶ月ごとに 1 つのリカバリポイントを 1 年間保持

この例では、最も古いリカバリポイントは、1 年 4 ヶ月 6 日前のものになります。

- 7 保持ポリシーの設定を完了したら、**Save (保存)** をクリックします。

Configuration (設定) ダイアログボックスが閉じます。

- 8 **Nightly Jobs (夜間ジョブ)** ダイアログボックスで、**OK** をクリックします。

Nightly Jobs (夜間ジョブ) ダイアログボックスが閉じます。定義した保持ポリシーは、毎晩行われるロールアップ中に適用されます。

また、任意の個々の保護されたマシンの保持ポリシーを指定するときは、これらの設定を適用することができます。保護対象マシンの保持ポリシーの設定についての詳細は、[保護対象マシンの保持ポリシー設定のカスタマイズ](#)を参照してください。

保護対象マシンの保持ポリシー設定のカスタマイズ

保護対象マシンの保持ポリシーはリポジトリ内に保存されるリカバリポイントの長さを指定します。通常、保護される各マシンは、この手順で説明されているように、カスタム保持ポリシーを指定しない限り、Core 用に確立されたデフォルトの保持ポリシーを使用します。

この手順を使用し、複製されたマシンを含む保護対象マシンのカスタム保持ポリシーを定義します。

- 1 Rapid Recovery コアコンソールの Protected Machines (保護されるマシン) メニューから、変更するマシンの名前をクリックします。

選択したマシンの **Summary (概要)** ページが表示されます。

- 2 **Settings (設定)** メニューをクリックします。

Settings (設定) ページが表示され、選択したマシンの設定が表示されます。

- 3 オプションで、**Nightly Jobs (夜間ジョブ)** リンクをクリックして、Settings (設定) ページをスクロールダウンし、夜間ジョブ設定を表示します。

- 4 Nightly Jobs (夜間ジョブ) 見出しの下で、 **Change (変更)** をクリックします。

Nightly Jobs (夜間ジョブ) ダイアログボックスが表示されます。

- 5 必要に応じてバックアップデータを保持する時間間隔を指定するには、**Rollup (ロールアップ)** を選択して、**Settings (設定)** をクリックします。

保持ポリシーの **Configuration (設定)** ダイアログボックスが表示されます。

- 6 複製されたマシンの保持ポリシーをカスタマイズする場合で、ご使用のリポジトリで Integrity Check (整合性チェック) を実行することを通知する警告が表示される場合は、この手順を続行します。それ以外の場合は、次の手順に進みます。

a ジョブを実行する準備ができている場合は、**Check Integrity (整合性チェック)** をクリックします。

b **Yes (はい)** をクリックして、Integrity Check (整合性チェック) のジョブを確認をします。

① メモ: このジョブの実行は、お使いのリポジトリのサイズに基づいており、かなりの時間がかかることがあります。この時間中には、リポジトリ内の他のアクション (スナップショット、レプリケーション、仮想エクスポートなど) は実行できません。このジョブの詳細については、[DVM リポジトリの整合性チェックについて](#)を参照してください。

・ Check Integrity (整合性チェック) のジョブがすべての子ジョブを正常に完了したら、この手順に戻り、次のステップに進みます。

- 7 **Configuration (設定)** ダイアログボックスで、次のいずれかを行います。

- ・ この保護対象マシンにデフォルトの保持ポリシーを使用するには **Use Core default retention policy (コアのデフォルト保持ポリシーを使用)** を選択し、**Save (保存)** をクリックします。デフォルトのポリシーがこのエージェントに適用されます。
- ・ このエージェントのカスタム保持ポリシーをを定義するには、**Use custom retention policy (カスタム保持ポリシーを使用)** を選択し、次のステップに進みます。

Configuration (設定) ダイアログボックスを展開し、カスタム保持ポリシーの情報を表示します。

- 8 次の表にある説明通りに、リカバリポイント保持のカスタムスケジュールを入力します。

表 126. カスタム保持ポリシーのスケジュールオプション

テキストボックス	説明
Keep all recovery points for n [retention time period] (すべて	リカバリポイントの保持期間を指定します。 保持期間を示す数字を入力し、期間を選択します。デフォルトは3日間です。

テキストボックス	説明
のリカバリポイントを n [保持期間] 保持)	日、週、月、年から選択できます。
...and then keep one recovery point per hour for n [retention time period] (...さらに、1 時間につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとしてプライマリ設定と共に使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 日間です。 日、週、月、年から選択できます。
...and then keep one recovery point per day for n [retention time period] (...さらに、1 日につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 4 日間です。 日、週、月、年から選択できます。
...and then keep one recovery point per week for n [retention time period] (...さらに、1 週につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 3 週間です。 週、月、年から選択できます。
...and then keep one recovery point per month for n [retention time period] (...さらに、1 ヶ月につき 1 つのリカバリポイントを n [保持期間] 保持)	より詳細なレベルの保持を指定します。このオプションはビルディイングブロックとして使用され、リカバリポイントを維持する期間をさらに詳細に定義します。保持期間を示す数字を入力し、期間を選択します。デフォルトは 2 ヶ月間です。 月、年から選択できます。
...and then keep one recovery point per year for n [retention time period] (...さらに、1 年につき 1 つのリカバリポイントを n [保持期間] 保持)	保持期間を示す数字を入力し、期間を選択します。 年から選択できます。

次に、保持期間の計算方法の例を示します。

すべてのリカバリポイントを 3 日間保持します。

...さらに、1 時間ごとに 1 つのリカバリポイントを 3 日間保持

...さらに、1 日ごとに 1 つのリカバリポイントを 4 日間保持

...さらに、1 週ごとに 1 つのリカバリポイントを 3 週間保持

...さらに、1 ヶ月ごとに 1 つのリカバリポイントを 2 ヶ月間保持

...さらに、1 ヶ月ごとに 1 つのリカバリポイントを 1 年間保持

この例では、最も古いリカバリポイントは、1 年 3 ヶ月です。

- 9 お使いのプライマリレポジトリですべてのリカバリポイントを保持する場合には、**Relocate outdated recovery points to an R3 repository (R3 レポジトリへ旧式のリカバリポイントを再配置)** オプションをオフにして、次の手順を省略します。
- 10 お使いのプライマリレポジトリからのリカバリポイントを Dell DR シリーズバックアップアプライアンスに保存されている R3 のレポジトリに再配置するには、次の操作を実行します。
 - a **Relocate outdated recovery points to an R3 repository** (古いリカバリポイントを R3 のレポジトリへ再配置) オプションを選択します。

- b お使いのプライマリレポジトリからのリカバリポイントを R3 のレポジトリに再配置する経過時間を指定します。週、月または年で経過時間を指定できます。設定することができますの最短期間は1週間です。
- c **Select a repository (リポジトリの選択)** ドロップダウンメニューから、指定されたリカバリポイントをティアリングする R3 のレポジトリを選択します。

① **メモ:** リカバリポイントは配置場所（ローカル DVM レポジトリまたは DR バックアップアプライアンス上のリモート R3 レポジトリ）に関係なく、保持ポリシーに従属しており、引き続きロールアップされます。以前のリカバリポイントを保持する必要がある場合は、1つの方法としてアーカイブがあります。もう1つのアプローチでは、ロールアップが無効にされるか、関連する保護対象マシンの保持期間が延長されます。

11 **Save (保存)** をクリックします。

保護対象マシンのロールアップの強制実行

リカバリポイントを強制的に作成することで、スケジュールされた保存ポリシーをスキップし、保護対象マシンのレベルでロールアップすることができます。

- 1 Rapid Recovery Core Console の 保護対象マシン メニューから、特定の保護対象マシンの名前をクリックします。選択したマシンの **サマリ** ページが表示されます。
- 2 保護対象マシンのビューの一番上にある **詳細** ドロップダウンメニューをクリックし、**保持ポリシー** を選択します。選択したマシンの **保持ポリシー** ページが表示されます。
- 3 **ロールアップの強制実行** をクリックします。
- 4 ダイアログボックスで、**はい** をクリックして確認します。

Rapid Recovery が、保持ポリシーのスケジュールに関係なく、このマシンのロールアップを開始します。

レプリケーション

本項では、ディザスタリカバリに備えるため、Rapid Recovery ソース Core から Rapid Recovery ターゲット Core への保護対象データのレプリケーションを設定および管理する方法について説明します。

Rapid Recovery でのレプリケーション

本項では、Rapid Recovery でのレプリケーションの概念と設定の手順について説明します。

レプリケーションは、1つの Rapid Recovery Core からリカバリポイントをコピーし、ディザスタリカバリ目的で別の Rapid Recovery Core に送信するプロセスです。このプロセスには、2つ以上の Core 間でのソースとターゲットのペアの関係が必要です。

ソース Core は選択された保護対象マシンのリカバリポイントをコピーした後、非同期的かつ継続的にそのスナップショットデータをターゲット Core に転送します。

レプリケーションのスケジュールを設定してデフォルトの動作を変更しない限り、すべてのバックアップスナップショット、チェックサムチェック、アタッチ可否チェック、夜間ジョブが完了するとすぐに、Core はレプリケーションジョブを開始します。詳細については、「**レプリケーションのスケジュール**」を参照してください。

最適なデータセキュリティを確保するために、管理者は通常、ターゲット Core をリモートディザスタリカバリサイトで使用します。アウトバウンドレプリケーションは、会社が所有するデータセンターやリモートディザスタリカバリサイト（つまり「自己管理型」ターゲット Core）に対して設定することができます。または、オフサイトバックアップおよびディザスタリカバリサービスをホストするサードパーティマネージドサービスプロバイダ (MSP) またはクラウドプロバイダに対して設定することができます。サードパーティのターゲット Core へレプリケートを行う場合は、組み込みのワークフローを使用して接続をリクエストしたり、自動フィードバック通知を受け取ったりすることができます。

レプリケーションは保護対象マシンごとに管理されます。ソース Core で保護またはレプリケートされる任意のマシン（またはすべてのマシン）をターゲット Core にレプリケートするように設定できます。

次のようなレプリケーションのシナリオが考えられます。

- ・ **ローカルの場所へのレプリケーション。** ターゲット Core がローカルデータセンターまたはオンサイトの場所にあり、レプリケーションは常に維持されます。この設定では、Core がなくなってもリカバリは妨げられません。
- ・ **オフサイトの場所へのレプリケーション。** ターゲット Core は、損失が発生した場合のリカバリのため、オフサイトのディザスタリカバリ施設にあります。
- ・ **相互レプリケーション。** 2 つの場所にある 2 つのデータセンターのどちらにも Core があり、マシンを保護していて、お互いにオフサイトディザスタリカバリバックアップとして動作しています。このシナリオでは、それぞれの Core がもう一方のデータセンターにある Core に保護対象マシンをレプリケートします。
- ・ **ホストされているレプリケーションおよびクラウドレプリケーション。** Rapid Recovery MSP パートナーは、データセンターまたはパブリッククラウドで複数のターゲット Core を維持しています。これらの各 Core で、MSP パートナーにより、1 つ、または複数の顧客が、リカバリポイントを顧客のサイトにあるソース Core から MSP のターゲット Core に有料でレプリケートすることができます。

① | **メモ:** このシナリオでは、顧客は自分のデータにだけアクセスできます。

次のようなレプリケーションの設定が考えられます。

- ・ **Point-to-Point レプリケーション。** 1 つ、または複数の保護対象マシンを 1 つのソース Core から 1 つのターゲット Core にレプリケートします。

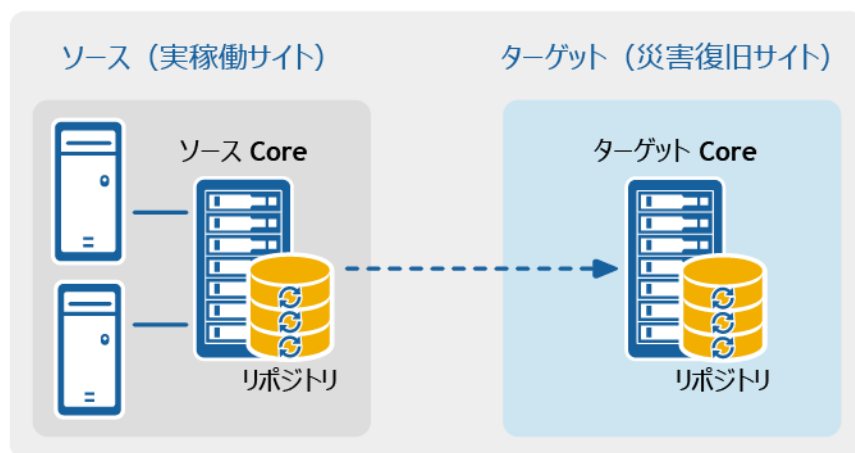


図 9. Point-to-Point レプリケーションの設定

- ・ **Multipoint-to-Point レプリケーション。** 複数のソース Core から 1 つのターゲット Core に保護対象マシンをレプリケートします。

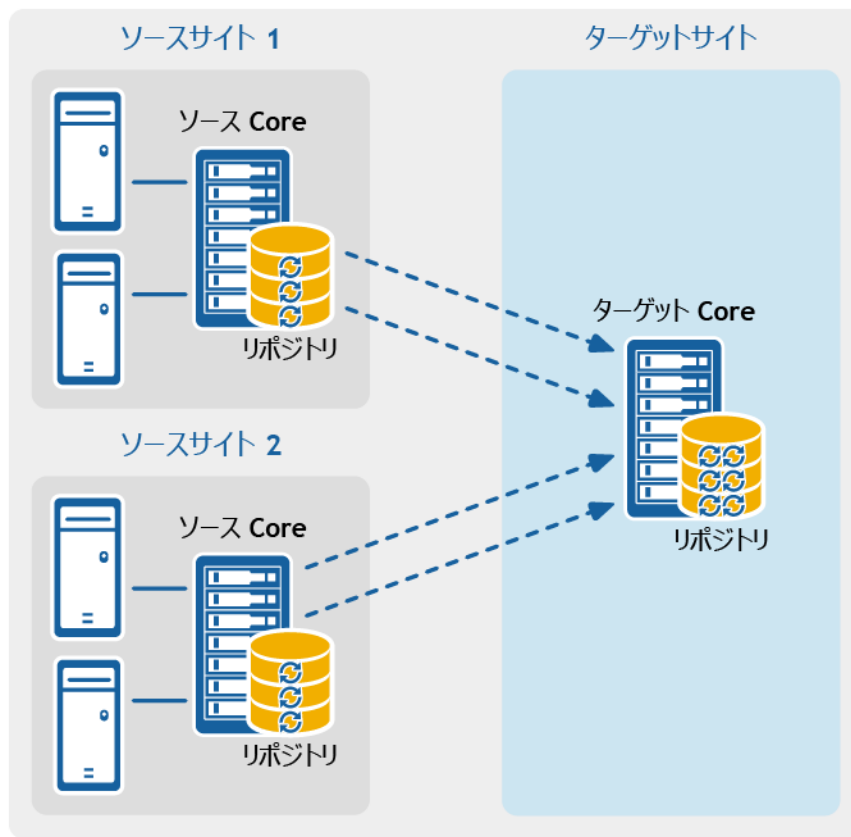


図 10. Multipoint-to-Point レプリケーションの設定

- ・ **Point-to-Multipoint** レプリケーション。1つ、または複数の保護対象マシンを1つのソース Core から複数のターゲット Core にレプリケートします。

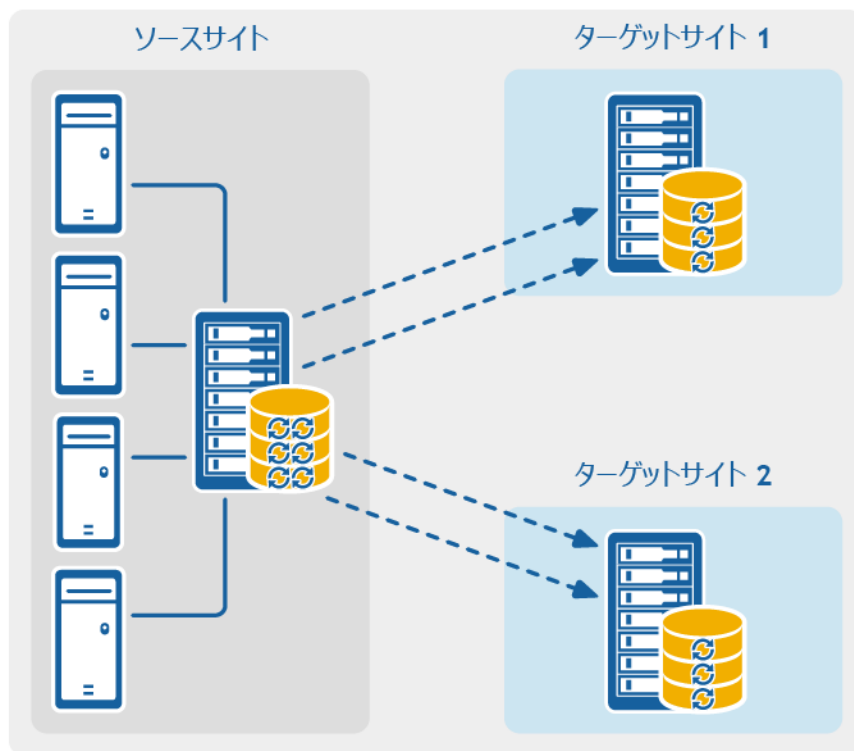


図 11. Point-to-Multipoint レプリケーションの設定

- ・ マルチホップレプリケーション。1つ、または複数の保護対象マシンを1つのターゲット Core から他のターゲット Core にレプリケートして、レプリケートした Core で追加のフェイルオーバーオプションまたはリカバリオプションを生成します。

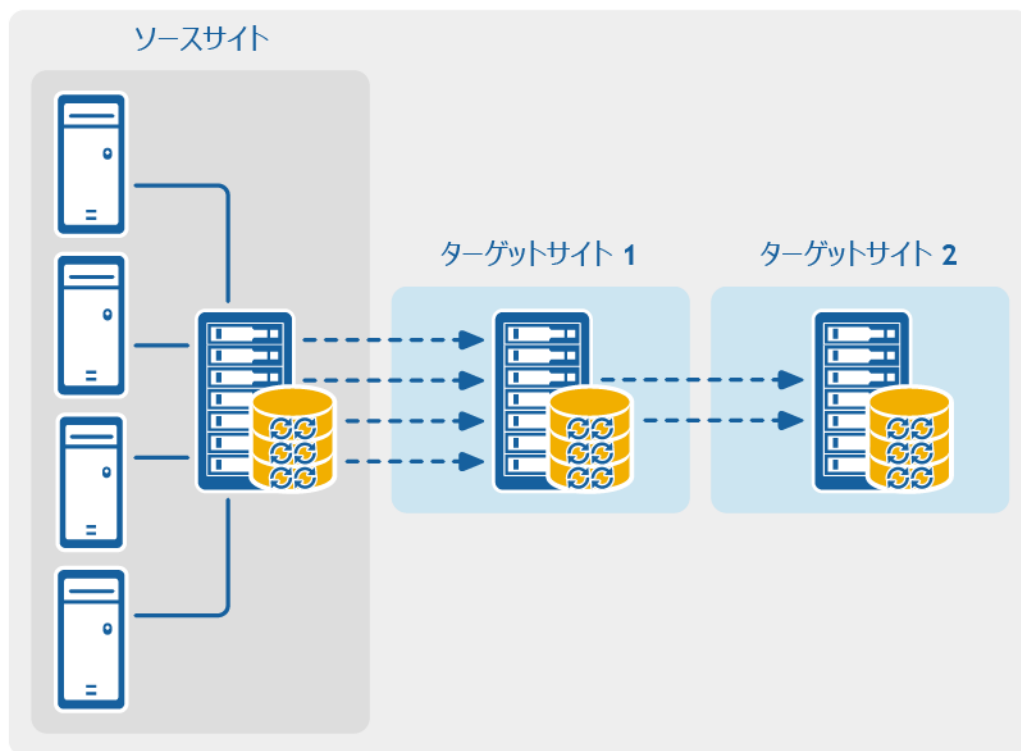


図 12. マルチホップレプリケーションの設定

DL1x00 または DL4x00 シリーズなどの Dell Data Protection バックアップアプライアンスを使用している場合は、レプリケートするターゲット Core に有効なソフトウェアライセンスが設定されている必要があります。これらのハードウェアアプライアンスには購入したレプリケーションターゲットライセンスが含まれます。アプライアンスを購入した際に受信した、ようこそメールメッセージのライセンスキーを確認してください。サポートが必要な場合は、ライセンスアシスタンスウェブサイト (<https://support.software.dell.com/ja-jp/licensing-assistance>) にアクセスするか、license@software.dell.com までメールでお問い合わせください。

リカバリポイントチェーンとオーファン

Rapid Recovery は保護対象マシンのスナップショットをキャプチャし、リカバリポイントとしてデータをリポジトリに保存します。Core に保存される最初のリカバリポイントは、ベースイメージと呼ばれます。ベースイメージには、オペレーティングシステム、アプリケーション、および保護することを選択した各ボリュームの設定と、それらのボリューム上の全データが含まれます。それ以降のバックアップは増分スナップショットになります。これは、保護されたボリュームで最後のバックアップ以降に変更されたデータのみで構成されます。ベースイメージとすべての増分スナップショットを併せて、完全なリカバリポイントチェーンが形成されます。

完全なリカバリポイントチェーンからは、Rapid Recovery で利用可能なあらゆるリカバリオプションを使用して、簡単かつ信頼性に優れた方法でデータを復元することができます。これらのオプションには、ファイルレベルの復元、ボリュームレベルの復元、およびベアメタル復元が含まれます。

存在しないデータを復元することは論理的に不可能なため、リカバリポイントチェーンが不完全な場合、ボリュームレベルでデータを復元したり、ベアメタル復元を実行したりすることはできません。このような場合は、ファイルレベルでリカバリポイントに存在しているデータを復元することだけができます。

リカバリポイントから復元する情報が Core で利用できない以前のバックアップ(以前の増分スナップショットまたはベースイメージ)である場合、そのリカバリポイントはオーファン化していると見なされます。オーファン化したリカバリポイントは、一部のレプリケーションシナリオでよく見られます。

たとえば、最初にレプリケーションを確立したとき、レプリケートされたリカバリポイントから復元できるデータのオプションは限られています。ソース Core からすべてのバックアップデータがターゲット Core に転送され、そのオーファンから完全なリカバリポイントチェーンが作成されるまで、ファイルレベルの復元以外はできなくなります。

レプリケーション開始のタイミング

レプリケーション転送ジョブは、定期的にスケジュールされたバックアップ転送が完了した後すぐにデフォルトで、Core によって自動的にキューに入れます。したがって、保護対象マシンのレプリケーションスケジュールがカスタマイズされないかぎり、そのレプリケーションスケジュールは、標準的なバックアップスナップショットスケジュールに基づいています。

レプリケーションを初めてセットアップするとき、ソース Core 上に1つまたは複数のリカバリポイントが存在する場合は、レプリケーションプロセスが直ちに開始されます。ただし、以下の場合を除きます。

- ・ 最初にレプリケーションを一時停止するオプションを選択している場合。または、
- ・ 初回転送の実行にシードドライブを使用実行にシードドライブを使用するオプションを選択している場合。

最初にレプリケーションを一時停止している場合は、明示的にレプリケーションを再開したときに、レプリケーションが開始されます。

レプリケーションをセットアップしてシードドライブを使用するようにした場合、ターゲット Core へのレプリケーションは、定期的にスケジュールされた次のバックアップスナップショットから開始されます。

① メモ: レプリケーションを確立した後で、保護対象マシンのバックアップを強制的に実行することもできます。これによって、保護対象マシンのスナップショットが完了したらすぐにレプリケーションが開始されます。

レプリケーションのセットアップ時にシードドライブを指定した場合は、将来のバックアップ転送のみがレプリケートされます。元の保護対象マシンから既存のリカバリポイントをターゲット Core 上に保存する場合は、保護対象マシンからデータをシーディングする必要があります。データをシーディングするには、ソース Core からシードドライブを作成し、ターゲット Core でそのシードドライブを消費します。

保護対象マシンのレプリケーションスケジュールをカスタマイズすることもできます。たとえば、1時間ごとに1回バックアップするデフォルトの保護スケジュールを使用している場合は、異なるスケジュールで（毎日、午前2時に1回など）ソース Core からターゲット Core にレプリケートするように指定できます。

シーディングの要件と戦略の決定

以降のトピックでは、レプリケートされたデータからの復元についてと、ソース Core からリカバリポイントデータをシーディングする必要があるかどうかについて説明します。

シーディングデータが必要になる場合

最初にレプリケーションを確立したとき、シードドライブを使用するように指定しない限り、選択されたマシンのすべてのリカバリポイントはソース Core からターゲット Core へ送信され始めます。ネットワーク経由でデータを送信すると長時間かかる場合があります。これには、ネットワークの速度、ネットワークアーキテクチャの堅牢性、およびターゲット Core に送信されるデータの量などが関係しています。たとえば、ソース Core 上のバックアップデータが 10 GB で、WAN リンク転送速度が 24 Mbps の場合、転送が完了するまでに約 1 時間かかることがあります。

ターゲット Core にコピーする情報の量に基づいて、シードドライブは数百から数千ギガバイトにもおよぶデータを追加できます。このため、多くの組織では必要なネットワーク帯域幅を消費する代わりに、シードドライブを定義してこれを消費することを選択しています。詳細については、「[レプリケートされたデータ転送のパフォーマンスに関する考慮事項](#)」を参照してください。

レプリケーションを定義するときにシードドライブを使用するように指定した場合は、レプリケーションの確立後にソース Core に保存されたリカバリポイントのみがターゲット Core へレプリケートされます。レプリケーションの確立前にソース Core に保存されたバックアップは、次のプロセスを使用して明示的にデータをシーディングするまで、ターゲット Core 上に保存されません。

履歴データの転送が集中してネットワークの速度が低下しないようにするためには、**シードドライブ**を使用して以前のバックアップデータをターゲット Core にシーディングします。シードドライブは、ソース Core から一連の重複排除されたベースイメージと増分スナップショットを**コピーする**アーカイブファイルです。シードドライブのファイルには、ソース Core からターゲット Core にレプリケートする、保護されたマシンの以前のリカバリポイントの完全なセットが含まれています。

シードドライブのファイルをストレージボリュームに移動し、ターゲット Core で使用できるようにします。次に、シードドライブからの情報を**消費**します。これには、シードドライブのイメージとボリュームをターゲット Core にアタッチし、Core Console からリポジトリにデータをインポートする作業が含まれます。このプロセスでは、ターゲット Core にレプリケートされた増分スナップショットをそのベースイメージと結びつけてオーファンを修復し、1つ、または複数の完全なリカバリポイントのチェーンが形成されます。このプロセスは、コピー/消費と呼ばれることもあります。

ソース Core からデータをシーディングする必要はありません。たとえば、次のとおりです。

- ・ 新しい Rapid Recovery Core のレプリケーションをセットアップする場合、シーディングは不要です。
- ・ 以前のスナップショットのデータはレプリケーションデータにとって重要ではなく、レプリケーションのセットアップ後に保存されたデータのみを復元する必要があります。シーディングは必要ありません。

① **メモ:** このような場合、Dell では、レプリケーションをセットアップする直前および直後に新しいベースイメージをキャプチャすることをお勧めします。この手順により、ターゲット Core 上に完全なリカバリポイントチェーンが保存され、将来データを復元するために使用できるようになります。

- ・ レプリケーションのセットアップ直前にベースイメージをキャプチャし、それ以降の日付にキャプチャしたデータのみを復元する必要がある場合、シーディングは不要です。
- ・ シードドライブを指定せずにレプリケーションをセットアップした場合は、ネットワーク経由でスナップショットデータがソース Core からターゲット Core に送信されます。

上記のいずれかの状況が当てはまる場合、データをシーディングする必要はありません。このような状況では、ソース Core からレプリケーションを完全に終了させることができます。

既存のリカバリポイントと Core に対するレプリケーションをセットアップし、そのボリュームレベルで復元する必要があり、BMR を実行したり、以前のベースイメージまたは増分スナップショットからデータを復元したりする場合は、シーディングが必要です。このような状況では、シーディングのニーズと戦略について検討してください。このトピックの内容を参照して、ターゲット Core にシーディングするかどうかと使用方法を決定します。

データのシーディング方法

ターゲット Core 上のレプリケーション対象マシンに、元のソース Core 上にある以前保存したデータへのアクセス権を付与する場合は、次のいずれかの方法を使用して ターゲット Core をシーディングします。

- 1 **ネットワーク経由でターゲット Core にシーディングします。**レプリケーションを定義するときにシードドライブを使用するように指定します。これによって、シードドライブが含まれているフォルダをターゲット Core と共有し、ネットワーク経由でシードドライブのファイルを消費できるようになります。データ量が大きい場合や接続速度が遅い場合は、この方法でシーディングすると長時間かかったり、ネットワーク帯域幅を大量に消費したりすることがあります。

① **メモ:** Dell では、ネットワークを経由して大量のデータをシーディングすることはお勧めしません。初回のシーディングでは非常に大きなデータを扱うことがあり、通常の WAN 接続に負担をかける可能性があります。

- 2 **物理ストレージメディアを使用してソース Core からバックアップデータを転送します。**シードドライブのファイルを外付けのポータブルリムーバブルストレージデバイスに転送します。一般に、この方法はデータセットの規模が大きい場合や、サイトのネットワーク接続が遅い場合に便利です。この方法を使用してシーディングを行うには、次の手順を実行します。
 - a ソース Core からシードアーカイブを作成し、リムーバブルメディアにそれを保存します。

- b シードドライブをターゲット Core 上の物理的な場所に移動させます。
- c そのドライブをターゲット Core にアタッチします。
- d ターゲット Core のリポジトリにシードドライブからデータを取り込みます。

サードパーティの Core にレプリケートする場合は、MSP でいったんユーザーのメディアを受信し、通常、データセンターの担当者がそのメディアを添付して、シードデータを Core に取り込む（またはインポートする）準備ができたことをユーザーに通知します。

① **メモ:** 大量のデータをストレージデバイスにコピーする必要があるため、**eSATA、USB 3.0、またはその他の高速接続の使用をお勧めします。**シードデータのアーカイブの合計サイズがリムーバブルメディアの空きスペースより大きい場合、そのアーカイブは複数のデバイスに分けられます。

- 3 ソース Core とターゲット Core が仮想ホストに保存されている場合は、仮想ハードディスクを使用してバックアップデータを転送します。ソース Core とターゲット Core の両方が仮想ホスト上にある場合は、仮想ストレージメディア上にシードドライブを定義して消費することができます。この方法を使用してシーディングを行うには、次の手順を実行します。
 - a シードドライブのファイルをソース Core から作成し、それを仮想ストレージボリュームに保存します。
 - b 対象ボリュームをソース Core からデタッチしてターゲット Core にアタッチします。
 - c ターゲット Core のリポジトリにシードドライブからデータを取り込みます。

① **メモ:** 増分スナップショットのレプリケーションはシーディングが完了する前にソース Core とターゲット Core 間で発生する可能性があります。ソースからターゲットに転送されるレプリケート済みのスナップショットは、初期データが消費されるまでオフライン化したままで、レプリケートされたベースイメージと組み合わせられます。

関連リンク

- ・ シードドライブを使用するプロセスの詳細については、「[ターゲット Core 上のシードドライブの消費](#)」のトピックを参照してください。
- ・ オフライン化したリカバリポイントの詳細については、「[孤立したリカバリポイントチェーンの削除](#)」を参照してください。
- ・ シードドライブの準備については、「[シードドライブについて](#)」と「[ターゲットコア上のシードドライブの消費](#)」を参照してください。

関連するリンク

[ターゲット Core 上のシードドライブの消費](#)
[孤立したリカバリポイントチェーンの削除](#)

レプリケートされたデータ転送のパフォーマンスに関する考慮事項

ソース Core とターゲット Core の間の帯域幅で、保存されているリカバリポイントの転送に対応できない場合は、レプリケーションを設定し、シードドライブを使用するよう指定します。このプロセスでは、ソース Core で保護されている選択済みサーバからのベースイメージとリカバリポイントをターゲット Core にシードします。このシーディングプロセスは、いつでも実行することができます。シーディングは、データの最初の転送の一部として実行できます。これは、定期的に予定されているレプリケーションの基礎として機能します。また、レプリケーションが一時停止または削除されている場合に、以前にレプリケートされたマシンのデータをシードすることもできます。この場合は、「リカバリポイントチェーンを作成」オプションを使用して、まだレプリケートされていないリカバリポイントをシードドライブにコピーすることができます。

レプリケーションを準備するときは、以下の点に注意する必要があります。

- ・ **変更レート。**変更レートは、保護されたデータが蓄積されるレートです。レートは、保護されたボリュームで変化したデータ量とボリュームの保護間隔によって異なります。Exchange 電子メールサーバなど、一部のマシンタイプでは通常、変更レートが高くなっています。変更レートを低くする方法の1つは、保護間隔を短くすることです。
- ・ **帯域幅。**帯域幅は、ソース Core とターゲット Core の間で使用できる転送速度です。レプリケーションが、スナップショットが作成するリカバリポイントに追従できるようにするには、帯域幅が変更レートより大きくしておくことが重要です。Core 間で転送されるデータ量が膨大な場合は、最大 1 GB の Ethernet 接続の有線速度で実行するために、複数のパラレルストリームが必要になることがあります。

① **メモ:** ISP が指定する帯域幅は通常、利用可能な合計帯域幅です。ネットワーク上のデバイスはすべて、発信帯域幅を共有します。レプリケーションが変更レートに対応できるだけの十分な空き帯域幅があることを確認してください。

- ・ **保護対象マシンの数。** ソース Core ごとの保護対象マシンの数と、ターゲット Core にレプリケートをする予定のマシン数を考慮しておくことは重要です。ソース Core で保護されているすべてのマシンのレプリケーションが必要なわけではありません。Rapid Recovery では、保護対象マシンごとにレプリケーションを実行することができるため、必要に応じて、一部のマシンだけをレプリケートすることもできます。ソース Core 上のすべての保護対象マシンをレプリケートする必要がある場合は、通常、変更レートが高くなります。この要因は、ソース Core とターゲット Core 間の帯域幅が、レプリケートされているリカバリポイントの数とサイズに対して不十分な場合に該当します。

次の表に、WAN 接続タイプごとの最大変更レートと、合理的な変更レートで必要なギガバイトあたりの帯域幅の例を示します。

表 127. ギガバイトあたりの帯域幅の例

ブロードバンド	帯域幅	最大変更レート
DSL	768 Kbps 以上	330MB / 時
ケーブル	1 Mbps 以上	429MB / 時
T1	1.5 Mbps 以上	644MB / 時
ファイバー	20 Mbps 以上	8.38GB / 時

① **メモ:** 最適な結果を得るために、次の表に示す推奨事項に従ってください。

データ転送中にリンクが切断された場合は、(リンク機能が回復されると) レプリケーションが前回の不具合ポイントから再開されます。

ネットワーク設定によっては、レプリケーションは非常に時間のかかるプロセスになります。レプリケーション、バックアップなどのその他の Rapid Recovery 転送、および実行する必要があるその他の重要なアプリケーションに対応するために十分な帯域幅を確保してください。

問題が発生した場合は、特に特定の保護対象マシンまたはレプリケートされたマシンにネットワーク上で正常にデータを転送するために、それらのマシンのデータ転送レートを調整することを検討してください。詳細については、「[転送設定の変更について](#)」および「[転送速度のスロットル](#)」を参照してください。

レプリケーションおよび暗号化されたリカバリポイントについて

シードドライブにはソース Core レジストリと証明書のバックアップが含まれていませんが、ソースからターゲットにレプリケートされているリカバリポイントが暗号化されている場合は、ソース Core からの暗号化キーが含まれています。レプリケートされたリカバリポイントは、ターゲット Core に転送された後、暗号化されたままになります。ターゲット Core の所有者または管理者は、暗号化されたデータをリカバリするためのパズルが必要です。

レプリケーションの保持ポリシーについて

ソース Core およびターゲット Core の保持ポリシーは同期されません。ロールアップおよびオンデマンド削除は、初回のアクションや夜間ジョブの際に Core ごとに個別に実行されます。

保持ポリシーの詳細については、「[保持ポリシーの管理](#)」を参照してください。

自己管理ターゲット Core へのレプリケーション

この設定は、オフサイトロケーションへのレプリケーション、および相互レプリケーションに適用されます。次の手順が必要条件です。

- ・ Rapid Recovery コアは、すべてのソースおよびターゲットマシンにインストールする必要があります。
- ・ Rapid Recovery をマルチポイントツーポイントレプリケーションに設定する場合、このタスクをすべてのソース Core と 1 つのターゲット Core で実行する必要があります。これらのレプリケーション設定の説明については、[レプリケーション](#) を参照してください。
- ・ シードドライブを作成し、物理的なリムーバブルストレージボリュームに転送し、既存のリカバリポイントの初期転送を実行する必要がある場合は、適切なポータブルストレージデバイスを用意する必要があります。シードドライブのアーカイブにコピーをアタッチするには、ソース Core マシンに対する物理的アクセスを確保する必要があります。
- ・ 自己管理ターゲット Core でシードドライブを使用している場合、ご自身または信頼できる管理者がターゲット Core に対する物理的アクセスを確保する必要があります。

自己管理ターゲット Core は、アクセスのある Core のことです。たとえば、自己管理 Core はオフサイトロケーションでご自分の会社により管理されるか、ソース Core ではない別の地理的な場所でホストされることがよくあります。シードドライブを使用してデータをシードする選択を行わない限り、レプリケーション全体はソース Core で設定できます。このような場合は、この手順に従ってシードドライブを作成し、後でシードドライブをターゲット Core に後でアタッチし、アーカイブされたリカバリポイントデータを消費する必要があります。詳細については、[シーディングの要件と戦略の決定](#) を参照してください。

次の手順を完了し、自己管理 Core へのレプリケーションを行うためにソース Core を設定します。

- 1 ソース Core の Rapid Recovery コアコンソールへ移動します。
- 2 ボタンバーで、 **Replicate (レプリケーション)** をクリックします。
Replication (レプリケーション) ウィザードが表示されます。
- 3 Replication (レプリケーション) ウィザードの **Target Core (ターゲットコア)** ページで、以前このソース Core とペアにされたターゲット Core でレプリケーションを確立する場合、**Use an existing target Core (既存のターゲット Core を使用)** を選択し、ドロップダウンリストから適切なターゲット Core を選択します。手順 5 に進みます。
- 4 Replication (レプリケーション) ウィザードの **Target Core (ターゲットコア)** ページで、今回初めてこのソース Core からターゲット Core でレプリケーションを確立するには、**I have my own Target Core (自分のターゲット Core があります)** を選択し、次の表の説明に従って情報を入力します。

表 128. ターゲットコアの情報

テキストボックス	説明
ホスト名	レプリケート先のコアマシンのホスト名または IP アドレスを入力します。
ポート	Rapid Recovery コアがマシンと通信するポート番号を入力します。 デフォルトポート番号は 8006 です。
ユーザー名	マシンにアクセスするためのユーザー名を入力します。
パスワード	マシンにアクセスするためのパスワードを入力します。

- 5 **次へ** をクリックします。

① メモ: ターゲットコアにリポジトリが存在しない場合は、ソース Core をターゲット Core とペアにできるが、リポジトリが確立されるまでエージェント (保護対象マシン) をこの場所にレプリケーションできないことを通知する警告が表示されます。リポジトリを Core に設定する方法の詳細については、[DVM リポジトリの作成](#) を参照してください。
- 6 **Request (リクエスト)** ページで、たとえば SourceCore1 というように、このレプリケーションの名前を入力します。これは、ターゲット Core の Replication (レプリケーション) ページの Incoming Replication (受信レプリケーション) ペインで使用される表示名です。
- 7 **次へ** をクリックします。
- 8 **Protected Machines (保護されたマシン)** ページで、レプリケーションする保護対象マシンを選択し、Repository (リポジトリ) 列のドロップダウンリストを使用して各保護対象マシンのリポジトリを選択します。
- 9 ベースデータ転送用のシーディングプロセスを実行する場合は、次の手順を実行します。

① メモ: 大量のデータをポータブルストレージデバイスにコピーするため、ポータブルストレージデバイスには **eSATA、USB 3.0、またはその他の高速接続の使用を Dell はお勧めします。**

- a Replication（レプリケーション）ウィザードの **Protected Machines（保護されたマシン）** ページで、**Use a seed drive to perform the initial transfer（初期転送を実行するためにシードドライブを使用）** を選択します。
- 現在1つまたは複数の保護対象マシンをターゲット Core へ複製している場合、**Include already replicated recovery points in the seed drive（シードドライブにすでにレプリケーションされたリカバリポイントを含める）** を選択することにより、これらの保護対象マシンをシードドライブへ含めることができます。
- b **次へ** をクリックします。
- c Replication（レプリケーション）ウィザードの **Seed Drive Location（シードドライブの場所）** ページで、**Location type（場所のタイプ）** ドロップダウンリストを使用して、次の宛先タイプから選択を行います。
- ローカル
 - ネットワーク
 - クラウド
- d 手順 c で選択した場所のタイプに基づき、次の表の説明に従ってシードドライブファイルの詳細を入力します。

表 129. アーカイブの詳細

オプション	テキストボックス	説明
ローカル	Output Location（出力先）	出力先を入力します。これは、シードドライブアーカイブを格納する場所のパスを定義するために使用されます。たとえば、D:\work\archive などです。
ネットワーク	Output Location（出力先）	出力先を入力します。これは、アーカイブを格納する場所のパスを定義するために使用されます。たとえば、\\servername\sharename などです。
	ユーザー名	ユーザー名を入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。これは、ネットワーク共有のログオン資格情報を確立するために使用されます。
クラウド	Account（アカウント）	ドロップダウンリストからアカウントを選択します。
	Container（コンテナ）	ドロップダウンメニューからお使いのアカウント関連づけられているコンテナを選択します。
	Folder Name（フォルダ名）	アーカイブされたデータを保存するフォルダの名前を指定します。デフォルトの名前は Rapid-Recovery-Archive-[作成日]-[作成時間] です。



メモ: クラウドアカウントを選択するには、最初にコアコンソールに追加しておく必要があります。詳細については、[クラウドアカウントの追加](#) を参照してください。

- e **次へ** をクリックします。
- f Replication（レプリケーション）ウィザードの **Seed Drive Options（シードドライブのオプション）** ページで、次の表の説明に従って情報を入力します。

表 130. シードドライブオプション

アイテム	説明
Maximum size（最大サイズ）	大規模なデータのアーカイブは複数のセグメントに分割することができます。次の操作のいずれかを行って、シードドライブ作成のために予約するセグメントの最大サイズを選択します。 Seed Drive Location（シードドライブの場所）ページで入力したパスに、今後の使用のために使用可能な容量をすべて予約するには、Entire Target（ターゲット全体） を選択します。たとえば、場所が D:\work\archive になっていると、シードドライブのコピーに必要な場合に D: ドライブ上の使用可能な容量すべてが予約されますが、コピープロセスを開始してすぐには予約されません。

アイテム	説明
	・ 予約したい最大容量をカスタマイズするには、テキストボックスを選択し、値を入力して、ドロップダウンリストから値の単位を選択します。デフォルトは 250 MB です。
Recycle action (リサイクルアクション)	パスにすでにシードドライブが含まれている場合は、次のいずれかのオプションを選択します。 ・ Do not reuse (再使用しない)。その場所の既存のデータを上書きしたり、クリアしたりしません。その場所が空の場合、シードドライブの書き込みは失敗します。 ・ Replace this core (このコアを置き換える)。このコアに関連する既存シードデータを上書きしますが、他のコアのデータはそのまま残します。 ・ Erase completely (完全に消去)。シードドライブを書き込む前にディレクトリからすべてのデータをクリアします。
Comment (コメント)	シードドライブを説明するコメントを入力します。
Add all Agents to Seed Drive (シードドライブにすべてのエージェントを追加する)	シードドライブを使用するソースコア上のすべての保護対象マシンをレプリケーションするために、このオプションを選択します。このオプションはデフォルトで選択されます。
Build recovery point chains (fix orphans) (リカバリポイントチェーンの構築 (オーフアン ^① の修正))	リカバリポイントチェーン全体をシードドライブに複製するには、このオプションを選択します。このオプションはデフォルトで選択されています。 メモ: AppAssure 5.4 での一般的なシーディングでは、最新のリカバリポイントのみをシードドライブに複製することによって、シードドライブの作成に必要な時間と容量を軽減しました。シードドライブへのリカバリポイント (RP) チェーンの構築を選択すると、指定された保護対象マシンからの最新リカバリポイントを保存するために十分な容量がシードドライブ上に必要であり、その作業を完了するためにさらに時間がかかる場合があります。

g 次の手順のいずれか 1 つを実行します。

- ・ **Add all Agents to Seed Drive (すべてのエージェントをシードドライブに追加)** チェックボックスをオフにした場合は、**Next (次へ)** をクリックします。
- ・ **Add all Agents to Seed Drive (すべてのエージェントをシードドライブに追加)** を選択した場合は、手順 10 に進みます。

h Replication (レプリケーション) ウィザードの **Protected Machines (保護されたマシン)** ページで、シードドライブを使用してターゲット Core にレプリケーションを行う保護対象マシンを選択します。

10 **終了** をクリックします。

11 シードドライブを作成した場合は、お使いのターゲットコアに送信します。
ソース Core のターゲット Core とのペアリングが完了しました。

- 最初にレプリケーションを一時停止するオプションが選択されていない限り、レプリケーションプロセスはすぐに開始されます。
- 1 シードドライブを使用するオプションを選択した場合は、シードドライブが消費され、必要なベースイメージが提供されるまでは、レプリケーションがターゲット Core に孤立したリカバリポイントを生成します。
 - 2 ドライブの使用を指定した場合、シードドライブのアーカイブファイルがボリューム (共有フォルダ、仮想ディスク、またはリムーバブルストレージメディア) に転送されます。次に、シードドライブが消費されます。

入力方向および出力方向のレプリケーションの表示

アイコンバーから **レプリケーション**  アイコンをクリックすると、**レプリケーション** ページが表示されます。このページでは、Core のスコープからレプリケーションについて理解することができます。このページには 2 つのペインがあります。

- ・ **出力方向のレプリケーション** ペインには、この Core で保護されていて、別の Core 上にレプリケートされるマシンがリストされます。

- ・ **入力方向のレプリケーション** ペインには、この Core にレプリケートされるマシンと、これらのマシンにレプリケートされるソース Core がリストされます。

この項では、これらのペインに表示される情報について説明します。

次の表では、Rapid Recovery Core から出力されるレプリケーションに関する情報について説明しています。

表 131. 出力方向のレプリケーションに関する情報

UI エlement	説明
アイテムの選択	サマリ表の列ごとにチェックボックスをオンにして、テーブルの上にあるメニューオプションのリストからアクションを実行することができます。
タイプ	マシンタイプを表示します。ターゲット Core を展開して、レプリケートされた各マシンを表示することができます。
ステータスインジケータ	レプリケーションのステータス。「ステータス」列の色付きの円は、レプリケートされたマシンがオンラインであるか到達不能であることを示します。色付きの円にカーソルを合わせると、ステータス状態が表示されます。ステータス状態には、緑（レプリケーションが確立済みでオンライン）、黄色（レプリケーションが一時停止中）、赤（認証エラー）、灰色（オフラインまたは到達不能）があります。
レプリケーション名	マシンにこのソース Core からレプリケートされる Core マシンの表示名。
マシン	選択したターゲット Core にレプリケートされたマシンの数をリストします。
同期化	ターゲット Core にレプリケーションが最後に転送された日付と時刻。
	この行でアクション ドロップダウンメニューをクリックした場合、実行すると特定のレプリケーション関係に影響を与えるアクションのリストが表示されます。

出力方向のレプリケーション グリッドにリストされた 2 つ以上のターゲット Core で、アクションを実行できます。複数のターゲット Core でアクションを実行するには、グリッドの各 Core のチェックボックスをオンにして、グリッドの上にあるメニューから実行するアクションを選択します。次の表で説明されているアクションを実行できます。

表 132. 出力方向のレプリケーション ペインで利用できるグローバルアクション

UI エlement	説明
ターゲット Core を追加	ソース Core 上の保護対象マシンをレプリケートするように、別のターゲット Core マシンを定義できます。
更新	テーブル内の表示されている情報を更新します。
Force	レプリケーションを強制実行します。
Pause	確立されたレプリケーションを一時停止します。
Resume	一時停止したレプリケーションを再開します。
Copy	レプリケーションウィザードを開いて、選択した保護対象マシンの既存のリカバリポイントをシードドライブにコピーします。
Delete	出力方向のレプリケーションを削除します。
シードドライブ	このメニューオプションは、レプリケーションのセットアップ時にデータがシードドライブにコピーされていると表示されます。 シードドライブの保存日時など、シードドライブのファイルに関する情報が表示されます。ターゲット Core とシードドライブのファイルが生成された保護対象マシンを示す、折り畳み可能なメニュー。

UI エlement	説明
	この行でアクション ドロップダウンメニューをクリックした場合、実行すると特定のレプリケーション関係に影響を与えるアクションのリストが表示されます。

次の表では、別のコアからの入力方向のレプリケーションに関する情報について説明しています。

表 133. 入力方向のレプリケーションに関する情報

UI エlement	説明
アイテムの選択	サマリテーブルの列ごとにチェックボックスをオンにして、テーブルの上にあるメニューオプションのリストからアクションを実行することができます。
タイプ	マシンタイプを表示します。ソース Core を展開して、レプリケートされた各マシンを表示することができます。
ステータスインジケータ	レプリケーションのステータス。「ステータス」列の色付きの円は、レプリケートされたマシンがオンラインであるか到達不能であることを示します。色付きの円にカーソルを合わせると、ステータス状態が表示されます。ステータス状態には、緑（レプリケーションが確立済みでオンライン）、黄色（レプリケーションが一時停止中）、赤（認証エラー）、灰色（オフラインまたは到達不能）があります。
レプリケーション名	現在のターゲット Core 上にレプリケートされる保護対象マシンを含む、ソース Core マシンの表示名。レプリケーションウィザードを使用してソース Core 上にレプリケーションを確立した場合は、必要に応じてこの名前を指定することができます。
マシン	ターゲット Core にレプリケートされるソース Core 上で保護されているマシンの数がリストされます。
同期化	ソース Core からレプリケーションが最後に転送された日付と時刻。
	この行でアクション ドロップダウンメニューをクリックした場合、実行すると特定のレプリケーション関係に影響を与えるアクションのリストが表示されます。

入力方向のレプリケーション グリッドにリストされた 2 つ以上のソース Core で、アクションを実行できます。複数のソース Core でアクションを実行するには、グリッドの各 Core のチェックボックスをオンにして、グリッドの上にあるメニューから実行するアクションを選択します。次の表で説明されているアクションを実行できます。

表 134. 入力方向のレプリケーション ペインで利用できるグローバルアクション

UI エlement	説明
更新	テーブル内の表示されている情報を更新します。
Force	レプリケーションを強制実行します。
Pause	確立されたレプリケーションを一時停止します。
Resume	一時停止したレプリケーションを再開します。
Delete	入力方向のレプリケーションを削除します。

レプリケーションの設定

Rapid Recovery を使用してデータをレプリケートするには、ソースコアおよびターゲットコアをレプリケーション用に設定する必要があります。レプリケーションの設定後、保護対象マシンのデータのレプリケーション、レプリケーションの監視と管理、およびリカバリの実行を行うことができます。

Rapid Recovery でのレプリケーションの実行には、以下の操作の実行が含まれます。

- ・ ターゲットコア上にリポジトリをセットアップします。ターゲットコアへリポジトリの追加する詳細については、[DVM リポジトリの作成](#) を参照してください。
- ・ 自己管理複製の設定。自己管理ターゲットコアへの複製の詳細については、「[自己管理ターゲット Core へのレプリケーション](#)」を参照してください。
- ・ 第三者のレプリケーションを設定します。第三者ターゲットコアへレプリケーションを行う詳細については、[サードパーティのターゲット Core へのレプリケート](#) を参照してください。
- ・ 既存の保護対象マシンをレプリケートします。ソースコアによってすでに保護されているマシンをレプリケートする詳細については、[既存のレプリケーションへのマシンの追加](#) を参照してください。
- ・ シードドライブを消費します。ターゲットコアにおけるシードドライブデータの消費の詳細については、[ターゲット Core 上のシードドライブの消費](#) を参照してください。
- ・ レプリケーションの優先順位を保護対象マシンに対して設定します。保護対象マシンのレプリケーションの優先順位付けの詳細については、[保護対象マシンのレプリケーション優先度の設定](#) を参照してください。
- ・ 保護対象マシンのレプリケーションスケジュールを設定します。レプリケーションスケジュールの設定の詳細については、[レプリケーションのスケジュール](#) を参照してください。
- ・ 必要に応じてレプリケーションを監視します。レプリケーションの監視の詳細については、[入力方向および出力方向のレプリケーションの表示](#) を参照してください。
- ・ 必要に応じた複製設定の管理。複製設定の管理の詳細については、「[レプリケーション設定の管理](#)」を参照してください。
- ・ 災害またはデータ損失の発生時の複製済みデータのリカバリ。複製済みデータのリカバリの詳細については、「[レプリケートされたデータのリカバリ](#)」を参照してください。

サードパーティのターゲット Core へのレプリケート

サードパーティ Core は、MSP によって管理、維持されているターゲット Core です。サードパーティによって管理されている Core にレプリケートする場合、ユーザーはターゲット Core にアクセスする必要がありません。

サードパーティ Core へのレプリケートプロセスには、ユーザーおよびサードパーティが実行する必要があるタスクがあります。ユーザーがソース Core または Core でのレプリケーションのリクエストを送信した後で、MSP がそのリクエストを確認して、ターゲット Core の設定を完了する必要があります。

- ① **メモ:** この設定は、ホストされたレプリケーションおよびクラウドレプリケーションに適用されます。**Rapid Recovery Core** は、すべてのソース **Core** マシンにインストールされている必要があります。マルチポイントツーポイントレプリケーション用に **Rapid Recovery** を設定している場合は、すべてのソース **Core** でこのインストールタスクを実行する必要があります。

サードパーティによって管理されているターゲット Core をレプリケートするには、次のタスクを実行します。

- ・ サードパーティサービスプロバイダへのレプリケーションリクエストの送信
- ・ カスタマからのレプリケーションリクエストの確認
- ・ カスタマからのレプリケーションリクエストの無視

サードパーティサービスプロバイダへのレプリケーションリクエストの送信

サードパーティによって管理されている Core をサブスクリプションしている MSP などのエンドユーザーの場合、サードパーティサービスプロバイダにレプリケーションリクエストを送信するには、次の手順を実行します。

- 1 Rapid Recovery Core に移動します。
- 2 アイコンボタンのバーで  **レプリケート** をクリックします。
レプリケーションウィザード が表示されます。
- 3 レプリケーションウィザードの **ターゲット Core** ページで、**オフサイトバックアップとディザスタリカバリサービスを提供するサードパーティに対するサブスクリプションがある** を選択し、次の表の説明に従って情報を入力します。

表 135. サードパーティのターゲット Core の情報

テキストボックス	説明
ホスト名	サードパーティの Core マシンのホスト名、IP アドレス、または FQDN を入力します。
ポート	第三者サービスプロバイダから提供されたポート番号を入力します。 デフォルトポート番号は 8006 です。

- ・ 追加する必要がある Core が以前にソース Core とペアリングされていた場合は、次の手順を実行できます。
 - 1 「既存のターゲット Core を使用」を選択します。
 - 2 ドロップダウンリストからターゲット Core を選択します。
 - 3 「次へ」をクリックします。
 - 4 手順 7 に進みます。
- 4 「次へ」をクリックします。
- 5 レプリケーションウィザードの リクエスト ページで、次の表の説明に従って情報を入力します。

表 136. サードパーティのターゲット Core の詳細

テキストボックス	説明
電子メールアドレス	サードパーティサービスのサブスクリプションに関連付けられている電子メールアドレスを入力します。
カスタマ ID (省略可能)	必要に応じて、サービスプロバイダによって割り当てられたカスタマ ID を入力します。

- 6 「次へ」をクリックします。
- 7 レプリケーションウィザードの 保護対象マシン ページで、サードパーティの Core にレプリケートする保護対象マシンを選択します。
- 8 ベースデータを転送するためにシーディングプロセスを実行する場合は、次の手順を実行します。

① **メモ:** 大量のデータをポータブルストレージデバイスにコピーする必要があるため、ポータブルストレージデバイスには **eSATA、USB 3.0、またはその他の高速接続の使用をお勧めします。**

- a レプリケーションウィザードの 保護対象マシン ページで、初回転送の実行に **シードドライブを使用** を選択します。
 - ・ 現在、1 台または複数の保護対象マシンをターゲット Core にレプリケートしている場合は、**レプリケート済みのリカバリポイントをシードドライブに含める** オプションをオンにして、そのシードドライブにこれらのマシンを含めることができます。
- b 「次へ」をクリックします。
- c レプリケーションウィザードの **シードドライブの場所** ページで、**場所** タイプのドロップダウンリストを使用して、次の宛先タイプの中から選択します。
 - ・ ローカル
 - ・ ネットワーク
 - ・ クラウド
- d 手順 c で選択した場所のタイプに基づき、次の表の説明に従ってアーカイブの詳細を入力します。

表 137. アーカイブの詳細

オプション	テキストボックス	説明
ローカル	出力先	出力の場所を入力します。D:\work\archive など、アーカイブを格納するシードドライブの場所のパスを定義するために使用されます。
ネットワーク	出力先	出力の場所を入力します。\\servername\sharename など、アーカイブを格納する場所のパスを定義するために使用されます。

オプション	テキストボックス	説明
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
クラウド	アカウント	ドロップダウンリストからアカウントを選択します。
		① メモ: クラウドアカウントを選択するには、先に、Core Console にクラウドアカウントが追加されている必要があります。詳細については、「クラウドアカウントの追加」を参照してください。
	コンテナ	ドロップダウンメニューからアカウントに関連付けられているコンテナを選択します。
	フォルダ名	アーカイブデータの保存先のフォルダ名を入力します。デフォルト名は、Rapid-Recovery-Archive-[作成日]-[作成時間] です。

e 「次へ」をクリックします。

f レプリケーションウィザードの **シードドライブのオプション** ページで、次の表の説明に従って情報を入力します。

表 138. シードドライブのオプション

アイテム	説明
最大サイズ	容量の大きいデータアーカイブは、複数のセグメントに分割できます。次のいずれかを実行して、シードドライブを作成するために確保する必要のある最大領域サイズを選択します。 「ターゲット全体」を選択して、「シードドライブの場所」 ページで指定されたパスのすべての使用可能な領域を確保します（たとえば、場所が D:\work\archive である場合は、D: ドライブ上のすべての使用可能な領域が確保されます）。 - 空白のテキストボックスを選択して、数量を入力し、ドロップダウンリストから単位を選択して、確保する最大領域をカスタマイズします。
リサイクルアクション	パスにすでにシードドライブが含まれている場合は、次のいずれかのオプションを選択します。 再使用不可。 この場所から既存のシードデータを上書きまたはクリアしません。指定の場所が空の場合、シードドライブの書き込みは失敗します。 この Core を置換。 この Core に関連する既存のシードデータを上書きしますが、他の Core のデータはそのまま残します。 完全に消去。 シードドライブへの書き込みの前にディレクトリからすべてのシードデータを消去します。
コメント	シードドライブを説明するコメントを入力します。
すべての Agent をシードドライブに追加	シードドライブを使用してソース Core のすべての保護対象マシンをレプリケートするには、このオプションを選択します。このオプションは、デフォルトで、選択されています。
リカバリポイントチェーンを作成 (オフライン修正)	シードドライブにリカバリポイントチェーン全体をレプリケートするには、このオプションを選択します。このオプションは、デフォルトで、選択されています。 ① メモ: AppAssure 5.4 での通常のシーディングでは、最新のリカバリポイントのみをシードドライブにレプリケートすることで、シードドライブの作成に必要な時間と領域を削減します。シードドライブにリカバリポイント (RP) チェーンを作成する場合は、指定の 1 つ以上の保護対象マシンの最新のリカバリポイントを保存できる十分な領域がシードドライブに必要です。また、このタスクの完了にさらに時間がかかる場合があります。

g 次の手順のいずれかを実行します。

- 「**すべての Agent をシードドライブに追加**」チェックボックスをオフにした場合は、「次へ」をクリックします。

- ・ **すべてのエージェントをシードドライブに追加** チェックボックスをオンにした場合は、[手順 9](#)に進みます。
- h レプリケーションウィザードの **マシン** ページで、シードドライブを使用してターゲット Core にレプリケートする保護対象マシンを選択します。
- 9 「終了」をクリックします。
 - 10 シードドライブを作成した場合は、サードパーティサービスプロバイダの説明に従ってシードドライブを送信します。

カスタマからのレプリケーションリクエストの確認

エンドユーザーが「サードパーティサービスプロバイダへのレプリケーションリクエストの送信」の手順を完了すると、レプリケーションリクエストが、ソース Core からサードパーティのターゲット Core に送信されます。サードパーティとして、リクエストを確認してから、お客様のレプリケーション開始を承認するか、リクエストを拒否してレプリケーションの実行を回避することができます。

次のオプションから選択します。

- ・ [レプリケーションリクエストの承認](#)
- ・ [レプリケーションリクエストの拒否](#)

レプリケーションリクエストの承認

サードパーティのターゲット Core でのレプリケーションリクエストを承認するには、次の手順を実行します。

- 1 ターゲット Core で Rapid Recovery Core Console に移動します。
 - 2 アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
 - 3 レプリケーション ページで **リクエスト (#)** をクリックします。
Pending Replication Requests (保留中の複製リクエスト) セクションが表示されます。
 - 4 「保留中のレプリケーションリクエスト」で、確認するリクエストの横にあるドロップダウンメニューをクリックして、「**確認**」をクリックします。
Review Replication Request (レプリケーションリクエストの確認) ウィンドウが表示されます。
- ① **メモ:** このウィンドウの「ソース Core ID」セクションに表示される情報は、カスタマが実行するリクエストによって決まります。
- 5 「ソース Core ID」で、次のいずれかを実行します。
 - ・ **Replace an existing replicated Core** (既存のレプリケーション済みコアの置き換え) を選択して、ドロップダウンリストからコアを選択します。
 - ・ **新規のソース Core を作成** を選択し、指定されている Core 名、カスタマの電子メールアドレス、およびカスタマ ID が正しいことを確認します。必要に応じて、情報を編集します。
 - 6 「Agents」で、承認の適用先のマシンを選択して、「リポジトリ」列のドロップダウンリストを使用して各マシンで適切なリポジトリを選択します。
 - 7 必要に応じて、**コメント** テキストボックスに、カスタマへの応答に含める説明またはメッセージを入力します。
 - 8 「**応答を送信**」をクリックします。
レプリケーションが許可されます。

レプリケーションリクエストの拒否

カスタマからサードパーティ Core に送信されたレプリケーションリクエストを拒否するには、次の手順を実行します。

リクエストを確認せずに拒否するには、「[カスタマからのレプリケーションリクエストの無視](#)」を参照してください。

- 1 ターゲット Core で Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
- 3 レプリケーション ページで リクエスト (#) をクリックします。
Pending Replication Requests (保留中の複製リクエスト) セクションが表示されます。
- 4 「保留中のレプリケーションリクエスト」で、確認するリクエストの横にあるドロップダウンメニューをクリックして、「**確認**」をクリックします。
Review Replication Request (レプリケーションリクエストの確認) ウィンドウが表示されます。
- 5 「**拒否**」をクリックします。
レプリケーションが拒否されます。ソース Core のイベントページのアラートに、拒否の通知が表示されます。

カスタマからのレプリケーションリクエストの無視

ターゲット Core のサードパーティサービスプロバイダは、カスタマから送信されたレプリケーションリクエストを無視することができます。このオプションは、リクエストが誤って送信された場合や、リクエストを確認することなく拒否する場合に、使用できます。

レプリケーションリクエストの詳細については、「[カスタマからのレプリケーションリクエストの確認](#)」を参照してください。

カスタマからのレプリケーションリクエストを無視するには、次の手順を実行します。

- 1 ターゲット Core で Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
- 3 レプリケーション ページで リクエスト (#) をクリックします。
Pending Replication Requests (保留中の複製リクエスト) セクションが表示されます。
- 4 「保留中のレプリケーションリクエスト」で、無視するリクエストの横にあるドロップダウンメニューをクリックして、「**無視**」をクリックします。
- 5 **リクエストを無視します** ダイアログボックスで、**はい** をクリックしてコマンドを確認します。
リクエストが無視されたという通知がソース Core に送信され、ターゲット Core のレプリケーションページから、そのリクエストが削除されます。

既存のレプリケーションへのマシンの追加

ソース Core とターゲット Core との間でレプリケーションが確立された後は、ターゲットにレプリケートする新しい保護対象マシンを追加できます。レプリケーション用にペアリングされたターゲット Core に新しい保護対象マシンを追加するには、次の手順をソース Core で実行します。

レプリケーションの詳細については、「[レプリケーション](#)」および「[自己管理ターゲット Core へのレプリケーション](#)」を参照してください。

- 1 ソース Core の Rapid Recovery Core Console に移動します。
- 2 ボタンバーで  レプリケート をクリックします。
保護対象マシン ページで レプリケーションウィザードが開きます。
- 3 **保護対象マシン** ページで、レプリケートする保護対象マシンを選択し、リポジトリ列のドロップダウンリストを使用して各保護対象マシンのリポジトリを選択します。

4 ベースデータを転送するためにシーディングプロセスを実行する場合は、次の手順を実行します。

① **メモ:** 大量のデータをポータブルストレージデバイスにコピーするため、ポータブルストレージデバイスには **eSATA、USB 3.0、またはその他の高速接続の使用をお勧めします。**

- a レプリケーションウィザードの **保護対象マシン** ページで **初回転送の実行にシードドライブを使用** を選択します。
 - ・ 現在、1台または複数の保護対象マシンをターゲット Core にレプリケートしている場合は、**レプリケート済みのリカバリポイントをシードドライブに含める** を選択して、これらのマシンをシードドライブに含めることができます。
- b 「次へ」をクリックします。
- c ウィザードの **シードドライブの場所** ページで **場所のタイプ** ドロップダウンリストを使用して、次の宛先タイプから選択します。
 - ・ ローカル
 - ・ ネットワーク
 - ・ クラウド
- d 手順 c で選択した場所のタイプに基づき、次の表の説明に従ってアーカイブの詳細を入力します。

表 139. アーカイブの詳細

オプション	テキストボックス	説明
ローカル	出力先	出力の場所を入力します。d:\work\archive などアーカイブを格納する場所のパスの定義のために使用されます。
	出力先	出力の場所を入力します。\\servername\sharename などアーカイブを格納する場所のパスの定義のために使用されます。
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
ネットワーク	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	アカウント	ドロップダウンリストからアカウントを選択します。
	コンテナ	ドロップダウンメニューからアカウントに関連付けられているコンテナを選択します。
クラウド	フォルダ名	アーカイブデータの保存先のフォルダ名を入力します。デフォルト名は、Rapid-Recovery-Archive-[作成日]-[作成時間] です。

① **メモ:** クラウドアカウントを選択するには、先に、**Core Console** にクラウドアカウントが追加されている必要があります。詳細については、「**クラウドアカウントの追加**」を参照してください。

- e 「次へ」をクリックします。
- f ウィザードの **シードドライブのオプション** ページで、次の表の説明に従って情報を入力します。

表 140. シードドライブのオプション

アイテム	説明
最大サイズ	容量の大きいデータアーカイブは、複数のセグメントに分割できます。次のいずれかを実行して、シードドライブを作成するために確保する必要のある最大領域サイズを選択します。 ・ 「ターゲット全体」を選択して、「シードドライブの場所」 ページで指定されたパスのすべての使用可能な領域を確保します（たとえば、場所が D:\work\archive である場合は、D: ドライブ上のすべての使用可能な領域が確保されます）。

アイテム	説明
	空白のテキストボックスを選択して、数量を入力し、ドロップダウンリストから単位を選択して、確保する最大領域をカスタマイズします。
リサイクルアクション	パスにすでにシードドライブが含まれている場合は、次のいずれかのオプションを選択します。 - 再使用不可。この場所から既存のシードデータを上書きまたはクリアしません。指定の場所が空の場合、シードドライブの書き込みは失敗します。 - この Core を交換。この Core に関連する既存のシードデータを上書きしますが、他の Core のデータはそのまま残します。 - 完全に消去。シードドライブへの書き込みの前にディレクトリからすべてのシードデータを消去します。
コメント	シードドライブを説明するコメントを入力します。
すべての Agent をシードドライブに追加	シードドライブを使用してソース Core のすべての保護対象マシンをレプリケートするには、このオプションを選択します。このオプションは、デフォルトで、選択されています。
リカバリポイントチェーンを作成 (オーファンの修正)	シードドライブにリカバリポイントチェーン全体をレプリケートするには、このオプションを選択します。このオプションは、デフォルトで、選択されています。 ① メモ: Rapid Recovery 5.4 での通常のシーディングでは、最新のリカバリポイントのみをシードドライブにレプリケートすることで、シードドライブの作成に必要な時間と領域が削減されます。シードドライブにリカバリポイント (RP) チェーンを作成する場合は、指定の 1 つ以上の保護対象マシンの最新のリカバリポイントを保存できる十分な領域がシードドライブに必要です。また、このタスクの完了にさらに時間がかかる場合があります。

g 次の手順のいずれかを実行します。

- 「すべての Agent をシードドライブに追加」チェックボックスをオフにした場合は、「次へ」をクリックします。
- すべての Agent をシードドライブに追加 チェックボックスをオンにした場合は、手順 5 に進みます。

h ウィザードの保護対象マシン ページで、シードドライブを使用してターゲット Core にレプリケートする保護対象マシンを選択します。

5 「終了」をクリックします。

ターゲット Core 上のシードドライブの消費

ターゲット Core 上のシードドライブのデータを消費するには、次の手順を実行します。

① メモ: この手順は、自己管理ターゲット Core へのレプリケーションまたはサードパーティのターゲット Core へのレプリケートの一部としてシードドライブファイルが作成されている場合に限り、必要です。

- 1 USB ドライブなどのポータブルストレージデバイスにシードドライブファイルが保存されている場合は、ターゲット Core にドライブを接続します。
- 2 ターゲット Core で Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。レプリケーション ページが表示されます。
- 3 レプリケーション ページの入力方向のレプリケーション の下で、正しいソース Core のドロップダウンメニューをクリックし、消費 を選択します。消費 ダイアログボックスが表示されます。
- 4 場所のタイプ フィールドのドロップダウンリストから、次のいずれかのオプションを選択します。
 - ローカル
 - ネットワーク
 - クラウド
- 5 手順 4 で選択した場所のタイプに基づき、次の表の説明に従ってシードドライブアーカイブファイルの詳細を入力します。

表 141. アーカイブの詳細

オプション	テキストボックス	説明
ローカル	場所	アーカイブのパスを入力します。
ネットワーク	場所	アーカイブのパスを入力します。
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
クラウド	アカウント	ドロップダウンリストからアカウントを選択します。
		① メモ: クラウドアカウントを選択するには、先に、Core Console にクラウドアカウントが追加されている必要があります。詳細については、「クラウドアカウントの追加」を参照してください。
	コンテナ	ドロップダウンメニューからアカウントに関連付けられているコンテナを選択します。
	フォルダ名	Rapid-Recovery-Archive-[作成日]-[作成時間] など、アーカイブデータが保存されているフォルダ名を入力します。

6 ファイルのチェック をクリックします。

Core でファイルを検索します。

ファイルが見つかると、[手順 4](#)、[手順 5](#)、およびファイルから収集されたデータが既に入力された状態の消費ウィンドウに、次のテキストボックスが表示されます。「日付範囲」では、シードドライブに含まれている最古と最新のリカバリポイントの日付が表示されます。シードドライブの作成時に入力したコメントがある場合は、自動的にインポートされます。

7 消費 ダイアログボックスのエージェントの下で、データの消費対象となるマシンを選択します。

8 消費 をクリックします。

9 データの消費の進捗状況をモニタするには、 イベント ページをクリックしてください。

シードドライブの破棄

ターゲット Core で消費するためにシードドライブを作成した後、消費しないことにした場合は、シードドライブを破棄することができます。

シードドライブを破棄または消費するまで、未処理のシードドライブのリンクは、ソース Core 上の 出力方向のレプリケーション ペインに残ります。

シードドライブから情報を送信するまでは、孤立したリカバリポイント（元の保護対象マシンには存在するが、ターゲット Core には存在しない）を使用してデータを復元することはできません。

△ 注意: シードドライブを破棄した場合は、元のリカバリポイント（シードドライブファイルに定義されている）が、次のレプリケーションジョブ時にネットワーク経由でターゲット **Core** に送信されます。古いリカバリポイントをネットワーク経由で送信すると、特にリカバリポイント数が多い場合に、ネットワークのパフォーマンスが大幅に低下する可能性があります。

未処理のシードドライブを破棄するには、次の手順を実行します。

① **メモ:** **Core Console** 内のシードドライブを破棄しても、所定のストレージ場所にあるシードドライブファイルには影響しません。

1 ソース Core で、Rapid Recovery Core Console を開き、アイコンバーで （レプリケーション）をクリックします。

レプリケーション ページが表示されます。

- 2 レプリケーション ページの 出力方向のレプリケーション ペインで **シードドライブ (#)** をクリックします。
出力方向のレプリケーション ペインに、未処理のシードドライブに関する情報を含むセクションが表示されます。
- 3 必要に応じて、下矢印 ▼ をクリックし、縮小表示メニューを展開します。
未処理のシードドライブについての情報が表示されます。情報には、ターゲット Core や、シードドライブに含まれるリカバリポイントの日付範囲などがあります。
- 4  をクリックして、破棄するシードドライブファイルのドロップダウンメニューをクリックし、**放棄** を選択します。
- 5 確認ウィンドウで、シードドライブを破棄することの確認操作を行います。
シードドライブが削除されます。

ソース Core にその他のシードドライブがない場合は、シードドライブ (#) リンクおよび未処理のシードドライブのセクションが、出力方向のレプリケーション ペインから削除されます。

レプリケーション設定の管理

Rapid Recovery では、Core レベル、保護対象マシンレベル、または全体レベルで、レプリケーションをモニタ、スケジュール、および調整できます。

次のレプリケーション設定を編集できます。

- ・ レプリケーションジョブをスケジュールするには、「[レプリケーションのスケジュール](#)」を参照してください。
- ・ レプリケーション用にペアリング済みの保護対象マシンのシードドライブを作成するには、[Copy 機能を使用したシードドライブの作成](#)を参照してください。
- ・ レプリケーションジョブの進捗状況をモニタするには、「[入力方向および出力方向のレプリケーションの表示](#)」を参照してください。
- ・ レプリケーションジョブを一時停止するか、一時停止したジョブを再開するには、「[レプリケーションの一時停止と再開](#)」を参照してください。
- ・ 保護対象マシンの受信または送信レプリケーションを強制実行するには、「[レプリケーションの強制実行](#)」を参照してください。
- ・ すべてのターゲット Core およびレプリケーション手順の設定を管理するには、「[送信レプリケーションの設定の管理](#)」を参照してください。
- ・ 個別のターゲット Core の設定を管理するには、「[ターゲット Core の設定の変更](#)」を参照してください。
- ・ ターゲット Core にレプリケートする個別の保護対象マシンの優先度設定を管理するには、「[保護対象マシンのレプリケーション優先度の設定](#)」を参照してください。

レプリケーションのスケジュール

レプリケーションのスケジュールを設定してデフォルトの動作を変更しないかぎり、バックアップスナップショット、チェックサムチェック、アタッチ可否検証、および夜間ジョブの完了後、ただちに Core はレプリケーションジョブを開始します。詳細については、「[レプリケーションのスケジュール](#)」を参照してください。

ネットワークの負荷を削減するために、レプリケーションのスケジュールを変更することができます。

レプリケートされた任意のマシンのレプリケーションスケジュールを設定するには、次の手順を実行します。

- 1 ターゲット Core で Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
- 2 出力方向のレプリケーション ペインで、 をクリックしてレプリケーションをスケジュールする Core の横にあるドロップダウンメニューを開き、**スケジュール** を選択します。
[Core 名] に対するレプリケーションスケジュール ダイアログボックスが開きます。

3 次の3つのオプションのいずれかを選択します。

- ・ **常時**。新しいスナップショット、チェックサムチェック、アタッチ可否チェック後に必ず、また、夜間ジョブの完了後にレプリケートを行います。
- ・ **毎日（指定された期間のみレプリケーションを開始）**。指定された時間内のみレプリケーションを開始します。
 - 1 「開始」テキストボックスで、レプリケーションを開始する最も早い時間を入力します。
 - 2 「終了」テキストボックスで、レプリケーションを開始する最も遅い時間を入力します。

① **メモ**：スケジュールされた時間が終了したときにレプリケーションが進行中の場合、そのレプリケーションジョブは割り当てられた時間の後に完了します。

- ・ **カスタム**。指定した期間のみレプリケーションが開始され、平日は1回のみ、週末はその他の期間、というように設定することができます。
 - 1 「平日」の横にある「開始」テキストボックスで、平日にレプリケーションを実行する最も早い時間を入力します。次に、「終了」テキストボックスで、平日にレプリケーションを実行する最も遅い時間を入力します。
 - 2 「週末」の横にある「開始」テキストボックスで、週末にレプリケーションを実行する最も早い時間を入力します。次に、「終了」テキストボックスで、週末にレプリケーションを実行する最も遅い時間を入力します。

4 「保存」をクリックします。

スケジュールは、選択したターゲット Core へのすべてのレプリケーションに適用されます。

Copy 機能を使用したシードドライブの作成

レプリケーションを設定する際にシードドライブを作成しないよう選択した場合は、「保護対象マシン」ドロップダウンメニューの Copy 機能を使用してシードドライブを作成できます。

- 1 ソース Core で Rapid Recovery Core Console を開き、アイコンバーで （レプリケーション）をクリックします。
レプリケーション ページが表示されます。
- 2 レプリケーション ページの 出力方向のレプリケーション ペインで、▼ をクリックし、シードドライブを作成するマシンを保護している Core を展開します。
これによって、指定した Core 内の各保護対象マシンが表示されます。
- 3 シードドライブを作成する各マシンを選択するには、テーブルの最初の行をクリックします。
- 4 出力方向のレプリケーション ペインの下にあるメニューで、コピー をクリックします。
レプリケーションウィザードが表示されます。
- 5 ウィザードの シードドライブの場所 ページで、場所 ドロップダウンリストを使用して、次の宛先タイプの中から選択します。
 - ・ ローカル
 - ・ ネットワーク
 - ・ クラウド
- 6 前の手順で選択した場所のタイプに基づき、次の表の説明に従ってシードドライブアーカイブの詳細を入力します。

表 142. アーカイブの詳細

オプション	テキストボックス	説明
ローカル	出力先	出力の場所を入力します。d:\work\archive などアーカイブを格納する場所のパスの定義のために使用されます。
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
ネットワーク	出力先	出力の場所を入力します。\\servername\sharename などアーカイブを格納する場所のパスの定義のために使用されます。
	ユーザー名	ユーザー名を入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。
	パスワード	ネットワークパスのパスワードを入力します。ネットワーク共有用のログオン資格情報を確立するために使用されます。

オプション	テキストボックス	説明
クラウド	アカウント	ドロップダウンリストからアカウントを選択します。
		① メモ: クラウドアカウントを選択するには、先に、 Core Console にクラウドアカウントが追加されている必要があります。詳細については、「 クラウドアカウントの追加 」を参照してください。
	コンテナ	ドロップダウンメニューからアカウントに関連付けられているコンテナを選択します。
	フォルダ名	アーカイブデータの保存先のフォルダ名を入力します。デフォルト名は、Rapid-Recovery-Archive-[作成日]-[作成時間] です。

- 7 「次へ」をクリックします。
- 8 「シードドライブのオプション」 ページで、次の表の説明に従って情報を入力します。

表 143. シードドライブのオプション

アイテム	説明
最大サイズ	容量の大きいデータアーカイブは、複数のセグメントに分割できます。次のいずれかを実行して、シードドライブを作成するために確保する必要のある最大領域サイズを選択します。 「ターゲット全体」を選択して、「シードドライブの場所」 ページで指定されたパスのすべての使用可能な領域を確保します（たとえば、場所が D:\work\archive である場合は、D: ドライブ上のすべての使用可能な領域が確保されます）。 - 空白のテキストボックスを選択して、数量を入力し、ドロップダウンリストから単位を選択して、確保する最大領域をカスタマイズします。
リサイクルアクション	パスにすでにシードドライブが含まれている場合は、次のいずれかのオプションを選択します。 再使用不可。 この場所から既存のシードデータを上書きまたはクリアしません。指定の場所が空の場合、シードドライブの書き込みは失敗します。 この Core を置換。 この Core に関連する既存のシードデータを上書きしますが、他の Core のデータはそのまま残します。 完全に消去。 シードドライブへの書き込みの前にディレクトリからすべてのシードデータを消去します。
コメント	シードドライブを説明するコメントを入力します。
すべての Agent をシードドライブに追加	シードドライブを使用してソース Core のすべての保護対象マシンをレプリケートするには、このオプションを選択します。このオプションは、デフォルトで、選択されています。
リカバリポイントチェーンの修正)	シードドライブにリカバリポイントチェーン全体をレプリケートするには、このオプションを選択します。このオプションは、デフォルトで、選択されています。 ① メモ: Rapid Recovery 5.4 での通常のシーディングでは、最新リカバリポイントのみをシードドライブにレプリケートすることで、シードドライブの作成に必要な時間と領域を削減します。シードドライブにリカバリポイントチェーンを作成する場合は、指定した保護対象マシンの最新のリカバリポイントを保存できる十分な領域がシードドライブに必要です。また、このタスクの完了にさらに時間がかかる場合があります。

- 9 次の手順のいずれかを実行します。
 - 「**すべての Agent をシードドライブに追加**」 チェックボックスをオフにした場合は、「次へ」をクリックします。
 - すべてのエージェントをシードドライブに追加** チェックボックスをオンにした場合は、[手順 10](#)に進みます。
- 10 ウィザードの **保護対象マシン** ページで、シードドライブを作成する保護対象マシンを選択します。
- 11 「終了」をクリックします。

レプリケーションのモニタリング

レプリケーションのセットアップが完了すると、ソース Core とターゲット Core のレプリケーションタスクのステータスを監視できます。ステータス情報の更新、レプリケーション詳細の表示などを行うことができます。

- 1 ソース Core で、Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
- 2 このページで、次の表の説明に従って、レプリケーションタスクの情報の表示とステータスの監視を行うことができます。

表 144. レプリケーションタスク

項	説明	利用可能なアクション
シードドライブ (#)	レプリケーションを定義する際にシードドライブの使用を指定した後は、シードドライブを破棄または消費するまで、ソース Core の出力方向のレプリケーションペインに シードドライブ (#) リンクが表示されます。表示される番号は、保留中のシードドライブの数を示しています。  メモ: このリンクは、保留中のシードドライブがない場合は表示されません。 このリンクをクリックして、書き込みは終了済みでもターゲット Core による消費はされていないシードドライブのリストを表示します。さらに折りたたみ式のメニューを展開して、未処理のシードドライブについての情報を表示します。情報には、ターゲット Core や、シードドライブに含まれるリカバリポイントの日付範囲などがあります。	ドロップダウンメニューで 破棄 をクリックして、シードプロセスを破棄またはキャンセルします。wn メニュー
送信レプリケーション	ソース Core がレプリケートしているすべてのターゲット Core のリストが表示されます。これには、状態インジケータ、ターゲット Core 名、レプリケート中のマシンの数、およびレプリケーション転送の進捗状況が含まれています。	ソース Core の  ドロップダウンメニューで、次のオプションを選択できます。 ・ 詳細 には、レプリケートされたコアの ID、URL、表示名、状態、カスタム ID、電子メールアドレス、およびコメントのリストが表示されます。 ・ 設定を変更。表示名のリストが表示され、ターゲット Core のホストとポートを編集することができます。 ・ スケジュール。対象のターゲット Core へのレプリケーションのスケジュールをカスタマイズ設定できます。 ・ マシンを追加。ドロップダウンリストからホストを選択して、レプリケートする保護対象マシンを選択し、新しい保護対象マシンの初回転送用のシードドライブを作成できます。必要に応じて、すでにレプリケーションに追加されているマシンのリカバリポイントを含めることもできます。 ・ 削除。ソース Core とターゲット Core 間のレプリケーション関係を削除することができます。この操作を実行すると、対象の Core へのすべてのレプリケーションが停止します。

項	説明	利用可能なアクション
受信レプリケーション	レプリケートされたデータをターゲットに送信するソースマシンをすべてリストします。リモート Core 名、状態、マシン、および進捗状況が表示されます。 レプリケートされたデータをターゲット Core に送信するソース Core をすべてリストします。レプリケーションを定義するときに、リスト内のソース Core の表示名は、レプリケーションウィザード内の値から入力されます。これには、状態インジケータ、リモート Core 名、およびレプリケーション転送の進行状況が含まれます。	ターゲット Core の  ドロップダウンメニューで、次のオプションを選択できます。 詳細。レプリケートされた Core の ID、ホスト名、カスタマ ID、電子メールアドレス、およびコメントをリストします。 消費。シードドライブからの初期データを消費し、ローカルリポジトリに保存します。 削除。ターゲット Core とソース Core 間のレプリケーション関係を削除することができます。この操作を実行すると、削除対象 Core からのすべてのレプリケーションが停止します。
保留中のレプリケーションリクエスト	この情報は、マネージドサービスプロバイダにのみ適用されます。入力方向のレプリケーションペインの リクエスト リンクをカスタマがクリックすると、サマリ表セクションが表示され、リクエストのカスタマ ID、電子メールアドレス、およびホスト名のリストが表示されます。	ドロップダウンメニューで 無視 をクリックしてリクエストを無視または拒否するか、レビュー をクリックして保留中のリクエストを確認します。

レプリケーションの一時停止と再開

ソース（出力方向）Core またはターゲット（入力方向）Core のレプリケーションを一時的に停止することができます。

レプリケーションを一時停止するオプションは、レプリケーションがアクティブな場合にのみ使用できます。レプリケーションを再開するオプションは、レプリケーションを一時停止している場合にのみ使用できます。

レプリケーションを一時停止または再開するには、次の手順を実行します。

- Rapid Recovery Core Console を開き、アイコンバーで （レプリケーション）をクリックします。
レプリケーション ページが表示されます。
- レプリケートされたすべてのマシンのレプリケーションを一時停止するには、次の操作を実行します。
 - サマリ表の上部にあるチェックボックスをクリックして、ソース Core またはターゲット Core を選択します。
 - サマリ表の上部のメニューで **一時停止** をクリックします。
選択した Core のすべての保護対象マシンのレプリケーションが一時停止されます。
- 特定のマシンのみのレプリケーションを一時停止するには、次の操作を実行します。
 - Core の右にある ▼ の矢印をクリックします。
ビューが展開され、選択した Core でレプリケーション中の各保護対象マシンが表示されます。
 - 1列目をクリックして、レプリケーションを一時停止する各マシンを選択します。一時停止しないマシンのチェックボックスがオンになっている場合は、再度クリックしてオフにします。
 - サマリ表の上部のメニューで **一時停止** をクリックします。
選択した保護対象マシンのレプリケーションが一時停止されます。
- レプリケートされたすべてのマシンのレプリケーションを再開するには、次の操作を実行します。
 - サマリ表の上部にあるチェックボックスをクリックして、ソース Core またはターゲット Core を選択します。
 - サマリ表の上部のメニューで **再開** をクリックします。
選択した Core のすべての保護対象マシンのレプリケーションが再開されます。
- 特定のマシンのみのレプリケーションを再開するには、次の操作を実行します。
 - Core の右にある ▼ の矢印をクリックします。
ビューが展開され、選択した Core でレプリケーション中の各保護対象マシンが表示されます。
 - 1列目をクリックして、レプリケーションを再開する各マシンを選択します。再開しないマシンのチェックボックスがオンになっている場合は、再度クリックしてオフにします。

- c サマリ表の上部のメニューで **再開** をクリックします。
選択した保護対象マシンのレプリケーションが再開されます。

レプリケーションの強制実行

バックアップまたはアタッチ可否検証などの特定イベントの後には、レプリケーションジョブの順番を待つのではなく、いつでもソース Core から強制的にレプリケーションを実行することができます。

ソース Core またはターゲット Core からレプリケーションを強制実行するには、次の手順を実行します。

- 1 ソース Core で、Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
- 2 次の手順のいずれかを実行します。
 - ・ ソース Core でレプリケーションを強制実行するには、**出力方向のレプリケーション** ペインで Core を選択し、サマリ表の上部にあるメニューで  **強制** をクリックします。
 - ・ ターゲット Core でレプリケーションを強制実行するには、**入力方向のレプリケーション** ペインで Core を選択し、サマリ表の上部にあるメニューで  **強制** をクリックします。

レプリケーションを強制 ダイアログボックスが表示されます。

- 3 必要に応じて、オフライン化したチェーンまたはリカバリポイントを修復する場合は、**オフラインになったリカバリポイントチェーンをリストアします** を選択します。
- 4 レプリケーションを強制 ダイアログボックスで **はい** をクリックして確認します。
ダイアログボックスが閉じ、レプリケーションが強制実行されます。

送信レプリケーションの設定の管理

これらの設定に行われた変更は、そのソース Core に関連付けられているすべてのターゲット Core へのデータ転送に影響します。

- 1 ソース Core で、Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
- 2 **出力方向のレプリケーション** ペインでサマリ表の一番上にある  (設定) をクリックします。
レプリケーション設定 ダイアログボックスが表示されます。
- 3 **レプリケーション設定** ダイアログボックスで、次の表の説明に従ってレプリケーション設定を編集します。

表 145. レプリケーション設定

オプション	説明
キャッシュの有効期間 (秒)	ソース Core によって実行される各ターゲット Core のステータスリクエスト間の時間を指定します。
ボリュームイメージセッションのタイムアウト (分)	ソース Core がターゲット Core にボリュームイメージを転送するときに費やす時間を指定します。
最大パラレルストリーム	1つの保護対象マシンがマシンのデータをレプリケートするために同時に使用できるネットワーク接続の数を指定します。
最大転送速度 (MB/秒)	レプリケートされたデータの転送速度の上限を指定します。
最大転送データサイズ (GB)	転送できる、レプリケートされたデータのブロックの最大サイズを GB 単位で指定します。

オプション	説明
Restore Defaults	すべてのレプリケーション設定をシステムデフォルト設定に変更するには、このオプションを選択します。
① メモ: このオプションを選択する前に、カスタマイズされた設定をすべてメモしておいてください。このアクションでは、確認を求めるプロンプトは表示されません。	

- 4 変更を完了したら、**保存** をクリックして、レプリケーション設定を保存し、ダイアログボックスを閉じます。

ターゲット Core の設定の変更

個々のターゲット Core のホストおよびポートの設定をソース Core から変更することができます。

- 1 ソース Core で、Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。

出力方向のレプリケーション ペインのサマリ表には、このソース Core からリカバリポイントをレプリケートするよう設定されている各ターゲット Core の行が含まれています。

- 2 変更するターゲット Core の  (設定) ドロップダウンメニューをクリックし、**設定を変更** を選択します。
Settings (設定) ダイアログボックスが表示されます。
- 3 次の表の説明に従ってオプションを編集します。

表 146. ターゲット Core の設定

オプション	説明
ホスト	ターゲット Core のホストを入力します。
ポート	ソース Core との通信に使用するターゲット Core のポートを入力します。
① メモ: デフォルトポートは 8006 です。	

- 4 「**保存**」をクリックします。

保護対象マシンのレプリケーション優先度の設定

レプリケーションの優先度によって、Core に最初に送信されるレプリケーションジョブが決定されます。優先度は、順番に 1 ～ 10 のスケールで設定します。優先度 1 が最優先され、優先度 10 が最後になります。任意のマシンのレプリケーションを最初に確立すると、その優先度は 5 に設定されます。ソース Core からの保護対象マシンレベルで、優先度を表示および変更することができます。

場合によっては、一部のレプリケーションジョブが破棄される可能性があります。たとえば、お使いの環境で変更レートが非常に遅くなった場合や、ネットワークに十分な帯域幅がない場合に、レプリケーションジョブが破棄されることがあります。このような状況は、お使いの環境でレプリケーションを実行する時間帯を制限するようなスケジュールを設定している場合に、起こりやすくなります。レプリケーションスケジュールの設定の詳細については、「[レプリケーションのスケジュール](#)」を参照してください。

重要なマシンに関するレプリケーションが最初に実行されるようにするには、重要なサーバの優先度を小さい数値 (1 ～ 5) に設定します。重要度の低いマシンの優先度は、より大きい値 (6 ～ 10) に設定します。

任意の保護対象マシンのレプリケーション優先度を 4 に設定すると、そのレプリケーションジョブはデフォルトのレプリケーション優先度 5 を持つマシンよりも先に開始されます。同様に、優先度が 3 であるマシンのレプリケーションジョブは、4 よりも前のキューに入られます。優先度の数字が小さいほど、レプリケーションジョブは先に送信されます。優先度 1 が最も重要であるこ

とは簡単にわかります。レプリケーションの優先度が1であるマシンは、レプリケーションの最初の実行キューに入れます。

保護対象マシンのレプリケーション優先度を編集するには、次の手順を実行します。

- 1 ソース Core で Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。
- 2 出力方向のレプリケーション ペインで、ソース Core の右側にある ▼ 矢印をクリックします。
ビューが展開されて、ターゲット Core にレプリケートされる、このソース Core の各保護対象マシンが表示されます。
- 3 優先度を付ける保護対象マシンの  (設定) ドロップダウンメニューをクリックし、**設定** をクリックします。
ダイアログボックスが表示されます。
- 4 **優先度** ドロップダウンリストをクリックし、要件に基づいて **1 (最大)** から **10 (最小)** の間で優先度を選択します。
- 5 **「保存」** をクリックします。
ダイアログボックスが閉じて、選択したマシンのレプリケーション優先度がアップデートされます。

レプリケーションの削除

レプリケーションとは、1つの Rapid Recovery Core (ソース Core) から別の Core (ターゲット) に、保護対象マシンのリカバリポイントを用意して複製することです。

レプリケーションの目的は、元の保護対象マシンのデータの可用性を維持することです。データセキュリティを最適にするために、Dell では別の地理的な場所にターゲット Core を配置することをお勧めします。

レプリケーションスケジュールを設定してデフォルトの動作を変更しない限り、Core では、すべてのバックアップスナップショット、チェックサムチェック、アタッチ可否検証、夜間ジョブが完了した直後にレプリケーションジョブが開始されます。詳細については、「[レプリケーションのスケジュール](#)」を参照してください。

レプリケーションを削除すると、それ以降のソース Core からターゲット Core へのリカバリポイントのコピーが中止されます。レプリケーションを削除しても、元の (ソース) Core に保存されたデータには影響しません。

また、レプリケーションを削除すると、元のマシンから複製されたリカバリポイントをターゲット Coreに残したままにするか、削除するかを選択できます。削除したレプリケート済みマシンのリカバリポイントを保持している場合は、そのマシンのリカバリポイントが、リカバリポイント専用マシンとして Core に表示されます。これらの保持されているリカバリポイントがターゲット Coreに残っている間は、このリカバリポイントからデータを参照するか、ファイルレベルでファイルを復元することができます。

レプリケーションは、次のアプローチのいずれかを使用して削除することができます。

- ・ [ソース Core からの出力方向のレプリケーションの削除](#)
- ・ [ターゲット Core からの入力方向のレプリケーションの削除](#)

ソース Core からの出力方向のレプリケーションの削除

ソース Core 上のレプリケーションから、1台または複数の保護対象マシンを削除するには、次の手順を実行します。

- 1 ソース Core で、Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。

出力方向のレプリケーション ペインのサマリ表には、このソース Core からリカバリポイントをレプリケートするよう設定されている各ターゲット Core の行が含まれています。
- 2 必要に応じて、ターゲット Core の右側にある ▼ の矢印をクリックします。

ビューが展開され、このソース Core の各保護対象マシンが表示されます。これらのマシンが、指定されたターゲット Core にレプリケートされます。

3 出力方向のレプリケーションから削除する保護対象マシンを、次のように選択します。

- ・ このソース Core とあらゆるターゲット Core の間の既存のレプリケーション関係を完全に削除するには、ターゲット Core の  (設定) ドロップダウンメニュー をクリックし、**削除** を選択します。
- ・ 指定したターゲット Core でマシンのサブセットの出力方向のレプリケーションを削除するには、ビューを展開して、レプリケートされているすべてのマシンを表示し、削除する各レプリケート済みマシンのチェックボックスをオンにします。レ

プリケーションを続行するマシンのチェックボックスはすべてオフにします。次に、サマリ表の上にあるメニューで  **削除** をクリックします。

レプリケーション関係を削除するかどうかの確認を求めるメッセージが表示されます。

4 表示されるダイアログボックスで **はい** をクリックして削除を確認します。

ターゲット Core からの入力方向のレプリケーションの削除

ターゲット Core 上のレプリケーションから 1 台または複数の保護対象マシンを削除するには、次の手順を実行します。

① **メモ:** また、ソース Core の レプリケーション ページにある 出力方向のレプリケーション ペインから、保護対象マシンのレプリケーションを削除することもできます。詳細については、次を参照してください。 [ソース Core からの出力方向のレプリケーションの削除](#)

- 1 ターゲット Core で Rapid Recovery Core Console を開き、アイコンバーで  (レプリケーション) をクリックします。
レプリケーション ページが表示されます。入力方向のレプリケーション ペインのサマリ表には、この ターゲット Core がレプリケートする保護対象マシンを持った各ソース Core の列が表示されます。
- 2 削除するレプリケートされたマシンを、次のように選択します。
 - ・ ソース Core からターゲット Core にレプリケートされたマシンを**すべて**削除するには、入力方向のレプリケーション ペインでその Core のチェックボックスをオンにします。
 - ・ 同じソース Core から、より小さなマシンのサブセットを削除するには、次の手順を実行します。
 - a ソース Core の右側にある ▼ 矢印をクリックします。
ビューが展開されて、ターゲット Core にレプリケートされる、選択したソース Core の各マシンが表示されます。
 - b 削除するレプリケートされたマシンのチェックボックスを、それぞれオンにします。
 - c 選択したソース Core の親列から、 (設定) ドロップダウンメニューをクリックし、**削除** を選択します。
レプリケーションを削除 ダイアログボックスが表示されます。
- 3 **レプリケーションを削除** ダイアログボックスで、次のいずれかを実行します。
 - ・ ターゲット Core にレプリケートされたリカバリポイントをそのまま残す場合は、**既存のリカバリポイントを削除** オプションをオフにします。
 - ・ そのマシンから受信したレプリケート済みのリカバリポイントをすべて削除し、さらにそのソース Core もレプリケーションから削除する場合は、**既存のリカバリポイントを削除** をオンにします。
- 4 **はい** をクリックして削除を確認します。

 **警告:** このオプションをオンにすると、この **Core** にレプリケートされたリカバリポイントがすべて削除されます。

ソース Core で保護されている選択したマシンが、このターゲット Core 上のレプリケーションから削除されます。必要に応じて、リカバリポイントを削除するオプションを選択した場合は、この Core のリポジトリから削除されます。

レプリケートされたデータのリカバリ

「毎日実行」のレプリケーション機能はソース Core 上で行われますが、ディザスタリカバリに必要な機能はターゲット Core のみが実行できます。

ディザスタリカバリの場合、ターゲット Core は、レプリケートされたリカバリポイントを使用して保護対象マシンをリカバリできます。ターゲット Core から次のリカバリオプションを実行できます。

- ・ リカバリポイントをマウントする。詳細については、「[リカバリポイントのマウント](#)」を参照してください。
- ・ リカバリポイントまでロールバックする。詳細については、「[リカバリポイントからのボリュームの復元](#)」または「[コマンドラインを使用した Linux マシンのボリュームのリストア](#)」を参照してください。
- ・ **仮想マシン (VM) エクスポートを実行する**。詳細については、「[Rapid Recovery を使用した仮想マシンへのエクスポートについて](#)」を参照してください。
- ・ **Bare Metal Restore (BMR) を実行する**。詳細については、「[Windows マシンのベアメタルリストアの実行](#)」を参照してください。

データのリカバリ

リカバリの管理

Rapid Recovery Core では、リカバリポイントから物理または仮想マシンに対して、データの回復またはマシンの復元を瞬時に行うことができます。リカバリポイントには、ブロックレベルでキャプチャされたエージェントボリュームスナップショットが含まれます。これらのスナップショットはアプリケーションアウェアであり、すべての未処理トランザクションと進行中トランザクションのログが完了し、キャッシュがディスクにフラッシュされてから、スナップショットが作成されます。アプリケーションアウェアのスナップショットと Verified Recovery を使用することにより、次を含む複数のタイプのリカバリを Core で実行できます。

- ・ ファイルとフォルダのリカバリ
- ・ Live Recovery を使用したデータボリュームのリカバリ
- ・ Live Recovery を使用した Microsoft Exchange Server および Microsoft SQL Server のデータボリュームのリカバリ
- ・ Universal Recovery を使用したベアメタル復元
- ・ Universal Recovery を使用した異種ハードウェアへのベアメタル復元
- ・ 仮想マシンへのアドホックおよび継続エクスポート

スナップショットとリカバリポイント

このセクションでは、Rapid Recovery により生成されたスナップショットとリカバリポイントを使用し、管理する方法を説明します。リカバリポイントのマウント、表示、強制実行のほか、移行および削除についての情報が含まれています。

スナップショットとリカバリポイントの管理

リカバリポイントは、個々のディスクボリュームを取得したスナップショットの集まりで、リポジトリに保存されます。スナップショットでは、所定の時点でのディスクボリュームの状態が取得および保存されるため、データを生成するアプリケーションはそのまま使用できます。Rapid Recovery では、スナップショットの強制、スナップショットの一時停止、およびリポジトリ内の現在のリカバリポイントのリスト表示のほか、必要に応じてリカバリポイントの削除を実行することができます。リカバリポイントは、保護対象マシンをリストアしたり、ローカルファイルシステムにマウントしたりするために使用します。

Rapid Recovery でのスナップショットのキャプチャはアプリケーションアウェアで、ブロックレベルで行われます。つまり、すべての未処理トランザクションと実行中のトランザクションのログが完了し、キャッシュがフラッシュされたあと、スナップショットが作成されます。

Rapid Recovery はマウントされているボリュームが持つ低レベルボリュームフィルタドライバを使用し、次に行われるスナップショットのブロックレベルの変更をすべて追跡します。Microsoft Volume Shadow Services (VSS) は、クラッシュ整合性のあるアプリケーションスナップショットを容易に作成できるようにします。

保護対象マシンのリカバリポイントページの表示

保護対象マシンのリカバリポイントの完全リストを表示するには、次の手順を実行します。

- ① **メモ:** DAG または CCR サーバークラスタからデータを保護している場合、関連するリカバリポイントはクラスタレベルでは表示されません。これらは、ノードレベルまたはマシンレベルでのみ表示されます。

- 1 Rapid Recovery Core Console で、リカバリポイントを表示する保護対象マシンに移動します。
- 2 ページの上部にあるメニューから、**リカバリポイント** をクリックします。
リカバリポイント ページが表示され、リカバリポイントのサマリ ペインとリカバリポイント ペインが示されます。

次の表の説明に従って、マシンに関するリカバリポイントのサマリ情報を表示できます。

表 147. リカバリポイントのサマリ情報

情報	説明
合計リカバリポイント	このマシンのリポジトリに保存されているリカバリポイントの合計数をリストします。
保護データの合計	これらのリカバリポイントのリポジトリで使用されているストレージ領域の容量を示します。
DVM リポジトリ	これらのリカバリポイントが保存されるリポジトリの名前をリストします。
DVM リポジトリステータス	リカバリポイントが消費するスペースの量をグラフ表示します。使用されているリポジトリの割合、スペースの容量、およびリポジトリの合計容量を表示します。グラフをクリックすると、残りの容量が表示されます。

次の表の説明に従って、マシンに関するリカバリポイントの情報を表示できます。

表 148. リカバリポイントの情報

情報	説明
アイコン	リカバリポイント  、または展開した場合はリカバリポイント内のボリューム  をグラフィック表示したもの。リカバリポイントには右矢印  が表示され、詳細を展開できます。
暗号化済み	リカバリポイントが暗号化されているかどうかを示します。
ステータス	リカバリポイントの現在のステータスを示します。
コンテンツ	リカバリポイントに含まれているボリューム一覧を示します。  (情報) をクリックして容量使用状況およびファイルシステムを確認します。
タイプ	ベースイメージまたは増分 (差分) スナップショットのいずれかとしてリカバリポイントを定義します。
作成日	リカバリポイントが作成された日付を表示します。
サイズ	リポジトリ内でリカバリポイントが消費する容量を表示します。
	設定 ドロップダウンメニューでは、選択したリカバリポイントに対して特定の機能を実行できます。

- 3 必要に応じてリカバリポイントを展開し、保護対象ボリュームを表示します。

関連するリンク

[マシンのリカバリポイントの表示](#)

リカバリポイントステータスインジケータについて

保護された SQL Server または Exchange サーバ上でリカバリポイントがキャプチャされると、アプリケーションのリカバリポイントグリッド内で対応するカラーステータスインジケータが表示されます。特定マシンの **リカバリポイント** を表示すると、リカバリ

ポイント ペインにこのグリッドが表示されます。次の表に示すとおり、表示色は、保護対象マシンに対するチェックの設定、およびこれらのチェックの成功または失敗に応じて決定されます。

① **メモ:** リカバリポイントの表示の詳細については、「[保護対象マシンのリカバリポイントページの表示](#)」を参照してください。

Exchange データベースのリカバリステータスポイントカラー

次の表に、Exchange データベースについて表示されるステータスインジケータを記載しています。

表 149. Exchange データベースのステータスインジケータ

ステータスカラー	説明
白色	リカバリポイント、ボリューム、またはボリュームグループ内で Exchange データベースが検知されなかったことを示します。
黄色	Exchange データベースのマウント可否チェックがまだ実行されていないことを示します。
赤色	少なくとも1つのデータベースで、マウント可否チェックまたはチェックサムチェックが失敗したことを示します。
緑色	リカバリポイントに1つまたは複数のデータベースが含まれていること、マウント可否チェックが有効になっていること、およびマウント可否チェックが成功したこと（またはチェックサムチェックが成功したこと）を示します。

SQL データベースのリカバリステータスポイントカラー

次の表に、SQL データベースについて表示されるステータスインジケータを記載しています。

表 150. SQL データベースのステータスインジケータ

ステータスカラー	説明
白色	リカバリポイント、ボリューム、またはボリュームグループ内で SQL データベースが検知されなかったことを示します。
黄色	SQL データベースがオフラインであり、アタッチ可否検証が実行不能であったため、実行されなかったことを示します。
赤色	アタッチ可否検証が失敗したこと、SQL データベースがオフラインであったことを示します。
緑色	アタッチ可否チェックに合格したことを示します。

① **メモ:** 関連付けられている **Exchange** データベースまたは **SQL** データベースを持たないリカバリポイントは、白いステータスインジケータで表示されます。リカバリポイントに **Exchange** データベースと **SQL** データベースの両方が存在する場合は、そのリカバリポイントで最も重大なステータスのインジケータが表示されます。

リカバリポイントのマウント

Rapid Recovery では、ローカルファイルシステムを介して保存データにアクセスするため、Windows マシンにリカバリポイントをマウントすることができます。

① **メモ:** `local_mount` ユーティリティを使用して **Linux** リカバリポイントをマウントする方法については、「[Linux マシンでのリカバリポイントボリュームのマウント](#)」を参照してください。

① **メモ:** データ重複排除が有効になっているマシンからリストアされたデータのリカバリポイントをマウントする場合は、**Core** サーバー上でも重複排除が有効になっている必要があります。

- 1 Rapid Recovery Core Console で、ローカルファイルシステムにマウントするマシンに移動します。
選択した保護対象マシンの **サマリ** ページが表示されます。
- 2 **リカバリポイント** メニューをクリックします。
選択したマシンの **リカバリポイント** ページが表示されます。
- 3 必要に応じて、**リカバリポイント** ペインにあるリカバリポイントのリストで、右矢印 ▶ をクリックしてリカバリポイントの詳細を展開し、そのリカバリポイントに含まれているボリュームを表示します。
- 4 マウントするリカバリポイントの列で  をクリックし、ドロップダウンメニューから **マウント** を選択します。
マウントウィザード が表示され、**ボリューム** ページが表示されます。
- 5 **ボリューム** ページで、マウントするリカバリポイントのボリュームをそれぞれ選択し、**次へ** をクリックします。
マウントウィザードの **マウントオプション** ページが表示されます。
- 6 **マウントオプション** ページで、次の表の説明に従ってリカバリポイントのマウントに関する設定を編集します。

表 151. マウントオプションの設定

オプション	説明
ローカルフォルダ	マウントされたリカバリポイントへのアクセスに使用するパスを指定します。 たとえば、C:\ProgramData\AppRecovery\MountPoints\ MountPoint1 を選択します。
マウントタイプ	マウントしたリカバリポイントのデータにアクセスする方法を指定します。 ・ 読み取り専用 ・ 以前の書き込みとともに読み取り専用 ・ 書き込み可能
このマウントに Windows 共有を作成	必要に応じて、マウントされたリカバリポイントを共有できるかどうかを指定するチェックボックスをオンにして、共有名や許可されたグループなどそのリカバリポイントへのアクセス権を設定します。

- 7 **完了** をクリックして、リカバリポイントをマウントします。

① **メモ:** マウント済みリカバリポイントから別の **Windows** マシンにディレクトリまたはファイルをコピーする場合、**Windows Explorer** を使用して、デフォルトの権限または元のファイルアクセス権限を保持したままコピーできます。詳細については、**Windows Explorer** を使用したディレクトリまたはファイルのリストア～**Windows Explorer** を使用したディレクトリまたはファイルのリストアおよび権限の保持を参照してください。

- 8 必要に応じて、タスクの処理中に Core Console の **実行中のタスク** ドロップダウンメニューから進捗状況を確認したり、**イベント** ページで詳細情報を表示したりすることができます。Rapid Recovery イベントの監視の詳細については、「**タスク、アラート、およびジャーナルを使用したイベントの表示**」を参照してください。

リカバリポイントのマウント解除

Core 上にマウントされているリカバリポイントをマウント解除するには、次の手順を実行します。

① **メモ:** リモートにマウントされているリカバリポイントをマウント解除する場合、このアクションを **切断**といいます。

- 1 Rapid Recovery Core Console のアイコンバーで  (詳細) をクリックし、次に  **マウント** を選択します。
マウント ページが表示されます。「ローカルマウント」用のペイン (Core からマウントされるリカバリポイント) と「リモートマウント」用のもう 1 つのペイン (Local Mount Utility を使用してマウントされるリカバリポイント) があります。各ペインでは、マウントされた各リカバリポイントが、リストに表示されます。
- 2 **ローカルマウント** ペインで、ローカルマウントをマウント解除するには、次の手順を実行します。

- a マウント解除するローカルマウントポイントを選択します。
 - ・ すべてのリカバリポイントをマウント解除するには、ローカルマウント 表のタイトルバーでチェックボックスをオンにして、すべてのマウントポイントを選択します。
 - ・ 1つまたは複数のリカバリポイントをマウント解除するには、各列の最初の行で、接続解除するマウントポイントのチェックボックスをオンにします。
- b  **マウント解除** をクリックします。
確認のダイアログボックスが表示されます。
- c クリックして、選択したリカバリポイントのマウント解除を確認します。
ローカルのリカバリポイントがマウント解除されます。

① **メモ:** Toast アラートが有効になっている場合、使用すべきマウントポイントがマウント解除されると警告するアラートが表示されることがあります。

- 3 リモートでマウントされているリカバリポイントを接続解除するには、**リモートマウント** ペインで次の手順を実行します。
 - a 接続解除するリモートマウントポイントを選択します。
 - ・ すべてのリカバリポイントを接続解除するには、リモートマウント 表のタイトルバーでチェックボックスをオンにして、すべてのマウントポイントを選択します。
 - ・ 1つ、または複数のリカバリポイントを接続解除するには、各列の最初の行で、接続解除するマウントポイントのチェックボックスをオンにします。
 - b  **接続解除** をクリックします。
確認のダイアログボックスが表示されます。
 - c クリックして、選択したリカバリポイントの接続解除を確認します。
ローカルのリカバリポイントが接続解除されます。

① **メモ:** Toast アラートが有効になっている場合、使用すべきマウントポイントが接続解除されると警告するアラートが表示されることがあります。

- 4 必要に応じて、これまでマウントされていたリカバリポイントが「ローカルマウント」または「リモートマウント」リストに表示されていないことを確認します。

Linux リカバリポイントの操作

保護対象 Linux マシンからリカバリポイントのマウントとマウント解除を行う方法としてサポートおよび推奨されているのは、`local_mount` ユーティリティを使用する方法です。

以下の手順では、`local_mount` を使用して Linux リカバリポイントをマウントおよびマウント解除する方法を具体的に説明します。

① **メモ:** マウントおよびマウント解除以外の Linux リカバリポイントの管理方法については、「[スナップショットとリカバリポイントの管理](#)」を参照してください。これらの管理操作はすべて、**Core Console** から実行できます。

Linux マシンでのリカバリポイントボリュームのマウント

Rapid Recovery の `local_mount` ユーティリティを使用して、Linux マシン上で、リカバリポイントからローカルボリュームとしてボリュームをリモートでマウントできます。

① **メモ:** この手順を実行する場合、`aavdisk` ファイルがある `/tmp` フォルダにリカバリポイントをマウントしないでください。

- 1 リカバリポイントをマウントする新しいディレクトリを作成します (`mkdir` コマンドなどを使用できます)。
- 2 (`ls` コマンドなどを使用して) ディレクトリが存在していることを確認します。
- 3 ルートまたはスーパーユーザーとして Rapid Recovery `local_mount` ユーティリティを実行します。

```
sudo local_mount
```

- 4 Rapid Recovery のマウントプロンプトで、次のコマンドを入力して保護対象マシンのリストを表示します。

```
1m
```

- 5 プロンプトが表示されたら、Rapid Recovery Core サーバの IP アドレスまたはホスト名を入力します。

- 6 Core Server のログオン資格情報（ユーザー名とパスワード）を入力します。

Rapid Recovery サーバによって保護されるマシンのリストが表示されます。各マシンは、行アイテム番号、ホスト/IP アドレス、およびマシンの ID 番号によって識別されます。

例：7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba

- 7 次のコマンドを入力して、指定したマシンで使用できるリカバリポイントをリストします。

```
1r <line_number_of_machine>
```

❶ **メモ:** このコマンドには、行アイテム番号の代わりにマシンの ID 番号を入力することもできます。

マシンのベースリカバリポイントと増分リカバリポイントのリストが表示されます。リストには、行アイテム番号、日付/タイムスタンプ、ボリュームの場所、リカバリポイントのサイズ、ボリュームの ID 番号が表示されます（ID 番号の末尾には、リカバリポイントを特定するシーケンス番号が付きます）。

例：7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:
2

- 8 指定のリカバリポイントを選択して、指定のマウントポイント/パスでマウントするには、次のコマンドを入力します。

```
m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
```

このコマンドのフラグによって、リカバリポイントのマウント方法が決まります。次のいずれかのオプションを使用できます。

- ・ [r] - 読み取り専用でマウント（デフォルト）。リカバリポイントをマウントできますが、リカバリポイントに対する変更はできません。
- ・ [w] - 書き込み可能でマウント。リカバリポイントをマウントして、リカバリポイントに対する変更もできます。
- ・ [v] - 以前の書き込みでマウント。リカバリポイントをマウントする際に、前回の書き込み可能マウントで行われたが、現在は存在しないすべての変更内容を含めることができます。
- ・ [n] - nbd を <path> にマウントしない。nbd（ネットワークブロックデバイス）は、ローカルマウントの実行時に、Core と保護対象マシン間のソケット接続を作成します。このフラグを使用すると、nbd をマウントせずにリカバリポイントをマウントできます。これは、リカバリポイントのファイルシステムを手動でチェックする必要があるときに便利です。

❶ **メモ:** リカバリポイントの ID 番号の代わりに行番号をコマンドで指定して、リカバリポイントを特定することもできます。その場合は、(1m 出力の) マシンの行番号を使用し、その後リカバリポイントの行番号とボリューム文字を指定し、さらにその後パスを指定します（例：m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>）。たとえば、1m 出力で 3 つの保護対象マシンがリストされた場合に、番号 2 に対して 1r コマンドを入力し、リカバリポイント 23 のボリューム b を /tmp/mount_dir にマウントする場合、コマンドは m 2 23 b /tmp/mount_dir のようになります。

❶ **メモ:** 互換性のあるオペレーティングシステムから BTRFS ボリュームをマウントする場合（『*Dell Data Protection / Rapid Recovery* インストールおよびアップグレードガイド』の「*Rapid Recovery* リリース 6.1 のオペレーティングシステムのインストールと互換性マトリクス」のトピックを参照）は、次のパラメータを含める必要があります。

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

- 9 マウントが成功したことを確認するには、次のコマンドを入力します。これにより、アタッチされたリモートボリュームがリストされます。

```
1
```

Linux マシン上でのリカバリポイントのアンマウント

Linux マシンでリカバリポイントをマウント解除するには、次の手順を実行します。

- 1 ルートまたはスーパーユーザーとして Rapid Recovery local_mount ユーティリティを実行します。

```
sudo local_mount
```

- 2 Rapid Recovery のマウントプロンプトで、次のコマンドを入力して保護対象マシンのリストを表示します。

```
1m
```


- 3 プロンプトが表示されたら、Rapid Recovery Core サーバの IP アドレスまたはホスト名を入力します。
- 4 Core サーバーのログオン資格情報（ユーザー名とパスワード）を入力します。
Rapid Recovery サーバによって保護されるマシンのリストが表示されます。
- 5 次のコマンドを入力して、指定したマシンで使用できるリカバリポイントをリストします。

```
lr <line_number_of_machine>
```

① | **メモ:** このコマンドには、行アイテム番号の代わりにマシンの ID 番号を入力することもできます。

マシンのベースリカバリポイントと増分リカバリポイントのリストが表示されます。リストには、行アイテム番号、日付/タイムスタンプ、ボリュームの場所、リカバリポイントのサイズ、リカバリポイントを示すシーケンス番号が最後に付けられたボリュームの ID 番号が表示されます。

例: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

- 6 1 または list コマンドを実行してマウントされたネットワークブロックデバイス（NBD デバイス）のリストを表示します。リカバリポイントをマウントすると、1 または list コマンドを実行したときに NBD デバイスへのパスが表示されます。
- 7 次のコマンドを入力して、リカバリポイントをマウント解除します。
umount <path_of_nbd-device>
- 8 1 または list コマンドを実行してリカバリポイントが正常にマウント解除されていることを確認します。

スナップショット作成の強制実行

スナップショット作成の強制実行によって、現在保護対象のマシンのデータ転送を強制できます。スナップショット作成を強制実行すると、転送が直ちに実行されるか、またはその他のジョブが実行されている場合は、キューに追加されます。

2 種類のスナップショットから選択できます。

増分スナップショットを選択し、以前のリカバリポイントが存在しない場合は、ベースイメージがキャプチャされます。強制的にスナップショットを作成しても、スケジュールスナップショットのタイミングは変更されません。

① | **メモ:** Rapid Recovery では、ベース転送と増分転送の両方で Window 8、Windows 8.1、Windows Server 2012 および Windows Server 2012 R2 がサポートされています。

- ・ ベースイメージは、マシンの選択したボリュームにあるすべてのデータのスナップショットです。
 - ・ 増分スナップショットは、最後のスナップショット以降に変更されたすべてのデータをキャプチャします。
- 1 Rapid Recovery Core Console で、スナップショット作成を強制的に実行するリカバリポイントがあるマシンまたはクラスタに移動します。
 - 2 サマリ ページで、サマリ ペインの **スナップショットを強制的に作成** をクリックします。
スナップショットを強制的に作成 ダイアログボックスが表示されます。
 - 3 スナップショットを強制的に作成 ダイアログボックスで、1つまたは複数のボリュームまたは保護対象グループのチェックボックスをクリックします。
 - 4 **スナップショットを強制的に作成** または ベースイメージを強制的に作成 をそれぞれクリックします。
 - 5 ベースイメージを選択した場合は、クリックしてベースイメージを作成することを確認します。
ベースイメージでは、バックアップするボリュームのデータ量に基づいて、大量の時間かかることがあります。

選択したスナップショットがキューに格納され、その他のジョブが完了した直後に開始されます。

リカバリポイントの削除

特定のマシンのリカバリポイントをリポジトリから容易に削除できます。Rapid Recovery でリカバリポイントを削除する場合は、次のいずれかのオプションを指定できます。

- ・ **すべてのリカバリポイントの削除。** 選択した保護対象マシンのすべてのリカバリポイントをリポジトリから削除します。
- ・ **一定範囲のリカバリポイントを削除。** 現在より前からベースイメージまでの指定範囲のすべてのリカバリポイント、つまりマシン上のすべてのデータおよび、現在から次のベースイメージまでのすべてのリカバリポイントを削除します。

① **メモ:** 削除したリカバリポイントは復元することはできません。リカバリポイントに格納されているデータが必要な場合、データのアーカイブを最初に考えます。

- 1 Rapid Recovery Core Console の **保護対象マシン** メニューで、リカバリポイントを表示して削除するマシンの名前または IP アドレスをクリックします。
選択した保護対象マシンの サマリ ビューが表示されます。
- 2 マシン名または IP アドレスの横で **リカバリポイント** メニューをクリックします。
選択したマシンの **リカバリポイント** ページが表示されます。
- 3 **リカバリポイント** ペインまでスクロールダウンします。
ペインタイトルの下に、更新、範囲を削除、すべて削除 などのオプションが表示されます。
- 4 リカバリポイント ペインタイトルの下で、現在保存されているすべてのリカバリポイントを削除する場合、**すべて削除** をクリックし、確認のダイアログボックスでボタンをクリックして削除を確認します。
- 5 特定のデータ範囲内で一連のリカバリポイントを削除するには、次の手順を実行します。
 - a リカバリポイント ペインタイトルの下で、**範囲を削除** をクリックします。
範囲内のリカバリポイントを削除 ダイアログボックスが表示されます。
 - b **範囲内のリカバリポイントを削除** ダイアログボックスの **開始日時** フィールドで、リカバリポイントの削除を開始する日時を選択します。
 - c **終了日時** フィールドで、削除する最新のリカバリポイントの日時を選択します。
 - d **削除** をクリックします。
 - e 確認のダイアログボックスでクリックして削除を確認します。

孤立したリカバリポイントチェーンの削除

孤立したリカバリポイントとは、ベースイメージに関連付けられていない増分スナップショットのことです。後続のスナップショットは、継続してこのリカバリポイント上に構築されますが、ベースイメージがないとリカバリポイントが不完全になるため、リカバリを完了させるために必要なデータが含まれていない可能性が高くなります。これらのリカバリポイントは、孤立したリカバリポイントチェーンの一部として見なされます。この状況が発生した場合の最適な解決法は、チェーンを削除して、新しいベースイメージを作成することです。

ベースイメージの強制の詳細については、[スナップショット作成の強制実行](#)を参照してください。

- 1 Rapid Recovery Core Console で、孤立したリカバリポイントチェーンを削除する保護対象マシンに移動します。
- 2 ページの上部にあるメニューから、**リカバリポイント** をクリックします。
- 3 リカバリポイント ペインで、孤立したリカバリポイントを展開します。
このリカバリポイントの場合、タイプ 列に「増分、孤立」というラベルが表示されます。
- 4 アクション の横の **削除** をクリックします。
リカバリポイントを削除 ウィンドウが表示されます。
- 5 リカバリポイントを削除 ウィンドウで、**はい** をクリックします。

△ **注意:** リカバリポイントを削除すると、リカバリポイントのチェーン全体（次のベースイメージまでのリカバリポイントの前後に発生する増分リカバリポイントを含む）が削除されます。この操作は取り消せません。
孤立したリカバリポイントチェーンが削除されます。

異なるリポジトリへの手動によるリカバリポイントの移行

保護対象マシンのリカバリポイントを削除せずにリポジトリから移動する場合は、次の手順に従って手動で異なるリポジトリに移行します。このプロセスでは、ソースリポジトリからリカバリポイントをアーカイブした後、ターゲットリポジトリにアーカイブをインポートします。

たとえば、既存のリポジトリが一杯である場合、またはニーズが変わって別の Core とリポジトリを使用してマシンを保護する場合に、この手順を実行することができます。

△ 注意: リポジトリが以前に **AppAssure 5.3** または **5.4** からアップグレードされ、レプリケーションを使用していた場合、**Dell** では移行を開始する前にターゲット Core 内の各リポジトリにリポジトリの確認ジョブを実行することを推奨します。このジョブを実行すると、不規則なデータが新しい出力先リポジトリにコピーされることを防止できます。リポジトリの確認ジョブが Core に適用可能な場合、それは UI でのみ使用でき、実行に相当な時間がかかる可能性があります。このジョブについては、「**DVM リポジトリの整合性チェックについて**」を参照してください。このジョブの実行については、「**DVM リポジトリでのリポジトリの確認ジョブの実行**」を参照してください。

- 1 Rapid Recovery Core Console で、保護対象マシンまたはリカバリポイントを移行するマシンの保護を一時停止します。詳細については、「**保護の一時停止と再開**」を参照してください。
- 2 保護対象マシンまたはリカバリポイントを移行するマシンの現在の操作をすべてキャンセルするか、すべてが完了するまで待機します。
- 3 一時停止したマシンのリカバリポイントをアーカイブします。詳細については、「**アーカイブの作成**」を参照してください。
- 4 アーカイブを行い、アーカイブを検証したら、移行する保護対象マシンの既存のリカバリポイントを削除します。詳細については、「**リカバリポイントの削除**」を参照してください。

① | メモ: 既存のリカバリポイントを削除せずに、保護対象マシンのリポジトリを変更することはできません。

- 5 移行済みのリカバリポイントに対して新しいリポジトリを作成するか、新しい宛先リポジトリが存在することを確認します。詳細については、「**DVM リポジトリの作成**」を参照してください。
 - ・ 既存のリポジトリを使用する場合は、**ステップ 6**に進みます。
- 6 次の手順に従って、一時停止した各マシンのリポジトリを変更します。
 - a Core Console で、ナビゲーションツリーの保護対象マシンをクリックします。
 - b 保護対象マシンの **サマリ** ページで、**設定** をクリックします。
 - c **設定** ページの **一般** ペインで、**リポジトリ** ドロップダウンリストをクリックし、**手順 4** で作成したリポジトリの名前を選択します。
 - ・ 既存のリポジトリを使用する必要がある場合は、既存のリポジトリの名前を選択します。

① | メモ: リカバリポイントを既存のリポジトリに移行する場合は、既存のリポジトリに移行対象リカバリポイントを格納するための十分な空き領域があることを確認してください。

- d **OK** をクリックします。
- 7 一時停止したマシンの保護を再開します。詳細については、「**保護の一時停止と再開**」を参照してください。
 - 8 移動した各保護対象マシンの新規ベースイメージを取得します。詳細については、「**スナップショット作成の強制実行**」を参照して、ベースイメージを強制的に作成 オプションを使用してください。
 - 9 移行する必要があるマシンのアーカイブ済みデータをインポートします。詳細については、「**アーカイブのインポート**」を参照してください。

データのリストア

本項では、バックアップデータをリストアする方法について説明します。

Rapid Recovery を使用したデータのリストについて

Rapid Recovery Core は、物理または仮想マシンに対し、リカバリポイントから即時にデータのリストアまたはマシンのリカバリを行います。リカバリポイントには、ブロックレベルでキャプチャされた Agent ボリュームのスナップショットが含まれています。

これらのスナップショットはアプリケーションウェアです。つまり、スナップショットを作成する前に、すべての処理中のトランザクションとローリングトランザクションログのロールが完了され、キャッシュがディスクにフラッシュされることを意味します。アプリケーションウェアスナップショットを Verified Recovery と組み合わせて使用すると、Core で次のようないくつかのタイプのリカバリを実行できます。

- ・ ファイルとフォルダのリカバリ
- ・ Live Recovery でのデータボリュームのリカバリ
- ・ Live Recovery を使用した、Microsoft Exchange Server および Microsoft SQL Server のデータボリュームのリカバリ
- ・ Universal Recovery を使用した、Bare Metal Restore
- ・ Universal Recovery を使用した、異種ハードウェアへの Bare Metal Restore
- ・ 仮想マシンへのアドホックおよび継続エクスポート

① **メモ:** データをリストアするときまたは仮想エクスポートを実行するときには、使用するリカバリポイントが完全なリカバリポイントチェーンの一部である必要があります。リカバリポイントチェーンの詳細については、「[リカバリポイントチェーンとオーファン](#)」を参照してください。

Live Recovery について

Live Recovery は、Rapid Recovery Core にデータを復元する機能です。保護対象マシンで非システムの Windows ボリュームにデータ障害が発生した場合、Rapid Recovery Core 上のリカバリポイントからデータを復元することができます。Restore Wizard で Live Recovery を選択すると、ユーザーはほぼダウンタイムなしで業務をすぐに継続できます。復元中の Live Recovery では、Rapid Recovery によるデータの復元がバックグラウンドで継続されている間も、データにすぐにアクセスできます。この機能により、テラバイト単位のデータを復元する場合でも、リカバリ時間をほとんどなくすることができます。

Rapid Recovery Core は、リカバリプロセス中にターゲットサーバへの完全なユーザアクセスを提供する、独自のブロックベースのバックアップとリカバリテクノロジーを使用します。要求されたブロックはシームレスなリカバリとしてオンデマンドで復元されます。

Live Recovery は、次の例外を除き、Rapid Recovery Core によって保護された物理マシンおよび仮想マシンに適用されます。

- ・ Live Recovery は、非システムの Windows ボリュームにアクセスできます。Live Recovery を使用して、C:\ ドライブとシステムに予約されたパーティションを復元することはできません。
- ・ Live Recovery は、Rapid Recovery Agent を使用して Windows ベースのボリュームにアクセスできます。エージェントレスボリュームまたは Linux ボリュームでは Live Recovery の利点は得られません。

Live Recovery では物理サーバまたは仮想サーバを直接バックアップファイルから直ちに復元できます。非システムのボリュームが復元されると、Rapid Recovery にオペレーティングシステムへのボリュームメタデータが直ちに表示され、オンデマンドでデータが利用可能になります。たとえば、Microsoft Exchange のデータベースボリュームが破損している場合、Live Recovery を使用して、ボリューム、データベース、および Exchange サービスをすぐに復元できます。

この機能は、ダウンタイムを最小限にして大容量のデータをリカバリする場合に最速の方法を提供します。ユーザーはすぐに業務を継続できます。

Live Recovery を開始すると、復元されたボリュームとその内容が即座に使用可能になります。Rapid RecoveryCore は、ボリューム、データ、アプリケーションおよびサービスがすでに本稼動に戻っている場合でも、バックグラウンドでデータの復元を続行します。特定のデータが要求されると、バックグラウンドプロセスはすぐにそのデータの復元を優先的に行います。この高度な機能によって、最も厳しいサービスレベル契約でも満たすことができます。

Live Recovery を開始すると、ターゲットボリュームのメタデータ（ディレクトリ構造、セキュリティ記述子、NTFS ファイル属性、空き容量マップなど）が迅速に保護対象マシンに復元されます。それ以降、ボリュームとその内容はシステムで使用できるようになります。Rapid Recovery Agent はデータブロックの復元を Rapid Recovery Core サーバから開始し、ターゲットボリュームにブロックを書き込みます。

要求しているプログラムまたはシステムが復元されたばかりのブロックを認識していない場合、復元されていないデータの要求はすぐに応答されます。

リカバリポイントからのデータのリストア

Rapid Recovery は、Windows および Linux マシン上のデータを保護します。保護対象のエージェントマシンのバックアップが Rapid Recovery Core にリカバリポイントとして保存されます。これらのリカバリポイントから、3つの方法のいずれかを使用してデータを復元することができます。

Rapid Recovery Core Console からは、システムボリューム以外のリカバリポイントからボリューム全体を復元して、復元先マシンのボリュームを置き換えることができます。これは、Windows マシンでのみ行うことができます。詳細については、「[リカバリポイントからのボリュームの復元](#)」を参照してください。

リカバリポイントからオペレーティングシステムがあるボリュームを直接リストアすることはできません。これは、リストア先となるマシンで、リストアプロセスに含まれるオペレーティングシステムとドライブが使用されているためです。リカバリポイントからシステムボリューム（Agent マシンの C ドライブなど）をリストアする場合、Bare Metal Restore (BMR) を実行する必要があります。そのために、リカバリポイントからブータブルイメージ（オペレーティングシステム、設定ファイルおよびデータを含む）を作成し、そのブータブルイメージからターゲットマシンを起動してリストアを完了させる操作を実行します。リストアするマシンで使用されているオペレーティングシステム（Windows または Linux）によって、ブートイメージは異なります。リカバリポイント Windows マシン上のシステムボリュームにリストアする場合は、「[Windows マシンのベアメタルリストアの実行](#)」を参照してください。リカバリポイントから Linux マシン上のシステムボリュームをリストアする場合は、「[Windows マシンのベアメタルリストアの実行](#)」を参照してください。

ボリューム全体をリストアする場合とは異なり、Windows マシンからリカバリポイントをマウントし、個々のフォルダおよびファイルを参照して、特定のファイルセットのみをリカバリできます。詳細については、「[Windows Explorer を使用したディレクトリまたはファイルのリストア](#)」を参照してください。元のファイル権限を保持したまま、これを実行する必要がある場合（ファイルサーバ上のユーザーのフォルダをリストアする場合など）は、「[Windows Explorer を使用したディレクトリまたはファイルのリストアおよび権限の保持](#)」を参照してください。

本項のトピックでは、物理マシン上のデータのリストアについて説明します。Windows マシンから仮想マシンへの保護対象データのエクスポートの詳細については、「[VM エクスポート](#)」を参照してください。

① **メモ:** Windows マシン上のデータをリカバリするときに、リストアするボリュームで Windows データ重複排除が有効になっている場合、Core サーバー上でも重複排除が有効になっていることを確認する必要があります。Rapid Recovery では、通常の転送（ベース転送と増分転送の両方）、データのリストア、Bare metal restore、および仮想マシンのエクスポートで Windows 8、Windows 8.1、Windows 10、Windows Server 2012、および Windows Server 2012 R2 がサポートされています。バックアップおよびリカバリでサポートされるボリュームタイプとサポートされないボリュームタイプの詳細については、「[ダイナミックボリュームとベーシックボリュームのサポート](#)」を参照してください。

リカバリポイントからのボリュームの復元

Rapid Recovery コアに保存されるリカバリポイントから、保護対象マシンのボリュームをリストアできます。

① **メモ:** 以前のリリースでは、このプロセスはロールバックの実行と呼ばれていました。

① **メモ:** Rapid Recovery は、EISA パーティションで構成されたマシンの保護とリカバリをサポートします。サポートは、Windows 回復環境 (Windows RE) を使用する Windows 8、Windows 8.1、Windows Server 2012、および Windows Server 2012 R2 のマシンも拡張されます。

Rapid Recovery ボタンバーの Rapid Recovery アイコンをクリックすることで、Rapid Recovery（迅速な回復）コアコンソールの任意の場所からリストアを開始できます。この方法でリストアを開始する場合は、リストアするコアで保護されたマシンを指定し、リストアするボリュームまでドリルダウンする必要があります。

または、特定のマシンの Recovery Points（リカバリポイント）ページに移動し、特定のリカバリポイントのドロップダウンメニューをクリックし、**Restore（リストア）**を選択します。この方法でリストアを開始する場合は、[ステップ 5](#) から開始することでこの手順に従います。

リカバリポイントからシステムボリュームにリストアするか、起動 CD を使用してリカバリポイントからリストアする場合、ベアメタルリストア（BMR）を実行する必要があります。BMR の詳細については、[Windows マシンの Bare Metal Restore について](#) を参照してください。Windows または Linux オペレーティングシステムの必要条件については、[Windows マシンに対して Bare Metal Restore を実行するための前提条件](#) および [Linux マシンに対して Bare Metal Restore を実行するための前提条件](#) をそれぞれ参照してください。各オペレーティングシステムのロードマップに記載されているように、コアコンソールから BMR 機能にアクセスできます。Restore Machines（マシンのリストア）ウィザードから、BMR を実行することもできます。この手順は、ウィザードの適切な時点で手順 [マシンのリストアウィザードを使用した Bare Metal Restore の実行](#) ユーザーをガイドします。

リカバリポイントからのボリュームのリストア

保護対象マシンには Agent ソフトウェアがインストールされていて、リストア操作を実行できるリカバリポイントがある必要があります。

リカバリポイントからボリュームをリストアするには、次の手順を完了します。

- 1 リストアアイコンから保護対象マシン上のボリュームをリストアするには、Core Console に移動し、Rapid Recovery ボタンバーの **リストア** をクリックします。
マシンのリストア ウィザードが表示されます。
- 2 保護対象マシン ページで、データをリストアする保護対象マシンを選択し、**次へ** をクリックします。
リカバリポイント ページが表示されます。
- 3 リカバリポイントのリストから、Agent マシンにリストアするスナップショットを検索します。
 - ・ 必要に応じて、ページの下部にあるボタンを使用して、その他のリカバリポイントのページを表示します。
 - ・ 必要に応じて、ウィザードのリカバリポイント ページに表示されるリカバリポイント数を制限する場合、リカバリポイントのボリューム（定義されている場合）または作成日でフィルタできます。
- 4 それを選択するリカバリポイントをクリックし、**次へ** をクリックします。
宛先 ページが表示されます。
- 5 宛先 ページで、次のようにデータをリストアするマシンを選択します。
 - ・ 選択したリカバリポイントから同じマシンにデータをリストアする場合、リストアするボリュームにシステムボリュームが含まれていなければ、**保護対象マシンにリカバリ（非システムボリュームのみ）** を選択し、宛先マシンが選択されていることを確認して、**次へ** をクリックします。
ボリュームマッピング ページが表示されます。[手順 9](#) に進みます。
 - ・ 選択したリカバリポイントから別の保護対象マシンにデータをリストアする場合（Machine2 のコンテンツを Machine1 のデータで置き換える場合など）、**保護対象マシンにリカバリ（非システムボリュームのみ）** を選択し、宛先マシンを選択して、**次へ** をクリックします。
ボリュームマッピング ページが表示されます。[手順 9](#) に進みます。
 - ・ 選択したリカバリポイントから同じマシンにリストアするか、またはブート CD を使用して異なるマシンにリストアする場合、このプロセスでは bare metal restore（BMR）が考慮されます。BMR については、「[Windows マシンの Bare Metal Restore について](#)」を参照してください。

① メモ: BMR を実行する場合、リストアする Agent マシンのオペレーティングシステムによって特定の要件があります。これらの前提条件を理解するには、「[Windows マシンに対して Bare Metal Restore を実行するための前提条件](#)」および「[Linux マシンに対して Bare Metal Restore を実行するための前提条件](#)」をそれぞれ参照してください。
リストアするボリュームにシステムボリュームが含まれている場合は、**ブート CD** を使用して任意のターゲットマシンに**リカバリ**を選択します。このオプションではブート CD を作成するように要求されます。

- ・ そのまま マシンのリストア ウィザードを使用して選択したリカバリポイントの情報でブート CD を作成する場合、**次へ** をクリックして [Windows マシンのベアメタルリストアの実行](#) に進みます。
- ・ ブート CD を作成済みで、ブート CD を使用してターゲットマシンが起動されている場合、トピック「[#GUID-07C2DA5A-B8E2-4D01-82D5-E7A1F14E155E/ID-2490-0000487F](#)」の [手順 8](#) に進みます。

- ・ リカバリポイントからシステムボリューム（例：Machine1 という名前の Agent マシンの C ドライブ）にリストアする場合も、プロセスで BMR が考慮されます。**ブート CD を使用して任意のターゲットマシンにリカバリ** を選択します。このオプションではブート CD を作成するように要求されます。
 - ・ そのまま マシンのリストア ウィザードを使用して選択したリカバリポイントの情報でブート CD を作成する場合、次へをクリックして [Windows マシンのベアメタルリストアの実行](#)に進みます。
 - ・ ブート CD を作成済みの場合は、[手順 6](#)に進みます。
- 6 ブート CD を使用してリストアするマシンを起動します。Windows マシンでの BMR の詳細については、「[ブート CD のロードおよびターゲットマシンの起動](#)」を参照してください。また、Linux マシンでの BMR の詳細については、「[Live DVD のロードおよびターゲットマシンの起動](#)」を参照してください。
- 7 Core サーバで、マシンのリストア ウィザードの宛先 ページで、**ターゲットマシンで実行するブート CD を既に持っている** を選択し、次の表の説明に従って、接続するマシンの情報を入力します。

表 152. マシン情報

テキストボックス	説明
IP アドレス	リストアするマシンの IP アドレス。これは、URC に表示される IP アドレスと同じです。
認証キー	選択されたサーバーに接続するための特定のパスワード。これは、URC に表示される認証キーと同じです。

- 8 **次へ** をクリックします。
- 入力した接続情報が URC と一致し、Core およびターゲットサーバがネットワーク上で相互に正しく識別できる場合は、選択したリカバリポイントのボリュームがロードされます。ディスクマッピング ページが表示されます。

マシンのリストア ウィザードから BMR を実行するには、トピック「[#unique_342/ID-2490-00004B0D](#)」の[手順 9](#)に進みます。

- ① **メモ: Rapid Recovery では FAT32 と ReFS のパーティションがサポートされます。ReFS ではドライバの制限があるため、フルリストアと BMR のみがサポートされます。** リストアは、ユーザーモード、VM エクスポートなどで実装されます。**ReFS ファイルシステムを含む少なくとも 1 つの Agent ボリュームを Core で保護している場合は、ReFS のネイティブサポートを提供している、Windows 8/2012 上にインストールする必要があります。**これらにインストールされない場合、機能が制限され、ボリュームイメージのマウントなどが関係する操作が動作しなくなります。**Rapid Recovery Core Console** にこれらのオカレンスのエラーメッセージが表示されます。

このリリースでは、ストレージスペースのディスク構成の **Bare metal restore**（Windows 8.1 の機能）はサポートされません。詳細については、『[Rapid Recovery インストールおよびアップグレードガイド](#)』を参照してください。

- 9 ボリュームマッピング ページで、リストアするリカバリポイントのボリュームごとに、適切な宛先ボリュームを選択します。ボリュームをリストアしない場合、宛先ボリューム 列で、**リストア不可** を選択します。
- 10 **詳細設定オプションを表示** を選択し、次の手順を実行します。
- ・ Windows マシンへのリストアで、Live Recovery を使用する場合は、**Live Recovery** を選択します。
- Rapid Recovery の Live Recovery 即時リカバリテクノロジーを使用すると、Windows マシンの保存されたリカバリポイント（Microsoft Windows ストレージスペースを含む）から物理マシンまたは仮想マシンにデータを即時にリカバリまたはリストアできます。Live Recovery は、エージェントなしの保護を使用する Linux マシンまたは VM には使用できません。
- ・ リストアを開始する前に、選択したボリュームを強制的にマウント解除するには、**マウント解除を強制** を選択します。
- △ 注意:** データをリストアする前にマウント解除を強制しないと、ボリュームが使用中であるとのエラーでリストアに失敗する可能性があります。
- 11 **次へ** をクリックします。
- 12 データベースをマウント解除 ページで、リストアするボリュームに SQL データベースや Microsoft Exchange データベースが含まれている場合、マウント解除するよう要求されます。
- リストアの完了後にこれらのデータベースを再マウントする場合、**リカバリポイントの復元後にすべてのデータベースを自動的に再マウントする** を選択します。
- 13 **次へ** をクリックします。
- 警告 ページが表示され、リストアするボリューム上のすべてのプログラムを閉じるように要求される場合があります。その場合は、**次へ** をクリックします。
- 14 サマリ ページで、**重要!** この操作で、選択したボリュームが選択したリカバリポイントのデータで上書きされることを理解しています。 を選択し、ボリュームのリストアによる結果を理解していることを確認します。

⚠ 警告: このオプションでは、選択済みリカバリポイントの日時の後に選択済みボリューム上に保存されたデータはリストア時に失われるという結果が強調されています。

15 **終了** をクリックします。

Windows Explorer を使用したディレクトリまたはファイルのリストア

Windows Explorer を使用して、マウント済みリカバリポイントから任意の Windows マシンにディレクトリおよびファイルをコピーして貼り付けることができます。これは、リカバリポイントの一部だけをユーザーに配布する場合に便利です。

ディレクトリおよびファイルをコピーする場合、コピー操作を実行するユーザーのアクセス権限が使用され、貼り付けたディレクトリおよびファイルに適用されます。元のファイル権限を保持したまま、ユーザーのディレクトリおよびファイルを復元する場合（ファイルサーバ上のユーザーのフォルダを復元する場合など）は、「[Windows Explorer を使用したディレクトリまたはファイルのリストアおよび権限の保持](#)」を参照してください。

- 1 リストアするデータを含むリカバリポイントをマウントします。詳細については、[リカバリポイントのマウント](#)を参照してください。
- 2 Windows Explorer で、マウント済みリカバリポイントに移動し、リストアするディレクトリおよびファイルを選択します。右クリックして、「**コピー**」を選択します。
- 3 Windows Explorer で、データのリストア先となるマシンの場所に移動します。右クリックして、「**貼り付け**」を選択します。

Windows Explorer を使用したディレクトリまたはファイルのリストアおよび権限の保持

Windows Explorer を使用して、ファイルアクセス権限を保持したまま、マウント済みリカバリポイントから任意の Windows マシンにディレクトリおよびファイルをコピーして貼り付けることができます。

たとえば、特定のユーザーのみがアクセスできるファイルサーバー上のフォルダをリストアする必要がある場合、「コピー」および「権限付きの貼り付け」コマンドを使用すれば、リストアされるファイルは、アクセスを制限する権限を保持できます。こうすることで、リストアされたディレクトリおよびファイルに手動で権限を適用することを回避できます。

① メモ: 権限付きの貼り付け コマンドは、**Rapid Recovery Core** および **Agent** ソフトウェアとともにインストールされます。**Local Mount Utility** では使用できません。

- 1 リストアするデータを含むリカバリポイントをマウントします。詳細については、[リカバリポイントのマウント](#)を参照してください。
- 2 Windows Explorer で、マウント済みリカバリポイントに移動し、リストアするディレクトリおよびファイルを選択します。右クリックして、「**コピー**」を選択します。
- 3 Windows Explorer で、データのリストア先となるマシンの場所に移動します。右クリックして、「**権限付きの貼り付け**」を選択します。

① メモ: この手順の右クリックメニューで「権限付きの貼り付け」コマンドが無効になっている場合、コピーするファイルが **Windows Explorer** で認識されません。**手順 2** を繰り返して、右クリックメニューの 権限付きの貼り付け コマンドを有効にします。

クラスタとクラスタノードのリストアの実行

リストアとは、マシン上のボリュームをリカバリポイントから復元するプロセスです。サーバークラスタの場合、リストアはノードまたはマシンのレベルで実行します。本項では、クラスタボリュームに対してリストアを実行する際のガイドラインについて説明します。

CCR および DAG (Exchange) クラスタのリストアの実行

CCR および DAG (Exchange) クラスタのリストアを実行するには、以下の手順を行います。

- 1 1台を除くすべてのノードの電源をオフにします。
- 2 リカバリポイントからのボリュームの復元 および コマンドラインを使用した Linux マシンのボリュームのリストアに記載されているとおりに、標準の Rapid Recovery 手順を使用してマシンに対してリストアを実行します。
- 3 リストアが終了したら、クラスタボリュームのすべてのデータベースをマウントします。
- 4 ほかのすべてのノードの電源をオンにします。
- 5 Exchange の場合、Exchange Management Console に移動し、各データベースに対して、Update Database Copy (データベースコピーの更新) 操作を実行します。

SCC (Exchange、SQL) クラスタのリストアの実行

SCC (Exchange、SQL) クラスタのリストアを実行するには、以下の手順を行います。

- 1 1台を除くすべてのノードの電源をオフにします。
- 2 リカバリポイントからのボリュームの復元 および コマンドラインを使用した Linux マシンのボリュームのリストアに記載されているとおりに、標準の Rapid Recovery 手順を使用してマシンに対してリストアを実行します。
- 3 リストアが終了したら、クラスタボリュームのすべてのデータベースをマウントします。
- 4 他のすべてのノードの電源を1つずつオンにします。

① **メモ:** クォーラムディスクをロールバックする必要はありません。クォーラムディスクは、自動で、またはクラスタサービス機能を使用して再生できます。

添付されたアーカイブからのリストア

アーカイブからデータを復元する場合には、2つの方法があります。アーカイブをベアメタルリストア (BMR) のソースとして使用する方法、またはアーカイブのアタッチし、アーカイブからリカバリポイントをマウントしてから、アーカイブされたデータをリストアする方法です。

アーカイブをアタッチすると、コアコンソールの Archive (アーカイブ) ページの Attached Archives (アタッチされたアーカイブ) の下に表示されます。また、アーカイブのコンテンツは左のナビゲーション領域からアクセスできるようになります。コンテンツはアーカイブの名前の下に表示されます。アーカイブされたマシンは、リカバリポイントのみのマシンとして表示されますので、現時点で保護されているマシンと同様の方法でリカバリポイントにアクセスできます。リカバリポイントをマウントし、リカバリーするアイテムを配置し、Windows エクスプローラを使用して、宛先にコピーアンドペーストします。

リポジトリへのアーカイブのインポートではなく、アタッチされたアーカイブから接続されたリストアを行う場合、利点があります。

- ・ アタッチされたアーカイブからのリストアを行うと、リポジトリにアーカイブ全体をインポートする場合より時間を節約できます。
- ・ また、アーカイブをインポートするときに、アーカイブされたリカバリポイントがリポジトリに追加されます。これらのアーカイブされたリカバリポイントはリポジトリで最も古いアイテムである可能性が高いため、次の夜間ジョブの実行中は保持ポリシーに基づいてロールアップすることができます。(ただし、このアクションでは、アーカイブからは削除しません。次の日に再度インポートすることができます。)
- ・ 最後に、アーカイブをデタッチした後でも、アーカイブとのアタッチの関連付けを Core は記憶しています。これにより、アーカイブのアタッチを後でもう一度行う際、簡単かつすばやく行うことができます。アタッチされているアーカイブを削除することにより、関連付けを削除できます。

アタッチされたアーカイブからデータをリストアするには、関連リンクを使用して次の手順を完了します。

① **メモ:** アタッチされたアーカイブからのリストア手順は、ロールアップされたアーカイブリカバリポイントをセットアップ済みであることを前提としています。

- 1 アーカイブをアタッチします。
- 2 リカバリを行うデータを含むリカバリポイントをマウントします。
- 3 次のいずれかの方法を使用してデータをリストアします。
 - ・ リカバリポイントからファイルやフォルダなどのデータをリストアします。
 - ・ 全体のリカバリポイントをリストアします。
 - ・ 仮想マシンにリカバリポイントをエクスポートします。

関連するリンク

[アーカイブのアタッチ](#)

[リカバリポイントのマウント](#)

[Windows Explorer を使用したディレクトリまたはファイルのリストア](#)

[Rapid Recovery を使用した仮想マシンへのエクスポートについて](#)

[Windows のバックアップ](#)

[アーカイブについて](#)

[アーカイブのインポート](#)

[アーカイブからの BMR の実行](#)

Windows マシンの Bare Metal Restore について

本項では、同種または異種のベアメタルハードウェアから保護対象 Windows マシンをリストアする方法について説明します。

Windows マシンのベアメタル復元について

サーバーが予期したとおりに動作している場合は、設定されたタスクが実行されます。サーバーに障害が発生した場合に限り、状況が変わります。サーバーを動作不能にする致命的なイベントが発生した場合は、サーバーを以前の状態に復元するための迅速な対策を講じることが必要です。

Rapid Recovery には、Windows マシンまたは Linux マシンに Bare Metal Restore (BMR) を実行する機能が備えられています。BMR は、特定のシステムの完全なソフトウェア構成をリストアするプロセスです。リストア操作では、サーバーからデータをリカバリするだけでなく、ハードドライブの再フォーマットと、オペレーティングシステムおよびすべてのソフトウェアアプリケーションの再インストールが行われるため、「Bare Metal」という用語が使用されます。BMR を実行するには、保護対象マシンからリカバリポイントを指定し、指定の物理マシンまたは仮想マシンにロールバック（リストアを実行）します。システムボリュームにリストアを実行する場合は、BMR を検討してください。リストアを実行しようとしており、ブート CD が必要な場合も、BMR を検討してください。Bare metal restore は、ハードウェアのアップグレードやサーバーの交換を行った場合にも実行することがあります。いずれの場合も、リカバリポイントからアップグレードされたハードウェアまたは交換されたハードウェアにリストアを実行します。

Rapid Recovery では、FAT32 EFI パーティションから起動される Windows 8、8.1、Windows Server 2012、2012 R2 オペレーティングシステムと、Resilient File System (ReFS) ボリュームをサポートしており、保護またはリカバリに使用できます。

① **メモ:** このリリースでは、ストレージスペースのディスク構成の **Bare metal restore** (Windows 8.1 の機能) はサポートされません。現時点では、**ReFS** のドライバ制限によりフルリストアと **BMR** しかサポートされないため、リストアはユーザーモード、**VM** エクスポートなどで実現されます。**ReFS** ファイルシステムを含む **Agent** ボリュームを 1 つ以上 **Core** で保護している場合は、**ReFS** のネイティブサポートを提供している、**Windows 8**、**Windows 8.1**、**Windows Server 2012**、または **Windows Server 2012 R2** マシンに **Core** をインストールする必要があります。これらにインストールされない場合、機能が制限され、ボリュームイメージのマウントなどが関係する操作が動作しなくなります。この場合には、該当するエラーメッセージが **Rapid Recovery Core Console** に表示されます。サポートされている **Linux** オペレーティングシステムのみ保護/リカバリを使用できます。サポートされる **Linux** は、**Ubuntu®**、**Red Hat Enterprise Linux®**、**CentOS®**、**SUSE Linux Enterprise Server (SLES®)** となります。詳細については、『**Dell Data Protection | Rapid Recovery のインストールおよびアップグレードガイド**』を参照してください。

BMR の実行は、物理マシンまたは仮想マシンで可能です。Rapid Recovery には、ハードウェアが同種または異種に関係なく BMR を実行できるという利点もあります。Rapid Recovery の BMR は、オペレーティングシステムが特定のプラットフォームから分離され、高い移植性を得られます。

同種のハードウェアに対する BMR の実行例としては、既存のシステムのハードドライブの交換、同一マシンで障害が発生したサーバーのスワップアウトなどがあります。

異種のハードウェアに対する BMR の実行例としては、製造元や構成が異なるためにサーバーで障害が発生したシステムのリストアなどがあります。この処理には、ブート CD イメージの作成、イメージのディスクへの書き込み、ブートイメージからのターゲットサーバーの起動、リカバリ Console インスタンスへの接続、ボリュームのマッピング、リカバリの開始、プロセスの監視が含まれます。Bare Metal Restore が完了したら、リストアされたサーバーでオペレーティングシステムおよびソフトウェアアプリケーションをロードするタスクを続行してから、構成に必要な固有の設定を行うことができます。

Bare Metal Restore は、ディザスタリカバリの場合だけでなく、サーバーをアップグレードまたは置換するときのデータの移行にも使用できます。

Windows マシンのベアメタルリストアの実行

Windows マシンのベアメタルリストアを実行するには、次のタスクを実行します。

- Windows のブートイメージの作成。この起動 CD ISO イメージが宛先ドライブを起動するのに使用されます。ここからユニバーサルリカバリコンソールにアクセスし、Core のバックアップと通信できます。[Windows マシンのブート CD の作成について](#)を参照してください。
 - 物理メディアがターゲットマシンのスタートアップに必要な場合、起動 CD ISO イメージをメディアに転送する必要があります。[ブート CD の ISO イメージのメディアへの転送](#)を参照してください。
 - すべての場合、ターゲットサーバにブートイメージをロードして、ブートイメージからサーバーを起動する必要があります。[ブート CD のロードおよびターゲットマシンの起動](#)を参照してください。
- ① メモ:** このプロセスは、**Create Boot CD (起動 CD の作成)** ダイアログボックスからの**起動 CD イメージ**を管理する方法について説明します。**Restore Machine (マシンのリストア)** ウィザードからこれらの手順を実行することもできます。ウィザードの**起動 CD**のページから開始します。ウィザードの**Destination (宛先)** ページからの**起動 CD**を使用して任意のターゲットマシンに**Recover (回復)**を指定する場合に、これにアクセスします。ベアメタルリストアの一部としての**Restore Machine (マシンのリストア)** ウィザードからの**Windows のブートイメージの管理**に関する段階を踏んだ手順については、[マシンのリストアウィザードを使用した Bare Metal Restore について](#)を参照してください。
- Windows 用のベアメタルリストアを開始。ターゲットマシンが起動 CD から起動された後に、BMR を起動できます。[BMR への Universal Recovery Console の使用](#)を参照してください。次のタスクを行います。
 - Core のリカバリポイントからのリストアを開始します。[リカバリポイントの選択と BMR の開始](#)を参照してください。
 - ボリュームをマッピングします。「[Bare Metal Restore のボリュームをマップについて](#)」を参照してください。
 - 異なるハードウェアにリストアし、必要なストレージおよびネットワークドライブが起動 CD 上にない場合、ポータブルメディアデバイスからドライブをロードする必要があります。詳細については、[Universal Recovery Console を使用したドライブのロード](#)を参照してください。
 - Restore Machine (マシンのリストア) ウィザードからの BMR の実行。オプションとして、Windows のブートイメージを管理し、BMR を起動するプロセスは、すべてのサブタスクを含めて、Restore Machine (マシンのリストア) ウィザードから実行できます。ウィザードの起動の詳細については、[リカバリポイントからのボリュームの復元](#)の手順 1～5 を参照してから [マシンのリストアウィザードを使用した Bare Metal Restore について](#)を参照してください。
 - ベアメタルリストアの確認。ベアメタルリストアの開始後、進捗状況を確認し、監視することができます。[Bare Metal Restore の確認](#)を参照してください。
 - リストアの進捗状況を監視できます。[リカバリの進捗状況の表示](#)を参照してください。
 - 完了したら、リストアされたサーバーを開始することができます。[リストアされたターゲットサーバの起動](#)を参照してください。
 - BMR プロセスのトラブルシューティングを行います。[Universal Recovery Console への接続に関するトラブルシューティング](#)および [起動の問題の修復](#)を参照してください。

Windows マシンに対して Bare Metal Restore を実行するための前提条件

Windows マシンに対して Bare Metal Restore を実行するプロセスを開始する前に、次の条件および基準を満たしていることを確認する必要があります。

- ・ 64 ビット CPU。Win PE 5.1 オペレーティングシステムが含まれている Rapid Recovery ブート CD。Rapid Recovery BMR は、x86 ベースの CPU とは互換性がありません。BMR は 64 ビット CPU でのみ実行できます。

① | メモ: この要件は、6.0 の新しい要件です。

- ・ リストアするマシンのバックアップ。リストアする保護対象サーバのリカバリポイントが含まれた、機能している Rapid Recovery Core が必要です。
- ・ リストアするハードウェア（新規または既存、同種または異種）。ターゲットマシンは、Agent のインストール要件を満たしている必要があります。詳細については、『Dell Data Protection | Rapid Recovery インストールおよびアップグレードガイド』を参照してください。
- ・ イメージメディアとソフトウェア。空の CD または DVD とディスク書き込みソフトウェア、または ISO イメージの作成ソフトウェアが必要です。UltraVNC などの仮想ネットワークコンピューティングソフトウェアを使用してマシンをリモート管理する場合は、VNC ビューアが必要です。
- ・ 互換性のあるストレージドライバとネットワークアダプタドライバ。異種のハードウェアにリストアする場合は、RAID、AHCI、チップセットドライバなど、ターゲットマシンに互換性のあるストレージドライバとネットワークアダプタドライバが適宜必要です。
- ・ ストレージスペースとパーティション（適宜）ターゲットマシンでソースボリュームを含める宛先パーティションを作成するのに十分な容量がハードドライブにあることを確認します。宛先パーティションには、少なくとも元のソースパーティションと同じ容量が必要です。
- ・ 互換性のあるパーティション。FAT32 EFI パーティションから起動される Windows 8、Windows 8.1、Windows 10、Windows Server 2012、および Windows Server 2012 R2 オペレーティングシステムと、Resilient File System (ReFS) ボリュームは、保護またはリカバリに使用できます。UEFI パーティションは、単純な FAT32 ボリュームとして処理されます。増分転送は完全にサポートされ、保護されます。Rapid Recovery では、GPT ディスクの自動パーティション化を含め、BMR の UEFI システムのサポートが提供されます。

マシンのリストアウィザードを使用した Bare Metal Restore について

ウィザード使用した Windows のブートイメージの管理には、次のアクションが含まれています。

- ・ ブート CD の作成を開始する。
- ・ コアマシンにイメージのパスを定義する。
- ・ 復元場所のハードウェアに合ったリカバリ環境を選択する。
- ・ 必要に応じて、ネットワークまたは UltraVNC を使用するために復元されたエージェントの接続パラメーターを定義する。
- ・ 必要に応じて、復元場所のハードウェアでドライバを導入する。
- ・ 必要に応じて、ブートイメージを物理メディアに転送する。
- ・ CD からデータの復元先のマシンを起動する
- ・ Universal Recovery Console に接続する。
- ・ ボリュームのマッピング
- ・ Core 上の選択したリカバリポイントからの Bare Metal Restore を開始します。

① | メモ: ここでは、「マシンのリストア」ウィザードを使用して BMR の実行プロセスの一部として、「マシンのリストア」ウィザードからブート CD イメージを管理する方法を説明します。また、「ブート CD を作成」ダイアログボックスからもブートイメージを管理できます。「マシンのリストア」ウィザードを使用しないでブート CD イメージを管理する方法の詳細については、[Windows マシンのブート CD の作成について](#)を参照してください。

マシンのリストアウィザードを使用した Bare Metal Restore の実行

リストアウィザードを使用して、ブート CD を作成し、bare metal restore (BMR) を実行することができます。

BMR を実行する前に、必要に応じて、[Windows マシンに対して Bare Metal Restore を実行するための前提条件](#)または [Linux マシンに対して Bare Metal Restore を実行するための前提条件](#)を参照してください。Core Console から Windows マシンの BMR を開始する場合は、「[Windows マシンのベアメタルリストアの実行](#)」を参照してください。

保護対象マシンには Agent ソフトウェアがインストールされていて、リストア操作を実行できるリカバリポイントがある必要があります。

- 1 保護対象マシン上のボリュームをリストアするには、Core Console に移動し、Rapid Recovery ボタンバーの **リストア** をクリックします。
「マシンのリストア」ウィザードが表示されます。
- 2 マシンページで、リストアする保護対象マシンを選択し、**次へ** をクリックします。
「リカバリポイント」ページが表示されます。
- 3 マシンのリストア元を使用するリカバリポイントを選択します。
 - ・ 表示されるリカバリポイント数を制限する場合、リカバリポイントのボリューム（定義されている場合）または作成日でフィルタできます。特定のリカバリポイントの検索を実行することもできます。
- 4 「**次へ**」をクリックします。
- 5 宛先 ページで、**ブート CD** を使用して**任意のターゲットマシンにリカバリ**を選択します。
 - ・ リストアするマシンにブート CD をまだロードしていない場合は、**次へ** をクリックし、[手順 6](#)に進みます。
 - ・ ブート CD が BMR ターゲットマシンにすでにロードされている場合は、**ターゲットマシンで実行するブート CD を既に持っている**を選択し、**次へ** をクリックして、[手順 16](#)に進みます。
- 6 ブート CD ページで、出力パス テキストボックスに、ブート CD の ISO イメージの保存先となるパスを入力します。
 - ① **メモ:** イメージを保存する共有ドライブのディスク容量が不十分な場合は、必要に応じてパス内にディスクを作成できます (F:\filename.iso など)。
 - ① **メモ:** ファイルの拡張子は **.iso** である必要があります。パスを指定する場合には、英数字、ハイフン、バックスラッシュ（パス区切り文字としてのみ）、ピリオド（ホスト名とドメインを区切るためのみ）のみを使用します。**a** から **z** までの文字では、大文字と小文字は区別されません。スペースは使用できません。他の記号または句読点文字は無効です。
- 7 オプションで、ターゲットマシンのネットワークパラメーターを設定する場合や、UltraVNC 機能を追加する場合は、**詳細設定オプションを表示**を選択して、次のいずれかを行います。
 - ・ BMR ターゲットとのネットワーク接続を確立するには、**次の IP アドレスを使用**を選択し、次の表の説明に従って情報を入力します。

表 153. ネットワーク接続オプション

オプション	説明
IP アドレス	リストアするマシンの IP アドレス。
サブネットマスク	リストアするマシンのサブネットマスク。
デフォルトゲートウェイ	リストアするマシンのデフォルトゲートウェイを指定します。
DNS サーバー	リストアするマシンのドメインネームサーバーを指定します。
・ UltraVNC アカウントがあり、それを使用して BMR を実行する場合は、 UltraVNC を追加 を選択し、次の表の説明に従って情報を入力します。	

表 154. UltraVNC 接続資格情報

オプション	説明
パスワード	UltraVNC アカウントのパスワード。
ポート	BMR ターゲットへの接続に使用するポート。デフォルトポートは 5900 です。

- 8 「**次へ**」をクリックします。
- 9
 - ・ リストアするマシンのネットワーク接続を確立するには、次の表の説明に従って、「**次の IP アドレスを使用**」を選択します。

- UltraVNC 情報を定義するには、次の表の説明に従って、**UltraVNC を追加** を選択します。
このオプションは、リカバリ Console へのリモートアクセスが必要な場合に使用します。ブート CD の使用中は、Microsoft ターミナルサービスにはログオンできません。

表 155. UltraVNC 接続

オプション	説明
パスワード	この UltraVNC 接続のパスワードを指定します。
ポート	この UltraVNC 接続のポートを指定します。 デフォルトポートは 5900 です。

- 「ブート CD」ページの選択内容に問題がなければ、「次へ」をクリックします。
- 異なるハードウェアへのリストアを計画している場合は、ドライバの導入 ページで、次の手順を実行して、ターゲットシステムに適したストレージコントローラと他のドライバを導入することもできます。
 - サーバ製造元のウェブサイトからサーバ用のドライバをダウンロードし、解凍します。
 - 適切な圧縮ユーティリティ（WinZip など）を使用して、各ドライバを .zip ファイルに圧縮します。
 - マシンのリストアウィザードのドライバの導入 ページで、**ドライバのアーカイブを追加** をクリックします。
 - ファイリングシステムで圧縮済みのドライバファイルを検索し、ファイルを選択して、**開く** をクリックします。
 - 必要に応じて、すべての必要なドライバを導入するまで**手順 c**および**手順 d**を繰り返します。

ドライバの導入についての詳細については、「**ブート CD へのドライバの導入について**」を参照してください。

① メモ: すべてのバージョンの **Windows** が自動ドライバ導入と互換性があるわけではありません。使用しているオペレーティングシステムと互換性がない場合は、**C:\Program Files\AppRecovery\Core\BootCdKit\Drivers** にドライバを手動で保存します。

Rapid Recovery によってブート CD ISO イメージが作成されます。

- 「次へ」をクリックします。
- BMR ターゲットマシンを起動し、次のいずれかのオプションを実行します。
 - ブート CD の ISO イメージからターゲットマシンを起動できる場合、今すぐ起動します。
 - ターゲットマシンを起動できない場合、ISO イメージを物理メディア（CD または DVD）にコピーして、ターゲットマシンでディスクをロードし、ブート CD からロードするようにマシンを設定して、ブート CD から再起動します。

① メモ: 場合によっては、ターゲットマシンの BIOS 設定を変更し、最初にロードされるボリュームがブート CD であることを確認する必要があります。

ターゲットマシンがブート CD から起動されると、Universal Recovery Console（URC）インタフェースが表示されます。この環境は、Rapid Recovery Core から直接システムドライブまたは選択したボリュームをリストアする場合に使用します。URC の IP アドレスおよび認証キー資格情報は、ブート CD から起動されるたびに更新されます。

- マシンのリストアウィザードの接続ページで、リストアするマシンの URC インスタンスから次のように認証情報を入力します。

表 156. 認証オプション

オプション	説明
IP アドレス	ターゲットマシンの URC で提供されている IP アドレス。
認証キー	ターゲットマシンの URC で提供されている認証キー。

- 「次へ」をクリックします。
- ディスクのマッピングページで、ボリュームを手動でマップする場合は、**手順 10**に進みます。ボリュームを自動的にマップするには、次の手順を実行します。
 - ボリュームのマッピング ドロップダウンメニューから、**自動** を選択します。
 - ボリュームのリストから、リストアするボリュームが選択されていることを確認します。すべてのボリュームがデフォルトで選択されます。

リストアしないボリュームがリストされている場合、オプションをクリアします。

① | **メモ:** リストアを実行するには、ボリュームを少なくとも1つ選択する必要があります。

- c 右側で、リストアの宛先ディスクを選択します。
 - d 「次へ」をクリックします。
 - e 「ディスクマッピングのプレビュー」 ページで、選択したリストアアクションのパラメータを確認します。
 - f [手順 18](#)に進みます。
- 17 ボリュームを手動でマップするには、ディスクのマッピング ページで、次の手順を実行します。
- a ボリュームのマッピング ドロップダウンメニューから、**手動** を選択します。
 - b 宛先 列で、リストアする宛先ボリュームを選択します。リストアしないボリュームがリストされている場合、オプションをクリアします。

① | **メモ:** リストアを実行するには、ボリュームを少なくとも1つ選択する必要があります。

- 18 「終了」をクリックします。

△ | **注意:** ターゲットドライブ上にあるすべてのパーティションおよびデータは完全に削除され、選択したリカバリポイントの内容に置き換えられます。これには、オペレーティングシステムおよびすべてのデータが含まれます。

- 19 リストアするボリュームに SQL または Microsoft Exchange データベースが含まれており、ライブリストアを実行する場合、「データベースをマウント解除」 ページでこれらをマウント解除するように求められます。リストアの完了後にこれらのデータベースを再マウントする場合、「リカバリポイントがリストアされたら、すべてのデータベースを自動的に再マウントします」を選択します。
- 20 **リストア** をクリックします。
- 21 ステータスメッセージで、**OK** をクリックして、リストアプロセスが開始されたことを確認します。
- リストアが開始されます。進行状況は イベント ページで監視できます。詳細については、「[タスク、アラート、およびジャーナルを使用したイベントの表示](#)」を参照してください。

Windows マシンのブート CD の作成について

Windows 用の Bare Metal Restore には、ブート CD と呼ばれるブートイメージが必要です。これは、Rapid Recovery Core Console でパラメーターを定義して作成します。このイメージは、特定の要件に合わせて調整されます。イメージを使用して、宛先 Windows マシンを起動します。環境の特性に応じて、このイメージを CD や DVD などの物理メディアに転送する必要がある場合もあります。その後で、ブートイメージを仮想的または物理的にロードし、ブートイメージから Windows サーバーを起動する必要があります。

Windows マシンに対して Bare Metal Restore (BMR) を実行するときの最初の手順として、Rapid Recovery Core Console でブート CD を作成します。これは、システムドライブまたはサーバ全体を Rapid Recovery Core から直接リストアするために使用する、Rapid Recovery Universal Recovery Console (URC) インタフェースを含むブータブル ISO イメージです。

作成するブート CD の ISO イメージは、リストア中のマシンに合わせて調整されるため、適切なネットワークドライバおよび大容量ストレージドライバが含まれている必要があります。リカバリポイントの元となるマシンから異種のハードウェアにリストアすることが予測される場合は、ストレージコントローラドライバおよび他のドライバをブート CD に含める必要があります。ブート CD へのこれらのドライバの導入については、「[ブート CD へのドライバの導入について](#)」を参照してください。

ブート CD へのドライバの導入について

ネットワークを介して Rapid Recovery Core と通信するには、サーバのドライバを認識するためのストレージドライバと、ネットワークアダプタドライバがブート CD イメージに必要です。

Windows 8.1 の 64 ビットのストレージコントローラドライバおよびネットワークアダプタドライバの汎用セットは、Windows 用のブート CD を生成するときに自動的に含まれます。新しいバージョンの Dell システムの場合は、これで要件が満たされます。他の製造元のシステムまたは旧バージョンの Dell システムでは、ブート CD の作成時にストレージコントローラドライバまたはネットワークアダプタドライバを導入する必要があることがあります。リストアの完了に必要なドライバが、作成したブート CD に含ま

れていないことが判明した場合は、URC を使用してターゲットマシンでドライバをロードすることもできます。詳細については、[Universal Recovery Console を使用したドライバのロード](#)を参照してください。

ドライバ導入は、ブート CD の作成時に、ターゲットサーバー上のリカバリ Console、ネットワークアダプタ、およびストレージ間の操作性を容易にするために使用されます。

リカバリポイントからリストアされたデータには、以前に存在したハードウェアのドライバが含まれます。異種のハードウェアに Bare Metal Restore を実行する場合は、データをドライブにリストアした後で、URC を使用して、リストア中のオペレーティングシステムにストレージコントローラドライバも導入する必要があります。これにより、一連の新しいハードウェアを使用して、リストアされたオペレーティングシステムを起動できるようになります。リストア後に OS を起動したら、OS で新しいハードウェアとやり取りするために必要な他のドライバをダウンロードし、インストールできます。

ブート CD の ISO イメージの作成

ブート CD は、Rapid Recovery で、bare metal restore (BMR) を実行するために予約されている ISO イメージのポータブルストレージの場所を示すために使用されます。このイメージには、Rapid Recovery Universal Recovery Console (URC) が含まれています。

BMR をマシン上で実行するには、ブート CD を使用してマシンを起動する必要があります。これにより URC が起動します。URC を使用することで、リストアを実行するために使用する必要があるリカバリポイントの場所に BMR ターゲットを接続できます。

- 1 リストアする必要があるサーバが保護されている Rapid Recovery Core Console でアイコンバーの詳細メニューをクリックし、**ブート CD** をクリックします。
- 2 ブート CD ページで **ブート CD を作成** をクリックします。
ブート CD を作成 ダイアログボックスが表示されます。
- 3 ブート CD を作成 ダイアログボックスの **出力パス** テキストボックスに、ブート CD の ISO イメージを保存する場所を入力します。

① **メモ:** ファイルの拡張子は **.iso** である必要があります。パスを指定する場合には、英数字、ハイフン、バックスラッシュ (パス区切り文字としてのみ)、ピリオド (ホスト名とドメインを区切るためのみ) のみを使用します。a から z までの文字では、大文字と小文字は区別されません。スペースは使用できません。他の記号または句読点文字は無効です。

- 4 接続オプションで、次のいずれかの操作を実行します。
 - ・ 動的ホスト構成プロトコル (DHCP) を使用して IP アドレスを動的に取得するには、**IP アドレスを自動的に取得** を選択します。
 - ・ URC の静的 IP アドレスを指定するには、**次の IP アドレスを使用** を選択し、次の情報を入力します。
 - ・ IP アドレス
 - ・ サブネットマスク
 - ・ デフォルトゲートウェイ
 - ・ DNS サーバー

① **メモ:** この 4 つのフィールドは、すべて指定する必要があります。

- 5 リカバリコンソールにリモートアクセスする必要がある、UltraVNC がインストールされている場合は、UltraVNC オプションで、次の手順を実行します。

① **メモ:** UltraVNC を使用して、URC を使用中にリモートから管理できます。ブート CD の使用中は、**Microsoft** ターミナルサービスにはログオンできません。

- a **UltraVNC を追加** を選択します。
- b **UltraVNC パスワード** を入力します。
- c **UltraVNC ポート** を入力します。デフォルトポートは 5900 です。

① **メモ:** UltraVNC オプションは、UltraVNC が既にインストールされている場合のみ使用できます。これらのオプションを使用するには、<http://www.uvnc.com/downloads/ultravnc/> に移動して、x64 アーキテクチャ用の UltraVNC バージョン 1.0.9.1 以降をダウンロードします。インストールして、winvnc.exe ファイルを C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64\ に保存します。

- 6 異なるハードウェアへのリストアを計画している場合は、次の手順を実行して、ターゲットシステムに適したストレージコントローラと他のドライバを導入します。

① **メモ:** すべてのバージョンの **Windows** が自動ドライバ導入と互換性があるわけではありません。使用しているオペレーティングシステムと互換性がない場合は、**C:\Program Files\AppRecovery\Core\BootCdKit\Drivers** にドライバを手動で保存します。

- サーバ製造元のウェブサイトからサーバ用のドライバをダウンロードし、解凍します。
 - 適切な圧縮ユーティリティ（WinZip など）を使用して、各ドライバを .zip ファイルに圧縮します。
 - ブート CD を作成 ダイアログボックスの ドライバペインで、**ドライバのアーカイブを追加** をクリックします。
 - ファイリングシステムで圧縮済みのドライバファイルを検索し、ファイルを選択して、**開く** をクリックします。
- ドライバファイルがブート CD を作成 ダイアログボックスの ドライバペインに表示されます。
- 必要に応じて、すべての必要なドライバが追加されるまで**手順 c** および**手順 d** を繰り返します。
 - ドライバペインで、導入するドライバを選択します。

ドライバの導入の詳細については、「**ブート CD へのドライバの導入について**」を参照してください。

- 7 **ブート CD を作成** をクリックします。

Rapid Recovery によってブート CD が作成され、指定したファイル名で保存されます。

- 8 このタスクの進行状況を監視するには、アイコンバーに移動し、イベントアイコンをクリックします。

Rapid Recovery イベントの監視の詳細については、「**タスク、アラート、およびジャーナルを使用したイベントの表示**」を参照してください。

ISO イメージの作成が完了すると、イメージのレコードがブート CD ページに表示されます。これには、アイコンバーの詳細メニューからアクセスできます。

ISO イメージにアクセスするには、指定した出力パスに移動するか、ブート CD ページのリンクをクリックして、ネットワークドライブなどの、新しいシステムにロードできる場所にイメージを保存します。

ブート CD の ISO イメージのメディアへの転送

ブート CD ファイルを作成すると、指定したパスに ISO イメージとして保存されます。このイメージは、Bare Metal Restore を実行するサーバーで、ドライブとしてマウントできる必要があります。

ブート CD の ISO イメージを、システム起動時にアクセスできるコンパクトディスク（CD）またはデジタルビデオディスク（DVD）に書き込むことができます。

マシンをブート CD から起動すると、Universal Recovery Console が自動的に起動します。

仮想マシンで BMR を実行する場合は、この手順は不要です。ISO イメージをドライブにロードし、その仮想マシンの設定を編集してドライブから開始するだけです。

ブート CD のロードおよびターゲットマシンの起動

ブート CD イメージを作成したら、新しく作成したブート CD を使用してターゲットサーバーを起動する必要があります。

Rapid Recovery Core Console に接続または Chromium を使用して追加のドライバをダウンロードするには、最初にイーサネットコントローラおよびネットワークアダプタをロードする必要があります。詳細については、「**Universal Recovery Console を使用したドライバのロード**」を参照してください。

① **メモ:** **DHCP** を使用して**ブート CD**を作成した場合は、**IP アドレスとパスワードを取得する必要があります**。

- 新しいサーバで、適切な場所からブート CD イメージをロードし、ブート CD イメージからサーバを起動して、Rapid Recovery Agent ソフトウェアと Win PE 5.1 をロードします。
- ターゲットマシンの画面上部に 3 つのアイコンボタンが付いた青色の Dell 画面が表示されます。
- Rapid Recovery Universal Recovery Console (URC) ユーザーインターフェースを開くには、画面上部にある Dell アイコンをクリックします。

マシンの IP アドレスとパスワードが 認証 の下に表示されます。

① **メモ:** ブート CD を使用してマシンを起動する毎に、新しい一時パスワードが生成されます。「ネットワークアダプタ設定」ペインに表示される IP アドレスと、「認証」ペインに表示される認証パスワードをメモしてください。この情報は、データリカバリプロセスで **Console** にログインしなおすときに必要になります。

① **メモ:** IP アドレスが提供されていない場合は、イーサネットコントローラとネットワークアダプタをロードします。

3 IP アドレスを変更するには、選択してから「変更」をクリックします。

① **メモ:** ブート CD を作成 ダイアログボックスで IP アドレスを指定した場合、**Universal Recovery Console** によってこのアドレスが使用され、ネットワークアダプタの設定 画面に表示されます。

マシンを Core に接続する準備ができたなら、リカバリポイントを選択し、Bare Metal Restore プロセスを続行します。

BMR への Universal Recovery Console の使用

Windows 用の bare metal restore (BMR) を起動するには、次の条件が必要です。

- Core に保存されているリカバリポイントをリストアするには、適切なハードウェアが配置されている必要があります。詳細については、「[Windows マシンに対して Bare Metal Restore を実行するための前提条件](#)」を参照してください。
- BMR の宛先 Windows マシンは、ブート CD イメージを使用して起動する必要があります。詳細については、[Windows マシンのブート CD の作成について](#)を参照してください。

BMR によって、選択したリカバリポイントを使用してマシンが起動されます。リカバリポイントには、以前のハードウェアのドライバが含まれています。異種のハードウェアにリストアする場合は、データをドライブにリストアした後で、URC を使用して、リストア中のオペレーティングシステムにストレージコントローラドライバを導入する必要があります。これにより、一連の新しいハードウェアを使用して、リストアされたオペレーティングシステムを起動できるようになります。OS を起動したら、OS で新しいハードウェアとやり取りするために必要な他のドライバをダウンロードし、インストールできます。

Rapid Recovery Core Console から BMR を起動するには、次のタスクを実行します。

- [リカバリポイントの選択と BMR の開始](#)
- [Bare Metal Restore のボリュームをマップについて](#)
- [Universal Recovery Console を使用したドライバのロード](#)

この処理は、[Windows マシンのベアメタルリストアの実行の手順](#)です。

Universal Recovery Console ツールについて

Universal Recovery Console (URC) には、bare metal restore (BMR) の実行に役立つ可能性のあるツールへのアクセス権が含まれます。

URC で起動する BMR ターゲット上でデルスプラッシュ画面の上部中央のアイコンをクリックすると、次のツールを見つけることができます。

- Far Manager** : このツールは Windows エクスプローラに似ています。BMR を完了し、Windows エクスプローラなどの独自の参照機能でオペレーティングシステムをインストールするまで、サーバ上でファイルを参照する手段を提供します。
- Chromium** : このブラウザは Google chrome™ のオープンソースを基本としており、URC からロードされたネットワークコントローラのあるサーバ上でインターネットをブラウズできます。
- PuTTY** : このツールはオープンソースのターミナルエミュレータです。Rapid Recovery BMR においては、ユーザーインターフェースが含まれていない NAS ストレージデバイスに接続することができます。この機能は NAS 上にあるアーカイブから復元する場合に必要なことがあります。
- Notepad** : Windows オペレーティングシステムと同様に、このツールを使用して書式のないメモを入力したり、ログファイルを表示したりすることができます。

- ・ **タスクマネージャ**：Windows オペレーティングシステムと同様に、このツールを使用してプロセスを管理したり、復元の進行中にサーバのパフォーマンスを監視したりすることができます。
- ・ **レジストリエディタ**：Windows オペレーティングシステムと同様に、このツールを使用して BMR ターゲットのシステムレジストリを変更することができます。
- ・ **コマンドプロンプト**：このツールを使用して、ユーザーインターフェースをインストールするまでの間、URC の外部で BMR ターゲットでコマンドを実行することができます。

Universal Recovery Console を使用したドライバのロード

この機能を使用すると、Bare Metal Restore を正常に実行するために必要だが ISO イメージに含まれていないドライバを追加できます。

このタスクは、[Windows マシンのベアメタルリストアの実行の手順](#)です。これは、[BMR への Universal Recovery Console の使用](#)の処理の一部です。

ブート CD の作成時には、必要なドライバを ISO イメージに追加できます。ターゲットマシンで起動したら、Universal Recovery Console (URC) からストレージドライバまたはネットワークドライバをロードすることもできます。

異種のハードウェアにリストアする場合、ストレージコントローラ、RAID、AHCI、チップセット、および他のドライバがブート CD にすでに存在していなければ、導入する必要があります。これらのドライバを使用すると、リストア処理後にシステムを再起動したときに、ターゲットサーバ上のすべてのデバイスをオペレーティングシステムで正常に操作できるようになります。

URC を使用してドライバをロードするには、次のいずれかの手順を実行します。

- ・ [Universal Recovery Console でのポータブルメディアを使用したドライバのロード](#)
- ・ [Chromium を使用した URC でのドライバのロード](#)

Universal Recovery Console でのポータブルメディアを使用したドライバのロード

この手順には次のタスクの前提条件があります。

- ・ [ブート CD の ISO イメージの作成](#)
- ・ [ブート CD の ISO イメージのメディアへの転送](#)
- ・ [ブート CD のロードおよびターゲットマシンの起動](#)

Universal Recovery Console (URC) でポータブルメディアデバイスを使用してドライバをロードするには、次の手順を実行します。

- 1 インターネットに接続されたマシンで、メーカーのウェブサイトからサーバ用のドライバをダウンロードし、解凍します。
- 2 適切な圧縮ユーティリティ (WinZip など) を使用して、各ドライバを .zip ファイルに圧縮します。
- 3 ドライバの .zip ファイルをコピーして、USB ドライブなどのポータブルメディアデバイスに保存します。
- 4 接続済みのマシンからメディアを削除し、それをブートターゲットサーバに挿入します。
- 5 ターゲットサーバで、ブート CD をロードしてから、マシンを起動します。
デルスプラッシュ画面が表示されます。
- 6 URC を起動するには、**デルアイコン** をクリックします。
URC でブート CD ドライバマネージャ タブが開きます。
- 7 **その他のデバイス** リストを展開します。
このリストには、ハードウェアに必要なドライバでも、ブート CD に含まれていないドライバが表示されます。
- 8 リスト上のデバイスを右クリックしてから、**ドライバをロード** をクリックします。
- 9 ドライバロードモードの選択 ウィンドウで、次のいずれかのオプションを選択します。
 - ・ 単一のドライバパッケージをロードします (デバイスサポートを確認せずにドライバをロードします)
 - ・ フォルダをスキャンしてドライバパッケージを探します (選択されたフォルダで選択されたデバイスのドライバを検索します)
- 10 ポータブルメディアデバイスのドライブを展開し、ドライバ (ファイル拡張子が .inf) を選択して、**OK** をクリックします。
ドライバが、現在のオペレーティングシステムにロードされます。

- 11 情報ウィンドウで、**OK** をクリックし、ドライバが正常にロードされていることを確認します。
- 12 必要に応じて、ロードするドライバごとにこの手順を繰り返します。

Chromium を使用した URC でのドライバのロード

この手順には次のタスクの前提条件があります。

- ・ ブート CD の ISO イメージの作成
- ・ ブート CD の ISO イメージのメディアへの転送
- ・ ブート CD のロードおよびターゲットマシンの起動

ブート CD にインストールされている Chromium ブラウザを使用して URC でドライバをロードするには、次の手順を実行します。

- 1 ターゲットサーバで、ブート CD をロードしてから、マシンを起動します。
デルスプラッシュ画面が表示されます。
- 2 URC を起動するには、**デルアイコン** をクリックします。
URC でブート CD ドライバマネージャ タブが開きます。
- 3 BMR ターゲットで、画面の一番上にあるツール（中央のアイコン）をクリックし、**Chromium** をクリックします。
- 4 Chromium ブラウザで必要なドライバをダウンロードできるウェブサイトに移動します。
- 5 ローカルフォルダやネットワークファイル共有などの選択した場所にドライバをダウンロードします。
- 6 **その他のデバイス** リストを展開します。
このリストには、ハードウェアに必要なドライバでも、ブート CD に含まれていないドライバが表示されます。
- 7 リスト上のデバイスを右クリックしてから、**ドライバをロード** をクリックします。
- 8 ドライバロードモードの選択 ウィンドウで、次のいずれかのオプションを選択します。
 - ・ 単一のドライバパッケージをロードします（デバイスサポートを確認せずにドライバをロードします）
 - ・ フォルダをスキャンしてドライバパッケージを探します（選択されたフォルダで選択されたデバイスのドライバを検索します）
- 9 ドライバを保存した場所に移動し、ドライバを選択したら、**OK** をクリックします。
ドライバが、現在のオペレーティングシステムにロードされます。
- 10 情報ウィンドウで、**OK** をクリックし、ドライバが正常にロードされていることを確認します。
- 11 必要に応じて、ロードするドライバごとにこの手順を繰り返します。

リカバリポイントの選択と BMR の開始

Universal Recovery Console (URC) が bare metal restore (BMR) のターゲットマシン上でアクセスできるようになった後、復元するリカバリポイントを選択する必要があります。

ロードするリカバリポイントを選択する Core Console に移動し、復元するデータの宛先としてリカバリ Console を指定します。

① | メモ: この手順は、**BMR を実行するすべての Windows マシンで必須ですが、Linux マシンでは任意です。**

このタスクは、[Windows マシンのベアメタルリストアの実行](#)の手順です。これは、[BMR への Universal Recovery Console の使用](#)の処理の一部です。

Core Console から Linux マシンで BMR を実行する場合、このタスクは [Linux マシンでの Bare Metal Restore の実行](#) の手順でもあります。これは、[コマンドラインを使用して Linux マシンに対して Bare Metal Restore を起動する](#) のプロセスの一部です。

- 1 Rapid Recovery Core Console で、保護対象マシンのリストから、復元する保護対象マシンの名前をクリックします。
選択したマシンのサマリ ページが表示されます。
- 2 **リカバリポイント** をクリックします。
- 3 BMR に使用するリカバリポイントの横にあるドロップダウンメニューをクリックし、**復元** をクリックします。
「マシンのリストア」ウィザードが表示されます。

- 4 「ブート CD を使用して任意のターゲットマシンにリカバリ」を選択します。
- 5 「ターゲットマシンで実行するブート CD を既に持っています」を選択します。
認証テキストボックスが表示されます。
- 6 次の表の説明に従って、復元するマシンに関する情報を入力します。

表 157. ターゲットマシン情報

テキストボックス	説明
IP アドレス	リストアするマシンの IP アドレス。これは、URC に表示される IP アドレスと同じです。
認証キー	選択されたサーバーに接続するための特定のパスワード。これは、URC に表示される認証キーと同じです。

- 7 「次へ」をクリックします。
入力した接続情報が URC と一致し、Core およびターゲットサーバーがネットワーク上で相互に正しく識別できる場合は、選択したリカバリポイントのボリュームがロードされ、「ディスクマッピング」ページが表示されます。この例では、次のステップはボリュームをマップすることです。
- 8 ディスクマッピングのオプションについて学習するには [Bare Metal Restore のボリュームをマップについて](#)に進みます。

Bare Metal Restore のボリュームをマップについて

Universal Recovery Console に接続されたら、リカバリポイントに表示されるボリュームと、ターゲットハードウェアの既存のボリューム間で、ボリュームをマップする必要があります。

Rapid Recovery はボリュームを自動的にマップしようとします。デフォルトのマッピングを受け入れると、宛先マシンのディスクがクリーンアップおよび再パーティション化され、既存の以前のすべてのデータが削除されます。アライメントはリカバリポイントに表示されるボリュームの順番に実行され、ボリュームはサイズなどに従ってディスクに適切に割り当てられます。ターゲットドライブに十分な容量がある場合には、自動ディスクアライメントの使用時にパーティション化は必要ありません。1つのディスクを複数のボリュームで使用できます。ドライブを手動でマップする場合は、同じディスクを2度使用できないことに注意してください。

手動マッピングの場合は、リストアする前に、新しいマシンが正しくフォーマットされている必要があります。宛先マシンには、システムで予約済みのボリュームを含め、リカバリポイントのボリュームごとに別個のパーティションが必要です。詳細については、「[BMR への Universal Recovery Console の使用](#)」を参照してください。

次のいずれかのディスクマッピングオプションの次の手順を実行します。

- ・ [BMR のディスクの自動マッピング](#)
- ・ [BMR のディスクの手動でのマッピング](#)

△ 注意: Rapid Recovery では FAT32 パーティションと ReFS パーティションがサポートされますが、現時点では、ReFS のドライブ制限によりフルリストアと BMR しかサポートされないため、リストアはユーザーモード、VM エクスポートなどで実現されます。ReFS ファイルシステムを含む少なくとも1つの Agent ボリュームを Core で保護している場合は、ReFS のネイティブサポートを提供している、Windows 8、Windows 8.1、Windows 10、Windows Server 2012、および Windows Server 2012 R2 マシンに Core をインストールする必要があります。これらにインストールされない場合、機能が制限され、ボリュームイメージのマウントなどが関係する操作が動作しなくなります。Rapid Recovery Core Console にこれらのオカレンスのエラーメッセージが表示されます。

△ 注意: ストレージスペースのディスク構成の Bare metal restore (Windows 8.1 の機能) はサポートされません。詳細については、『[Dell Data Protection | Rapid Recovery のインストールおよびアップグレードガイド](#)』を参照してください。

このタスクは、[Windows マシンのベアメタルリストアの実行の手順](#)です。これは、[BMR への Universal Recovery Console の使用](#)の処理の一部です。

Core Console から Linux マシンで BMR を実行する場合、このタスクは [Linux マシンでの Bare Metal Restore の実行の手順](#)でもあります。これは、[Linux 用の Bare Metal Restore の開始](#)の処理の一部です。

BMR のディスクの自動マッピング

この手順では、マシンの復元ウィザードを使用する bare metal restore (BMR) 実行中に、自動的にディスクをマップすることができます。

リカバリするボリュームと、それらの復元先を自動的に選択するには、次の手順を実行します。

- 1 マシンの復元ウィザードのディスクのマッピング ページで、ボリュームのマッピングの横にあるドロップダウンメニューから **自動** を選択します。
- 2 左側の表で、適切なボリュームがリストされ、選択されていることを確認します。

① **メモ:** BMR では通常、システムで予約済みのボリューム（通常は C:\ のボリュームですが、常にそうであるとは限りません）を少なくともリストアップする必要があります。BMR を実行するには、少なくとも 1 つのボリュームを選択する必要があります。

- 3 右側の表で、ターゲットマシン上でボリュームをマップするディスク（複数可）を選択します。
- 4 「次へ」をクリックします。
- 5 ディスクマッピングプレビュー ページで、リカバリポイントボリュームと復元の宛先ボリュームのマッピングを確認します。
- 6 復元を開始するには、**終了** をクリックします。

△ **注意:** 復元を開始 をクリックすると、ターゲットドライブ上にあるすべてのパーティションおよびデータは完全に削除され、選択したリカバリポイントの内容に置き換えられます。これには、オペレーティングシステムおよびすべてのデータが含まれます。

BMR のディスクの手動でのマッピング

この手順では、リストアップされるマシン上のどのディスクをどこに保存するかを指定する方法について説明します。

ディスクを手動でマップするには、最初に BMR ターゲットマシン上のコマンドラインで DiskPart を使用してターゲットボリュームを作成してフォーマットする必要があります。詳細については、Microsoft Developer Network の「[DiskPart コマンドラインオプション \(標準 7 SP1\)](#)」を参照してください。

リカバリするボリュームと、それらのリストアップ先を選択するには、次の手順を実行します。

- 1 マシンのリストアップウィザードのディスクのマッピング ページで、ボリュームのマッピングの横にある **手動** を選択します。

① **メモ:** bare metal restore (BMR) を実行するマシンのドライブにボリュームが存在しない場合は、このオプションが表示されず、ボリュームを手動でマップできません。

- 2 ソースボリュームのボリュームマッピング領域で、ソースボリュームが選択されており、その下に適切なボリュームが表示され、選択されていることを確認します。
- 3 宛先の下にあるドロップダウンメニューから、選択されたリカバリポイントの BMR のターゲットボリュームとなる適切な宛先を選択し、**リストアップ** をクリックします。
- 4 確認ダイアログボックスで、リカバリポイントのソースとリストアップの宛先ボリュームのマッピングを確認します。
- 5 リストアップを開始するには、**リストアップを開始** をクリックします。

△ **注意:** リストアップを開始 を選択すると、ターゲットドライブにある既存のすべてのパーティションとデータが完全に削除され、選択されたリカバリポイントの内容（オペレーティングシステムおよびすべてのデータを含む）で置き換えられます。

アーカイブからの BMR の実行

Rapid Recovery を使用すると、アーカイブされたリカバリポイントを使用してベアメタルからマシンを復元できます。

この手順には次のタスクの前提条件があります。

- ・ [ブート CD の ISO イメージの作成](#)

・ ブート CD のロードおよびターゲットマシンの起動

Universal Recovery Console (URC) から Rapid Recovery Core にアクセスし、復元するリカバリポイントを取得できます。アーカイブに保存されているリカバリポイントからお使いのベアメタルマシンを復元することもできます。URC を使用すれば、このアーカイブがローカルドライブ、ネットワーク共有、またはクラウドアカウント上のどこにあるかどうかに関係なく、このアーカイブにアクセスできます。

- 1 URC で、**復元ポイントの詳細** タブをクリックします。
- 2 **場所のタイプ** ドロップダウンリストで、アーカイブの場所を選択します。次のいずれかのオプションを選択できます。
 - ・ ローカル
 - ・ ネットワーク
 - ・ クラウド
- 3 選択した場所のタイプに応じて、次の表に説明されている資格情報を入力します。

表 158. 場所のタイプの資格情報オプション

場所のタイプ	オプション	説明
ローカル	ローカルパス	アーカイブの現在の場所です。
ネットワーク	ネットワークパス	アーカイブの現在の場所です。
	ユーザー	ネットワーク共有アクセス用のユーザー名です。
	パスワード	ネットワーク共有アクセス用のパスワードです。
クラウド	クラウドタイプ	クラウドストレージの場所のプロバイダです。次のオプションから選択します。 ・ Microsoft Azure ・ Amazon™ S3 ・ OpenStack ベースのクラウド ・ Rackspace® クラウドファイル

- 4 クラウドタイプを選択した場合、お使いのクラウドプロバイダに関連する資格情報を入力します。
 - ・ Microsoft Azure の場合、次の手順を実行します。
 - 1 次の資格情報を入力します。
 - ・ ストレージアカウント名
 - ・ アクセスキー
 - 2 コンテナ名の場合、ドロップダウンリストからコンテナを選択します。
 - 3 クラウドパスの場合、ドロップダウンリストからアーカイブへのパスを選択します。
 - ・ Amazon™ S3 の場合、次の手順を実行します。
 - 1 次の資格情報を入力します。
 - ・ アクセスキー
 - ・ 秘密キー
 - 2 コンテナ名の場合、ドロップダウンリストからコンテナを選択します。
 - 3 クラウドパスの場合、ドロップダウンリストからアーカイブへのパスを選択します。
 - ・ Powered By OpenStack または Rackspace クラウドファイルのアカウントの場合、次の手順を実行します。
 - 1 次の情報を入力します。
 - ・ 地域
 - ・ ユーザー
 - 2 次のオプションのいずれかを選択します。
 - ・ パスワード

- ・ API キー
- 3 テキストボックスに、手順 c で選択した内容に基づいて情報を入力します。
- 4 次の情報を入力します。
 - ・ テナント ID
 - ・ 認証 URL
 - ・ コンテナ名
 - ・ クラウドパス
- 5 次へ をクリックします。
- 6 マシン ページで、復元するマシンを選択し、次へ をクリックします
- 7 リカバリポイント ページで、マシンの復元に使用するリカバリポイントを選択し、次へ をクリックします。
- 8 マッピング ページで、次のオプションのいずれかを選択し、対応する手順を実行します。
 - ・ ボリュームのマッピング ドロップダウンメニューから、自動 を選択します。
 - 1 左側の表で、適切なボリュームがリストされ、選択されていることを確認します。

① **メモ:** BMR では通常、システムで予約済みのボリュームとシステムボリューム（通常は C:\ ボリュームですが、常にそうであるとは限りません）を少なくとも復元する必要があります。BMR を実行するには、少なくとも 1 つのボリュームを選択する必要があります。
 - 2 右側の表で、ターゲットマシン上でボリュームをマップするディスク（複数可）を選択します。
 - ・ ボリュームのマッピング ドロップダウンメニューから、手動 を選択します。

① **メモ:** ディスクを手動でマップするには、コマンドラインで DiskPart を使用し、ターゲットボリュームを作成してフォーマットする必要があります。詳細については、Microsoft Developer Network の「DiskPart コマンドラインオプション（標準 7 SP 1）」を参照してください。

① **メモ:** bare metal restore（BMR）を実行するマシンのドライブにボリュームが存在しない場合は、このオプションが表示されず、ボリュームを手動でマップできません。
 - ・ 宛先ボリューム のドロップダウンメニューから、リカバリポイント内のボリュームごとに適切なターゲットボリュームを選択します。
- 9 マウントマップパス テキストボックスに、マッピングファイルを一時的に格納する宛先を入力します。
デフォルトの場所は X:\ProgramData\AppRecovery\IndexEntriesMaps です。

① **メモ:** 宛先に十分な空き容量があることを確認するには、マウントボリュームの総容量を 1,024 で割ります。たとえば、計算式 (Mount volume total capacity) / 1024 = Free space の後、1 TB / 1024 = 1 GB を使用します。
- 10 リストア をクリックします。
URC によって新しいディスクにボリュームがマッピングされます。
- 11 リストア をクリックします。
URC によってデータがターゲットマシンに復元されます。進行状況は リストアの進捗状況 タブで表示できます。
- 12 復元が完了したら、ブート CD を取り外します。
- 13 BMR ターゲットマシンを Windows で起動するには、マシンを再起動します。

オペレーティングシステムへのドライバのロード

この手順では、bare metal restore（BMR）ターゲット上のオペレーティングシステムにドライバをロードする方法について説明します。

オペレーティングシステムにドライバを導入するために、次の作業を完了しています。

- ・ Rapid Recovery Core Console で Boot CD Builder を使用してブート CD を作成しました。詳細については、「ブート CD の ISO イメージの作成」を参照してください。
- ・ ブート CD を BMR ターゲットにロードしました。詳細については、ブート CD のロードおよびターゲットマシンの起動を参照してください。

- ・ ストレージおよびネットワークの必要なドライバまたはコントローラをロードしました。詳細については、[Universal Recovery Console を使用したドライバのロード](#)を参照してください。
- ・ Rapid Recovery Core Console でマシンのリストアウィザードを使用するか、Universal Recovery Console (URC) からアーカイブを使用してリストアを実行しました。詳細については、「[マシンのリストアウィザードを使用した Bare Metal Restore の実行](#)」および「[アーカイブからの BMR の実行](#)」を参照してください。

リストアを実行した後で、bare metal restore (BMR) ターゲット上のオペレーティングシステムにドライバを導入するまで処理は完了しません。このタスクは、URC でのドライバのロードに加えて行います。

- 1 選択した BMR 手順でリストアをクリックした後で（前提条件を参照してください）、**既存の Windows ドライバマネージャ** タブをクリックします。
- 2 ドロップダウンリストから、オペレーティングシステムを選択します。
URC で使用可能なドライバが検索されます。
- 3 追加のドライバをロードするには、**ロードを強制** をクリックします。
- 4 ファイリングシステムで圧縮済みのドライバファイルを検索し、ファイルを選択します。
- 5 「OK」をクリックします。
URC によって、選択したオペレーティングシステムにドライバがロードされます。
- 6 ロードする必要がある追加のドライバごとに[手順 3 ～手順 5](#)を繰り返します。
- 7 BMR ターゲットマシンを再起動します。
BMR が完了します。再起動したときに問題が発生した場合は、「[起動の問題の修復](#)」を参照してください。

Linux マシンでの Bare Metal Restore の実行

Rapid Recovery では、システムボリュームの復元を含め、Linux マシンの bare metal restore (BMR) を実行できます。Linux マシンをリストアすると、ブートボリュームのリカバリポイントにロールバックします。local_mount コマンドラインユーティリティや Core Console UI から、BMR 機能を使用できます。

△ **注意:** BMR プロセスを開始する前に、リストアする Linux マシンに **ext2** ブートパーティションが存在しないことを確認してください。**ext2** パーティションタイプが存在するマシンで BMR を実行すると、通常、そのプロセスの結果、マシンが起動しなくなります。このようなマシンで BMR を実行するには、マシンの保護とバックアップを開始する前に、**ext2** パーティションを **ext3**、**ext4** または **XFS** に変換する必要があります。

△ **注意:** BMR の実行後初めて復元された Linux マシンを起動する際に、**Rapid Recovery** が復元されたマシンのベースイメージを取得します。このプロセスの所要時間は、マシン上のデータ量によっては、増分スナップショットを取得する場合よりも長くなることがあります。ベースイメージと増分スナップショットの詳細については、[保護スケジュールについて](#)を参照してください。

Linux マシンに対して Bare Metal Restore を実行するには、次のタスクを実行します。

- ・ Linux ブートイメージの管理。この Linux Live DVD ブートの ISO イメージは、宛先ドライブの起動に使用されます。このドライブから Universal Recovery Console にアクセスして Core 上のバックアップと通信できます。「[Linux ブートイメージの管理](#)」を参照してください。
 - ・ BMR の起動イメージを取得するには、必要なイメージをあらかじめ調べておき、ライセンスポータルからダウンロードする必要があります。[Linux 用のブート ISO イメージについて](#)を参照してから、[Linux 用のブート ISO イメージのダウンロード](#)を参照してください。
 - ・ 宛先 Linux マシンの起動に物理メディアが必要な場合は、ISO イメージをメディアに転送する必要があります。「[メディアへの Live DVD の ISO イメージの保存](#)」を参照してください。
 - ・ どの場合にも、宛先サーバーにブートイメージをロードして、ブートイメージからサーバーを起動する必要があります。「[Live DVD のロードおよびターゲットマシンの起動](#)」を参照してください。
 - ・ メディアをロードした後、Linux マシンを Rapid Recovery Core に接続する必要があります。「[Rapid Recovery Core から BMR ターゲットへの接続](#)」を参照してください。
- ・ パーティションの管理。Linux マシンで BMR を実行する前に、パーティションを作成またはマウントしなければならない場合があります。「[Linux パーティションの管理](#)」を参照してください。
 - ・ BMR を実行する Linux システムには、リカバリポイントのソースボリュームと同じパーティションが必要です。必要に応じて、ターゲットシステムで追加のパーティションを作成しなければならない場合があります。「[宛先ドライブでのパーティションの作成](#)」を参照してください。

- ・ 手動 BMR を実行する場合は、まずパーティションをマウントする必要があります。「[コマンドラインからのパーティションのマウント](#)」を参照してください。パーティションのマウント手順は、コマンドラインから BMR を実行するプロセスに含まれています。「[コマンドラインを使用して Linux マシンに対して Bare Metal Restore を起動する](#)」を参照してください。
Core Console から BMR を実行する場合に自動パーティション分割を使用する場合は、パーティションをマウントする必要はありません。Rapid Recovery で、復元中のリカバリポイントに含まれているのと同じパーティションが復元されます。
- ・ Linux 用の Bare Metal Restore の起動。Live DVD ブートイメージから宛先マシンを起動したら、BMR を起動できます。Rapid Recovery ユーザーインターフェースからこの操作を実行するか、local_mount ユーティリティを使用したコマンドラインから行うかによって、必要なタスクが異なります。「[Linux 用の Bare Metal Restore の開始](#)」を参照してください。
- ・ Core Console を使用する場合は、Core のリカバリポイントからリストアを開始する必要があります。「[リカバリポイントの選択と BMR の開始](#)」を参照してください。
- ・ Core Console を使用する場合は、UI からボリュームをマップする必要があります。「[Bare Metal Restore のボリュームをマップについて](#)」を参照してください。
- ・ コマンドラインから復元する場合は、必要に応じて、画面ユーティリティを使用するとターミナルコンソールでのスクロール機能および表示機能を拡張できます。このユーティリティはデフォルトで開きます。閉じた場合は、再起動できます。詳細については、「[Screen ユーティリティの開始](#)」を参照してください。
- ・ local_mount を使用する場合は、すべてのタスクがコマンドラインで実行されます。詳細については、「[コマンドラインを使用して Linux マシンに対して Bare Metal Restore を起動する](#)」を参照してください。
- ・ Bare Metal Restore の確認。Bare Metal Restore を開始したら、進捗状況を確認および監視できます。「[コマンドラインからの Bare Metal Restore の確認](#)」を参照してください。
- ・ リストアの進捗状況を監視できます。「[リカバリの進捗状況の表示](#)」を参照してください。
- ・ 処理が完了したら、リストアされたサーバーを起動できます。「[リストアされたターゲットサーバの起動](#)」を参照してください。
- ・ BMR プロセスのトラブルシューティングを行います。「[Universal Recovery Console への接続に関するトラブルシューティング](#)」および「[起動の問題の修復](#)」を参照してください。

Linux マシンに対して Bare Metal Restore を実行するための前提条件

Linux マシンに対して Bare Metal Restore を実行するプロセスを開始する前に、次の条件および基準を満たしていることを確認する必要があります。

- ・ リストアするマシンのバックアップ。リストアする保護対象サーバのリカバリポイントが含まれた、機能している Rapid Recovery Core が必要です。
- ・ リストアするハードウェア（新規または既存、同種または異種）。ターゲットマシンは、Agent のインストール要件を満たしている必要があります。詳細については、『Rapid Recovery インストールおよびアップグレードガイド』を参照してください。
- ・ Live DVD ブートイメージ。ブート可能な Linux バージョンが含まれる、Linux Live DVD の ISO イメージを取得します。Dell Data Protection | Rapid Recovery ライセンスポータル (<https://licenseportal.com>) からダウンロードします。Live DVD のダウンロードで問題がある場合は、Dell Rapid Recovery のサポートにお問い合わせください。
- ・ イメージメディアとソフトウェア。物理メディアを使用する場合は、空の CD または DVD とディスク書き込みソフトウェア、または ISO イメージの作成ソフトウェアが必要です。
- ・ 互換性のあるストレージドライバとネットワークアダプタドライバ。異種のハードウェアにリストアする場合は、RAID、AHCI、ターゲットオペレーティングシステムのチップセットドライバなど、ターゲットマシンに互換性のあるストレージドライバとネットワークアダプタドライバが適宜必要です。
- ・ ストレージスペースとパーティション（適宜）。ターゲットマシンでソースボリュームを含める宛先パーティションを作成するのに十分な容量がハードドライブにあることを確認します。宛先パーティションには、少なくとも元のソースパーティションと同じ容量が必要です。
- ・ リストアパス。リストアパスを特定します。これは、デバイスファイル記述子のパスです。デバイスファイル記述子のパスを特定するには、ターミナルウィンドウから fdisk コマンドを使用します。

Linux ブートイメージの管理

Linux 用の Bare Metal Restore には、Live DVD ブートイメージが必要です。これは、Dell Data Protection | Rapid Recovery ライセンスポータル からダウンロードします。このイメージを使用して、宛先 Linux マシンを起動します。環境の特性に応じて、このイメージを CD や DVD などの物理メディアに転送する必要がある場合もあります。その後で、ブートイメージを仮想的または物理的にロードし、ブートイメージから Linux サーバーを起動する必要があります。

① **メモ:** Live DVD は、以前は Live CD と呼ばれていました。

Linux ブートイメージの管理は、Linux マシンでの Bare Metal Restore の実行 の手順です。

次のタスクを実行できます。

Linux 用のブート ISO イメージについて

Linux マシンに対して Bare Metal Restore (BMR) を実行するときの最初の手順として、Dell Data Protection | Rapid Recovery ライセンスポータル から Live DVD の ISO イメージをダウンロードします。Live DVD は、Rapid Recovery でサポートされるすべての Linux ファイルシステムで動作し、Linux のブータブルバージョン、画面ユーティリティ、Rapid Recovery Universal Recovery Console (URC) インタフェースが含まれます。Rapid Recovery Universal Recovery Console は、Rapid Recovery Core から直接システムドライブまたはサーバー全体をリストアするために使用される環境です。

① **メモ:** 国際標準化機構 (ISO) は、ファイルシステムの標準を設定するさまざまな国家組織からの代表者で構成される国際的な組織です。ISO 9660 は、データ交換用の光学ディスクメディアに使用されるファイルシステム標準で、各種オペレーティングシステムをサポートします。ISO イメージとは、ディスクの全セクタに加え、ディスクのファイルシステムも含むアーカイブファイルまたはディスクイメージです。

Linux 用のブート ISO イメージのダウンロード

お使いの Rapid Recovery のバージョンと一致する Live DVD の ISO イメージをダウンロードする必要があります。Live DVD の現在のバージョンは Dell Data Protection | Rapid Recovery ライセンスポータル (<https://licenseportal.com>) から入手できます。別のバージョンが必要な場合は、Dell Rapid Recovery のサポートにお問い合わせください。

① **メモ:** Dell Data Protection | Rapid Recovery ライセンスポータルの詳細については、Dell Data Protection | Rapid Recovery ライセンスポータルの『ユーザーガイド』を参照してください。

このタスクは、Linux マシンでの Bare Metal Restore の実行 の手順です。これは、Linux ブートイメージの管理 の処理の一部です。

Live DVD の ISO イメージをダウンロードするには、次の手順を実行します。

- 1 Dell Data Protection | Rapid Recovery ライセンスポータル (<https://licenseportal.com>) にログインします。
- 2 「ダウンロード」エリアにアクセスします。
- 3 「Linux ベースのアプリケーション」にスクロールダウンし、「Linux Live DVD」セクションで「ダウンロード」をクリックします。
- 4 Live DVD の ISO イメージを保存します。仮想マシンからリストアする場合は、ネットワークの場所に保存でき、ISO イメージに関連付けられている CD/DVD ドライブから起動するよう仮想マシンを設定できます。
- 5 物理マシンからリストアする場合は、ブート CD の ISO イメージをコンパクトディスク (CD) またはデジタルビデオディスク (DVD) に書き込み、ターゲットマシンをこの CD/DVD から起動できます。詳細については、「メディアへの Live DVD の ISO イメージの保存」を参照してください。

メディアへの Live DVD の ISO イメージの保存

Linux Live DVD ファイルをダウンロードすると、指定したパスに ISO イメージとして保存されます。ターゲット Linux マシンを Live DVD イメージから起動できる必要があります。

このタスクは、Linux マシンでの Bare Metal Restore の実行 の手順です。これは、Linux ブートイメージの管理 の処理の一部です。

ブート CD の ISO イメージを、コンパクトディスク (CD) またはデジタルビデオディスク (DVD) に書き込みます。

仮想マシンで BMR を実行する場合は、この手順は不要です。ISO イメージをドライブにロードし、その仮想マシンのマシン設定を編集してドライブから開始するだけです。仮想エクスポートを使用して Linux 仮想マシンを復元することもできます。詳細については、「[VM エクスポート](#)」を参照してください。

Live DVD のロードおよびターゲットマシンの起動

Live DVD の ISO イメージを取得したら、新しく作成した Live DVD から Linux マシンを起動する必要があります。

このタスクは、「[Linux マシンでの Bare Metal Restore の実行](#)」のステップです。これは、「[Linux ブートイメージの管理](#)」のプロセスの一部です。

- 1 新しいサーバーに移動し、適切な場所から Live DVD イメージをロードします。サーバーを Live DVD イメージから起動することを指定します。
- 2 マシンを起動します。
Rapid Recovery スプラッシュ画面が表示されてターミナルウィンドウが開き、マシンの IP アドレスと認証パスワードが表示されます。

① **メモ:** Live DVD を使用してマシンを起動するたびに、新しい一時パスワードが生成されます。

- 3 最初の画面に表示される IP アドレスと認証パスワードをメモしてください。この情報は、データリカバリプロセスで Console にログインしなおすときに必要になります。

Rapid Recovery Core から BMR ターゲットへの接続

Live DVD を使用してターゲット Linux マシンを起動した後で、Core からこのマシンに接続して、Bare Metal Restore プロセスを開始できます。このプロセスを実行するには、次のいずれかの方法を使用できます。

- ・ Rapid Recovery Core Console からリストアを起動する。詳細については、「[Linux 用の Bare Metal Restore の開始](#)」を参照してください。
- ・ aamount ユーティリティを使用して、コマンドラインからリストアを起動する。詳細については、[コマンドラインを使用して Linux マシンに対して Bare Metal Restore を起動する](#)を参照してください。

Linux パーティションの管理

BMR を実行する場合、データのリストア先となる宛先ドライブには、リストア中のリカバリポイントと同じパーティションが必要です。この要件を満たすように、パーティションを作成する必要があります。

復元の起動は、aamount ユーティリティを使用してコマンドラインから行うか、Rapid Recovery Core Console から行うことができます。ユーザーインターフェースからリストアする場合は、まずパーティションをマウントする必要があります。

Linux パーティションの管理は、[Linux マシンでの Bare Metal Restore の実行](#)のステップです。

次のタスクを実行できます。

関連するリンク

- [宛先ドライブでのパーティションの作成](#)
- [宛先ドライブでのパーティションのフォーマット](#)
- [コマンドラインからのパーティションのマウント](#)

宛先ドライブでのパーティションの作成

BMR を実行する場合、宛先ドライブが1つのパーティションで構成される新規ボリュームであることがよくあります。宛先マシンのドライブには、ボリュームサイズを含め、リカバリポイントと同じパーティションテーブルが必要です。宛先ドライブに同じパーティションが含まれていない場合は、Bare Metal Restore を実行する前に作成する必要があります。fdisk ユーティリティを使用して、ソースドライブのパーティションと同じものを宛先ドライブに作成します。

△ 注意: 下の手順は例です。カスタマ環境は異なります。使用するコマンドは、お使いの環境の詳細に合わせて変更する必要があります。

このタスクは、[Linux マシンでの Bare Metal Restore の実行](#)の手順です。これは、[Linux パーティションの管理](#)の処理の一部です。

- 1 必要に応じて、Screen ユーティリティを使用できます。このユーティリティはデフォルトで起動し、マシンを再起動するまで、アクティブ状態が維持されます。

① **メモ:** 明示的にダイアログボックスを閉じてから、もう一度開く場合は、[Screen ユーティリティの開始](#)を参照してください。

- 2 コマンドラインから次のコマンドを入力して **<Enter>** を押し、管理者として実行するように権限を変更してから、既存のディスクパーティションを表示します。

```
sudo fdisk -l
```

すべてのボリュームのリストが表示されます。

この例では、パーティション化するボリュームを /dev/sda と想定しています。ボリュームが異なる（古いドライブでは /dev/hda と表示されるなど）場合は、コマンドを適宜変更します。

- 3 新しいブートパーティションを作成するには、次のコマンドを入力して **<Enter>** を押します。

```
sudo fdisk /dev/sda
```

- 4 新しいブートパーティションを作成するには、次のコマンドを入力して **<Enter>** を押します。

```
n
```

- 5 新しいプライマリパーティションを作成するには、次のコマンドを入力して **<Enter>** を押します。

```
p
```

- 6 パーティション番号を指定するには、パーティション番号を入力して **<Enter>** を押します。たとえば、パーティション 1 を指定するには、「1」と入力して **<Enter>** を押します。

- 7 最初のセクタである 2048 を使用するには、**<Enter>** を押します。

- 8 ブートパーティションに適切な容量を割り当てるには、プラス記号および割り当てる容量を入力して **<Enter>** を押します。たとえば、ブートパーティションに 500 M を割り当てるには、次のように入力して **<Enter>** を押します。

```
+512000K
```

- 9 （パーティションをブート可能にするため）ブートパーティションのブート可能フラグを切り替えるには、次のコマンドを入力して **<Enter>** を押します。

```
a
```

- 10 適切なパーティションにブート可能フラグを割り当てるには、パーティション番号を入力して **<Enter>** を押します。たとえば、パーティション 1 にブート可能フラグを割り当てるには、「1」と入力して **<Enter>** を押します。

- 11 必要に応じてディスクのパーティション作成を続行します。

- 12 fdisk ユーティリティでのすべての変更内容を保存するには、次のコマンドを入力して **<Enter>** を押します。

```
w
```

宛先ドライブでのパーティションのフォーマット

Bare Metal Restore を実行する宛先ドライブの新しいボリュームでパーティションを作成した後、自動パーティションを使用していない場合は、マウントする前にパーティションをフォーマットする必要があります。この状況に該当する場合は、次の手順を実行して、ext3、ext4、または XFS 形式でパーティションをフォーマットします。

その他のシナリオについては、このトピックに記載されているようにパーティションをフォーマットする必要はありません

このタスクは、[Linux マシンでの Bare Metal Restore の実行](#)の手順です。これは、[Linux パーティションの管理](#)の処理の一部です。

- 1 必要に応じて、Screen ユーティリティを使用できます。このユーティリティはデフォルトで起動し、マシンを再起動するまで、アクティブ状態が維持されます。

① **メモ:** 明示的にダイアログボックスを閉じてから、もう一度開く場合は、[Screen ユーティリティの開始](#)を参照してください。

- 2 コマンドラインから次のコマンドを入力して **<Enter>** を押し、管理者として実行するように権限を変更してから、既存のディスクパーティションを表示します。

```
sudo fdisk -l
```

すべてのボリュームのリストが表示されます。

この例では、フォーマットするパーティションを /dev/sda1 と想定しています。ボリュームが異なる（古いドライブでは /dev/hda と表示されるなど）場合は、コマンドを適宜変更します。

- 3 宛先パーティションで使用する形式に基づいて次のいずれかのコマンドを選択します。

- ・ ext3 形式でパーティションをフォーマットするには、次のコマンドを入力して **<Enter>** を押します。

```
sudo mkfs.ext3 /dev/sda1
```

- ・ ext4 形式でパーティションをフォーマットするには、次のコマンドを入力して **<Enter>** を押します。

```
sudo mkfs.ext4 /dev/sda1
```

- ・ XFS 形式でパーティションをフォーマットするには、次のコマンドを入力して **Enter** を押します。

```
sudo mkfs.xfs /dev/sda1
```

選択したパーティションが適宜フォーマットされます。

- 4 必要に応じて、その他のパーティションをフォーマットする必要がある場合は、この手順を繰り返します。

コマンドラインからのパーティションのマウント

Rapid Recovery Core Console を使用して BMR を実行する場合は、まず適切なパーティションを宛先マシンにマウントする必要があります。この操作は、Universal Recovery Console でコマンドラインから実行します。

このタスクは、[Linux マシンでの Bare Metal Restore の実行](#)の手順です。これは、[Linux パーティションの管理](#)の処理の一部です。

リストアを実行する前に Linux マシンでパーティションをマウントするには、次の手順を実行します。

- 1 コマンドラインから次のコマンドを入力して **<Enter>** を押し、管理者として実行するように権限を変更してから、既存のディスクパーティションを表示します。

```
sudo fdisk -l
```

すべてのボリュームのリストが表示されます。

- 2 マウントディレクトリに対して BMR を実行するために必要なパーティションをすべてフォーマットします。これは、リカバリポイントに含まれるボリュームと一致している必要があります。たとえば、マウントするボリュームが sda1 であり、マウントディレクトリが mnt の場合は、次のコマンドを入力して **<Enter>** を押します。

- 3 マウントディレクトリに対して BMR を実行するために必要なパーティションをすべてマウントします。これは、リカバリポイントに含まれるボリュームと一致している必要があります。たとえば、マウントするボリュームが sda1 であり、マウントディレクトリが mnt の場合は、次のコマンドを入力して **<Enter>** を押します。

```
mount /dev/sda1 /mnt
```

- 4 必要なボリュームをすべてマウントするまで、[手順 3](#) を必要に応じて繰り返します。

ボリュームをマウントした後で、Rapid Recovery Core Console から宛先 Linux マシンに対して復元を実行できます。「[Linux 用の Bare Metal Restore の開始](#)」を参照してください。

Linux 用の Bare Metal Restore の開始

Linux 用の Bare Metal Restore (BMR) を起動するには、次の条件が必要です。

- ・ Core に保存されているリカバリポイントをリストアするには、適切なハードウェアが配置されている必要があります。詳細については、「[Linux マシンに対して Bare Metal Restore を実行するための前提条件](#)」を参照してください。
- ・ BMR の宛先 Linux マシンは、Live DVD ブートイメージを使用して起動する必要があります。詳細については、[Linux ブートイメージの管理](#)を参照してください。

- ・ リストアする Linux マシン上のボリューム数は、リカバリポイントに含まれるボリューム数と一致している必要があります。また、Rapid Recovery Core Console または local_mount を使用したコマンドラインのどちらからリストアするかも決定する必要があります。詳細については、[Linux パーティションの管理](#)を参照してください。
- ・ Core Console UI からリストアする場合は、BMR の起動の最初の手順として、適切なリカバリポイントを選択してから、Universal Recovery Console から取得した IP アドレスと一時パスワードを指定して、ハードウェアにリストアを開始します。次に、ドライブをマップし、リストアを開始する必要があります。

この処理は、[Linux マシンでの Bare Metal Restore の実行](#)の手順です。

Rapid Recovery Core Console から BMR を起動するには、次のタスクを実行します。

- ・ [リカバリポイントの選択と BMR の開始](#)
- ・ [Bare Metal Restore のボリュームをマップについて](#)

local_mount ユーティリティを使用してコマンドラインからリストアする場合は、適切な権限の設定、ボリュームのマウント、local_mount の実行、マシンのリストから Core に関する情報の取得、Core への接続、リカバリポイントのリストの取得、ベアメタルにロールバックするリカバリポイントの選択、リストアの起動をまず行う必要があります。

必要に応じて、Screen ユーティリティを開始できます。

コマンドラインから BMR を起動するには、次のタスクを実行します。

- ・ [Screen ユーティリティの開始](#)
- ・ [コマンドラインを使用して Linux マシンに対して Bare Metal Restore を起動する](#)

Screen ユーティリティの開始

Live DVD には、Live DVD から Universal Recovery Console に起動する場合に使用できる Screen ユーティリティが含まれています。Screen ユーティリティを使用すると、1つの Secure Shell (SSH) セッションまたは Console ウィンドウから複数のシェルをユーザーが同時に管理できます。これにより、1つのタスク（マウント済みボリュームの確認など）をターミナルウィンドウで実行し、そのタスクの実行中に、別のシェルインスタンスを開くか切り替えて、別のタスク（local_mount ユーティリティの実行など）を実行できます。

Screen ユーティリティには独自のスクロールバックバッファもあり、画面をスクロールして、大量のデータ（リカバリポイントのリストなど）を表示することができます。

① | メモ: Screen ユーティリティはより便利に使っていただけるようにするためのものであり、必要に応じて使用してください。

Screen ユーティリティは、デフォルトでは、Live DVD で起動されたマシンで開始されます。ただし、このアプリケーションを終了した場合、次の手順に従って Live DVD から Screen ユーティリティを起動する必要があります。

マシンが Live DVD から起動された場合は、ターミナルウィンドウで、screen と入力して、**Enter** を押します。

Screen ユーティリティが起動します。

コマンドラインを使用して Linux マシンに対して Bare Metal Restore を起動する

BMR を実行するマシンで Live DVD の ISO イメージにアクセスでき、ターゲットマシンとベアメタルにリストアするリカバリポイント間でボリュームの数とサイズが一致したら、local_mount ユーティリティを使用してコマンドラインからリストアを開始できます。

① | メモ: このコンポーネントは以前、**aamount** と呼ばれていました。

Rapid Recovery Core Console UI を使用して BMR を実行する場合は、「[リカバリポイントの選択と BMR の開始](#)」を参照してください。

① | メモ: この手順を実行する場合、**rapidrecovery-vdisk**（以前の **aavdisk**）ファイルがある **/tmp** フォルダにリカバリポイントをマウントしないでください。

このタスクは、Linux マシンでの Bare Metal Restore の実行の手順です。これは、コマンドラインを使用して Linux マシンに対して Bare Metal Restore を起動するの処理の一部です。

Core でリカバリポイントを選択し、物理/仮想 BMR ターゲットマシンにロールバックするには、次の手順を実行します。

- 1
- Rapid Recovery local_mount ユーティリティをルートとして実行するには、次のコマンドを入力して **Enter** を押します。

sudo local_mount
- 2
- 保護対象マシンを表示するには、次のコマンドを入力して **Enter** を押します。

lm
- 3
- プロンプトが表示されたら、次の表の説明に従って、Rapid Recovery Core の接続情報を入力し、それぞれの必須コマンドの後で Enter を押します。

表 159. Rapid Recovery Core の接続情報

テキストボックス	説明	必須
Rapid Recovery Core の IP アドレスまたはホスト名	Rapid Recovery Core の IP アドレスまたはホスト名です。	はい
ドメイン	Rapid Recovery Core のドメインです。これは任意です。	いいえ
ユーザー	Core の管理ユーザーのユーザー名です。	はい
パスワード	管理ユーザーを Core に接続するために使用されるパスワードです。	はい

この Rapid Recovery Core で保護されているマシンがリストに表示されます。行アイテム番号、ホストの表示名または IP アドレス、マシンの ID 番号別に、検出されたマシンが表示されます。

- 4
- リストアするマシンのリカバリポイントを表示するには、次の構文を使用してリカバリポイントのリストコマンドを入力し、<Enter> を押します。

lr <machine_line_item_number>

メモ: このコマンドには、行アイテム番号の代わりにマシンの ID 番号を入力することもできます。

そのマシンのベースリカバリポイントと増分リカバリポイントのリストが表示されます。リストには次の内容が含まれます。

- ・ 行アイテム番号
- ・ 日付とタイムスタンプ
- ・ リカバリポイント内のボリューム文字リスト
- ・ ボリュームの場所
- ・ リカバリポイントのサイズ
- ・ リカバリポイントを示すシーケンス番号が最後に付けられた、ボリュームの ID 番号

- 5
- リストアするリカバリポイントを選択するには、次のコマンドを入力して <Enter> を押します。

r <recovery_point_ID_number> <path>

注意: システムボリュームがマウントされていないことを確認する必要があります。

メモ: マシンを Live DVD から起動した場合、システムボリュームはマウントされません。

このコマンドは、ID で指定されたボリュームイメージを、Core から指定のパスにロールバックします。リストアのパスは、デバイスファイル記述子のパスであり、マウント先のディレクトリではありません。

- ① **メモ:** リカバリポイントの ID 番号の代わりに行番号をコマンドで指定して、リカバリポイントを特定することもできます。その場合は、(lm 出力の) エージェント / マシンの番号を使用し、その後にリカバリポイントの行番号とボリューム文字を指定し (リカバリポイント内のボリューム文字リストから)、さらにその後にパスを指定します。例:

```
r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>
```

たとえば、次のように入力します。

```
r 1 24 a /dev/sda1
```

このコマンドの <path> は、実際のボリュームのファイル記述子です。

- 6 続行を指示するプロンプトが表示されたら、「はい」の場合は「y」と入力して **Enter** を押します。
リストアが開始すると、リストアの完了ステータスを示す一連のメッセージが表示されます。

- ① **メモ:** 例外メッセージが表示された場合、その例外に関する詳細は `local_mount.log` ファイルで確認できます。
`local_mount.log` ファイルは `/var/log/apprecovery` にあります。

- 7 リストアが正常に行われたら、「exit」と入力し、**Enter** を押して、`local_mount` を終了します。
8 次に、リストアを確認します。詳細については、「[コマンドラインからの Bare Metal Restore の確認](#)」を参照してください。

コマンドラインを使用した Linux マシンのボリュームのリストア

Rapid Recovery では、コマンドラインの `local_mount` ユーティリティを使用して、保護対象 Linux マシン上のボリュームをリストアできます。

- ① **メモ:** 以前は、このプロセスはロールバックと呼ばれていました。この手順を実行する場合、`rapidrecovery-vdisk` (以前の `aavdisk`) ファイルがある `/tmp` フォルダにリカバリポイントをマウントしないでください。**Rapid Recovery Core Console** 内の保護対象マシンのボリュームもリストアできます。詳細については、「[リカバリポイントからのボリュームの復元](#)」を参照してください。

- △ **注意:** システムまたはルート (/) パーティションまたはオペレーティングシステム全体をリストアする方法については、「[Linux マシンでの Bare Metal Restore の実行](#)」を参照してください。

- 1 次のように、ルートとして `Rapid Recoverylocal_mount` ユーティリティを実行します。

```
sudo local_mount
```

- 2 Rapid Recovery のマウントプロンプトで、次のコマンドを入力して保護対象マシンのリストを表示します。

```
lm
```

- 3 プロンプトが表示されたら、Rapid Recovery Core サーバの IP アドレスまたはホスト名を入力します。

- 4 このサーバのログオン資格情報 (ユーザー名とパスワード) を入力します。

この Rapid Recovery サーバで保護されているマシンがリストに表示されます。行アイテム番号、ホスト/IP アドレス、およびマシンの ID 番号 (例: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2) で検出された保護対象マシンがリストされます。

- 5 次のコマンドを入力して、指定したマシンで現在マウントされているリカバリポイントをリストします。

```
lr <machine_line_item_number>
```

- ① **メモ:** このコマンドには、行アイテム番号の代わりにマシンの ID 番号を入力することもできます。

そのマシンのベースリカバリポイントと増分リカバリポイントがリストに表示されます。このリストには、行アイテム番号、日付/タイムスタンプ、ボリュームの場所、リカバリポイントのサイズ、リカバリポイントを示すシーケンス番号が最後に付けられたボリュームの ID 番号 (例: 「293cc667-44b4-48ab-91d8-44bc74252a4f:2」) が表示されます。

- 6 次のコマンドを入力して、リストアするリカバリポイントを選択します。

```
r <volume_recovery_point_ID_number> <device path>
```

このコマンドは、ID で指定されたボリュームイメージを、Core から指定のパスにリストアします。リストアのパスは、デバイスファイル記述子のパスであり、マウント先のディレクトリではありません。

- ・ リカバリポイントの ID 番号の代わりに行番号をコマンドで指定して、リカバリポイントを特定することもできます。その場合は、(lm 出力の) 保護対象マシンの行番号を使用し、その後にリカバリポイントの行番号とボリューム文字を指定し、さらにその後にパスを指定します（例：r <machine_line_item_number> <recovery_point_line_number> <volume_letter> <path>）。このコマンドの <path> は、実際のボリュームのファイル記述子です。

たとえば、lm 出力で3つの保護対象マシンがリストアされて、保護対象マシン番号 1r に対して 2 コマンドを入力し、リカバリポイント 23 のボリューム b を /dev/sda5、ディレクトリにマウントされたボリュームにリストアする場合、コマンドは次のようになります。

```
r2 23 b /dev/sda5
```

- ① **メモ:** 必要に応じて / にリストアすることができます。Live DVD を使用して、Bare Metal Restore を実行する場合は、異なるマシンにリストアすると見なされます。詳細については、「Linux 用の Bare Metal Restore の開始」を参照してください。

- 7 続行を求めるプロンプトが表示されたら、Yes を示す「y」を入力します。
リストアが続行されると、ステータスを通知する一連のメッセージが表示されます。
- 8 ターゲットが以前に保護およびマウントされていた場合、リストアに成功すると、local_mount ユーティリティによって、リストアされたボリュームにカーネルモジュールが自動的にマウントされて再アタッチされます。保護およびマウントされていなかった場合、リストアされたボリュームをローカルディスクにマウントして、ファイルがリストアされていることを確認する必要があります（たとえば、sudo mount コマンドを使用してから、ls コマンドを使用できます）。

Bare Metal Restore の確認。

Bare Metal Restore (BMR) を実行したら、リストアの進捗状況を確認できます。操作が正常に完了したら、リストアしたサーバーを起動できます。Universal Recovery Console への接続で問題が発生してリストアを完了できない場合や、リストアしたマシンの起動時の問題を修復する必要がある場合のため、いくつかのトラブルシューティング手順があります。

次のタスクを実行できます。

関連するリンク

- [リカバリの進捗状況の表示](#)
- [リストアされたターゲットサーバの起動](#)
- [Universal Recovery Console への接続に関するトラブルシューティング](#)
- [起動の問題の修復](#)

リカバリの進捗状況の表示

Rapid Recovery Core Console で開始した、リカバリポイントからのデータのリストア（Bare Metal Restore を含む）の進捗状況を表示するには、次の手順を実行します。

- 1 リカバリポイントからのデータのリストアプロセスを開始したら、タスクの処理中に、Core Console の 実行中のタスク ドロップダウンメニューから進捗状況を表示できます。
- 2 必要に応じて、詳細情報を イベント ページに表示することもできます。Rapid Recovery イベントの監視の詳細については、「[タスク、アラート、およびイベントの表示](#)」を参照してください。

リストアされたターゲットサーバの起動

リストアされたターゲットサーバーを起動するには、次の手順を実行します。

- ① **メモ:** リストアされたターゲットサーバーを起動する前に、リカバリが正常に行われたことを確認する必要があります。詳細については、[リカバリの進捗状況の表示](#)を参照してください。

このタスクは、[Windows マシンのベアメタルリストアの実行](#)の手順です。これは、[Bare Metal Restore の確認](#)の処理の一部です。

- 1 ターゲットサーバで Rapid Recovery Universal Recovery Console がアクティブであることを確認します。
- 2 リストアされたサーバからブート CD を取り出するか、ブート CD イメージを含む物理メディアを切断します。
- 3 Universal Recovery Console で、画面の一番上にある電源メニューアイコンをクリックし、**再起動**をクリックします。
- 4 オペレーティングシステムの通常起動を指定します。
- 5 マシンにログオンします。システムは、リカバリポイントで取得された状態にリストアされます。

Universal Recovery Console への接続に関するトラブルシューティング

ブート CD イメージへの接続に関する次のトラブルシューティング手順は、[リカバリポイントの選択と BMR の開始](#)のプロセスの一部です。

Core からリモートサーバに接続できないことを示すエラーが表示された場合、いくつかの原因が考えられます。

- ・ URC に表示される IP アドレスと現在のパスワードが、リカバリ Console インスタンス ダイアログボックスで入力した情報と同じであることを確認します。
- ・ データをリストアするサーバに到達するには、ネットワーク上のサーバを Core で識別する必要があります。サーバ識別が可能であるかどうかを判断するには、Core でコマンドプロンプトを開き、ターゲット BMR サーバの IP アドレスを ping します。ターゲットサーバでコマンドプロンプトを開き、Rapid Recovery Core の IP アドレスを ping してもかまいません。
- ・ Core とターゲット BMR サーバ間で、ネットワークアダプタ設定に互換性があることを確認します。

起動の問題の修復

この手順には次のタスクの前提条件があります。

- ・ [ブート CD の ISO イメージの作成](#)
- ・ [ブート CD のロードおよびターゲットマシンの起動](#)
- ・ [Universal Recovery Console を使用したドライバのロード](#)

起動時の問題を修復するには、次の手順を実行します。異種のハードウェアにリストアした場合は、ストレージコントローラ、RAID、AHCI、チップセット、および他のドライバがブート CD にすでに存在していなければ、導入しておく必要があります。これらのドライバを使用すると、ターゲットサーバ上のすべてのデバイスをオペレーティングシステムで正常に操作できるようになります。詳細については、「[Universal Recovery Console を使用したドライバのロード](#)」を参照してください。ターゲットサーバで起動時の問題を修復するには、次の手順を実行します。

- 1 Universal Recovery Console で、**既存の Windows ドライバマネージャ** タブをクリックします。
- 2 **起動の問題の修復** をクリックします。
ターゲットサーバのブートレコードで、起動パラメータが自動的に修復されます。

コマンドラインからの Bare Metal Restore の確認

Dell では、次の手順を実行して、コマンドラインから完了した Bare Metal Restore を確認することをお勧めします。

このタスクは、[Linux マシンでの Bare Metal Restore の実行](#)の手順です。

関連するリンク

[復元されたボリュームでのファイルシステムチェックの実行](#)

[コマンドラインを使用して、復元された Linux マシンをブート可能にする方法](#)

復元されたボリュームでのファイルシステムチェックの実行

コマンドラインから Bare Metal Restore を実行したら、リストア済みのボリュームでファイルシステムチェックを実行して、リカバリポイントからリストアされたデータが破損していないことを確認する必要があります。

このタスクは、[Linux マシンでの Bare Metal Restore の実行](#)の手順です。これは、[コマンドラインからの Bare Metal Restore の確認](#)の処理の一部です。

リストア済みのボリュームでファイルシステムチェックを実行するには、次のタスクを実行します。

- 1 リストアした Linux マシンの Universal Recovery Console のコマンドラインから、適切なパーティションがマウントされているかどうかを確認するには、次のコマンドを入力して **<Enter>** を押します。

```
df
```

- 2 リストア済みのボリュームがマウントされていない場合は、[ステップ 3](#) にスキップします。リストア済みのボリュームがマウントされている場合は、次のコマンドを入力し、**<Enter>** を押して、マウント解除します。

```
umount <mount point>
```

- 3 次のコマンドを入力し、**<Enter>** を押して、リストア済みのボリュームでファイルシステムチェックを実行します。

```
fsck -f <volume>
```

fsck からクリーンと返された場合は、ファイルシステムが検証されたことを示します。

- 4 mount <volume> <folder> の形式で次のコマンドを入力し、**Enter** を押して、適切なボリュームをもう一度マウントします。

たとえば、ボリュームのパスが prod/sda1 であり、マウントするフォルダが mnt の場合は、次のコマンドを入力して **<Enter>** を押します。

```
mount /dev/sda1 /mnt
```

コマンドラインを使用して、復元された Linux マシンをブート可能にする方法

リストア済みボリュームでクリーンなファイルシステムチェックが完了したら、ブート可能なパーティションを作成する必要があります。

GNU Grand Unified Bootloader (GRUB) は、システムの起動時に使用するオペレーティングシステムや特定のカーネル構成を管理者が設定できるブートローダです。BMR の後、GRUB の設定ファイルを変更して、マシンでルートボリュームに適切なユニバーサル一意識別子 (UUID) が使用されるようにする必要があります。この操作を行う前に、ルートボリュームとブートボリュームをマウントし、それぞれの UUID をチェックする必要があります。これにより、パーティションから確実に起動できるようになります。

① メモ: この手順は、**GRUB1** または **GRUB2** を使用する **Linux マシン** に適用されます。この手順を実行する際には、ブートパーティションが正常でなおかつ保護されていることを確認する必要があります。

GRUB または GRUB2 は、通常、Linux オペレーティングシステムと一緒にインストールされます。お使いの Linux ディストリビューションに付属しているバージョンを使用してこの手順を実行できます。GRUB のバージョンがインストールされていない場合、お使いの Linux ディストリビューションに適したデフォルトのバージョンを再インストールする必要があります。

△ 注意: **BMR** の実行後初めて復元された **Linux マシン** を起動する際に、**Rapid Recovery** が復元されたマシンのベースイメージを取得します。このプロセスの所要時間は、マシン上のデータ量によっては、増分スナップショットを取得する場合よりも長くなることがあります。ベースイメージと増分スナップショットの詳細については、[保護スケジュールについて](#)を参照してください。

このタスクは、[Linux マシンでの Bare Metal Restore の実行](#)の手順です。これは、[コマンドラインからの Bare Metal Restore の確認](#)の処理の一部です。

コマンドラインを使用してブート可能なパーティションを作成するには、次のタスクを実行します。

- 1 まず、ルートボリュームをマウントしてから、ブートボリュームをマウントする必要があります。次のコマンドを使用して、リストア済みの各ボリュームをマウントします。

- a ルートボリュームをマウントするには、次のコマンドを入力して **<Enter>** を押します。

```
mount /<restored volume[root]> /mnt
```

たとえば、/dev/sda2 がルートボリュームの場合は、mount /dev/sda2 /mnt と入力して **Enter** を押します。

- b ブートボリュームをマウントするには、次のコマンドを入力して **<Enter>** を押します。

```
mount /<restored volume[boot]> /mnt/boot
```

たとえば、/dev/sda1 がブートボリュームの場合は、mount /dev/sda1 /mnt/boot と入力して **Enter** を押します。

① **メモ:** 一部のシステム構成では、ブートディレクトリがルートボリュームの一部として含まれている場合があります。

- 2 ボリュームサイズが増えている場合（つまり、新しい Linux マシンの宛先ボリュームがリカバリポイントのボリュームより大きい場合）は、既存のビットマップデータファイルを削除する必要があります。

- 3 blkid コマンドを使用して、新しいボリュームのユニバーサル一意識別子（UUID）を取得します。次のコマンドを入力して **<Enter>** を押します。

```
blkid [volume]
```

① **メモ:** また、**ls -l /dev/disk/by-uuid** コマンドも使用できます。

- 4 宛先マシンの新しいディスクで BMR を実行する場合は、ルートボリュームの fstab でスワップパーティションをコメント化します。

- 5 fstab および mtab パスの変更は、Live DVD ではなくリストア済みのボリュームで行います。Live DVD では、パスを変更する必要はありません。次のコマンドを入力して、Grand Unified Bootloader（GRUB）をインストールする準備をします。各コマンドの後で **<Enter>** を押します。

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

```
mount --bind /sys /mnt/sys
```

- 6 次のコマンドを入力し、**<Enter>** を押して、ルートディレクトリを変更します。

```
chroot /mnt /bin/bash
```

- 7 次のコマンドを入力し、**Enter** を押して、マウント済みのリカバリポイント /etc/fstab ファイルでパーティションの古い UUID を確認し、root（Ubuntu または CentOS の場合）、boot（CentOS または RHEL の場合）、またはデータパーティションの UUID と比較します。

```
less /mnt/etc/fstab
```

- 8 次のコマンドを入力し、**Enter** を押して、マウント済みのリカバリポイント /etc/mtab ファイルでパーティションの古い UUID を確認し、root（Ubuntu または CentOS の場合）、boot（CentOS または RHEL の場合）、およびデータパーティションの UUID と比較します。

```
less /mnt/etc/mtab
```

- 9 SLES 11 を使用する場合は、次のコマンドを入力して各コマンドの後に Enter を押し、GRUB をインストールします。

```
grub-install --recheck /dev/sda
```

```
grub-install /dev/sda
```

- 10 Ubuntu、CentOS 6.x、RHEL 6.x、または Oracle Linux 6.x を使用している場合は、次のコマンドを入力し、Enter を押して GRUB をインストールします。

```
grub-install /dev/sda
```

- 11 SLES 12、CentOS 7、RHEL 7、または Oracle 7 を使用している場合は、次のコマンドを入力し、Enter を押して GRUB2 をインストールをします。

```
grub2-install /dev/sda
```

- 12 インストールの完了後、次のいずれかのアップデートを実行します。

・ SLES の場合：

```
grub-install.unsupported --recheck /dev/sda
```

```
grub-install.unsupported /dev/sda
```

```
update-grub
```

① **メモ:** お使いの Linux ディストリビューションに **update-grub** コマンドが存在しない場合は、このオプションを省略します。

- ・ その他のディストリビューションの場合：

```
grub-install /dev/sda  
update-grub
```

① | **メモ:** お使いの **Linux** ディストリビューションに **update-grub** コマンドが存在しない場合は、このオプションを省略します。

- 13 CD-ROM または DVD ドライブから Live DVD ディスクを削除し、Linux マシンを再起動します。

レポートの生成と表示

この項では、Rapid Recovery Core と Rapid Recovery Central Management Console で使用可能なレポートの概要について説明します。

トピック：

- [Rapid Recovery レポートについて](#)
- [Central Management Console](#)

Rapid Recovery レポートについて

Rapid Recovery Core Console からレポートを生成することができます。これらの一部のレポートは Central Management Console から也可以使用できます。

次の表で使用可能なレポートについて説明しています。

表 160. Rapid Recovery レポート

レポートタイプ	説明
ジョブレポート	エラーが検出されたジョブ、成功したジョブ、失敗したジョブのステータスについてレポートを提供します。失敗したジョブの場合、失敗レポートで詳細を表示することができます。 ジョブタイプには、Core Console からの実行と、Central Management Console からの実行があります。 - Core から実行すると、このレポートは1つまたは複数の Core の詳細を指定できます。デフォルトでは、この情報のセットには、指定された Core のすべてのマシン（保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシン）のジョブが含まれます。レポートパラメーターで、レポートをカスタマイズできます。フィルタを使用して一部のマシンを選択または除外します。マシンから独立してジョブを選択または除外することもでき、その場合、レポートには、Core ジョブのみのステータスが表示されます。 - 保護対象のマシンの視点から Core Console から実行した場合は、生成されたレポートには保護対象のマシンのみのジョブのステータスが表示されます。 - Central Management Console から実行したときには、このレポートでは、コンソールで設定された Core グループの Core の任意の組み合わせの詳細を指定できます。設定可能なパラメーターは、レポートタイプと日付範囲のみです。 このレポートタイプの詳細については、「ジョブレポートについて」を参照してください。
失敗レポート	指定された条件の失敗した Core ジョブについての情報を提供します。 ジョブタイプには、Core Console からの実行と Central Management Console からの実行があります。 - Core から実行すると、このレポートでは保護対象マシンの詳細を追加または除外できます。ジョブレポートと同様に、このレポートを Core で選択した保護対象マシンからのみ実行することもできます。生成されるレポートには、選択された保護対象マシンのみの失敗したジョブについての詳細が表示されます。 - Central Management Console から実行したときには、このレポートでは、コンソールで設定された Core グループの Core の任意の組み合わせの失敗イベントを指定できます。設定可能なパラメータは、レポートタイプと日付範囲のみです。 このレポートタイプの詳細については、「失敗レポートについて」を参照してください。

レポートタイプ 説明

サマリレポート サマリ情報を提供します。デフォルトでは、この情報のセットには、指定された Core のすべてのマシン（保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシン）のジョブが含まれます。レポートパラメーターで、レポートをカスタマイズできます。フィルタを使用して一部のマシンを選択または除外します。マシンから独立してジョブを選択または除外することもでき、その場合、レポートには、Core ジョブのみのステータスが表示されます。

このレポートは、単一の保護対象マシンの観点からは使用できません。

ジョブタイプには、Core Console からの実行と Central Management Console からの実行があります。

- Core Console から実行すると、レポートの情報のカテゴリには、Core、ライセンス、リポジトリが含まれます。情報は、リスト、グラフ、表の形式で表示されます。
- Central Management Console から実行したときには、このレポートでは、コンソールで設定された Core グループの Core の任意の組み合わせのサマリ情報を指定できます。設定可能なパラメーターは、レポートタイプと日付範囲のみです。

このレポートの情報のカテゴリには、Core、ライセンス、リポジトリが含まれます。サマリレポートには、保護対象マシンのレポートとすべてのジョブに対する成功したジョブの比率も含まれています。情報は、リスト、グラフ、表の形式で表示されます。

このレポートタイプの詳細については、[サマリレポートについて](#)を参照してください

リポジトリレポート このレポートタイプには、選択した Core 上のすべてのリポジトリのレポートが用意されています。Core で利用できる任意の単一のリポジトリを選択することもできます。このレポートは、Core Console からのみ使用可能で、Core の視点からのみ使用できます。

このレポートタイプの詳細については、[リポジトリレポートについて](#)を参照してください

スケジュール設定されたレポート Core Console からこれらのレポートのいずれかをスケジュール設定することもできます。レポートをスケジュールすると、定義したスケジュールでレポートが繰り返し生成されます。
必要に応じて、レポートが生成されるたびに電子メール通知を指定できます。レポートのスケジュール設定、変更、一時停止、または削除の詳細については、「[Core Console からスケジュールされたレポートの管理](#)」を参照してください。

選択したレポートタイプとパラメーターに基づいて、1つまたは複数の Rapid Recovery Core または保護対象マシンのレポートを生成できます。

Central Management Console から実行したときには、そのコンソールで設定されている Core または Core グループの任意の組み合わせのレポートを生成できます。

Core Console からのレポートの生成

Core Console からオンデマンドでレポートを生成できます。次のルールが適用されます。

- すべてのレポートは、Core の視点から生成できます。
- また、保護対象マシンの視点から2つのジョブ・タイプ（ジョブレポートと失敗レポート）を生成できます。レポートには、選択されたマシンに関連するデータのみが生成されます。
- 失敗レポートには、選択した Core（または保護対象マシン）上のジョブが失敗した場合のみデータが含まれます。

オンデマンドでのレポートの生成方法も似ています。同様にコアの視点からレポートが生成されるか、保護対象マシンの視点から生成されます。ただし、ナビゲーションは少し異なります。

レポートをスケジュールして、繰り返し生成することもできます。レポートのスケジュール設定、変更、一時停止、または削除の詳細については、「[Core Console からスケジュールされたレポートの管理](#)」を参照してください。

オンデマンドでの Core レポートの生成

Rapid Recovery レポートについてのトピックで説明されているように、Core Console から使用可能なすべての範囲のレポートを生成できます。

Rapid Recovery Core の視点からレポートを生成するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (より多い) をクリックして、**レポート** を選択します。
ジョブレポート ページが表示されます。ページタイトルのレポート名の右側に、下方向矢印が表示され、別のレポートタイプを選択できます。

ジョブレポートを生成する場合は、[手順 6](#) に進み、レポート条件の指定を開始します。

- 3 別のレポートタイプを選択するには、レポート名の右にある矢印をクリックして使用可能なレポートのメニューを表示します。
- 4 スケジュール設定されたレポートの定義については、「[レポートのスケジュール設定](#)」を参照してください。
- 5 リポジトリレポートのみを生成する場合は、[手順 11](#) に進んでください。
- 6 ジョブレポート、ジョブサマリレポート、失敗レポート、またはサマリレポートでは、**日付範囲** ドロップダウンメニューから日付範囲を選択します。

日付範囲を選択しない場合は、デフォルトのオプション (最後の 31 日間) が使用されます。次の表のオプションから選択することができます。

オプション	説明
24 時間以内	レポートを生成する時刻を基準とした相対的な最終日のアクティビティをレポートします。
過去 7 日間	レポートを生成する時刻を基準とした相対的な前週のアクティビティをレポートします。
過去 31 日間	レポートを生成する時刻を基準とした相対的な過去 31 日間のアクティビティをレポートします。
過去 90 日間	レポートを生成する時刻を基準とした相対的な過去 90 日間のアクティビティをレポートします。
過去 365 日間	レポートを生成する時刻を基準とした相対的な前年のアクティビティをレポートします。
常時	この期間は、Core の耐用期間全体を対象とします。
カスタム	この期では、さらに開始日と終了日を指定する必要があります。
月累計	現在のカレンダー月の最初の日からレポートを生成する日までのアクティビティをレポートします。
年累計	現在のカレンダー年の最初の日からレポートを生成する日までのアクティビティをレポートします。

① メモ: どの場合でも、Core ソフトウェアが展開される前、または Core 上でマシンが保護される前のレポートデータは使用できません。

- 7 ジョブレポートまたはエラーレポートの場合は、**ターゲット Core:** ドロップダウンメニューからレポートを生成する対象の 1 つまたは複数の適切な Core を選択します。
デフォルトの選択にはすべての使用可能な Core が含まれます。
- 8 **保護対象マシン** ドロップダウンメニューから、レポートを生成する対象の 1 つまたは複数のマシンを選択します。
デフォルトでは、この情報のセットには、指定された Core のすべてのマシン (保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシン) のジョブが含まれます。レポートパラメーターで、レポートをカスタマイズできます。フィルタを使用して一部のマシンを選択または除外します。マシンから独立してジョブを選択または除外することもでき、その場合、レポートには、Core ジョブのみのステータスが表示されます。

次から選択できます。

オプション	説明
Select all	このオプションは、この Core で保護されているすべての保護対象マシンを選択します。

① メモ: すべてのマシンを選択した後で、一部の選択をクリアしてすべてのマシンのサブセット指定することができます。

オプション 説明

孤立マシン このオプションを選択すると、Core の視点からのジョブが含まれるレポートが生成されます。リポジトリの作成または削除、ブート CD の作成などのジョブタイプ、は、特定のマシンに関連付けられません。まだ保護されていないマシンに Agent ソフトウェアを展開する場合、このジョブタイプは孤立マシンと見なされます。これらのジョブは、結果のレポートの保護対象マシン列に保護対象マシンをリストしません。
対照的に、Core で既に保護されているマシンへの Agent ソフトウェアを展開する場合は、保護対象マシン名がレポートに含まれます。孤立マシンとは見なされません。

保護対象マシン このオプションは、この Core で保護されている保護対象マシンをリストします。それらをすべて選択すること、保護対象マシンのサブセットを選択することもできます。

リカバリポイントのみ このオプションは、以前に保護されていて、リカバリポイントが依然としてリポジトリに保存されているマシンをリストします。

[ソース Core] Core がターゲット Core で、ソース Core で保護されているいずれかのマシンのリカバリポイントをレプリケートする場合、そのソース Core の名前（すべて大文字）が表示されます。このオプションは、そのソース Core で保護されているすべてのマシンをリストします。このターゲット Core でレプリケートされたすべてのマシンを選択することもそれらのサブセットを選択することもできます。

[カスタムグループ] この Core 上でカスタムグループを作成した場合、各カスタムグループの名前がオプションとして表示されます。そのカスタムグループ内の各オブジェクトが表示されます。グループ内のすべてのオブジェクトまたはそれらのサブセットを選択することができます。

9 サマリレポートを生成する場合は、[手順 12](#) に進んでください。

10 ジョブレポート、ジョブサマリレポート、または失敗レポートでは、**ジョブタイプ** ドロップダウンメニューから適切なジョブタイプを選択します。

デフォルトでは、このセットの情報には、選択された保護されたマシンのすべてのジョブが含まれます。レポートパラメーターで、レポートをカスタマイズできます。フィルタを使用して、メインジョブカテゴリ内のすべてのジョブ、およびその他のジョブカテゴリ内のすべてのジョブを選択または除外します。ジョブパラメーターを定義するときにこれらの各カテゴリを展開し、いずれかのカテゴリからレポートに表示したいジョブタイプのみを選択できます。任意のジョブタイプのチェックボックスをクリックして選択するか、そのタイプをクリアします。いずれかのカテゴリから一部またはすべてのジョブを選択することができます。

次 **その他の** ジョブタイプから選択できます。

11 リポジトリレポートの場合は、リポジトリメニューからレポートに含める 1 つまたは複数のリポジトリを選択します。

デフォルトの選択にはすべての使用可能なリポジトリが含まれます。

12 **プレビュー** をクリックし、指定した条件を使用してレポートを生成します。

選択したレポート条件が見つからなかった場合は、レポートは生成されますが、空の行がレポートに含まれます。たとえば、エラーがなければ、レポートのエラーの列は NULL です。

13 次の手順のいずれかを実行します。

- 生成されたレポートをオンラインで表示します。
- 条件を変更し、**プレビュー** をもう一度クリックしてレポートを動的に更新します。
- レポートメニュー** を使用して、エクスポート形式（デフォルトの形式の PDF を含む）を選択し、 をクリックしてレポートをエクスポートします。レポートメニューの詳細については、「[レポートメニューの使用](#)」を参照してください。
- レポートツールバー** を使用して、レポートを表示、操作、または印刷します。レポートツールバーの詳細については、「[レポートのツールバーの使用](#)」を参照してください。

オンデマンドでの保護対象マシンのレポートの生成

任意の保護対象マシンのジョブレポートまたは失敗レポートを生成できます。

保護対象マシンのレポートを生成するには、次の手順を実行します。

- Rapid Recovery Core Console に移動します。
- 保護対象マシンメニューから、レポートを表示する対象となっている保護対象マシンをクリックします。
選択した保護対象マシンの サマリ ページが表示されます。
- ページの一番上にある、保護対象マシン名の横にあるメニューオプションから、レポートの横にある下向き矢印キーをクリックし、レポートタイプを選択します。

- ・ この保護対象マシンに関連する失敗したジョブを含むすべてのジョブでレポートを生成する場合は、**ジョブレポート** をクリックし、レポート条件を指定します。
- ・ この保護対象マシンに関連する失敗したジョブのリストのみを生成する場合は、**失敗レポート** をクリックし、レポート条件を指定します。

- 4 **ジョブレポート**または**エラーレポート**では、**日付範囲** ドロップダウンメニューから日付範囲を選択します。
日付範囲を選択しない場合は、デフォルトのオプション（最後の 31 日間）が使用されます。次の表のオプションから選択することができます。

オプション	説明
24 時間以内	レポートを生成する時刻を基準とした相対的な最終日のアクティビティをレポートします。
過去 7 日間	レポートを生成する時刻を基準とした相対的な前週のアクティビティをレポートします。
過去 31 日間	レポートを生成する時刻を基準とした相対的な過去 31 日間のアクティビティをレポートします。
過去 90 日間	レポートを生成する時刻を基準とした相対的な過去 90 日間のアクティビティをレポートします。
過去 365 日間	レポートを生成する時刻を基準とした相対的な前年のアクティビティをレポートします。
常時	この期間は、Core の耐用期間全体を対象とします。
カスタム	この期では、さらに開始日と終了日を指定する必要があります。
月累計	現在のカレンダー月の最初の日からレポートを生成する日までのアクティビティをレポートします。
年累計	現在のカレンダー年の最初の日からレポートを生成する日までのアクティビティをレポートします。

① **メモ:** どの場合でも、**Core** ソフトウェアが展開される前、または **Core** 上でマシンが保護される前のレポートデータは使用できません。

- 5 **ジョブタイプ** ドロップダウンメニューから適切なジョブタイプを選択します。
デフォルトでは、このセットの情報には、選択された保護されたマシンのすべてのジョブが含まれます。レポートパラメーターで、レポートをカスタマイズできます。フィルタを使用して、メインジョブカテゴリ内のすべてのジョブ、およびその他のジョブカテゴリ内のすべてのジョブを選択または除外します。ジョブパラメーターを定義するときにこれらの各カテゴリを展開し、いずれかのカテゴリからレポートに表示するジョブタイプのみを選択できます。任意のジョブタイプのチェックボックスをクリックして選択するか、そのタイプをクリアします。いずれかのカテゴリから一部またはすべてのジョブを選択することができます。
- 6 **プレビュー** をクリックして、指定した条件を使用してレポートを生成します。
選択したレポート条件が見つからなかった場合は、レポートは生成されますが、空の行がレポートに含まれます。たとえば、エラーがなければ、レポートのエラーの列は NULL になります。
- 7 次の手順のいずれかを実行します。
- ・ 生成されたレポートをオンラインで表示します。
 - ・ 条件を変更し、**プレビュー** をもう一度クリックしてレポートを動的に更新します。
 - ・ **レポートメニュー** を使用して、エクスポート形式を選択し、レポートをエクスポートします。レポートメニューの詳細については、[レポートメニューの使用](#) を参照してください。
 - ・ **レポートツールバー** を使用して、レポートを表示、操作、または印刷します。レポートツールバーの詳細については、「[レポートのツールバーの使用](#)」を参照してください。

Core Console からスケジュールされたレポートの管理

Core Console から使用可能なレポートのいずれかをスケジュール設定することができます。レポートをスケジュールすると、今後レポートが繰り返し生成されます。スケジュールは、日次、週次、または月次でレポートを生成するかどうかを定義します。

必要に応じて、Rapid Recovery でレポートが生成されたときに 1 人または複数の受信者に電子メール通知を送信することができます。電子メールは、レポートタイプ、レポート形式、日付範囲を指定し、添付ファイルとしてレポートを追加できます。

① **メモ:** 電子メールでレポートを送信する前に、**Core** の SMTP サーバを構成する必要があります。詳細については、「[電子メールサーバーの設定](#)」を参照してください。

電子メール通知を送信するように選択しているかどうかにかかわらず、生成されたレポートをローカル、またはネットワーク上のコアサーバからアクセスできる場所に保存することができます。

E メール通知と配信を指定するかレポートを保存する場所を指定する必要があります。両方のオプションを選択することもできます。

本項は、次のトピックで構成されています。

関連するリンク

- レポートのスケジュール設定
- レポートスケジュールの変更
- スケジュールされたレポートの一時停止、再開、または削除

レポートのスケジュール設定

Core Console から使用可能なレポートをスケジュールすることができます。レポートが、レポートを一時停止または削除するまで、定義されたスケジュールにレポートが生成されます。

E メール通知と配信を指定するかレポートを保存する場所を指定する必要があります。両方のオプションを選択することもできます。

レポートをスケジュールするには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで、 (より多い) をクリックして、**レポート** を選択します。
ジョブレポート ページが表示されます。下方向矢印が現在のレポート名の右側に表示されます。
- 3 レポート名の右側にある矢印をクリックし、ドロップダウンメニューから、**スケジュール設定されたレポート** を選択します。
スケジュール設定されたレポート ページが表示されます。
- 4 繰り返し生成されるレポートをスケジュールするには、**追加** をクリックします。
レポートスケジュールの設定ウィザードが表示されます。
- 5 ウィザードの **確認** ページで、スケジュールするレポート詳細を入力し、**次へ** をクリックします。次の表で確認オプションについて説明しています。

表 161. スケジュールされたレポートの設定オプション

マシン	使用可能なレポート
名前	この特定のスケジュールに割り当てる表示名を入力します。 デフォルトの名前は Schedule report 1 です。名前は 64 文字以下に制限されます。 使用禁止文字または禁止語は使用できません。
レポート形式	レポート出力形式を選択します。値を選択しないと、デフォルトのフォーマット (PDF) が使用されます。
レポートタイプ	繰り返し生成するレポートのタイプを選択します。
ラベル	スケジュールされているレポートに表示するラベルを選択します。少なくとも1つのラベルが必要です。 カスタムグループ機能が Core オブジェクトを1つの論理コンテナにグループ化し、グループに対してラベルを定義できます。 レポートスケジュールの設定ウィザードのラベルのパラメーターを使用して、スケジュールされたレポートが実行されるカスタムグループを選択できます。 カスタムラベルが存在しない場合は、ラベルドロップダウンメニューで使用可能なオプションに、すべて選択と保護対象マシンが含まれます。カスタムグループが表示された場合、各グループがオプションとして表示されます。任意のオプションを選択またはクリアして、スケジュール設定されたレポートでそれらのオブジェクトを追加または除外することができます。

マシン	使用可能なレポート
保護対象マシン	1台以上の保護対象マシンを選択し、レポートに含めます。 このオプションは、リポジトリレポートでは使用できません。
ジョブタイプ	レポートに表示するジョブタイプを選択します。 デフォルトでは、この情報のセットには、指定された Core のすべてのマシン（保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシン）のジョブが含まれます。レポートパラメーターで、レポートをカスタマイズできます。フィルタを使用して一部のマシンを選択または除外します。マシンから独立してジョブを選択または除外することもでき、その場合、レポートには、Core ジョブのみのステータスが表示されます。 ジョブタイプ パラメータは、Core のサマリ と リポジトリ のスケジュールされたレポートのタイプには使用できません。

- 6 ウィザードの **宛先** ページで、スケジュールするレポートの宛先を選択します。次のいずれかを選択する必要があります。両方選択することもできます。問題がなければ、**次へ** をクリックします。

- ・ **宛先電子メールアドレス** フィールドで1つまたは複数の有効な電子メールアドレスを入力します。これにより、スケジュール設定されたレポートが生成されたときに電子メールでユーザーに通知します。

① | メモ: 電子メール通知および配信を指定しない場合は、ストレージの場所を指定する必要があります。

- ・ **ファイルとして保存** を選択し、生成されたレポートファイルを指定した場所に保存すし、**場所のタイプ** ドロップダウンメニューで、ローカル、ネットワーク、またはクラウドストレージオプションを選択します。**場所** フィールドで、次の表に説明されているように追加の場所情報を指定します。

表 162. スケジュールされたレポートの場所オプション

場所のタイプ	場所のタイプの説明	場所
ローカル	生成したレポートを Core にアクセスできるローカルパスに保存するには、場所のタイプとしてローカルを選択します。	場所フィールドでパスを指定します。 Core にローカルでアクセスできる場所を入力します。 たとえば、D ドライブ上の Reports フォルダ内にレポートを保存するには、「D:\Reports\」と入力します。
ネットワーク	生成したレポートをネットワーク上の Core にアクセスできるパスに保存するには、場所のタイプとして Network（ネットワーク）を選択します。場所フィールドでパスを指定します。	場所フィールドでパスを指定します。 ネットワークから Core にアクセスできる場所を入力します。\\servername\sharename の形式を使用します。 たとえば、データサーバーの Reports という共有フォルダーにレポートを格納するには、「\\Data\Reports\」と入力します。 ユーザー名とパスワードフィールドで、ネットワーク認証情報を指定します。
クラウド	生成したレポートを Core で設定されているクラウドストレージアカウント内に保存するには、場所のタイプとしてクラウドを選択します。 この手順を実行する前にストレージアカウントがすでに定義されている必要があります。Core で使用するクラウドストレージアカウントのセットアップ方法については、「 クラウドアカウントの管理 」を参照してください。	アカウントフィールドから適切なクラウドストレージアカウントを選択し、生成したレポートを保存するために使用します。 コンテナフィールドで、ストレージアカウントの適切なコンテナを指定します。 フォルダ名 フィールドで、生成されたレポートを保存するフォルダを指定します。

- 7 宛先 オプションを確認したら、**次へ** をクリックします。

- 8 ウィザードの **スケジュール** ページで、**データを送信** メニューから指定したレポートを生成する頻度を決定するオプションを選択します。日次、週次、月次でレポートを生成することができます。各オプションには、次の表に示す独自のパラメーターがあります。

表 163. スケジュールされたレポートを生成するための頻度オプション

頻度	頻度の詳細	頻度パラメーター
日次	毎日 1 回指定した時刻に指定したレポートを生成して保存または送信します。 このアクションのデフォルトの時刻は 12:00 AM です (Core サーバ上の時間に基づきます)。	レポートを生成するデフォルトの時刻を変更するには、テキストフィールドに新しい値を入力するか、コントロールを使用して、時、分、午前 (AM) または午後 (PM) を変更します。
週次	毎週 1 回、指定した曜日と時刻に指定のレポートを生成して、保存または送信します。 このアクションのデフォルトの時刻は日曜日の 12:00 AM です (Core サーバ上の時間に基づきます)。	レポートを生成するデフォルトの曜日を変更するには、曜日 メニューから曜日を選択します。 レポートを生成するデフォルトの時刻を変更するには、テキストフィールドに新しい値を入力するか、コントロールを使用して、時、分、午前 (AM) または午後 (PM) を変更します。
月次	毎月 1 回、指定した日付と時刻に指定のレポートを生成して、保存または送信します。 このアクションのデフォルトの日付は各月の最初の日の 12:00 AM です (Core サーバ上の時間に基づきます)。	レポートを生成するデフォルトの日付を変更するには、月の日付 メニューから日付を選択します。 レポートを生成するデフォルトの時刻を変更するには、テキストフィールドに新しい値を入力するか、コントロールを使用して、時、分、午前 (AM) または午後 (PM) を変更します。

- 9 一時停止したレポートを再開するまでスケジュール設定されたレポートの生成を停止する場合は、ウィザードの **スケジュール** ページで、**最初にレポートを一時停止** を選択します。
このレポートをスケジュールどおりに生成する場合は、このオプションの選択を解除します。
- 10 スケジュールに問題がなければ、**完了** をクリックしてウィザードを終了し、実行中の作業を保存します。
サマリレポートのサマリ表に新しいレポートスケジュールが表示されます。

レポートスケジュールの変更

レポートがスケジュールされたら、パラメーターまたは詳細のいずれかを変更できます。レポートの設定情報 (レポート名、出力形式、レポートタイプ、含まれるリポジトリ) を編集できます。電子メール通知オプションと生成されたレポートの保存先を変更することもできます。最後に、レポートのスケジュールを変更することも可能です。

スケジュール設定されたレポートのパラメーターを変更するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  (詳細) をクリックし、次に **レポート** を選択します。
ジョブレポート ページが表示されます。下方向矢印が現在のレポート名の右側に表示されます。
- 3 レポート名の右側にある矢印をクリックし、ドロップダウンメニューから、**スケジュール設定されたレポート** を選択します。
スケジュール設定されたレポート ページが表示されます。
- 4 スケジュール設定されたレポートのサマリ表の変更するレポートの行で、 設定 アイコンをクリックし、**編集** を選択します。
レポートスケジュールの設定ウィザード が表示されます。
- 5 このウィザードのページを移動し、必要に応じてパラメーターを変更します。このウィザードのパラメーターの詳細については、「**レポートのスケジュール設定**」のトピックを参照してください。
- 6 ウィザードの **スケジュール** ページで、**完了** をクリックしてウィザードを閉じ、変更を保存します。
ウィザードが終了し、レポートのスケジュールが変更されます。

スケジュールされたレポートの一時停止、再開、または削除

レポートがスケジュールされると、定義されたスケジュールに従って生成されます。スケジュールされたレポートの生成を一時的に停止する場合は、スケジュールを一時停止することができます。

スケジュールされたレポートが一時停止されている場合、レポートの生成を再開する場合、レポートの生成を再開するにはこの手順で説明されているようにします。

スケジュールされたレポートを生成中にそのレポートを生成する必要がなくなった場合は、いつでも削除することができます。

任意のスケジュール設定されたレポートが一時停止されているかどうかを確認するには、スケジュール設定されたレポートのサマリ表のステータス列を確認します。緑色の球は、アクティブなスケジュールされたレポートを示します。黄色の球は一時停止したスケジュールを示し、赤の球はエラーを示します。

レポートのスケジュールを一時停止、再開、削除するには、次の手順を実行します。

- 1 Rapid Recovery Core Console に移動します。
- 2 アイコンバーで  詳細をクリックし、次に **レポート** を選択します。
ジョブレポート ページが表示されます。下方向矢印が現在のレポート名の右側に表示されます。
- 3 レポート名の右側にある矢印をクリックし、ドロップダウンメニューから、**スケジュール設定されたレポート** を選択します。
スケジュール設定されたレポート ページが表示されます。
- 4 スケジュール設定されたレポートのサマリ表で、色付きのインジケータを使用してすべてのスケジュールされたレポートのステータスを表示します。
- 5 各レポートを一時停止または再開するには、最初の列のチェックボックスをオンにします。
- 6 サマリ表の上にあるスケジュール設定されたレポートオプション、次のいずれかの操作を行います。
 - ・ 選択したレポートの生成を一時停止するには、**一時停止** をクリックします。
 - ・ スケジュール設定されて一時停止されているレポートの生成を再開するには、**再開** をクリックします。
 - ・ 既存のスケジュール設定されたレポートの選択したスケジュールを削除するには、**削除** をクリックします。
スケジュール設定されたレポートを削除すると、今後レポートは生成されなくなります。以前のスケジュール設定されたレポートが保存されている場合、それらは削除されません。

レポートメニューの使用

レポートメニューはレポートを表示しているときにページの一番上に表示されます。このメニューにはレポートタイトルが含まれ、これも使用可能なレポートタイプを表示できるドロップダウンメニューになっています。このメニューの下には、レポートの条件を定義するために役立つ1つまたは複数のフィルタがあります。

レポートタイプに応じて特定のフィルタを使用できます。各レポートタイプに適用されるパラメーターの詳細については、そのレポートタイプを理解するためのトピックを参照してください。

レポートメニューの右側にいくつかのコントロールが表示されます。次の表に記載されているこれらのコントロールは、レポートを生成してエクスポートするのに役立ちます。

表 164. レポートメニューのコントロール

UI エlement	説明
プレビューボタン	プレビューボタンをクリックすると選択したレポートタイプとフィルタで指定したレポートパラメーターを基にレポートが生成されます。
エクスポート形式ドロップダウンメニュー	エクスポート ドロップダウンメニューを使用してレポートの出力形式を選択できます。値を選択しないと、デフォルトのフォーマット（PDF）が使用されます。
ダウンロードボタン/アイコン	ダウンロード ボタンを選択すると、エクスポート メニューで選択した形式で生成されたレポートがエクスポートされます。

レポートには測定単位が含まれるため、GB、TB、秒などの列の単位を判別しやすくなっています。

生成またはエクスポートされたレポートの外観に満足できない場合、レポートで使用されるフォントを変更することができます。詳細については、「[レポート設定の管理](#)」を参照してください。

レポートが生成されたら、レポートツールバーを使用できます。

関連するリンク

[ジョブレポートについて](#)

[失敗レポートについて](#)

[サマリレポートについて](#)

[中央管理コンソールのコアレポートの理解](#)

レポートのツールバーの使用

レポートメニューから、生成した後は、レポートは、レポートツールバーの下に表示されます。ツールバーを使用すると、レポートの保存および印刷など、レポート出力を操作できます。

ツールバーの左側に、サイドバー切り替えオプションがあります。このツールは、サイドバーを展開または縮小していくつかの追加の表示オプションにアクセスします。ツールバーの右側にあるツールオプションは、ドロップダウンメニューを展開し、レポートナビゲーションコントロールを提供します。次の表でレポートツールバーの要素について説明しています。

表 165. レポートのツールバーアイコン

アイコン	説明
	サイドバーの切り替え。 すべてのレポートページがサムネールとして表示されます。サイドバー内の他のオプションはサポートされていません。
	サイドバー：サムネールの表示。 これは、生成されたレポートのすべてのページのデフォルトビューになります。
	サイドバー：文書のアウトラインの表示。 この機能はサポートされていません。
	サイドバー：添付ファイルの表示。 レポートには添付ファイルはありません。この機能はサポートされていません。
	検索。 生成されたレポート内のテキストを検索することができます。入力した条件に一致するすべてのテキストをハイライトするオプションや、大文字と小文字を区別するか区別しないかを指定するオプションがあります。

アイコン 説明



前のページ。レポート表示の前のページに移動します。



次のページ。レポート表示の次のページに移動します。



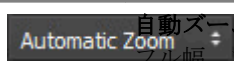
ページ番号の入力。ページ番号 テキストフィールドをクリックして、有効なページ番号を入力し、Enter キーを押してレポート表示内のそのページに移動します。



ズームアウト。生成されたレポートの表示をズームアウトすることができます。続けてクリックするたびにさらにズームアウトされ、最小で 25% までズームアウトできます。



ズームイン。生成されたレポートの表示をズームインすることができます。続けてクリックするたびにさらにズームインされ、最大で 1000% までズームアウトできます。



自動ズーム。生成されたレポートのズーム表示を制御することができます。実際のサイズ、ページに合わせて表示、フル幅、またはパーセンテージ（50%、75%、100%、125%、150%、200%、300%、または 400%）を指定できます。



ファイルを開く。ファイルシステム内を移動して保存されたレポートを見つけて開くことができます。



印刷。生成されたレポートを印刷することができます。



ツール。このアイコンをクリックしたときに、ツールドロップダウンメニューを展開または縮小させます。ツールオプションの説明については、下記を参照してください。



ツール：最初のページに移動。生成されたレポートの最初のページに移動します。



ツール：最後のページに移動。生成されたレポートの最後のページに移動します。



ツール：時計回りに回転。このオプションを使用すると、生成されたレポートのキャンバスが時計回りに回転します。



ツール：反時計回りに回転。このオプションを使用すると、生成されたレポートのキャンバスが反時計回りに回転します。



ツール：ハンドツール。このツールを選択すると、画面上でクリックおよびドラッグすることでレポートを移動できます。



ツール：ドキュメントのプロパティ。生成されたレポートのドキュメントプロパティについての情報を提供します。このウィンドウを閉じるには、**閉じる** をクリックします。

レポートの生成については、「[Core Console からのレポートの生成](#)」を参照してください。Central Management Console での複数の Core のレポートの生成については、「[Central Management Console からのレポートの生成](#)」を参照してください。

ジョブレポートについて

ジョブレポートは、Rapid Recovery Core および Core で保護されたマシンで使用できます。このレポートには、選択された Core または保護対象マシンで実行されたジョブのステータスを表示できます。レポートに表示されているデータのないデータの行または列は、テストしたパラメーターが Null であることを示します。たとえば、列（エラーなど）に情報が表示されない場合、選択されたレコードでエラーは発生していません。レポートに空の行が生成されている場合、選択されたレコードのジョブには、マシンに依存しないアクティビティが反映されます。

Core からのジョブレポートの生成方法については、「[オンデマンドでの Core レポートの生成](#)」を参照してください。保護対象マシンのジョブレポートの生成方法については、「[オンデマンドでの保護対象マシンのレポートの生成](#)」を参照してください。

ジョブレポートを生成するときに、レポートの詳細には、次の項目が含まれています。

- ・ レポートの選択基準
- ・ サマリ表には、指定された日付範囲にある各ジョブに対して行が表示されます。適切な Core、保護対象マシン、ジョブタイプを表示するだけでなく、それぞれの行には次のものが含まれます。
 - ・ ジョブのサマリ
 - ・ ジョブステータス
 - ・ ジョブに関連するエラー
 - ・ ジョブの開始日および終了日
 - ・ ジョブの時間（秒）
 - ・ 合計作業時間（MB）

情報は特定のカテゴリに関係ない場合、レポートのそのセルに情報が表示されません。たとえば、指定された保護対象マシンで Core にエラーがない場合、エラーレポート内のその行のエラーの列は空白です。

ジョブサマリレポートについて

ジョブサマリレポートは、Core の視点のみによって報告される場合に利用できます。また、このレポートは、保護対象マシンのレポートでは利用できません。このレポートには、1つのサマリがあり、ジョブの失敗数、成功数、キャンセル数を含む、Core で実行されたすべてのジョブに関する情報が示されます。ジョブサマリレポートは、各ジョブはレポート内で個別の行として指定されるため、ジョブレポートよりも詳細な情報が表示されます。

ジョブサマリレポートの生成方法については、「[Core Console からのレポートの生成](#)」を参照してください。

このレポートタイプのレポートパラメーターには、次のものがあります。

- ・ 日付範囲
- ・ 保護対象マシン
- ・ ジョブタイプ

ジョブサマリレポートを生成すると、レポートの詳細には、保護対象マシン、ボリューム、およびジョブタイプに関する情報に加えて、レポートの選択基準が含まれます。

Core 情報

サマリレポートの Core 部分には、Rapid Recovery Core に関するデータが含まれます。次の情報が含まれます。

- ・ Rapid Recovery Core により保護されるマシンの数
- ・ ジョブが失敗したマシンの数

保護対象マシンサマリ

サマリレポートの保護対象マシン部分には、選択した Rapid Recovery Core で保護されるすべてのマシンと、それらのマシンのポリシーのデータが含まれます。

グラフは、ジョブタイプとマシンごとの線グラフであり、成功したジョブの割合（全タイプ対象）、時間経過したジョブの数、失敗したジョブ数、およびキャンセルされたジョブ数が含まれます。（キャンセルされたジョブはこれらの統計の対象外になります）。

失敗レポートについて

失敗レポートはジョブレポートのサブセットで、Rapid Recovery Core および Core 上の保護対象マシンについて使用できます。失敗レポートには、ジョブレポートに表示されるキャンセルおよび失敗したジョブのみが含まれ、印刷およびエクスポート可能な1つのレポートにまとめられます。レポートが空白行で生成される場合、レポート条件で指定した日付範囲内にエラーはありません。

① **メモ:** ターゲット Core および保護対象マシンのパラメータの結果は、Core レベルのレポートでのみ表示されます。

Core からのジョブレポートの生成方法については、「[オンデマンドでの Core レポートの生成](#)」を参照してください。保護対象マシンのジョブレポートの生成方法については、「[オンデマンドでの保護対象マシンのレポートの生成](#)」を参照してください。

失敗レポートを生成するときに、サマリ表が表示され、指定された日付範囲にある各ジョブに対して行が表示されます。適切な Core、保護対象マシン、ジョブタイプを表示するだけでなく、それぞれの行には次のものが含まれます。

- ・ ジョブのサマリ
- ・ ジョブステータス
- ・ ジョブに関連するエラー
- ・ ジョブの開始日および終了日
- ・ ジョブの時間（秒）
- ・ 合計作業時間（MB）

サマリレポートについて

サマリレポートは1つまたは複数の Core で使用できます。このレポートは、保護対象マシンのレポートからは使用できません。サマリレポートには、選択された Rapid Recovery Core のリポジトリに関する情報と、その Core で保護されるマシンに関する情報が含まれます。2つのサマリ情報が1つのレポートに表示されます。

サマリレポートの生成方法については、「[Core Console からのレポートの生成](#)」を参照してください。

このレポートタイプのレポートパラメーターには、次のものがあります。

- ・ 日付範囲
- ・ 保護対象マシン

サマリレポートを生成すると、レポートの詳細にレポートの選択条件、リポジトリおよび保護対象マシンに関する情報が含まれます。

Core 情報

サマリレポートの Core 部分には、Rapid Recovery Core に関するデータが含まれます。次の情報が含まれます。

- ・ ライセンスキー（識別子）

- ・ Rapid Recovery Core ソフトウェアの現在のバージョン

リポジトリサマリ

サマリレポートのリポジトリ部分には、選択された Rapid Recovery Core にあるリポジトリのデータが含まれます。次の情報が含まれます。

- ・ Rapid Recovery Core 内のリポジトリ数
- ・ Core 上のリポジトリのサマリ。

保護対象マシンサマリ

サマリレポートの保護対象マシン部分には、選択された Rapid Recovery Core で保護されるすべてのマシンのデータが含まれます。これには、グラフおよびサマリ表が含まれています。

グラフには失敗したジョブと比較した成功したジョブ（任意のタイプ）割合で保護対象マシンが表示されます（キャンセルされたジョブはこれらの統計の対象外になります）。

X 軸または垂直方向の軸には、保護対象マシンの数が表示されます。Y 軸または水平方向の軸には、成功した階層が表示されます。具体的に、Y 軸には、保護対象マシン別に次の数が表示されます。

- ・ ジョブが実行されていません
- ・ 50% 未満成功レート
- ・ 50% 以上成功レート
- ・ 100% 成功レート

グラフの下に、保護対象マシンについての情報が表示されます。次の情報が含まれます。

- ・ 保護対象マシンの数
- ・ 失敗したジョブがある保護対象マシンの数
- ・ サマリ表には、保護対象マシン別に次の情報が表示されます。
 - ・ 保護対象マシン名
 - ・ マシンによって保護されるボリューム
 - ・ 保護容量 (GB 単位)
 - ・ 毎日の変更率 (平均と中央値)
 - ・ ジョブの統計情報 (成功、完了、失敗、キャンセル)
 - ・ 暗号化が適用されたかどうか
- ・ Core バージョン

リポジトリレポートについて

リポジトリレポートには、選択された Rapid Recovery Core のリポジトリに関する情報と、その Core で保護されるマシンに関する情報が含まれます。2つのサマリ情報が1つのレポートに表示されます。

Core からのリポジトリレポートの生成方法については、「[オンデマンドでの Core レポートの生成](#)」を参照してください。

このレポートタイプのレポートパラメーターには、リポジトリのみがあります。

リポジトリレポートを生成する場合、各リポジトリごとのレポート詳細には、Core 上のリポジトリの要約リストが含まれます。

Central Management Console

Rapid Recovery Central Management Console は、2 つ以上の Rapid Recovery Cores がある環境用のオプションコンポーネントです。このコンポーネントは、単一のインタフェースを使用して複数の Core をグループ化および管理し、レポートを生成できるウェブポータルです。

Central Management Console のオペレーティングシステム要件は Rapid Recovery Core の要件と同一です。これらのコンポーネントは、必要に応じて同じマシン上、または異なるマシン上にインストールすることができます。

インストール後に、個別または Core グループの一部として管理する Core を追加して、Central Management Console を設定する必要があります。

① | **メモ:** インストーラは、ローカル管理者権限を使用して実行する必要があります。

Windows 8、8.1、10、および Windows Server 2012、2012 R2 オペレーティングシステムで GUI を適切にロードするには、ASP.NET 4.5 機能がサーバにインストールされている必要があります。この設定は、Rapid Recovery Installer の一部として組み込まれています。

このコンポーネントをインストールする方法の詳細については、『*Rapid Recovery インストールおよびアップグレードガイド*』の Dell Data Protection | Rapid Recovery Central Management のインストールに関する項を参照してください。

このコンポーネントを構成する方法の詳細については、『*Dell Data Protection | Rapid Recovery ユーザーガイド*』の「Dell Data Protection | Rapid Recovery」を参照してください。

このコンポーネントの UI の詳細については、『*Dell Data Protection | Rapid Recovery ユーザーガイド*』の「Dell Data Protection | Rapid Recovery」を参照してください。

Rapid Recovery Central Management Console について

Central Management Console を開くとき、コンソールビューに情報が表示されます。ようこそ ページが表示され、次の要素を確認できます。

表 166. Rapid Recovery Central Management Console の UI 要素

UI エレメント	説明
「ブランド設定」エリア	一般的な環境では、Central Management Console の左上側に完全な親製品名、Dell Data Protection Rapid Recovery でブランドが表示されます。ブランド領域の任意の場所をクリックすると、デルサポートウェブサイトにある製品マニュアルに移動します。
左側のナビゲーションエリア	左側のナビゲーションエリアは、ユーザーインタフェースの左側にある「ブランド設定」エリアの下に表示されます。ナビゲーション領域の機能は、Central Management Console の右上で選択したモードに基づいて異なります。 コンソールモード。 コンソールモードでは、ナビゲーション領域で任意の Core または Core グループをクリックすると、選択した Core または Core グループが Rapid Recovery Core Console 内で開きます。 レポートモード。 レポートモードでは、ナビゲーション領域で Core または Core グループを選択すると、レポート生成時に表示される情報のセットが決定されます。 管理モード。 管理モードでは、ナビゲーション領域で Core および Core グループの設定をナビゲートすることができます。管理モードでは Core および Core グループを追加、削除することもできます。矢印をクリックすると、メニューを展開したり折りたたんだりできます。組織、Core グループ、Core の階層レベルが含まれています。左矢印をクリックすると、ナビゲーション領域が折りたたまれます。ナビゲーション領域を展開するには、右矢印をクリックします。

UI エlement	説明
リンク メニュー	デルサポートにお問い合わせください。 ライブチャット、ビデオチュートリアル、Rapid Recovery ナレッジベース記事、FAQ などを提供するデルサポートウェブサイト に新しいブラウザウィンドウでリンクします。
リンク メニュー	マニュアル。 ライブチャット、ビデオチュートリアル、Rapid Recovery ナレッジベース記事、FAQ などを提供するデルサポートウェブサイト に新しいブラウザウィンドウでリンクします。
リンク メニュー	バージョン。 Central Management Console の現在のバージョンがリストされます。このリンクをクリックすると、バージョン情報 ダイアログボックスが開きます。
リンク メニュー	モードセクタ。 現在ログインしている Windows ユーザーの名前が リンク メニューの右上のドロップダウンメニューに表示されます。 このメニューから、Central Management Console のビューを変更できます。次のいずれかのビューを選択できます。 コンソール。 これはデフォルトのモードで、お使いの環境で Core と Core グループを一元的に表示できます。 レポート： このモードから、このコンソールで設定された Core からレポートを生成、表示、およびエクスポートできます。 管理。 管理 モードから、Central Management Console に、単独でまたはまとめて、Core をさらに追加したり、削除したりすることができます。 言語。 ローカリゼーションをサポートするバージョンでは、言語 オプションがリストされます。このオプションを選択すると 言語の切り替え ダイアログボックスが開き、Central Management Console の表示言語を選択することができます。 アカウントキャッシュをクリアする。 ログインユーザーアカウントの既存の情報をクリアするには、このオプションを選択します。

モードセクタ（ページの右上にあるドロップダウンメニュー）のオプションを選択することで、Central Management Console のビューを変更できます。たとえば、次のとおりです。

- ・ 既に設定されている Core または Core グループを管理するには、Console のビューを使用します。
- ・ Central Management Console を設定するには、管理 ビューに切り替えます。
- ・ レポートを生成するには、レポート ビューに切り替えます。

管理および表示できる Core は左側のナビゲーションメニューに表示されます。個別の Core を設定することも、グループごとに整理することもできます。Windows ユーザー名またはグループを使用して、特定のグループで Core へのアクセスを制限することができます。

Rapid Recovery Central Management Console の設定

Rapid Recovery Central Management Console の設定には、Core および Core グループの追加、設定の確立、グループのアクセス設定を指定（必要に応じて）が含まれます。

設定を完了したら、中央の 1 箇所から設定の管理やすべての Core の管理ができるようになります。

Central Management Console を設定するには、次の関連リンクにリストされたすべてのタスクを実行できます。

関連するリンク

- [Central Management Console への Core の追加](#)
- [Central Management Console での Core 設定の構成](#)
- [Central Management Console への Core グループの追加](#)
- [Core グループの設定](#)
- [Core グループへのアクセスの設定](#)

Central Management Console への Core の追加

Core を Core グループに追加する場合は、最初にグループを作成する必要があります。詳細については、「[Central Management Console への Core グループの追加](#)」を参照してください。Core の詳細を後で編集し、グループを指定することもできます。

1つ、または複数の Core を Central Management Console に追加して管理するか、単一のインターフェースからレポートを生成します。

Central Management Console に Core を追加するには、次の手順を実行します。

- 1 Rapid Recovery Central Management Console で、モードセレクトドロップダウンメニューをクリックし、**管理** を選択します。ページが更新され、Core の追加 アイコン、グループの追加 アイコン、および削除 アイコンが表示されます。
- 2 左側のナビゲーションメニューの上部で、**Core の追加** をクリックします。**Core の追加** ページが表示されます。
- 3 次の表の説明に従って、Core の接続に必要な情報を入力します。

表 167. Core の詳細の追加

テキストボックス	説明
親グループ	必要に応じて、Core を既存の Core グループに追加する場合は、適切な組織から親グループを選択します。
表示名	Core の表示名を入力します。 表示名は 150 文字以下に制限する必要があります。ベストプラクティスは、この名前を 33 文字未満にすることです。 禁止されている文字と禁止されている語句は、使用できません。禁止されている文字または禁止されている語句の詳細については、『 <i>Dell Data Protection Rapid Recovery ユーザーガイド</i> 』を参照してください。
ホスト名	Core へのアクセスに使用する IP アドレスを入力します。 追加する Core が現在のサーバの場合、localhost を使用できます。
ポート	接続に使用するポート番号を入力します。デフォルト値は 8006 です。
ユーザー名	新たに追加された Core について、Core サービスにアクセスするために使用するユーザー名を入力します。
パスワード	新たに追加された Core について、Core サービスにアクセスするために使用するパスワードを入力します。

- 4 **接続テスト** をクリックして、設定をテストします。
テストが正常に行われると、成功したことを示すメッセージが表示されます。**OK** をクリックして確認メッセージを閉じます。
- 5 **保存** をクリックします。
変更内容が保存され、Core が親グループに追加されました。

関連するリンク

[Central Management Console への Core グループの追加](#)

Central Management Console での Core 設定の構成

Central Management Console に Core 設定を構成するには、次の手順を実行します。

- 1 Rapid Recovery Central Management Console で、モードセレクトドロップダウンメニューをクリックし、**管理** を選択します。ページが更新され、Core の追加 アイコン、グループの追加 アイコン、および削除 アイコンが表示されます。
- 2 左のナビゲーションメニューで、適切な Core の名前をクリックします。

選択した Core の **設定** ページが表示されます。

- 3 設定 タブで、次の表の説明に従って、Core 情報を変更します。

表 168. Core 設定

テキストボックス	説明
親グループ	追加する新しい Core 設定について、Core の親グループ名を選択します。
表示名	Core の表示名を入力します。
ユーザー名	Core のユーザー名を入力します。
パスワード	Core のパスワードを入力します。
[Core 名] に管理ポータルを接続する方法は?	接続を指定するオプションを選択します。次のオプションがあります。 ・ [Core 名] の最新の既知の IP アドレス (xxx.xxx.xxx.xxx) を使用する ・ ホスト名または IP アドレス [ホスト名または IP アドレス] を使用する ホスト名または IP アドレスを使用した接続を選択する場合、ホスト名または IP アドレスのフィールドに適切な情報を入力する必要があります。
[Core 名] がリスンしているポートは?	いずれかのポートオプションを選択します。次を選択できます。 ・ デフォルトのポート (8006) ・ カスタムポート [ポート] ポートを指定する場合、カスタムポート フィールドにポート番号を入力します。

- 4 **接続テスト** をクリックします。
テストが成功すると、接続が成功したことを示すメッセージが表示されます。
- 5 **保存** をクリックします。

Central Management Console への Core グループの追加

Rapid Recovery Central Management Console に Core グループを追加するには、次の手順を実行します。

- 1 Rapid Recovery Central Management Console で、モードセレクトドロップダウンメニューをクリックし、**管理** を選択します。
ページが更新され、Core の追加 アイコン、Core グループの追加 アイコン、および削除 アイコンが表示されます。
- 2 左側のナビゲーションメニューの一番上から、**グループの追加** をクリックします。
グループを追加 ページが表示されます。
- 3 次の表の説明に従って、親グループおよび表示名を選択します。

表 169. Core グループの追加

テキストボックス	説明
親グループ	追加する新しい Core グループについて、Core の親グループ名を選択します。
表示名	Core グループの表示名を入力します。 表示名は 150 文字以下に制限する必要があります。ベストプラクティスは、この名前を 33 文字未満にすることです。 禁止されている文字と禁止されている語句は、使用できません。禁止されている文字または禁止されている語句の詳細については、『Dell Data Protection Rapid Recovery ユーザーガイド』を参照してください。

- 4 **保存** をクリックします。

関連するリンク

[Central Management Console への Core グループの追加](#)

Core グループの設定

Core グループの設定またはアクセスを設定する前に、まずグループを作成する必要があります。詳細については、「[Central Management Console への Core グループの追加](#)」を参照してください。

Core グループを設定するには、次の手順を実行します。

- 1 Rapid Recovery Central Management Console で、モードセレクトドロップダウンメニューをクリックし、**管理**を選択します。ページが更新され、Core の追加 アイコン、Core グループの追加 アイコン、および削除 アイコンが表示されます。
- 2 左のナビゲーションメニューで、設定する Core グループの名前をクリックします。選択した Core グループの 設定 ページが表示されます。
- 3 次の表の説明に従って、Core グループの情報を変更します。

表 170. Core グループの設定

テキストボックス	説明
親グループ	追加する新しい Core グループ設定について、Core の親グループ名を選択します。
表示名	Core グループの表示名を入力します。 表示名は 150 文字以下に制限する必要があります。ベストプラクティスは、この名前を 33 文字未満にすることです。 禁止されている文字と禁止されている語句は、使用できません。禁止されている文字または禁止されている語句の詳細については、『Dell Data Protection Rapid Recovery ユーザーガイド』を参照してください。
保存	保存 をクリックします。

Core グループへのアクセスの設定

Core グループの設定またはアクセスを設定する前に、まずグループを作成する必要があります。詳細については、「[Central Management Console への Core グループの追加](#)」を参照してください。

Central Management Console で Core を追加または表示するには、現在のユーザーアカウントが Active Directory ドメイン Administrator グループのメンバーである必要があります。または、この手順を使用して個々のユーザーまたはグループにアクセスを提供できます。

Core グループへのアクセスを設定するには、次の手順を実行します。

- 1 Rapid Recovery Central Management Console で、モードセレクトドロップダウンメニューをクリックし、**管理**を選択します。ページが更新され、Core の追加 アイコン、グループの追加 アイコン、および削除 アイコンが表示されます。
- 2 左のナビゲーションメニューで、設定する Core グループの名前をクリックします。選択した Core グループの 設定 ページが表示されます。
- 3 **アクセス** タブをクリックします。Core グループのアクセス設定が表示されます。
- 4 **追加** をクリックします。**アクセス許可** ダイアログボックスが表示されます。個人またはグループにアクセスを提供することができます。
- 5 次の手順のいずれかを実行します。
 - ・ 個人にアクセスを提供する場合は、**名前** テキストフィールドにその個人の名前を入力し、**ユーザー** をクリックします。これは、デフォルトのオプションです。

たとえば、Administrator（または、マシンがドメイン内に存在する場合は、[domain name] \Administrator）と入力します。

- ・ グループにアクセスを提供する場合は、**名前** テキストフィールドにそのグループの名前を入力し、**グループ** をクリックします。

たとえば、AdminGroup（または、マシンがドメイン内に存在する場合は、[domain name] \AdminGroup）と入力します。

- 6 **名前のチェック** をクリックして、指定したユーザー名またはグループ名がアクセス可能であることを確認します。

入力した名前が有効な場合は、アカウントの確認メッセージが表示されます。

- 7 名前を入力して確認したら、**保存** をクリックします。

アクセス許可 ダイアログボックスが閉じ、変更が保存されます。Core グループの **アクセス** タブにアクセス名が表示されます。

中央管理コンソールのコアレポートの理解

Rapid Recovery により、複数の Rapid Recovery コアジョブレポート、エラーレポート、サマリ情報を生成し、表示できます。Core の詳細は、[ジョブレポートについて](#)、[失敗レポートについて](#)、および [サマリレポートについて](#) のセクションで説明されている同じカテゴリの一覧表に表示されます。

複数のコアに関するレポートを生成する方法については、[Central Management Console からのレポートの生成](#) を参照してください。

Central Management Console からのレポートの生成

Central Management Console から複数の Rapid Recovery Core のレポートを生成するには、次の手順を実行します。

- 1 Rapid Recovery Central Management Console で、右上にあるモードセレクトドロップダウンメニューをクリックし、**レポート** を選択します。
レポート選択 ページが表示されます。CoreJobReport は、デフォルトで選択されています。レポート名の右側に、下方向矢印が表示され、別のレポートタイプを選択できます。
- 2 左側のナビゲーションメニューで、個々 Rapid Recovery Core または Core グループの任意の組み合わせを選択してレポートに追加します。
- 3 レポートタイプ ドロップダウンメニューから、生成するレポートのタイプを選択します。次のいずれかのオプションを選択できます。
 - ・ ジョブレポート
 - ・ 失敗レポート
 - ・ サマリレポート
 - ・ ジョブサマリレポート

これらのレポートタイプの詳細については、以下を参照してください。 [Rapid Recovery レポートについて](#)。

- 4 日付範囲ドロップダウンメニューから、日付範囲を選択します。

次の表のオプションから選択することができます

オプション	説明
日	レポートを生成する時刻を基準とした相対的な最終日のアクティビティをレポートします。
週	レポートを生成する時刻を基準とした相対的な前週のアクティビティをレポートします。
月	レポートを生成する時刻を基準とした相対的な過去 31 日間のアクティビティをレポートします。
年	レポートを生成する時刻を基準とした相対的な前年のアクティビティをレポートします。
常時	この期間は、Core の耐用期間全体を対象とします。
カスタム	この期間では、さらに開始日と終了日を指定する必要があります。

- ① **メモ:** どの場合でも、**COre** ソフトウェアが展開される前、または **Core** 上でマシンが保護される前のレポートデータは使用できません。

- 5 次の手順のいずれかを実行します。

- ・ **プレビュー** をクリックして、生成されたレポートをオンラインで表示します。
- ・ レポートの条件を変更し、**プレビュー** をもう一度クリックしてレポートを動的に更新します。
- ・ エクスポート形式（デフォルトの形式の XLSX を含む）を選択し、**ダウンロード** をクリックします。
- ・ **レポートツールバー** を使用して、レポートを表示、操作、または印刷します。レポート ツールバーの詳細については、以下を参照してください。 [レポートのツールバーの使用](#)。

Rapid Recovery Command Line Management ユーティリティについて

Dell Data Protection | Rapid Recovery はいくつかのソフトウェアコンポーネントで構成されています。このトピックに関連する重要なコンポーネントには、次のようなものがあります。

- ・ Rapid Recovery Core は、保護対象マシンの認証の管理、バックアップとレプリケーションのためのデータ転送のスケジュール設定、仮想マシンのエクスポート、および同様または異種ハードウェアへのベアメタル復元（BMR）を実行します。
- ・ Rapid Recovery Agent は、ボリュームスナップショットと、AppAssure Core への高速なデータ転送を行います。
- ・ Rapid Recovery Command Line Management ユーティリティの cmdutil.exe は、サードパーティがシステム機能にアクセスして管理できるようにします。このツールは、Rapid Recovery Core の管理機能のスク립ト化を許可します。

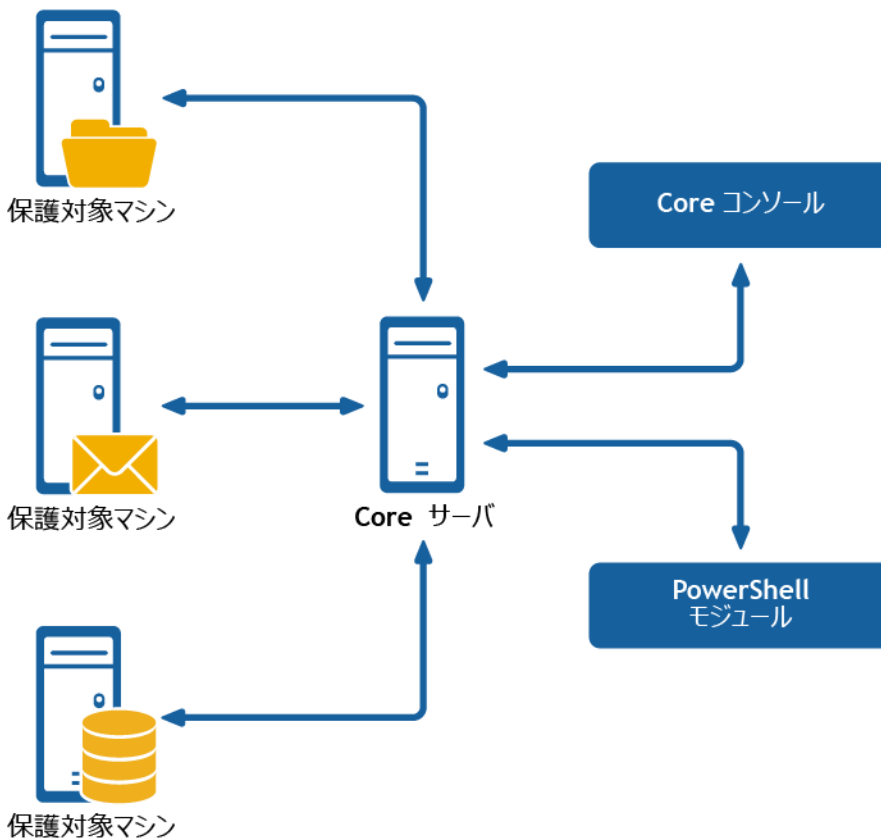


図 13. Rapid Recovery Command Line Management はコマンドライン機能を提供します

Rapid Recovery Command Line Management は、Windows コマンドラインユーティリティで、ユーザーはこれを使用して Rapid Recovery Core サーバを操作できます。これは、Rapid Recovery Core Console グラフィックユーザーインターフェースと同じいくつかの機能を提供します。たとえば、Rapid Recovery Command Line Management では、リカバリポイントをマウントしたり、スナップショット作成を強制的に実行したりすることができます。

Rapid Recovery Command Line Management ユーティリティは、Rapid Recovery Core のすべてのインストールに組み込まれています。デフォルトインストール用の Command Line Management ユーティリティを開くには、**C:\Program Files\AppRecovery\CoreService**に移動し、cmdutil.exe ファイルをダブルクリックします。

コマンドラインモードでは、コマンドオプションおよび修飾子を選択して、アクションフラグを Rapid Recovery Command Line Management ユーティリティに渡し、機能は限定されるが管理機能を実行できます。

トピック：

- ・ [コマンドこまんど](#)
- ・ [ローカライゼーションローからいぜーしょん](#)

コマンドこまんど

本項では、Rapid Recovery Command Line Management ユーティリティで使えるコマンドおよびオプションについて説明します。次のコマンドを使用できます。

- ・ [Archive](#)
- ・ [CancelActiveJobs](#)
- ・ [CheckRepository](#)
- ・ [CreateArchiveRepository](#)
- ・ [CreateBootCD](#)
- ・ [CreateRepository](#)
- ・ [DeleteRepository](#)
- ・ [Dismount](#)
- ・ [DismountArchiveRepository](#)
- ・ [EditEsxServer](#)
- ・ [Force](#)
- ・ [ForceAttach](#)
- ・ [ForceChecksum](#)
- ・ [ForceLogTruncation](#)
- ・ [ForceMount](#)
- ・ [ForceReplication](#)
- ・ [ForceRollup](#)
- ・ [ForceVirtualStandby](#)
- ・ [ヘルプ](#)
- ・ [List](#)
- ・ [マウント](#)
- ・ [MountArchiveRepository](#)
- ・ [NewCloudAccount](#)
- ・ [OpenDvmRepository](#)
- ・ [Pause](#)
- ・ [Protect](#)
- ・ [ProtectCluster](#)
- ・ [ProtectEsxServer](#)
- ・ [RemoveAgent](#)
- ・ [RemoveArchiveRepository](#)
- ・ [RemovePoints](#)

- RemoveScheduledArchive
- RemoveVirtualStandby
- レプリケート
- レプリケーション
- RestoreAgent
- RestoreArchive
- RestoreUrc
- Resume
- SeedDrive
- StartExport
- UpdateRepository
- バージョン
- VirtualStandby

Archive

企業では、準拠および非準拠データの両方のアーカイブに長期ストレージを使用することがよくあります。Rapid Recovery のアーカイブ機能は、準拠および非準拠データの長期保存をサポートします。管理者は、-path パラメーターと資格情報を指定して、アーカイブをローカルストレージやネットワークの場所に保存できます。

使用法：

コマンドの使用法を次に示します。

```
/archive -core [host name] -user [user name] -password [password] -all | -protectedserver [name  
| IP address] -path [location] -startdate [time string] -enddate [time string] -archiveusername  
[name] -archivepassword [password] -comment [text]
```

コマンドオプション

次の表は、archive コマンドで使用できるオプションを説明しています。

表 171. Archive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	Core 上のすべての保護対象マシンのすべてのリカバリポイントをアーカイブします。
-protectedserver	リカバリポイントをアーカイブする保護対象マシン。複数のマシン名を指定するには、二重引用符で囲み、スペースで区切ります。

オプション	説明
-path	アーカイブデータを配置するパス。パスの例：d:\work\archive、ネットワーク パスの例：\\servername\sharename。
-startdate	選択するリカバリポイントの作成日範囲の開始日。値は二重引用符で囲む必要があります。例： "04/30/2012 02:55 PM"
-enddate	省略可能。選択するリカバリポイントの作成日範囲の終了日。値は二重引用符で囲む必要があります。 例："05/31/2012 11:00 AM"デフォルトでは、現在のシステム時刻が使用されます。
-archiveusername	省略可能。リモートマシンに対するユーザー名。ネットワークパスのみで必要です。
-archivepassword	省略可能。リモートマシンに対するパスワード。ネットワークパスのみで必要です。
-comment	省略可能。コメントテキストは二重引用符で囲む必要があります。例：-comment "comment goes here..."。

例：

Core 上のすべてのマシンで、作成日が 04/30/2012 02:55 PM 以降のすべてのリカバリポイントをアーカイブします。

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -path d:\work\archive -startdate "04/30/2012 02:55 PM" -all
```

2 台の保護対象マシンで、特定の日付範囲内のリカバリポイントをアーカイブします。

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -protectedserver "10.20.30.40" "20.20.10.1" -path d:\work\archive -startdate "04/30/2012 02:55 PM" -enddate "05/31/2012 11:00 AM"
```

CancelActiveJobs

cancelactivejobs コマンドを使用して、転送やレプリケーションなど、進行している特定タイプのすべてのジョブの実行をキャンセルします。

使用法：

コマンドの使用法を次に示します。

```
/cancelactivejobs -core [host name] -user [user name] -password [password] -jobtype [job type filter]
```

コマンドオプション

次の表は、cancelactivejobs コマンドで利用できるオプションを説明しています。

表 172. CancelActiveJobs コマンドオプション

オプション	説明
-?	コマンドのヘルプを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログインユーザーの資格情報が使用されます。
-protectedserver	ジョブをキャンセルする保護対象マシンを決定します。
-all	すべての保護対象サーバーで、指定したタイプのイベントを選択およびキャンセルします。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値は次のとおりです。 「transfer」(データ転送) 「repository」(リポジトリのメンテナンス) 「replication」(ローカルおよびリモートレプリケーション) 「backup」(バックアップおよびリストア) 「bootcdbuilder」(ブート CD の作成) 「diagnostics」(ログのアップロード) 「exchange」(Exchange Server ファイルのチェック) 「export」(リカバリポイントのエクスポート) 「pushinstall」(Agent の導入) 「restore」(リカバリポイントの復元) 「rollup」(リカバリポイントのロールアップ) 「sqlattach」(Agent のアタッチ可否チェック) 「mount」(リポジトリのマウント) デフォルトでは、指定したタイプのすべてのジョブがキャンセルされます。

例：

Core 10.10.10.10 のすべての転送ジョブをキャンセルします。

```
>cmdutil /cancelactivejobs -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -
jobtype transfer
```

CheckRepository

CheckRepository コマンドを使用して、AppAssure Core または Rapid Recovery Core で作成された既存の DVM リポジトリの整合性を確認することができます。

使用法：

コマンドの使用法を次に示します。

```
/checkrepository -repository [repository name] | -all [check all repositories] -core [host name] -user [user name] -password [password] name] -force
```

コマンドオプション

次の表は、CheckRepository コマンドで使用できるオプションを説明しています。

表 173. CheckRepository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	省略可能。このオプションは、Core に関連付けられているすべての DVM リポジトリをチェックします。
-repository	DVM リポジトリの名前。
-force	省略可能。このオプションは、確認せずにチェックを実行します。

例：

DVM リポジトリチェックを開始します。

```
>cmdutil /checkrepository -repository "Repository1" -core 10.10.10.10 -user administrator -password 23WE@#$sdd
```

CreateArchiveRepository

アーカイブリポジトリを作成するときに、スケジュール設定されたアーカイブのコンテンツの出力先を作成します。この機能を使用すると、アーカイブをインポートせずに、アーカイブされたリカバリポイントをマウントし、マシンをリストアできます。

使用法：

コマンドの使用法を次に示します。

```
/createarchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name] -path [path to the archive] -archiveusername [network user name] -archivepassword [network password] -cloudaccountname [name of the cloud account] -cloudcontainer [name of the cloud container]
```

コマンドオプション

次の表は、CreateArchiveRepository コマンドで利用できるオプションを説明しています。

表 174. CreateArchiveRepository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	必須。アーカイブリポジトリの名前。
-path	既存のアーカイブへのパス。ローカル、ネットワーク、またはクラウドの場所を指定できます。例: d:\work\archive or \\servername\sharename。
-archiveusername	省略可能。このオプションは、リモートマシンに対するログインです。ネットワークパスのみで必要です。
-archivepassword	省略可能。このオプションは、リモートマシンに対するパスワードです。ネットワークパスのみで必要です。
-cloudaccountname	省略可能。このオプションは既存のクラウドアカウントの表示名です。クラウドパスのみに必要です。
-cloudcontainer	省略可能。クラウドコンテナはアーカイブが配置されている場所です。クラウドパスのみに必要です。

例 :

"NewArchive:" という名前でアーカイブリポジトリを作成します。

```
>cmdutil /createarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -password 23WE@#$$dd -path d:\work\archive
```

また、アーカイブに複数の場所が含まれていた場合は、コマンドには 1 から N の順番ですべてのセグメントのパスを含める必要があります。N はセグメントの数と等しくなります。

"NewSegmentArchive:" という名前でアーカイブリポジトリを作成します。

```
>cmdutil /createarchiverepository -name NewSegmentArchive -path1 \\RemmoteServer1\Share\Archive\Segment1 - archiveusername1 Administrator -archivepassword1 23WE@#$$dd -path2 Archives\NewSegment -cloudcontainer2 ArchiveContainer -cloudaccountname AmazonS3Local - path3 d:\work\archive\Third
```


CreateBootCD

このコマンドを使用すると、Rapid Recovery Core Console を使用せずに、bare metal restore (BMR) ブート CD を作成できます。

使用法：

コマンドの使用法を次に示します。

```
/createbootcd -ip [IP address] -mask -defaultgateway -dnsserver -vncpassword -vncport -isofilepath [destination for the boot image]
```

コマンドオプション

次の表は、CreateBootCD コマンドで利用できるオプションを説明しています。

表 175. CreateBootCD コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-ip	省略可能。このオプションは、ターゲット BMR マシンの IP アドレスを指定します。デフォルトでは自動的に生成されます。
-mask	省略可能。このオプションは、ターゲット BMR マシンのサブネットマスクを指定します。デフォルトでは自動的に生成されます。
-defaultgateway	省略可能。このオプションは、ターゲット BMR マシンのデフォルトゲートウェイを指定します。デフォルトでは自動的に生成されます。
-dnsserver	省略可能。このオプションは、ターゲット BMR マシンの DNS サーバを指定します。デフォルトでは自動的に生成されます。
-vncpassword	省略可能。このオプションは、既存の UltraVNC アカウントのユーザーパスワードを指定します。このオプションはデフォルトでは空白になっています。
-vncport	省略可能。このオプションは、UltraVNC で使用するポートを指定します。-vncpassword オプションを使用した場合にのみ変更することができます。デフォルトのポートは 5900 です。
-isofilepath	省略可能。このオプションは、ブート CD ファイルのパッチを指定します。デフォルトのパスは C:\ProgramData\AppRecovery\Boot CDs です。

例：

ブート CD を作成します。

```
>cmdutil /createbootcd -ip 192.168.20.188 -mask 255.255.255.0 -defaultgateway 192.168.20.2 -dnsserver 192.168.20.2 -isofilepath D:\bcd\newbcd3.iso
```

CreateRepository

createrepository コマンドを使用して、ローカルマシンまたは CIFS 共有の場所に新しい DVM リポジトリを作成します。

使用法：

ローカルの場所にリポジトリを作成するコマンドの使用法を次に示します。

```
/createrepository -name [repository name] -size [size allocated for repository] -datapath [data path of repository] -metadatapath [metadata path of repository] -core [host name] -user [user name] -password [password]
```

共有の場所に DVM リポジトリを作成するコマンドの使用法を次に示します。

```
/createrepository -name [repository name] -size [size allocated for repository] -uncpath [path for data and metadata] -shareusername [user name for share location] -sharepassword [password for share user name] -concurrentoperations [number of operations to occur at one time] -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、createrepository コマンドで利用できるオプションを説明しています。

表 176. CreateRepository コマンドオプション

オプション	説明
-?	コマンドのヘルプを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	リポジトリ名。
-size	リポジトリストレージの場所のサイズ。使用できる単位は b、Kb、Mb、Gb、Tb、Pb です。
-datapath	ローカルの場所のみ。リポジトリストレージの場所のデータパスを決定します。
-metadatapath	ローカルの場所のみ。リポジトリストレージの場所のメタデータパスを決定します。
-uncpath	共有の場所のみ。リポジトリストレージの場所のデータおよびメタデータパスを決定します。
-shareusername	共有の場所のみ。場所を共有するためのユーザー名を決定します。
-sharepassword	共有の場所のみ。場所を共有するためのパスワードを決定します。
-comment	省略可能。リポジトリの説明。

オプション	説明
-concurrentoperations	省略可能。同時に保留することができる操作の最大数。値はデフォルトで 64 です。

例：

ローカルの場所で DVM リポジトリを作成します。

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -datapath d:\repository -
metadatapath d:\repository -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

共有の場所で DVM リポジトリを作成します。

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -uncpath \\share\repository -
shareusername login -sharepassword pass123 -comment "First repository." -concurrentoperations 8
-core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

DeleteRepository

DeleteRepository コマンドを使用して、AppAssure Core または Rapid Recovery Core で作成された DVM リポジトリ全体を削除することができます。

使用法：

コマンドの使用法を次に示します。

```
/deleterepository -core [host name] -user [user name] -password [password] name] -name
[repository name] | -a [all repositories]
```

コマンドオプション

次の表は、DeleteRepository コマンドで使用できるオプションを説明しています。

表 177. DeleteRepository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-a	省略可能。このオプションは、Core に関連付けられているすべての DVM リポジトリを削除します。
-name	削除する DVM リポジトリの名前。

例：

すべての DVM リポジトリを削除します。

```
>cmdutil /deleterepository -a
```

"RepositoryName:" という名前のリポジトリを削除します。

```
>cmdutil /deleterepository -name RepositoryName
```

Dismount

dismount コマンドを使用して、-path オプションで指定されたマウント済みリカバリポイントのマウント解除、-protectedserver パラメーターによって選択されたエージェントのポイントのマウント解除、またはすべてのリカバリポイントのマウント解除 (-all) を行うことができます。

使用法：

コマンドの使用法を次に示します。

```
/dis[mount] -core [host name] -user [user name] -password [password] [-all | -protectedserver [name | IP address] | -path [location]
```

コマンドオプション

次の表は、dismount コマンドで使用できるオプションを説明しています。

表 178. Dismount コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	マウントされたすべてのリカバリポイントをマウント解除します。
-protectedserver	現在の Agent のマウントされたすべてのリカバリポイントをマウント解除します。
-path	選択したマウントポイントをマウント解除します。

例：

フォルダ c:\mountedrecoverypoint にマウントされたリカバリポイントをマウント解除します。

```
>cmdutil /dismount -core 10.10.10.10 -user administrator -password 23WE@#sdd -path c:\mountedRecoveryPoint
```

DismountArchiveRepository

マウントされたアーカイブから必要な情報を取得した後に、発生する可能性がある問題を避けるために、アーカイブをマウント解除する必要があります。

使用法：

コマンドの使用法を次に示します。

```
/dismountarchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name]
```

コマンドオプション

次の表は、DismountArchiveRepository コマンドで使用できるオプションを説明しています。

表 179. DismountArchiveRepository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	必須。アーカイブリポジトリの名前。

例：

"NewArchive:" という名前のリポジトリをマウント解除します。

```
>cmdutil /dismountarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path d:\work\archive
```

EditEsxServer

必要なときにはいつでも `editesxserver` コマンドを使用してエージェントなし保護する VMware ESX(i) 仮想マシンの数を変更できます。

使用法：

コマンドの使用法を次に示します。

```
/editEsxServer -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -add | -remove -virtualMachines [virtual machines collection | all] -autoProtect [object ID or name collection]
```

コマンドオプション

次の表は、`editesxserver` コマンドで使用できるオプションを説明しています。

表 180. EditEsxServer コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-repository	必須。仮想マシンを保護するために使用する Core に関連付けられているリポジトリの名前。 ❗ メモ: 名前を二重引用符で囲む必要があります。
-protectedserver	このオプションを使用して、特定の保護対象マシンの vCenter および ESX(i) オブジェクトを編集します。
-add	このオプションを使用して、指定された vCenter または ESXi オブジェクトを追加します。
-remove	このオプションを使用して、指定された vCenter または ESXi オブジェクトを削除します。
-virtualmachines	省略可能。このオプションを使用すると、保護する仮想マシンが一覧で表示されます。
-autoprotect	省略可能。このオプションを使用して、自動的に保護する新しい仮想マシンを一覧表示します。

例：

Core を使用して vCenter または ESXi サーバの特定の vCenter または ESXi オブジェクトを自動的に保護します。

```
>cmdutil /editEsxServer -protectedserver 10.10.8.150 -add -autoprotect "Folder1" "Folder2"
```


Force

force コマンドは、指定した保護対象サーバのスナップショット作成を強制的に実行します。スナップショット作成の強制実行によって、現在保護対象のマシンのデータ転送を強制できます。スナップショット作成を強制的に実行すると、転送がただちに開始されるか、キューに追加されます。以前のリカバリポイントから変更されたデータのみが転送されます。以前のリカバリポイントが存在しない場合は、保護対象ボリューム上のすべてのデータが転送されます。

使用法：

コマンドの使用法を次に示します。

```
/force [snapshot] default | [base] [-all | -protectedserver [name | IP address]] -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、force コマンドで使用できるオプションを説明しています。

表 181. Force コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-force	省略可能。作成するスナップショットのタイプ。使用できる値：「snapshot」（増分スナップショット）および「base」（ベースイメージスナップショット）。デフォルトでは、増分スナップショットが実行されます。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	Core 上のすべてのマシンのスナップショット作成を強制的に実行します。
-protectedserver	特定の保護対象マシンのスナップショット作成を強制的に実行します。

例：

Core 上のすべてのマシンのスナップショット作成を強制的に実行します。

```
>cmdutil /force snapshot -core 10.10.10.10 -user administrator -password 23WE@#sdd -all
```

ForceAttach

forceattach コマンドでは、SQL データベースファイルのアタッチ可否検証を強制実行できます。アタッチ可否検証を強制実行すると、検証がただちに開始されます。

使用法：

コマンドの使用法を次に示します。

```
/forceattach -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

コマンドオプション

次の表は、forceattach コマンドで使用できるオプションを説明しています。

表 182. ForceAttach コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	アタッチ可否チェックを実行する保護対象マシン。
-rpn	チェックを実行するリカバリポイントの連続する番号（コマンド /list rps を実行して番号を取得）。1つのコマンドで複数のリカバリポイントのチェックを実行するには、複数の番号間をスペースで区切ります。
-time	作成日時でリカバリポイントを選択します。正確な日時を「mm/dd/yyyy hh:mm tt」形式（「2/24/2012 09:00 AM」など）で指定する必要があります。PC で設定されているタイムゾーンでの日時の値を指定します。

例：

番号 5 と 7 のリカバリポイントのアタッチ可否チェックを実行します。

```
>cmdutil /forceattach -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22 -rpn 5 7
```

ForceChecksum

forcechecksum コマンドでは、指定したリカバリポイントに存在している Exchange メッセージデータベース（MDB）の整合性チェックを強制実行できます。チェックサムチェックを強制実行すると、コマンドがただちに開始されます。

使用法：

コマンドの使用法を次に示します。

```
/forcechecksum -core [host name] -user [user name] -password [password] -protectedserver [name  
| IP address] -rpn [number | numbers] -time [time string]
```

コマンドオプション

次の表は、forcechecksum コマンドで使用できるオプションを説明しています。

表 183. ForceChecksum コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	チェックサムチェックを実行する保護対象マシン。
-rpn	チェックを実行するリカバリポイントの連続する番号 (コマンド /list rps を実行して番号を取得)。1つのコマンドで複数のリカバリポイントのチェックを実行するには、複数の番号間をスペースで区切ります。
-time	作成日時でリカバリポイントを選択します。正確な日時を「mm/dd/yyyy hh:mm tt」形式 (「2/24/2012 09:00 AM」など) で指定する必要があります。PC で設定されているタイムゾーンでの日時の値を指定します。

例：

番号 5 と 7 のリカバリポイントのチェックサムチェックを実行します。

```
>cmdutil /forcechecksum -core 10.10.10.10 -user administrator -password 23WE@#$$dd -  
protectedserver 10.10.5.22 -rpn 5 7
```

ForceLogTruncation

ログの切り捨ての強制によって、ジョブを 1 回限りオンデマンドで実行できます。指定した SQL Server Agent マシンのログがただちに切り捨てられます。

使用法：

コマンドの使用法を次に示します。

```
/[forcelogtruncation | flt] -core [host name] -user [user name] -password [password] -  
protectedserver [name | IP address]
```

コマンドオプション

次の表は、forcelogtruncation コマンドで使用できるオプションを説明しています。

表 184. ForceLogTruncation コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	ログファイルの切り捨てを実行する保護対象マシン。

例：

保護対象サーバーのログの切り捨てを強制実行します。

```
>cmdutil /forcelogtruncation -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -protectedserver 10.10.20.20
```

ForceMount

forcemount コマンドを使用して、1回限りのリカバリポイントのマウント可否チェックを実行します。このチェックで、指定したリカバリポイントがマウント可能で、バックアップデータのリストアに使用できるかどうか判断されます。チェックを実行する1つ以上のリカバリポイント、またはリカバリポイントが作成された時間の範囲のいずれかを指定する必要があります。

使用法：

コマンドの使用法を次に示します。

```
/forcemount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

コマンドオプション

次の表は、forcemount コマンドで使用できるオプションを説明しています。

表 185. ForceMount コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	マウント可否チェックを実行する保護対象マシン。
-rpn	チェックを実行するリカバリポイントの連続する番号 (コマンド /list rps を実行して番号を取得)。1つのコマンドで複数のリカバリポイントのチェックを実行するには、複数の番号間をスペースで区切ります。
-time	作成日時でリカバリポイントを選択します。正確な日時を「mm/dd/yyyy hh:mm tt」形式 (「2/24/2012 09:00 AM」など) で指定する必要があります。PC で設定されているタイムゾーンでの日時の値を指定します。

例 :

番号 5 と 7 のリカバリポイントのマウント可否チェックを実行します。

```
>cmdutil /forcemount -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.20.20 -rpn 5 7
```

ForceReplication

forcereplication コマンドを使用して、ソース Core からターゲット Core へのレプリケートデータの 1 回限りの転送を強制実行します。特定の 1 台の保護対象サーバーまたはすべての保護対象サーバーをレプリケートできます。保護対象サーバーが既にレプリケーション用に設定されている必要があります。

使用法 :

コマンドの使用法を次に示します。

```
[/forcereplication |frep] -core [host name] -user [user name] -password [password] -targetcore [host name] -all | -protectedserver [name | IP address]
```

コマンドオプション

次の表は、forcereplication コマンドで使用できるオプションを説明しています。

表 186. ForceReplication コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-targetcore	レプリケーションを強制実行するターゲット Core のホスト名。
-protectedserver	レプリケートする保護対象マシン。
-all	ターゲット Core へのすべてのマシンのレプリケートを強制実行します。

例：

特定のターゲット Core で、保護対象サーバーのレプリケートを強制実行します。

```
>cmdutil /forcereplication -target core 10.10.10.10 -protectedserver 10.20.30.40
```

ForceRollup

forcerollup コマンドを使用して、保護対象マシンのリカバリポイントのロールアップを強制実行します。

使用法：

コマンドの使用法を次に示します。

```
/[forcerollup | fro] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address]
```

コマンドオプション

次の表は、forcerollup コマンドで使用できるオプションを説明しています。

表 187. ForceRollup コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	省略可能。ロールアップを実行する保護対象マシン。

例：

Core 上の Agent 10.10.10.1 のロールアップを強制実行します。

```
>cmdutil /forcerollup -core 10.10.10.10 - user administrator -password 23WE@#sdd -
protectedserver 10.10.10.1
```

ForceVirtualStandby

保護対象マシンから仮想マシンにデータをエクスポートすると、仮想スタンバイマシンが作成されます。継続的に仮想エクスポートを設定する場合は、事前に設定されたスケジュールに関係なく、このコマンドを使用して Rapid Recovery によるオンデマンドのデータエクスポートを強制実行できます。

使用法：

コマンドの使用法を次に示します。

```
/forcevirtualstandby -core [host name] -user [user name] -password [password login] -
protectedserver [name] | -all
```

コマンドオプション

次の表は、ForceVirtualStandby コマンドで使用できるオプションを説明しています。

表 188. ForceVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	仮想マシンの名前またはスペースで区切られた名前。
-all	このコマンドは、スケジュールされたすべての仮想エクスポートを強制するかどうかを指定します。

例：

すべての仮想スタンバイエクスポートを強制します。

```
>cmdutil /forcevirtualstandby -all
```

2 台のマシンの仮想スタンバイを強制します。

```
>cmdutil /forcevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

ヘルプ

help コマンドでは、使用できるコマンドとその定義のリストが表示されます。著作権とバージョンの詳細も表示されます。

使用法：

コマンドの使用法を次に示します。

```
/help
```

例：

コマンドラインのヘルプを要求します。

```
>cmdutil /help
```

List

list コマンドは、Core によって現在保護されている指定した Agent またはサーバのリストでのすべてのリカバリポイント、アクティブなジョブ、完了したジョブ、失敗したジョブ、無効な（失敗した）リカバリポイント、有効な（成功した）リカバリポイント、マウント、保護対象サーバ、ボリューム、仮想サーバ、保護されていないボリューム、クラスタ、保護グループ、SQL データベース、Exchange データベース、レプリケートされたサーバ、リポジトリに関する情報を返します。デフォルトでは最新のレコードが返されます。すべてのレコードを表示したり、number パラメータを使用して表示するレコード数を指定することもできます。このパラメーターには、文字 "l"（最新のリカバリポイント）と "f"（最初のリカバリポイント）を含める必要があります。各リカバリポイントには、管理者がマウントに使用できる固有の番号が割り当てられています。

使用法：

コマンドの使用法を次に示します。

```
/list [rps | passed | failed | mounts | volumes | protectedservers | activejobs | completed  
jobs | failedjobs | virtualizedservers | unprotectedvolumes | clusters | protectiongroups |  
sqldatabases | exchangemailstores | replicatedservers | repositories] -protectedserver [name |  
IP address] -core [host name] -user [user name] -password [password] -number [all | l<number> |  
f<number> | <number>] -jobtype
```

コマンドオプション

次の表は、list コマンドで使用できるオプションを説明しています。

表 189. List コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-list	次のオプションのいずれかを選択します。 - すべてのリカバリポイント (「rps」) - 有効なリカバリポイント (「passed」) - 無効なリカバリポイント (「failed」) - マウント (「mounts」) - 保護対象ボリューム (「volumes」) - 保護されていないボリューム (「unprotectedvolumes」) - 保護対象マシン (「protectedservers」) - アクティブなジョブ (「activejobs」) - 失敗したジョブ (「failedjobs」) - 完了したジョブ (「completedjobs」) - 仮想サーバー (「virtualizedservers」) - クラスタ (「clusters」) - 保護グループ (「protectiongroups」) - SQL Server database (「sqldatabases」) - MS Exchange データベース (「exchangemailstores」) - レプリケートされたサーバー (「replicatedservers」) - リポジトリ (「repositories」)
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	ジョブの表示のみ。Core サーバー上の指定したタイプ (アクティブ/失敗/完了) のすべてのイベントを表示します。
-protectedserver	リカバリポイントを表示する保護対象マシン。
-number	省略可能。表示するデータアイテム数。「rps」、「activejobs」、「completedjobs」、「failedjobs」指定子と併用する場合にのみ使用するオプションです。使用できる値は次のとおりです。 - all (すべてのデータアイテムを取得) - l[number] または [number] (最新の ## 件のデータアイテムを取得) - f[number] (最初の ## 件のデータアイテムを取得) リカバリポイントとジョブを表示する場合にのみ有効です。
-jobtype	省略可能。ジョブタイプ別のフィルタ出力。使用できる値は、

- ・ 「transfer」 (データ転送)
- ・ 「repository」 (リポジトリのメンテナンス)
- ・ 「replication」 (ローカルおよびリモートレプリケーション)
- ・ 「backup」 (バックアップおよびリストア)
- ・ 「bootcdbuilder」 (ブート CD の作成)
- ・ 「diagnostics」 (ログのアップロード)
- ・ 「exchange」 (Exchange Server ファイルのチェック)
- ・ 「export」 (リカバリポイントのエクスポート)
- ・ 「pushinstall」 (Agent の導入)
- ・ 「restore」 (リカバリポイントの復元)
- ・ 「rollup」 (保護対象マシンのロールアップ)
- ・ 「sqlattach」 (Agent のアタッチ可否チェック)
- ・ 「mount」 (リポジトリのマウント)

例 :

最新 30 件のリカバリポイントを表示します。

```
>cmdutil /list rps -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -number 130
```

保護対象マシンで実行され失敗したすべてのデータ転送ジョブを表示します。

```
>cmdutil /list failed jobs -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -number all -jobtype transfer
```

マウント

mount コマンドは、1つ以上のドライブのスナップショットをマウントします。マウントには、読み取り専用、書き込み可能、または以前の書き込みとともに読み取り専用を指定できます。デフォルトの選択は読み取り専用です。

使用法 :

コマンドの使用法を次に示します。

```
/mount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -mounttype [read | write | readOnlyWithPreviousWrites] -drives [drive names] -volumes [volume names] -path [location] -rpn [number | numbers] | -time [time string]
```

コマンドオプション

次の表は、mount コマンドで使用できるオプションを説明しています。

表 190. Mount コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	リカバリポイントをマウントする保護対象マシン。
-mounttype	省略可能。マウントモードを指定します。使用可能な値は 'read' (read-only)、'readOnlyWithPreviousWrites' (以前の書き込みとともに読み取り専用)、'write' (書き込み可能) です。デフォルトのモードは read-only です。
-volumes	省略可能。マウントするボリューム名のリスト。指定しない場合は、すべてのボリュームがマウントされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。例: "c:" "d:"。ボリューム名の末尾にスラッシュを使用しないでください。
-path	リカバリポイントをマウントする Core サーバー上のフォルダのパス。フォルダが存在しない場合は自動的に作成されます。
-rpn	省略可能。マウントするリカバリポイントの連続する番号 (/list rps コマンドを使用して番号を取得)。1つのコマンドで複数のリカバリポイントをマウントするには、複数の番号をスペースで区切って指定します。この場合、各リカバリポイントのデータは個別の子フォルダに保存されます。注: -time と -rpn のどちらのオプションも指定しない場合は、整合性チェックに成功した最新のリカバリポイントがマウントされます。
-time	省略可能。マウントに選択されるリカバリポイントを決定します。使用できる値は、「latest」、「passed」、「mm/dd/yyyy hh:mm tt」形式の正確な時間 (例: 「2/24/2012 09:00 AM」) です。PC で設定されているタイムゾーンでの日時の値を指定します。-time と -rpn のどちらのオプションも指定しない場合は、整合性チェックに成功した最新のリカバリポイントがマウントされます。
-localdrive	省略可能。ローカル PC のユーザーディスクに対するマウントを実行します。

例:

ボリューム「c:\」と「d:\」を含む最新のリカバリポイントを読み取り専用モードでマウントします。

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -mounttype read -volumes "c:" "d:"
```

番号 2 と 7 のリカバリポイントをマウントします。

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -rpn 2 7
```

MountArchiveRepository

Rapid Recovery でアーカイブからデータをリストアするには、最初にマウントする必要があります。

使用法：

コマンドの使用法を次に示します。

```
/mountarchiverepository -core [host name] -user [user name] -password [password] -name [archive repository name]
```

コマンドオプション

次の表は、mountarchiverepository コマンドで使用できるオプションを説明しています。

表 191. MountArchiveRepository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	必須。アーカイブリポジトリの名前。

例：

"NewArchive:" という名前のリポジトリをマウントします。

```
>cmdutil /mountarchiverepository -name NewArchive
```

NewCloudAccount

NewCloudAccount コマンドを使用して Rapid Recovery Core へのクラウドプロバイダにアカウントを追加します。この後、アカウントを使用して保持またはレプリケーション用にアーカイブを保存できます。

使用法：

コマンドの使用法を次に示します。

```
/newcloudaccount -core [host name] -user [user name] -password [password] -displayname [name for the account] -type [cloud account provider] -username [user name for the account] -key [secret key] -region [region for account] -tenantid [tenant ID] -authurl [authorization URL]
```


コマンドオプション

次の表は、NewCloudAccount コマンドで利用できるオプションを説明しています。

表 192. NewCloudAccount コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-displayname	クラウドアカウントに使用する名前です。
-type	クラウドアカウントのタイプです。サポートされる値は次のとおりです。 - amazon - openstack - rackspace - windowsazure "windows azure" - azure
-username	追加するクラウドアカウントのユーザー名です。これは認証プロセスで使用する資格情報です。クラウドタイプに基づいて、プロパティには次のバリエーションがあります。 - Amazon - アクセスキー - OpenStack - ユーザー名 - Rackspace - ユーザー名 - Windows Azure - ストレージアカウント名
-key	追加するクラウドアカウントの認証キー。これは認証プロセスで使用する資格情報です。クラウドタイプに基づいて、プロパティには次のバリエーションがあります。 - Amazon - 秘密キー - OpenStack - API キー - Rackspace - API キー - Windows Azure - アクセスキー
-region	追加するクラウドアカウントのリージョン。このオプションは、OpenStack と Rackspace アカウントの場合にのみ必要です。
-tenantid	OpenStack クラウドアカウントの認証に使用する ID。このオプションは、OpenStack アカウントの場合にのみ必要です。
-authurl	OpenStack クラウドアカウントの認証に使用する URL。このオプションは、OpenStack アカウントの場合にのみ必要です。

例：

アクセスキー「akey」と秘密キー「skey」を持つ、「Amazon S3 Account」という名前の新しいクラウドアカウントを追加します。

```
>cmdutil /newcloudaccount -displayname "Amazon S3 Account" -type amazon -username akey -key skey
```

OpenDvmRepository

このコマンドを使用して、AppAssure Core または Rapid Recovery Core で作成された既存の DVM リポジトリ全体を開きます。

使用法：

コマンドの使用法を次に示します。

```
/opendvmrepository -localpath [local path] -sharepath [network share path] -shareusername [user name for network share] -sharepassword [network share password]
```

コマンドオプション

次の表は、OpenDvmRepository コマンドで使用できるオプションを説明しています。

表 193. OpenDvmRepository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-localpath	ローカルの Core 上の DVM リポジトリのあるフォルダへのパスです。
-sharepath	CIFS 共有上の DVM リポジトリのあるフォルダへのパスです。
-shareusername	共有フォルダへのログインに使用するユーザー名です。
-sharepassword	共有フォルダへのログインに使用するパスワードです。

例：

ローカルマシン上で既存の DVM リポジトリを開きます。

```
>cmdutil /opendvmrepository -localpath E:\Repository
```

Pause

管理者は、スナップショットの一時停止、仮想マシンへのエクスポート、または Core のレプリケートができます。pause コマンドは、snapshot、vmexport、および replication の 3 つのパラメータを受け入れます。指定できるパラメータは 1 つのみです。time パラメータを指定すれば、スナップショットを一定時間一時停止できます。

ユーザーは、次の3つの方法でレプリケーションを一時停止できます。

- すべての保護されたマシンのソースコア上です。(-[outgoing])。
管理者は、送信レプリケーションのペア設定を使用してリモートマシン名を指定し、ソース Core 上の送信レプリケーションを一時停止する必要があります。

```
>cmdutil /pause replication /o 10.10.12.10
```

- 1台の保護対象マシンのソースコア上 (-protectedserver) :

```
>cmdutil /pause replication /protectedserver 10.10.12.97
```

- ターゲット Core 上 (-incoming)。

ローカル Core がターゲット Core の場合、管理者は incoming パラメータでソース Core を指定して、レプリケーションを一時停止できます。

```
>cmdutil /pause replication /i 10.10.12.25
```

使用法：

コマンドの使用法を次に示します。

```
/pause [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

コマンドオプション

次の表は、pause コマンドで使用できるオプションを説明しています。

表 194. Pause コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-pause	[snapshots]、[replication] または [vmexport]。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	省略可能。選択した Core 上のすべての Agent を一時停止します。
-protectedserver	省略可能。現在の保護対象サーバーを一時停止します。
-incoming	省略可能。Core マシンにレプリケートするリモート Core のホスト名。
-outgoing	省略可能。データがレプリケートされるリモートターゲット Core のホスト名。
-time	省略可能。スナップショットを再開する時間。「Day-Hours-Minutes」形式で指定 (スナップショットが一時停止している場合のみ)。

例：

特定の保護対象サーバーのスナップショット作成を一時停止します。

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -  
protectedserver 10.10.10.4
```

保護対象マシンのスナップショット作成を一時停止し、3 日、20 時間、50 分後に再開します。

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -  
protectedserver 10.10.10.4 -time 3-20-50
```

Core 上のすべての保護対象マシンの仮想マシンへのエクスポートを一時停止します。

```
>cmdutil /pause vmexport -core 10.10.10.10 /user administrator -password 23WE@#$sdd -all
```

特定の保護対象マシンの Core 上の送信レプリケーションを一時停止します。

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -  
protectedserver 10.10.1.76
```

ターゲット Core 上のすべての保護対象マシンの送信レプリケーションを一時停止します。

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password -23WE@#$sdd -  
outgoing 10.10.1.63
```

ターゲット Core 上のすべてのマシンの受信レプリケーションを一時停止します。

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -  
incoming 10.10.1.82
```

Protect

protect コマンドは、Core によりプロテクション下にあるサーバを追加します。

使用法：

コマンドの使用法を次に示します。

```
/protect -core [host name] -user [user name] -password [password] -repository [name] -agentname  
[name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -  
volumes [volume names]
```

コマンドオプション

次の表は、protect コマンドで使用できるオプションを説明しています。

表 195. Protect コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-repository	保護対象マシンのデータの保存先となる Core 上のリポジトリ名。名前は二重引用符で囲む必要があります。
-agentname	保護対象サーバーの名前または IP アドレス。
-agentusername	保護対象サーバーに対するユーザー名。
-agentpassword	保護対象サーバーに対するパスワード。
-agentport	保護対象サーバーのポート番号。
-volumes	保護するボリュームのリスト。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。例：“c:” “d:”。

例：

Core でサーバーの特定のボリュームを保護します。

```
>cmdutil /protect -core 10.10.10.10 -username administrator -password 23WE@#sdd -repository "Repository 1" -agentname 10.10.9.120 -agentport 5002 -agentusername administrator agentpassword 12345 -volumes "c:" "d:"
```

ProtectCluster

protectcluster コマンドは、Core で保護されるクラスタを追加します。

使用法：

コマンドの使用法を次に示します。

```
/protectcluster -core [host name] -user [user name] -password [password] -repository [name] -clustername [name | IP address] -clusterusername [user name] -clusterpassword [password] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes collection]
```

コマンドオプション

次の表は、protectcluster コマンドで使用できるオプションを説明しています。

表 196. ProtectCluster コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-repository	保護対象マシンのデータの保存先となる Core 上のリポジトリ名。名前は二重引用符で囲む必要があります。
-clustername	保護対象クラスタの名前または IP アドレス。
-clusterusername	保護対象クラスタに対するユーザー名。
-clusterpassword	保護対象クラスタに対するパスワード。
-clusterport	保護対象クラスタサーバーのポート番号。
-clustervolumes	保護するボリュームのリスト。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。例：“c:” “d:”。
-clusternodes	各ノードで保護するクラスタノードとボリュームのリスト。

例：

Core でクラスタサーバーの特定のボリュームを保護します。

```
>cmdutil /protectcluster -core 10.10.10.10 -username administrator -password 23WE@#sdd -
repository "Repository 1" -clustername 10.10.8.150 -clusterport 8006 -clusterusername
clusterAdmin clusterpassword password -volumes "C:\ClusterStorage\Volumel" -clusternodes
nodeName 10.10.8.150 volumes "c:" nodeName 10.10.8.151 volumes "c:"
```

ProtectEsxServer

VMware ESX (i) 仮想マシンの保護を追加するたびに protectesxserver コマンドを使用することができます。

使用法：

コマンドの使用法を次に示します。

```
/protectesxserver -core [host name] -user [user name] -password [password] -repository
[repository name] -server [name | IP address] -serverusername [user name] -serverpassword
[password for server login] -serverport [port] -virtualMachines [virtual machines collection |
all] -autoProtect [object ID or name collection]
```

コマンドオプション

次の表は、protectesxserver コマンドで使用できるオプションを説明しています。

表 197. ProtectEsxServer コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-repository	必須。仮想マシンを保護するために使用する Core に関連付けられているリポジトリの名前。 ① メモ: 名前を二重引用符で囲む必要があります。
-server	保護する vCenter または ESXi サーバの名前または IP アドレス。
-serverusername	保護する vCenter または ESXi サーバにログインするためのユーザー名。
-serverpassword	保護する vCenter または ESXi サーバにログインするためのパスワード。
-serverport	省略可能。保護する vCenter または ESXi サーバのポート番号。
-virtualmachines	省略可能。このオプションを使用して、保護する仮想マシンを一覧表示します。
-autoprotect	省略可能。このオプションを使用して、自動的に保護する新しい仮想マシンを一覧表示します。

例 :

Core を使用して vCenter または ESXi サーバから特定の仮想マシンを保護します。

```
>cmdutil /protectesxserver -core 10.10.10.10 -user admin -password password -repository "Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root -serverpassword password -virtualmachines "VM1" "VM2" -autoprotect "Folder1"
```

RemoveAgent

RemoveAgent コマンドでは、Core の保護から保護対象マシンを削除したり、必要に応じて、削除したマシンのリカバリポイントを削除したりできます。リカバリポイントを削除しないと、Rapid Recovery でリカバリポイントが保持されて、リカバリポイントのみのマシンとしてラベル表示されます。

使用法 :

コマンドの使用法を次に示します。

```
/removeagent -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -deleterecoverypoints
```

コマンドオプション

次の表は、RemoveAgent コマンドで使用できるオプションを説明しています。

表 198. RemoveAgent コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	保護から削除するサーバーの名前または IP アドレス。
-deleterecoverypoints	省略可能。削除するマシンのすべてのリカバリポイントを削除します。

例：

保護からマシンを削除し、関連付けられたリカバリポイントを削除します。

```
>cmdutil /removeagent -protectedserver 10.10.1.1 -deleterecoverypoints
```

RemoveArchiveRepository

removearchiverepository コマンドを使用して Rapid Recovery Core からリポジトリを削除できます。

使用法：

コマンドの使用法を次に示します。

```
/removearchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name]
```

コマンドオプション

次の表は、removearchiverepository コマンドで使用できるオプションを説明しています。

表 199. RemoveArchiveRepository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	必須。アーカイブリポジトリの名前。

例 :

ローカルコアから "NewArchive" というリポジトリを削除します。

```
>cmdutil /removearchiverepository -name NewArchive
```

RemovePoints

removepoints コマンドでは、保護対象マシンの特定のリカバリポイントを削除できます。

使用法 :

コマンドの使用法を次に示します。

```
/removepoints -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

コマンドオプション

次の表は、removepoints コマンドで使用できるオプションを説明しています。

表 200. RemovePoints コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-protectedserver	リカバリポイントを削除するサーバーの名前または IP アドレス。
-rpn	省略可能。削除するリカバリポイントの連番（番号を取得するには /list rps コマンドを使用）。1つのコマンドで複数のリカバリポイントを削除するには、複数の番号をスペースで区切って指定します。
-time	省略可能。作成時間を使用して、削除するリカバリポイントを決定します。正確な日時を「mm/dd/yyyy hh:mm tt」形式（「2/24/2012 09:00 AM」など）で指定します。PC で設定されているタイムゾーンでの日時の値を指定します。

例：

番号 5 と 7 のリカバリポイントを削除します。

```
>cmdutil /removepoints -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22 -rpn 5 7
```

RemoveScheduledArchive

既存の Rapid Recovery がスケジュールされた継続的なアーカイブを中断するには、このコマンドを使用します。

使用法：

コマンドの使用法を次に示します。

```
/removescheduledarchive -core [host name] -user [user name] -password [password] name] -all -ids [id | id1 id2]
```

コマンドオプション

次の表は、removescheduledarchive コマンドで使えるオプションを説明しています。

表 201. RemoveScheduledArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	このオプションは、この Core に関連付けられている、スケジュールされたすべてのアーカイブを削除するかどうかを指定します。
-ids	削除対象のスケジュールされた各アーカイブの ID（複数可）をリストするにはこのオプションを使用します。複数の ID はスペースで区切ります。

例：

スケジュールされたすべてのアーカイブを削除します。

```
>cmdutil /removescheduledarchive -all
```

スケジュールされた1つのアーカイブを削除します。

```
>cmdutil /removescheduledarchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

RemoveVirtualStandby

Rapid Recovery コマンドユーティリティで仮想マシンへのデータの連続エクスポートを中断するには、このコマンドを使用します。

使用法：

コマンドの使用法を次に示します。

```
/removevirtualstandby -core [host name] -user [user name] -password [password login] -  
protectedserver [name] | -all
```

コマンドオプション

次の表は、removevirtualstandby コマンドで使用できるオプションを説明しています。

表 202. RemoveVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	仮想マシンの名前またはスペースで区切られた名前。
-all	このコマンドは、スケジュールされたすべての仮想エクスポートを削除するかどうかを指定します。

例：

すべての仮想スタンバイエクスポートを削除します。

```
>cmdutil /removevirtualstandby -all
```

2 台のマシンの仮想スタンバイエクスポートを削除します。

```
>cmdutil /removevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

レプリケート

Replicate コマンドを使用して、2 つの Rapid Recovery Core の間のレプリケーションを設定します。

使用法：

コマンドの使用法を次に示します。

```
/replicate -request [email | email customer ID] -targetserver [host name | hostname port |  
hostname user name password | hostname port user name password] -replicationname [name] -  
seeddrive [localpath | network path username password] [comment] -protectedserver [name | name  
repository]
```

コマンドオプション

次の表は、Replicate コマンドで使用できるオプションを説明しています。

表 203. Replicate コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-request	省略可能。オフサイトバックアップとディザスタリカバリサービスを提供するサードパーティに対するサブスクリプションを使用する場合は、このオプションを指定します。
-targetserver	レプリケーションを確立するサーバの名前。次のようなパラメーターがあります。 ・ ポート ・ ユーザー名 ・ password ポートパラメーターはオプションです。デフォルト値は 8006 です。request オプションを使用する場合は、ターゲットサーバのユーザー名とパスワードも使用する必要があります。
-replicationname	省略可能。request オプションを使用しない場合は、レプリケーションジョブの名前を使用します。
-seeddrive	省略可能。このオプションを使用して、初期データ転送用のシードドライブを指定します。コメントパラメーターは省略可能です。

オプション	説明
-protectedserver	レプリケートする保護対象マシンのリスト。request オプションを使用する場合は、保護対象マシンの名前または IP アドレスのみをリストします。それ以外の場合は、保護対象マシンと対応するリモートリポジトリ名の両方をリストします。

例：

2つの保護対象マシンをリモート Core へネットワーク共有からシードドライブを使用してレプリケートします。

```
>cmdutil /replicate -targetserver 10.10.1.100 Administrator 123Q -replicationname ReplicationName -seeddrive Network \\10.10.1.100\seeddrive Administrator 123Q -protectedserver 10.10.1.1 Repository1 10.10.1.2 Repository2
```

レプリケーション

replication コマンドを使用して、2つの Rapid Recovery Core 間の既存のレプリケーションをコントロールし、保留されているレプリケーションリクエストを管理します。

① **メモ:** このコマンドは、**Replicate** コマンドの後継であり、**Core** 間のペアリングと呼ばれる接続を確立し、最初のデータ転送用のシードドライブを使用します。このコマンドの詳細については、「**レプリケート**」を参照してください。

使用法：

コマンドの使用法を次に示します。

```
/replication [-list [incoming | outgoing | pending] -accept | -deny | -ignore | -delete | -edit] -id [replication ID] -protectedserver [name | name repository] -responsecomment [comment] -deleterecoverypoints -scheduletype [type] -dailystarttime [time] -dailyendtime [time] -weekdaystarttime [time] -weekdayendtime [time] -weekendstarttime [time] -weekendendtime [time]
```

コマンドオプション

次の表は、replication コマンドで使用できるオプションを説明しています。

表 204. Replication コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-list	入力または出力方向のレプリケーションジョブまたは保留中のレプリケーションのリクエストのリスト。
-accept	レプリケーションリクエスト受け入れます。

オプション	説明
-deny	レプリケーションリクエストを拒否します。
-ignore	レプリケーションリクエストを無視します。
-delete	既存のレプリケーションジョブまたはマシンをレプリケーションジョブから削除するには、このオプションを使用します。-id パラメーターのみを指定してアプリケーション関係全体を削除するか、-id と -protectedserver の両方のパラメーターを指定して特定のマシンのみをレプリケーションから削除します。
-edit	既存のレプリケーションジョブのスケジュールを編集します。
-id	レプリケーションジョブまたは保留中のレプリケーションリクエストの識別子。リモート Core ID、ホスト名、カスタム ID、電子メールアドレス、または保留中のレプリケーションリクエストの ID です。
-protectedserver	レプリケーションリクエストに回答する際に、このオプションを使用して、リポジトリ名または ID を含む保護サーバのリストに回答を適用します。すべてのリクエストされたマシンに回答を適用するには、パラメーター "all" を使用します。
-responsecomment	保留中のレプリケーションリクエストへの回答に表示するコメント。
-deleterecoverypoints	削除されたレプリケートされたマシンから特定のリカバリポイントも削除する必要がある場合は、このオプションを使用します。
-schedulingtype	-edit オプションを使用する場合は、このオプションはレプリケーションスケジュールのタイプを指定します。次の 4 つの値のいずれかの値を指定します。 - atalltimes - 任意の時点で自動的にレプリケートします。 - daily - 日次でレプリケートします。-dailystarttime と -dailyendtime パラメーターを指定します。 - custom - 日次のレプリケーションを使用する場合、この値を使用して平日または週末のレプリケーションをスケジュールします。-weekdaystarttime、-weekdayendtime、-weekendstarttime、および -weekendendtime パラメーターを指定します。
-dailystarttime	-schedulingtype オプションの日次の値にのみ使用します。レプリケーションが行われるときの期間を確立するために使用されます。このオプションを使用して、最も早いレプリケーションの開始時刻を指定します。
-dailyendtime	-schedulingtype オプションの日次の値にのみ使用します。レプリケーションが行われるときの期間を確立するために使用されます。このオプションを使用して、最も遅いレプリケーションの開始時刻を指定します。
-weekdaystarttime	-schedulingtype オプションのカスタム値にのみ使用します。レプリケーションが行われるときの期間を確立するために使用されます。このオプションを使用して、平日の最も早いレプリケーションの開始時刻を指定します。
-weekdayendtime	-schedulingtype オプションのカスタム値にのみ使用します。レプリケーションが行われるときの期間を確立するために使用されます。このオプションを使用して、平日の最も遅いレプリケーションの開始時刻を指定します。
-weekendstarttime	-schedulingtype オプションのカスタム値にのみ使用します。レプリケーションが行われるときの期間を確立するために使用されます。このオプションを使用して、週末の最も早いレプリケーションの開始時刻を指定します。
-weekendendtime	-schedulingtype オプションのカスタム値にのみ使用します。レプリケーションが行われるときの期間を確立するために使用されます。このオプションを使用して、週末の最も遅いレプリケーションの開始時刻を指定します。

例：

すべての入力方向のレプリケーションをリストします。

```
>cmdutil /replication -list incoming
```

2つの保護対象マシンの保留中のレプリケーションリクエストを受け入れます。

```
>cmdutil /replication -accept -id customer@email.address -protectedserver 10.10.1.1 Repository1  
10.10.1.2 Repository2 -responsecomment A response comment
```

保留中のレプリケーションリクエストを拒否します。

```
>cmdutil /replication -deny -id customer@email.address
```

既存のレプリケーションとレプリケートされたリカバリポイントを削除します。

```
>cmdutil /replication -delete -id RemoteServerHostname -deleterecoverypoints
```

既存のレプリケーションから2つのマシンを削除します。

```
>cmdutil /replication -delete -id "156d7a46-8e44-43f4-9ed8-60d998e582bf" -protectedserver  
10.10.1.1 10.10.1.2
```

指定された平日と週末の時刻を使用してレプリケーションを編集します。

```
>cmdutil /replication -edit -id RemoteServerHostName -scheduletype custom -weekdaystarttime  
"9:00 AM" -weekdayendtime "6:00 PM" -weekendstarttime "9:00 AM" -weekendendtime "6:00 PM"
```

RestoreAgent

restoreagent コマンドを使用すると、保護対象マシンまたはボリュームを特定の Rapid Recovery リカバリポイントから復元することができます。

使用法：

コマンドの使用法を次に示します。

```
/restoreagent -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs |  
names | all] -targetmachine [name] -targetvolume [volume name] -forcedismount -autorestart
```

コマンドオプション

次の表は、restoreagent コマンドで使用できるオプションを説明しています。

表 205. RestoreAgent コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	復元対象サーバの名前または IP アドレス。
-rpn	マシンの復元に使用するリカバリポイントの ID 番号。正しい番号を検索するには、/list rps コマンドを使用します。
-volumes	リストアするボリュームの ID または名前。すべての保護ボリュームをリストアするには、-volumes all コマンドを使用します。
-targetmachine	保護対象マシンのリストア先のマシンの名前。
-targetvolume	マシンを復元するボリューム象の名前または ID。
-forcedismount	省略可能。オンデマンドでデータベースのマウント解除を強制するには、このオプションを使用します。
-autorestart	省略可能。Exchange Server マシンの再起動が必要な場合はこのコマンドを使用します。

例：

強制的データベースマウント解除オプションを含め、IP アドレス 192.168.20.130 の保護対象マシンにマシンを復元します。

```
>cmdutil /restoreagent -protectedserver 192.168.20.130 -rpn 259 -volumes "F:" "E:" "C:" -targetmachine 192.168.20.174 -targetvolume "E:" "G:" "F:" -forcedismount
```

RestoreArchive

このコマンドは、ローカルアーカイブまたは共有からアーカイブをリストアし、リストアしたデータを指定したリポジトリ内に配置します。

使用法：

コマンドの使用法を次に示します。

```
/restorearchive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -repository [name] -archiveusername [name] -archivepassword [password] -path [location]
```

コマンドオプション

次の表は、restorearchive コマンドで使用できるオプションを説明しています。

表 206. RestoreArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	アーカイブファイルからすべての保護対象マシンのデータをリストアします。
-protectedserver	リカバリポイントをリストアする保護対象マシン。複数のマシン名を指定するには、二重引用符で囲み、スペースで区切ります。
-repository	リストアしたリカバリポイントの配置先となる Core 上のリポジトリ名。名前は二重引用符で囲む必要があります。
-archiveusername	省略可能。リモートマシンに対するユーザー名。ネットワークパスのみで必要です。
-archivepassword	省略可能。リモートマシンに対するパスワード。ネットワークパスのみで必要です。
-path	アーカイブデータをリストアする場所。パスの例: d:\work\archive、ネットワーク パスの例: \\servername\sharename。

例 :

すべての保護対象サーバーのアーカイブ済みデータをリストアします。

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$$sdd -all -repository repository1 -path d:\work\archive
```

特定の保護対象サーバーのアーカイブ済みデータをリストアします。

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$$sdd -protectedserver "10.10.20.30" "20.10.10.5" -repository repository1 -path d:\work\archive
```

RestoreUrc

restoreurc コマンドを使用すると、Universal Recovery Console (URC) を使用して、保護されたマシンまたはボリュームを特定の Rapid Recovery リカバリポイントからベアメタルマシンにリストアすることができます。

使用法 :

コマンドの使用法を次に示します。

```
/restoreurc -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs | names | all] -targetmachine [IP address] -urcpassword [password from the URC] -targetdisk [disk number | all]
```

コマンドオプション

次の表は、restoreurc コマンドで使用できるオプションを説明しています。

表 207. RestoreUrc コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	URC のリストア先のサーバの名前または IP アドレス。
-rpn	マシンの復元に使用するリカバリポイントの ID 番号。正しい番号を検索するには、/list rps コマンドを使用します。
-volumes	リストアするボリュームの ID または名前。すべての保護ボリュームをリストアするには、-volumes all コマンドを使用します。
-targetmachine	保護対象マシンのリストア先のマシンの名前。
-urcpassword	URC からの認証キー。
-targetdisk	マシンのリストア先のディスクの番号。URC を使用してマシンからすべてのディスクを選択するには、-targetdisk all を使用します。

例：

URC を使用してマシンのディスク 0 と 1 にマシンをリストアします。URC マシンの IP アドレスは 192.168.20.175 です。

```
>cmdutil /restoreurc -protectedserver 192.168.20.130 -rpn 259 -volumes "C:" "E:" -targetmachine 192.168.20.175 -urcpassword ***** -targetdisk 0 1
```

Resume

管理者はこのコマンドを使用して、スナップショット、仮想マシンへのエクスポート、またはレプリケートを再開できます。再開の要求はパラメータで指定する必要があります。有効なパラメータは snapshot、vmexport、および replication です。詳細については、「[Pause](#)」を参照してください。

使用法：

コマンドの使用法を次に示します。

```
/resume [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

コマンドオプション

次の表は、resume コマンドで使用できるオプションを説明しています。

表 208. Resume コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-restore	[snapshots]、[replication] または [vmexport]
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	選択した Core 上のすべての Agent を再開します。
-protectedserver	現在の保護対象サーバーを再開します。
-incoming	Core マシンにレプリケートするリモート Core のホスト名。
-outgoing	データがレプリケートされるリモートターゲット Core のホスト名。

例：

特定の保護対象サーバーのスナップショットを再開します。

```
>cmdutil /resume snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.10.4
```

Core 上のすべての保護対象マシンの仮想マシンへのエクスポートを再開します。

```
>cmdutil /resume vmexport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

特定の保護対象マシンの Core 上の送信レプリケーションを再開します。

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.1.76
```

ターゲット Core 上のすべての保護対象マシンの送信レプリケーションを再開します。

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -outgoing 10.10.1.63
```

ターゲット Core 上のすべてのマシンの受信レプリケーションを再開します。

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#sdd -incoming 10.10.1.82
```

SeedDrive

Rapid Recovery レプリケーションを確立するときに初期データ転送用のシードドライブを使用できます。

使用法：

コマンドの使用法を次に示します。

```
/seeddrive [-list | -startcopy | -startconsume | -abandon] -path [local | network path] -seeddriveusername [user name] -seeddrivepassword [password] -remotecore [name] [-targetcore [name or IP] | -protectedserver [name] | -all] -usecompatibleformat
```

コマンドオプション

次の表は、seeddrive コマンドで利用できるオプションを説明しています。

表 209. SeedDrive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-list	未処理のシードドライブと拡張された情報のリスト。
-startcopy	シードドライブへのデータのコピーを開始します。
-startconsume	シードドライブの消費を開始します。
-abandon	未処理のシードドライブリクエストを破棄します。
-path	シードドライブのローカルまたはネットワークパス。
-seeddriveusername	省略可能。シードドライブのネットワークの場所のユーザー名。
-seeddrivepassword	省略可能。シードドライブのネットワークの場所のパスワード。
-targetcore	省略可能。-copy オプションでのみ使用します。リモート Core の名前または IP アドレス。この Core にレプリケートするすべての保護対象マシンにシードドライブのリカバリポイントが提供されます。

オプション	説明
-remotecore	-consume オプションでのみ使用します。シードドライブのリカバリポイントの作成または消費元になるリモート Core の名前。
-protectedserver	リカバリポイントのシードドライブを作成または消費するために使用する保護対象マシンの名前または IP アドレス。例: -protectedserver "10.10.60.48" "10.10.12.101"
-all	このオプションは、すべての使用可能な保護対象マシンを消費またはコピーするかどうかを指定します。
-usecompatibleformat	新しいアーカイブ形式では、パフォーマンスが向上しますが、古い Core との互換性はありません。レガシーの AppAssure Core で作業する際にこのオプションを使用します。

例 :

未処理のシードドライブをリストします。

```
>cmdutil /seeddrive -list
```

2 つの保護対象マシンをネットワーク共有上のシードドライブにコピーします。

```
>cmdutil /seeddrive -startcopy -remotecore TargetCoreName -path \\10.10.1.1\Share\Seed\ -seeddriveusername Administrator -seeddrivepassword 12345 -usecompatibleformat
```

シードドライブの消費を開始します。

```
>cmdutil /seeddrive -startconsume -path \\10.10.1.1\Share\Seed\ -seeddriveusername Adminsitator -seeddrivepassword 12345 -remotecore RemoteCoreName
```

未処理のシードドライブリクエストを破棄します。

```
>cmdutil /seeddrive -abandon RemoteCoreHostName
```

StartExport

startexport コマンドは、保護対象マシンから仮想サーバへの 1 回限りのデータのエクスポートを強制実行します。ESXi、VMware Workstation、Hyper-V、または VirtualBox 仮想マシンにエクスポートできます。ESXi にエクスポートする場合、シックまたはシンディスクプロビジョニングを指定する必要があります。

使用法 :

コマンドの使用法を次に示します。

```
/startexport -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -volumes [volume names] -rpn [recovery point number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual hostport number] -hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocalmachine]
```

コマンドオプション

次の表は、startexport コマンドで利用できるオプションを説明しています。

表 210. StartExport コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-exporttype	保護対象サーバーから ESXi サーバー（「esxi」）、VMware Workstation サーバー（「vmj」）、Hyper-V サーバー（「hyperv」）、または VirtualBox サーバー（「vb」）へのデータのエクスポートを実行します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	リカバリポイントをエクスポートする保護対象マシン。
-volumes	省略可能。エクスポートするボリューム名のリスト。指定しない場合は、すべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。例: "c:" "d:"。ボリューム名の末尾にスラッシュを使用しないでください。
-rpn	省略可能。エクスポートするリカバリポイントの連続する番号（Get-RecoveryPoints コマンドを使用して番号を取得）。「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-time	省略可能。エクスポートに選択されるリカバリポイントを決定します。正確な日時を「mm/dd/yyyy hh:mm tt」形式（「2/24/2012 09:00 AM」など）で指定する必要があります。PC で設定されているタイムゾーンでの日時の値を指定します。注: 「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-vmname	仮想マシンの Windows 名。
-hostname	ESXi および Hyper-V 仮想エクスポートのみで使用するオプション。仮想サーバーのホスト名。
-linuxhostname	VirtualBox エクスポートのみで使用するオプション。仮想サーバーのホスト名。
-hostport	ESXi および Hyper-V 仮想エクスポートのみで使用するオプション。仮想サーバーのポート番号。
-hostusername	ESXi および Hyper-V 仮想エクスポートのみで使用するオプション。仮想サーバーホストに対するユーザー名。
-hostpassword	ESXi および Hyper-V 仮想エクスポートのみで使用するオプション。仮想サーバーホストに対するパスワード。
-ram	このオプションを使用して、仮想サーバ上に特定の容量の RAM を割り当てます。
-usesourceram	省略可能。このオプションを使用して、ソースマシンに含まれる仮想サーバに同じ容量の RAM を割り当てます。
-diskprovisioning	ESXi エクスポートでのみ使用するオプション。省略可能。仮想マシンに割り当てるディスク容量。次の 2 つのいずれかの仕様を使用します。 - Thick - この仕様は、仮想ディスクを保護対象マシン上の元のドライブと同じ大きさにします。 - Thin - この仕様は、元のドライブで使用されている実際のディスク容量に数メガバイト追加して割り当てます。 デフォルトの仕様は "thin" です。

オプション	説明
-diskmapping	ESXi エクスポートでのみ使用するオプション。省略可能。このオプションは、保護対象マシンから仮想マシンへのディスクのマッピング方法を決定します。次のいずれかの値を選択します。 ・ auto - この値を選択すると、ディスクが自動的にマッピングされます。 ・ manual - この値を使用して、ディスクを手動でマッピングすることができます。 ・ withvm - この値を選択すると、選択したデータストア内に仮想ディスクが格納されます。 デフォルト値は "auto" です。
-targetpath	VMware Workstation または VirtualBox へのエクスポートのみで使用するオプション。このオプションでは、仮想マシンファイルを格納するフォルダのローカルまたはネットワークパス、または Linux パス (VirtualBox の場合のみ) を指定します。
-pathusername	VMware Workstation のエクスポートのみで使用するオプション。これはネットワークマシンのユーザー名です。-targetpath オプションでネットワークパスを指定した場合にのみ必要です。
-pathpassword	VMware Workstation のエクスポートのみで使用するオプション。ネットワークパスのパスワードです。-targetpath オプションでネットワークパスを指定した場合にのみ必要です。
-uselocalmachine	Hyper-V エクスポートのみで使用するオプション。省略可能。このコマンドを使用して、ローカル Hyper-V サーバに接続します。このオプションでは、-hostname、-hostport、-hostusername、および -hostpassword オプションは無視されます。

例：

特定の名前、およびソース保護対象サーバーと同じ量の RAM とディスクサイズの ESXi 仮想マシンにデータをエクスポートします。

```
>cmdutil /startexport -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@# $sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

リカバリポイント 4 の保護対象データを使用して、ローカルドライブに VMware Workstation マシンファイルを作成します。

```
>cmdutil /startexport -exporttype vmstation -core 10.10.10.10 -user administrator -password 23WE@# $sdd -protectedserver 10.10.5.22 -rpn 4 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```

リモートマシンで保存される Hyper-V マシンファイルを作成します。

```
>cmdutil /startexport -exporttype hyperv -core 10.10.10.10 -user administrator -password 23WE@# $sdd -protectedserver 10.10.5.22 -vmlocation \\WIN7-Bobby\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword 12QWsdxc@# -ram 4096
```

UpdateRepository

updaterepository コマンドは、既存のリポジトリに新しいストレージの場所を追加します。

使用法：

コマンドの使用法を次に示します。

```
/updaterepository -name [repository name] -size [size of the repository] [-datapath [data path] -metadatapath [metadata path] | [-uncpath [UNC path] -shareusername [share user name] -sharepassword [share password] -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、`updaterepository` コマンドで使用できるオプションを説明しています。

表 211. `UpdateRepository` コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-name	リポジトリ名。
-size	リポジトリストレージの場所のサイズ。使用できる単位は b、Kb、Mb、Gb、Tb、Pb です。
-datapath	ローカルの場合のみ。リポジトリストレージの場所のデータパスを決定します。
-metadatapath	ローカルの場合のみ。リポジトリストレージの場所のメタデータパスを決定します。
-uncpath	共有の場合のみ。リポジトリストレージの場所のデータおよびメタデータパスを決定します。
-shareusername	共有の場合のみ。場所を共有するためのユーザー名を決定します。
-sharepassword	共有の場合のみ。場所を共有するためのパスワードを決定します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

ローカル DVM リポジトリに新しいストレージの場所を作成します。

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -datapath d:\repository -  
metadatapath d:\repository -core 10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

共有の場所に DVM リポジトリ用のストレージ場所を作成します。

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -uncpath \\share\repository -  
shareusername login -sharepassword 23WE@#$sdd -core 10.10.10.10:8006 -username administrator -  
password 23WE@#$sdd
```

バージョン

`version` コマンドでは、指定したサーバにインストールされている Rapid Recovery ソフトウェアのバージョンに関する情報が表示されます。Core サーバーまたは保護対象サーバーを指定しない場合、現在作業している Core に関する情報が返されます。

使用法：

コマンドの使用法を次に示します。

```
/[version | ver] -protectedserver [name | IP address]
```

コマンドオプション

次の表は、version コマンドで使用できるオプションを説明しています。

表 212. Version コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	省略可能。バージョン情報を表示する保護対象マシン。保護対象マシンを指定しない場合、作業している Core マシンに関する情報が返されます。

例：

現在の Rapid Recovery Core にインストールされている Rapid Recovery のバージョンに関する情報が表示されます。

```
>cmdutil /version
```

VirtualStandby

virtualstandby コマンドを使用すると、Rapid Recovery で保護されたマシンから互換性のある仮想マシンにデータをエクスポートすることができます。

使用法：

コマンドの使用法を次に示します。

```
/virtualstandby -edit -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -volumes [volume names] -vmname [virtual machine name] -gen2 -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocal machine] -initialexport
```

コマンドオプション

次の表は、virtualstandby コマンドで利用できるオプションを説明しています。

表 213. VirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-exporttype	このオプションは、保護対象マシンから次のいずれかの指定された仮想サーバにデータをエクスポートします。 • esxi (ESXi) • vm (VMware Workstation) • hyperv (Hyper-V) • vb (VirtualBox)
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	リカバリポイントをエクスポートする保護対象マシンを指定するには、このオプションを使用します。
-volumes	省略可能。エクスポートするボリュームの名前を一覧表示するには、このオプションを使用します。ボリュームを指定しない場合、リカバリポイント内のすべてのボリュームがエクスポートされます。値を二重引用符で囲み、スペースで区切ります (例: "c:" "d:"). ボリューム名の末尾にスラッシュを使用しないでください。
-ram	このオプションを使用して、仮想サーバ上に特定の容量の RAM を割り当てます。
-usesourceram	省略可能。このオプションを使用して、ソースマシンに含まれる仮想サーバに同じ容量の RAM を割り当てます。
-vmname	仮想マシンの Windows 名。
-gen2	省略可能。このオプションは、第 2 世代の VM サーバを指定します。世代を指定しない場合、コマンドで第 1 世代が使用されます。次のオペレーティングシステムでは、第 2 世代がサポートされます。 • Windows • Windows Server 2012 R2 • Windows 8.1 • Ubuntu Linux • CentOS • RHEL • Oracle Linux 7
-hostname	ESXi および Hyper - V 仮想エクスポートのみで使用するオプション。仮想サーバーのホスト名。
-linuxhostname	VirtualBox エクスポートのみで使用するオプション。仮想サーバーのホスト名。

オプション	説明
-hostport	ESXi および Hyper - V 仮想エクスポートのみで使用するオプション。仮想サーバーのポート番号。
-hostusername	ESXi および Hyper - V 仮想エクスポートのみで使用するオプション。仮想サーバホストに対するユーザー名。
-hostpassword	ESXi および Hyper - V 仮想エクスポートのみで使用するオプション。仮想サーバホストに対するパスワード。
-diskprovisioning	ESXi エクスポートのみで使用するオプション。省略可能。仮想マシンに割り当てるディスク容量。次の2つのいずれかの仕様を使用します。 - Thick - この仕様は、仮想ディスクを保護対象マシン上の元のドライブと同じ大きさにします。 - Thin - この仕様は、元のドライブで使用されている実際のディスク容量に数メガバイト追加して割り当てます。 デフォルトの仕様は "thin" です。
-diskmapping	ESXi エクスポートのみで使用するオプション。省略可能。このオプションは、保護対象マシンから仮想マシンへのディスクのマッピング方法を決定します。次のいずれかの値を選択します。 - auto - この値を選択すると、ディスクが自動的にマップされます。 - manual - この値を使用すると、ディスクを手動でマップすることができます。 - withvm - この値を選択すると、選択したデータストア内に仮想ディスクが格納されます。 デフォルト値は "auto" です。
-targetpath	VMware Workstation または VirtualBox へのエクスポートのみで使用するオプション。このオプションでは、仮想マシンファイルを格納するフォルダのローカルまたはネットワークパス、または Linux パス (VirtualBox の場合のみ) を指定します。
-pathusername	VMware Workstation のエクスポートのみで使用するオプション。これはネットワークマシンのユーザー名です。-targetpath オプションでネットワークパスを指定した場合にのみ必要です。
-pathpassword	VMware Workstation のエクスポートのみで使用するオプション。ネットワークパスのパスワードです。-targetpath オプションでネットワークパスを指定した場合にのみ必要です。
-uselocalmachine	Hyper-V エクスポートのみで使用するオプション。省略可能。このコマンドを使用してローカルの Hyper-V サーバに接続します。このオプションでは、-hostname、-hostport、-hostusername、および -hostpassword オプションは無視されます。
-edit	省略可能。このオプションを使用すると、既存の仮想マシンを編集できます。-exporttype と -initialexport オプションは無視します。
-initialexport	省略可能。このオプションは、継続的な仮想スタンバイを設定した後に、オンデマンドの最初の仮想マシンのエクスポートを開始するかどうかを指定します。

例：

ソースの保護サーバの名前、RAM の容量、ディスクサイズを使用して、ESXi 仮想マシンへの仮想スタンバイのエクスポートをセットアップします。

```
>cmdutil /virtualstandby -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@#
$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -
hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

ローカルドライブ上の VMWare Workstation マシンのファイルに Virtual Standby のエクスポートをセットアップします。

```
>cmdutil /virtualstandby -exporttype vm -core 10.10.10.10 -user administrator -password 23WE@#  
$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```

Hyper-V マシンのファイルに仮想スタンバイのエクスポートをセットアップし、それらをリモートマシンに保存します。

```
>cmdutil /virtualstandby -exporttype hyperv -core 10.10.10.10 -user administrator -password  
23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -vmlocation \\WIN7-Bobby  
\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword  
12QWsdxc@# -ram 4096
```

ローカライゼーションローからいぜーしょん

Rapid Recovery Core がインストールされているマシンで Rapid Recovery Command Line Management ユーティリティを実行すると、その表示言語は、Rapid Recovery Core で設定されている言語がベースになります。本リリースでは、英語、中国語（簡体字）、フランス語、韓国語、ドイツ語、日本語、ポルトガル語（ブラジル）、スペイン語がサポートされます。

Rapid Recovery Command Line Management ユーティリティが別のマシンにインストールされている場合、英語のみがサポートされます。

Core Console リファレンス

この付録には、Rapid Recovery Core Console で使用可能な機能およびアイコンの多くを説明する参照表があります。これは『[Dell Data Protection | Rapid Recovery ユーザーガイド](#)』の「Dell Data Protection | Rapid Recovery」の章を補完するものです。

トピック：

- Core Console ユーザーインターフェースの表示
- Protected Machines（保護されたマシン）ペインの表示

Core Console ユーザーインターフェースの表示

Core Console は、ユーザーが Rapid Recovery とやり取りするために使用するメイン UI です。Rapid Recovery Core Console にログインすると、次のエレメントが表示されます。

表 214. Core Console の UI エレメント

UI エレメント	説明
「ブランド設定」エリア	一般的な環境では、Core Console の左上部にはデルのロゴなど、完全な製品名が表示されます。製品名領域の任意の場所をクリックすると、Web ブラウザで新しいタブが開き、サポート Web サイトの製品マニュアルが表示されます。
ボタンバー	ボタンバーは製品名領域の右側に表示され、Core Console の任意の場所からアクセス可能なボタンが含まれています。これらのボタンから、マシンの保護、リカバリポイントからのリストアの実行、アーカイブの作成、アタッチ、またはインポート、このソース Core からターゲット Core へのレプリケーションなどの一般的なタスクを達成するためのウィザードが起動されます。 ボタンバーの各ボタンは「 表 215. ボタンバーのボタンとメニュー 」テーブルでさらに説明されています。
実行中のタスク数	現在実行されているジョブの数が表示されます。この値は、システムの状態に基づいて動的に変化します。ドロップダウンメニューをクリックすると、現在実行中のすべてのジョブのステータスサマリが表示されます。いずれかのジョブの X をクリックして、そのジョブをキャンセルすることができます。
ヘルプのドロップダウンメニュー	このヘルプメニューは、次のオプションで構成されています。 ヘルプ：製品内ヘルプへのリンクであり、別のブラウザウィンドウで開きます。 マニュアル。デルサポート Web サイトの Rapid Recovery 技術文書にリンクしています。 サポート。ライブチャット、ビデオチュートリアル、Rapid Recovery ナレッジベース記事、FAQ などを提供するデルサポート Web サイトにリンクしています。 クイックスタートガイド。「クイックスタートガイド」は、Rapid Recovery を設定および使用する際に推奨されるタスクの流れをガイド付きで表示します。この機能を無効にしていない場合、Core Console にログインするたびにこのガイドが自動的に開きます。ヘルプメニューから「クイックスタートガイド」を開くこともできます。「クイックスタートガイド」の詳細については、「クイックスタートガイドについて」を参照してください。 バージョン情報：バージョン情報とソフトウェアの説明が記載されている、Dell Data Protection Rapid Recovery Core バージョン情報 ダイアログボックスが開きます。
サーバーの日時	Rapid Recovery Core サービスを実行しているマシンの現在の日時が Core Console の右上に表示されます。時間にマウスポインタを合わせると、サーバ日付も表示されます。これは、システムによって記録されたイベント（ロ

UI エLEMENT 説明

グ、スケジュール、レポートなど)の日付と時間です。たとえば、保護スケジュールを適用する場合、Core Console に表示されている時間が使用されます。データベースサーバーや、ブラウザが実行しているクライアントマシンでタイムゾーンが異なる場合も、Core Console に表示されている時間が適用されます。

アイコンバー アイコンバーには、Core Console でアクセス可能な主要機能のアイコンが表示されます。それは、ユーザーインターフェイス (UI) の左側に、製品名領域のすぐ下に表示されます。アイコンバーの該当のアイテムをクリックすると、UI の対応するセクションに移動し、その機能を管理できます。
アイコンバーにある各アイコンは、さらに「[表 216. アイコンバー](#)」テーブルで説明されています。

左側のナビゲーションエリア 左のナビゲーション領域は、アイコンバーの下にあるユーザーインターフェイスの左側に表示されます。

- ・ 左のナビゲーション領域には、テキストフィルタおよび保護対象マシン メニューが表示されます。
- ・ レプリケーションをこの Core に追加している場合、このエリアには レプリケートされたマシン メニューが表示されます。
- ・ マシンが保護から削除されたが、そのリカバリポイントは保存されている場合、このエリアには リカバリポイントのみ メニューが表示されます。
- ・ カスタムグループを追加している場合、このエリアには カスタムグループ メニューが表示されます。
- ・ アーカイブをアタッチしている場合は、この領域に アタッチされたアーカイブ メニューが表示されます。

左側のナビゲーションエリアの表示は、オンとオフを切り替えることができます。これは、UI のメインナビゲーションエリアでより多くの内容を表示する必要がある場合に便利です。このセクションを非表示にするには、左側のナビゲーションエリアとメインナビゲーションエリアの間にある灰色の境界線をクリックします。この UI エLEMENT をもう一度表示するには、灰色の境界線を再度クリックします。

左側のナビゲーション領域にある各ELEMENTについては、さらに「[表 218. 左のナビゲーション領域およびメニュー](#)」テーブルで説明されています。

コンテキスト
依存のヘルプ



Rapid Recovery Core Console から、ヘルプアイコン (青い疑問符) をクリックするたびに、サイズ変更可能な 2 つのフレームで構成されるブラウザウィンドウが開きます。左のフレームには、『Dell Rapid Recovery ユーザーガイド』のトピックを表示するナビゲーションツリーが表示されています。右のフレームには、選択したヘルプトピックの内容が表示されます。ヘルプナビゲーションツリーを展開すると、いつでも、選択したトピックの階層の場所が表示されます。このコンテキスト依存のヘルプの機能を使用すると、すべてのユーザーガイドのトピックを参照できます。トピックの参照が終了したら、ブラウザを閉じます。
ヘルプ メニューの ヘルプ オプションからヘルプを開くこともできます。

ボタンバー

ボタンバーの詳細について、次の表に示します。

表 215. ボタンバーのボタンとメニュー

UI ELEMENT 説明

ボタンバー:保護
ボタンとメ
ニュー



保護 ボタンを使用して、マシンの保護 ウィザードを開始し、Rapid Recovery Core の 1 つのマシンを保護できます。また、他の保護オプションは、このボタンの横にあるドロップダウンメニューからアクセスできます。次のオプションがあります。

- ・ **マシンの保護** オプションを使用して、マシンの保護 ウィザードを開始し、1 つのマシンを保護することもできます。
- ・ **クラスタを保護** オプションでは、サーバクラスタに接続できます。
- ・ **複数のマシンを保護** オプションにより、複数のマシンの保護ウィザードが開き、複数のマシンを同時に保護することができます。

- ・ **Agent ソフトウェアの展開** オプションにより、Rapid Recovery Agent ソフトウェアを1つまたは複数のマシンに同時にインストールすることができます。この機能では Agent ソフトウェアの導入 ウィザードが使用されます。

ボタンバー: 復元ボタンとメニュー



保護 ボタンを使用して、マシンのリストア ウィザードを開き、保護対象マシンから保存されたリカバリポイントからデータをリストアできます。

また、他の復元またはエクスポートオプションは、このボタンの横にあるドロップダウンメニューからアクセスできます。次のオプションがあります。

- ・ **マシンをリストア** オプションを使用して、マシンをリストア ウィザードを開始し、データをリストアすることもできます。
- ・ **リカバリポイントをマウント** オプションにより、マウント ウィザードが起動し、保護対象マシンからのリカバリポイントをマウントすることができます。
- ・ **VMのエクスポート** オプションを使用すると、エクスポート ウィザードが開きます。このウィザードでは、Rapid Recovery Core で保存されたリカバリポイントから仮想マシンを作成できます。1回限りのエクスポートを作成することも、保護対象マシンの各スナップショットの後に継続的にアップデートされる VM のパラメータを定義することもできます。

ボタンバー: アーカイブボタンとメニュー



アーカイブ ボタンを使用すると、アーカイブ ウィザードが開きます。このウィザードから、選択したリカバリポイントからの1回限りのアーカイブを作成するか、またはアーカイブを作成し、定義したスケジュールに基づいてそのアーカイブに継続的に保存することができます。

また、他のアーカイブオプションは、このボタンの横にあるドロップダウンメニューからアクセスできます。次のオプションがあります。

- ・ または、**アーカイブを作成** オプションを使用し、アーカイブを作成 ウィザードを起動して1回限りのアーカイブを作成するか継続的にアーカイブすることもできます。
- ・ **アーカイブのインポート** オプションを使用すると、アーカイブのインポート ウィザードが起動し、アーカイブをインポートすることができます。
- ・ **アーカイブのアタッチ** オプションを使用すると、ファイルシステムとして内容を読み取ることができるようにアーカイブがマウントされます。

ボタンバー: レプリケーションボタン



レプリケーション ボタンを使用すると、レプリケーション ウィザードが開きます。このウィザードからは、ターゲット Core を指定し、ソース Core で保護されているマシンを選択し、選択したマシンから指定したレポジトリ内のターゲット Core にリカバリポイントを複製することができます。

定義するときにレプリケーションを一時停止するか、またはすぐにレプリケーションを開始することもできます。

また、既存のリカバリポイントのデータをターゲット Core にコピーするためにシードドライブを使用するかどうかを指定することができます。

アイコンバー

アイコンバーの詳細について、次の表に示します。

表 216. アイコンバー

UI エlement	説明
アイコンバー	アイコンバーには、Core Console でアクセス可能な主要機能のアイコンが表示されます。該当のアイテムをクリックすると、ユーザーインターフェースの対応するセクションに移動し、その機能を管理できます。アイコンバーには次のようなアイコンが表示されます。
アイコンバー: ホームアイコン	 ホーム。 Core のホームページに移動するには、ホームアイコンをクリックします。
アイコンバー: レプリケーションアイコン	 レプリケーション: 送受信レプリケーションを表示または管理するには、レプリケーションアイコンをクリックします。
アイコンバー: Virtual Standbyアイコン	 Virtual Standby: リカバリポイントの情報をブート可能な仮想マシンにエクスポートするには、Virtual Standby アイコンをクリックします。
アイコンバー: イベントアイコン	 イベント。 Rapid Recovery Core に関連するすべてのシステムイベントのログを表示するには、イベント アイコンをクリックします。
アイコンバー: 設定アイコン	 設定。 設定 アイコンをクリックし、Rapid Recovery Core の設定を表示または管理します。Core の設定値をバックアップまたは復元することができます。ポートまたは表示の要素を制御するために、一般設定を設定することができます。また、次のカテゴリの設定を設定することができます。自動更新、夜間ジョブ、転送キュー設定、クライアントタイムアウト設定、DVM 重複排除キャッシュ設定、Replay Engine の設定、および展開の設定。データベース接続、SMTP サーバ設定、クラウドストレージアカウントを表示または変更することができます。レポートのフォント設定を変更することができます。SQL アタッチ可否設定、コアのジョブ設定、ライセンス設定、SNMP の設定、および vSphere 設定を設定することができます。
アイコンバー: 詳細アイコン	 詳細。 詳細 アイコンをクリックして他の重要な機能にアクセスできます。それぞれに独自のアイコンがあり、次に一覧表示します。
アイコンバー: 詳細システム情報アイコン	 システム情報。 システム情報 をクリックし、Rapid Recovery Core サーバに関するデータを表示します。Core のホスト名、OS、アーキテクチャ、およびメモリが表示されます。Core Console に表示される名前を表示できます。ネットワーク上の Core の完全修飾ドメイン名、キャッシュメタデータのパス、および重複排除キャッシュを表示することもできます。 表示名の変更の詳細については、「 Core のシステム情報について 」を参照してください。 重複排除キャッシュの詳細については、「 重複排除キャッシュと保存場所について 」を参照してください。 設定の調整の詳細については、「 重複排除キャッシュ設定の構成 」を参照してください。
アイコンバー: 詳細アーカイブアイコン	 アーカイブ。 Rapid Recovery により、Core からの情報のアーカイブを管理することができます。スケジュールされているアーカイブまたはアタッチされているアーカイブに関する情報を表示でき、また、アーカイブを追加、確認、インポートすることができます。
アイコンバー: 詳細マウントアイコン	 マウント。 ローカルマウントを表示およびマウント解除し、リモートマウントを表示および接続解除することができます。

UI エlement	説明
アイコンバー: 詳細アイコン ブート CD	 ブート CD。 通常、bare metal restore (BMR) に使用されるブート CD を管理できます。ブート CD の ISO イメージを作成するか、既存のイメージを削除するか、イメージのパスをクリックしてそれを開くか保存することができます。
アイコンバー: 詳細アイコン リポジトリ	 リポジトリ。 Core に関連付けられているリポジトリを表示および管理できます。
アイコンバー: 詳細アイコン 暗号化キー	 暗号化キー。 保護対象マシンに適用可能な暗号化キーを表示、管理、インポート、または追加することができます。使用されていない場合は、暗号化キーを削除することができます。
アイコンバー: 詳細アイコン クラウドアカウント	 クラウドアカウント。 Core とクラウドストレージアカウント間の接続を表示および管理できます。
アイコンバー: 詳細アイコン 保持ポリシー	 保持ポリシー。 リカバリポイントをロールアップして最終的に削除する前に保持する時間の長さを含む、Core の保持ポリシーを表示および変更できます。
アイコンバー: 詳細アイコン 通知	 通知。 Core イベントに関する通知を設定し、電子メール通知用の SMTP サーバ設定を定義し、同じイベントに関する通知の繰り返しを抑制するための繰り返し回数を設定することができます。
アイコンバー: 詳細アイコン ダウンロード	 ダウンロード。 Agent ソフトウェアの Web インストーラ、ローカルマウントユーティリティ、または SNMP ブラウザで使用するためのイベント情報が含まれている MIB ファイルをダウンロードすることができます。
アイコンバー: 詳細アイコン レポート	 レポート。 Core レポートまたはスケジュールレポートにアクセスし、継続的に生成することができます。
アイコンバー: 詳細アイコン Core ログ	 Core ログ。 診断目的で Core ログファイルをダウンロードすることができます。

左側のナビゲーションメニュー

左側のナビゲーションエリアに表示されるメニューの完全なセットについては、次の表で説明します。

表 217. 左側のナビゲーションメニューオプション

UI エlement	説明
保護されているマシンメニュー	Core で 1 つ以上のマシンが保護されている場合、左側のナビゲーションエリアには 保護されているマシンメニューが最初に表示されます。 このペインに表示される特定のマシン名をクリックすると、サマリ ページが表示され、選択したマシンのサマリ情報が表示されます。サマリ ページで実行できる操作の詳細については、「保護対象マシンのサマリ情報の表示」を参照してください。
レプリケートされたマシンメニュー	最上位のナビゲーションメニューとして別の Rapid Recovery Core の名前が表示される場合は、Core Console を表示している Core がターゲット Core です。メニューはソース Core から命名され、その下にリストされる各マシンは、このターゲット上でレプリケートされるそのソース Core からのマシンを表します。 このターゲット Core が複数のソース Core からのリカバリポイントをレプリケートする場合、各ソース Core は左側のナビゲーションエリアで独自の移動可能なメニューとして表示されます。

UI エレメント	説明
	レプリケートされたマシン メニューに表示される特定のマシン名をクリックすると、サマリ ページが表示され、選択したレプリケートされたマシンのサマリ情報が表示されます。 レプリケーションの詳細については、「レプリケーション」を参照してください。
リカバリポイントのみ メニュー	リカバリポイントのみ メニューが表示される場合、Core は以前保護またはレプリケートされたマシンのリカバリポイントを保持します。そのマシンは新しいスナップショットをキャプチャしなくなりますが、以前 Core でキャプチャされたリカバリポイントはそのまま残ります。これらのリカバリポイントはファイルレベルのリカバリで使用できますが、Bare Metal Restore、ボリューム全体のリストア、またはスナップショットデータの追加には使用できません。
カスタムグループメニュー	カスタムグループを作成すると、ナビゲーションメニューに カスタムグループ メニューが表示されます。カスタムグループはマシンをまとめてグループ化する論理コンテナです（たとえば、機能ごと、組織ごと、または地理的位置ごと）。カスタムグループには異機種混在のオブジェクト（保護対象マシン、レプリケートされたマシンなど）を含めることができます。他のメニューと同様に、カスタムグループのラベルを定義できます。名前はすべて大文字でメニューに表示されます。 カスタムグループタイトルの右側にある矢印をクリックすると、カスタムグループ内の類似するアイテムの操作を実行できます。たとえば、カスタムグループ内のすべての保護対象マシンのスナップショットを強制的に実行することができます。 カスタムグループを作成および管理する方法の詳細については、「カスタムグループについて」を参照してください。
アタッチされたアーカイブメニュー	アーカイブを Core にアタッチすると、各アーカイブが左側のナビゲーションメニューにリストされます。このラベルはアーカイブの名前です。このリストには、アーカイブに含まれる各マシンが表示されます。

左側のナビゲーション領域にあるエレメントの詳細を次の表に示します。

表 218. 左のナビゲーション領域およびメニュー

UI エレメント	説明
マシンメニューのテキストフィルタ	 テキストフィルタは、保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシンの各メニューに表示される項目をフィルタできるテキストフィールドです。このフィルタに条件を入力すると、基準を満たすマシンのみが該当するメニューに表示されます。
詳細の展開と縮小	 テキストフィルタの右にある矢印をクリックすると、保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシンの各メニューの詳細が展開または縮小されます。
保護されているマシンメニュー	   保護対象マシン メニューは、UI の左側のナビゲーションエリアに表示されます。このメニューでは、Core で設定された保護対象マシン、保護対象クラスタ、またはレプリケートされたマシンを表示できます。保護対象グループまたはリカバリポイントのみのマシンがある場合、それらもこのメニューの一部として表示されます。 Core の保護対象マシンのビューを縮小表示または展開するには、このメニューラベルの左側にある矢印をクリックします。 表示されるアイコンによってマシンタイプが次のように示されます。 ・ 単純なマシンアイコンは、物理マシンか、Rapid Recovery Agent ソフトウェアがインストールされている保護対象 VM を表します。 ・ 複数マシンのアイコンは、保護されたクラスタを表します。 ・ 白抜き 2 台のマシンのアイコンは、エージェントレス保護を使用している VMware 仮想マシンを表します。 ・ 白抜き 3 台のマシンのアイコンは、VMware vCenter ホストを表します。

保護対象マシン メニューをクリックすると、保護対象マシン ページが表示されます。このページの 保護対象マシン ペインには、この Core のすべての保護対象マシンが表示されます。詳細については、「[保護対象マシン メニューの表示](#)」を参照してください。

レプリケートされたマシンメニュー

別の Rapid Recovery Core からマシンをレプリケートする場合、その Core の名前が個別のメニューとして 保護対象マシン メニューの下に表示されます。リストされたソース Core からこのターゲット Core 上に複製された各マシンは、このメニューの下に表示されます。

複製された各マシンについて、複製されるマシンのタイプがアイコンで示されます。たとえば、単一のマシンを複製する場合、アイコンで1台のマシンが示されます。サーバクラスタを複製する場合、アイコンはクラスタを表します。

このメニューラベルの左側にある矢印をクリックして、レプリケートされたマシンの表示を縮小表示したり展開したりできます。

レプリケートされたマシン メニューから、すべてのレプリケートされたマシンに対してアクションを実行できます。

レプリケートされたマシン メニューをクリックすると、マシン ページが表示されます。このページには、このターゲット Core にレプリケートされる、別の（ソース）Core 上で保護されているすべてのマシンが表示されます。詳細については、「[ナビゲーションメニューからのレプリケートされたマシンの表示](#)」を参照してください。

リカバリポイントのみメニュー

Core で以前に保護されていたマシンが保護から削除されたが、リカバリポイントは削除されていない場合、リカバリポイントのみ メニューが表示されます。リカバリポイントが保存されている、以前の保護対象マシンがこのリストに表示されます。

このメニューラベルの左側にある矢印をクリックして、リカバリポイントのみのマシンの表示を折りたたんだり展開したりできます。

リカバリポイントのみ メニューから、この Core のすべてのリカバリポイントのみのマシンのリカバリポイントを削除できます。

リカバリポイントのみ メニューをクリックすると、マシン ページが表示されます。このタブには、リカバリポイントが保存されたマシンが表示されます。詳細については、「[リカバリポイントのみメニューの表示](#)」を参照してください。

カスタムグループメニュー

Core にカスタムグループが含まれている場合、左側のナビゲーションエリアには カスタムグループ メニューが表示されます。そのカスタムグループ内の各オブジェクトがこのリストに表示されます。

Core のカスタムグループのビューを縮小表示または展開するには、このメニューの左側にある矢印をクリックします。

カスタムグループ メニューから、グループ内のアイテムなどに対してアクションを実行できます。

カスタムグループ メニューをクリックすると、マシン ページが表示されます。このページには、保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシンというグループに表示される各 Rapid Recovery オブジェクトのペインが表示されます。詳細については、「[カスタムグループメニューの表示](#)」を参照してください。

アタッチされたアーカイブメニュー



Core にアーカイブをアタッチすると、左のナビゲーションエリアに、アタッチされたアーカイブごとのメニューが含まれます。アーカイブに含まれている保護対象の各マシンがこのリストに表示されます。メニューラベルには、アーカイブが保存されたときに指定された名前が使用されます。

Core にアタッチされたアーカイブのビューを縮小表示または展開するには、このメニューの左側にある矢印をクリックします。

アタッチされたアーカイブメニューから、グループ内のアイテムなどに対してアクションを実行できます。

アタッチされたアーカイブメニューをクリックすると、マシンページが表示されます。このページには、保護対象マシン、レプリケートされたマシン、リカバリポイントのみのマシンというグループに表示される各 Rapid Recovery オブジェクトのペインが表示されます。詳細については、「[カスタムグループメニューの表示](#)」を参照してください。

Protected Machines（保護されたマシン）ペインの表示

Protected Machines（保護されたマシン）ペインは、この Rapid Recovery コアで保護されるすべてのマシンに関する情報を含みます。保護される各マシンに対して（いずれかのマシンがまだ保護されている場合）、次の表で説明する情報がグリッドで表示されます。

表 219. 保護されたマシンそれぞれについての情報

UI 要素	説明
項目を選択	概要テーブルの各行に対して、表の上のメニューオプションのリストからアクションを実行ために、チェックボックスを選択できます。
タイプ	マシンタイプを示します。
ステータスインジケータ	Status（ステータス）列の色つきの円は、マシンがオンラインまたはアクセスできないかどうかを示します。色つきの円の上にカーソルを置くと、ステータスの状態が表示されます。ステータスの状態には、緑（オンラインで保護つき）、黄色（保護が一時停止）、赤色（認証エラー）、および灰色（オフラインまたはアクセス不可能）が含まれます。
暗号化ステータス	ロックアイコンは、選択された保護対象マシンの暗号化のステータスを示します。開かれたロックは暗号化がないことを示し、閉じられたロックは暗号化キーが確立されていることを示します。暗号化の詳細については、 暗号化キーの理解 を参照してください。
Display name（表示名）	保護対象マシンの表示名
最後のスナップショット	このマシンの最後のバックアップ転送を行った日付と日時をリストします。
Repository Name（リポジトリ名）	このマシンのデータが格納されるリポジトリをリストします。
Recovery Points（リカバリポイント）	リカバリポイントの数と、リポジトリ内で占めるスペースを一覧表示します。
バージョン	Rapid Recovery エージェントソフトウェアのバージョンがマシンにロードされます。
処置	この列の Settings（設定）ドロップダウンメニューをクリックすると、アクション、選択した保護対象マシン上で具体的に実行されるアクションが一覧表示されます。

この Core で保護されたマシンのいずれかが仮想スタンバイ用に設定されている場合は、次の表の説明に従って追加情報を参照してください。

表 220. 仮想スタンバイ用に設定された保護対象マシンに関する情報

UI 要素	説明
Last export (最後のエクスポート)	最後の仮想エクスポートの日付と日時。
Destination (送信先)	仮想マシンとして保護されたマシンを保存する先。たとえば、ESXi、VMware Workstation、Hyper-V、または VirtualBox。
ステータス	仮想スタンバイ用に設定されているマシンのステータス。ステータスの状態には「In Sync (同期中)」、「Paused (一時停止)」、および「Not enabled (無効)」が含まれます。

Protected Machines (保護されたマシン) ペインの Actions (アクション) ドロップダウンメニューから、次の表で説明されているアクションを実行できます。一部のオプションは、Exchange Server または SQL Server のみに表示されます。

表 221. Protected Machines (保護されたマシン) ペインで実行可能なアクション

UI 要素	説明
Force Snapshot (スナップショットの強制)	選択した保護対象マシン上のすべての保護対象ボリュームの増分スナップショットまたはベースイメージを強制できます。詳細については、 スナップショット作成の強制実行 を参照してください。
One-time Export (1 回限りのエクスポート)	Virtual Machine Export (仮想マシンのエクスポート) ウィザードを起動します。このウィザードでは、サポートされる VM の形式で、保護対象マシンからのリカバリポイントデータを 1 回限りエクスポートできます。詳細については、 VM エクスポート を参照してください。
Virtual Standby (仮想スタンバイ)	Virtual Machine Export (仮想マシンのエクスポート) ウィザードを起動します。このウィザードでは、サポートされる VM の形式で、保護対象マシンからのリカバリポイントデータの継続的エクスポートの仮想スタンバイを実行できます。詳細については、 VM エクスポート を参照してください。
Mount (マウント)	Mount (マウント) ウィザードが起動します。このウィザードでは、選択された保護対象マシンからリカバリポイントをマウントできます。
Recovery Points (リカバリポイント)	Recovery Points Summary (リカバリポイントの概要) ページが開きます。
復元	Restore Machine (マシンのリストア) ウィザードを起動します。このプロセスでは、Core 上のリカバリポイントから保護対象マシンにデータをリストアすることができます。詳細については、 リカバリポイントからのボリュームの復元 を参照してください。
Remove Machine (マシンの削除)	Rapid Recovery コアの保護から選択したマシンを削除し、Rapid Recovery コアに既にあるリカバリポイントを削除するか保持するかを選択できるようにします。詳細については、 マシンの削除 を参照してください。

保護されたマシンのグリッドに表示されている 2 台以上のマシンでアクションを実行できます。複数のマシン上で操作を実行するには、保護される各マシン用のチェックボックスを選択します。次に、概要の表の上にあるメニューから、次の表で説明するいずれのアクションを実行できます。

表 222. マシンが選択されたときに、**Protected Machines**（保護されたマシン）ペインで追加のアクションが利用できます

UI 要素	説明
Force Snapshot（スナップショットの強制）	選択した保護対象マシン上のすべての保護対象ボリュームの増分スナップショットを強制できます。詳細については、 スナップショット作成の強制実行 を参照してください。
Force Base Image（ベースイメージの強制）	選択した保護対象マシン上で保護されたすべてのボリュームのベースイメージを強制できます。詳細については、 スナップショット作成の強制実行 を参照してください。
Protection > Pause or Resume（保護 > 一時停止または再開）	選択したマシンに対する保護を一時停止したり（保護がアクティブな場合）、選択したマシンに対する保護を再開する（保護が一時停止されている場合）ことができます。詳細については、 保護の一時停止と再開 を参照してください。
レプリケーション	レプリケーションの有効化、強制、コピー、一時停止、または再開を実行できます。シードドライブの既存のリカバリポイントをコピーすることもできます。詳細については、 レプリケーション設定の管理 を参照してください。
キャンセル	選択したマシンの現在アクティブなすべての操作をキャンセルすることができます。または、選択したマシンの現在実行されているスナップショットだけを取り消すことができます。これは、将来的にスケジュールされている操作には影響を与えません。
Remove Machines（マシンの削除）	Rapid Recovery コアの保護から選択したマシンを削除し、Rapid Recovery コアに既にあるリカバリポイントを削除するか保持するかを選択できるようにします。詳細については、 マシンの削除 を参照してください。

保護される各マシン用の Configuration（構成）ドロップダウンメニューから、次の表に示すアクションを実行できます。一部のオプションは、Exchange Server または SQL Server のみに対して表示されます。

表 223. **Protected Machines**（保護されたマシン）ペインで実行可能なアクション

UI 要素	説明
Force Snapshot（スナップショットの強制）	選択したマシン上の1つまたは複数のボリュームに対する増分スナップショットまたはベースイメージを強制できます。詳細については、 スナップショット作成の強制実行 を参照してください。
Force Log Truncation for Exchange（Exchange のログ切り捨ての強制）	保護対象の Exchange Server マシンに対して、Exchange サーバの容量を解放する Exchange ログの切り捨てを強制します。詳細については、 SQL マシンのログの切り捨ての強制実行 を参照してください。
Force Log Truncation for SQL（SQL のログ切り捨ての強制）	保護された SQL Server マシンの場合は、SQL サーバー上の空きスペースを識別する SQL Server ログの切り捨てが強制されます。詳細については、 SQL マシンのログの切り捨ての強制実行 を参照してください。
エクスポート	Export（エクスポート）ウィザードを起動します。このウィザードでは、サポートされる VM の形式で、保護対象マシンから仮想マシンにリカバリポイントデータをエクスポートすることができます。継続的エクスポートのために1回限りのエクスポートを実行するか、仮想スタンバイを設定できます。詳細については、 VM エクスポート を参照してください。
Mount（マウント）	Mount Recovery Point（リカバリポイントのマウント）ダイアログボックスが開き、Rapid Recovery コアに保存されるスナップショットデータを通じてブラウズを行い、特定のリカバリポイントをマウントできます。詳細については リカバリポイントのマウント or Linux マシンでのリカバリポイントボリュームのマウント のそれぞれを参照してください。
Recovery Points（リカバリポイント）	選択したエージェントマシンの Recovery Points（リカバリポイント）タブが開きます。詳細については、 スナップショットとリカバリポイントの管理 を参照してください。

UI 要素	説明
復元	Restore Machine (マシンのリストア) ウィザードを起動します。このプロセスでは、Core 上のリカバリポイントから保護対象マシンにデータをリストアすることができます。詳細については、 リカバリポイントからのボリュームの復元 を参照してください。
Remove Machine (マシンの削除)	Rapid Recovery コアの保護から選択したマシンを削除し、Rapid Recovery コアに既にあるリカバリポイントを削除するか保持するかを選択できるようにします。詳細については、 マシンの削除 を参照してください。

保護対象マシンのイベントの表示

イベントページには、選択した保護対象マシンに対する実行済みまたは進行中のジョブが表示されます。ページの上部にあるボタンを使用すると、アクティビティの3つの各カテゴリのジョブのリストに移動できます。

- ・ **タスク**：正常に操作するために Rapid Recovery で実行する必要があるジョブ。
- ・ **アラート**。エラーや警告など、タスクまたはイベントに関連する通知。
- ・ **ジャーナル**。すべての保護対象マシンのタスクとアラートの複合。

次の表は、イベント ページの各要素を説明しています。

表 224. イベント ページの要素

UI エlement	説明
検索キーワード	各カテゴリ内の特定のアイテムを検索できます。タスクでのみ使用可能です。
送信者	検索を開始する日付を入力して、結果を絞り込むことができます。タスクでのみ使用可能です。
宛先	検索を終了する日付を入力して、結果を絞り込むことができます。タスクでのみ使用可能です。
ステータスアイコン	各アイコンは、さまざまなジョブステータスを表しています。アラートとタスクの場合は、いずれかのアイコンをクリックすると、そのステータスでリストをフィルタでき、実質的にレポートが生成されます。アイコンを2回クリックすると、そのステータスのフィルタは削除されます。複数のステータスでフィルタすることができます。次のようなステータスがあります。 ・ アクティブ。進行中のジョブ。 ・ キューに登録済み：開始できるようになるまで別のジョブの完了を待機しているジョブ。 ・ 待機しています。シードドライブなど、承認または完了を待機しているジョブ（シードドライブの詳細については、「レプリケーション」を参照してください）。 ・ 完了しました。正常に完了したジョブ。 ・ 失敗しました：失敗して完了できなかったジョブ。
サービスアイコン	このボタンを使用すると、サービスジョブがジョブのリストに追加されます。このアイコンをクリックすると、各ステータスアイコン上に小さなサービスアイコンが表示され、それらのステータスを持つサービスジョブでフィルタできるようになります（サービスジョブが存在する場合）。サービスジョブの例として、インデックスファイルの削除や保護からのマシンの削除などが挙げられます。
エクスポートタイプ ドロップダウンリスト	ドロップダウンリストには、イベントレポートをエクスポートできる形式が表示されます。タスクでのみ使用可能です。次のような形式があります。 ・ PDF ・ HTML ・ CSV ・ XLS ・ XLSX

UI エlement	説明
 (エクスポートアイコン)	選択した形式にイベントレポートを変換します。タスクでのみ使用可能です。
ページ選択	イベントレポートには、複数のページにわたって数個のジョブを含めることができます。イベント ページの下部にある番号や矢印を使用して、レポートの他のページに移動できます。

イベント ページでは、すべてのイベントが1つの表に表示されます。次の表は、項目 ごとに表示される情報のリストです。

表 225. イベントのサマリ表の詳細情報

UI エlement	説明
ステータス	タスク、アラート、またはジャーナルのアイテムのステータスが表示されます。アラートまたはジャーナルのアイテムで使用可能です。ヘッダーをクリックすると、ステータスで結果がフィルタされます。
名前	名前はタスクにのみ使用できます。このテキストフィールドには、この保護対象マシンの完了したタスクタイプのリストが表示されます。例としては、ボリュームの転送、リポジトリの維持、ロールアップ、実行マウント可否チェック、チェックサムチェックなどがあります。
開始時刻	タスク、アラート、およびジャーナルのアイテムで使用可能です。ジョブまたはタスクが開始された日付と時刻を表示します。
終了時刻	タスクでのみ使用可能です。タスクが完了した日付と時刻を表示します。
 ジョブの詳細	タスクでのみ使用可能です。アクティブなタスクをモニタ ダイアログボックスが開き、特定のジョブまたはタスクの詳細を表示することができます。これらの詳細には、ジョブの ID、Core がデータを転送したレート（該当する場合）、ジョブの完了までの経過時間、ギガバイト単位での作業の合計、およびジョブに関連付けられている子タスクが含まれます。
Message（メッセージ）	アラートおよびジャーナルのアイテムで使用可能です。このテキストフィールドには、アラートまたはジャーナルのアイテムを説明するメッセージが表示されます。

保護されたマシンの More（詳細）メニューの表示

More（詳細） メニューは、追加オプションを提供し、選択した保護対象マシンの管理を支援します。これらのツールにアクセスするには、More（詳細）ドロップダウンメニューをクリックして、次の表で説明するオプションのいずれかを選択します。

表 226. 保護されたマシンの More（詳細）オプションからアクセス可能なツール

UI 要素	説明
	保護対象マシンに関する情報、システム情報、ボリューム、プロセッサ、ネットワークアダプタ、およびこのマシンの IP アドレスを示します。 詳細については、「 保護対象マシンのシステム情報の表示 」を参照してください。
システム情報	
	Local Mounts（ローカルマウント）ペインから、ローカルでマウントされたボリュームを表示するか、マウント解除できます。Remote Mounts（リモートマウント）ペインから、ローカルマウントユーティリティを使用してマウントされたボリュームを表示するか、マウントを解除できます。 ボリュームのマウント解除の詳細については、 リカバリポイントのマウント解除 を参照してください。
マウント	

UI 要素

説明

リカバリポイントをローカルにマウントに関する情報は、[リカバリポイントのマウント](#) または [Linux マシンでのリカバリポイントボリュームのマウント](#) をそれぞれ参照してください。



選択したマシンの保持ポリシーを指定できます。Core のデフォルトのポリシーを使用する選択もできます。または、このマシンの保持ポリシーのみを区別できます。詳細については、[保護対象マシンの保持ポリシー設定のカスタマイズ](#) を参照してください。

保持ポリシー



選択したマシンに関連するイベントのカスタム通知グループを指定できます。これは、Core 上にすでに設定されている通知は変更しません。詳細については、[通知グループの設定](#) を参照してください。

通知



Rapid Recovery エージェントソフトウェアを使用して、マシンのログファイルをダウンロードし、表示します。詳細については、[保護対象マシンのログファイルのダウンロードと表示](#) を参照してください。

エージェントのログ

Rapid Recovery PowerShell モジュールについて

Dell Data Protection | Rapid Recovery はいくつかのソフトウェアコンポーネントで構成されます。このトピックに関連する重要なコンポーネントには、次のようなものがあります。

- ・ Rapid Recovery Core は、保護対象マシンの認証の管理、バックアップとレプリケーションのデータ転送のスケジュール設定、仮想マシンへのエクスポート、レポート作成、類似または異種ハードウェアへの Bare Metal Restore (BMR) を行います。
- ・ Rapid Recovery Agent は、ボリュームスナップショットの取得と、Core が管理するリポジトリへの高速なデータ転送を行います。
- ・ Rapid Recovery PowerShell モジュールは、Windows PowerShell® スクリプトを使用してユーザーが Core サーバを操作できるようにする Windows ユーティリティです。このモジュールは、Rapid Recovery Core Console のグラフィカルユーザーインターフェース (GUI) で提供される機能と同じ機能をいくつか提供します。たとえば、Rapid Recovery PowerShell モジュールでは、Rapid Recovery リカバリポイントをマウントしたり、保護対象マシンのスナップショットの作成を強制的に実行したりできます。

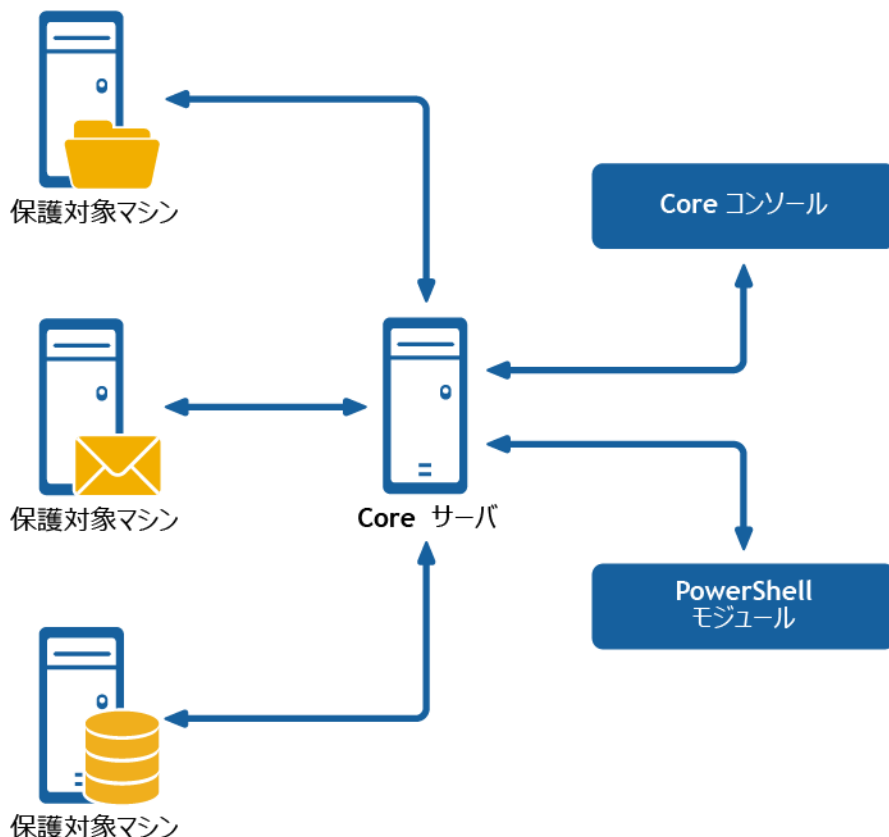


図 14. Rapid RecoveryCore と通信する PowerShell モジュール

PowerShell は、管理の自動化のために設計された Microsoft .NET Framework 関連環境です。本項では、Rapid Recovery Core GUI を操作せずに特定の機能のスクリプトに管理者が使用できる Rapid Recovery PowerShell モジュールとコマンドレットについて説明します。

① **メモ:** 事前スクリプトや事後スクリプトとして **PowerShell** スクリプトを実行することもできます。詳細およびサンプルスクリプトについては、「[スクリプトによる Rapid Recovery ジョブの拡張](#)」を参照してください。

トピック：

- ・ PowerShell 使用の前提条件
- ・ コマンドとコマンドレットの操作
- ・ Rapid Recovery PowerShell モジュールコマンドレット
- ・ ローカライゼーションローからいぜーしょん
- ・ 修飾子しゅうしょくし

PowerShell 使用の前提条件

Rapid Recovery PowerShell モジュールを使用する前に、Windows PowerShell 2.0 以降がインストールされている必要があります。PowerShell 3.0 では、オブジェクトプロパティへの簡単なアクセス、PowerShell Web アクセス、REST 呼び出しのサポートなどの新機能が導入されているため、Dell では、PowerShell 3.0 以降を使用することをお勧めします。

① **メモ:** powershell.exe.config ファイルが PowerShell ホームディレクトリにあることを確認してください。たとえば、C:\WindowsPowerShell\powershell.exe.config です。

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0.30319"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

PowerShell の起動とモジュールのインポート

他のシステムモジュールとは異なり、Rapid Recovery PowerShell モジュールはデフォルトではロードされません。各セッションに対して、管理者権限で Windows PowerShell を開き、モジュールをインポートできます。PowerShell を起動し、Rapid Recovery PowerShell モジュールをインポートするには、次の手順を実行します。

- 1 Windows PowerShell の管理者特権でのコマンドプロンプトを開きます。たとえば、「スタート」メニューで「Windows PowerShell」と入力し、検索された Windows PowerShell アプリケーションを右クリックして「**管理者として実行**」を選択します。

Windows PowerShell が新しいコマンドウィンドウで開きます。

- 2 次のコマンドを入力して <Enter> を押します。

```
Import-Module "RapidRecoveryPowerShellModule"
```

現在のセッションの Rapid Recovery PowerShell モジュールがインポートされます。既存のコマンドウィンドウでコマンドレットを実行できるようになります。

コマンドとコマンドレットの操作

コマンドレットは、1つの関数を実行する Windows PowerShell スクリプト内の特殊コマンドです。通常、コマンドレットは動詞-名詞のペアで表されます。コマンドレットによって返される結果はオブジェクトです。

PowerShell コマンドにパイプラインを設定し、1つのコマンドレットの出力を別のコマンドレットの入力としてパイプ処理できます。簡単な例として、Rapid Recovery PowerShell モジュール内のコマンドのリストをリクエストし、そのリストを名前順にソートできます。このスクリプトの例を次に示します。

```
Get-Command -module rapidrecoverypowershellmodule | sort-object name
```

コマンドレットのヘルプと例の取得

PowerShell を開いて Rapid Recovery PowerShell モジュールをインポートすると、Get-Help <command_name> コマンドレットを使用していつでも追加情報をリクエストできます。たとえば、仮想マシンのエクスポートコマンドレットに関する情報を取得するには、次のコマンドレットを入力して <Enter> を押します。

```
Get-Help Start-VMExport
```

返されるオブジェクトには、コマンド名、概要、構文、およびコマンドで使用可能なオプションが含まれます。

特定のコマンドレットのヘルプを取得する別の方法は、コマンド名に続けて -? を入力することです。たとえば、次のとおりです。

```
Start-VMExport -?
```

次のコマンドを実行して、コマンドレットの例をリクエストすることもできます。

```
>Get-Help Start-VMExport -examples
```

Rapid Recovery PowerShell モジュールコマンドレット

本項では、Rapid Recovery PowerShell モジュールで使えるコマンドレットおよびオプションについて説明します。Rapid Recovery PowerShell モジュールのすべてのコマンドレットは、次の共通パラメータをサポートします。

- Verbose
- デバッグ
- ErrorAction
- ErrorVariable
- WarningAction
- WarningVariable
- OutBuffer
- OutVariable

詳細については、Get-Help about_commonparameters を使用してください。

使用可能なコマンドレットを次の表に示します。

表 227. Rapid Recovery PowerShell モジュールのコマンドレット

コマンドレット名	説明
Edit-EsxiVirtualStandby	既存の ESXi 仮想スタンバイ設定を編集します。
Edit-HyperVVirtualStandby	既存の Hyper-V 仮想スタンバイ設定を編集します。
Edit-VBVirtualStandby	既存の VirtualBox 仮想スタンバイ設定を編集します。
Edit-VMVirtualStandby	既存の VMware Workstation 仮想スタンバイ設定を編集します。
Edit-ScheduledArchive	既存のスケジュール設定されたアーカイブ設定を編集します。
Get-ActiveJobs	アクティブジョブのコレクションを取得します。

コマンドレット名	説明
Get-CloudAccounts	Core に保存されたクラウドアカウントに関する情報を取得します。
Get-Clusters	保護対象クラスタのコレクションを取得します。
Get-CompletedJobs	完了したジョブのコレクションを取得します。
Get-ExchangeMailStores	Exchange メールストアのコレクションを取得します。
Get-Failed	失敗したリカバリポイントに関する情報を取得します。
Get-FailedJobs	失敗したジョブのコレクションを取得します。
Get-Mounts	マウントされたすべてのリカバリポイントを表示します。
Get-Passed	成功したリカバリポイントに関する情報を取得します。
Get-ProtectedServers	保護対象サーバに関する情報を取得します。
Get-ProtectionGroups	保護グループのコレクションを取得します。
Get-QueuedJobs	キューで待機中のジョブのコレクションを取得します。
Get-RecoveryPoints	リカバリポイントに関する情報を取得します。
Get-ReplicatedServers	レプリケートされたサーバに関する情報を取得します。
Get-Repositories	リポジトリに関する情報を取得します。
Get-ScheduledArchive	定期的なアーカイブジョブに関する情報を取得します。
Get-SqlDatabases	SQL データベースのコレクションを取得します。
Get-UnprotectedVolumes	保護されていないボリュームのコレクションを取得します。
Get-VirtualizedServers	仮想サーバに関する情報を取得します。
Get-Volumes	ボリュームに関する情報を取得します。
New-Base	ベースイメージのスナップショットを強制的に作成します。
New-CloudAccount	Core に新規クラウドアカウントを追加します。
New-EncryptionKey	新しい暗号化キーを作成します。
New-EsxiVirtualStandby	新規 ESXi 仮想スタンバイマシンを作成します。
New-HyperVVirtualStandby	新規 Hyper-V 仮想スタンバイ仮想マシンを作成します。
New-Mount	リカバリポイントをマウントする。
New-Replication	レプリケーションを設定して強制実行します。
New-Repository	新規 DVM リポジトリを作成します。
New-ScheduledArchive	新規定期アーカイブをスケジュール設定します。
New-Snapshot	スナップショットを強制的に作成します。
New-VBVirtualStandby	新規 VirtualBox 仮想スタンバイ仮想マシンを作成します。
New-VMVirtualStandby	新規 VMware Workstation 仮想スタンバイ仮想マシンを作成します。
Push-Replication	レプリケーションを強制実行する。
Push-Rollup	ロールアップを強制実行します。

コマンドレット名	説明
Remove-Agent	保護からマシンを削除します。
Remove-Mount	リカバリポイントをマウント解除します。
Remove-Mounts	マウントされたすべてのリカバリポイントをマウント解除します。
Remove-RecoveryPoints	保護対象マシンのリカバリポイントを削除します。
Remove-Repository	既存の DVM リポジトリを削除します。
Remove-ScheduledArchive	スケジュール設定されたアーカイブを停止します。
Remove-VirtualStandby	Core から仮想スタンバイ仮想マシンを削除します。
Resume-Replication	レプリケーションを再開します。
Resume-RepositoryActivity	リポジトリアクティビティを再開します。
Resume-ScheduledArchive	スケジュール設定されたアーカイブを再開します。
Resume-Snapshot	スナップショットを再開します。
Resume-VirtualStandby	仮想スタンバイ仮想マシンへのデータのエクスポートを再開します。
Start-Archive	リカバリポイントをアーカイブします。
Start-AttachabilityCheck	保護対象 MS SQL データベースのアタッチ可否チェックを強制実行します。
Start-ChecksumCheck	保護対象 Exchange メールストアのチェックサムチェックを強制実行します。
Start-EsxiExport	ESXi サーバへのエクスポートを強制実行します。
Start-HypervExport	Hyper-V サーバへのエクスポートを強制実行します。
Start-LogTruncation	ログの切り捨ての強制実行。
Start-MountabilityCheck	保護対象 Exchange メールストアのマウント可否チェックを強制実行します。
Start-Protect	サーバを保護します。
Start-ProtectCluster	クラスタを保護します。
Start-RepositoryCheck	DVM リポジトリチェックを強制実行します。
Start-RestoreArchive	アーカイブのリカバリポイントをリストアします。
Start-ScheduledArchive	スケジュール設定されたアーカイブのデータ転送を強制実行します。
Start-VBExport	VirtualBox サーバへのエクスポートを強制実行します。
Start-VirtualStandby	既存の仮想スタンバイ仮想マシンへのデータ転送を強制実行します。
Start-VMExport	VMWare Workstation サーバへのエクスポートを強制実行します。
Stop-ActiveJobs	アクティブジョブをキャンセルします。
Suspend-Replication	レプリケーションを一時停止します。
Suspend-RepositoryActivity	リポジトリのアクティビティを一時停止します。

コマンドレット名	説明
Suspend-ScheduledArchive	スケジュール設定されたアーカイブのデータ転送を一時停止します。
Suspend-Snapshot	スナップショットを一時停止します。
Suspend-VirtualStandby	仮想スタンバイ仮想マシンへのデータ転送を一時停止します。
Update-Repository	DVM リポジトリにエクステンントを追加します。

Edit-EsxiVirtualStandby

Edit-EsxiVirtualStandby コマンドを使用すると、PowerShell を使用して ESXi 仮想マシン（VM）に対する既存の仮想エクSPORTを変更できます。

使用法：

コマンドの使用法を次に示します。

```
Edit-EsxiVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-HostPassword <String>] [-DiskProvisioning <String>] [-DiskMapping <String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-ErrorAction<ActionPreference>] [-WarningAction<ActionPreference>] [-ErrorVariable String] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

コマンドオプション

次の表は、Edit-EsxiVirtualStandby コマンドで使用できるオプションを説明しています。

表 228. Edit-EsxiVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。

オプション	説明
	all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export' (リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントのロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例：

ローカル Core 上のアクティブなすべてのジョブをリストします。

```
>Get-activejobs -all
```

Edit-HyperVVirtualStandby

Edit-HyperVVirtualStandby コマンドを使用すると、PowerShell で Hyper-V 仮想マシン (VM) に対する既存の仮想エクスポートを変更できます。

使用法：

コマンドの使用法を次に示します。

```
Edit-HyperVVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-HostPassword <String>] [-VMLocation <String>] [-UseLocalMachine] [-gen2] [-UseVhdx] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

コマンドオプション

次の表は、Edit-HyperVVirtualStandby コマンドで使用できるオプションを説明しています。

表 229. Edit-HyperVVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export' (リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントのロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例：

ローカル Core 上のアクティブなすべてのジョブをリストします。

```
>Get-activejobs -all
```

Edit-ScheduledArchive

Edit-ScheduledArchive コマンドを使用すると、PowerShell で既存のスケジュール済みアーカイブを変更することができます。

使用法：

コマンドの使用法を次に示します。

```
Edit-ScheduledArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -path [location] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -scheduletype [type] -dayofweek [name] -dayofmonth [number] -time [time] -initialpause -id [id]
```

コマンドオプション

次の表は、Edit-ScheduledArchive コマンドで使用できるオプションを説明しています。

表 230. Edit-ScheduledArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	アーカイブするリカバリポイントを持つ保護対象マシン。複数のマシン名を指定するには、二重引用符で囲み、カンマで区切ります。
-all	すべての保護対象マシンのリカバリポイントをアーカイブします。
-path	アーカイブされたデータの保存先へのパス。たとえば、次のとおりです。 - ローカルマシン： "d:\work\archive" - ネットワークパス： "\\servername\sharename" - クラウドアカウントのフォルダ： "Folder Name"  メモ: ローカルネットワークの場所を表す場合、記号の数は 100 を超えないようにします。また、クラウドの場所を表す場合、記号の数は 150 を超えないようにします。
-cloudaccountname	省略可能。クラウドアーカイブでのみ使用します。アーカイブを保存するクラウドアカウントの名前。
-cloudcontainer	省略可能。クラウドアーカイブでのみ使用します。選択したクラウドアカウントのクラウドコンテナの名前。ここに、アーカイブが保存されます。このオプションを使用する場合は、"-cloudaccountname" パラメータも指定します。
-recycleaction	リサイクルアクションのタイプ。次の 4 つの値のうち、いずれかを使用して指定します。 "replacethiscore" - この Core に関連する既存のアーカイブを上書きしますが、他の Core のデータはそのまま残します。

オプション	説明
	• "erasecompletely" - 新しいアーカイブへの書き込みの前に、ディレクトリからすべてのアーカイブデータをクリアします。 • "incremental" - 既存のアーカイブにリカバリポイントを追加できます。リカバリポイントを比較して、アーカイブに既に存在するデータの重複を回避します。
-scheduletype	スケジュールインターバルのタイプ。次の4つの値のうち、いずれかを使用してオプションを指定します。 • "daily" - 毎日、アーカイブを自動的に作成する場合。 • "weekly" - 毎週、アーカイブを自動的に作成する場合。"-dayofweek" パラメータを指定する必要があります。 • "monthly" - 毎月、アーカイブを自動的に作成する場合。"-dayofmonth" パラメータを指定する必要があります。日付 ("31" など) が指定されない限り、その月のアーカイブは実行されません。 • "lastdayofmonth" - 各月の最終日にアーカイブを自動的に作成する場合。
-dayofweek	"-schedulescheduletype" パラメータの "weekly" オプションでのみ使用します。アーカイブを自動的に作成する曜日 ("Monday" など)。
-dayofmonth	"-schedulescheduletype" パラメータの "month" オプションでのみ使用します。アーカイブを自動的に作成する対象月の日付 ("15" など)。
-time	アーカイブを作成する時間。
-initialpause	省略可能。アーカイブスケジュールの設定後、最初にアーカイブを一時停止する場合は、このオプションを指定します。
-id	編集するスケジュールされたアーカイブの識別子。

例：

ローカル Core 上のスケジュール済みアーカイブを編集します。

```
>Edit-ScheduledArchive -protectedserver protectedserver1 -path d:\work\archive -
cloudaccountname cloud1 -cloudcontainer cloudarchives -recycleaction incremental -schedulescheduletype
daily -time 12:00 AM -initialpause -i
d archiveid
```

Edit-VBVirtualStandby

Edit-VBVirtualStandby コマンドを使用すると、PowerShell で VirtualBox 仮想マシン (VM) に対する既存の仮想エクスポートを変更できます。

使用法：

コマンドの使用法を次に示します。

```
Edit-VBVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-LinuxHostName <String>] [-HostPort <UInt32>] [-AccountUserName <String>] [-AccountPassword
<String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam]
[-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-
WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

コマンドオプション

次の表は、Edit-VBVirtualStandby コマンドで使用できるオプションを説明しています。

表 231. Edit-VBVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export' (リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントのロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例 :

ローカル Core 上のアクティブなすべてのジョブをリストします。

```
>Get-activejobs -all
```

Edit-VMVirtualStandby

Edit-VMVirtualStandby コマンドを使用すると、PowerShell を使用して VMware Workstation 仮想マシン (VM) に対する既存の仮想エクスポートを変更できます。

使用法：

コマンドの使用法を次に示します。

```

Edit-VMVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User
<String>] [-Core <String>]
[-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction
<ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer
<Int32>]
```

コマンドオプション

次の表は、Edit-VMVirtualStandby コマンドで使用できるオプションを説明しています。

表 232. Edit-VMVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export'

オプション	説明
	(リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントの ロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例：

ローカル Core 上のアクティブなすべてのジョブをリストします。

```
>Get-activejobs -all
```

Get-ActiveJobs

Get-ActiveJobs コマンドは、Core からアクティブなすべてのジョブを返します。-jobtype パラメータは、特定のジョブを監視するために使用できます。

使用法：

コマンドの使用法を次に示します。

```
Get-ActiveJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -
jobtype [type] -time [time]
```

コマンドオプション

次の表は、Get-ActiveJobs コマンドで使用できるオプションを説明しています。

表 233. Get-ActiveJobs コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。

オプション	説明
	指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export' (リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントのロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例：

ローカル Core 上のアクティブなすべてのジョブをリストします。

```
>Get-activejobs -all
```

Get-Clusters

Get-Clusters コマンドは、Core の保護対象サーバクラスタに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-Clusters -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、Get-Clusters コマンドで使用できるオプションを説明しています。

表 234. Get-Clusters コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

ローカル Core 上の保護対象サーバークラスタをリストします。

```
>Get-Clusters
```

Get-CompletedJobs

Get-CompletedJobs コマンドは、Core で完了したジョブのリストを返します。-jobtype パラメータは、特定のジョブを監視するために使用できます。

使用法：

コマンドの使用法を次に示します。

```
Get-CompletedJobs -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -  
jobtype [type] -time [time]
```

コマンドオプション

次の表は、Get-CompletedJobs コマンドで使用できるオプションを説明しています。

表 235. Get-CompletedJobs コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。

オプション	説明
	指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export' (リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントのロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例：

ローカル Core 上のアクティブなすべてのジョブをリストします。

```
>Get-CompletedJobs -all
```

ローカル Core 上の完了したすべてのリポジトリ作成ジョブをリストします。

```
>Get-CompletedJobs -jobtype repository
```

Get-ExchangeMailStores

Get-ExchangeMailStores コマンドは、Core によって保護されている Exchange Server のメールストアに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-ExchangeMailStores -core [host name] -user [user name] -password [password]  
-protectedserver [server name or IP address]
```

コマンドオプション

次の表は、Get-ExchangeMailStores コマンドで使用できるオプションを説明しています。

表 236. Get-ExchangeMailStores コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。

例：

ローカル Core の Exchange Server の Exchange メールストアをリストします。

```
>Get-ExchangeMailStores -protectedserver 10.10.10.10
```

Get-Failed

Get-Failed コマンドは、ローカル Core の失敗したリカバリポイントに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-Failed -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

コマンドオプション

次の表は、Get-Failed コマンドで利用できるオプションを説明しています。

表 237. Get-Failed コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。

例 :

失敗したすべてのリカバリポイントをリストします。

```
>Get-failed -protectedserver 10.10.10.10
```

Get-FailedJobs

Get-FailedJobs コマンドは、ローカル Core の失敗したすべてのジョブを返します。

使用法 :

コマンドの使用法を次に示します。

```
Get-FailedJobs -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -  
jobtype [type] -time [time]
```

コマンドオプション

次の表は、Get-FailedJobs コマンドで使えるオプションを説明しています。

表 238. Get-FailedJobs コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export' (リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントのロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例 :

ローカル Core 上の失敗したすべてのジョブをリストします。

```
>Get-FailedJobs -all
```


ローカル Core 上の失敗したすべてのバックアップ作成ジョブをリストします。

```
>Get-FailedJobs -type backup
```

Get-Mounts

Get-Mounts コマンドは、ローカル Core でマウントされたすべてのリカバリポイントを返します。

使用法：

コマンドの使用法を次に示します。

```
Get-Mounts -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address]
```

コマンドオプション

次の表は、Get-Mounts コマンドで使用できるオプションを説明しています。

表 239. Get-Mounts コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。

例：

マウントされたすべてのリカバリポイントを表示します。

```
>Get-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$$dd -protectedserver 10.10.5.22
```

Get-Passed

Get-Passed コマンドは、Core 上の検証チェックに合格したリカバリポイントに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-Passed -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

コマンドオプション

次の表は、Get-Passed コマンドで使用できるオプションを説明しています。

表 240. Get-Passed コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

検証チェックに合格したローカル Core 上のすべてのリカバリポイントをリストします。

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

Get-ProtectedServers コマンドは、ローカル Core 上の保護対象マシンに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-ProtectedServers -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、Get-ProtectedServers コマンドで使用できるオプションを説明しています。

表 241. Get-ProtectedServers コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

ローカル Core 上の現在保護されているすべてのマシンをリストします。

```
>Get-ProtectedServers
```

Get-ProtectionGroups

Get-ProtectionGroups コマンドは、ローカル Core 上の保護グループに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address]
```

コマンドオプション

次の表は、Get-ProtectionGroups コマンドで使用できるオプションを説明しています。

表 242. Get-ProtectionGroups コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。

例：

ローカル Core 上の保護グループをリストします。

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-QueuedJobs

Get-QueuedJobs コマンドは、Core からの開始を待機しているすべてのジョブを返します。

使用法：

コマンドの使用法を次に示します。

```
Get-QueuedJobs -core [host name] -user [login] -password [password] -all | -protectedserver
[name | IP address] -number [all | f[number] | l[number] | number] -jobtype [type] -time [time]
```

コマンドオプション

次の表は、Get-ActiveJobs コマンドで使用できるオプションを説明しています。

表 243. Get-ActiveJobs コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-all	Core およびすべての保護対象サーバーで実行されたジョブを含む、すべてのジョブを表示します。

オプション	説明
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 'transfer' (データ転送)、'repository' (リポジトリのメンテナンス)、'replication' (ローカルおよびリモートレプリケーション)、'backup' (バックアップおよびリストア)、'bootcdbuilder' (ブート CD の作成)、'diagnostics' (ログのアップロード)、'exchange' (Exchange Server ファイルのチェック)、'export' (リカバリポイントのエクスポート)、'pushinstall' (Agent の導入)、'rollback' (リカバリポイントからのリストア)、'rollup' (リカバリポイントの ロールアップ)、'sqlattach' (Agent のアタッチ可否チェック)、'mount' (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブが返されます。
-time	省略可能。開始されたジョブの日時で出力をフィルタします。入力に使用できる種類は次のとおりです。 #d または DD (# は現在までの日数を表す数値です) #h または #H (# は現在までの時間数を表す数値です) "time date 1", "time date 2" (コンマの前の日付からコンマの後の日付までのカスタム範囲を表示します)。

例 :

ローカル Core 上のすべての待機ジョブをリストします。

```
>Get-QueuedJobs -all
```

Get-RecoveryPoints

Get-RecoveryPoints コマンドは、ローカル Core 上の保護対象マシンのリカバリポイントに関する情報を返します。

使用法 :

コマンドの使用法を次に示します。

```
Get-RecoveryPoints -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

コマンドオプション

次の表は、Get-RecoveryPoints コマンドで使用できるオプションを説明しています。

表 244. Get-RecoveryPoints コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-number	省略可能。表示されるレコード数を決定します。使用できる値は次のとおりです。 all (すべてのジョブを表示)、l[number] または [number] (実行と時間によってソートされた最新の ## 件のジョブを取得)、f[number] (実行と時間によってソートされた最初の ## 件のリカバリジョブを表示)。デフォルトでは、最新 20 件のジョブを表示します。

例：

ローカル Core 上の保護対象マシンのリカバリポイントをリストします。

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

Get-ReplicatedServers コマンドは、Core 上のレプリケートされたマシンに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-ReplicatedServers -core [host name] -user [user name] -password [password]
```

コマンドを使用して値を返す場合、デルでは、セキュリティを考慮することをお勧めします。たとえば、このコマンドはレプリケートされた各サーバーの管理者のパスワードを返します。ターゲット Core からの MSP 環境で使用した場合、管理者ユーザーのログインパスワードが公開される可能性があります。リポジトリデータが暗号化されている環境では、これによる大きなセキュリティ上の問題は発生しません。

コマンドオプション

次の表は、Get-ReplicatedServers コマンドで使用できるオプションを説明しています。

表 245. Get-ReplicatedServers コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

ローカル Core 上のレプリケートされたすべてのサーバーをリストします。

```
>Get-ReplicatedServers
```

Get-Repositories

Get-Repositories コマンドは、Core 上のリポジトリに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-Repositories -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、Get-Repositories コマンドで使用できるオプションを説明しています。

表 246. Get-Repositories コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

ローカル Core 上のリポジトリをリストします。

```
>Get-Repositories
```

Get-ScheduledArchives

Get-ScheduledArchives コマンドを使用すると、PowerShell で Core に関連付けられた既存のスケジュール済み Rapid Recovery アーカイブの情報を表示することができます。

使用法：

コマンドの使用法を次に示します。

```
Get-ScheduledArchives -core [host name] -user [login] -password [password]
```

コマンドオプション

次の表は、Get-ScheduledArchives コマンドで使えるオプションを説明しています。

表 247. Get-ScheduledArchives コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

現在の Core に含まれている、スケジュールされたアーカイブの情報を取得します。

```
>Get-ScheduledArchives -core 10.10.10.10 -user administrator -password password
```

Get-SqlDatabases

Get-SqlDatabases コマンドは、指定された保護対象マシンから SQL データベースのリストを返します。

使用法：

コマンドの使用法を次に示します。

```
Get-SqlDatabases -core [host name] -user [user name] -password [password]  
-protectedserver [server name or IP address]
```

コマンドオプション

次の表は、Get-SqlDatabases コマンドで使用できるオプションを説明しています。

表 248. Get-SqlDatabases コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。

例：

ローカル Core 上のすべての SQL データベースジョブをリストします。

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-UnprotectedVolumes

Get-UnprotectedVolumes コマンドは、Core 上の保護が可能で、現在保護されていないボリュームに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-UnprotectedVolumes  
-core [host name] -user [user name] -password [password] -protectedserver [server name or IP  
address]
```

コマンドオプション

次の表は、Get-UnprotectedVolumes コマンドで使用できるオプションを説明しています。

表 249. Get-UnprotectedVolumes コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。

例：

指定された Agent マシン上の保護が可能で、現在保護されていないすべてのボリュームをリストします。

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-VirtualizedServers

Get-VirtualizedServers コマンドは、仮想サーバに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-VirtualizedServers -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、Get-VirtualizedServers コマンドで使用できるオプションを説明しています。

表 250. Get-VirtualizedServers コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

ローカル Core 上のすべての仮想サーバーをリストします。

```
>Get-VirtualizedServers
```

Get-Volumes

Get-Volumes コマンドは、Core によって保護されている指定されたマシン上のボリュームに関する情報を返します。

使用法：

コマンドの使用法を次に示します。

```
Get-Volumes -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

コマンドオプション

次の表は、Get-Volumes コマンドで使えるオプションを説明しています。

表 251. Get-Volumes コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。

例：

指定されたマシン上のすべてのボリュームをリストします。

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-Base

New-Base コマンドは、新しいベースイメージの作成を強制的に実行します。これにより、現在の保護対象マシンのデータが転送されます。ベースイメージの作成を強制的に実行すると、転送がただちに開始されるか、キューに追加されます。以前のリカバリポイントから変更されたデータのみが転送されます。以前のリカバリポイントが存在しない場合は、保護対象ボリューム上のすべてのデータが転送されます。

使用法：

コマンドの使用法を次に示します。

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、New-Base コマンドで使用できるオプションを説明しています。

表 252. New-Base コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	すべての Agent のベースイメージ。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	現在の保護対象マシン名の強制。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

すべての保護対象マシンのベースイメージを強制実行します。

```
>New-Base -all
```

New-CloudAccount

New-CloudAccount コマンドを使用すると、新しいクラウドアカウントを Rapid Recovery Core に追加できます。

使用法：

コマンドの使用法を次に示します。

```
New-CloudAccount -core [host name] -user [login] -password [password] -displayname [display name] -type [cloud account type] -username [user name] - key [secret key] -region [region] - tenantid [tenant Id] - authurl [authorization url]
```

コマンドオプション

次の表は、New-CloudAccount コマンドで使用できるオプションを説明しています。

表 253. New-CloudAccount コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-displayname	表示されるクラウドアカウントの名前。
-type	追加するクラウドアカウントのタイプ。サポートされる値は次のとおりです。 - amazon - openstack - rackspace - windowsazure "windows azure" - azure

オプション	説明
-username	追加するクラウドアカウントのユーザー名。これは、認証プロセスで使用されます。このプロパティは、Amazon™ クラウドの場合は「アクセスキー」、Rackspace および OpenStack の場合は「ユーザー名」、Windows Azure クラウドアカウントの場合は「ストレージアカウント名」として解決されます。
-key	追加するクラウドアカウントのキー。これは、認証プロセスで使用されます。このプロパティは、Amazon™ クラウドの場合は「シークレットキー」、Rackspace および OpenStack の場合は「API キー」、Windows Azure クラウドアカウントの場合は「アクセスキー」として解決されます。
-region	追加するクラウドアカウントのリージョン。このプロパティは、Rackspace および OpenStack クラウドアカウントの場合にのみ必要です。
-tenantid	OpenStack クラウドアカウントの認証プロセスで使用される識別子。このオプションは、OpenStack クラウドアカウントの場合にのみ必要です。
-authurl	OpenStack クラウドアカウントの認証プロセスで使用される URL。このオプションは、OpenStack クラウドアカウントの場合にのみ必要です。

例：

アクセスキー「akey」とシークレットキー「skey」を持つ、「Amazon S3 Account」という名前の Amazon™ S3 クラウドアカウントを作成します。

```
>New-CloudAccount -displayname "Amazon S3 Account" -type Amazon -username akey -key skey
```

New-EncryptionKey

New-EncryptionKey コマンドを使用すると、お使いの Rapid Recovery のバックアップデータを保護するために、新しい暗号化キーを作成できます。

使用法：

コマンドの使用法を次に示します。

```
New-EncryptionKey -core [host name] -user [login] -password [password] -name [encryption key
name] -passphrase [pas
sphrase] -comment [comment]
```

コマンドオプション

次の表は、New-EncryptionKey コマンドで使用できるオプションを説明しています。

表 254. New-EncryptionKey コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	作成する暗号化キーの名前。
-passphrase	作成する暗号化キーのパスフレーズ。
-comment	省略可能。暗号化キーの説明。

例：

ローカル Core で暗号化キーを作成します。

```
>New-EncryptionKey -name EncryptionKey1 -passphrase 123456
```

New-EsxiVirtualStandby

New-EsxiVirtualStandby PowerShell コマンドを使用すると、Rapid Recovery を使用して新しい ESXi 仮想スタンバイマシンを作成できます。

使用法：

コマンドの使用法を次に示します。

```
New-EsxiVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -initialexport
```

コマンドオプション

次の表は、New-EsxiVirtualStandby コマンドで使えるオプションを説明しています。

表 255. New-EsxiVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。

オプション	説明
	指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-volumes	省略可能。エクスポートするボリューム名をリストします。指定しない場合は、リカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります（例："c:" "d:"）。 ① メモ: ボリューム名の末尾にスラッシュを使用しないでください。
-vmname	仮想マシンの Microsoft Windows 名。
-hostname	仮想サーバホストの名前。
-hostport	仮想サーバとの通信に使用するポート番号。
-hostusername	仮想サーバホストへのログインに使用するユーザー名。
-hostpassword	仮想サーバホストへのログインに使用するパスワード。
-ram	仮想サーバーに特定の量の RAM を割り当てます。
-usesourceram	省略可能。ソースの保護対象マシンと同じ容量の RAM を仮想サーバに割り当てます。
-diskprovisioning	省略可能。仮想マシンに割り当てられるディスク容量。使用できる値は、 - Thick - 仮想ディスクを保護対象サーバの元のドライブと同じ大きさにするには、「thick」を指定します。 - Thin - 元のドライブで使用している実施のディスク容量に数メガバイト追加して割り当てするには、「thin」を指定します。 デフォルトのディスクプロビジョニングは「thin」です。
-diskmapping	省略可能。これにより、リカバリポイントから仮想マシンにディスクをマップする方法が決定されます。使用できる値は、 - auto - manual - withvm デフォルト設定は「auto」です。
-initialexport	省略可能。仮想スタンバイを設定した後で、オンデマンドの仮想マシンの初回エクスポートを開始する必要がある場合に、このオプションを指定します。

例：

新しい ESXi 仮想スタンバイを作成します。

```
>New-EsxiVirtualStandby -protectedserver 10.10.10.4 -vmname ExportedMachine -hostname 10.10.10.127 -hostport 443 -hostusername root -hostpassword pass123 -usesourceram -diskprovisioning thin -diskmapping auto
```

New-HyperVVirtualStandby

New-HyperVVirtualStandby PowerShell コマンドを使用すると、Rapid Recovery を使用して新しい Hyper-V 仮想マシン (VM) を作成できます。

使用法：

コマンドの使用法を次に示します。

```
New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver  
[name | IP address]  
-volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]  
| -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -  
hostpassword [virtual host password] -rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

コマンドオプション

次の表は、New-HyperVVirtualStandby コマンドで使用できるオプションを説明しています。

表 256. New-HyperVVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-volumes	省略可能。エクスポートするボリューム名をリストします。指定しない場合は、リカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります (例: "c:" "d:")。 📌 メモ: ボリューム名の末尾にスラッシュを使用しないでください。
-vmname	仮想マシンの Microsoft Windows 名。
-gen2	省略可能。第 2 世代の VM を使用するように指定します。指定しない場合は、第 1 世代が使用されます。Rapid Recovery は、Windows Server 2012 R2 から Windows 8.1 までの第 2 世代をサポートします。

オプション	説明
-usevhdx	省略可能。このオプションを指定すると、Rapid Recovery は VHDX ディスクフォーマットを使用して VM を作成します。指定しない場合は、VHD ディスクフォーマットが使用されます。第 2 世代は VHDX フォーマットのみを使用します。
-uselocalmachine	省略可能。ローカル Hyper-V サーバーに接続します。この値を指定すると、Rapid Recovery は次のオプションを無視します。 ・ hostname ・ hostport ・ hostusername ・ hostpassword
-hostname	仮想サーバホストの名前。
-hostport	仮想サーバとの通信に使用するポート番号。
-hostusername	仮想サーバホストへのログインに使用するユーザー名。
-hostpassword	仮想サーバホストへのログインに使用するパスワード。
-vmlocation	仮想マシンのファイルを保存するフォルダへのローカルまたはネットワークパス。
-ram	仮想サーバーに特定の量の RAM を割り当てます。
-usesourceram	省略可能。ソースの保護対象マシンと同じ容量の RAM を仮想サーバに割り当てます。
-initialexport	省略可能。仮想スタンバイを設定した後で、オンデマンドの仮想マシンの初回エクスポートを開始する必要がある場合に、このオプションを指定します。

例：

新しい Hyper-V 仮想スタンバイマシンを作成します。

```
>New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host password] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

New-Mount

New-Mount コマンドは、1つまたは複数のドライブのスナップショットをマウントします。

使用法：

コマンドの使用法を次に示します。

```
New-Mount -core [host name] -user [user name] -password [password] -protectedserver [machine
name] -mounttype [read | write | readonlywithpreviouswrites] -drives [drive names] -path
[location] -time [MM/DD/YYYY hh:mm:ss tt | passed | latest] -rpn [number]
```


コマンドオプション

次の表は、New-Mount コマンドで使用できるオプションを説明しています。

表 257. New-Mount コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-protectedserver	保護対象サーバーの IP アドレスまたはマシン名 (特定のマシンがどのように保護されているのかによって異なる)。
-time	省略可能。マウントするリカバリポイントのタイムスタンプ。これは、現在の PC の OS で指定されている形式である必要があります。管理者は、最新のリカバリポイント、または渡されたパラメータ値で最後にチェックしたリカバリポイントを指定し、最新のリカバリポイントを取得できます。デフォルトでは、最終時刻のオプションが選択されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-path	マウントされるリカバリポイントへの Core マシン上のパス。
-mounttype	省略可能。マウントモードを指定します。使用できるオプションは、'read'、'readOnlyWithPreviousWrites' (以前の書き込みとともに読み取り専用)、'write' (書き込み可能) です。デフォルトモードは read-only です。
-volumes	省略可能。マウントするボリューム名のリスト (スペース区切り)。ボリュームの名前にスペースまたは特殊文字が含まれている場合、二重引用符を使用して指定する必要があります。指定しない場合、すべてのボリュームがマウントされます。
-drivers	省略可能。マウントするボリューム名のコンマ区切りリスト。指定しない場合、すべてのボリュームがマウントされます。 ① メモ: このオプションは旧形式です。代わりに、'-volumes' を使用してください。
-rpn	省略可能。マウントのリカバリポイント番号。これは、get-mounts コマンドを使用して取得できます。1 つのコマンドで異なるポイントをマウントするには、rpn パラメーターに複数の番号を指定します。 ① メモ: 複数のマウントポイントを設定すると、各ポイントは個別の子ディレクトリに配置されます。名前は、リカバリポイントが作成された時間を表します。マウント解除を呼び出すと、すべての子ディレクトリが削除されます。親ディレクトリは手動で削除する必要があります。

例 :

```
>New-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$$dd -protectedserver 10.10.5.22 -path C:\MountedRecoveryPoint -mounttype read -volumes c "d, ko"
```

複数のリカバリポイントをマウントします。

```
>New-Mount -rpn 10 52 41 -protectedserver localhost -path "D:/Folder for mount"
```

特定の時間に作成されたリカバリポイントをマウントします。

```
>New-Mount -protectedserver 10.10.5.56 -path "D:/Folder for mount" -time "8/24/2012 11:46 AM"
```

Resume-Replication

New-Replication コマンドを使用すると、保護される 1 台または複数のサーバのレプリケーションをセットアップして、強制的に実行できます。

使用法：

コマンドの使用法を次に示します。

```
New-Replication -core [host name] -user [login] -password [password] -targetserver [host name] -protectedserver [name | IP address]
```

コマンドオプション

次の表は、New-Replication コマンドで使用できるオプションを説明しています。

表 258. New-Replication コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-replicationname	ターゲット Core 上のレプリケーション設定の名前。
-targetserver	ターゲット Core のホスト名、ユーザー名、およびパスワード。
-protectedserver	レプリケーションのセットアップに使用する、ターゲット Core 上の保護対象マシンとリポジトリの名前。

例：

保護対象マシン (IP 10.10.10.4) の新しいレプリケーションを作成します。

```
>New-Replication -targetserver 10.10.10.128 -protectedserver 10.10.10.4
```

New-Repository

New-Repository コマンドは、Rapid Recovery Core に新しい DVM リポジトリを作成します。250 MB ～ 16 TB のサイズを指定する必要があります。

使用法：

コマンドの使用法を次に示します。

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath [location]
```

コマンドオプション

次の表は、New-Repository コマンドで使用できるオプションを説明しています。

表 259. New-Repository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	リポジトリ名。
-size	リポジトリのエクステントのサイズ。使用できる単位は b、Kb、MB、GB、TB、PB です。
-datapath	ローカルの場所のみ。リポジトリのエクステントのデータパスを決定します。
-metadatapath	ローカルの場所のみ。リポジトリのエクステントのメタデータパスを決定します。
-uncpath	共有の場所のみ。リポジトリのエクステントのデータおよびメタデータパスを決定します。
-shareusername	共有の場所のみ。場所を共有するためのログインを決定します。
-sharepassword	共有の場所のみ。場所を共有するためのパスワードを決定します。
-comment	省略可能。リポジトリの説明。
-concurrent Operations	省略可能。同時に保留することができる操作の最大数。値はデフォルトで 64 です。

例：

最小サイズの新しい DVM リポジトリをローカルドライブ E: に作成します。

```
>New-Repository -name Repository2 -size 250Mb -datapath e:\Repository\Data -metadatapath e:\Repository\Metadata
```

New-ScheduledArchive

New-ScheduledArchive コマンドを使用すると、PowerShell を使用して既存のスケジュール済みアーカイブを変更できます。

使用法：

コマンドの使用法を次に示します。

```
New-ScheduledArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address] -path [location] -archiveusername [name] -archivepassword [password] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -schdeuletype [type] -dayofweek [name] -dayofmonth [number] -time [time]
```

コマンドオプション

次の表は、New-ScheduledArchive コマンドで使用できるオプションを説明しています。

表 260. New-ScheduledArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	アーカイブするリカバリポイントを持つ保護対象マシン。複数のマシン名を指定するには、二重引用符で囲み、カンマで区切ります。
-all	すべての保護対象マシンのリカバリポイントをアーカイブします。
-path	アーカイブされたデータの保存先へのパス。たとえば、次のとおりです。 - ローカルマシン : "d:\work\archive" - ネットワークパス : "\\servername\sharename" - クラウドアカウントのフォルダ : "Folder Name"  メモ: ローカルやネットワークの場所を表す場合、記号の数は 100 を超えないようにします。また、クラウドの場所を表す場合、記号の数は 150 を超えないようにします。
-archiveusername	省略可能。リモートマシンへのログインに使用するユーザー名。ネットワークパスでのみ必要です。
-archivepassword	省略可能。リモートマシンへのログインに使用するパスワード。ネットワークパスでのみ必要です。

オプション	説明
-cloudaccountname	省略可能。クラウドアーカイブでのみ使用します。アーカイブを保存するクラウドアカウントの名前。
-cloudcontainer	省略可能。クラウドアーカイブでのみ使用します。選択したクラウドアカウントのクラウドコンテナの名前。ここに、アーカイブが保存されます。このオプションを使用する場合は、"-cloudaccountname" パラメーターも指定します。
-recycleaction	リサイクルアクションのタイプ。次の 4 つの値のうち、いずれかを使用して指定します。 • "replacethiscore" - この Core に関連する既存のアーカイブを上書きしますが、他の Core のデータはそのまま残します。 • "erasecompletely" - 新しいアーカイブへの書き込みの前に、ディレクトリからすべてのアーカイブデータをクリアします。 • "incremental" - 既存のアーカイブにリカバリポイントを追加できます。リカバリポイントを比較して、アーカイブに既に存在するデータの重複を回避します。
-schedulescheduletype	スケジュールインターバルのタイプ。次の 4 つの値のうち、いずれかを使用してオプションを指定します。 • "daily" - 毎日、アーカイブを自動的に作成する場合。 • "weekly" - 毎週、アーカイブを自動的に作成する場合。"-dayofweek" パラメーターを指定する必要があります。 • "monthly" - 毎月、アーカイブを自動的に作成する場合。"-dayofmonth" パラメーターを指定する必要があります。日付 ("31" など) が指定されない限り、その月のアーカイブは実行されません。 • "lastdayofmonth" - 各月の最終日にアーカイブを自動的に作成する場合。
-dayofweek	"-schedulescheduletype" パラメーター "weekly" オプションでのみ使用します。アーカイブを自動的に作成する曜日 ("Monday" など)。
-dayofmonth	"-schedulescheduletype" パラメーターの "month" オプションでのみ使用します。アーカイブを自動的に作成する対象月の日付 ("15" など)。
-time	アーカイブを作成する時間。
-initialpause	省略可能。アーカイブスケジュールの設定後、最初にアーカイブを一時停止する場合は、このオプションを指定します。

例：

Core 上のすべてのマシンで、作成日が 2012 年 4 月 30 日 02:55 PM 以降のリカバリポイントをすべてアーカイブし、Coreに残っていたこれまでのアーカイブデータを置き換えます。

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path "d:\work\archive" -s
tartdate "04/30/2012 02:55 PM" -all -recycleaction replacethiscore
```

2 台の保護対象マシンのデータ範囲内に入っているリカバリポイントをアーカイブし、新しいアーカイブが書き込まれる前にそのディレクトリからすべてのアーカイブデータをクリアします。

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -
protectedserver "10.20.30.40" "20.20.10.1" -path "d:\work\archive" -startdate "04/30/2012 02:55
PM" -enddate "05/31/2012 11:00 AM" -recycleaction erasecompletely
```

Core 上のすべてのマシンで、作成日が 2012 年 4 月 30 日 02:55 PM 以降の全リカバリポイントの増分アーカイブに対し、「amazon S3」という名前のクラウドアカウントと「Container」という名前のコンテナを作成します。

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path
"ArchiveOnCloud" -cloudaccountname "Amazon S3" -cloudcontainer "Container" -startdate
"04/30/2012 02:55 PM" -all -recycleaction incremental
```

New-Snapshot

New-Snapshot コマンドは、スナップショット作成を強制的に実行します。これにより、現在の保護対象マシンのデータが転送されます。スナップショット作成を強制的に実行すると、転送がただちに開始されるか、キューに追加されます。以前のリカバリポイントから変更されたデータのみが転送されます。以前のリカバリポイントが存在しない場合は、保護対象ボリューム上のすべてのデータが転送されます。

使用法：

コマンドの使用法を次に示します。

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user name] -
password [password]
```

コマンドオプション

次の表は、New-Snapshot コマンドで使用できるオプションを説明しています。

表 261. New-Snapshot コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	すべての保護対象マシンを強制します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	現在の保護対象マシン名の強制。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

すべての保護対象マシンのスナップショット作成を強制実行します。

```
>New-Snapshot -all
```


New-VBVirtualStandby

New-VBVirtualStandby コマンドを使用すると、PowerShell で VirtualBox 仮想マシン (VM) に新しい仮想エクスポートを作成することができます。

使用法：

コマンドの使用法を次に示します。

```
New-VBVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total megabytes] | -usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location] -pathusername [login] -pathpassword [password] -initialexport
```

コマンドオプション

次の表は、New-VBVirtualStandby コマンドで使用できるオプションを説明しています。

表 262. New-VBVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-volumes	省略可能。エクスポートするボリューム名をリストします。指定しない場合は、リカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります (例: "c:" "d:")。 📌 メモ: ボリューム名の末尾にスラッシュを使用しないでください。
-vmname	仮想マシンの Microsoft Windows 名。
-ram	仮想サーバーに特定の量の RAM を割り当てます。
-usesourceram	省略可能。ソースの保護対象マシンと同じ容量の RAM を仮想サーバに割り当てます。
-linuxhostname	Linux VirtualBox サーバのホスト名。
-hostport	Linux VirtualBox サーバのポート。

オプション	説明
-targetpath	仮想マシンのファイルを保存するフォルダへのローカル、ネットワーク、または Linux パス。
-pathusername	ネットワークマシンへのログインに使用するユーザー名。ターゲットパス用にネットワークの場所を指定する場合のみ要求されます。
-pathpassword	ネットワークマシンへのログインに使用するパスワード。ターゲットパス用にネットワークの場所を指定する場合のみ要求されます。
-accountusername	省略可能。エクスポートされた仮想マシンの登録に使用する、ユーザーアカウントを指定できます。ユーザーアカウントへのログインに使用するユーザー名。このオプションは、ローカルまたはネットワークマシンに対してのみ使用します。
-accountpassword	省略可能。エクスポートされた仮想マシンの登録に使用する、ユーザーアカウントを指定できます。ユーザーアカウントへのログインに使用するパスワード。このオプションは、ローカルまたはネットワークマシンに対してのみ使用します。
-initialexport	省略可能。仮想スタンバイを設定した後で、オンデマンドの仮想マシンの初回エクスポートを開始する必要がある場合に、このオプションを指定します。

例：

指定した場所に、ExportedMachine1 という名前の VirtualBox 仮想スタンバイマシンを作成します。

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

New-VMVirtualStandby

New-VMVirtualStandby PowerShell コマンドを使用すると、Rapid Recovery を使用して新しい VMware Workstation 仮想スタンバイマシンを作成できます。

使用法：

コマンドの使用法を次に示します。

```
New-VMVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total
megabytes] | -usesourceram] -targetpath [location] -pathusername [login] -pathpassword
[password] -initialexport
```

コマンドオプション

次の表は、New-VMVirtualStandby コマンドで使用できるオプションを説明しています。

表 263. New-VMVirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	IP アドレスで示された、特定の保護対象マシンのジョブを表示します。
-volumes	省略可能。エクスポートするボリューム名をリストします。指定しない場合は、リカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります（例："c:" "d:"）。 ① メモ: ボリューム名の末尾にスラッシュを使用しないでください。
-vmname	仮想マシンの Microsoft Windows 名。
-ram	仮想サーバーに特定の量の RAM を割り当てます。
-usesourceram	省略可能。ソースの保護対象マシンと同じ容量の RAM を仮想サーバに割り当てます。
-pathusername	ネットワークマシンへのログインに使用するユーザー名。ターゲットパス用にネットワークの場所を指定する場合のみ要求されます。
-pathpassword	ネットワークマシンへのログインに使用するパスワード。ターゲットパス用にネットワークの場所を指定する場合のみ要求されます。
-initialexport	省略可能。仮想スタンバイを設定した後で、オンデマンドの仮想マシンの初回エクスポートを開始する必要がある場合に、このオプションを指定します。

例：

新しい VMware Workstation 仮想スタンバイを作成します。

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -usesourceram -targetpath I:\VMExport
```

スクリプトを一時停止します。ユーザーは適切なワークステーションのインデックス番号を指定する必要があります。完了するスクリプトのインデックス番号（この場合は2）を入力します。例（続き）：

```
2
Verify location ...
Virtual Standby successfully configured
PS C:\Users\Administrator>
```

Push-Replication

Push-Replication コマンドは、1 台以上の保護対象マシンのレプリケーションを強制実行します。

使用法：

コマンドの使用法を次に示します。

```
Push-Replication -core [host name] -user [user name] -password [password] -targetcore [host name] -all | -protectedserver [machine name | IP address]
```

コマンドオプション

次の表は、Push-Replication コマンドで使用できるオプションを説明しています。

表 264. Push-Replication コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	ターゲット Core へのすべてのマシンのレプリケーションを強制実行します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	レプリケーションを強制実行するターゲット Core 上の保護対象マシン名。
-user	省略可能。リモート Core のホストマシンに対するログイン。ログインを指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

1つの保護対象マシンのレプリケーションをプッシュします。

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -targetcore 10.10.10.20:8006 -protectedserver 10.10.5.22
```

すべての保護対象マシンのレプリケーションをプッシュします。

```
>Push-Replication -all
```

Push-Rollup

Push-Rollup コマンドは、保護対象マシンのロールアップを強制実行します。

使用法：

コマンドの使用法を次に示します。

```
Push-Rollup -core [host name] -user [user name] -password [password] -protectedserver [machine name | IP address]
```

コマンドオプション

次の表は、Push-Rollup コマンドで使用できるオプションを説明しています。

表 265. Push-Rollup コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	すべての保護対象マシンを強制します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	現在の保護対象マシン名の強制。
-user	省略可能。リモート Core のホストマシンに対するログイン。ログインを指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

1つの保護対象マシンのロールアップをブッシュします。

```
>Push-Rollup -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22
```

すべての保護対象マシンのロールアップをブッシュします。

```
>Push-Rollup -all
```

Remove-Agent

Remove-Agent PowerShell コマンドを使用すると、Rapid Recovery Core の保護対象からマシンを削除できます。

使用法：

コマンドの使用法を次に示します。

```
Remove-Agent -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -deleterecoverypoints -all
```

コマンドオプション

次の表は、Remove-MountAgent コマンドで使用できるオプションを説明しています。

表 266. Remove-Agent コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	現在の保護対象マシンのすべてのマウント済みリカバリポイントをマウント解除します。
-deleterecoverypoints	省略可能。この保護対象マシンのリカバリポイントをすべて削除します。
-all	省略可能。Core からすべての保護対象マシンを削除します。

例：

すべての保護対象マシンとそのリカバリポイントをマウント解除します。

```
>Remove-Agent -core 10.10.10.10:8006 -user administrator -password 23WE@#$$sdd -deleterecoverypoints -all
```

Remove-Mount

Remove-Mount コマンドは、/Path で指定したマウント済みリカバリポイントをマウント解除します。-protectedserver パラメーターを使用して選択したマシンのポイントをマウント解除するか、-all パラメーターを使用してすべてのマウント済みリカバリポイントをマウント解除します。

使用法：

コマンドの使用法を次に示します。

```
Remove-Mount -core [host name] -user [user name] -password [password] [-protectedserver [machine name] | -path [mount path]]
```

コマンドオプション

次の表は、Remove-Mount コマンドで使用できるオプションを説明しています。

表 267. Remove-Mount コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	マウントされたすべてのリカバリポイントをマウント解除します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-path	選択したマウントポイントをマウント解除します。
-protectedserver	現在の保護対象マシンのすべてのマウント済みリカバリポイントをマウント解除します。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

パスで指定したリカバリポイントをマウント解除します。

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -path C:\mountedRecoveryPoint
```

Remove-Mounts

Remove-Mounts コマンドは、すべてのマウント済みリカバリポイントをマウント解除します。

使用法：

コマンドの使用法を次に示します。

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、Remove-Mounts コマンドで使用できるオプションを説明しています。

表 268. Remove-Mounts コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。

オプション	説明
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

例：

指定した Core 上のすべてのリカバリポイントをマウント解除します。

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$$dd
```

Remove-RecoveryPoints

Remove-RecoveryPoints PowerShell コマンドは、特定のマシンのリカバリポイントを削除できます。

使用法：

コマンドの使用法を次に示します。

```
Remove-RecoveryPoints -core [host name] -user [login] -password [password] -[range | chain | all] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string | time interval specified by two time strings]
```

コマンドオプション

次の表は、Remove-RecoveryPoints コマンドで使えるオプションを説明しています。

表 269. Remove-RecoveryPoints コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	現在の保護対象マシンのすべてのマウント済みリカバリポイントをマウント解除します。
-rpn	省略可能。チェーン削除の場合のみ (ベースイメージと増分またはオーファン状態のポイントのチェーン)。削除するリカバリポイントの連続する番号 (Get-RecoveryPoints コマンドを使用して番号を取得)。番号の間をスペースで区切って指定することで、1つのコマンドで複数のリカバリポイントを削除できます。

オプション	説明
-time	リカバリポイントのチェーンを削除するには、このオプションを使用します。 省略可能。単一のリカバリポイントを削除するには、その作成時刻によってリカバリポイントを選択します。正確な日時を「mm/dd/yyyy hh:mm tt」形式（「2/24/2012 09:00 AM」など）で指定します。コンピュータで設定されているタイムゾーンでの日時の値を指定します。 必須。日付範囲の場合、2つの時刻文字列をカンマおよびスペースで区切って時間間隔を指定し、削除するリカバリポイントの範囲を選択します。
-range	省略可能。時間間隔による削除するリカバリポイントの範囲。
-chain	省略可能。リカバリポイント番号またはリカバリポイントの作成時刻で選択されたベースイメージおよび連続する増分ポイントまたはオフライン化した連続するポイントのセット。
-all	省略可能。すべての保護対象マシンを Core から削除します。

例：

日付で指定したリカバリポイントを削除します。

```
>Remove-RecoveryPoints -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -time "2/24/2012 09:00 AM"
```

Remove-Repository

Remove-Repository PowerShell コマンドは、Rapid Recovery リポジトリとそのコンテンツを Core から削除します。

使用法：

コマンドの使用法を次に示します。

```
Remove-Repository -core [host name] -user [login] -password [password] -name [repository name] -all
```

コマンドオプション

次の表は、Remove-Repository コマンドで使用できるオプションを説明しています。

表 270. Remove-Repository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	削除するリポジトリの名前。
-all	この Core に関連付けられているすべてのリポジトリを削除します。

例：

ローカル Core 上のすべてのリポジトリを削除します。

```
>Remove-repository -all
```

Remove-ScheduledArchive

特定のマシンのリカバリポイントを定期的にアーカイブするように Rapid Recovery をスケジュールする場合、Remove-ScheduledArchive PowerShell コマンドで Core からのそのスケジュールされたアーカイブを削除することができます。

使用法：

コマンドの使用法を次に示します。

```
Remove-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

コマンドオプション

次の表は、Remove-ScheduledArchive コマンドで使用できるオプションを説明しています。

表 271. Remove-ScheduledArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	Core に関連付けられているすべてのアーカイブを削除します。

オプション	説明
-id	削除するアーカイブの識別子。複数のアーカイブの一覧を表示するには、各 ID をスペースで区切ります。

例：

ローカル Core からいくつかのスケジュールされたアーカイブを削除します。

```
>Remove-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Remove-VirtualStandby

仮想マシンに継続的にエクスポートするように Rapid Recovery をスケジュールした場合は、Remove-VirtualStandby PowerShell コマンドを使用してスケジュールされたジョブをキャンセルおよび削除できます。

使用法：

コマンドの使用法を次に示します。

```
Remove-VirtualStandby -core [host name] -user [login] -password [password] -all | -protectedserver [name(s) | IP address]
```

コマンドオプション

次の表は、Remove-VirtualStandby コマンドで使用できるオプションを説明しています。

表 272. Remove-VirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	Core に関連付けられているすべての Virtual Standby ジョブを削除します。
-protectedserver	Virtual Standby を削除する保護対象マシンの名前または IP アドレス。

例：

Coreに関連付けられているすべての Virtual Standby ジョブを削除します。

```
>Remove-VirtualStandby -all
```

Resume-Replication

Resume-Replication コマンドを使用すると、レプリケーションを再開できます。詳細については、「[Suspend-Replication](#)」を参照してください。

使用法：

コマンドの使用法を次に示します。

```
Resume-Replication -core [host name] -user [user name] -password [password] -all | -  
protectedserver [machine name | IP address] -incoming [host name] | -outgoing [host name]
```

コマンドオプション

次の表は、Resume-Replication コマンドで使用できるオプションを説明しています。

表 273. Resume-Replication コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	すべての保護対象サーバー。
- protectedserver	指定されたマシンのレプリケーションを再開します。
-incoming	Core マシンにレプリケートするリモート Core のホスト名。リモート Core 上のすべての保護対象マシンでレプリケーションが再開されます。
-outgoing	データがレプリケートされるリモートターゲット Core のホスト名。リモート Core 上のすべての保護対象マシンでレプリケーションが再開されます。

例：

使用されるリポジトリを指定して、ローカル Core の保護対象マシン（IP 10.10.10.128）のレプリケーションを再開します。

```
>Resume-Replication replicationname Replication1 -targetserver 10.10.10.128,Administrator,123asdQ -protectedserver 10.10.10.4
```

```
# Repository
- -----
```

```
1 Repository A
2 Repository B
```

Please, input number of Repository from the list above or type 'exit' to exit:

スクリプトを一時停止します。ユーザーは適切なリポジトリのインデックス番号を指定する必要があります。完了するスクリプトのインデックス番号（この場合は2）を入力します。例（続き）：

```
2
Replication job was started.
True
PS C:\Users\Administrator>
```

Resume-Snapshot

管理者は、スナップショットの再開、仮想マシンへのエクスポート、およびレプリケーションの実行ができます。詳細については、「[Start-VMExport](#)」を参照してください。

使用法：

コマンドの使用法を次に示します。

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

コマンドオプション

次の表は、Resume-Snapshot コマンドで使用できるオプションを説明しています。

表 274. Resume-Snapshot コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	すべての保護対象サーバー。

オプション	説明
- protectedserver	指定したマシンのスナップショットを再開します。

例：

ローカル Core の保護対象マシン（IP 10.10.10.4）のスナップショットを再開します。

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume-VirtualStandby

Resume-VirtualStandby PowerShell コマンドを使用すると、中断された Rapid Recovery 仮想スタンバイマシンへのデータのエクスポートを再開できます。

使用法：

コマンドの使用法を次に示します。

```
Resume-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP address]
```

コマンドオプション

次の表は、Resume-VirtualStandby コマンドで使えるオプションを説明しています。

表 275. Resume-VirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	すべての仮想スタンバイマシンに対してエクスポートを再開します。
- protectedserver	再開する仮想スタンバイマシンを使用して保護されるマシンの名前（複数の名前を指定する場合はコンマとスペースで区切ります）。

例：

保護対象マシンに対して仮想スタンバイのエクスポートを再開します。

```
>Resume-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22
```

Resume-VMExport

Resume-VMExport コマンドを使用すると、管理者は仮想マシンにエクスポートすることができます。詳細については、「[Suspend-VMExport](#)」を参照してください。

使用法：

コマンドの使用法を次に示します。

```
Resume-VMExport -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

コマンドオプション

次の表は、Resume-VMExport コマンドで使用できるオプションを説明しています。

表 276. Resume-VMExport コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	すべての保護対象サーバー。
-protectedserver	指定したマシンのスナップショットを再開します。

例：

ローカル Core 上の各保護対象マシンの仮想マシンへのエクスポートを再開します。

```
>Resume-VMExport -all
```

Start-Archive

企業では、準拠および非準拠データの両方のアーカイブに長期ストレージを使用することがよくあります。Rapid Recovery のアーカイブ機能は、準拠および非準拠データの延長保持をサポートするために使用します。Administrator は、/Path コマンドと認証情報を指定して、アーカイブをローカルストレージやネットワークの場所に保存できます。

使用法：

コマンドの使用法を次に示します。

```
Start-Archive -path -startdate -enddate [-all] | -protectedserver [machine name] or [IP]] -core [host name] -user [user name] -password [password]
```

コマンドオプション

次の表は、Start-Archive コマンドで使用できるオプションを説明しています。

表 277. Start-Archive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-path	場所のパス。パスの例：「D:\work\archive」、ネットワークパスの例：「\\servername\sharename」。
-all	Core 上のすべてのマシンのリカバリポイントをアーカイブします。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-startdate	作成されたリカバリポイントの日付範囲の開始日。現在の PC の OS で指定されている形式である必要があります。
-enddate	日付範囲の終了日。デフォルトでは、現在日付になっています。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	指定したマシンのリカバリポイントをアーカイブします。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-archiveusername	省略可能。ネットワークパスのみで必要です。
-archivepassword	省略可能。ネットワークパスのみで必要です。
-comment	省略可能。例：-comment 'Before install new application'。

例：

Core 上のすべてのマシンのすべてのリカバリポイントをアーカイブします。

```
>Start-Archive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-AttachabilityCheck

Start-AttachabilityCheck コマンドは、Core で保護されるすべての SQL Server データベースに対してアタッチ可否チェックを強制的に実行します。

使用法：

コマンドの使用法を次に示します。

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]  
- protectedserver [machine name | IP address] -rpn [number | numbers] | -time [time string]
```

コマンドオプション

次の表は、Start-AttachabilityCheck コマンドで使えるオプションを説明しています。

表 278. Start-AttachabilityCheck コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	SQL アタッチ可否チェックを実行する保護対象マシン。
-rpn	省略可能。SQL アタッチ可否チェックを実行するリカバリポイントの連番。 -GetRecoveryPoints コマンドを使用して、リカバリポイント番号を取得できます。1つのコマンドで複数のリカバリポイントに対してチェックを実行するには、番号の間をスペースで区切って指定します。 ① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがアタッチ可否チェックに使用されます。
-time	省略可能。SQL アタッチ可否チェックに使用するリカバリポイントを決定します。“MM/DD/YYYY hh:mm tt”（例：“04/24/2015 09:00 AM”）の形式で正確な時刻を指定する必要があります。ローカルマシンで設定されているタイムゾーンでの日時の値を指定します。 ① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。

例：

指定された保護対象 SQL server の最新のリカバリポイントで:SQL アタッチ可否チェックを実行します。

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start-ChecksumCheck

Start-ChecksumCheck PowerShell コマンドを使用して、Exchange Server のリカバリポイントのチェックサムチェックを強制的に行うことができます。

使用法：

コマンドの使用法を次に示します。

```
Start-ChecksumCheck -core [host name] -user [login] -password [password] -protectedserver [name  
| IP address] -rpn [number | numbers] | -time [time string]
```

コマンドオプション

次の表は、Start-ChecksumCheck コマンドで使用できるオプションを説明しています。

表 279. Start-ChecksumCheck コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	保護対象マシンの名前。
-rpn	省略可能。チェーン削除の場合のみ (ベースイメージと増分またはオーファン状態のポイントのチェーン)。チェックするリカバリポイントの連続する番号 (Get-RecoveryPoints コマンドを使用して番号を取得)。番号の間をスペースで区切って指定することで、1つのコマンドで複数のリカバリポイントを削除できます。
-time	省略可能。連続した番号の代わりに、作成時間でチェックするリカバリポイントを選択します。正確な日時を「mm/dd/yyyy hh:mm tt」形式 (「2/24/2012 09:00 AM」など) で指定します。コンピューターで設定されているタイムゾーンでの日時の値を指定します。

例：

2つのリカバリポイントでチェックサムチェックを開始します。

```
> Start-ChecksumCheck -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 5 7
```

Start-EsxiExport

Start-EsxiExport PowerShell コマンドは、ESX(i) サーバの仮想マシンに対して、選択された Rapid Recovery リカバリポイントから仮想エクスポートの起動を開始します。

必須パラメータには、エクスポートするリカバリポイントを含む保護対象マシンの名前、エクスポート先となる仮想マシンの名前、仮想マシンに割り当てられる RAM 容量、Linux サーバーホストのホスト名とポート、および生成された仮想マシンファイルを保存するローカルフォルダ、ネットワークフォルダ、または Linux フォルダへのパスがあります。

使用法：

コマンドの使用法を次に示します。

```
Start-EsxiExport -core [host name] -user [user name] -password [password] -protectedserver [machine name | IP address] -volumes [volume names] -rpn [number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm]
```

コマンドオプション

次の表は、Start-EsxiExport コマンドで使用できるオプションを説明しています。

表 280. Start-EsxiExport コマンドオプション

オプション	説明
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	リカバリポイントをエクスポートする保護対象マシン。
-volumes	省略可能。エクスポートするボリューム名のリスト。指定しない場合、指定されたリカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。たとえば、「C:/」ではなく、「C:」と指定します。

オプション	説明
-rpn	省略可能。エクスポートするリカバリポイントの連番 Get-RecoveryPoints コマンドを使用して、リカバリポイント番号を取得できます。 ❶ メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-time	省略可能。エクスポート対象として選択されるリカバリポイントを特定します。“MM/DD/YYYY hh:mm tt” (例: “04/24/2015 09:00 AM”) の形式で正確な時刻を指定する必要があります。ローカルマシンで設定されているタイムゾーンでの日時の値を指定します。 ❶ メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-vmname	仮想マシンのウィンドウ名。
-hostname	仮想サーバーのホスト名。
-hostport	仮想サーバーのポート番号。
-hostusername	仮想サーバーホストに対するユーザー名。
-hostpassword	仮想サーバーホストに対するパスワード。
-ram	仮想サーバー上に特定の容量の RAM を割り当てます。
-usesourceram	省略可能。ソース保護対象マシンと同じ容量の RAM を仮想サーバーに割り当てます。
-diskprovisioning	省略可能。仮想マシンに割り当てられるディスク容量。仮想ディスクに保護対象サーバー上の元のドライブと同じ大きさを割り当てる場合は「thick」、元のドライブの実際のディスク容量に数メガバイトを追加した量を割り当てる場合は「thin」を指定します。 デフォルトでは、「thin」プロビジョニングが選択されています。
-diskmapping	省略可能。「auto」、「manual」、「withvm」のいずれかを選択します。デフォルトでは、自動マッピングが有効になっています。
-resetup	省略可能。仮想マシンが指定した場所に既に存在している場合は仮想マシンを再作成します。
-datacenter	省略可能。使用するデータセンターを指定します。
-resourcepool	省略可能。使用するリソースプールを指定します。
-datastore	省略可能。使用するデータストアを指定します。
-computeresource	省略可能。使用する計算リソースを指定します。
-version	省略可能。使用する ESXi のバージョンを指定します。

Start-HypervExport

Start-HypervExport PowerShell コマンドは、Hyper-V サーバの仮想マシンに対して、選択された Rapid Recovery リカバリポイントから仮想エクスポートの起動を開始します。

使用法：

コマンドの使用法を次に示します。

```
Start-HypervExport -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] | -time [time string] [-vmname [uselocalmachine] | -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] -hostpassword [virtual host password] -vmlocation [location]] [-ram [total megabytes] | -usesourceram] -diskformat [VHD | VHDX]
```

コマンドオプション

次の表は、Start-HypervExport コマンドで使用できるオプションを説明しています。

表 281. Start-HypervExport コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	リカバリポイントをエクスポートする保護対象マシン。
-volumes	省略可能。エクスポートするボリューム名のリスト。指定しない場合、指定されたリカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。たとえば、「C:/」ではなく、「C:」と指定します。
-rpn	省略可能。エクスポートするリカバリポイントの連番 Get-RecoveryPoints コマンドを使用して、リカバリポイント番号を取得できます。 ① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-time	省略可能。エクスポート対象として選択されるリカバリポイントを特定します。“MM/DD/YYYY hh:mm tt” (例: “04/24/2015 09:00 AM”) の形式で正確な時刻を指定する必要があります。ローカルマシンで設定されているタイムゾーンでの日時の値を指定します。 ① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-vmname	仮想マシンのウィンドウ名。
-gen2	省略可能。2 番目の VM の世代を使用することを指定します。指定されていない場合は、第 1 世代が使用されます。Rapid Recovery は、Windows Server 2012 R2 ~ Windows 8.1 で第 2 世代をサポートします。

オプション	説明
-usevhdx	省略可能。このオプションを指定した場合、Rapid Recovery は、VHDX ディスクフォーマットを使用して仮想マシンを作成します。指定しない場合は、VHD ディスクフォーマットを使用します。第 2 世代では VHDX 形式のみを使用します。
-uselocalmachine	省略可能。ローカル Hyper-V サーバーを接続します。このパラメータを使用すると、hostname、host port、host username、host password の各オプションは無視されます。
-hostname	仮想サーバーのホスト名。
-hostport	仮想サーバーのポート番号。
-hostusername	仮想サーバーホストに対するユーザー名。
-hostpassword	仮想サーバーホストに対するパスワード。
-vmlocation	仮想マシンファイルを保存するフォルダのローカルまたはネットワークパス。
-ram	仮想サーバー上に特定の容量の RAM を割り当てます。
-usesourceram	省略可能。ソース保護対象マシンと同じ容量の RAM を仮想サーバーに割り当てます。

Start-LogTruncation

Start-LogTruncation コマンドは、指定された保護対象の SQL Server または Microsoft Exchange Server に対して、ログの切り捨てを強制的に実行します。

使用法：

コマンドの使用法を次に示します。

```
Start-LogTruncation -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -target [sql | exchange]
```

コマンドオプション

次の表は、Start-LogTruncation コマンドで使用できるオプションを説明しています。

表 282. Start-LogTruncation コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-protectedserver	指定したマシンのリカバリポイントのアーカイブ。
-target	ログの切り捨てのタイプ（「sql」または「exchange」のいずれか）を指定します。指定しない場合は、すべてのデータベースでログが切り捨てられます。

例：

SQL ログを切り捨てます。

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

Core 上のすべてのマシンのすべてのリカバリポイントで Exchange Server ログを切り捨てます。

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

Start-MountabilityCheck コマンドは、保護対象 Microsoft Exchange メールストアに対してマウント可否チェックを強制的に実行します。

使用法：

コマンドの使用法を次に示します。

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -rpn [number | numbers] | -time [time string]
```

コマンドオプション

次の表は、Start-MountabilityCheck コマンドで使用できるオプションを説明しています。

表 283. Start-MountabilityCheck コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	指定したマシンのリカバリポイントのアーカイブ。
-rpn	省略可能。エクスポートするリカバリポイントの連番-GetRecoveryPoints コマンドを使用して、リカバリポイント番号を取得できます。

オプション	説明
	① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-time	省略可能。エクスポート対象として選択されるリカバリポイントを特定します。“MM/DD/YYYY hh:mm tt”（例：“04/24/2015 09:00 AM”）の形式で正確な時刻を指定する必要があります。ローカルマシンで設定されているタイムゾーンでの日時の値を指定します。
	① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。

例：

Core 上のすべてのマシンのすべてのリカバリポイントに対してマウント可否チェックを開始します。

```
> Start-MountabilityCheck -protected EX01
```

Start-Protect

Start-Protect コマンドを使用すると、管理者は Core で保護されているサーバを追加できます。

使用法：

```
Start-Protect -core [host name] -user [user name] -password [password] -repository [repository name] -agent [name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -volumes [volume names]
```

コマンドオプション

次の表は、Start-Protect コマンドで使用できるオプションを説明しています。

表 284. Start-Protect コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-repository	保護対象マシンのデータの保存先の Core 上のリポジトリ名。
-agentname	保護対象マシンの名前または IP アドレス。
-agentusername	保護対象サーバーへのログオン。

オプション	説明
-agentpassword	保護対象サーバーへのパスワード。
-agentport	保護対象サーバーのポート番号。
-volumes	保護するボリュームのリスト。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。たとえば、"c:" や "d:" です。

例：

次のコマンドでは、サーバーのボリュームを保護します。

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername administrator -agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

Start-ProtectCluster コマンドを使用すると、管理者は Core で保護されているサーバークラスタを追加できます。

使用法：

コマンドの使用法を次に示します。

```
Start-ProtectCluster -core [host name] -user [user name] -password [password] -repository [repository name] -clustername [name | IP address] -clusterusername [user name for cluster] -clusterpassword [password for cluster] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes names and volumes]
```

コマンドオプション

次の表は、Start-ProtectCluster コマンドで使用できるオプションを説明しています。

表 285. Start-ProtectCluster コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-repository	保護対象マシンのデータの保存先の Core 上のリポジトリ名。名前は二重引用符で囲む必要があります。
-clustername	保護するクラスタの名前。
-clusterusername	保護対象クラスタに対するユーザー名。

オプション	説明
-clusterpassword	保護対象クラスタへのパスワード。
-clusterport	保護対象クラスタに対するポート番号。
-clustervolumes	保護するボリュームのリスト。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。たとえば、「c:」や「d:」と指定します。
-clusternodes	保護するボリュームを持つクラスタノードのリスト。まず、ラベル「nodename」を指定してから、ノード名を入力します。次に、ラベル「volumes」を指定してから、ノードのボリュームのリストを入力します。 例: "nodename", "10.10.10.10", "volumes", "c:", "e:", "nodename", "10.10.10.11", "volumes", "c:"

例：

次のコマンドでは、サーバーのボリュームを保護します。

```
>Start-ProtectCluster -repository "Repository 1" -clustername 10.10.9.120 -clusterusername administrator -clusterpassword 12345 -clusterport 5002 -clustervolumes "c:" "d:" -clusternodes nodename 10.10.10.10 volumes "c:" "e:"
```

Start-RepositoryCheck

Start-RepositoryCheck PowerShell コマンドを使用して、リポジトリの整合性をチェックすることができます。

使用法：

コマンドの使用法を次に示します。

```
Start-RepositoryCheck -name [repository name] | -all [check all repositories] -password [password] -force
```

コマンドオプション

次の表は、Start-RepositoryCheck コマンドで使用できるオプションを説明しています。

表 286. Start-RepositoryCheck コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。

オプション	説明
	指定しない場合は、ログオンユーザーの資格情報が使用されます。
-repository	必須。チェックするリポジトリの名前。
-all	省略可能。Core に関連付けられているすべてのリポジトリをチェックします。
-force	省略可能。確認メッセージを表示せずに、リポジトリチェックを実行します。

例：

リポジトリチェックを開始します。

```
>Start-RepositoryCheck -repository newRepository1 -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd
```

Start-RestoreArchive

企業では、準拠および非準拠データの両方のアーカイブに長期ストレージを使用することがよくあります。Rapid Recovery のアーカイブ機能は、準拠および非準拠データの延長保持をサポートするために使用します。管理者は、-Path コマンドと資格情報を指定して、アーカイブをローカルストレージやネットワークの場所に保存できます。

使用法：

コマンドの使用法を次に示します。

```
Start-RestoreArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -repository [name] -archiveusername [name] -archivepassword [password] -path [location] -cloudaccountname [name] -cloudcontainer [name]
```

コマンドオプション

次の表は、Start-RestoreArchive コマンドで使用できるオプションを説明しています。

表 287. Start-RestoreArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-all	すべての保護対象マシンのリカバリポイントをアーカイブします。
-protectedserver	アーカイブするリカバリポイントが含まれる保護対象マシン。複数のマシン名を指定するには、二重引用符で囲み、カンマで区切ります。
-repository	復元されたリカバリポイントを配置するリポジトリの名前。名前を二重引用符で囲む必要があります (例: "Repository1")。
-archiveusername	省略可能。リモートマシンにログインするためのユーザー名。ネットワークパスのみで必要です。
-archivepassword	省略可能。リモートマシンにログインするためのパスワード。ネットワークパスのみで必要です。
-path	アーカイブされたデータを保存する場所のパス。たとえば、次のとおりです。 - ローカルマシン: "d:\work\archive" - ネットワークパス: "\\servername\sharename " - クラウドアカウントのフォルダ: "フォルダ名"  メモ: シンボルの数は、ローカルおよびネットワークの場所の場合は 100 以下、クラウドの場所の場合は 150 以下にする必要があります。
-cloudaccountname	省略可能。クラウドアーカイブのみで使用します。アーカイブを保存するクラウドアカウントの名前。
-cloudcontainer	省略可能。クラウドアーカイブのみで使用します。選択したクラウドアカウント内でアーカイブが保存されるクラウドコンテナの名前。このオプションを使用するときには、"-cloudaccountname" パラメーターも指定する必要があります。
-manifestcore	省略可能。復元されたアーカイブの目録から使用する Core を指定します。

例：

Core 上のすべてのマシンのすべてのリカバリポイントをアーカイブし、それらをローカルマシンに保存します。

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-ScheduledArchive

Start-ScheduledArchive PowerShell コマンドを使用して、Rapid Recovery でスケジュール設定されたアーカイブを強制的に開始できます。事前に確立されたスケジュールは関係ありません。

使用法：

コマンドの使用法を次に示します。

```
Start-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

コマンドオプション

次の表は、Start-ScheduledArchive コマンドで使用できるオプションを説明しています。

表 288. Start-ScheduledArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	スケジュールされたすべてのアーカイブを強制します。
-id	強制するスケジュールされたアーカイブの識別番号またはスペースで区切られた識別子。

例：

スケジュールされた複数のアーカイブジョブを開始します。

```
>Start-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Start-VBExport

start-VBExport コマンドは、Oracle VirtualBox サーバの仮想マシンに対して、選択されたリカバリポイントから仮想エクスポートの起動を開始します。

必須パラメータには、エクスポートするリカバリポイントを含む保護対象マシンの名前、エクスポート先となる仮想マシンの名前、仮想マシンに割り当てられる RAM 容量、Linux サーバーホストのホスト名とポート、および生成された仮想マシンファイルを保存するローカルフォルダ、ネットワークフォルダ、または Linux フォルダへのパスがあります。

使用法：

コマンドの使用法を次に示します。

```
Start-VBExport -core -user [user name] -password [password] -protectedserver [machine name] or  
[IP address] -volumes [volume names] -rpn [number | numbers] |  
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |  
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]  
pathusername [user name] - pathpassword [password]
```

コマンドオプション

次の表は、Start-VBExport コマンドで使用できるオプションを説明しています。

表 289. Start-VBExport コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	リカバリポイントをエクスポートする保護対象マシン。
-volumes	省略可能。エクスポートするボリューム名のリスト。指定しない場合、指定されたリカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。たとえば、「C:/」ではなく、「C:」と指定します。
-rpn	省略可能。エクスポートするリカバリポイントの連番 (Get-RecoveryPoints コマンドを使用して、リカバリポイント番号を取得できます) ① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-time	省略可能。エクスポート対象として選択されるリカバリポイントを特定します。“MM/DD/YYYY hh:mm tt” (例: “04/24/2015 09:00 AM”) の形式で正確な時刻を指定する必要があります。ローカルマシンで設定されているタイムゾーンでの日時の値を指定します。 ① メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-vmname	仮想マシンのウィンドウ名。
-ram	仮想サーバー上に特定の容量の RAM を割り当てます。
-usesourceram	省略可能。ソース保護対象マシンと同じ容量の RAM を仮想サーバーに割り当てます。
-linuxhostname	Linux VirtualBox サーバーのホスト名。
-hostport	Linux VirtualBox サーバーのポート。
-targetpath	仮想マシンのファイルを保存するフォルダのローカルパス、ネットワークパス、または Linux パス。
-pathusername	ネットワークマシンに対するユーザー名。パラメーター -targetpath でネットワークパスを指定する場合にのみ必要です。
-pathpassword	ネットワークマシンに対するパスワード。パラメーター -targetpath でネットワークパスを指定する場合にのみ必要です。

オプション	説明
- accountusername	省略可能。エクスポートした仮想マシンを登録するユーザーアカウントを指定できる場合に使用します。ローカルマシンまたはネットワークマシンのみで使用するオプション。
- accountpassword	省略可能。パラメーター -accountusername. を使用して、エクスポートした仮想マシンを登録するユーザーアカウントを指定できる場合にのみ使用します。ローカルマシンまたはネットワークマシンのみで使用するオプション。

例：

マシン 10.10.12.97 の最新のリカバリポイントからすべてのボリュームを NewVirtualBoxVM という仮想マシンにエクスポートします。

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram usesourceram -targetpath D:/exports
```

Start-VirtualStandby

Start-VirtualStandby PowerShell コマンドを使用すると、Rapid Recovery でデータを仮想スタンバイマシンに強制的にエクスポートできます。このオンデマンドエクスポートは、定期的にスケジュールされている仮想スタンバイへのエクスポート以外で実行することができます。

使用法：

コマンドの使用法を次に示します。

```
Start-VirtualStandby -core [host name] -user [login] -password [password] -all | -protectedserver [name(s) | IP address]
```

コマンドオプション

次の表は、Start-VirtualStandby コマンドで使用できるオプションを説明しています。

表 290. Start-VirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	すべての仮想スタンバイマシンのエクスポートを強制します。

オプション	説明
- protectedserver	カンマとスペースで区切ったエクスポートを強制する保護対象マシンの名前（複数可）。

例：

保護対象マシンの仮想スタンバイのエクスポートを強制します。

```
>Start-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Start-VMExport

Start-VMExport コマンドは、VMware Workstation サーバの仮想マシンに対して、選択されたリカバリポイントから仮想エクスポートの起動を開始します。

必須パラメータには、エクスポートするリカバリポイントを含む保護対象マシンの名前、エクスポート先となる仮想マシンの名前、仮想マシンに割り当てられる RAM 容量、および生成された仮想マシンファイルを保存するローカルフォルダまたはネットワークフォルダへのパスがあります。

使用法：

コマンドの使用法を次に示します。

```
Start-VMExport -core -user [user name] -password [password] -protectedserver [machine name] or
[IP address]] -volumes [volume names] -rpn [number | numbers] |
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]
pathusername [user name] - pathpassword [password]
```

コマンドオプション

次の表は、Start-VMExport コマンドで使用できるオプションを説明しています。

表 291. Start-VMExport コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
- protectedserver	リカバリポイントをエクスポートする保護対象マシン。

オプション	説明
-volumes	省略可能。エクスポートするボリューム名のリスト。指定しない場合、指定されたリカバリポイントのすべてのボリュームがエクスポートされます。ボリュームを二重引用符で囲み、ボリューム間はスペースで区切る必要があります。ボリューム名の末尾にスラッシュを使用しないでください。たとえば、「C:/」ではなく、「C:」と指定します。
-rpn	省略可能。エクスポートするリカバリポイントの連番 Get-RecoveryPoints コマンドを使用して、リカバリポイント番号を取得できます。 ❶ メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-time	省略可能。エクスポート対象として選択されるリカバリポイントを特定します。“MM/DD/YYYY hh:mm tt” (例: “04/24/2015 09:00 AM”) の形式で正確な時刻を指定する必要があります。ローカルマシンで設定されているタイムゾーンでの日時の値を指定します。 ❶ メモ: このコマンドで「time」と「rpn」のどちらのオプションも指定しない場合は、最新のリカバリポイントがエクスポートされます。
-vmname	仮想マシンのウィンドウ名。
-ram	仮想サーバー上に特定の容量の RAM を割り当てます。
-usesourceram	省略可能。ソース保護対象マシンと同じ容量の RAM を仮想サーバーに割り当てます。
-targetpath	仮想マシンのファイルを保存するフォルダのローカルパス、ネットワークパス、または Linux パス。
-pathusername	ネットワークマシンに対するユーザー名。パラメーター -targetpath でネットワークパスを指定する場合にのみ必要です。
-pathpassword	ネットワークマシンに対するパスワード。パラメーター -targetpath でネットワークパスを指定する場合にのみ必要です。
-version	使用する VMware Tools のバージョン。有効なバージョンは、7、8、9、10 です。

例 :

マシン 10.10.12.97 の最新のリカバリポイントからすべてのボリュームを NewVMwareVM という仮想マシンにエクスポートします。

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -targetpath D:/exports
```

Stop-ActiveJobs

Stop-ActiveJobs コマンドは、指定された保護対象マシンのアクティブジョブをキャンセルします。

使用法 :

コマンドの使用法を次に示します。

```
Stop-ActiveJobs [-protectedserver [machine name | IP address]] [-core [host name]] -user [user name] -password [password] -jobtype [jobtype]
```

コマンドオプション

次の表は、Stop-ActiveJobs コマンドで使用できるオプションを説明しています。

表 292. Stop-ActiveJobs コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	すべての保護対象マシンで、指定されたタイプのイベントを選択およびキャンセルします。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	ジョブをキャンセルする保護対象マシンを特定します。
-jobtype	省略可能。ジョブタイプのフィルタを指定します。使用できる値: 「transfer」 (データ転送)、「repository」 (リポジトリのメンテナンス)、「replication」 (ローカルおよびリモートレプリケーション)、「backup」 (バックアップおよびリストア)、「bootcdbuilder」 (ブート CD の作成)、「diagnostics」 (ログのアップロード)、「exchange」 (Exchange Server ファイルのチェック)、「export」 (リカバリポイントのエクスポート)、「pushinstall」 (保護対象マシンへの Agent ソフトウェアの導入)、「rollback」 (リカバリポイントからのデータのリストア)、「rollup」 (リカバリポイントのロールアップ)、「sqlattach」 (Agent のアタッチ可否チェック)、「mount」 (リポジトリのマウント)。デフォルトでは、指定したタイプのすべてのジョブがキャンセルされます。

例：

保護対象マシンで転送ジョブを停止します。

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -jobtype transfer
```

特定の保護対象マシンですべてのジョブを停止します。

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -all
```

Suspend-Replication

Suspend-Replication コマンドを使用すると、管理者はレプリケーションを一時停止できます。

ユーザーは、次の3つの方法でレプリケーションを一時停止できます。

- すべての保護対象マシンのマスター Core 上のレプリケーションを一時停止します (-outgoing parameter)。管理者は、送信レプリケーションのペア設定を使用してリモートマシン名を指定し、マスタ Core 上の送信レプリケーションを一時停止する必要があります。

```
>Suspend-replication -outgoing 10.10.12.10
```
- 1つの保護対象マシンのマスター Core 上のレプリケーションを一時停止します (-protectedserver パラメーター)。

```
>Suspend-replication -protectedserver 10.10.12.97
```
- ターゲット Core 上のレプリケーションを一時停止します (-incoming parameter パラメーター)。ローカル Core がターゲット Core の場合、管理者は incoming パラメータでマスタ Core を指定して、レプリケーションを一時停止できます。

コマンドオプション

次の表は、Suspend-Replication コマンドで使用できるオプションを説明しています。

表 293. Suspend-Replication コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	選択した Core 上のすべての保護対象マシンを一時停止します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-pause	[snapshots]、[replication]、または [vmexport]。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-protectedserver	現在の保護対象サーバーを一時停止します。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-incoming	Core マシンにレプリケートするリモート Core のホスト名。リモート Core 上のすべての保護対象マシンに対してレプリケーションが一時停止されます。
-outgoing	データがレプリケートされるリモートターゲット Core のホスト名。リモート Core 上のすべての保護対象マシンに対してレプリケーションが一時停止されます。

例 :

1つの保護対象マシン (IP アドレス : 10.10.1.76) に対してリモート Core (IP アドレス : 10.10.1.15) 上の送信レプリケーションを一時停止します。

```
>Suspend-replication -core 10.10.1.15 -protectedserver 10.10.1.76
```

すべての保護対象マシンのローカル Core からリモートターゲット (IP アドレス : 10.10.1.63) への送信レプリケーションを一時停止します。

```
>Suspend-replication -outgoing 10.10.1.63
```

10.10.1.82 からのリモート Core (IP アドレス : 10.10.1.15) への受信レプリケーションを一時停止します (管理者は、マシン全体の受信レプリケーションのみ一時停止できます)。

```
>Suspend-replication -core 10.10.1.15 -incoming 10.10.1.82
```

Suspend-RepositoryActivity

Suspend-RepositoryActivity PowerShell コマンドを使用して、Rapid Recovery リポジトリのアクティビティを一時停止することができます。アクティビティを一時停止すると、データを入力または終了できないようリポジトリがロックされます。

使用法 :

コマンドの使用法を次に示します。

```
Suspend-RepositoryActivity -core [host name] -user [login] -password [password] -all | -repository ["name" | "name1 " "name2"]
```

コマンドオプション

次の表は、Suspend-RepositoryActivity コマンドで使用できるオプションを説明しています。

表 294. Suspend-RepositoryActivity コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	Core に関連付けられているすべてのリポジトリのアクティビティを一時停止します。
-repository	ロックしたいリポジトリの名前。名前は二重引用符で囲む必要があります。いくつかのスペースで区切られたリポジトリを指定することができます。

例 :

複数のリポジトリのアクティビティを一時停止します。

```
>Suspend-RepositoryActivity -repository "repository1" "repository2"
```

すべてのリポジトリのアクティビティを一時停止します。

```
>Suspend-RepositoryActivity -all
```

Suspend-ScheduledArchive

Suspend-ScheduledArchive PowerShell コマンドを使用して、Rapid Recovery のスケジュール設定されたアーカイブを一時停止することができます。このコマンドにより、再アクティブ化するまでアーカイブがスケジュールどおりに実行されなくなります。

使用法：

コマンドの使用法を次に示します。

```
Suspend-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

コマンドオプション

次の表は、Suspend-ScheduledArchive コマンドで使用できるオプションを説明しています。

表 295. Suspend-ScheduledArchive コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	すべてのスケジュール設定されたアーカイブを一時停止します。
-id	一時停止するスケジュールされたアーカイブの識別番号またはスペースで区切られた番号。

例：

複数のスケジュールされたアーカイブを一時停止します。

```
>Suspend-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Suspend-Snapshot

Suspend-Snapshot コマンドを使用すると、管理者はスナップショットを一時停止できます。

使用法：

コマンドの使用法を次に示します。

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |  
-protectedserver [name | IP address] -time [time string]
```

コマンドオプション

次の表は、Suspend-Snapshot コマンドで使用できるオプションを説明しています。

表 296. Suspend-Snapshot コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-all	選択した Core 上のすべての保護対象マシンを一時停止します。
-core	省略可能。リモート Core のホストマシンの IP アドレス（省略可能なポート番号を含む）。 デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-time	スナップショットを再開する時間。'Day-Hours-Minutes'」形式で指定（スナップショットが一時停止している場合のみ）。

例：

ローカル Core の保護対象マシン（IP 10.10.10.4）のスナップショットを一時停止し、特定の時間で再開します。

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend-VirtualStandby

Suspend-VirtualStandby PowerShell コマンドを使用すると、Rapid Recovery 仮想スタンバイマシンへのデータのエクスポートを一時停止することができます。

使用法：

コマンドの使用法を次に示します。

```
Suspend-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP address]
```

コマンドオプション

次の表は、Suspend-VirtualStandby コマンドで使用できるオプションを説明しています。

表 297. Suspend-VirtualStandby コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ログオンも入力する必要があります。 指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	すべての仮想スタンバイマシンのエクスポートを一時停止します。
-protectedserver	カンマとスペースで区切った一時停止する仮想スタンバイマシンが含まれる保護対象マシンの名前 (複数可)。

例 :

保護対象マシンの仮想スタンバイのエクスポートを一時停止します。

```
>Suspend-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$$sdd -protectedserver 10.10.5.22
```

Suspend-VMExport

Suspend-VMExport コマンドを使用すると、管理者は仮想マシンへのエクスポートを一時停止できます。

使用法 :

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

コマンドオプション

次の表は、Suspend-VMExport コマンドで使用できるオプションを説明しています。

表 298. Suspend-VMExport コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-all	選択した Core 上のすべての保護対象マシンを一時停止します。
-protectedserver	現在の保護対象サーバーを一時停止します。

例：

ローカル Core の保護対象マシン (IP 10.10.10.4) に対して仮想マシンのエクスポートを中断します。

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

Update-Repository コマンドは、既存のリポジトリにエクステントを追加します。250 MB ~ 16 TB のサイズを指定する必要があります。

使用法：

```
Update-Repository -name [repository name] -size [size] [[[-datapath [datapath]
-metadatapath [metadata path]] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password]]] -core [host name] -user [user name]
-password [password]
```

コマンドオプション

次の表は、Update-Repository コマンドで使用できるオプションを説明しています。

表 299. Update-Repository コマンドオプション

オプション	説明
-?	ヘルプメッセージを表示します。
-core	省略可能。リモート Core のホストマシンの IP アドレス (省略可能なポート番号を含む)。デフォルトでは、ローカルマシンにインストールされている Core に接続されます。
-user	省略可能。リモート Core のホストマシンに対するユーザー名。ユーザー名を指定した場合は、パスワードも入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。

オプション	説明
-password	省略可能。リモート Core のホストマシンに対するパスワード。パスワードを指定した場合は、ユーザー名も入力する必要があります。指定しない場合は、ログオンユーザーの資格情報が使用されます。
-name	DVM リポジトリ名。
-size	DVM リポジトリのエクステンツのサイズ。使用できる単位は、b、Kb、MB、GB、TB、PB です。
-datapath	ローカルのみ。DVM リポジトリのエクステンツのデータパスを決定します。
-metadatapath	ローカルのみ。DVM リポジトリのエクステンツのメタデータパスを決定します。
-uncpath	共有のみ。DVM リポジトリのエクステンツのデータおよびメタデータパスを決定します。
-shareusername	共有のみ。場所を共有するためのログインを決定します。
-sharepassword	共有のみ。場所を共有するためのパスワードを決定します。

例：

最小サイズの DVM リポジトリにエクステンツを追加します。

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -metadatapath C:\repository\Metadata
```

ローカライゼーションローからいぜーしょん

Rapid Recovery Core がインストールされているマシンで Rapid Recovery PowerShell モジュールを実行すると、その表示言語は、Core で設定されている言語がベースになります。このバージョンなどのローカライズされた Rapid Recovery のバージョンは、英語、中国語（簡体字）、フランス語、韓国語、ドイツ語、日本語、ポルトガル語（ブラジル）、およびスペイン語をサポートします。

Rapid Recovery PowerShell モジュールが別のマシンにインストールされている場合、英語のみがサポートされます。

修飾子しゅうしょくし

次の表は、Rapid Recovery PowerShell モジュールで使える修飾子を説明しています。

表 300. Rapid Recovery PowerShell モジュール修飾子

修飾子	使用法：
-core <Rapid Recovery Core Name>	Core のホスト名。 デフォルト：localhost
-ProtectedServer <Protected Server Name>	Rapid Recovery Agent のホスト名/IP アドレス。 デフォルト：localhost（複数のサーバが保護される場合）。これ以外の場合は1台のサーバが保護されます。
-Mode <READ, READWRITE, WRITE>	リカバリポイントのマウントモード。 デフォルト：Read。
-Volumes <Snapshot Volume Letter>	Rapid Recovery Agent からのスナップショットボリューム文字。 デフォルト：All。

修飾子

使用法：

-User <User Name>

Rapid Recovery Core に接続するために使用されるユーザー名。
通常、これはサービスユーザーになります。

-Domain <Domain Name>

/User で定義されたユーザーが属するドメイン。

-Password <Password>

/User で定義されるユーザーのパスワード。

-Path <Target path to mount,
dismount recovery points or
archive location>

例：C:\RapidRecoveryMount。

スクリプトによる Rapid Recovery ジョブの拡張

管理者は Rapid Recovery を使用してコマンドやスクリプトを実行することで、特定のタイミングでのリソースの制御や管理を自動化できます。Rapid Recovery ソフトウェアは、Windows 用 PowerShell Scripting と Linux 用 Bourne Shell Scripting の使用をサポートしています。

Rapid Recovery Core で、レプリケーション、仮想エクスポート、またはバックアップスナップショットなどの操作を開始すると、Core ジョブが自動的に作成されます。これらのジョブは、その前後にスクリプトを実行して拡張することができます。これらは、事前スクリプトおよび事後スクリプトと呼ばれます。

本項には、Rapid Recovery for Windows および Linux で管理者が指定されたタイミングで使用できるスクリプトについての説明が記載されています。

△ 注意: このドキュメントで提供されている **PowerShell** と **Bourne** のサンプルスクリプトは、適格な管理者によって設計どおりに実行されると機能します。作業バージョンを保持するために機能しているスクリプトに変更を加える場合は、注意が必要です。このドキュメントに含まれるサンプルスクリプトに行った変更、つまり、ユーザーが作成したスクリプトは、カスタマイズと見なされ、通常、**Dell** サポートのサポート対象となりません。

トピック：

- ・ [Rapid Recovery での PowerShell スクリプトの使用](#)
- ・ [PowerShell Scripting の入力パラメータ](#)
- ・ [PowerShell スクリプトのサンプル](#)
- ・ [Rapid Recovery での Bourne Shell スクリプティングの使用](#)
- ・ [Bourne Shell スクリプティングの入力パラメータ](#)
- ・ [Bourne Shell スクリプトのサンプル](#)

Rapid Recovery での PowerShell スクリプトの使用

Windows PowerShell は、管理の自動化のために設計された Microsoft .NET Framework 関連環境です。Rapid Recovery には、PowerShell Scripting 用の包括的なクライアントソフトウェア開発キット（SDK）が含まれています。これにより、管理者ユーザーは、指定されたタイミング（たとえば、スナップショット、アタッチ可否およびマウント可否のチェックの前後など）で、ユーザー提供の PowerShell スクリプトを実行できます。管理者は、Rapid Recovery Core と保護対象マシンの両方からスクリプトを実行できます。スクリプトにはパラメータを指定できます。また、スクリプトの出力は Core と保護対象マシンのログファイルに書き込まれます。

① メモ: 夜間ジョブの場合、1つのスクリプトファイルと **JobType** 入力パラメータを保持して夜間ジョブを区別します。

スクリプトファイルは **%ALLUSERSPROFILE%\AppRecovery\Scripts** フォルダにあります。

- ・ Windows 7 の場合、%ALLUSERSPROFILE% フォルダのパスは **C:\ProgramData** です。
- ・ Windows 2003 の場合、フォルダのパスは **Documents and Settings\All Users\Application Data** です。

① メモ: **Rapid Recovery** スクリプトを実行する前に、**Windows PowerShell** が必要であり、これがインストールされ、設定されている必要があります。

PowerShell スクリプトの使用の詳細については、「[PowerShell スクリプトのサンプル](#)」、「[PowerShell Scripting の入力パラメータ](#)」、「[Bourne Shell スクリプティングの入力パラメータ](#)」、「[Bourne Shell スクリプトのサンプル](#)」を参照してください。

PowerShell Scripting の前提条件

Rapid Recovery で PowerShell スクリプトを実行するには、Windows PowerShell 2.0 以降がインストールされている必要があります。PowerShell 3.0 では、オブジェクトプロパティへの簡単なアクセス、PowerShell Web アクセス、REST 呼び出しのサポートなどの新機能が導入されているため、Dell では、PowerShell 3.0 以降を使用することをお勧めします。

① **メモ:** powershell.exe.config ファイルを PowerShell ホームディレクトリに配置します。たとえば、C:\WindowsPowerShell\powershell.exe.config です。

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0.30319"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

PowerShell スクリプトのテスト

実行する予定のスクリプトをテストしたい場合は、PowerShell グラフィカルエディタ powershell_is を使用してこれを行うことができます。設定ファイル powershell_is.exe.config を設定ファイル powershell.exe.config と同じフォルダに追加する必要があります。

① **メモ:** 設定ファイル powershell_is.exe.config には、powershell.exe.config ファイルと同じ内容が存在する必要があります。

△ **注意:** PowerShell スクリプトの前後の処理が失敗すると、ジョブも失敗します。

ローカライゼーションローからいぜーしょん

Rapid Recovery Core がインストールされているマシンで Rapid Recovery PowerShell モジュールを実行すると、その表示言語は、Core で設定されている言語がベースになります。このような Rapid Recovery のローカライズされたバージョンでは、英語、中国語（簡体字）、フランス語、韓国語、ドイツ語、日本語、ポルトガル語（ブラジル）、およびスペイン語がサポートされています。

Rapid Recovery PowerShell モジュールが別のマシンにインストールされている場合、英語のみがサポートされます。

修飾子しゅうしょくし

次の表は、Rapid Recovery PowerShell モジュールで使える修飾子を説明しています。

表 301. Rapid Recovery PowerShell モジュール修飾子

修飾子	使用法：
-core <Rapid Recovery Core Name>	Core のホスト名。

修飾子	使用法 :
	デフォルト : Localhost
-ProtectedServer <Protected Server Name>	Rapid Recovery Agent のホスト名/IP アドレス。 デフォルト : Localhost (複数のサーバが保護される場合)。これ以外の場合は1台のサーバが保護されます。
-Mode <READ, READWRITE, WRITE>	リカバリポイントのマウントモード。 デフォルト : Read。
-Volumes <Snapshot Volume Letter>	Rapid Recovery Agent からのスナップショットボリューム文字。 デフォルト : All。
-User <User Name>	Rapid Recovery Core に接続するために使用されるユーザー名。 通常、これはサービスユーザーになります。
-Domain <Domain Name>	/User で定義されたユーザーが属するドメイン。
-Password <Password>	/User で定義されるユーザーのパスワード。
-Path <Target path to mount, dismount recovery points or archive location>	例 : C:\RapidRecoveryMount。

PowerShell Scripting の入力パラメータ

サンプルスクリプトでは、使用可能な入力パラメータがすべて使用されています。次の表でパラメータについて説明しています。

① | **メモ:** スクリプトファイルは、サンプルスクリプトファイルと同じ名前を処理します。

AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents)

次の表には、AgentProtectionStorageConfiguration パラメータに使用可能なオブジェクトを示しています。

表 302. AgentProtectionStorageConfiguration パラメータのオブジェクト

メソッド	説明
public Guid RepositoryId { get; set; }	Agent のリカバリポイントが保存されるリポジトリの ID を取得または設定します。
public string EncryptionKeyId { get; set; }	この Agent のリカバリポイントの暗号化キー ID を取得または設定します。空のストリングは暗号化されていないことを意味します。

AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

次の表には、AgentTransferConfiguration パラメータに使用可能なオブジェクトを示しています。

表 303. AgentTransferConfiguration パラメータのオブジェクト

メソッド	説明
<code>public uint MaxConcurrentStreams { get; set; }</code>	データを転送するために、Agent に対して Core が確立する同時 TCP 接続の最大数を取得または設定します。
<code>public uint MaxTransferQueueDepth { get; set; }</code>	書き込み用にキューに入れることができるブロックエクステンツの最大数を取得または設定します。ある範囲のブロックを転送ストリームから読み取るときに、その範囲はプロデューサーまたはコンシューマーキューに設定され、コンシューマースレッドはここでエポックオブジェクトに対する読み取りおよび書き込みを行います。リポトリがネットワークの読み取りよりも遅い速度で書き込むと、このキューは満杯になります。キューが満杯になり読み取りが停止する時点が、最大転送キューの深さです。
<code>public uint MaxConcurrentWrites { get; set; }</code>	いつでもエポック上に未処理の書き込みを残しておくようにブロック書き込み操作の最大数を取得または設定します。このパラメーターで指定された書き込み操作の最大数を超えて、追加のブロックを受信した場合、それらの追加ブロックは、未処理のいずれかの書き込みが終了するまで無視されます。
<code>public ulong MaxSegmentSize { get; set; }</code>	1つのリクエストで転送する連続ブロックの最大数を取得または設定します。テストによっては、高い値または低い値が最適になる可能性があります。
<code>public Priority Priority { get; set; }</code>	転送リクエストの優先度を取得または設定します。
<code>public uint GetChangedBlocksRetries { get; set; }</code>	エージェントからの最初の変更済みブロック取得に失敗した場合、再試行の回数を取得または設定します。
<code>public int MaxRetries { get; set; }</code>	失敗した転送が失敗と判断されるまでの最大再試行回数を取得または設定します。
<code>public bool UseDefaultMaxRetries { get; set; }</code>	含まれている場合、デフォルトの最大再試行回数（転送設定で指定）が使用されます。
<code>public Guid ProviderId { get; set; }</code>	このホスト上のスナップショットに使用するための VSS プロバイダの GUID を取得または設定します。管理者は通常デフォルトを受け入れます。
<code>public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }</code>	このスナップショットから除外されるべき VSS ライター ID の集合を取得または設定します。ライター ID はライターの名前で決定されます。この名前は文書化目的にのみ使用され、ライターの名前とは必ずしも一致しません。
<code>public ushort TransferDataServerPort { get; set; }</code>	保護対象マシンから Core へのデータの転送で Core からの接続を受け付けるための TCP ポートを含む値を取得または設定します。保護対象マシンはこのポートでリスンしようとしていますが、ポートが使用中の場合は、保護対象マシンは代わりに別のポートを使用することができます。Core は、スナップショットを実行された各ボリュームの VolumeSnapshotInfo オブジェクトの BlockHashesUri および BlockDataUri プロパティに指定されたポート番号を使用します。
<code>public TimeSpan CleanSnapshotTimeout { get; set; }</code>	転送が完了した後にスナップショットをクリーンアップするまでの待機時間を取得または設定します。
<code>public TimeSpan SnapshotTimeout { get; set; }</code>	VSS スナップショット操作の実行が停止およびタイムアウトするまでの待機時間を取得または設定します。
<code>public TimeSpan TransferTimeout { get; set; }</code>	スナップショットを破棄するまでの、Core からの追加連絡の待機時間を取得または設定します。
<code>public TimeSpan NetworkReadTimeout { get; set; }</code>	転送に関連するネットワーク読み取り操作のタイムアウトを取得または設定します。
<code>public TimeSpan NetworkWriteTimeout { get; set; }</code>	転送に関連するネットワーク書き込み操作のタイムアウトを取得または設定します。
<code>public uint InitialQueueSize { get; set; }</code>	初期キューまたはリクエストのサイズを取得または設定します。

メソッド	説明
public uint MinVolumeFreeSpacePercents { get; set; }	パーセントで測定される、ボリューム上の最小空き容量を取得または設定します。空き容量がこのパラメーターで指定された量より少ない場合、すべての変更ログが削除され、ベースイメージが強制されます。
public uint MaxChangeLogsSizePercents { get; set; }	パーセントで測定される、ボリューム容量の一部であるドライバ変更ログの最大サイズを取得または設定します。変更ログの一部がこの値よりも大きい場合は、すべての変更ログが削除され、ベースイメージが強制されます。
public bool EnableVerification { get; set; }	Core に送信される各ブロックの診断検証を実行すべきかどうかを示す値を取得または設定します。

BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

次の表には、BackgroundJobRequest パラメータに使用可能なオブジェクトを示しています。

表 304. BackgroundJobRequest パラメータのオブジェクト

メソッド	説明
public AgentIdsCollection AgentIds { get; set; }	保護対象マシンの ID を取得または設定します。
public bool IsNightlyJob { get; set; }	バックグラウンドジョブが夜間ジョブであるかどうかを示す値を取得または設定します。
public Guid NightlyJobTransactionId { get; set; }	夜間ジョブトランザクションの ID を取得または設定します。
public Guid JobId { get; set; }	バックグラウンドジョブの ID を取得または設定します。
public bool Force { get; set; }	ジョブが強制されたかどうかを示す値を取得または設定します。
public uint JobStartsCount { get; set; }	ジョブ開始の試行回数を取得または設定します。
public virtual bool InvolvesAgentId(Guid agentId)	指定された Agent がジョブに関わっているかどうかを示す値を判別します。

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

パラメータ DatabaseCheckJobRequestBase から値を継承します。

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

パラメーター BackgroundJobRequest から値を継承します。

表 305. DatabaseCheckJobRequestBase パラメーターのオブジェクト

メソッド	説明
public string RecoveryPointId { get; set; }	データベースが検証されるリカバリポイントの ID を取得または設定します。

ExportJobRequest (namespace Replay.Core.Contracts.Export)

パラメーター BackgroundJobRequest から値を継承します。

次の表には、ExportJobRequest パラメータに使用可能なオブジェクトを示しています。

表 306. ExportJobRequest パラメータのオブジェクト

メソッド	説明
public uint RamInMegabytes { get; set; }	エクスポートされた VM のメモリサイズを取得または設定します。ソースマシンのメモリサイズを使用する場合はゼロ (0) に設定します。
public ushort CpuCount { get; set; }	エクスポートされた VM の CPU の数を取得または設定します。ソースマシンの CPU の数を使用する場合は 0 に設定します。
public ushort CoresPerCpu { get; set; }	エクスポートされた VM の CPU あたりの Core の数を取得または設定します。ソースマシンの CPU あたりの Core の数を使用する場合は 0 に設定します。
public VirtualMachineLocation Location { get; set; }	このエクスポートのターゲットの場所を取得または設定します。これは抽象ベースクラスです。
public VolumemageldsCollection Volumemagelds { get; private set; }	VM エクスポートに含めるボリュームイメージを取得または設定します。
public ExportJobPriority Priority { get; set; }	エクスポートリクエストの優先度を取得または設定します。

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

パラメーター BackgroundJobRequest から値を継承します。

表 307. NightlyAttachabilityJobRequest パラメーターのオブジェクト

メソッド	説明
public int SimultaneousJobsCount { get; set; }	同時に実行できるジョブの数を取得または設定します。

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

パラメーター BackgroundJobRequest から値を継承します。

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

次の表には、TakeSnapshotResponse パラメータに使用可能なオブジェクトが示されています。

表 308. TakeSnapshotResponse パラメータのオブジェクト

メソッド	説明
public Guid SnapshotSetId { get; set; }	VSS によってこのスナップショットに割り当てられた Guid を取得または設定します。
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	スナップショット内に含まれる各ボリュームのスナップショット情報の集合を取得または設定します。

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

パラメーター BackgroundJobRequest から値を継承します。

次の表には、TransferJobRequest パラメータに使用可能なオブジェクトを示しています。

表 309. TransferJobRequest パラメータのオブジェクト

メソッド	説明
public VolumeNameCollection VolumeNames { get; set; }	転送のボリューム名の集合を取得または設定します。 VolumeNames は、次のデータが含まれているデータ構造です。 - GuidName : ボリュームに関連付けられた Guid。DisplayName が設定されていない場合に、名前として使用されます。 - DisplayName : ボリュームの表示名。
public VolumeNameCollection TransferredVolumes { get; set; }	転送済みボリュームの集合を取得または設定します。
public VolumeNameCollection DependentVolumeNames { get; set; }	依存ボリュームの集合を取得または設定します。
public QuotaSettingsCollection EnabledDiskQuotas { get; set; }	ボリュームで有効になっているクォータを取得または設定します。
public ShadowCopyType ShadowCopyType { get }	転送のコピーの種類を取得します。次の値を使用できます。 - Copy - Full
public AgentTransferConfiguration TransferConfiguration { get; set; }	転送設定を取得または設定します。 AgentTransferConfiguration は、次のデータを持つオブジェクトです。 - MaxConcurrentStreams : データを転送するために Agent に対して Core が確立する同時 TCP 接続の最大数。 - MaxTransferQueueDepth : 書き込み用にキューに入れることができるブロックエクステンションの最大数。

- ・ MaxConcurrentWrites : 任意の時点でエポックに未処理で残しておけるブロック書き込み操作の最大数。追加のブロックを受信した場合に、この数のブロック書き込みが未処理になっているときは、それらの追加ブロックは、未処理のいずれかのブロックの書き込みが終了するまで無視されます。
- ・ MaxSegmentSize : 1つのリクエストで転送する連続ブロックの最大数。
- ・ Priority : このオブジェクトには、次のデータが含まれます。
 - ・ 未定義
 - ・ 1
 - ・ 2
 - ・ 3
 - ・ 4
 - ・ 5
 - ・ 6
 - ・ 7
 - ・ 8
 - ・ 9
 - ・ 10
 - ・ 最大 (1 と同じ)
 - ・ 最小 (10 と同じ)
 - ・ デフォルト (5 と同じ)
- ・ MaxRetries : 失敗した転送が失敗と判断されるまでの最大試行回数。
- ・ UseDefaultMaxRetries : 再試行の最大数がデフォルト値であることを示す値。
- ・ ProviderId : このホスト上のスナップショットを使用するための VSS プロバイダの GUID。通常はデフォルト設定を使用します。

public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	ストレージ設定を取得または設定します。
public string Key { get; set; }	転送リクエストを認証するためのワンタイムパスワードとして使用できる疑似ランダム (暗号化されていない) キーを生成します。
public bool IsBaseImage { get; set; }	ベースイメージが取得されるかどうかを示す値を取得または設定します。
public bool IsForced { get; set; }	転送が強制されたかどうかを示す値を取得または設定します。
public Guid ProtectionGroupId { get; set; }	保護対象グループの ID を取得または設定します。
public TargetComponentTypes LogTruncationTargets { get; set; }	ログの切り捨てが実行されるデータベース (SQL または Exchange) を示す値を取得または設定します。
public bool ForceBaseImage { get }	ベースイメージが強制されたかどうかを示す値を取得します。
public bool IsLogTruncation { get }	ログの切り捨てジョブが実行されたかどうかを示す値を取得します。

TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

TransferScriptParameterBase パラメーターから値を継承します。

TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

次の表には、TransferPostscript パラメータに使用可能なオブジェクトを示しています。TransferScriptParameterBase パラメーターから値を継承します。

表 310. TransferPostscript パラメータのオブジェクト

メソッド	説明
public VolumeNameCollection VolumeNames { get; set; }	転送のボリューム名の集合を取得または設定します。 VolumeNames は、次のデータが含まれているデータ構造です。 - GuidName : ボリュームに関連付けられた Guid。DisplayName が設定されていない場合に、名前として使用されます。 - DisplayName : ボリュームの表示名。
public ShadowCopyType ShadowCopyType { get; set; }	転送のコピータイプを取得または設定します。ShadowCopyType は値を含む列挙です。次の値を使用できます。 - Unknown - Copy - Full
public AgentProtectionStorageConfigurationCom mon StorageConfiguration { get; set; }	ストレージ設定を取得または設定します。
public AgentTransferConfiguration TransferConfiguration { get; set; }	転送設定を取得または設定します。 AgentTransferConfiguration は、次のデータを持つオブジェクトです。 - MaxConcurrentStreams : データを転送するために Agent に対して Core が確立する同時 TCP 接続の最大数。 - MaxTransferQueueDepth : 書き込み用にキューに入れることができるブロックエクステンツの最大数。 - MaxConcurrentWrites : 任意の時点でエポックに未処理で残しておけるブロック書き込み操作の最大数。追加のブロックを受信した場合に、この数のブロック書き込みが未処理になっているときは、それらの追加ブロックは、未処理のいずれかのブロックの書き込みが終了するまで無視されます。 - MaxSegmentSize : 1つのリクエストで転送する連続ブロックの最大数。 - Priority : このオブジェクトには、次のデータが含まれます。 "Undefined "One "Two "Three "Four "Five "Six "Seven "Eight "Nine "Ten

	・ "Highest (1 と同じ) ・ "Lowest (10 と同じ) ・ "Default (5 と同じ) ・ MaxRetries : 失敗した転送が失敗と判断されるまでの最大試行回数。 ・ UseDefaultMaxRetries : 再試行の最大数がデフォルト値であることを示す値。 ・ ProviderId : このホスト上のスナップショットを使用するための VSS プロバイダの GUID。管理者は通常デフォルトを受け入れます。
public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)	・ ExcludedWriterIds : このスナップショットから除外される必要のある VSS ライター ID。ライター ID はライターの名前に関連しています。この名前は文書化目的にのみ使用され、ライターの実際の名前と完全に一致する必要はありません。 ・ TransferDataServerPort : Agent から Core への実際のデータ転送で、Core からの接続を受け付けるための TCP ポートの値。 ・ SnapshotTimeout : VSS スナップショット操作の実行が停止およびタイムアウトするまでの待機時間。 ・ TransferTimeout : スナップショットを破棄するまでの、Core からの追加の連絡の待機時間。 ・ NetworkReadTimeout : この転送に関連するネットワーク読み取り操作のタイムアウト。 ・ NetworkWriteTimeout : この転送に関連するネットワーク書き込み操作のタイムアウト。 ・ InitialQueueSize : リクエストの初期キューサイズ。 ・ MinVolumeFreeSpacePercents : ボリューム上の最小空き容量 (パーセント単位)。 ・ MaxChangeLogsSizePercents : ボリューム容量に対するドライバ変更ログの最大サイズ (パーセント単位)。 ・ EnableVerification : Core に送信される各ブロックの診断検証を実行すべきかどうかを示す値。
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	ストレージ設定を取得または設定します。 AgentProtectionStorageConfiguration オブジェクトには次のデータが含まれています。 ・ RepositoryId : この Agent のリカバリポイントを保存するリポジトリの名前。 ・ EncryptionKeyId : この Agent のリカバリポイントの暗号化キー ID。空のストリングは暗号化されていないことを意味します。
public string Key { get; set; }	Key メソッドは、転送要求を認証するためのワンタイムパスワードとして使用できる疑似ランダム (暗号化されていない) キーを生成します。
public bool ForceBaseImage { get; set; }	転送が強制されたベースイメージ取得であったかどうかを示す値を取得または設定します。
public bool IsLogTruncation { get; set; }	ロギングが切り捨てられているかどうかを示す値を取得または設定します。
public uint LatestEpochSeenByCore { get; set; }	最新のエポック値を取得または設定します。 LatestEpochSeenByCore メソッドは、Core が取得する最新スナップショットの序数です。これは、VSS を使用して特定のスナップショットが取られたときに、フィルタドライバによってそのスナップショットに割り当てられる「エポック番号」です。
public Guid SnapshotSetId { get; set; }	VSS によってこのスナップショットに割り当てられた Guid を取得または設定します。
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	スナップショット内に含まれる各ボリュームのスナップショット情報の集合を取得または設定します。

TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution)

次の表には、TransferScriptParameterBase パラメータに使用可能なオブジェクトを示しています。

表 311. TransferScriptParameterBase パラメータのオブジェクト

メソッド	説明
public AgentTransferConfiguration TransferConfiguration { get; set; }	転送設定を取得または設定します。
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	ストレージ設定を取得または設定します。

VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

次の表には、VirtualMachineLocation パラメータに使用可能なオブジェクトを示しています。

表 312. VirtualMachineLocation パラメータのオブジェクト

メソッド	説明
public string Description { get; set; }	この場所のわかりやすい説明を取得または設定します。
public string Name { get; set; }	VM の名前を取得または設定します。

VolumeImageldsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

パラメーター System.Collections.ObjectModel.Collection<string> から値を継承します。

VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

次の表には、VolumeName パラメータに使用可能なオブジェクトを示しています。

表 313. VolumeName パラメータのオブジェクト

メソッド	説明
public string GuidName { get; set; }	ボリュームの ID を取得または設定します。
public string DisplayName { get; set; }	ボリュームの名前を取得または設定します。

メソッド	説明
public string UriEncode()	URL 上で安全に渡すことができる URL エンコードされたバージョンの名前を取得または設定します。
	① メモ: パスのエスケープ文字が URI テンプレートで正しく機能することを妨げる .NET 4.0 WCF に存在する既知の問題 (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312) です。ボリューム名に「\」と「?」の両方が含まれているため、特殊文字「\」と「?」を他の特殊文字と置き換える必要があります。
public string GetMountName()	ボリュームイメージをいくつかのフォルダにマウントするために有効な、このボリュームの名前を返します。

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

パラメータ System.Collections.ObjectModel.Collection<VolumeName> から値を継承します。

次の表には、VolumeNameCollection パラメータに使用可能なオブジェクトを示しています。

表 314. VolumeNameCollection パラメータのオブジェクト

メソッド	説明
public override bool Equals(object obj)	このインスタンスと指定されたオブジェクト (VolumeNameCollection オブジェクトであることも必要) が同じ値を持っているかどうかを判別します。(Object.Equals(Object) をオーバーライドします。)
public override int GetHashCode()	この VolumeNameCollection のハッシュコードを返します。(Object.GetHashCode() をオーバーライドします。)

VolumeSnapshotInfo (namespace Replay.Common.Contracts.Transfer)

次の表には、VolumeSnapshotInfo パラメータに使用可能なオブジェクトを示しています。

表 315. VolumeSnapshotInfo パラメータのオブジェクト

メソッド	説明
public Uri BlockHashesUri { get; set;}	ボリュームブロックの MD5 ハッシュを読み取ることができる URI を取得または設定します。
public Uri BlockDataUri { get; set;}	ボリュームデータブロックを読み取ることができる URI を取得または設定します。

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

パラメータ System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo> から値を継承します。

PowerShell スクリプトのサンプル

管理ユーザーが PowerShell スクリプトを実行するのに役立つ次のサンプルスクリプトが提供されています。

関連するリンク

[PreTransferScript.sh](#)
[PostTransferScript.ps1](#)
[PreExportScript.ps1](#)
[PostExportScript.ps1](#)
[PreNightlyJobScript.ps1](#)
[PostNightlyJobScript.ps1](#)

PreTransferScript.ps1

PreTransferScript は、スナップショットの転送前に保護対象マシンで実行されます。

PreTransferScript のサンプル

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
    echo 'TransferPrescriptParameterObject parameter is null'
}
else {
    echo 'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguration
    echo 'StorageConfiguration:' $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

PostTransferScript は、スナップショットの転送後に保護対象マシンで実行されます。

PostTransferScript のサンプル

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
```



```

$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];
# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
    echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
    echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType
    echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage
    echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}

```

PreExportScript.ps1

PreExportScript は、エクスポートジョブの前に Core で実行されます。

PreExportScript のサンプル

```

# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
    echo 'ExportJobRequestObject parameter is null'
}
else {
    echo 'Location:' $ExportJobRequestObject.Location
    echo 'Priority:' $ExportJobRequestObject.Priority
}

```

PostExportScript.ps1

PostExportScript は、エクスポートジョブの後に Core で実行されます。

① **メモ:** エクスポートされた保護対象マシンで初回起動後に、一度だけ使用され、**PostExportScript** の入力パラメータはありません。通常の保護対象マシンでは、このスクリプトは、**PowerShell** スクリプトフォルダに **PostExportScript.ps1** という名前で含まれています。

PostExportScript のサンプル

```

# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

```

```

$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
    echo 'ExportJobRequestObject parameter is null'
}
else {
    echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
    echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}

```

PreNightlyJobScript.ps1

PreNightlyJobScript は、Core 側で毎夜間ジョブ前に行われます。パラメータ \$JobClassName があり、子ジョブを別々に処理するのに役立ちます。

PreNightlyJobScript のサンプル

```

# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'SimultaneousJobsCount:' $RollupJobRequestObject.SimultaneousJobsCount;
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as "System.Collections.Generic.List`1[System.Guid]"
        if($AgentsCollection -eq $null) {

```

```

        echo 'AgentsCollection parameter is null';
    }
    else {
        echo 'Agents GUIDs:'
        foreach ($a in $AgentsCollection) {
            echo $a
        }
    }
    break;
}
# working with Checksum Check Job
ChecksumCheckJob {
    $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
    echo 'Exchange checksumcheck job results:';
    if($ChecksumCheckJobRequestObject -eq $null) {
        echo 'ChecksumCheckJobRequestObject parameter is null';
    }
    else {
        echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
        echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
        echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
    }
    break;
}
# working with Log Truncation Job
TransferJob {
    $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
    echo 'Transfer job results:';
    if($TransferJobRequestObject -eq $null) {
        echo 'TransferJobRequestObject parameter is null';
    }
    else {
        echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
        echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
    }
    echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
    break;
}
}

```

PostNightlyJobScript.ps1

PostNightlyJobScript は、Core で毎夜間ジョブの後に実行されます。パラメータ \$JobClassName があり、子ジョブを別々に処理するの役に立ちます。

PostNightlyJobScript のサンプル

```

# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and

```

```

Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results: ';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results: ';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as "System.Collections.Generic.List`1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
            echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                echo $a
            }
        }
        break;
    }
# working with Checksum Check Job
    ChecksumCheckJob {
        $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
        echo 'Exchange checksumcheck job results: ';
        if($ChecksumCheckJobRequestObject -eq $null) {
            echo 'ChecksumCheckJobRequestObject parameter is null';
        }
        else {
            echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
            echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Log Truncation Job
    TransferJob {
        $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results: ';
        if($TransferJobRequestObject -eq $null) {
            echo 'TransferJobRequestObject parameter is null';
        }
        else {
            echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
            echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
        }
        echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
    }
}

```

```

$TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
if ($TakeSnapshotResponseObject -eq $null) {
    echo 'TakeSnapshotResponseObject parameter is null';
}
else {
    echo 'ID of this transfer session:' $TakeSnapshotResponseObject.SnapshotSetId;
    echo 'Volumes:' $TakeSnapshotResponseObject.VolumeSnapshots;
}
break;
}
}

```

Rapid Recovery での Bourne Shell スクリプティングの使用

Bourne Shell (sh) は、Unix ベースのオペレーティングシステム用シェル言語またはコマンドラインインタプリタです。Bourne Shell は、Linux とともに Rapid Recovery で使用することで、環境のカスタマイズをしたり、事前に設定した順番で特定の操作が行われるように指定したりすることができます。Bourne シェルファイルのファイル拡張子は .sh であり、これが命名規則になります。

Bourne Again Shell (BASH) は同じようなシェル言語で、同じ文法、パラメータ、変数の展開、リダイレクト、引用符の処理を実装します。また、BASH では、同じ .sh ファイル拡張子を使用します。ここに記載されている情報は、BASH にも同じように適用されます。

転送処理の前後にエクスポートスクリプトフックを使用して、転送またはエクスポートの前後にシステム操作を実行できます。たとえば、転送の実行中に特定の cronjob を無効にし、転送が完了したらそれを有効にすることができます。また、アプリケーション固有のデータをディスクにフラッシュするコマンドを実行する必要がある場合もあります。内容は一時ファイルに書き込まれ、exec を使用して実行されます。その後、スクリプトの最初の行に定義されたインタプリタ ((#!/usr/bin/env bash) など) を使用してスクリプトが実行されます。指定したインタプリタを使用できない場合には \$SHELL 環境変数で定義されたデフォルトシェルがスクリプトで使用されます。

任意のインタプリタを代わりに使用できます。たとえば、設定に応じて、スクリプトの #! 行で「bash」を「zsh」(Z Shell) や「tcsh」(tee Shell) に置き換えることができます。

TransferPrescript パラメータから使用可能なオブジェクトを追加することも、独自のコマンドを PreTransferScript.sh および PostTransfer.sh スクリプトに追加してそれらをカスタマイズすることもできます。

本項には、Rapid Recovery for Windows および Linux で管理者が指定されたタイミングで使用できるスクリプトについての説明が記載されています。次のトピックで構成されています。

- [Bourne Shell スクリプティングの入力パラメータ](#)
- [Bourne Shell スクリプトのサンプル](#)

Bourne Shell スクリプティングの前提条件

Rapid Recovery では、転送の前後に Linux Agent マシン上で Bourne Shell スクリプトを実行できます。Rapid Recovery Agent ソフトウェアで保護された Linux マシンでは、次のスクリプトがサポートされています。

❶ **メモ:** スクリプトが実行可能ファイルではない場合、転送ジョブは失敗します。

- PreTransferScript.sh
- PostTransferScript.sh
- PostExportScript.sh

これらのスクリプトを使用するには、これらが /opt/apprecovery/scripts/ ディレクトリに置かれていることを確認します。

サポートされる転送および事後転送スクリプトパラメータ

次のパラメータは、転送スクリプト用に Linux でサポートされています。詳細については、「[Bourne Shell スクリプトのサンプル](#)」を参照してください。

- TransferPrescriptParameter_VolumeNames=\$TransferPrescriptParameter_VolumeNames
- TransferPrescriptParameter_ShadowCopyType=\$TransferPrescriptParameter_ShadowCopyType
- TransferPrescriptParameter_TransferConfiguration=\$TransferPrescriptParameter_TransferConfiguration
- TransferPrescriptParameter_StorageConfiguration=\$TransferPrescriptParameter_StorageConfiguration
- TransferPrescriptParameter_Key=\$TransferPrescriptParameter_Key
- TransferPrescriptParameter_ForceBaselImage=\$TransferPrescriptParameter_ForceBaselImage
- TransferPrescriptParameter_IsLogTruncation=\$TransferPrescriptParameter_IsLogTruncation
- TransferPrescriptParameter_LatestEpochSeenByCore=\$TransferPrescriptParameter_LatestEpochSeenByCore

次のパラメータは、事後転送スクリプト用に Linux でサポートされています。

- TransferPostscriptParameter_VolumeNames=\$TransferPostscriptParameter_VolumeNames
- TransferPostscriptParameter_ShadowCopyType=\$TransferPostscriptParameter_ShadowCopyType
- TransferPostscriptParameter_TransferConfiguration=\$TransferPostscriptParameter_TransferConfiguration
- TransferPostscriptParameter_StorageConfiguration=\$TransferPostscriptParameter_StorageConfiguration
- TransferPostscriptParameter_Key=\$TransferPostscriptParameter_Key
- TransferPostscriptParameter_ForceBaselImage=\$TransferPostscriptParameter_ForceBaselImage
- TransferPostscriptParameter_IsLogTruncation=\$TransferPostscriptParameter_IsLogTruncation
- TransferPostscriptParameter_LatestEpochSeenByCore=\$TransferPostscriptParameter_LatestEpochSeenByCore

Bourne Shell スクリプティングのテスト

script (.sh) ファイルのエディタを使用して、実行するスクリプトをテストできます。

① **メモ:** 事前 **Bourne Shell** スクリプトまたは事後 **Bourne Shell** スクリプトが失敗すると、ジョブも失敗します。ジョブに関する情報は、`/var/log/apprecovery/apprecovery.log` ファイルにあります。スクリプトが正常に処理されると、終了コード **0** が返されます。

Bourne Shell スクリプティングの入力パラメータ

次の表には、Rapid Recovery の Bourne Shell スクリプティング パラメータについての説明が示されています。

TransferPrescriptParameters_VolumeNames

次の表には、TransferPrescript パラメータに使用可能なオブジェクトを示しています。

表 316. TransferPrescript オブジェクト

メソッド	説明
public VolumeNameCollection VolumeNames (get; set;)	転送のボリューム名の集合を取得または設定します。

メソッド	説明
	VolumeNames は、次のデータが含まれているデータ構造です。 - GuidName : ボリュームに関連付けられた Guid。DisplayName が設定されていない場合に、名前として使用されます。 - DisplayName : ボリュームの表示名。
public ShadowCopyType ShadowCopyType { get; set; }	転送のコピーの種類を取得または設定します。ShadowCopyType は値を含む列挙です。次の値を使用できます。 - Unknown - Copy - Full
public string Key { get; set; }	Key メソッドは、転送要求を認証するためのワンタイムパスワードとして使用できる疑似ランダム（暗号化されていない）キーを生成します。
public bool ForceBaseImage { get; set; }	転送が強制されたベースイメージ取得であったかどうかを示す値を取得または設定します。
public bool IsLogTruncation { get; set; }	ロギングが切り捨てられているかどうかを示す値を取得または設定します。
public uint LatestEpochSeenByCore { get; set; }	最新のエポック値を取得または設定します。 LatestEpochSeenByCore メソッドは、Core が取得する最新スナップショットの序数です。これは、VSS を使用して特定のスナップショットが取られたときに、フィルタドライバによってそのスナップショットに割り当てられる「エポック番号」です。

TransferPostscriptParameter

次の表には、TransferPostscript パラメータに使用可能なオブジェクトを示しています。

表 317. TransferPostscript オブジェクト

メソッド	説明
public VolumeNameCollection VolumeNames { get; set; }	転送のボリューム名の集合を取得または設定します。 VolumeNames は、次のデータが含まれているデータ構造です。 - GuidName : ボリュームに関連付けられた Guid。DisplayName が設定されていない場合に、名前として使用されます。 - DisplayName : ボリュームの表示名。
public ShadowCopyType ShadowCopyType { get; set; }	転送のコピータイプを取得または設定します。ShadowCopyType は値を含む列挙です。次の値を使用できます。 - Unknown - Copy - Full
public string Key { get; set; }	Key メソッドは、転送要求を認証するためのワンタイムパスワードとして使用できる疑似ランダム（暗号化されていない）キーを生成します。
public bool ForceBaseImage { get; set; }	転送が強制されたベースイメージ取得であったかどうかを示す値を取得または設定します。
public bool IsLogTruncation { get; set; }	ロギングが切り捨てられているかどうかを示す値を取得または設定します。

メソッド	説明
<pre>public uint LatestEpochSeenByCore { get; set; }</pre>	最新のエポック値を取得または設定します。 LatestEpochSeenByCore メソッドは、Core が取得する最新スナップショットの序数です。これは、VSS を使用して特定のスナップショットが取られたときに、フィルタドライバによってそのスナップショットに割り当てられる「エポック番号」です。

Bourne Shell スクリプトのサンプル

本項では、管理ユーザーが保護対象マシンで実行できる Bourne Shell スクリプトのサンプルについて説明します。

△ 注意: このドキュメントで提供されている **Bourne** のサンプルスクリプトは、適格な管理者によって設計どおりに実行されると機能します。作業バージョンを保持するために機能しているスクリプトに変更を加える場合は、注意が必要です。このドキュメントに含まれるサンプルスクリプトに加えた変更、つまり、ユーザーが作成したスクリプトはカスタマイズと見なされ、通常、Dell のサポートの対象外となります。

① メモ: 保護対象マシンは「**exec**」シェルコマンドを使用して、スクリプトを開始します。スクリプトの最初の行に情報を定義することで、どのインタプリタでスクリプトを実行する必要があるかを示すことができます。インタプリタを指定しなければ、デフォルトシェルによってスクリプトが解釈されます。デフォルトシェル以外のものを選択する場合、指定されたインタプリタが保護対象のすべてのマシンで使用できることを確認する必要があります。

次の保護対象マシンサンプルスクリプトがあります。

PreTransferScript.sh

PreTransferScript は、スナップショットの転送前に保護対象マシンで実行されます。

次のスクリプトは、ルートホームディレクトリに置かれて保存されている Pre(Post)TransferScriptResult.txt に、入力パラメータから値を保存します。

PreTransferScript のサンプル

```
#!/bin/bash
echo "TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
TransferPrescriptParameter_LatestEpochSeenByCore=
$TransferPrescriptParameter_LatestEpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

PostTransferScript は、スナップショットの転送後に保護対象マシンで実行されます。

次のスクリプトは、ルートホームディレクトリに置かれて保存されている Pre(Post)TransferScriptResult.txt に、入力パラメータから値を保存します。

PostTransferScript のサンプル

```
#!/bin/bash
echo "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
```

```
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
TransferPostscriptParameter_LatestEpochSeenByCore=
$TransferPostscriptParameter_LatestEpochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

PostExportScript は、転送後に保護対象マシンで実行されます。

次のスクリプトは、ルートホームディレクトリに置かれて保存されている Pre(Post)ExportScriptResult.txt に、入力パラメータから値を保存します。

PostExportScript のサンプル

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```

Rapid Recovery API

このセクションの目的は、Rapid Recovery Representational State Transfer (REST) API の概要、使用、機能を説明することです。

Rapid Recovery ウェブサービス API は RESTful で、Rapid Recovery ソフトウェアソリューションの特定の機能やタスクを自動化およびカスタマイズして、ビジネス目標の達成をサポートします。

これらの API は、Dell Data Protection | Rapid Recovery ライセンスポータル の **ダウンロード** ページからアクセスできます。

トピック：

- ・ [対象読者](#)
- ・ [Rapid Recovery REST API の使用](#)
- ・ [Core および Agent API のダウンロードと表示](#)
- ・ [参考資料](#)

対象読者

Rapid Recovery API は、Rapid Recovery を各自のアプリケーションで統合および拡張するアプリケーション開発者や、Rapid Recovery Core サーバとスクリプトでやり取りする管理者が使用することを想定しています。

Rapid Recovery REST API の使用

Rapid Recovery API は、REST スタイルの API です。つまり、HTTP リクエストを使用して、URI 経由でリソース（データエンティティ）にアクセスします。Rapid Recovery API では、標準的な HTTP メソッド（GET、PUT、POST、および DELETE など）を使用します。REST API は、オープン標準に基づいているため、HTTP 呼び出しをサポートする任意の言語またはツールを使用できます。

アプリケーション開発者および管理者が Rapid Recovery API を操作する方法は 2 つあります。その方法は次のとおりです。

- ・ C# または他の .DLL 言語を使用して、Rapid Recovery .NET クライアント DLL ファイルを直接使用する。
- ・ HTTP エンドポイントと直接通信して、独自の XML を生成する。

最初の方法をお勧めします。クライアント DLL は Rapid Recovery SDK に含まれています。Rapid Recovery API を呼び出す方法は、.NET 4.5X Windows Communication Foundation (WCF) サービスを使用する方法と同じです。

Core および Agent API のダウンロードと表示

Dell Data Protection | Rapid Recovery ソフトウェア開発キット (SDK) には、Rapid Recovery Core と Rapid Recovery Agent コンポーネント用の REST API、サンプルおよびサポートファイルが含まれています。これらの内容は、次のフォルダに格納され、圧縮されたアーカイブには、次のコンポーネントが含まれています。

表 318. SDK アーカイブに含まれているコンポーネント

フォルダ名	コンテンツ	説明
core.contracts	Rapid Recovery Core API	開発者や管理者が、Rapid Recovery Core の機能をスクリプト化するために役立つ API が含まれています。2 組のサービス契約があります。 1 CoreWeb.Client HTML ファイルをウェブブラウザで開き、一般的な REST 標準に関する情報を表示します。サービス契約が一覧表示されます。ブラウザで対応するハイパーリンク URI (Uniform Resource Identifier) をクリックすると、core.contracts / docweb / ディレクトリ内の情報が表示されます。表示されるページに、メソッドや説明など一般的な REST サービス操作に関する情報が表示されます。 2 Core.Client HTML ファイルをウェブブラウザで開き、詳細な C# 情報を表示します。ハイパーリンクのサービス契約 (クラス) をクリックしたときに、ブラウザで core.contracts / doc / ディレクトリ内の情報が開きます。表示されるページに選択したクラスのすべての C# メソッドの詳細情報が表示されます。
Agent.Contracts	Rapid Recovery Agent API (これは廃止されました)	開発者または管理者が、保護対象マシン上で Rapid Recovery Agent を操作するために使用できる API が含まれています。 △ 注意: Agent API は廃止されました。SDK の今後のバージョンから削除されます。Agent API の直接操作を行うことはお勧めできません。これらの API の使用はカスタマイズと見なされ、サポートされていません。この情報は、履歴のためにマニュアルに記載されています。 1 AgentWeb.Client HTML ファイルをウェブブラウザで開き、一般的な REST 標準に関する情報を表示します。 2 AgentWeb.Client HTML ファイルをウェブブラウザで開き、詳細な C# 情報を表示します。
AppRecoveryAPI Samples	コードサンプルと DLL	AppRecoveryAPISamples には、C# プログラミング言語で記述されたコードサンプルが含まれています。API を使用して GUI や管理システムなどをカスタマイズする場合、これらのファイルはコードスニペットを表示するための開始点として有効です。 aAppRecoveryAPISamples\Dependencies には、Rapid Recovery Core で使用する DLL ファイルが含まれています。DLL には、データ契約 (Core でよく使用されるタイプ) およびサービス契約 (Core で処理を強制的に行うために使用できる管理方法および操作) が含まれています。独自のグラフィックユーザーインターフェースをカスタマイズするか、管理システムを使用して、Rapid Recovery Core を操作するには、これらの DLL が必要です。 ① メモ: 使用されている DLL バージョンは Core のバージョンと一致している必要があります。

SDK はアーカイブ (API-Reference-x.x.x-xxxx) としてダウンロードすることができます。それぞれの x は、関連するリリースのビルド番号の桁を表します。

上記の手順を完了して SDK を取得するには、指定された宛先にファイルをダウンロードし、ファイルを解凍して、Core と Agent API の使用を準備します。

- 1 Dell Data Protection | Rapid Recovery ライセンスポータル (<https://licenseportal.com>) にログインします。
- 2 ライセンスポータルの左側にあるナビゲーションエリアで、**ダウンロード** をクリックします。
ライセンスポータルの **ダウンロード** ページが表示されます。
- 3 **ダウンロード** ページで、Windows ベースのアプリケーションセクションで、SDK の説明まで下にスクロールし、**ダウンロード** をクリックします。
- 4 ダウンロードしたアーカイブを任意の場所に保存します。
- 5 アーカイブを解凍します。
新しい API-Reference-x.x.x-xxxx フォルダに、前の表で説明されているファイルの独立したセットが表示されます。

6 前の表に記載されている主要な HTML ファイルをウェブブラウザで開き、API に関するガイダンスを参照してください。

参考資料

『*Dell Data Protection | Rapid Recovery のインストールおよびアップグレードガイド*』では、Rapid Recovery アーキテクチャの概要について説明し、Rapid Recovery コンポーネントのインストールに必要な手順と、Core および Agent コンポーネントの以前のバージョンからのアップグレードに必要な手順について説明しています。

このガイドは、<https://support.software.dell.com/rapid-recovery/release-notes-guides/> で表示またはダウンロードできます。

デルは、お客様の声に耳を傾け、お客様の信頼に応えて、価値ある革新的なテクノロジー、ビジネスソリューション、およびサービスを世界中に提供しています。詳細については、「<http://software.dell.com>」を参照してください。

デルへのお問い合わせ

セールスまたはその他のお問い合わせについては、「<http://software.dell.com/company/contact-us.aspx>」を参照するか、+1-949-754-8000 までお電話ください。

テクニカルサポート：

テクニカルサポートは、有効な保守契約が付属する Dell ソフトウェアを購入している場合、または試用版を保有している場合にご利用いただけます。サポートポータルにアクセスするには、「<https://support.software.dell.com>」に移動します。

サポートポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプツールがあり、24 時間 365 日ご利用いただけます。また、サポートポータルでは、オンライン上のサービスリクエストシステムを介して製品サポートエンジニアに直接アクセスできます。

サポートポータルでは、次の操作が可能です。

- ・ サービスリクエスト（ケース）の作成、アップデート、および管理
- ・ サポート技術情報記事の参照
- ・ 製品通知の取得
- ・ ソフトウェアのダウンロード。評価版ソフトウェアについては、「<http://software.dell.com/trials>」を参照してください。
- ・ コミュニティディスカッションへの参加

Agent

Rapid Recovery Agent ソフトウェアを物理マシンまたは仮想マシン上にインストールすることで、そのマシンを Rapid Recovery Core で保護対象に追加できるようになります。

Rapid Recovery

Rapid Recovery は、バックアップ、レプリケーション、リカバリを1つのソリューションにまとめることにより、統合的データ保護の新たなスタンダードを提示します。そのソリューションは、仮想マシン (VM)、物理マシン、クラウド環境のデータ保護のために、最速かつ最も信頼性の高いバックアップを実現するように設計されています。

ベースイメージ

Core に保存される最初のバックアップ転送は、ベースイメージスナップショットと呼ばれます。指定したすべてのボリュームのすべてのデータ（オペレーティングシステム、アプリケーション、および設定を含む）は、Core に保存されます。詳細については、「[スナップショット](#)」を参照してください。

Central Management Console

Rapid Recovery Central Management Console は、2 つ以上の Rapid Recovery Cores がある環境用のオプションコンポーネントです。このコンポーネントは、ウェブポータルで、単一のウェブベースのインタフェースを使用して複数の Core をグループ化および管理し、レポートを生成できます。

チェックサム

チェックサムは、転送またはストレージ実行中に発生した偶発的なエラーを検知するために使用されるデータのブロックを作成する機能です。

クラスタ

[Windows フェイルオーバークラスタ](#)を参照してください。

cluster continuous replication (CCR)

非共有ストレージのフェイルオーバークラスタソリューションである CCR は、ビルトインの非同期ログ配布テクノロジーを使用して、フェイルオーバークラスタにある二次的なサーバーに各ストレージグループのコピーを作成し、維持します。CCR は、1つ、または2つのデータセンターソリューション用に設計されており、高可用性とサイト耐久性の両方を提供します。これは、Exchange 2007 で使用できる2つのクラスター化メールボックスサーバー (CMS) 展開タイプのうちの1つです。

クラスタノード

Windows フェイルオーバークラスタの一部を成す個々のマシンです。

圧縮

Storage Networking Industry Association (SNIA) の定義によると、圧縮は、サイズを小さくするためにデータを符号化するプロセスです。

Core

Rapid Recovery Core は、Rapid Recovery アーキテクチャの中心的なコンポーネントです。Core は、バックアップ、リカバリ、保持、レプリケーション、アーカイブ、および管理に不可欠なサービスを提供します。レプリケーションにおいては、Core はソース Core とも呼ばれます。ソース Core がレプリケーション元の Core、ターゲット Core がレプリケーション先の Core です（保護対象マシンまたはクラスタがリプリケートされる、専用サーバ上の別の Rapid Recovery Core）。

Core Console

Rapid Recovery Console は、Rapid Recovery Core を完全に管理できる、ウェブベースのインタフェースです。

データベース可用性グループ (DAG)

データベース、サーバー、またはネットワークの不具合から、自動でデータベースレベルのリカバリを実行する、最大 16 の Microsoft Exchange Server 2010 Mailbox サーバー一式です。DAG は継続的なレプリケーションと、Windows フェイルオーバー クラスタリングテクノロジーを使用して、高可用性とサイト耐久性を提供します。DAG 内の Mailbox サーバーは、お互いの不具合を監視します。Mailbox サーバーが DAG に追加されると、DAG 内の他のサーバーと連携して、データベースの不具合から自動でデータベースレベルのリカバリを実行します。

暗号化

データの暗号化は、適切な復号キーを所有する権限のあるユーザーのみがアクセスできるようにするために行われます。データは、暗号ブロック連鎖 (CBC) モードで 256 ビット AES を使用して暗号化されます。CBC では、データの各ブロックが暗号化される前に、それらに対して以前の暗号文を使用した XOR 演算が行われます。こうすることにより、新しい各暗号文ブロックが先行するプレーンテキストブロックのすべてに依存するようになります。初期化ベクトルには、パズフレーズが使用されます。

イベント

イベントは Core によって記録されるプロセスです。イベントを Core Console 内で表示するには、アイコンバーから  (イ

ベント) アイコンをクリックします。  (イベント) アイコンをクリックしたときのデフォルトビューには、**タスク** ページが表示されます。このビューでは、ジョブに関連するイベントを表示します。通知される優先度イベントは、**警告** ページで確認できます。すべてのイベントのログは **ジャーナル** ページに表示されます。既存の通知グループをセットアップまたは変更することで、任意のイベントの通知をカスタマイズできます。このアクションでは、イベントを **警告** ページに表示することにより、イベントの優先度を上げます。通知グループのメンバーは、グループの通知オプションで設定された通知方法を使用してイベントの通知を受けます。

グローバル重複排除

Storage Networking Industry Association (SNIA) の定義によると、データ重複排除とは、ストレージ空間や帯域を節約するために、さまざまな粒度レベルのデータの複数コピーを、共有コピーへの参照に置き換えることを意味します。Rapid Recovery ボリュームマネージャは、論理ボリューム内でグローバルデータ重複排除を実行します。重複排除の粒度レベルは、8 KB です。Rapid Recovery における重複排除の範囲は、同じレポジトリおよび暗号化キーを使用する保護対象マシンに限定されます。

増分スナップショット

前回のバックアップ以降に保護対象マシンで変更されたデータのみで構成されるバックアップ。定義した間隔 (たとえば 60 分ごと) に基づいて定期的に Core に保存されます。詳細については、「[スナップショット](#)」を参照してください。

ライセンスキー

ライセンスキーは、お使いの Rapid Recovery ソフトウェアまたはアプライアンスを登録する際に使用する方法の 1 つです (ライセンスファイルを使用することもできます)。ライセンスキーまたはファイルは、Dell Data Protection | Rapid Recovery ライセンスポータルをアカウントに登録するときに取得できます。詳細については、「[ライセンスポータル](#)」を参照してください。

ライセンスポータル

Dell Data Protection | Rapid Recovery ライセンスポータルはウェブインタフェースで、ここでユーザーおよびパートナーがソフトウェアのダウンロード、Rapid Recovery アプライアンスの登録、ライセンスのサブスクリプションの管理を行うことができます。ライセンスポータルでは、アカウントの登録、Rapid Recovery Core および Agent ソフトウェアのダウンロード、グループの管理、グループアクティビティの追跡、マシンの登録、アプライアンスの登録、ユーザーの招待、レポートの生成を実行できます。詳細については、『*Dell Data Protection | Rapid Recovery ライセンスポータル ユーザーガイド*』を参照してください。

Live Recovery

Rapid Recovery Live Recovery は、VM およびサーバーの即時リカバリを行うテクノロジーです。このテクノロジーにより、仮想または物理サーバー内のデータボリュームへほとんど中断なくアクセスでき、ほぼ 0 分の RTO および RPO でボリューム全体をリカバリできます。

Local Mount Utility

Local Mount Utility (LMU) は、どのマシンからでもリモートの Rapid Recovery Core にリカバリポイントをマウントできるようにする、ダウンロード可能なアプリケーションです。

ログの切り捨て

ログの切り捨ては、トランザクションログからログ記録を削除する機能です。SQL Server マシンでは、SQL Server ログの切り捨てを強制実行すると、この処理により、SQL Server 上の空き容量が特定されます。Exchange Server マシンでは、Exchange Server ログの切り捨てを強制実行すると、この操作により、Exchange Server 上の領域が解放されます。

管理役割

Rapid Recovery Central Management Console では、管理役割という新しい概念が導入されました。管理役割は、アクセス制御に加え、信頼できるデータ管理者およびサービス管理者の間での管理責任の分割を可能にし、セキュアかつ効率的な管理の委任をサポートします。

マウント可否

Exchange マウント可否は、管理者に潜在的な障害を通知し、障害が発生した場合に Exchange Server 上のすべてのデータが正常にリカバリできることを保証する破損検出機能です。

オブジェクトファイルシステム

Rapid Recovery Scalable Object Store は、オブジェクトファイルシステムコンポーネントです。これは、スナップショットが取得されたすべてのデータブロックをオブジェクトとして扱います。また、これらのオブジェクトの保存、取得、維持、およびレプリケートします。このコンポーネントは、グローバルなデータ重複排除、暗号化および保持管理と連携してスケーラブルな入力および出力 (I/O) パフォーマンスを実現するように設計されています。オブジェクトファイルシステムは、業界標準のテクノロジーと直接的に相互動作します。

パスフレーズ

パスフレーズは、データの暗号化に使用されるキーです。パスフレーズを失うと、データを回復することはできません。

PowerShell Scripting

Windows PowerShell は、管理の自動化のために設計された Microsoft .NET Framework 関連環境です。Rapid Recovery には PowerShell Scripting の包括的なクライアント SDK が含まれており、管理者が直接、またはスクリプトを使用してコマンドを実行することによって、Rapid Recovery リソースの管理を自動化することができます。

使用禁止文字

使用禁止文字とは、Rapid Recovery Core Console でオブジェクトに命名するときに使用できない文字のことです。たとえば、保護対象マシンの表示名を定義する際に、次の特殊文字を使用してはなりません。

表 319. 使用禁止文字

文字	文字名	禁止場所
?	疑問符	マシン表示名、暗号化キー、リポジトリ、パスの説明
	パイプ	マシン表示名、暗号化キー、リポジトリ、パスの説明
:	コロンの	マシン表示名、暗号化キー、リポジトリ パスを指定する際にはコロンの使用できます (例: c:\data)。
/	順スラッシュ	マシン表示名、暗号化キー、リポジトリ、パスの説明
\	逆スラッシュ	マシン表示名、暗号化キー、リポジトリ ローカルパスやネットワークパスを指定する際には逆スラッシュを使用できます (例: c:\data、\\ComputerName\SharedFolder\)
*	アスタリスク	マシン表示名、暗号化キー、リポジトリ、パスの説明
"	引用符	マシン表示名、暗号化キー、リポジトリ、パスの説明
<	開き山括弧	マシン表示名、暗号化キー、リポジトリ、パスの説明
>	閉じ山括弧	マシン表示名、暗号化キー、リポジトリ、パスの説明

禁止語

禁止語とは、オペレーティングシステム用に予約されているため、Rapid Recovery Core Console でオブジェクトを命名する際に使用してはならない語（文字のセット）のことです。禁止語はできるかぎり使用しないようにするのがベストプラクティスです。たとえば、保護対象マシンの表示名を定義する際に、次の語を使用しないでください。

表 320. 禁止語

語	一般的な意味	禁止場所
con	コンソール	マシン表示名、暗号化キー、リポジトリ、パスの説明
prn	プリンタポート	マシン表示名、暗号化キー
aux	補助ポート	マシン表示名、暗号化キー
nul	ヌル値	マシン表示名、暗号化キー
com1, com2... ~ com9	通信ポート	マシン表示名、暗号化キー
lpt1, lpt2... ~ lpt9	ラインプリンタ端末ポート	マシン表示名、暗号化キー、リポジトリ、パスの説明

保護対象マシン

保護対象マシン ("エージェント" と呼ばれることもあります) は、Rapid Recovery Core によって保護されている物理コンピュータまたは仮想マシンのことです。バックアップデータは、保護対象マシンから Core で指定されたリポジトリに事前定義された保護間隔を使用して送信されます。ベースイメージはすべてのデータ（オペレーティングシステム、アプリケーション、および設定を含む）をリカバリポイントに送信します。後続の各増分スナップショットは、保護対象マシンの指定されたディスクボリューム上の変更されたブロックのみをコミットします。ソフトウェアベースの保護対象マシンには、Rapid Recovery エージェントのソフトウェアがインストールされています。一部の仮想マシンはエージェントなしでも保護できますが、いくつかの制限があります。

クォーラム

フェイルオーバークラスタの場合、特定のクラスタが稼働し続けるためにオンラインである必要のあるエレメントの数です。ここで言うエレメントとは、クラスタノードを指します。この用語は、クラスタのリカバリに必要な構成データを維持するために選択されたクォーラム対応リソースを意味する場合もあります。このデータには、クラスタデータベースに適用されたすべての変更に関する詳細が含まれています。クォーラムリソースは、クラスタノードのすべてが最近のデータベース変更にアクセスできるようにするため、他のクラスタリソースからもアクセス可能であるのが一般的です。デフォルトで、クォーラムリソースはサーバークラスタごとに1つのみです。特定のクォーラム設定（フェイルオーバークラスタ用設定）により、クラスタの動作を停止させる障害数の超過ポイントが決定されます。

リカバリポイント

リカバリポイントは、さまざまなディスクボリュームのスナップショットの集合です。たとえば、C:、D:、および E: です。

リカバリポイントのみのマシン

リカバリポイントのみのマシンは、以前に Core で保護されていて削除されたマシンからのリカバリポイントを Core 上で表現します。レプリケーションを削除してもリカバリポイントを保持している場合、この結果、リカバリポイントのみのマシンになります。この情報は、ファイルレベルで表示し、回復することができます。リカバリポイントのみのマシンを使用して BMR を実行したり、またはフル ボリュームを復元したりすることはできません。リカバリポイントのみのマシンにデータを追加することもできません。

リモート Core

リモート Core は、非 Core マシンからローカルマウントユーティリティまたは中央管理コンソールを使用してアクセスされる Rapid Recovery Core を表します。

レプリケーション

レプリケーションは、災害復旧を目的として1つの Rapid Recovery Core からリカバリポイントをコピーして、それらを別の Rapid Recovery Core に転送するプロセスです。この処理には、2 つ以上の Core 間で、ソースとターゲットのペアの関係が必要です。レプリケーションは保護対象マシンごとに管理されます。ソース Core で保護またはレプリケートされる任意のマシン（またはすべてのマシン）をターゲット Core にレプリケートするように設定できます。これは、ターゲットコアにコピーされたリカバリポイントです。

リポジトリ

リポジトリは、ベースイメージと、Rapid Recovery Core 保護対象マシンから取得された増分スナップショットの集まりです。リポジトリは、高速なプライマリストレージデバイス上に作成する必要があります。DVM リポジトリのストレージ場所には Core マシンのローカルディレクトリを選択することができます（その場合、サポートされている Windows OS 上にのみホストされます）。直接接続されているストレージ、ストレージエリアネットワークを、または適切なレートのネットワークに接続されたサーバを使用できます。

REST API

REST（Representational State Transfer）は拡張性のために設計された単純なステートレスソフトウェアアーキテクチャです。Rapid Recovery は、このアーキテクチャを API で使用し、特定の機能やタスクをカスタマイズおよび自動化します。Core 機能および保護対象（エージェント）マシン用の個別の REST API のセットがあります。

リストア

マシン上の1つ以上のストレージボリュームを Rapid Recovery Core に保存されたリカバリポイントから復元するプロセスのことをリストアといいます。これは以前、ロールバックと呼ばれていました。

保持

保護対象マシンのバックアップスナップショットが Rapid Recovery Core で保存される期間を定義します。保持ポリシーは、ロールアッププロセスを通じてリカバリポイントに適用されます。

rollup

ロールアッププロセスは、毎晩行われる内部メンテナンス手順で、古いリカバリポイントを無効化し、排除することによって保持ポリシーを適用します。Rapid Recovery では、ロールアップがメタデータ操作専用に削減されます。

シーディングレーでいんぐ

レプリケーションでは、保護対象 Agent の重複排除されたベースイメージと増分スナップショットの初回の送信のことであり、合計のデータ容量は数百～数千ギガバイトに及ぶことがあります。初回のレプリケーションは、外部メディアを使用してターゲット Core にシードすることが可能で、データの規模が大きい場合や、サイトのリンクが遅い場合に便利です。

サーバークラスタ

「[Windows フェイルオーバークラスタ](#)」を参照してください。

SharePoint バックアップ

SharePoint バックアップとは、システム障害発生後、SharePoint サーバー上のデータをリストアおよびリカバリするために使用するデータのコピーのことです。SharePoint バックアップから、SharePoint ファーム全体のリカバリ、またはファームの1つ以上のコンポーネントのリカバリを実行できます。

シングルコピークラスタ

共有ストレージフェイルオーバークラスタソリューションで、クラスタ内のノード間で共有されるストレージにあるストレージグループの単一コピーを使用します。これは、Exchange 2007 で利用できる2つのクラスタ化メールボックスサーバー導入タイプの1つです。

Smart Agent

Rapid Recovery Smart Agent は、Rapid Recovery Core で保護されるマシンにインストールされます。ディスクボリュームで変更されたブロックを追跡し、変更されたブロックのスナップショットをあらかじめ定義された保護間隔で作成します。

スナップショットすなっぶしょっと

スナップショットは、アプリケーションを実行したままで、指定のポイントのディスクボリュームの状態を取得し、保存できる機能を定義する、一般的な業界用語です。停止またはシステム障害が原因でシステムリカバリが必要な場合、スナップショットは重要です。Rapid Recovery のスナップショットはアプリケーションアウェアです。つまり、すべての未処理トランザクションと実行中のトランザクションのログが完了し、キャッシュがフラッシュされたあと、スナップショットが作成されます。Rapid Recovery は Microsoft Volume Shadow Services (VSS) を使用して、クラッシュ整合性のあるアプリケーションスナップショットを容易に作成できるようにします。

SQL アタッチ可否

SQL アタッチの可否は、すべての SQL リカバリポイントにエラーがなく、障害発生時にバックアップ用に使用できることを確認するために Rapid Recovery Core 内で実行されるテストです。

SQL バックアップ

SQL バックアップとは、システム障害発生後、SQL サーバー上のデータをリストアおよびリカバリするために使用するデータの複製のことです。SQL バックアップから、SQL データベース全体のリカバリ、または SQL データベースの 1 つ以上のコンポーネントのリカバリを実行できます。

SQL 差分バックアップ

データベース差分バックアップとは、SQL データベースの前のフルバックアップ以降に行われたデータ変更の累積複製のことです。差分バックアップは通常、フルバックアップよりも作成所要時間が短くて済むため、データベースのリカバリに必要なトランザクションログの数も少なくなります。

ターゲット Core

ターゲット Core (Rapid Recovery と呼ばれることもあります) は、レプリケートされたデータをソース Core から受け取る Rapid Recovery Core です。

Transport Layer Security

Transport Layer Security (TLS) は、インターネット経由の通信セキュリティを確保するために設計された、最新の暗号化ネットワークプロトコルです。このプロトコルは、インターネット技術標準化委員会で定義され、Secure Sockets Layer (SSL) に代わるものです。SSL という用語は引き続き一般的に使用され、プロトコルは相互運用可能です (SSL サーバーと通信するために TLS クライアントをダウングレードできます)。

True Scale

True Scale は、スケーラブルな Rapid Recovery のアーキテクチャです。

Universal Recovery

Rapid Recovery Universal Recovery テクノロジーは、マシンのリストアに無限の柔軟性をもたらします。このテクノロジーにより、選択したあらゆる物理または仮想プラットフォームへの一体的リカバリ、またはこれらのプラットフォームからの一体的リカバリに加えて、あらゆる物理または仮想ソースから仮想マシンへの増分リカバリアップデートも実行できます。また、アプリケーションレベル、アイテムレベル、およびオブジェクトレベル (個々のファイル、フォルダ、電子メール、予定表アイテム、データベースおよびアプリケーション) でリカバリを実行できます。

Verified Recovery

Verified Recovery テクノロジーは、自動リカバリテストおよびバックアップ検証の実行に使用されます。このテクノロジーは、さまざまなファイルシステムおよびサーバーをサポートします。

Virtual Standby

Virtual Standby は、保護対象マシンのクローン仮想マシンを作成するプロセスです。元のソースマシンには物理または仮想を使用できますが、製品は常に仮想です。Virtual Standby は、必要に応じて 1 回のみ作成することも、ブータブル VM の作成に関する要件を定義して、ソースの保護対象マシン上で各スナップショットが取得された後に要件を継続的に更新することもできます。

ボリュームマネージャ

Rapid Recovery ボリュームマネージャは、オブジェクトを管理し、それを論理ボリュームとして保存し、表示します。この機能は、動的パイプラインアーキテクチャを活用して、TruScale のスケーラビリティ、並列処理、および最小 I/O レイテンシで高スループットを実現する非同期入力および出力 (I/O) モデルを提供します。

ホワイトラベル

Rapid Recovery では、バックアップサービスおよびディザスタリカバリサービスのプロバイダが独自の名前で Rapid Recovery をホワイトラベル化またはリブランド化して、独自の製品またはサービスとして販売または配布できます。

Windows フェイルオーバークラスタ

アプリケーションおよびサービスの可用性を拡大するために、連携して動作する個々のコンピュータのグループ。クラスタ化されたサーバー（ノードと呼ばれます）は物理ケーブルおよびソフトウェアで接続されます。クラスタノードのいずれかに障害が発生すると、別のノードがサービスの提供を開始します（フェイルオーバーとして知られる処理です）。サービスの中断は最小に抑えられます。Rapid Recovery では、SQL Server および Exchange Server の多数のクラスタタイプを保護できます。